

	Identifikationskartensysteme Branchenübergreifende elektronische Geldbörse Teil 3: Datenelemente und Datenaustausch Deutsche Fassung EN 1546-3:1999	DIN EN 1546-3
--	--	---

ICS 35.240.15

Identification card systems – Inter-sector electronic purse –
Part 3: Data elements and interchanges;
German version EN 1546-3:1999

Systèmes de cartes d'identification – Porte-monnaie électronique
intersectoriel – Partie 3: Données et interfaces;
Version allemande EN 1546-3:1999

Die Europäische Norm EN 1546-3:1999 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“.

Für die in Abschnitt 2 zitierten Normen wird im Folgenden auf die entsprechenden Deutschen Normen hingewiesen:

EN 726-3	siehe DIN EN 726-3
EN 1546-1	siehe DIN EN 1546-1
EN 1546-2	siehe DIN EN 1546-2
EN 1546-4	siehe DIN EN 1546-4
ISO 4217	siehe DIN EN 24217
ISO/IEC 7812-1	siehe DIN EN ISO/IEC 7812-1

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN 24217, *Codes für Währungen und Zahlungsmittel (ISO 4217:1990); Deutsche Fassung EN 24217:1993.*

DIN EN ISO/IEC 7812-1, *Identifikationskarten – Kennzeichnung eines Kartenausgebers – Teil 1: Nummerierungssystem (ISO/IEC 7812-1:1993); Deutsche Fassung EN ISO/IEC 7812-1:1995.*

Fortsetzung 70 Seiten EN

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

– Leerseite –

Deutsche Fassung

Identifikationskartensysteme

Branchenübergreifende elektronische Geldbörse

Teil 3: Datenelemente und Datenaustausch

Identification card systems –
Inter-sector electronic purse –
Part 3: Data elements and interchanges

Systèmes de cartes d'identification –
Porte-monnaie électronique intersectoriel –
Partie 3: Données et interfaces

Diese Europäische Norm wurde von CEN am 20. Mai 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.

CEN

EUROPÄISCHES KOMITEE FÜR NORMUNG

European Committee for Standardization

Comité Européen de Normalisation

Zentralsekretariat: rue de Stassart 36, B-1050 Brüssel

Inhalt

	Seite		Seite
Vorwort	2	Anhang C (informativ) Eine PSAM-Realisierung	36
1 Anwendungsbereich	3	C.1 Allgemeine Bemerkungen	36
2 Normative Verweisungen	3	C.2 PSAM-spezifische Datenelemente ...	36
3 Definitionen	4	C.3 Eine Dateistruktur für ein PSAM	40
4 Symbole und Abkürzungen	5	C.4 Anwendungsspezifische Befehle an das PSAM	44
5 Allgemeine Angaben	7	Anhang D (informativ) In IEP-Systemen verwendete BeendigungsCodes .	60
5.1 Einführung	7	D.1 Liste aller BeendigungsCodes	60
5.2 Benutzerbestimmte Daten	7	D.2 Verweis auf von IEPs verwendete BeendigungsCodes	63
6 IEP-Datenelemente	8	D.3 Verweis auf von PSAMs verwendete BeendigungsCodes	64
6.1 Allgemeine Bemerkungen	8	Anhang E (informativ) Datenelemente für DES	66
6.2 Liste der Datenelemente	8	E.1 Allgemeine Bemerkungen	66
7 IEP-Befehle und -Antworten	13	E.2 Liste der Datenelemente	66
7.1 Allgemeine Bemerkungen	13	Anhang F (informativ) Datenelemente für RSA	67
7.2 Auswahl der Anwendung	14	F.1 Allgemeine Bemerkungen	67
7.3 Anwendungsspezifische Befehle an die IEP	16	F.2 Liste der Datenelemente	67
Anhang A (informativ) Beispiele für weitere IEP-Befehle	24	Anhang G (informativ) Datenelemente für DSS	68
A.1 Applikationsspezifische Befehle zur IEP	24	G.1 Allgemeine Bemerkungen	68
Anhang B (informativ) Beispiel für eine IEP-Dateistruktur	28	G.2 Liste der Datenelemente	68
B.1 Allgemeine Bemerkungen	28	Literaturverzeichnis	70
B.2 Begriffe	28		
B.3 Allgemeine Bemerkungen	29		
B.4 Datenelemente	29		
B.5 Logisches Modell für eine IEP	31		
B.6 Allgemeine Datendateien	32		
B.7 Anwendungsspezifische Dateien	32		

Vorwort

Diese Europäische Norm wurde vom Technischen Komitee CEN/TC 224 „Maschinenlesbare Karten und zugehörige Geräteschnittstellen und Verfahren“ 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 Januar 2000, und etwaige entgegenstehende nationale Normen müssen bis Januar 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: Datenobjekte

1 Anwendungsbereich

Dieser Teil von EN 1546 liefert die notwendigen Informationen über die zu speichernden und auszutauschenden Datenelemente, damit IEP-Systeme, die dieser Norm entsprechen, zu einer Zusammenarbeit fähig sind.

Die Transaktionstypen, die IEPs nach EN 1546-1 (Definitionen, Konzepte und Strukturen) und EN 1546-2 umfassen, werden in diesem Teil von EN 1546 behandelt.

Formate für Befehle und Antworten, die die detaillierten Definitionen einzelner Datenelemente enthalten, werden definiert, während der genaue Weg, wie die Daten in den Komponenten gespeichert werden können, nicht im Anwendungsbereich von EN 1546 liegt.

Es sind Verfahren für die Auswahl der IEP-Anwendung definiert.

Beispiele für Formate von Befehlen und Antworten zur Implementierung von informativen Transaktionstypen, wie sie in EN 1546-2 definiert sind, sind im Anhang A enthalten.

Eine mögliche Dateistruktur für die IEP und Verfahren zum Auslesen des Inhalts von Dateien werden nicht definiert, soweit dies für die Fähigkeit zur Zusammenarbeit nicht kritisch ist. Im Anhang B wird jedoch ein Beispiel angegeben.

Die Befehlsverarbeitung innerhalb der Empfangseinrichtungen wird in diesem Teil von EN 1546 nicht definiert, soweit sie vom Sicherheitsstandpunkt aus in EN 1546-2 (Sicherheitsarchitektur) behandelt wird.

Die Schnittstelle und die Funktionalität der IEP werden genau festgelegt, sofern die Einrichtung, die die IEP realisiert, entscheidend für das Erreichen der Fähigkeit zur Zusammenarbeit zwischen verschiedenen IEP-Systemen ist. Ein Beispiel einer PSAM-Realisierung ist im informativen Anhang C angegeben, während LSAMs und PPSAMs als nicht zu diesem Teil von EN 1546 gehörend betrachtet werden.

2 Normative Verweisungen

Dieser europäische Standard übernimmt 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 gelten spätere Änderungen oder Überarbeitungen dieser Publikationen für diesen europäischen Standard nur, falls sie durch Änderung oder Überarbeitung eingearbeitet worden sind. Bei undatierten Verweisungen gilt die letzte Ausgabe der in Bezug genommenen Publikation.

