

Identifikationskartensysteme
Branchenübergreifende elektronische Geldbörse
Teil 1: Definitionen, Begriffe und Strukturen
Deutsche Fassung EN 1546-1 : 1999

DIN
EN 1546-1

ICS 01.040.35; 35.240.15

Identification card systems – Inter-sector electronic purse –

Part 1: Definitions, concepts and structures;

German version EN 1546-1 : 1999

Systèmes de cartes d'identification – Porte-monnaie électronique intersectoriel –

Partie 1: Définitions, concepts et structures;

Version allemande EN 1546-1 : 1999

Die Europäische Norm EN 1546-1 : 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 20 Seiten EN

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

– Leerseite –

Deutsche Fassung

Identifikationskartensysteme
Branchenübergreifende elektronische Geldbörse
Teil 1: Definitionen, Begriffe und Strukturen

Identification card systems – Inter-sector electronic purse –
Part 1: Definitions, concepts and structures

Systèmes de cartes d'identification – Porte-monnaie
électronique intersectoriel – Partie 1: Définitions, concepts
et structures

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
Einleitung	2
1 Anwendungsbereich	3
2 Normative Verweisungen	3
3 Definitionen	3
4 Abkürzungen	5
5 Überblick über ein IEP-System	5
Anhang A (informativ) Begriffe und Strukturen	6
Literaturhinweise	20

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 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 besteht aus folgenden Teilen unter dem allgemeinen Titel „Identifikationskartensysteme – Branchenübergreifende elektronische Geldbörse“:

Teil 1: Definitionen, Begriffe und Strukturen

Teil 2: Sicherheitsarchitektur

Teil 3: Datenelemente und Datenaustausch

Teil 4: Datenobjekte

Einleitung

EN 1546 definiert Schnittstellen und die Funktionalität für IEP-Systeme (Systeme der branchenübergreifenden elektronischen Geldbörse) bis zu einem Genauigkeitsgrad, der für Geldbörseninhaber für eine mögliche Anwendung ihrer IEPs in anderen IEP-Systemen notwendig ist, z. B. in anderen Ländern.

In gleicher Weise unterstützt EN 1546 die Anwendung von IEPs mehrerer Geldbörsenanbieter in derselben Einrichtung, wenn das durch Geschäftsvereinbarungen zulässig ist.

Es liegt nicht im Anwendungsbereich von EN 1546, Verwaltungsabläufe und Organisationsstrukturen festzulegen, jedoch werden für eine Verbesserung des allgemeinen Verständnisses die Geschäftsbeziehungen für ein allgemeines IEP-System beschrieben.

Wenn die Möglichkeit besteht, bezieht sich EN 1546 auf andere bestehende ISO- und CEN-Normen.

„Indirekte“ Beteiligte, wie Instanzen, die IEP-Systeme betreffende allgemeine und/oder spezielle Gesetze erlassen, Gerichte und möglicher Clearingverkehr werden nicht behandelt.

1 Anwendungsbereich

Dieser Teil von EN 1546 gibt einen Überblick über ein IEP-System, indem die Beteiligten, die physikalischen Einrichtungen und die notwendigen Funktionen beschrieben werden.

Die hier dargestellten Modelle sind alle sehr allgemein, und einfachere Systeme („geschlossene Systeme“) können durch die Auswahl von Teilgruppen der beschriebenen Funktionalitäten entwickelt werden. Das kann jedoch auch zu Beschränkungen der Fähigkeit zur Zusammenarbeit führen.

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 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 30202-1

Bankkarten – Sicherheitsarchitektur in Zahlungsverkehrssystemen für Karten mit integrierten Schaltkreisen (IC-Karten) – Teil 1: Kartenzyklus (ISO 10202-1 : 1991)

3 Definitionen

Für die Anwendung dieser Norm gelten folgende Definitionen:

3.1

annehmende Stelle

eine Organisation, die Transaktionen mehrerer Zahlungseinrichtungen und/oder von weiteren Hauptrechnern von annehmenden Stellen für die Lieferung an einen oder mehrere Geldbörsenanbieter erfaßt

3.2

Hauptrechner der annehmenden Stelle

die von der annehmenden Stelle verwendete Einrichtung zur Ausführung der IEP-bezogenen Aufgaben für die annehmende Stelle

3.3

Aktivierung

ein Sicherheitsverfahren unter Kontrolle des Geldbörsenanbieters, das eine IEP oder ein SAM für den normalen Betrieb in den aktiven Betriebszustand schaltet

