

	Identifikationskartensysteme Branchenübergreifende elektronische Geldbörse Teil 2: Sicherheitsarchitektur Deutsche Fassung EN 1546-2:1999	DIN EN 1546-2
ICS 35.240.15 Identification card systems – Inter-sector electronic purse – Part 2: Security architecture; German version EN 1546-2:1999 Systèmes de cartes d'identification – Porte-monnaie électronique intersectoriel – Partie 2: Architecture de sécurité; Version allemande EN 1546-2:1999	Die Europäische Norm EN 1546-2:1999 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 im Abschnitt 2 zitierten Normen wird im Folgenden auf die entsprechenden Deutschen Normen hingewiesen: ISO 8372 siehe DIN ISO 8372 Nationaler Anhang NA (informativ) Literaturhinweise DIN ISO 8372, <i>Informationsverarbeitung – Betriebsarten für einen 64-bit-Blockschlüsselalgorithmus.</i> Fortsetzung 82 Seiten EN Normenausschuss Informationstechnik (NI) im DIN Deutsches Institut für Normung e.V.	

– Leerseite –

Deutsche Fassung

Identifikationskartensysteme

Branchenübergreifende elektronische Geldbörse

Teil 2: Sicherheitsarchitektur

Identification card systems – Inter-sector electronic
purse – Part 2: Security architecture

Systèmes de cartes d'identification – Porte-monnaie
électronique intersectoriel – Partie 2: Architecture de
sécurité

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 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	3	C.3.2 Anforderungen an das Schlüsselmanagement	42
1 Anwendungsbereich	3	C.3.3 Topologie des IEP-Systems	42
2 Normative Verweisungen	3	C.3.4 Betriebsanforderungen	42
3 Begriffe, Symbole und Abkürzungen	4	C.3.5 Vorbetriebliche Anforderungen	43
3.1 Begriffe	4	C.3.6 Anforderungen an die Schlüsselmodifizierung in der Betriebsphase	44
3.1.1 In EN 1546-1 festgelegte Benennungen	4	C.3.7 Spezifikation von PKCs	45
3.1.2 Spezifische Benennungen für diesen Teil von EN 1546	4	C.3.8 Anforderungen an das Schlüsselmanagement für interaktive Signaturen	45
3.2 Symbole	5	Anhang D (informativ)	
3.3 Abkürzungen	5	Überblick über die Zahlungstransaktion	45
3.4 Besondere Schreibweise	6	Anhang E (informativ)	
4 Sicherheitsarchitektur	7	Sicherheitsprotokolle unter Verwendung des DES ..	49
4.1 Sicherheitsanforderungen und Eigenschaften	7	E.1 Besondere Anmerkungen zu DES	49
4.2 Fehlerbehandlung	7	E.1.1 Verschlüsselung/Entschlüsselung unter Verwendung des DES	49
4.3 Sicherheitsrelevante Datenelemente	8	E.1.2 Authentisierung unter Verwendung des DES ..	49
4.4 Sicherheitsprozeduren	9	E.1.3 Realisierungsanmerkungen für DES	49
4.4.1 Allgemeine Anmerkung	9	E.2 Zu DES spezifische Datenelemente	49
4.4.2 Aufladen (optional)	10	E.3 Sicherheitsprotokolle	50
4.4.3 Zahlung	17	E.3.1 Aufladen	50
4.4.4 Zahlungsabbruch/IEP-Saldbereinigung (optional)	21	E.3.2 Zahlung	55
Anhang A (informativ)		E.3.3 Abholung	58
Zusätzliche Sicherheitsprozeduren	24	Anhang F (informativ)	
A.1 IEP-Transaktionen	24	Sicherheitsprotokolle unter Verwendung von RSA/DSS	62
A.1.1 Währungsumrechnung	24	F.1 Besondere Anmerkungen zu RSA	62
A.1.2 IEP-Kontrolle	25	F.1.1 Authentisierung unter Verwendung von RSA	62
A.1.3 IEP-Parameter Aktualisieren	26	F.1.2 Zertifizierung mit Hilfe eines öffentlichen Schlüssels unter Verwendung von RSA	62
A.2 SAM-Transaktionen	28	F.2 Besondere Anmerkungen zu DSS	63
A.2.1 Abholung	28	F.2.1 Authentisierung unter Verwendung von DSS	63
A.2.2 SAM-Kontrolle	32	F.2.2 Zertifizierung mit Hilfe eines öffentlichen Schlüssels unter Verwendung von DSS	64
A.2.3 SAM-Parameter Aktualisieren	32	F.3 Verwendung von Zertifikaten mit Hilfe öffent- licher Schlüssel in IEP-Systemen	64
A.2.4 SAM bereit	35	F.4 Zu RSA/DSS spezifische Datenelemente	65
A.2.5 SAM nicht bereit	35	F.5 Realisierungsanmerkungen zu RSA/DSS	65
Anhang B (informativ)		F.6 Sicherheitsprotokolle	65
Sicherheitsanforderungen und Sicherheits- mechanismen	36	F.6.1 Aufladen	65
Anhang C (informativ)		F.6.2 Zahlung	71
Schlüsselmanagement	38	F.6.3 Abholung	74
C.1 Allgemeines	38	Anhang G (informativ)	
C.2 Schlüsselmanagement für symmetrische Algorithmen	38	Zahlungstransaktion unter Verwendung von interaktiven 3-Stufen-Signaturen	79
C.2.1 IEP/PSAM-Kommunikation	38	G.1 Datenelemente	79
C.2.2 Aufgeteilte Hauptschlüssel für die Zahlungstransaktion	39	G.2 Änderungen zu Abschnitt 4.4.3	79
C.2.3 IEP/PPSAM-Kommunikation	39	G.3 Besondere Anmerkungen zu interaktiven Signaturen	79
C.2.4 PSAM/PPSAM-Kommunikation	39	G.4 Spezifische Datenelemente zu interaktiven Signaturen	80
C.2.5 LSAM/PPSAM-Kommunikation	40	G.5 Sicherheitsprotokolle	80
C.2.6 Schlüsseltrennung	40	G.5.1 Zahlung	80
C.2.7 Schlüsselmodifikation	40		
C.3 Schlüsselverwaltung für asymmetrische Algorithmen	40		
C.3.1 Allgemeine Anforderungen für die Schlüsselzertifizierung	40		

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.

Anhänge, die als „normativ“ bezeichnet sind, gehören zum Norminhalt. Anhänge, die als „informativ“ bezeichnet sind, enthalten nur Informationen. In dieser Norm sind die Anhänge A bis G informativ.

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 legt die ausführliche Sicherheitsarchitektur für IEP-Systeme nach EN 1546-1 fest. Er beschreibt ebenfalls die Anwendungsprotokolle, die Verwendung von kryptographischen Algorithmen und einige grundlegende Voraussetzungen, die das notwendige Schlüsselmanagement betreffen, um IEP-Systeme mit einem ausreichenden Sicherheitsniveau zu realisieren.

Die hier beschriebene allgemeine Architektur lässt viele Arten der Realisierung zu. Es sollte beachtet werden, dass sich die informativen Anhänge dieser Norm auf bestimmte Realisierungen richten.

Es wird erwartet, dass im Laufe der Zeit andere Realisierungen in den Mittelpunkt rücken können.

Die Sicherheitsarchitektur legt die Sicherheitsprozeduren fest, die auf der Anwendungsebene der Transaktionen und Funktionen des IEP-Systems nach EN 1546-1, A.5 und EN 1546-1, A.6, gebraucht werden. Diese Architektur stützt sich auf die Grundannahmen nach EN 1546-1, 1.4.

Die manuelle Fehlerbehebung liegt außerhalb des Anwendungsbereichs dieser Norm. Protokollinformationen, die zur Durchführung von manuellen Fehlerbehebungsprozeduren gebraucht werden, sind in diese Norm jedoch einbezogen.

Die Beschreibung in diesem Teil der Norm erfolgt in Form des geordneten Datenaustauschs zwischen verschiedenen vom Konzept vorgegebenen Geräten. Von diesen Geräten ausgeführte Betriebsbefehle erzeugen den geforderten geordneten Austausch. Beispiele für die Bedeutungen der geforderten Betriebsbefehle sind als mathematische Formeln in den informativen Anhängen dargestellt. Die Transaktionsdefinitionen in diesem Teil der Norm sind als funktionelle Anforderungen beschrieben. Sie beschreiben die Reihenfolge der kryptographischen Nachweise und Überprüfungen und die mit ihnen verbundenen Datenelemente, die notwendig sind, um die Sicherheit in einem IEP-System zu erreichen.

Ein IEP-System, das der Sicherheitsarchitektur entspricht, die in diesem Teil von EN 1546 beschrieben wird, kann in physikalischen Geräten unter Verwendung allgemein gebräuchlicher Programmieretechniken realisiert werden. Eine Optimierung von Berechnungen und Datenaustausch, die die Betriebsanforderungen des geordneten Datenaustauschs aufrechterhält, darf ebenfalls realisiert werden.

Die Datenelemente und der Datenaustausch, die in diesem Teil von EN 1546 beschrieben werden, betreffen im Grunde Sicherheitsfragen. Um andere Anforderungen des IEP-Systems zu erfüllen, müssen weitere Datenelemente und weitere Daten-Austauschabläufe hinzugefügt werden. Die ausführlichen Formate von Datenelementen und Datenaustausch zwischen Geräten sind in EN 1546-3 (Datenelemente und Datenaustausch) beschrieben.