EN 726-3, *Endgeräte (TE) – Anforderungen an IC-Karten und Endgeräte im Telekommunikationsbereich – Teil 3: Applikationsunabhängige Anforderungen an die Karte.*

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

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

EN 1546-4, *Identifikationskartensysteme – Branchenübergreifende elektronische Geldbörse – Teil 4: Geräte.*

ISO 4217, *Codes for representation of currencies and funds.*

ISO/IEC 7812-1:1993, *Identification cards – Numbering system.*

ISO/IEC 7816-3:1989, *Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols.*

ISO/IEC 7816-4:1995, *Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 4: Inter-industry commands for interchange.*

ISO/IEC 7816-5:1994, *Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 5: Registration system for applications in IC cards.*

ISO/IEC 7816-6:1996, *Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 6: Inter-industry data elements.*

ISO/IEC 9797, *Data cryptographic techniques – Data integrity mechanism using a cryptographic check function employing a block cipher algorithm.*

3 Definitionen

Für diese Europäische Norm gelten folgende Definitionen:

3.1

Aktivierung

siehe EN 1546-1

3.2

Beendigungscode

siehe EN 1546-2

3.3

Deaktivierung

siehe EN 1546-1

3.4

benutzerbestimmte Daten

optionale Datenelemente, die entsprechend der Definition des Börsenanbieters zu Nachrichten hinzugefügt werden

3.5

IEP-Saldo

siehe EN 1546-1

3.6

IEP-System

siehe EN 1546-1

3.7

Aufladen

siehe EN 1546-1

3.8

Aufladeeinrichtung

siehe EN 1546-1

3.9

Aufladeprotokoll

siehe EN 1546-1

3.10

Auflade-SAM

siehe EN 1546-1

3.11

Message Authentication Code

siehe EN 1546-2

3.12

Sperrliste

siehe EN 1546-1

3.13

Zahlung

siehe EN 1546-1

3.14

Zahlungseinrichtung

siehe EN 1546-1

3.15

Zahlungsprotokoll

siehe EN 1546-1

3.16

Zahlungs-SAM

siehe EN 1546-1

3.17

Börsenanbieter

siehe EN 1546-1

3.18

Börsenanbieter-SAM

siehe EN 1546-1

3.19

Anwendungssicherheitsmodul

siehe EN 1546-1

3.20

Signatur

siehe EN 1546-2

3.21

Endsumme

siehe EN 1546-1

Um die für ein allgemeines IEP-System spezifischen Benennungen in dieser gesamten Europäischen Norm hervorzuheben, beginnen diese Benennungen (im englischen Original) mit großen Anfangsbuchstaben, z. B. Purse Provider (Börsenanbieter).

4 Symbole und Abkürzungen

K	Verkettung (von Datenelementen)
A	Vektor (Bezeichner für eine geordnete Menge von Datenelementen)
'0'.. '9' und 'A'.. 'F'	die sechzehn Hexadezimalzeichen
AID	Application Identifier <i>Anwendungsbezeichner</i>
ALG	Algorithm <i>Algorithmus</i>
AM	Authentication Mode <i>Authentisierungsmodus</i>
AP	Application Profile <i>Anwendungsprofil</i>
APDU	application protocol data unit <i>Dateneinheit des Anwendungsprotokolls</i> (siehe ISO/IEC 7816-4)
ATR	Answer-To-Reset
BAL	Balance <i>Saldo</i>

BALmax	Maximum Balance <i>maximaler Saldo</i>
BCD	Binary Coded Decimal
CC	Completion Code <i>Beendigungscode</i>
CURR	Currency <i>tatsächliche Währung</i>
DACT	Activation Date <i>Aktivierungsdatum</i>
DD	Discretionary Data <i>benutzerbestimmte Daten</i>
DDEA	Deactivation Date <i>Deaktivierungsdatum</i>
DES	Data Encryption Standard (cryptographic algorithm) <i>kryptographischer Algorithmus</i>
DEXP	Expiry Date <i>Ablaufdatum</i>
DSS	Digital Signature Standard (cryptographic algorithm) <i>kryptographischer Algorithmus</i>
FCI	File Control Information <i>Dateisteuerinformation</i>
IC	Integrated Circuit <i>integrierte Schaltung</i>
ICC	IC Card <i>Chipkarte</i>
ID	Identifier <i>Bezeichner</i>
IEP	Inter-Sector Electronic Purse <i>branchenübergreifende elektronische Geldbörse</i>
IK	Key Information <i>Schlüsselinformation</i>
LDA	Load Device Application <i>Aufladeeinrichtungsanwendung</i>
LSAM	Load SAM <i>Auflade-SAM</i>
LSB	Least Significant Byte <i>niedrigstwertiges Byte</i>
M	Amount <i>Transaktionsbetrag</i>
MAC	Message Authentication Code <i>Nachrichtenbeglaubigungscode</i>
MSB	Most Significant Byte <i>höchstwertiges Byte</i>
MTOT	Total Amount <i>Endsummenbetrag der Transaktion</i>
NT	Transaction Number <i>Transaktionsnummer</i>
PAR	Parameter

PDA	Purchase Device Application <i>Zahlungseinrichtungsanwendung</i>
PIN	Personal Identification Number <i>persönliche Identifikationsnummer</i>
PIX	Proprietary Application Identifier Extension <i>anwendereigene Erweiterung des Anwendungsbezeichners</i>
PP	Purse Provider <i>Börsenanbieter</i>
PPSAM	Purse Provider SAM <i>Börsenanbieter-SAM</i>
PSAM	Purchase SAM <i>Zahlungs-SAM</i>
R	Random Number <i>Zufallszahl</i>
RFU	Reserved For Future Use <i>für eine spätere Anwendung freigehalten</i>
RID	Registered Identifier <i>registrierter Bezeichner</i>
RSA	Rivest, Shamir and Adleman (cryptographic algorithm) <i>kryptographischer Algorithmus</i>
SAM	Secure Application Module <i>Anwendungssicherheitsmodul</i>
SW	Status Word <i>Statusbyte</i>
TPDU	Transmission Protocol Data Unit <i>Dateneinheit des Anwendungsprotokolls (siehe ISO/IEC 7816-4)</i>

5 Allgemeine Angaben

5.1 Einführung

Alle Definitionen von Datenelementen und Nachrichten, die für IEP-Anwendungen verwendet werden, betreffen nur die Schnittstellenebene, sofern dies für die Zusammenarbeit zwischen verschiedenen IEP-Systemen erforderlich ist.

Andere Datenelemente, wie zum Beispiel kryptographische Schlüssel, werden benötigt, aber soweit keine Notwendigkeit besteht, diese bei normalem Betrieb der IEP-Anwendung zur Schnittstelle der ICC zu senden, ist die Codierung und die mögliche Speicherung in einer oder mehreren internen Dateien für unterschiedliche Realisierungen offengelassen.

5.2 Benutzerbestimmte Daten

Um in bestimmten Realisierungen von IEP-Systemen die Verwendung zusätzlicher Daten zu ermöglichen, dürfen Befehle und Antworten benutzerbestimmte Daten innerhalb der Nachricht enthalten.

Die Verarbeitung derartiger benutzerbestimmter Daten, z. B. wie benutzerbestimmte Daten in Dateien aktualisiert werden, die auf benutzerbestimmten Daten beruhen und die in Befehlen empfangen werden, gehört nicht zum Anwendungsbereich dieser Norm.

Aus Gründen der Fähigkeit zur Zusammenarbeit sollte keine Einrichtung von solchen an sie gesendete benutzerbestimmten Daten abhängen, z. B. sollte eine IEP, wenn sie in einer Zahlungseinrichtung verwendet wird, die keine benutzerbestimmten Daten sendet, noch in der Lage sein, normale Zahlungstransaktionen durchzuführen. Auf dieselbe Weise muss die PDA/PSAM alle benutzerbestimmten Daten ablegen, wenn sie nicht verarbeitet werden können, und sie muss noch in der Lage sein, die Transaktion durchzuführen.