3.4

Datenzusammenfassung

für jeden Geldbörsenanbieter und jede Währung der Additionsvorgang mehrerer Endsummen zu einer Gesamtendsumme. Das Ergebnis ist eine neue Endsumme mit dem Wert, der der Summe aller ursprünglichen Endsummen entspricht

3.5

Authentisierung

ein kryptographischer Vorgang, bei dem eine Instanz die Identität und die Integrität der Daten prüft, die sie zu einer weiteren Instanz senden darf

3.6

Kartenausgeber

die Organisation, die für die Bereitstellung und den

Vertrieb von ICCs zur Anwendung in einem IEP-System verantwortlich ist

ANMERKUNG: Diese Definition eines IEP-Kartenausgebers darf nicht mit der allgemeinen Verwendung dieser Benennung in anderen auf Karten beruhenden Zahlungssystemen verwechselt werden.

3.7

Erfassung

bei Transaktionen der Vorgang der Datenübertragung von PSAMs und/oder Zahlungseinrichtungen zu (einem) Hauptrechner(n) und PPSAM(s), der direkt oder über annehmende Stellen erfolgt

3.8

Währungsumrechnung

eine Online-Transaktion zum Hauptrechner des Geldbörsenanbieters, bei der der gesamte IEP-Saldo von einer Währung in eine andere umgerechnet wird

3.9

Protokoll der Währungsumrechnung

eine Datei im nichtflüchtigen Speicher einer IEP, die für die Aufzeichnung der Informationen über mindestens die letzte Währungsumrechnungstransaktion verwendet wird

3.10

Deaktivierung

ein Sicherheitsverfahren unter Kontrolle des Geldbörsenanbieters, das eine IEP oder ein SAM aus dem aktiven Betriebszustand in einen dauerhaft abgeschalteten Zustand schaltet. Im deaktivierten Zustand ist nur das Lesen nicht geheimer Daten möglich

3.11

elektronischer Wert; Wert

der in einem IEP-System gespeicherte und ausgetauschte (elektronische) Wert. Der elektronische Wert stellt einen wirklichen Geldbetrag in der bestimmten Währung dar

3.12

Fehlerbehebung

Verfahren für die Korrektur bestimmter Fehler, die bei der Verarbeitung normaler Transaktionen, z. B. von Zahlungstransaktionen, festgestellt werden

3.13

IC-Karte (ICC)

eine Karte mit integrierten Schaltkreisen, auf der mindestens eine IEP eingerichtet ist

3.14

IC-Einbatter

die Organisation, die IC-Baugruppen und Kunststoffkarten zu ICCs zusammenfaßt. Sie könnte die IEP auch personalisieren

3.15

IC-Hersteller

die Organisation, die die ICs für ICCs herstellt

3.16

Identität

eine Bitkette, die ausgewählt wurde, um einen eindeutigen Wert zu besitzen, und die zum Beispiel für die Unterscheidung zwischen Fällen von IEPs, SAMs und Transaktionen verwendet wird

3.17

IEP-Saldo

der aktuelle Betrag eines Wertes in einer IEP (in einer bestimmten Währung). Er wird durch Aufladetransaktionen (und Zahlungsabbruchtransaktionen) erhöht und durch Zahlungstransaktionen verringert

3.18

branchenübergreifende elektronische Geldbörse (IEP)

eine Anwendung auf einer ICC, die in der Lage ist, einen elektronischen Wert nach EN 1546 zu speichern und zu verarbeiten

3.19

IEP-Kontrollanzeige

ein möglicherweise tragbares Gerät, mit dem öffentliche Informationen in der IEP wie der IEP-Saldo und Protokollinformationen ausgelesen werden können

3.20

IEP-System

Die Benennung verweist auf alle beschriebenen Beteiligten, Einrichtungen und Funktionen, die von EN 1546 behandelt werden

3.21

Installation

der Vorgang, bei dem eine IEP- oder SAM-Anwendung und ihre zugehörigen Parameter in eine ICC geladen werden

3.22

Schlüsselmanagement

die in einem IEP-System verwendeten Techniken für die Erzeugung, Verteilung, Speicherung, Aktualisierung und Vernichtung kryptographischer Schlüssel und des zugehörigen Verschlüsselungsmaterials. Die in dieser Norm angegebenen Empfehlungen gelten sowohl für manuelle als auch automatisierte Techniken für einen sicheren Austausch von Schlüsseln und Verschlüsselungsmaterial zwischen den verschiedenen Komponenten des IEP-Systems, der entweder direkt oder indirekt unter Anwendung gemeinsamer Zentren für das Schlüsselmanagement erfolgt, denen vom (von den) Geldbörsenanbieter(n) die Verantwortung übertragen wurde