2 Normative Verweisungen

Diese Europäische Norm 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 gehören spätere Änderungen oder Überarbeitungen dieser Publikationen nur zu dieser Europäischen Norm, falls sie durch Änderung oder Überarbeitung eingearbeitet worden 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 1546-3, *Identifikationskartensysteme – Branchenübergreifende elektronische Geldbörse – Teil 3: Datenelemente und Datenaustausch.*

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

ISO 8372:1987, *Information processing – Modes of operation for a 64-bit block cipher algorithm.*

ISO/IEC 9797:1994, *Information technology – Security techniques – Data integrity mechanism using a cryptographic check function employing a block cipher algorithm.*

3 Begriffe, Symbole und Abkürzungen

3.1 Begriffe

3.1.1 In EN 1546-1 festgelegte Benennungen

Dieser Teil von EN 1546 verwendet folgende in EN 1546-1 festgelegte Benennungen:

- 1) Aktivierung;
- 2) Datenzusammenfassung;
- 3) Authentisierung;
- 4) Abbruch;
- 5) Abholung;
- 6) Währungsumrechnung;
- 7) Deaktivierung;
- 8) Elektronischer Wert;
- 9) Fehlerbehebung;
- 10) Identität;
- 11) Branchenübergreifende elektronische Geldbörse (IEP);
- 12) IEP-Saldo;
- 13) IEP-Kontrollanzeige;
- 14) IEP-System;
- 15) Schlüsselmanagement;
- 16) Schlüsselmanagementsystem;
- 17) Aufladen;
- 18) Aufladebevollmächtigter;
- 19) Aufladeeinrichtung;
- 20) Aufladeprotokoll;
- 21) Auflade-SAM;
- 22) Sperrliste;
- 23) Persönliche Identifikationsnummer (PIN);
- 24) Zahlung;
- 25) Zahlungsabbruch;
- 26) Zahlungseinrichtung;
- 27) Zahlungsprotokoll;
- 28) Zahlungs-SAM;
- 29) Börseninhaber;
- 30) Börsenanbieter;
- 31) Zentralrechner des Börsenanbieters;
- 32) Börsenanbieter-SAM;
- 33) Anwendungssicherheitsmodul (SAM);
- 34) SAM-Kontrollanzeige;
- 35) Sicherheitsarchitektur;
- 36) Leistungsanbieter;
- 37) Endsumme;
- 38) Wert.

Um die für ein allgemeines IEP-System spezifische Benennungen in der gesamten EN 1546 hervorzuheben, beginnen diese Benennungen (im englischen Original) mit großen Anfangsbuchstaben, z. B. Service Provider (Leistungsanbieter).

3.1.2 Spezifische Benennungen für diesen Teil von EN 1546

Im Sinne dieses Teils von EN 1546 gelten folgende Definitionen:

3.1.2.1

Beendigungscode

Ein Teil der Antwort an jede Komponente mit Bezug auf einen gegebenen Befehl. Er gibt an, ob der Befehl erfolgreich ausgeführt wurde oder nicht; im letzteren Fall gibt der Beendigungscode den Grund dafür an, warum der Befehl nicht erfolgreich durchgeführt werden konnte.

3.1.2.2

Unterbrechungs-Angriff

Systematischer Versuch zur Unterbrechung der normalen Funktionen eines IEP-Systems durch Verhinderung der Durchführung von Transaktionen, so z. B. den Saldo in einer Komponente zu vermindern, ohne eine Gutschrift auf den zugehörigen Saldo in einer anderen Komponente.

3.1.2.3

Gegenseitige Authentisierung

Dieses Verfahren findet nur bei Incremental Purchase Transactions Anwendung, wo der erste Schritt des Vorgangs Belastung/Gutschrift als Zweiweg-Authentisierung durchgeführt wird und die weiteren Schritte als Einweg-Authentisierung.

3.1.2.4

Zahlungstransaktionen mit fester Buchung

Eine Zahlungstransaktion, die in mehreren aufeinander folgenden Schritten durchgeführt wird, bei der jeweils das IEP belastet und dem PSAM gutgeschrieben wird.

3.1.2.5

Maskerade

Durch Simulation erzeugte Vortäuschung, ein echtes Gerät zu sein, z. B. eine IEP. Kann durch die Verwendung von geheimen Informationen verhindert werden, z. B. Schlüssel innerhalb des echten Gerätes.

3.1.2.6

Message Authentication Code

Ein Code in einer Nachricht zwischen einem Sender und einem Empfänger, der verwendet wird, um die Quelle und einen Teil oder den gesamten Text einer Nachricht zu überprüfen. Der Code ist das Ergebnis einer vereinbarten Berechnung.

3.1.2.7

Nicht Bestreitbarkeit

Liefert den kryptographischen Nachweis, dass weder der Erzeuger noch der Empfänger bestreiten kann, eine bestimmte Nachricht mit ihrem ursprünglichen Inhalt gesendet/empfangen zu haben.

3.1.2.8

Einweg-Authentisierung

Eine Transaktion zwischen zwei Komponenten, bei der nur eine Komponente durch die andere authentisiert wird, so z.B. wird nur das IEP vom PSAM bei Kauftransaktionen authentisiert.

3.1.2.9

Wiederholung

Erhalt von Nachrichten aus einer echten IEP-Transaktion und der Versuch, sie später zu wiederholen, um eine Transaktion zu vervielfältigen oder Ähnliches. Kann durch den Besitz einiger eindeutiger Informationen verhindert werden, die nur für eine einzige Transaktion gültig sind.

3.1.2.10

Signatur

In dieser Norm werden (digitale) Signaturen in den Sicherheitsprotokollen verwendet, um sowohl Geräte als auch die Integrität der Daten zu authentisieren.

3.1.2.11

Zweiweg-Authentisierung

Eine Transaktion zwischen zwei Komponenten, bei der jede der Komponenten von der anderen authentisiert wird.

Um die für ein allgemeines IEP-System spezifische Benennungen in der gesamten EN 1546 hervorzuheben, beginnen diese Benennungen (im englischen Original) mit großen Anfangsbuchstaben, z. B. Completion Code (Beendigungscode).

3.2 Symbole

^	Logisches UND
∨	Logisches ODER
∈	enthalten in
∉	nicht enthalten in
κ	Verkettung (von Datenelementen)
{ }	Menge (von Datenelementen)
() oder []	geordnete Menge (von Datenelementen)
:=	Zuweisung
::=	Definition
→	Vektor (Bezeichner für eine geordnete Menge von Datenelementen)

3.3 Abkürzungen

DES	Data Encryption Standard (kryptographischer Algorithmus)
DSS	Digital Signature Standard (kryptographischer Algorithmus)
IEP	(Inter-sector Electronic Purse) Branchenübergreifende elektronische Geldbörse
LDA	(Load Device Application) Aufladeeinrichtungsanwendung
LSAM	(Load SAM) Auflade-SAM

PDA	(Purchase Device Application) Zahlungseinrichtungsanwendung
PIN	(Personal Identification Number) Persönliche Identifikationsnummer
PK	(Public Key) Öffentlicher Schlüssel
PKC	(Public Key Certificate) Zertifikat mit Hilfe eines öffentlichen Schlüssels
PSAM	(Purchase SAM) Zahlungs-SAM
PPSAM	(Purse Provider SAM) Börsenanbieter-SAM
RSA	(Rivest, Shamir and Adleman) Rivest, Shamir und Adleman (kryptographischer Algorithmus)
SAM	(Secure Application Module) Anwendungssicherheitsmodul

3.4 Besondere Schreibweise

Die in den Bildern für die in 4.4 festgelegten Sicherheitsprotokolle verwendete Schreibweise wird nachfolgend festgelegt. Jedes Bild zeigt die in eine spezifische Transaktion einbezogenen Komponenten, z. B. sind in eine Zahlungstransaktion eine IEP, eine PDA und ein PSAM einbezogen.

Für jedes einbezogene Gerät sind zwei Spalten festgelegt. Für die linke Spalte gelten folgende Definitionen:

Cn: Kennzeichnet einen zu einer anderen Komponente gesendeten Befehl.

An: Kennzeichnet die Aktion (Aktionen), die durch die empfangende Komponente durchzuführen ist (sind).

Rn: Kennzeichnet eine Antwort, die an den Erzeuger des Befehls zu senden ist.

In der nächsten Spalte wird die Definition dafür angezeigt, was für eine bestimmte Aktion zu tun ist. Weiterhin werden die in einem Befehl oder einer Antwort zu sendenden Parameter aufgeführt. In den Bildern sind nur sicherheitsbezogene Datenelemente enthalten.

Mit dieser Spalte zusammenhängende besondere Schreibweisen sind Folgende (diese besondere Schreibweise wird hauptsächlich in den Bildern im normativen Teil dieser Norm verwendet):

compare()	Vergleiche die in den Klammern aufgeführten Parameter.
decipher()	Entschlüssele die in den Klammern aufgeführten Parameter.
encipher()	Verschlüssele die in den Klammern aufgeführten Parameter.
parameters()	Übertrage die in den Klammern aufgeführten Parameter als einen Befehl.
response()	Übertrage die in den Klammern aufgeführten Parameter als eine Antwort.
select()	Wähle die in den Klammern aufgeführten Parameter.
sign()	Signiere die in den Klammern aufgeführten Parameter.
verify()	Überprüfe die in den Klammern aufgeführten Parameter.
write()	Schreibe/aktualisiere die in den Klammern aufgeführten Parameter.

Spezifische Definitionen dieser Operationen werden in den Anhängen verwendet, die in ausführlichen Beispielen beschreiben, wie die Transaktionen unter Verwendung verschiedener kryptographischer Algorithmen zu realisieren sind.

command() []	Der durch den Namen in den Klammern angegebene Befehl wird unter Verwendung der in den eckigen Klammern aufgeführten Parameter gesendet.
decipher(K) []	Die Entschlüsselungsfunktion wird mit den in den eckigen Klammern aufgeführten Parametern unter Verwendung des Schlüssels K berechnet.
encipher(K) []	Die Verschlüsselungsfunktion wird mit den in den eckigen Klammern aufgeführten Parametern unter Verwendung des Schlüssels K berechnet.
hash[]	Eine Hash-Funktion wird mit den in den eckigen Klammern aufgeführten Parametern berechnet.
response()	Die Parameter in den Klammern werden in einer Antwort gesendet (immer einschließlich eines Beendigungs-codes).
select() []	Die in den Klammern beschriebene Information wird aus einer in den eckigen Klammern aufgeführten Menge von Datenelementen ausgewählt.
sign(K) []	Die Signaturfunktion wird mit den in den eckigen Klammern aufgeführten Parametern unter Verwendung des Schlüssels K berechnet.
verify(K) []	Die Verifikationsfunktion wird mit den in den eckigen Klammern aufgeführten Parametern unter Verwendung des Schlüssels K berechnet. Im Gegensatz zur allgemeinen verify()-Funktion ist diese Funktion eine besondere kryptographische Operation, die vom gegebenen Algorithmus abhängt.
write() []	Die in den eckigen Klammern aufgeführten Parameter werden in die Datei geschrieben, die in den normalen Klammern angezeigt wird. Kommentare zeigen an, ob die Daten zur Datei hinzugefügt werden oder verwendet werden, um die bestehenden Daten zu aktualisieren.