6 IEP-Datenelemente

6.1 Allgemeine Bemerkungen

Für jedes Datenelement dürfen folgende Deskriptoren vorhanden sein:

- Verweis (wenn vorhanden, bezieht er sich auf eine bestehende Norm, die ein ähnliches Datenelement definiert);
- Zweck (eine Kurzbeschreibung der Verwendung des angegebenen Datenelements);
- Format (gibt die empfohlene vorgegebene Größe des Datenelements und möglicherweise ein symbolisches Format an, das zur Beschreibung des Inhalts verwendet wird);
- Inhalt (die genaue Definition für die Codierung des Datenelements);
- Bemerkungen (andere Angaben).

6.2 Liste der Datenelemente

In diesem Abschnitt werden Datenelemente definiert, die die IEP unterstützen und die zu oder von der IEP übertragen werden. Datenelemente, die nicht in verpflichtenden Befehlen verwendet werden, sind wahlfrei.

Datenelemente können wahlfrei als Datenobjekte unter Verwendung von ASN.1-BER (Notation Eins für darstellungsunabhängige Syntax, grundlegende Codierungsregeln) verwaltet werden. Dieser Mechanismus wird in EN 1546-4 beschrieben.

6.2.1 AID_{IEP} (Anwendungsbezeichner für eine IEP)

Verweis: ISO/IEC 7816-5, ISO/IEC 7816-6 (Identifizierungskennzeichen '4F')

Zweck: Um der PDA zu ermöglichen, die IEP-Anwendung vor Durchführung der in dieser Europäischen Norm definierten Transaktionen, z.B. Zahlung und Aufladen, auszuwählen. Wenn die Karte eine implizite Auswahl verwendet, ist der AID in den Historical Bytes der Answer-to-reset-Nachricht enthalten.

Format: 5 – 16 Bytes.

Inhalt: RID || PIX, wobei RID der globale, registrierte 5 Byte-Bezeichner nach ISO/IEC 7816-5 ist und PIX (0 – 11 Bytes) für eine freie Verwendung vom Börsenanbieter zur Verfügung steht.

Bemerkungen: AID_{IEP} wird als Dateiname für DF_{IEP} verwendet, um eine leichte Auswahl der IEP-Anwendung in Komponenten mit Mehrfachanwendung zu ermöglichen.

6.2.2 ALG_{IEP} (von einer IEP verwendeter kryptographischer Algorithmus)

Zweck: Ein in der IEP gespeicherter Wert, der eindeutig den von der IEP verwendeten kryptographischen Algorithmus identifiziert (einschließlich der Betriebsarten usw.), der für die Authentisierung und/oder Verschlüsselung zwischen IEP, PSAM, LSAM und PPSAM verwendet wird.

Format: 1 Byte.

Inhalt: Die Codierung liegt im Ermessen des Börsenanbieters.

Bemerkungen: Jeder Wert muss implizit alle die Informationen enthalten, die zur Realisierung des Algorithmus benötigt werden, z.B. den Algorithmentyp (wenn mehrere bestehen) und die Schlüssellänge.

6.2.3 AM_{IEP} (von einer IEP vorgeschriebener Authentisierungsmodus)

Zweck: Zur Identifizierung des von der IEP für Zahlungstransaktionen vorgeschriebenen Authentisierungsmodus. Weiterhin legt es die Anforderung für S₁ fest und eine signierte Quittung vom PSAM am Ende der Transaktion.

Format: 1 Byte.

Inhalt: Die möglichen Werte werden in Tabelle 1 definiert.

Tabelle 1 – Codierung von AM_{IEP}

b8	b7	b6	b5	b4	b3	b2	b1	Bedeutung
x	–	–	–	–	–	–	–	Behandlung von S_1 :
0	–	–	–	–	–	–	–	– S_1 wird von der IEP nicht gesendet
1	–	–	–	–	–	–	–	– S_1 wird von der IEP gesendet
–	x	–	–	–	–	–	–	Erfordernis einer signierten Quittung:
–	0	–	–	–	–	–	–	– signierte Quittung nicht erforderlich
–	1	–	–	–	–	–	–	– signierte Quittung erforderlich
–	–	–	–	–	–	x	x	Von der IEP vorgeschriebener Authentisierungsmodus:
–	–	–	–	–	–	0	0	– RFU
–	–	–	–	–	–	0	1	– Einweg-Authentisierung
–	–	–	–	–	–	1	0	– Zweiweg-Authentisierung
–	–	–	–	–	–	1	1	– Dualmodus-Authentisierung
–	–	x	x	x	x	–	–	RFU

Bemerkungen: Die freigehaltenen Bits (b6 – b3) müssen auf NULL gesetzt werden.

6.2.4 AP_{IEP} (Anwendungsprofil einer IEP)

Zweck: Zur Identifizierung folgender wahlfreier Funktionen, die in einer IEP realisiert sind:

- Möglichkeit der Ausführung von Zahlungstransaktionen mit festen Buchungsstufen;
- Zahlungsabbruch/IEP-Saldowiederherstellung;
- Währungsumrechnung;
- Aktualisierung von Anwendungsparametern;
- Verwendung von ASN.1-BER-Formaten.

Format: 2 Bytes.

Inhalt: Die möglichen Werte für das erste Byte werden in Tabelle 2 definiert. Alle Bits im zweiten Byte sind für eine spätere Verwendung freigehalten.

Tabelle 2 – Codierung von AP_{IEP}

b8	b7	b6	b5	b4	b3	b2	b1	Bedeutung
x	–	–	–	–	–	–	–	Zahlung mit festen Buchungsstufen
0	–	–	–	–	–	–	–	– feste Buchungsstufen nicht zulässig
1	–	–	–	–	–	–	–	– feste Buchungsstufen zulässig
–	x	–	–	–	–	–	–	Zahlungsabbruch/IEP-Saldowiederherstellung
–	0	–	–	–	–	–	–	– Abbruch nicht zulässig
–	1	–	–	–	–	–	–	– Abbruch zulässig
–	–	x	–	–	–	–	–	Währungsumrechnungsfunktion
–	–	0	–	–	–	–	–	– Währungsumrechnung nicht zulässig
–	–	1	–	–	–	–	–	– Währungsumrechnung zulässig
–	–	–	x	–	–	–	–	Aktualisierungsfunktion der IEP-Parameter
–	–	–	0	–	–	–	–	– Aktualisierung nicht zulässig
–	–	–	1	–	–	–	–	– Aktualisierung zulässig
–	–	–	–	x	x	x	–	Verwendung des ASN.1-BER-Formates
–	–	–	–	0	0	0	–	– feste Formate
–	–	–	–	0	0	1	–	– siehe EN 1546-4
–	–	–	–	0	1	0	–	– siehe EN 1546-4
–	–	–	–	0	1	1	–	– siehe EN 1546-4
–	–	–	–	1	0	0	–	– siehe EN 1546-4
–	–	–	–	1	0	1	–	– siehe EN 1546-4
–	–	–	–	1	1	0	–	– siehe EN 1546-4
–	–	–	–	1	1	1	–	– siehe EN 1546-4
–	–	–	–	–	–	–	x	RFU

Bemerkungen: Das reservierte Bit (b1) muss auf NULL gesetzt werden.