3.23

Schlüsselmanagementsystem

die tatsächliche Realisierung des Schlüsselmanagements in einem IEP-System

3.24

Aufladen

die mit einer Aufladeeinrichtung ausgeführte Transaktion, bei der ein Wert vom PPSAM zu einer IEP übertragen wird. Als Antwort erhält entweder der Auflade-Bevollmächtigte oder der Geldbörsenanbieter eine Zahlung vom Geldbörseninhaber. Die Benennung Aufladen schließt nachfolgende Aufladungen einer IEP (Nachladungen) ein

3.25

Auflade-Bevollmächtigter

die Organisation, die die von den Geldbörseninhabern zu benutzenden Aufladeeinrichtungen bereitstellt. Weiterhin kann der Auflade-Bevollmächtigte Zahlungen von den Geldbörseninhabern im Austausch für Aufladetransaktionen erhalten

3.26

Aufladeeinrichtung

eine physikalische Einrichtung, die von einem Auflade-Bevollmächtigten betrieben wird und gemeinsam von einem Geldbörseninhaber und dem Auflade-Bevollmächtigten benutzt wird, um einen Wert vom PPSAM zur IEP (des Geldbörseninhabers) zu übertragen

3.27

Aufladeprotokoll

eine Datei im nichtflüchtigen Speicher einer IEP, die für die Aufzeichnung von Informationen über mindestens die letzte Aufladetransaktion verwendet wird

3.28

Auflade-SAM (LSAM)

ein logisches Modul, das in (einer) Aufladeeinrichtung(en), die von einem Auflade-Bevollmächtigten betrieben wird, der die Zahlung unmittelbar erhält, Sicherheit bietet

3.29

Sperrliste

eine Liste, die keinen oder mehrere Bereich(e) von Bezeichnern für IEPs enthält, die für die Ausführung von Transaktionen im IEP-System nicht zugelassen sind. Falls vorhanden, sollte die Liste für SAMs zum Zeitpunkt der Transaktion verfügbar sein

3.30

Persönliche Identifikationsnummer (PIN)

Daten, die vor der Anwendung angefordert werden können, und die, bevor Daten verarbeitet werden können, der Karte von ihrem Anwender zu übermitteln sind

3.31

Zahlung

die mit einer Zahlungseinrichtung ausgeführte Transaktion, wobei ein Wert von einer IEP zu einem PSAM übertragen wird. Als Antwort erhält der Geldbörseninhaber eine Leistung vom Leistungsanbieter

3.32

Zahlungsabbruch

die in einer Zahlungseinrichtung ausgeführte Transaktion, um die letzte Zahlungstransaktion für die beteiligte IEP und das beteiligte PSAM zu widerrufen

3.33

Zahlungseinrichtung

eine physikalische Einrichtung, die von einem Leistungsanbieter betrieben wird und gemeinsam von einem Geldbörseninhaber und dem Leistungsanbieter benutzt wird, um einen Wert von der IEP des Geldbörseninhabers zu der zur Zahlungseinrichtung gehörenden PSAM zu übertragen

3.34

Zahlungsprotokoll

eine Datei im nichtflüchtigen Speicher einer IEP, die zur Aufzeichnung von Informationen über mindestens die letzte Zahlungstransaktion verwendet wird

3.35

Zahlungs-SAM (PSAM)

ein in der Verantwortung des Geldbörsenanbieters ausgegebenes SAM, das in Verbindung mit der (den) Zahlungseinrichtung(en) eingerichtet wird und die notwendige Sicherheit für zahlungsbezogene Transaktionen und Abholungsvorgänge bietet

3.36

Geldbörseninhaber

eine Person, die in Besitz einer (ICC mit einer) IEP ist. In der Gesamtlebensdauer der IEP nicht unbedingt immer dieselbe Person

3.37

Geldbörsenvertreiber

die Organisation, die für die gesamte Funktionalität und Sicherheit eines IEP-Systems verantwortlich ist. Auch die Organisation, die dazu berechtigt ist, im Austausch für Aufladetransaktionen Gelder zu empfangen und den Leistungsanbietern entsprechend den in ihren Zahlungseinrichtungen vorgenommenen Transaktionen Gutschriften zu leisten