4 Sicherheitsarchitektur

Die hier beschriebene Sicherheitsarchitektur ist als Schutz gegen vorsätzlichen Betrug sowie einige Gerätefehlfunktionen vorgesehen. Es gibt jedoch keinen Schutz gegen menschliche Fehler bei der Bedienung des Gerätes, z. B. Eintasten eines falschen Betrags, da dies von dem Gerät selbst nicht festgestellt werden kann. Diese Fehler müssen durch Fehlerprozeduren bearbeitet werden, die möglicherweise menschliches Eingreifen erfordern.

Bedienungsabläufe und geschäftliche Vereinbarungen zwischen den Teilnehmern werden in dieser Norm nicht behandelt, obwohl einige grundlegende Voraussetzungen berücksichtigt worden sind. Dieser Teil von EN 1546 enthält jedoch Anforderungen für das Vorhalten von Informationen und Nachweisen, die für diese Abläufe notwendig sind.

Abwägen zwischen den Sicherheitsniveaus und den Kosten für die Realisierung und den Betrieb eines IEP-Systems werden nicht ausdrücklich behandelt.

Unabhängig von der gewählten Sicherheitsarchitektur können Kryptosysteme mit geheimen und öffentlichen Schlüsseln einbezogen werden. Die dazu notwendigen Schlüssel müssen kontrolliert erzeugt und verteilt werden, um deren Kompromittierung zu vermeiden.

Die Grundvoraussetzungen für das erforderliche Schlüsselmanagement zur Festlegung der Sicherheitsarchitektur sind im Anhang C (informativ) beschrieben, die Realisierung eines bestimmten Schemas für ein Schlüsselmanagement liegt jedoch außerhalb des Anwendungsbereichs dieses Teils der EN 1546.

4.1 Sicherheitsanforderungen und Eigenschaften

Die Hauptanforderungen an die Sicherheitsarchitektur sind, zu verhindern, dass:

- a) ein Wert in IEPs oder SAMs in einer Weise abgebucht oder gutgeschrieben wird, die vom Börsenanbieter nicht vorgesehen ist;
- b) ein Wert ohne Vereinbarung zwischen den beteiligten Teilnehmern, z. B. dem Börseninhaber und dem Leistungsanbieter, ausgetauscht wird;
- c) Teilnehmer andere ohne Aufdeckung betrügen.

und zu ermöglichen:

- d) den abgeglichenen Austausch eines Wertes;
- e) Behebungsprozeduren im Fehlerfall;
- f) die Bereitstellung von erforderlichen Angaben zur Lösung von Konflikten.

Ausführlichere Sicherheitsanforderungen für jede Transaktion in IEP-Systemen werden im Anhang B dargelegt.

Die Sicherheitsarchitektur von IEP-Systemen hat folgende grundlegenden Eigenschaften, vorausgesetzt, dass die in EN 1546-1, 1.4 angegebenen Grundvoraussetzungen erfüllt werden:

- a) In einem IEP-System trägt der Börsenanbieter das Risiko eines Betrugs im System und legt somit das notwendige Sicherheitsniveau durch Auswahl einer bestimmten Sicherheitsarchitektur fest;
- b) Teile der gesamten Sicherheit eines IEP-Systems beruhen auf vertraglichen Vereinbarungen zwischen einzelnen Geschäftspartnern. Dies ist besonders wichtig, wenn eine Übertragung von Aufgaben und Verantwortung stattfindet;
- c) die Sicherheitsarchitektur bietet Schutz gegen Vervielfältigung und unberechtigte Veränderung von Transaktionen, Maskerade und Bestreiten von Transaktionen, nachdem sie ausgeführt worden sind;
- d) im Allgemeinen wird ein SAM gebraucht, wenn kritische sicherheitsbezogene Funktionen wie Authentisierung und nicht Bestreiten durchgeführt werden müssen oder wenn kritische Daten wie kryptographische Schlüssel und eine Sperrliste(n) sicher gespeichert werden müssen;
- e) Ende-zu-Ende-Sicherheitsprotokolle bestehen zwischen den folgenden Komponentenpaaren, soweit vorhanden:
 - IEP ↔ PPSAM, z. B. für Aufladetransaktionen,
 - IEP ↔ PSAM, z. B. für Zahlungstransaktionen,
 - LSAM ↔ PPSAM, z. B. für Aufladetransaktionen,
 - PSAM ↔ PPSAM, z. B. für Abholungstransaktionen;
- f) jede IEP und jedes SAM müssen eindeutig gekennzeichnet werden;
- g) Aktualisierungen von Daten in zwei verschiedenen Komponenten, z. B. dem IEP-Saldo und der Endsumme im PSAM, sollen das Risiko eines Synchronisierungsverlustes minimieren. Falls eine Transaktion vorzeitig abgebrochen wird, ermöglichen die beiden Komponenten, soweit keine Sicherheitsbedenken bestehen, ein Rückgängigmachen, um alle schon ausgeführten Aktualisierungen abzuberechnen (oder ein Weitermachen, um alle schon ausgeführten Aktualisierungen zu vollenden), was aber ein menschliches Eingreifen erfordern kann;
- h) eine Protokollierung, die auf einzelnen Transaktionen beruht, ist möglich;
- i) es sind Funktionen zur Aufrechterhaltung zumindest einer begrenzten Sperrliste (begrenzten Sperrlisten) in einigen oder allen SAMs im IEP-System festgelegt;
- j) es wird vorausgesetzt, dass die IEP nur einen kryptographischen Algorithmustyp enthält.

4.2 Fehlerbehandlung

Eine Fehlerbehandlung findet in verschiedenen Geräten statt, von denen nur einige das Vertrauen des Börsenanbieters haben. Außerdem findet die Fehlerbehandlung in verschiedenen Protokollschichten statt. Ein vereinfachtes Modell, das zwei Kommunikationsgeräte zeigt, von denen jedes aus einer Transportschicht und einer Anwendungsschicht sowie einem lokalen Datenspeicher besteht, die auch Fehler verursachen können, wird in Bild 1 gezeigt.

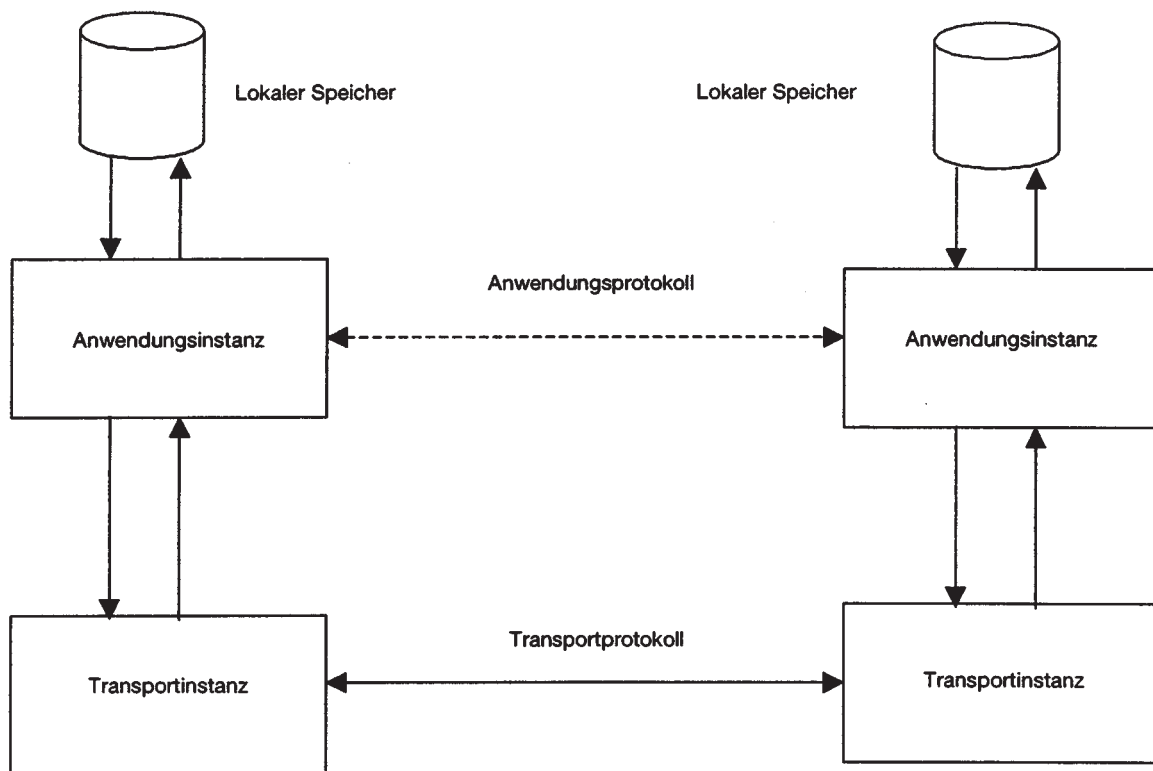


Bild 1 – Protokollschichten im IEP-System

Im Anwendungsbereich dieses Teils von EN 1546 liegt nur die Fehlerbehandlung in der Anwendungsschicht. Fehler in einer unteren Schicht müssen entweder in dieser Schicht behoben werden oder an die Anwendungsschicht als nicht behebbar angezeigt werden.

Vom Sicherheitsstandpunkt aus kann von Geräten, die nicht unmittelbar vom Börsenanbieter kontrolliert werden, keine Behandlung kritischer Fehler erwartet werden. Die Fehlerbehandlung in solchen Geräten kann jedoch eine sichere Fehlerbehandlung in vertrauenswürdigen Geräten auslösen.

Ein Gerät, das die Kommunikation zwischen zwei vertrauenswürdigen Geräten steuert, z. B. einer Zahlungseinrichtung, die eine Kommunikation zwischen einer IEP und einem PSAM herstellt, muss normalerweise versuchen, das andere Gerät zu informieren, für den Fall, dass ein Gerät einen Befehl zurückweist (oder ein nicht behebbarer Fehler in einer unteren Schicht festgestellt wird). Ebenso muss solch ein Steuergerät das ausgefallene Gerät auffordern, die aktuelle Transaktion gegebenenfalls zu beenden. Schließlich sollte das Steuergerät Informationen über den Fehler speichern.