6.2.5 BAL_{IEP} (Saldo einer IEP)

Verweis: ISO 4217 betrifft Währungscode und Währungsexponent.

Zweck: Definiert den tatsächlichen Wert in der IEP. Er kann nur zusammen mit CURR_{IEP} interpretiert werden.

Format: 4 Bytes.

Inhalt: Eine vorzeichenlose ganze Dualzahl, die den tatsächlichen Saldo definiert. Der Saldo wird in der kleinsten Einheit der entsprechenden Währung, wie im Währungscode (CURR_{IEP}) festgelegt, dargestellt.

Bemerkungen: Dieses Datenelement kann durch BALmax_{IEP} begrenzt werden.

6.2.6 BALmax_{IEP} (maximaler Saldo einer IEP)

Verweis: ISO 4217 betrifft Währungscode und Währungsexponent.

Zweck: Definiert den maximalen Wert einer vorgegebenen IEP, bis zu dem ein Aufladen zulässig ist. Er kann nur zusammen mit CURR_{IEP} interpretiert werden. Kann aufgrund nationaler Gesetzgebung oder aufgrund von Anforderungen des Börseninhabers notwendig sein. Kann unter Verwendung einer IEP-Kontrolle ausgelesen werden. Er kann mit der Transaktion IEP-Parameter Aktualisieren aktualisiert werden und muss als Teil der Währungsumrechnungstransaktion aktualisiert werden.

Format: 4 Bytes.

Inhalt: Eine vorzeichenlose ganze Dualzahl, die den maximalen Saldo definiert.

6.2.7 CC_{IEP} (Beendigungscode einer IEP)

Verweis: ISO/IEC 7816-3 und ISO/IEC 7816-4.

Zweck: Das Ergebnis der Aktionen innerhalb einer IEP, die einen vorgegebenen Befehl ausführt. Er wird in der Antwort übertragen, um anzuzeigen, ob (ein) Fehler aufgetreten (ist) sind (und welche).

Format: Es werden die beiden Zustandsbytes SW1 und SW2 verwendet.

Inhalt: Die möglichen Werte für jeden Befehl werden in Abschnitt 7.3 definiert, und ein Überblick ist in Anhang D (informativ) angegeben.

6.2.8 CURR_{IEP}/CURR_{LDA}/CURR_{PDA} (tatsächliche Währung für eine IEP, LDA oder PDA)

Verweis: ISO 4217 und ISO/IEC 7816-6 (Identifizierungskennzeichen '5F2A' und '5F36').

Zweck: Zur Identifizierung der Währung des Saldos einer angegebenen IEP oder der von der LDA oder PDA festgelegten Währung zusammen mit einem Betrag in einer Auflade- oder Zahlungstransaktion. Weiterhin zur Angabe der Anzahl von Dezimalstellen in Betragsfeldern.

Format: 3 + 1 Stelle (2 + 1 Byte).

Inhalt: Nach ISO 4217: Die ersten beiden Bytes enthalten den numerischen Währungscode und das letzte Byte zeigt die Stellung des Dezimalpunktes an (die Anzahl der Dezimalstellen).

Bemerkungen: Die 4 höchstwertigen Bits im Währungscode müssen auf NULL gesetzt werden. Auf die beiden Teile dieses Datenelements darf einzeln zugegriffen werden.

6.2.9 DACT_{IEP} (Aktivierungsdatum einer IEP)

Verweis: ISO/IEC 7816-6 (Identifizierungskennzeichen '5F25').

Zweck: Um überprüfen zu können (unter Verwendung der IEP-Kontrolle), an welchem Datum die IEP aktiviert wurde.

Format: 6 Stellen (3 Byte) im Format YYMMDD.

Inhalt: YY: Die beiden niedrigstwertigen Stellen des Jahres der Aktivierung, in BCD codiert.

MM: Die Nummer des Monats der Aktivierung, in BCD codiert (Januar ist Monat Nummer 1).

DD: Die Nummer des Tages im Monat der Aktivierung, in BCD codiert.

Bemerkungen: Der Vorgabewert '000000' gibt an, dass die IEP noch nicht aktiviert wurde. Um Probleme mit dem Jahr 2000 zu vermeiden, müssen folgende Vereinbarungen gelten:

- a) Wenn das Jahr im Bereich von 1990 – 1999 liegt, muss YY im Bereich von '90' – '99' liegen.
- b) Wenn das Jahr im Bereich von 2000 – 2089 liegt, muss YY im Bereich von '00' – '89' liegen.
- c) Wenn das Jahr außerhalb dieser beiden Bereiche liegt, kann es mit diesem Datenelement nicht dargestellt werden.

6.2.10 DD (benutzerbestimmte Daten)

Zweck: Um realisierungsabhängige Daten zu ermöglichen, die an Befehle und Antworten angefügt werden.

Format: n Bytes.

Inhalt: Im Ermessen des Börsenanbieters.

6.2.11 DDEA_{IEP} (Deaktivierungsdatum einer IEP)

Zweck: Um identifizieren zu können, an welchem Datum die IEP deaktiviert wurde.

Format: Wie für DACT_{IEP} (siehe 6.2.9).

Inhalt: Wie für DACT_{IEP} (siehe 6.2.9).

Bemerkungen: Wie für DACT_{IEP} (siehe 6.2.9).

6.2.12 DEXP_{IEP} (Ablaufdatum einer IEP)

Verweis: ISO/IEC 7816-6 (Identifizierungskennzeichen '5F24').

Zweck: Das Ablaufdatum kann durch das jeweilige PSAM oder ein PPSAM in der Initialisierungsphase einer Aufladetransaktion, einer Zahlungstransaktion oder einer Aktualisierungstransaktion der IEP-Parameter geprüft werden, um Transaktionen unter Verwendung einer abgelaufenen Komponente zu verhindern.

Format: Wie für DACT_{IEP} (siehe 6.2.9).

Inhalt: Wie für DACT_{IEP} (siehe 6.2.9).

Bemerkungen: Wie für DACT_{IEP} (siehe 6.2.9).

6.2.13 ID_{IEP} (Bezeichner für eine IEP)

Zweck: Zur eindeutigen Identifizierung jeder IEP, die zum Börsenanbieter gehört.

Format: 5 Bytes.

Inhalt: Im Ermessen des Börsenanbieters.

Bemerkungen: Der IEP-Bezeichner muss für einen gegebenen Börsenanbieter einmalig sein und darf während der Lebensdauer der IEP nicht verändert werden.

6.2.14 ID_{LDA} (Bezeichner für eine LDA)

Zweck: Zur eindeutigen Identifizierung jedes Ladegeräts.

Format: 4 Bytes.

Inhalt: Im Ermessen des Börsenanbieters.

Bemerkungen: Der LDA-Bezeichner sollte einmalig sein.

6.2.15 ID_{PPSAM} (Bezeichner für ein PPSAM)

Zweck: Zur eindeutigen Identifizierung jedes PPSAM, das zum Börsenanbieter gehört.

Format: 4 Bytes.

Inhalt: Im Ermessen des Börsenanbieters.

Bemerkungen: Der PPSAM-Bezeichner muss für den gegebenen Börsenanbieter einmalig sein. Dieses Datenelement darf während der Lebensdauer des PPSAM nicht verändert werden.