3.38

Hauptrechner des Geldbörsenvertreibers

ein Datenverarbeitungssystem mit der notwendigen Funktionalität zur sicheren Durchführung der IEP-Funktionen des Geldbörsenvertreibers unter Anwendung des PPSAM

3.39

SAM des Geldbörsenvertreibers (PPSAM)

das SAM des Geldbörsenvertreibers, das die notwendige Funktionalität für die sichere Funktion des IEP-Systems vom Standpunkt des Geldbörsenvertreibers aus gesehen bietet, d. h., sichere Aktivierungs-, Aufladungs-, Erfassungs- und Protokollierungsfunktionen

3.40

Anwendungssicherheitsmodul (SAM)

eine logische Einrichtung, die Sicherheit für unsichere Umgebungen bietet. Es ist vor Fälschung geschützt und speichert geheime und/oder kritische Informationen. Für ein IEP-System sind mehrere Arten von SAMs definiert

3.41

SAM-Ausgeber

die zertifizierte Organisation, die für die Ausgabe von SAMs, z. B. Zahlungs-SAMs, für die Anwendung in einem IEP-System verantwortlich ist

3.42

SAM-Kontrollanzeige

eine Einrichtung, mit der öffentliche Informationen im SAM z. B. als Endsummen ausgelesen werden können

3.43

Sicherheitsarchitektur

die Verwendung detaillierter Sicherheitsmechanismen einschließlich kryptographischer Algorithmen und des Schlüsselmanagements, die in geeigneter Weise den Sicherheitsanforderungen des IEP-Systems entsprechen

3.44

Leistung

Jede Art der Leistung und/oder von Waren, die einem Geldbörseninhaber von einem Leistungsanbieter zur Verfügung gestellt werden und für die in einer Zahlungstransaktion bezahlt wird

3.45

Leistungsanbieter

die Organisation, die einem Geldbörsenvertreiber (eine) Leistung(en) zur Verfügung stellt, für die unter Anwendung einer IEP zu bezahlen ist. Der Leistungsanbieter betreibt eine oder mehrere Zahlungseinrichtung(en)

3.46

Abrechnung

ein vom Geldbörsenvertreiber oder einer annehmenden Stelle im Interesse des Geldbörsenvertreibers ausgeführter Vorgang. Beruhend auf Daten von Zahlungs- und Aufladetransaktionen wird die Zahlung vom Geldbörsenvertreiber zum Leistungsanbieter und in einigen Fällen von den Auflade-Bevollmächtigten zum Geldbörsenvertreiber bewirkt

3.47

Endsumme

eine Zusammenfassung einzelner Zahlungstransaktionen. Sie enthält (mindestens) die Gesamtanzahl der Transaktionen und den Gesamtbetrag dieser Transaktionen. Eine Endsumme kann nur Informationen für einen Geldbörsenvertreiber und für in einer Währung vorgenommene Transaktionen enthalten

3.48

Wert

siehe elektronischer Wert

3.49

Überprüfung

ein Vorgang, bei dem bestimmt wird, ob der Vorleger einer ICC oder eines SAM ein berechtigter Nutzer ist, z. B. durch Anwendung einer PIN oder durch biometrische Maße

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. Service Provider (Leistungsanbieter).

4 Abkürzungen

IC	Integrated Circuit integrierter Schaltkreis
ICC	IC Card Karte mit integrierten Schaltkreisen
IEP	Inter-sector Electronic Purse branchenübergreifende elektronische Geldbörse
LSAM	Load SAM Auflade-SAM
PIN	Personal Identification Number persönliche Identifikationsnummer
PSAM	Purchase SAM Zahlungs-SAM
PPSAM	Purse Provider SAM SAM des Geldbörsenvertreibers
SAM	Secure Application Module Anwendungssicherheitsmodul

5 Überblick über ein IEP-System

5.1 Haupteigenschaften des Systems

Das IEP-System besitzt folgende Haupteigenschaften:

- es beruht auf einer Sicherheitsarchitektur, die gegen Mißbrauch schützt;
- eine IEP ist auf einer Mikroprozessor-gestützten ICC (Karte mit integrierten Schaltkreisen) mit Kontakten oder ohne Kontakte installiert;
- eine IEP beruht auf einer Vorauszahlung. Der in der IEP enthaltene elektronische Wert ist der Gegenwert eines Bankguthabens;
- es besteht die Möglichkeit der Benutzung der IEP in vielen unterschiedlichen Arten von Zahlungseinrich-