Als Grundprinzip müssen die festgelegten Sicherheitskomponenten immer alle vorgeschriebenen Aktionen durchführen, wenn sie einen Befehl empfangen. Falls die Stromversorgung unterbrochen oder die Komponente zurückgesetzt wird, müssen ausreichende Informationen vorliegen, um nach dem Einschalten der Stromversorgung, bzw. nach dem erfolgten Zurücksetzen, die vollständige Rückgängigmachung oder die Fortsetzung auszuführen, soweit keine Sicherheitsbedenken bestehen. Diese Fehlerbehebung muss ausgeführt werden, bevor andere Befehle angenommen werden.

Eine ausführlichere Fehlerbehandlung wird in EN 1546-4 beschrieben und ein Verzeichnis der Beendigungscode wird in EN 1546-3 angegeben.

4.3 Sicherheitsrelevante Datenelemente

Dieser Teil der EN 1546 legt die sicherheitsbezogenen Aspekte aller Transaktionen in einem IEP-System fest. Zur Klarstellung werden begriffliche Datenelemente ebenfalls definiert, auch wenn sie in der eigentlichen Implementation nicht vorhanden sind.

Datenelemente werden in unterschiedlichen Komponenten des IEP-Systems gespeichert (COMP ::= IEP/LSAM/PSAM/PPSAM).

Soweit anwendbar, sind mögliche Werte für die Datenelemente in Klammern angegeben.

Für einen bestimmten Algorithmus spezifische Datenelemente sind in (informativen) Anhängen E, F und G für den gegebenen Algorithmus festgelegt.

ALG_{COMP}	Kennzeichnet den von der Komponente verwendeten Algorithmus.
AM_{IEP}	Authentisierungsmodus (Authentisierungsmodi), der von der IEP für Zahlungstransaktionen benötigt wird (ONE_WAY/TWO_WAY/DUAL_MODE). Weiterhin legt er fest, ob S ₁ von der IEP (S1_BIT) berechnet wird und ob eine signierte Quittung benötigt wird (ACK_BIT).
BAL_{COMP}	Saldo der Komponente.
BAL_{COMP}	Datenvektor, der den Saldo und den zugehörigen Währungscode enthält.
BAL_{maxCOMP}	Höchstsaldo der Komponente.
CC_{COMP}	Beendigungscode (von der Komponente gesendet).

CT	Beendigungsstatus im PSAM bezogen auf eine Endsumme (ACTIVE/OFF-LINE_COLLECTED/ON-LINE_COLLECTED).
CURR_{COMP}	Währungscode der Komponente.
DACT_{COMP}	Aktivierungsdatum der Komponente.
DATE_{COMP}	Aktuelles Datum der Komponente.
DDEA_{COMP}	Deaktivierungsdatum der Komponente.
DEXP_{COMP}	Ablaufdatum für die Komponente.
FD_{IEP}	Fester Datenvektor, der von der IEP übertragen wird. Er umfasst folgende Datenelemente: PP _{IEP} , ID _{IEP} , ALG _{IEP} , IK _{IEP} und DEXP _{IEP} .
FD_{LSAM}	Fester Datenvektor, der vom LSAM übertragen wird. Er umfasst folgende Datenelemente: PP _{LSAM} , ID _{LSAM} , ALG _{LSAM} , IK _{LSAM} und DEXP _{LSAM} .
FD_{PSAM}	Fester Datenvektor, der vom PSAM übertragen wird. Er umfasst folgende Datenelemente: ALG _{PSAM} , IK _{PSAM} und DEXP _{PSAM} .
ID_{COMP}	Identifikator der Komponente.
IEP	Bezeichner für die IEP.
IK_{COMP}	Fester Datenvektor, der die Schlüsselinformation (algorithmabhängig) für die Komponente umfasst. Dieser Datenvektor kann leer sein.
IND	Fester Datenvektor des PSAM, der folgende Daten für einzelne Transaktionen enthält: PP _{PSAM} , ID _{PSAM} , NC, NT _{PSAM} , NI(NC), ID _{IEP} , NT _{IEP} , AM _{IEP} , CURR(NC), MTOT _{PSAM} , CC _{PSAM} und Transaktionstyp (Quittung oder Abbruch/IEP Balance Recovery).
M_{COMP}	Transaktionsbetrag von der Komponente (durch PDA oder LDA bestimmt).
M_{COMP}	Datenvektor, der M und CURR umfasst.
MTOT_{COMP}	Betrag einer Transaktion, der in den Komponenten IEP und PSAM fest gebucht wird (für eine Zahlungstransaktion mit festen Buchungstufen).
NC	Nummer der Abholung (Bezeichner für Endsummen eines gegebenen PSAM); durch X(NC) wird in einem anderen Datenelement X ein Verweis auf diese Endsumme gemacht.
NF_{PSAM}	Durch das PSAM kontrollierte Sperrliste.
NI	Anzahl der einzelnen Transaktionen bezogen auf eine Endsumme.
NT_{COMP}	Transaktionsnummer der Komponente.
NU_{COMP}	Aktualisierungsnummer, die vom PPSAM berechnet wird und in einer Offline-PSAM-Parameteraktualisierung verwendet wird.
NV	Neuer Wert für einen Parameter (wird verwendet bei IEP/SAM-Parameter Aktualisieren).
PAR	Bezeichner des zu aktualisierenden Parameters (wird verwendet bei IEP/SAM-Parameter Aktualisieren).
PEXP	Vom PSAM verwendeter Binärwert, um die Gültigkeit des Ablaufdatums zu kontrollieren. Es kann ein im PSAM gespeicherter fester Wert sein, oder er kann während jeder Transaktion aus Transaktionsparametern berechnet werden, die im PSAM verfügbar sind.
PIND	Binärwert, der im PSAM gespeichert wird oder vom PSAM während der Transaktionsverarbeitung aus Transaktionsparametern und Parametern, die im PSAM gespeichert sind, berechnet wird. Er kontrolliert die Erzeugung von einzelnen Transaktionen.
PP_{COMP}	In der Komponente gespeicherter Börsenanbieter-ID.
R	Vom PPSAM berechnete Zufallszahl.
S_n	Signatur.
STAT_{COMP}	Betriebsstatus einer Komponente, der anzeigt, ob sie für Transaktionen bereit oder nicht bereit ist.
TM	Gesamtbetrag einer Endsumme.
TOTAL	Datenvektor, der mit einem Gesamtbetrag des PSAM für einen Börsenanbieter und für eine Währung verbunden ist. Er umfasst die Datenelemente: PP _{PSAM} , ID _{PSAM} , NC, NI(NC), TM(NC), CURR(NC) und CT(NC).
VK_{COMP}	Von der Komponente verwendete Schlüsselversion.

4.4 Sicherheitsprozeduren

4.4.1 Allgemeine Anmerkung

Die in 4.4 beschriebenen Transaktionen verfügen über gemeinsame Features. Zur Vereinfachung der Beschreibung und zur Vermeidung von Wiederholungen werden diese gemeinsamen Features nur einmal in diesem Abschnitt beschrieben.

4.4.1.1 Überprüfung des internen Status

Für jede vom Gerät gestartete Transaktion muss der Status der Sicherheitskomponente gleich ACTIVE sein, mit Ausnahme der Aktualisierungsparameter der Transaktionen (wenn zum Beispiel DACT_{COMP} gesetzt werden muss) und der Kontrolle (wenn zum Beispiel das Aktivierungsdatum gesetzt werden muss, und das Ablaufdatum nicht). Dieselbe Bemerkung ist für den Status OPEN von SAMs gültig.

4.4.1.2 Selektion/Erzeugung von Schlüsseln

Für jedes kryptographische Verfahren (Signieren, Überprüfen, Verschlüsseln, Entschlüsseln) muss die Sicherheitskomponente einen oder mehrere Schlüssel auswählen und/oder erzeugen. Wie dies im Einzelnen durchzuführen ist, hängt von der Art des Algorithmus und z. B. von der Entscheidung ab, ob für jede Sitzung unterschiedliche Schlüssel zu verwenden sind.

4.4.1.3 Transaktionsprotokolle

Jede Sicherheitskomponente, die ein oder mehrere Transaktionsprotokolle verwaltet, bereitet einen neuen Eintrag für jede Transaktion vor.

Im Fall einer Zahlungstransaktion mit mehreren festen Buchungsstufen wird ein einziger Datensatz erzeugt und initialisiert. Dieser Datensatz wird dann für jeden folgenden Abbuchungs-IEP-Befehl aktualisiert.

Die folgenden Protokolldateien werden in diesem Teil von EN 1546 verwendet: Zahlungsprotokoll und Aufladeprotokoll.

4.4.1.4 Beendigungscode

Ein Beendigungscode wird an jede IEP-Antwort auf jeden Befehl angefügt. Er enthält Informationen über das Ergebnis der Ausführung des Befehls, die für das Steuergerät bei der Entscheidung wichtig sind, wie mit der Transaktion weiter verfahren werden soll. Er ist deshalb besonders wichtig für die Fehlerbehandlung. Da die Bilder nur fehlerfreie Ausführungen der Transaktionen beschreiben, wird der Beendigungscode nur erwähnt, wenn er in der Transaktion aus besonderen Sicherheitsgründen verwendet wird.

4.4.1.5 Aufforderungen zur Authentisierung

Die in diesem Teil von EN 1546 beschriebene Authentisierung stützt sich auf zwei Arten von Aufforderungen zum Schutz gegen Wiederholung:

- Zähler für Aufforderungen, die von IEPs, PSAMs und LSAMs erzeugt werden (zur einfachen Erzeugung und Protokollierung ausgewählt);
- Zufallszahlen für Aufforderungen, die von PPSAMs erzeugt werden (wird wegen der Nicht-Vorhersagbarkeit ausgewählt).

Die ausgewählte Art der PPSAM-Aufforderung (entweder auf Zähler oder Zufallszahlen gestützt) ist nicht entscheidend, da in beiden Fällen Wiederholungen feststellbar sind.

Folglich kann eine bestimmte PPSAM-Realisierung Aufforderungen verwenden, die sich entweder auf Zähler oder Zufallszahlen stützen. Es ist jedoch vom Standpunkt der IEP wichtig, dass beide dasselbe Format haben. Eine ausführlichere Beschreibung ist in EN 1546-3 angegeben.