6.2.16 ID_{PSAM} (Bezeichner für ein PSAM)

- Zweck:* Zur eindeutigen Identifizierung jedes PSAM, das zum Börsenanbieter gehört.
- Format:* 4 Bytes.
- Inhalt:* Im Ermessen des Börsenanbieters.
- Bemerkungen:* Der PSAM-Bezeichner muss für den gegebenen Börsenanbieter einmalig sein. Dieses Datenelement darf während der Lebensdauer des PSAM nicht verändert werden.

6.2.17 IK_{IEP}/IK_{PSAM}/IK_{PPSAM} (Schlüsselinformation für eine IEP, PSAM oder PPSAM)

- Zweck:* Um einer anderen Komponente die notwendigen Informationen zur Überprüfung oder Berechnung von Signaturen zu geben.
- Format:* Algorithmenabhängig.
- Inhalt:* Algorithmenabhängig.
- Bemerkungen:* Die Größe und der Inhalt von IK_{COMP} hängt vom verwendeten Algorithmus und vom angewendeten Schlüsselmanagementprogramm ab. Beispiele für die DES-, RSA- bzw. DSS-Algorithmen sind in den Anhängen E, F und G angegeben.

6.2.18 M_{PDA}/M_{LDA} (Transaktionsbetrag einer PDA oder LDA)

- Verweis:* ISO 4217 betrifft die Verwendung des Währungsexponenten.
- Zweck:* Um die beteiligten Komponenten über den Transaktionsbetrag zu informieren (Auflade-, Zahlungs- und Zahlungsabbruch-/IEP-Saldowiederherstellungstransaktionen).
- Format:* 4 Bytes.
- Inhalt:* Der Transaktionsbetrag als eine vorzeichenlose ganze Dualzahl codiert.
- Bemerkungen:* Der Transaktionsbetrag ist immer mit einem Währungscode und einem Währungsexponenten verbunden.

6.2.19 MTOT_{IEP} (Endsummenbetrag der Transaktion für eine Zahlung)

- Verweis:* ISO 4217 betrifft die Verwendung des Währungsexponenten.
- Zweck:* Zur Summierung der Beträge von Zahlungen mit festen Buchungsstufen in einem Endsummenwert für die Zahlungstransaktion.
- Format:* 4 Bytes.
- Inhalt:* Der Betrag in der durch CURR_{IEP} vorgegebenen Währung, durch den Währungsexponenten modifiziert, der ebenfalls in CURR_{IEP} definiert ist. Er ist als eine vorzeichenlose ganze Dualzahl codiert.

6.2.20 NT_{IEP}/NT_{PSAM} (Transaktionsnummer für eine IEP, ein PSAM)

- Verweis:* ISO/IEC 7816-6 (Identifizierungskennzeichen '5F32').
- Zweck:* Um als ein Bezeichner für eine spezielle Transaktion zu dienen (zusammen mit PP_{IEP} und IEP bzw. PP_{PSAM} und PSAM). Weiterhin, um als Challenge-Parameter für andere Komponenten, z. B. PSAMs, zu arbeiten.
- Format:* NT_{IEP}: 2 Bytes.
NT_{PSAM}: 4 Bytes.
- Inhalt:* Die 16- oder 32 Bit-Transaktionsnummer als eine vorzeichenlose ganze Dualzahl codiert.
- Bemerkungen:* NT_{IEP} wird bei jeder von der IEP initiierten Transaktion um eins erhöht. Die vergebene Zahl darf sich nicht wiederholen. NT_{PSAM} muss sich bei aufeinanderfolgenden Transaktionen ändern und dort im Ermessen des Börsenanbieters implementiert werden.

6.2.21 PAR (Parameterbezeichner für Aktualisierungen)

- Zweck:* Zur Identifizierung des zu aktualisierenden Datenelements.
- Format:* 2 Bytes.
- Inhalt:* Im Ermessen des Börsenanbieters.

6.2.22 PP_{IEP} (Bezeichner eines Börsenanbieters für eine IEP)

Verweis: ISO/IEC 7812-1.

Zweck: Zur eindeutigen Identifizierung, welcher Börsenanbieter die IEP ausgegeben hat.

Format: 6 Stellen (3 Bytes).

Inhalt: Nach ISO/IEC 7812-1, Abschnitt 4.2, als BCD-Ziffern codiert.

Bemerkungen: Wenn der Bezeichner des Ausgebers aus weniger als 6 Stellen besteht, muss der Bezeichner linksbündig ausgerichtet und mit angehängten hexadezimalen 'F's aufgefüllt werden.

6.2.23 R_{PPSAM}/R_{LDA} (von einem PPSAM oder einer LDA berechnete Zufallszahl)

Zweck: Um als Aufforderung vom PPSAM oder LDA an eine IEP zu dienen.

Format: 4 Bytes.

Inhalt: Zufallsbits.

Bemerkungen: Der zur Berechnung von R ausgewählte Algorithmus liegt nicht im Anwendungsbereich dieser Norm.

7 IEP-Befehle und -Antworten

7.1 Allgemeine Bemerkungen

7.1.1 Übereinstimmung mit ISO/IEC 7816-4

Die Nachrichtenstruktur usw., die in diesem gesamten Abschnitt verwendet wird, entspricht ISO/IEC 7816-4, Abschnitte 5.3, 5.4 und 5.5 in folgender Weise:

- eine IEP muss auf einen Befehl immer mit der entsprechenden Antwortmeldung antworten (auch in dieser Norm definiert). Wenn die Verarbeitung des Befehls nicht erfolgreich ist, darf die Antwort aus nur zwei Bytes (SW1 und SW2) bestehen, die den Grund dafür angeben, warum der Befehl zurückgewiesen wurde;
- die Nachrichten in dieser Norm definieren die APDUs (Dateneinheiten des Anwendungsprotokolls), wie sie in ISO/IEC 7816-4 verwendet werden. Diese APDUs müssen nach den in Anhang A (für T = 0) und Anhang B (für T = 1) von ISO/IEC 7816-4 aufgeführten Regeln auf die TPDUs (Dateneinheiten des Übertragungsprotokolls) abgebildet werden;
- das Klassenbyte, das für IEP-Befehle ausgewählt wurde ('80'), gibt an, dass die Befehlsnachricht anwendereigen ist, d. h. nicht von ISO/IEC 7816-4 behandelt wird. Es wird jedoch dieselbe Nachrichtenstruktur verwendet;
- eine Anzahl von Befehlsbytes (INS) wurde zugewiesen, um die anwendungsspezifischen Befehle zu identifizieren. Die Werte wurden außerhalb des Bereiches der von ISO, ETSI und EMV bereits definierten Codes ausgewählt;
- die Parameterbytes P1 und P2 sind von ISO/IEC 7816-4 nicht eingeschränkt und werden in einigen der anwendungsspezifischen Befehle als weiterführende Kennzeichner für das Befehlsbyte verwendet;
- die Codierung der Zustandsbytes (SW1 und SW2) entspricht hinsichtlich der allgemeinen Fehler-situation ISO/IEC 7816-4. Zusätzliche Werte der Zustandsbytes sind in Bereichen definiert, die nicht zum Anwendungsbereich von ISO/IEC 7816-4 gehören;
- geschützte Nachrichtenübermittlung nach ISO/IEC 7816-4 wird von IEPs nicht verwendet, da die Sicherheit ein integrierter Teil des Übertragungsprotokolls ist.

7.1.2 Längenfelder

In ISO/IEC 7816-4 sind kurze und lange Längenfelder in den Befehlen definiert, um die Länge der Parameter anzugeben, die im Befehl (falls vorhanden) übertragen werden, sowie die erwartete Länge der Antwort. Diese Längenfelder werden mit L_c bzw. L_e bezeichnet.

Wenn die Menge der benutzerbestimmten Daten groß ist, kann das kurze (1 Byte) Längenfeld nicht ausreichen, da aber sehr lange Nachrichten einen großen Nachteil für die Transaktionszeit mit sich

bringen würden, sind in dieser Norm die meisten Befehle darauf begrenzt, nur kurze Längenfelder zu verwenden.

Wenn öffentliche Schlüssel und entsprechende Zertifikate für öffentliche Schlüssel übertragen werden, sind lange Längenfelder zulässig, da die Datenmenge 255 Bytes überschreiten könnte, z. B. wenn der öffentliche Schlüssel einer IEP von verschiedenen Instanzebenen zertifiziert wird.

Mehrere in diesem Teil von EN 1546 definierte Datenelemente in den Befehlen und Antworten besitzen Längen, die von anderen Parametern, z. B. dem verwendeten Algorithmus, abhängen. Derartige Datenelemente werden mit einer Länge beschrieben, die „variabel“ ist. Die beteiligten Einrichtungen sind jedoch in der Lage, die Nachrichten zu analysieren, da sie über die Parameter informiert sind, die die tatsächliche Länge beeinflussen.

7.1.3 Allgemeine Beendigungscodes

Eine IEP muss entweder die zutreffenden Beendigungscodes SW1 und SW2 auf ein IEP-Kommando zurücksenden, wie sie in ISO/IEC 7816-4, Abschnitt 5.4.5, definiert sind, oder die IEP-Anwendung spezifiziert solche, wie sie für einige Kommandos in den folgenden Unterabschnitten dieses Standards definiert sind.

Tabelle 3 – Allgemeine Beendigungscodes

SW1	SW2	Bedeutung
'91'	'01'	Anwendung ist nicht aktiv
'91'	'06'	Anwendung wurde deaktiviert
'92'	'01'	Anwendung ist geschlossen ¹⁾
'95'	'8X'	Befehl außerhalb der Reihenfolge, gegenwärtiger Zustand ist X
1) Der Beendigungscode darf verwendet werden, wenn die IEP durch Verwendung einer PIN oder eines ähnlichen Mechanismus geschlossen wurde.		

7.1.4 Allgemeine Beendigungscodes

Eine zurückkommende Nachricht eines Kommandos besteht nur aus einem Beendigungscode, mit einer Ausnahme: die zurückkommende Nachricht auf das Kommando IEP-Gutschrift für Aufladen enthält zusätzlich zum Beendigungscode eine Signatur.

Die zurückkommenden Nachrichten sind hier nicht definiert.

7.2 Auswahl der Anwendung

Folgende zwei Verfahren für die Auswahl der IEP-Anwendung vor Durchführung der in EN 1546 definierten Transaktionen bestehen:

- direkte Auswahl der Anwendung, die von allen Karten unterstützt werden müssen;
- implizite Auswahl der Anwendung, die zusätzlich von Karten für eine Einfachanwendung unterstützt werden.

Die Verwendung der impliziten Auswahl für Karten für eine Einfachanwendung kann in einigen Fällen zu niedrigeren Transaktionszeiten führen, wie in Abschnitt 7.2.2 beschrieben.

Weitere Verfahren zur Anwendungsauswahl, die von der ICC unterstützt werden können, die in die (den) IEP-Anwendung(en) aufgenommen wird, gehören nicht zum Anwendungsbereich dieses Teils von EN 1546.

7.2.1 Direkte Anwendungsauswahl

Die ICC muss mindestens die direkte Anwendung (nach ISO/IEC 7816-4, Abschnitt 9.3.2) unterstützen, wobei entweder der vollständige AID oder der RID (die ersten fünf Bytes des AID) als Dateiname als Parameter für einen Select File-Befehl verwendet wird. Von der ICC muss in der Antwort zu diesem Befehl die Dateisteuerinformation (FCI) zurückgesendet werden.

Das Betriebssystem der ICC muss einen Kanal der gegenwärtig ausgewählten Anwendung halten und darf, während dieser ausgewählt ist, nur die Befehle zulassen, die für diese besondere Anwendung anwendbar sind.

Die Antwort zu Select File, wenn die ausgewählte Datei DF_{IEP} ist, muss nach Tabelle 4 codiert werden.

Tabelle 4 – Codierung der Antwort auf den Select File-Befehl für die Auswahl von DF_{IEP}

Feld	Wert	Obligatorisch/ wahlfrei	Länge (Bytes)
Identifizierungskennzeichen	'6F' (FCI)	O	1
Länge	hängt von der Anzahl der enthaltenen Datenobjekte ab	O	1
Identifizierungskennzeichen	'84' (DF-Name)	O	1
Länge	'05' – '10'	O	1
AI _{IEP}	Anwendungsbezeichner der IEP	O	5–16
Identifizierungskennzeichen	'A5' (anwendereigene Daten)	O	1
Länge	hängt von der Anzahl der enthaltenen Datenobjekte ab	O	1
Identifizierungskennzeichen	'87' (Anwendungsprioritätsanzeiger)	W	1
Länge	'01'	W	1
API	Anwendungsprioritätsanzeiger	W	1
Identifizierungskennzeichen	'9F38' (Datenobjektliste der Verarbeitungsoptionen)	W	2
Länge	hängt von der Anzahl der enthaltenen Datenobjekte ab	W	1
PDOL	Datenobjektliste der Verarbeitungsoptionen	W	n
Identifizierungskennzeichen	'BF0C' (benutzerbestimmte FCI-Daten des Ausgebers)	O	2
Länge	hängt von der Anzahl der enthaltenen Datenobjekte ab	O	1
Identifizierungskennzeichen	'C1' (Bezeichner des Börsenanbieters)	O	1
Länge	'03'	O	1
PP _{IEP}	Bezeichner des Börsenanbieters	O	3
Identifizierungskennzeichen	'C9' (Anwendungsprofil)	O	1
Länge	'02'	O	1
AP _{IEP}	Anwendungsprofil der IEP	O	2
Identifizierungskennzeichen	'5F2A' (Währungscode)	W	2
Länge	'02'	W	1
CURR _{IEP}	Währungscode (die ersten zwei Bytes)	W	2
Identifizierungskennzeichen	'5F36' (Währungsexponent)	W	2
Länge	'01'	W	1
CURR _{IEP}	Währungscode (letztes Byte)	W	1
Identifizierungskennzeichen	'C4' (IEP-Saldo)	W	1
Länge	'04'	W	1
BAL _{IEP}	IEP-Saldo	W	4
Identifizierungskennzeichen	'C4' (maximaler Saldo)	W	1
Länge	'04'	W	1
BAL _{maxIEP}	maximaler Saldo	W	4
SW1-SW2	Zustandsbytes	O	2

ANMERKUNG Die Reihenfolge der in der Antwort enthaltenen Datenobjekte darf veränderlich sein und weitere Datenobjekte dürfen wahlfrei hinzugefügt werden.