4.4.1.6 Digitale Signaturen

Eine digitale Signatur weist folgende Eigenschaften auf:

- nur der Unterzeichner kann eine gültige Signatur mit den gegebenen Daten berechnen; es sollte für jeden anderen unmöglich sein, (erfolgreich) eine Signatur zu fälschen;
- die Signatur kann von jedem überprüft werden. Der Überprüfungsvorgang authentisiert nicht nur die gegebenen Daten, sondern auch den Ursprung der Daten;
- ein unparteiischer dritter Beteiligter kann auf der Grundlage der signierten Daten Kontroversen bezüglich einer Fälschung klären.

Echte digitale Signaturen mit diesen Eigenschaften sind asymmetrischen Algorithmen für öffentliche Schlüssel eigen. Mit symmetrischen Algorithmen für geheime Schlüssel können die meisten dieser Eigenschaften simuliert werden, wenn angriffs-sichere Hardware (SAMs) verfügbar ist. Die Eigenschaft der Signaturüberprüfung durch jeden ist jedoch nicht realisierbar. In diesem Teil von EN 1546 werden digitale Signaturen in den Sicherheitsprotokollen verwendet, um Geräte und die Integrität der Daten zu authentisieren.

4.4.1.7 Beliebige Daten

Zu einer Transaktion hinzugefügte beliebige Daten können kryptographisch geschützt werden, wenn die dazugehörige Signatur in den Befehlen/Antworten der Transaktion schon existiert. In diesem Fall werden entweder alle oder ein Teil dieser beliebigen Daten an die signierten Daten angehängt. Die Länge der beliebigen Daten muss im zutreffenden Befehl/der zutreffenden Antwort festgelegt werden, siehe EN 1546-3 für Einzelheiten dieses Mechanismus.

4.4.1.8 Börsenanbieter-spezifische Transaktionen

Einige Transaktionen, wie Abholung, SAM-Parameter aktualisieren und SAM bereit/nicht bereit, könnten als Transaktionen betrachtet werden, die für jeden Börsenanbieter spezifisch sind, weil sie eine weniger deutliche Auswirkung auf die Fähigkeit zur Zusammenarbeit mit anderen Börsensystemen haben als IEP-bezogene Transaktionen. Als solche werden diese Transaktionen im informativen Anhang dieses Teils der EN 1546 gegeben, da anzuerkennen ist, dass Börsenanbieter ihr eigenes spezifisches Protokoll realisieren können; besonders wenn die Fähigkeit zur Zusammenarbeit nicht beeinflusst wird. Die Protokolle im informativen Anhang sollten mindestens als eine Richtlinie für das in diesen Transaktionen erforderliche Sicherheitsniveau dienen.

4.4.2 Aufladen (optional)

Die Aufladetransaktion, die von der LDA als eine Interaktion zwischen der IEP und dem PPSAM ausgeführt wird, bucht vom PPSAM den vereinbarten Betrag ab und schreibt der IEP den gleichen Betrag gut.

Für die Aufladetransaktion sind zwei Lösungen festgelegt. Von der IEP aus gesehen, sind die Initialisierungs- und die Gutschriftphasen für beide Lösungen die gleichen:

- die Lösung aus Bild 2, beschrieben in 4.4.2.1, setzt voraus, dass der Börsenanbieter überzeugt ist, dass eine konventionelle Zahlung stattfinden wird oder tatsächlich stattgefunden hat und dass es sich um ein Online-Ende-zu-Ende-Protokoll handelt, das nur die IEP und das PPSAM umfasst. Diese Lösung unterstützt eine Lösung mit nur zwei Online-Nachrichten;
- die Lösung aus Bild 3, beschrieben in 4.4.2.2, setzt voraus, dass der Börsenanbieter auf eine andere Geschäftsinstanz angewiesen ist, die eine Garantie gibt, dass der Börsenanbieter eine konventionelle Zahlung erhalten wird. Dieses Protokoll setzt auch das Vorhandensein einer LSAM-Komponente voraus. Der Kommunikationspfad von der IEP zum LSAM muss geschützt werden, um zu garantieren, dass die IEP-Parameter nicht geändert werden können.

4.4.2.1 Aufladen ohne LSAM

Dieses Protokoll zeigt die Transaktion IEP Aufladen ohne ein LSAM. Der vereinbarte Aufladebetrag wird von der LDA festgehalten.

Nach der Initialisierung des PPSAM und der IEP für die Aufladetransaktion, erzeugt die LDA eine Anforderung für das IEP-Aufladen an das PPSAM (einschließlich S_1). Das PPSAM überprüft (mit zusätzlichen Daten, die von außerhalb empfangen worden sein könnten, und über Wege außerhalb des Anwendungsbereichs dieser Norm), dass die konventionelle, dem Aufladebetrag entsprechende Zahlung vom Börsenanbieter erhalten worden ist oder werden wird.

Der Börsenanbieter muss sicher sein, dass der Zahlungspflichtige eingewilligt hat, für das Aufladen einer gegebenen IEP zu bezahlen.

Das PPSAM authentisiert die IEP und erzeugt ein IEP-Aufladezertifikat (S_2) und bucht von seinem Saldo ab, bevor S_2 zur IEP übertragen wird. Die IEP überprüft S_2 (was die Authentisierung des PPSAM bedeutet), bevor sie ihrem Saldo den Aufladebetrag gutschreibt und das Aufladeprotokoll aktualisiert. Die IEP erzeugt eine signierte Quittung, ob das Aufladen erfolgreich war oder nicht (S_3), die zum PPSAM übertragen wird. Diese signierte Quittung kann für Zwecke der Protokollierung verwendet werden.

Diese Aufladetransaktion realisiert eine Zweiweg-Authentisierung zwischen dem PPSAM und der IEP und ist zum Schutz vor folgenden Gefahren vorgesehen:

- Aufladen von anderen IEPs als der identifizierten IEP (S_1);
- Aufladen durch falsche PPSAMs (S_2);
- Bestreiten eines erfolgreichen Aufladens (S_3);
- Unterbrechungs-Angriffe, wie ein nicht berechtigtes Abbuchen von einem PPSAM-Saldo (S_1).

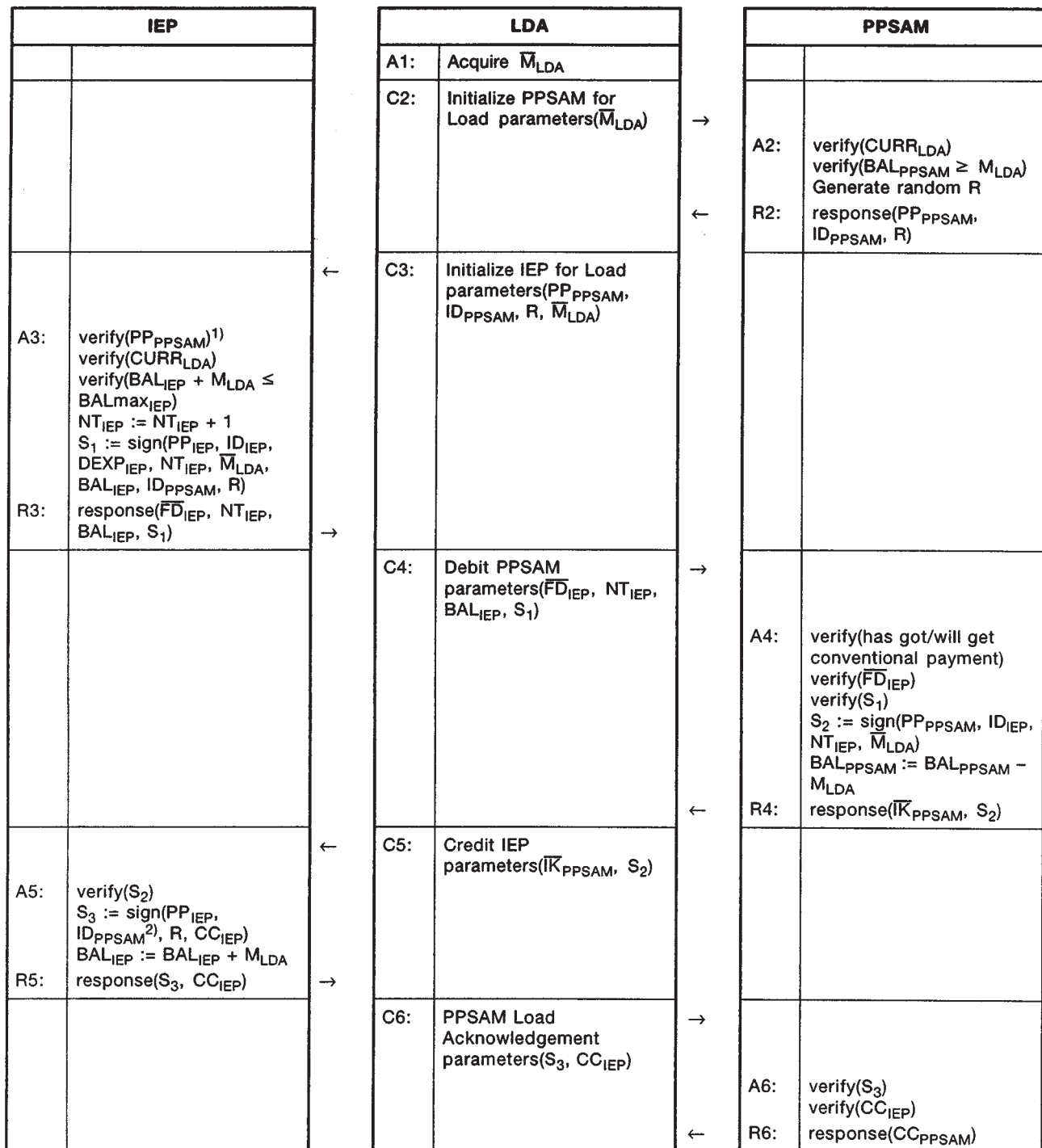


Bild 2 – Aufladetransaktion ohne LSAM

ANMERKUNG Es handelt sich hierbei um ein begriffliches Modell, das nicht als Beispiel einer Implementation gewertet werden sollte. Gültige Implementationen müssen den Sicherheitsanforderungen dieses Teils der EN 1546 Rechnung tragen. So unterstützt dieses Aufladeprotokoll, zum Beispiel, Aufladetransaktionen, die auf einem einzigen Austausch basieren, wobei das kritische Aufladezertifikat S_2 mit übertragen wird. Die Anfangsanforderung und die signierte Quittung kann zum Beispiel in der vorherigen bzw. in der nächsten Transaktion übertragen werden oder lokal generiert bzw. überprüft werden.

4.4.2.2 Aufladen mit LSAM

Für den Fall, dass die Aufladetransaktion ein LSAM einschließt, vereinbaren der Aufladebevollmächtigte und der Börseninhaber den Betrag, der aufzuladen ist.

1) Diese Überprüfung kann ohne Übertragung des PP_{PPSAM} über Schnittstellen an Karten durchgeführt werden. So lässt sich zum Beispiel eine Überprüfung durch nachfolgende Überprüfung von S_1 erreichen.

2) Nur hinzugefügt, um die gleich bleibende Verwendung von S_3 bei der Währungsumrechnung und der Aktualisierung der IEP-Parameter zu ermöglichen.

Nach der Initialisierung des PPSAM, der IEP und des LSAM durch die LDA für die Aufladetransaktion (einschließlich des Betrags), startet die LDA eine Anforderung PPSAM Abbuchen, die Authentisierungsparameter der IEP und des LSAM enthält. Nach dieser Abbuchungsanforderung erzeugt das PPSAM seinerseits ein IEP-Aufladezertifikat (S_3) und verschlüsselt dies, sodass nur das LSAM es für die Übertragung zur IEP entschlüsseln kann. Zusätzlich überträgt das PPSAM in seiner Antwort ausreichende Schlüsselinformationen, um dem LSAM zu ermöglichen, S_3 und später die von der IEP als Quittung empfangene Signatur S_5 zu überprüfen.

Die Verschlüsselung ist notwendig, weil der Aufladebevollmächtigte nicht in der Lage sein sollte, S_3 zur IEP zu übertragen, ohne sie an das LSAM weiterzugeben, und dann den Empfang der Antwort des PPSAM zu bestreiten. Nach dem Empfang überprüft das LSAM S_3 , bevor sie zur IEP übertragen wird.

Die IEP überprüft S_3 , bevor sie ihrem Saldo den Aufladebetrag gutschreibt und das Aufladeprotokoll aktualisiert. Die IEP erzeugt eine signierte Quittung über das erfolgreiche Aufladen (S_5), die zum LSAM übertragen wird. Das LSAM berechnet nach der Überprüfung von S_5 ein Quittungszertifikat (S_6), das dann zum PPSAM gesendet wird. Das PPSAM berechnet nach der Überprüfung von S_6 eine signierte Quittung und ein Zertifikat (S_7), das vom LSAM überprüft wird und als ein weiterer Nachweis von der LDA gespeichert wird.

Diese Aufladetransaktion realisiert eine Zweiweg-Authentisierung zwischen dem PPSAM und der IEP und zwischen dem LSAM und dem PPSAM. Es ist zum Schutz vor folgenden Gefahren vorgesehen:

- es kann nur die vom LSAM identifizierte IEP aufgeladen werden (Gutschreiben desselben Betrags der Aufladetransaktion auf mehr als eine IEP) (S_2);
- Maskerade (Simulation einer IEP durch eine andere) (S_1);
- Bestreiten von erfolgreichen Aufladetransaktionen durch den Aufladebevollmächtigten, den Börsenanbieter und den Börseninhaber (S_3 -Verschlüsselung, S_7 , S_5);
- Bestreiten eines nicht erfolgreichen Aufladens durch den Börsenanbieter (S_5);
- Unterbrechungs-Angriffe als systematische Versuche, ein PPSAM abzubuchen (S_1);
- Fehlfunktionen der IEP (S_1).

Das Verhältnis zwischen dem Börseninhaber, dem Aufladebevollmächtigten und dem Börsenanbieter stützt sich auf folgende Annahmen:

- die Erzeugung von S_2 bedeutet, dass der Aufladebevollmächtigte vom Börseninhaber bezahlt worden ist;
- falls die Überprüfung von S_1 oder S_2 im PPSAM misslingt, darf der Börsenanbieter kein Geld vom Aufladebevollmächtigten fordern;
- die Erzeugung von S_3 und die Entschlüsselung mit dem Schlüssel des LSAM garantiert, dass weder der Börsenanbieter noch der Aufladebevollmächtigte bestreiten kann, S_3 im Kontext einer erfolgreichen Aufladetransaktion gesendet und empfangen zu haben;
- S_6 ist eine signierte Quittung für das erfolgreiche oder nicht erfolgreiche Aufladen der IEP vom LLSAM.

Es sind vier Fälle möglich:

- wenn die IEP richtig aufgeladen wurde und S_6 vom PPSAM empfangen wird, muss der Aufladebevollmächtigte dem Börsenanbieter den entsprechenden Betrag bezahlen;
- wenn die IEP nicht richtig aufgeladen wurde und S_5 vom LSAM und S_6 vom Börsenanbieter empfangen wird, verlangt letzterer vom Aufladebevollmächtigten keine Bezahlung und S_3 wird im LSAM ungültig. Statt dessen zahlt der Aufladebevollmächtigte an den Börseninhaber zurück;
- wenn die IEP richtig aufgeladen wurde und S_6 vom PPSAM nicht empfangen wird, nimmt der Börsenanbieter von vornherein an, dass die Transaktion erfolgreich war, und der Aufladebevollmächtigte muss den Börsenanbieter bezahlen, falls keine andere geschäftliche Vereinbarung besteht;
- wenn die IEP nicht richtig aufgeladen wurde und S_5 von der IEP nicht erzeugt werden kann, muss der Börseninhaber die von ihm an den Aufladebevollmächtigten getätigte Bezahlung vom Börsenanbieter zurückfordern und der Aufladebevollmächtigte muss den Börsenanbieter bezahlen.

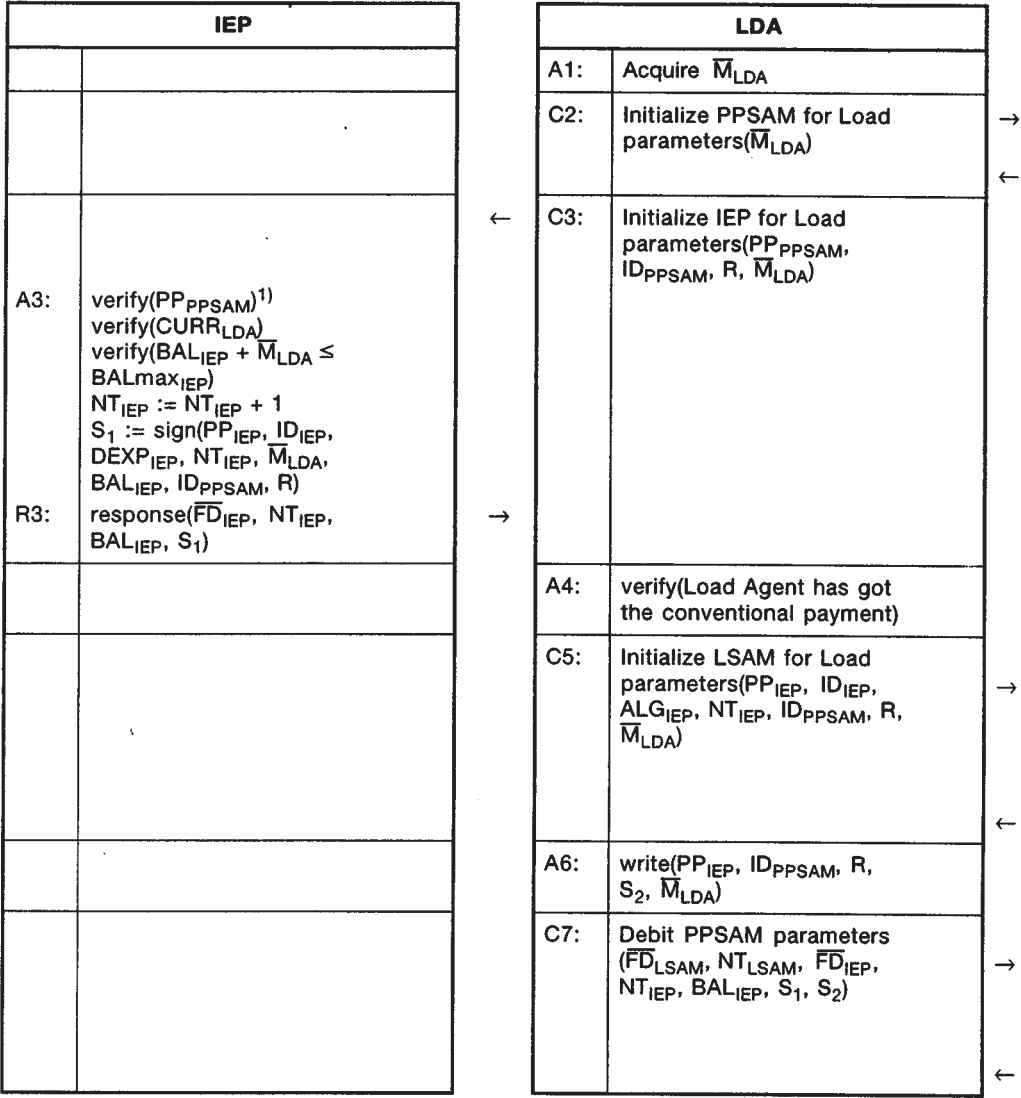


Bild 3 – Aufladetransaktion mit LSAM – linke Hälfte (fortgesetzt)

1) Diese Überprüfung kann ohne Übertragung des PP_{PPSAM} über Schnittstellen an Karten durchgeführt werden. So lässt sich zum Beispiel eine Überprüfung durch nachfolgende Überprüfung von S_1 erreichen.