7.2.2 Implizite Anwendungsauswahl

Der AID der IEP-Anwendung muss nach ISO/IEC 7816-4, Abschnitt 8.3 und ISO/IEC 7816-5, Abschnitt 6.3.3 in den Historical Bytes des ATR enthalten sein. Andere Datenobjekte, die von der PDA/LDA benötigt werden können, wie z. B. PP_{IEP} und AP_{IEP} , dürfen nicht vorhanden sein, da die Anzahl der Historical Bytes auf 15 begrenzt ist.

Die implizite Anwendungsauswahl kann von Karten für eine Einfachanwendung angeboten werden, um Transaktionen in PDAs/LDAs zu beschleunigen, bei denen der Börsenanbieter und das Anwendungsprofil zusammen mit einem angegebenen AID („lokale“ Karten) bekannt sind. Derartige Einrichtungen können IEP-Transaktionen sofort nach dem Rücksetzen ohne Senden eines Select File-Befehls starten.

Bei PDAs/LDAs, bei denen die zugehörigen Daten nicht bekannt sind (oder wenn es keine feste Beziehung gibt), müssen den in Abschnitt 7.2.1 beschriebenen Select File-Befehl ausgeben. Der zu verwendende Dateiname ist der AID, der in den Historical Bytes des ATR empfangen wird.

7.3 Anwendungsspezifische Befehle an die IEP

7.3.1 Liste der Befehle

In Tabelle 5 sind die anwendungsspezifischen Befehle zusammengefasst, die eine IEP in einem IEP-System ausführen muss, um alle definierten Transaktionstypen zu verarbeiten.

Tabelle 5 – Liste der IEP-Befehle

Befehl	INS	P1	P2	Obligatorisch/ wahlfrei
IEP Initialisieren a) für Aufladen b) für Zahlung c) für Zahlungsabbruch/IEP–Saldowiederherstellung	'50'	'00' '01' '02'	'00' '00' '00'	W O W
IEP-Gutschrift a) für Aufladen b) für Zahlungsabbruch/IEP–Saldowiederherstellung	'52'	'00' '01'	'00' '00'	W W
IEP-Abbuchung a) Zahlung – erste Buchungsstufe b) Zahlung nachfolgende Buchungsstufen c) Zahlungsquittung	'54'	'00' '01' '02'	'00' '00' '00'	O W W
Frühere IEP-Signatur Auffinden	'5A'	'00'	'00'	W
Kontrollanzeige IEP ¹⁾	nicht im Anwendungsbereich von EN 1546-3			
1) Abhängig von der Realisierung kann die Funktionalität der Kontrolle unter Verwendung einer oder mehrerer der von der ISO definierten Befehle realisiert werden: Read Binary, Read Record(s) und Get Data oder durch Verwendung eines anwendungsspezifischen Befehls, der in diesem Teil von EN 1546 nicht definiert ist.				

7.3.2 IEP Initialisieren

7.3.2.1 Definition und Zweck

Dieser Befehl wird verwendet, um eine neue Transaktion mit der IEP zu starten. Es werden verschiedene Formate beschrieben, da jede Transaktionsinitialisierung verschiedene Daten entweder für die Eingabe oder die Ausgabe benötigt.

Es bestehen folgende drei Varianten:

- IEP für Aufladen Initialisieren;
- IEP für Zahlung Initialisieren;
- IEP für Zahlungsabbruch/Saldowiederherstellung Initialisieren.

7.3.2.2 Befehlsnachricht

Die Befehlsnachricht für IEP für Aufladen Initialisieren muss nach Tabelle 6 codiert werden.

Tabelle 6 – Befehlsnachricht für IEP für Aufladen Initialisieren

Feld	Wert	Länge (Bytes)
CLA	'80'	1
INS	'50'	1
P1	'00'	1
P2	'00'	1
L _c	abhängig von DD	1
M _{LDA}	aufzuladender Betrag	4
CURR _{LDA}	Währungscode	3
ID _{PPSAM} /ID _{LDA} ¹⁾	PPSAM-Bezeichner/LDA-Bezeichner	4
R _{PPSAM} /R _{LDA} ¹⁾	Zufallszahl von dem PPSAM/Zufallszahl von einer LDA	4
DD	benutzerbestimmte Daten	variabel
L _e	maximale Anzahl der in der Antwort erwarteten Datenbytes	1 oder 2

1) Datenelemente kommen vom PPSAM oder von einer LDA, wenn die Transaktion vom LDA initiiert wird, ohne eine Verbindung zum Rechner des Börsenanbieters zu haben.

ANMERKUNG PP_{PPSAM} ist nicht enthalten, weil PP_{IEP} schon während der Anwendungsauswahl ausgetauscht wurde und PP_{IEP} indirekt gleich PP_{PPSAM} ist.

Die Befehlsnachricht für die Initialisierung der IEP für eine Abbuchung muss nach Tabelle 7 codiert werden.

Tabelle 7 – Befehlsnachricht für Initialisierung der IEP für eine Abbuchung

Feld	Wert	Länge (Bytes)
CLA	'80'	1
INS	'50'	1
P1	'01'	1
P2	'00'	1
L _c	abhängig von DD (fehlt, wenn keine benutzerbestimmten Daten gesendet werden)	1 oder fehlt
DD	benutzerbestimmte Daten	variabel
L _e	maximale Anzahl der in der Antwort erwarteten Datenbytes	1 oder 3

Die Befehlsnachricht für die Initialisierung der IEP für Zahlungsabbruch/IEP-Saldowiederherstellung muss nach Tabelle 8 codiert werden

Tabelle 8 – Befehlsnachricht für IEP Zahlungsabbruch/IEP-Saldowiederherstellung

Feld	Wert	Länge (Bytes)
CLA	'80'	1
INS	'50'	1
P1	'02'	1
P2	'00'	1
L _c	abhängig von DD (fehlt, wenn keine benutzerbestimmten Daten gesendet werden)	1 oder fehlt
DD	benutzerbestimmte Daten	variabel
L _e	maximale Anzahl der in der Antwort erwarteten Datenbytes	1 oder 3

7.3.2.3 Antwortmeldung (typischer Fall)

Die Antwortmeldung für das Initialisieren der IEP für Aufladen muss nach Tabelle 9 codiert werden.

Tabelle 9 – Antwortmeldung für das Initialisieren der IEP für Aufladen

Feld	Wert	Länge (Bytes)
PP _{IEP}	Bezeichner des Börsenanbieters	3
ID _{IEP}	IEP-Bezeichner	5
ALG _{IEP}	von der IEP verwendeter Algorithmus	1
DEXP _{IEP}	Ablaufdatum	3
BAL _{IEP}	Saldo der IEP	4
NT _{IEP}	Transaktionsnummer der IEP	2
IK _{IEP}	Schlüsselinformation (algorithmensabhängig)	variabel
S ₁	Signatur der IEP	variabel
SW1-SW2	Zustandsbytes (= CC _{IEP})	2

Die Antwortmeldung für IEP für Zahlung Initialisieren muss nach Tabelle 10 codiert werden.

Tabelle 10 – Antwortmeldung für das Initialisieren der IEP für Zahlung

Feld	Wert	Länge (Bytes)
PP _{IEP}	Bezeichner des Börsenanbieters	3
ID _{IEP}	IEP-Bezeichner	5
ALG _{IEP}	von der IEP verwendeter Algorithmus	1
DEXP _{IEP}	Ablaufdatum	3
BAL _{IEP}	Saldo der IEP	4
CURR _{IEP}	Währungscode	3
AM _{IEP}	Authentisierungsmodus der IEP	1
NT _{IEP}	Transaktionsnummer der IEP	2
IK _{IEP}	Schlüsselinformation (algorithmensabhängig)	variabel
S ₁	Signatur der IEP (abhängig vom Algorithmus und AM)	variabel
SW1-SW2	Zustandsbytes (= CC _{IEP})	2

Die Antwortmeldung für IEP für Zahlungsabbruch/IEP-Saldowiederherstellung Initialisieren muss nach Tabelle 11 codiert werden.

Tabelle 11 – Antwortmeldung für das Initialisieren der IEP für Zahlungsabbruch/IEP-Saldowiederherstellung

Feld	Wert	Länge (Bytes)
PP _{IEP}	Bezeichner des Börsenanbieters	3
ID _{IEP}	IEP-Bezeichner	5
ALG _{IEP}	von der IEP verwendeter Algorithmus	1
DEXP _{IEP}	Ablaufdatum	3
NT _{IEP}	Transaktionsnummer der IEP	2
MTOT _{IEP} (log)	Endsummenbetrag der Zahlung	4
M _{PDA} (log)	zu annullierender Betrag	4
CURR _{PDA} (log)	Währungscode	3
ID _{PSAM} (log)	PSAM-Bezeichner der letzten Zahlung	4
NT _{PSAM} (log)	Transaktionsnummer des PSAM	4
IK _{IEP}	Schlüsselinformation (algorithmensabhängig)	variabel
S ₁	Signatur der IEP (abhängig vom Algorithmus und AM)	variabel
SW1-SW2	Zustandsbytes (= CC _{IEP})	2

7.3.2.4 Zustandsbedingungen

Die in Tabelle 12 aufgeführten Zustandsbedingungen können auftreten, wenn der Befehl IEP für Aufladen Initialisieren verarbeitet wird.

Tabelle 12 – Zustandsbedingungen für IEP für Aufladen Initialisieren

SW1	SW2	Bedeutung
'91'	'02'	NT hat ihre Grenze erreicht
'94'	'01'	Währung wird nicht unterstützt
'94'	'02'	Betrag ist zu hoch für Gutschrift

Die in Tabelle 13 aufgeführten Zustandsbedingungen können auftreten, wenn der Befehl IEP für Zahlung Initialisieren verarbeitet wird.

Tabelle 13 – Zustandsbedingungen für IEP für Zahlung Initialisieren

SW1	SW2	Bedeutung
'91'	'02'	NT hat ihre Grenze erreicht

Die in Tabelle 14 aufgeführten Zustandsbedingungen können auftreten, wenn der Befehl IEP für Zahlungsabbruch/IEP-Saldowiederherstellung Initialisieren verarbeitet wird.

Tabelle 14 – Zustandsbedingungen für IEP für Zahlungsabbruch/IEP-Saldowiederherstellung Initialisieren

SW1	SW2	Bedeutung
'91'	'02'	NT hat ihre Grenze erreicht
'94'	'02'	Betrag ist zu hoch für Gutschrift
'94'	'09'	letzte Transaktion war keine Zahlung
'95'	'04'	entsprechende Zahlung war nicht erfolgreich
'95'	'05'	entsprechende Zahlung wurde annulliert

7.3.3 IEP-Gutschrift

7.3.3.1 Definition und Zweck

Dieser Befehl erhöht schrittweise den IEP-Saldo bei einer IEP Aufladetransaktion oder einer Zahlungsabbruch-/IEP-Saldowiederherstellungstransaktion.

7.3.3.2 Befehlsnachricht

Die Befehlsnachricht für IEP-Gutschrift für Aufladen muss nach Tabelle 15 codiert werden.

Tabelle 15 – Befehlsnachricht für IEP-Gutschrift für Aufladen

Feld	Wert	Länge (Bytes)
CLA	'80'	1
INS	'52'	1
P1	'00'	1
P2	'00'	1
L _c	abhängig von ALG oder DD	1 oder 3
IK _{PPSAM}	PPSAM-Schlüsselinformation (algorithmensabhängig)	variabel
S ₂ ¹⁾	Signatur des PPSAM (algorithmensabhängig)	variabel
ID _{PPSAM} ²⁾	PPSAM-Bezeichner	4
R _{PPSAM} ²⁾	Zufallszahl von dem PPSAM	4
DD	benutzerbestimmte Daten	variabel
L _e	maximale Anzahl der in der Antwort erwarteten Datenbytes	1

1) Nach EN 1546-2 im Aufladen mit einem LSAM mit S₃' bezeichnet.

2) Diese Datenelemente werden nur dann übertragen, wenn die Ladetransaktion ohne Verbindung zu einem PPSAM durchgeführt wird. In diesem Fall beinhaltet das Zertifikat (S₂) und die unterschriebene Bestätigung (S₃) die Datenelemente ID_{PPSAM} und R_{PPSAM}.

Die Befehlsnachricht für IEP-Rückbuchung für Zahlungsabbruch/IEP-Saldowiederherstellung muss nach Tabelle 16 codiert werden.

Tabelle 16 – Befehlsnachricht für IEP-Rückbuchung für Zahlungsabbruch/IEP-Saldowiederherstellung

Feld	Wert	Länge (Bytes)
CLA	'80'	1
INS	'52'	1
P1	'01'	1
P2	'00'	1
L _c	abhängig von ALG	1 oder 3
IK _{PSAM}	PSAM-Schlüsselinformation (algorithmenabhängig)	variabel
S ₂	Signatur des PSAM (algorithmenabhängig)	variabel
DD	benutzerbestimmte Daten	variabel

7.3.3.3 Antwortmeldungen (typischer Fall)

Die Antwortmeldung für IEP-Gutschrift für Aufladen muss nach Tabelle 17 codiert werden.

Dieses Format muss auch bei den Fehlerzuständen in Tabelle 19 benutzt werden.

Tabelle 17 – Antwortmeldung für IEP-Gutschrift für Aufladen

Feld	Wert	Länge (Bytes)
S ₃ ¹⁾	Signatur der IEP (algorithmenabhängig)	variabel
DD	benutzerbestimmte Daten	variabel
SW1-SW2	Zustandsbytes (= CC _{IEP})	2

1) Nach EN 1546-2 im Aufladen mit einem LSAM mit S₅ bezeichnet.

Die Antwortmeldung für IEP-Rückbuchung für Zahlungsabbruch/IEP-Saldowiederherstellung muss nach Tabelle 18 codiert werden.

Tabelle 18 – Antwortmeldung für IEP-Rückbuchung für Zahlungsabbruch/IEP-Saldowiederherstellung

Feld	Wert	Länge (Bytes)
DD	benutzerbestimmte Daten	variabel
SW1-SW2	Zustandsbytes (= CC _{IEP})	2

7.3.3.4 Zustandsbedingungen

Die in Tabelle 19 aufgeführten Zustandsbedingungen können auftreten, wenn entweder der Befehl IEP-Gutschrift für Aufladen oder der Befehl IEP-Rückbuchung für Zahlungsabbruch/IEP-Saldowiederherstellung verarbeitet wird.

Tabelle 19 – Zustandsbedingungen für IEP-Gutschrift für Aufladen und IEP-Rückbuchung für Zahlungsabbruch/IEP-Saldowiederherstellung

SW1	SW2	Bedeutung
'93'	'01'	ungültiger öffentlicher Schlüssel oder ungültiges Zertifikat für öffentlichen Schlüssel
'93'	'02'	ungültige Signatur
'95'	'01'	Signatur fehlt