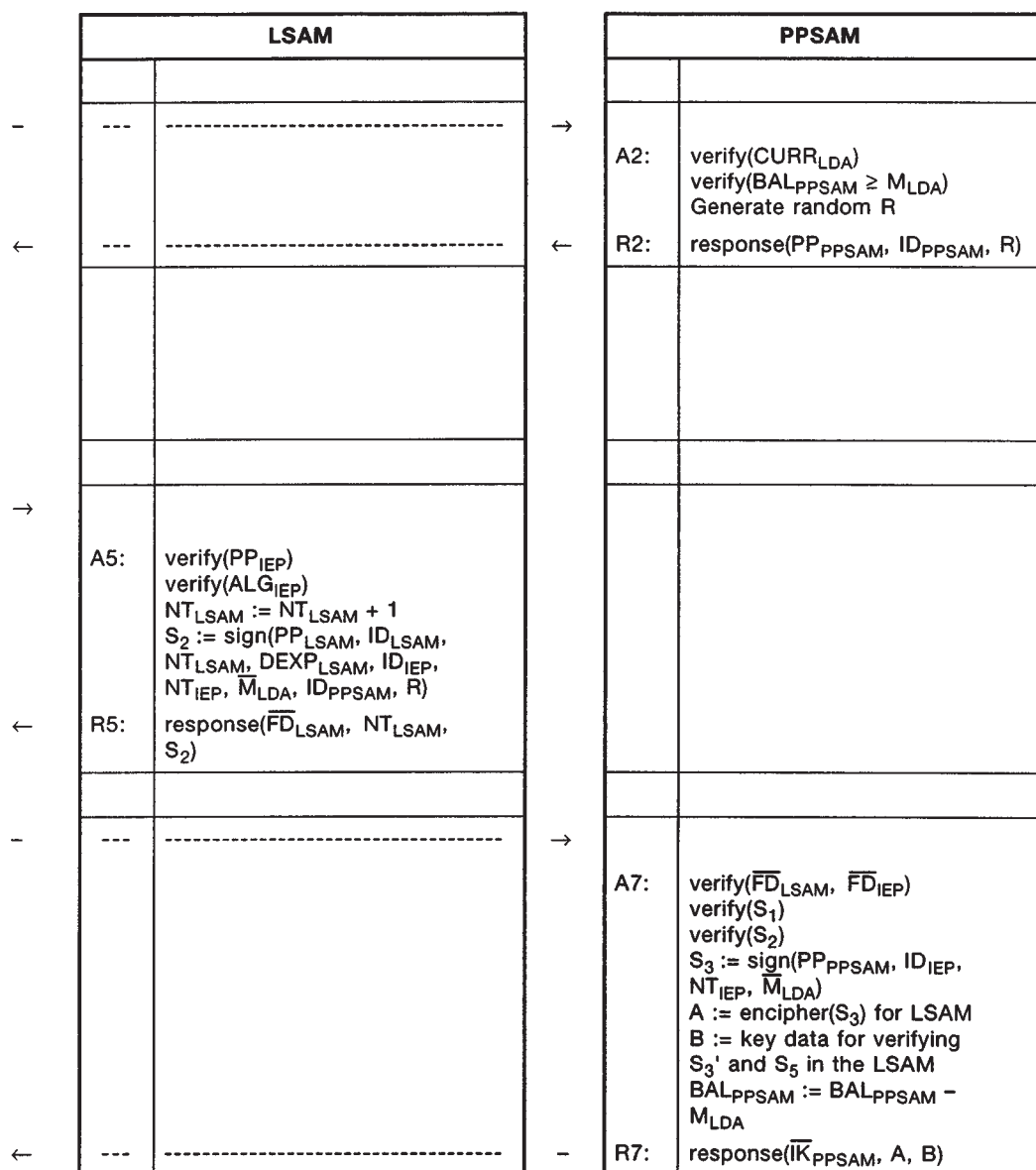


Bild 3 – Aufladetransaktion mit LSAM – rechte Hälfte (fortgesetzt)

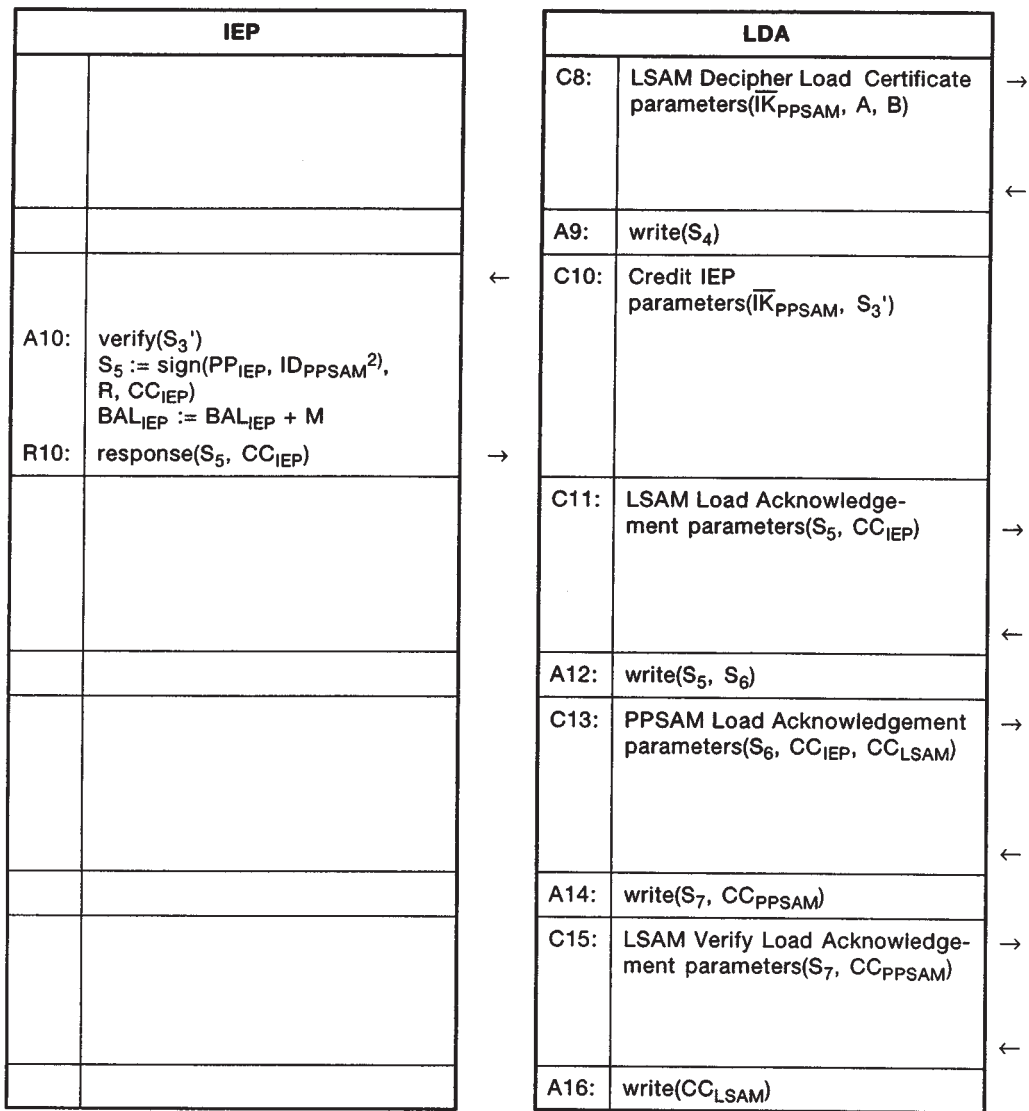


Bild 3 – Aufladetransaktion mit LSAM – linke Hälfte (abgeschlossen)

2) Nur hinzugefügt, um die gleich bleibende Verwendung von S_3 bei der Währungsumrechnung und der Aktualisierung der IEP-Parameter zu ermöglichen.

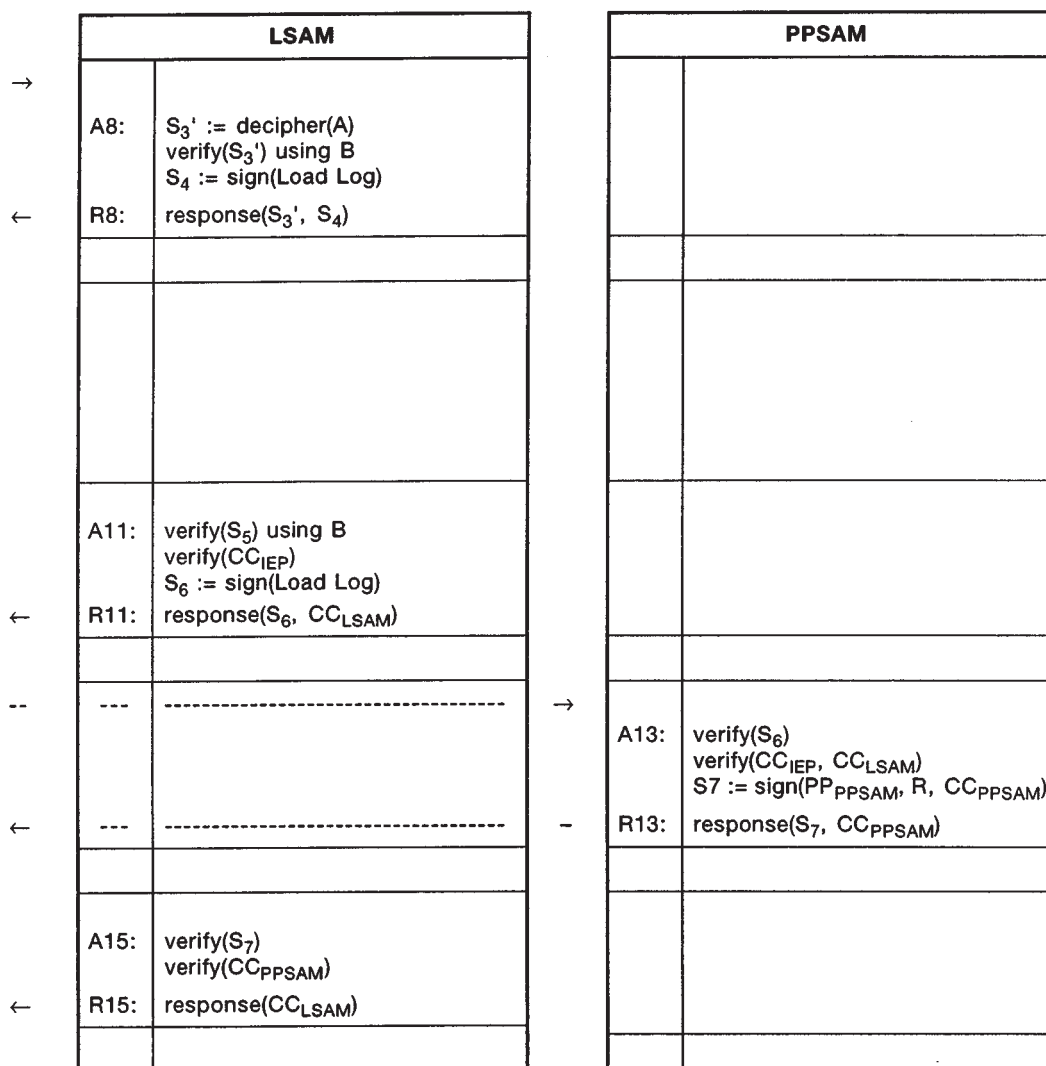


Bild 3 – Aufladetransaktion mit LSAM – rechte Hälfte (abgeschlossen)

ANMERKUNG Es handelt sich hierbei um ein begriffliches Modell, das nicht als Beispiel einer Implementation gewertet werden sollte. Gültige Implementationen müssen den Sicherheitsanforderungen dieses Teils der EN 1546 Rechnung tragen. So unterstützt dieses Aufladeprotokoll zum Beispiel Aufladetransaktionen, wie sie im Hinweis zu Bild 2 bereits beschrieben worden sind.

4.4.3 Zahlung

Die Zahlungstransaktion, die von der PDA als eine Interaktion zwischen der IEP und dem PSAM ausgeführt wird, bucht vom IEP-Saldo den vereinbarten Zahlungsbetrag ab und schreibt dem PSAM denselben Betrag gut. Das Zahlungstransaktionsprotokoll wird in Bild 4 (ausführlich) und in Anhang D (Überblick) dargestellt.

Für die Zahlungstransaktion bezieht diese Norm folgende Optionen ein:

- Einweg-, Zweiweg- oder Dualmodus-Authentisierung zwischen der IEP und dem PSAM, die Schutz gegen verschiedene Arten von Gefahren bieten (in 4.4.3.1 beschrieben);
- eine zusätzliche Signatur (S_1 in Bild 4), die Schutz gegen zusätzliche Gefahren bietet (in 4.4.3.1 beschrieben);
- eine signierte Quittung (Schritte C6 – R6 in Bild 4), die verschiedene Möglichkeiten der Fehlerbehebung bietet (in 4.4.3.2 beschrieben);
- feste Buchungsstufen, die eine schnelle wiederholte Abbuchungs-/Gutschrift-Phase (Schritte A3 – R5 in Bild 4) der Zahlungstransaktion bieten, was für einige Leistungen, z. B. Telekommunikation (in 4.4.3.3 beschrieben) nützlich ist.
- Einweg-Authentisierung mit individueller Transaktion, wie Abholung, die keine angriffssichere Realisierung eines PSAM erfordern.

So ist es zum Beispiel möglich, ein IEP-System ohne physikalischen PSAM zu implementieren, oder kombiniert mit einem PDA-PSAM, oder mit einem PSAM, das keine Gesamtsummen aufrechnet.

Die eigentlichen Nachrichten, die zwischen den Geräten einer Implementation ausgetauscht werden, werden in EN 1546-3 näher beschrieben; dort finden sich auch normierte Beschreibungen der Nachrichten zwischen IEP und PDA.

In manchen Systemen sind möglicherweise keine physikalisch angriffssicheren PSAMs implementiert. In diesem Fall muss die Authentizität der Software, Schlüssel und, wo erforderlich, Gesamtsummen usw. durch die Prozedur geschützt werden.

Die Kombinationsmöglichkeiten dieser Optionen sind in der folgenden Tabelle dargestellt:

Tabelle 1 – Übersicht der Optionen für Zahlungstransaktionen

Typ der Authentisierung	S_1	Signierte Quittung	Feste Buchungsstufen
Einweg	Nein	Nein	Nein
Einweg	Nein	Nein	Ja
Zweiweg	Nein	Nein	Nein
Zweiweg	Nein	Nein	Ja
Zweiweg	Nein	Ja	Nein
Zweiweg	Nein	Ja	Ja
Zweiweg	Ja	Nein	Nein
Zweiweg	Ja	Nein	Ja
Zweiweg	Ja	Ja	Nein
Zweiweg	Ja	Ja	Ja
Dualmodus	Nein	Nein	Ja
Dualmodus	Ja	Nein	Ja

4.4.3.1 Sicherheitsmerkmale der Zahlungstransaktion

Die Zahlungstransaktion kann unter Verwendung der Einweg-, Dualmodus- oder Zweiweg-Authentisierung realisiert werden. Dualmodus bedeutet, dass der erste Schritt unter Verwendung der Zweiweg-Authentisierung ausgeführt wird und die folgenden unter Verwendung der Einweg-Authentisierung.

Die IEP unterstützt entweder die Einweg-, Dualmodus- oder Zweiweg-Authentisierung. Der von der IEP geforderte Authentisierungsmodus wird in der Antwort auf den Initialisierungsbefehl festgelegt. Das PSAM sollte aus Gründen der Fähigkeit zur Zusammenarbeit in der Lage sein, mit allen Modi zu arbeiten.

Im Fall der Einweg-Authentisierung wird die IEP nach Identifikation des PSAM abgebucht. Im Fall der Zweiweg-Authentisierung wird die IEP nur abgebucht, nachdem sie das PSAM durch wahlweises Signieren von S_1 und Überprüfen von S_2 authentisiert hat. Eine Zweiweg-Authentisierung ohne S_1 ist auch möglich. In allen Fällen berechnet die IEP einen kryptographischen Nachweis (S_3) von ihrer Abbuchung, der vom PPSAM authentisiert wird. Der Zahlungsbetrag wird dem PSAM nur nach einer erfolgreichen Authentisierung des Nachweises der Abbuchung gutgeschrieben.

Eine Einweg-Authentisierung (die nur S_3 verwendet) der IEP durch das PSAM ist zum Schutz vor folgenden Gefahren vorgesehen:

- falsche (simulierte) IEPs;
- Wiederholen von Zahlungstransaktionen gegenüber PSAMs;
- Maskerade (Simulation einer IEP durch eine andere);
- Gutschreiben derselben Zahlungstransaktion auf mehr als ein PSAM.

Eine Zweiweg-Authentisierung (die S_2 und S_3 verwendet) ist zusätzlich zum Schutz vor folgenden Gefahren vorgesehen:

- Gutschrift durch falsche oder gestörte PSAMs oder Anwendungen;
- Unterbrechungs-Angriffe (systematische Versuche, von IEPs abzubuchen).

Durch S_1 ist es nicht möglich, einen reinen S_2 von einem reinen PSAM zu erhalten ohne einen reinen IEP zu haben. Folglich ist es nicht möglich, einen gefälschte PDA zu erzeugen, mit der man unerlaubterweise eine Gutschrift auf eine beliebige Zweiweg-Authentisierungs-IEP bekannter Identität und NT_{IEP} durchführen könnte.

Bei einem als Softwareimplementierung realisierten PSAM, das nicht in einem angriffssicheren Gerät, z.B. einem ICC, enthalten ist, kann eine Endsumme nur dann sicher aufgerechnet werden, wenn Details aller Transaktionen gespeichert werden. Die Zahlungstransaktion bei dieser Realisierung der PDA-PSAM-Komponente unterstützt nur die Einweg-Authentisierung (S_3).

4.4.3.2 Signierte Quittung zur IEP

Eine Fehlerbehebung nach einem Fehler (Fehlern) in der Zahlungstransaktion kann sich auf die Protokolle der IEP und des PSAM oder eine signierte Quittung der IEP stützen.

4.4.3.3 Feste Buchungsstufen

Eine Zahlungstransaktion kann ausgeführt werden als eine einzige Buchungsstufe des Zahlungsbetrags oder in mehreren festen Buchungsstufen von Teilbeträgen. Für jede benötigte feste Buchungsstufe wird die Folge [A3, C4, A4, R4, C5, A5, R5] wiederholt.

Nachdem R5 erhalten wurde, entscheidet die PDA, wie fortzufahren ist. Es bestehen die folgenden drei Möglichkeiten:

- mit A3 im Fall einer Zahlung mit fester Buchung, und wenn es eine weitere auszuführende Stufe gibt;
- mit C6, wenn die Transaktion abgeschlossen werden sollte und AM_{IEP} in R1 die Notwendigkeit für eine signierte Quittung anzeigt;
- mit C7, wenn die Transaktion abgeschlossen werden sollte und keine solche signierte Quittung benötigt wird.

Die Option der festen Buchungsstufe hat folgende Sicherheitseigenschaften:

- wenn Einweg- oder Zweiweg-Authentisierung verwendet wird, ist die Sicherheit gleich dem entsprechenden Authentisierungsmodus für eine Transaktion mit einer einzigen Buchungsstufe;
- wenn eine Dualmodus-Authentisierung verwendet wird, ist die Sicherheit mindestens gleichwertig einer Zahlungstransaktion mit einer einzigen Buchungsstufe unter Verwendung der Einweg-Authentisierung.

Im Fall einer Zahlungstransaktion mit fester Buchung werden unter Verwendung von entweder der Einweg- oder der Zweiweg-Authentisierung für jede feste Buchungsstufe, wie vom AM festgelegt, von der IEP die festgelegten festen Buchungsbeträge abgebucht und der PSAM gutgeschrieben. Für einige Realisierungen jedoch, z. B. im Telekommunikationsbereich, darf dem PSAM nur einmal (in der letzten Stufe) der gesamte Betrag gutgeschrieben werden, der von der IEP während der Transaktion abgebucht wird. In diesem Fall wird im Befehl PSAM Gutschreiben nur die Signatur (S₃) der letzten Stufe übertragen und M wird durch MTOT ersetzt, das durch die PDA berechnet wird.

Im Fall einer Zweiweg-Authentisierung berechnet das PSAM S₂, die entweder als ein Authentisierungsparameter dient, den die IEP überprüft, bevor sie ihr Saldo abbucht (für alle festen Buchungsstufen außer der letzten) oder als eine Quittung für die IEP nach der letzten Stufe, falls dies erforderlich ist. In einer Transaktion mit fester Buchung ohne Quittung braucht das letzte S₂ nicht vom PSAM berechnet zu werden, wenn die PDA in A3 erkennt, dass dies eigentlich die letzte Stufe ist, z. B. hat der Börseninhaber im Fall eines Telefongesprächs eingehängt.

Im Fall der Dualmodus-Authentisierung braucht das PSAM S₂ nur für die erste Stufe zu berechnen (wenn der Befehl Initialisieren der PSAM zur Zahlung empfangen wird) und für die letzte feste Buchungsstufe, falls die PDA die letzte Stufe zum PSAM bestimmen kann.

4.4.3.4 Signieren und Protokollieren einzelner Transaktionen

Dieser Teil von EN 1546 beruht im Allgemeinen auf dem Austausch von Endsummen (eine Endsumme je Börsenanbieter je Währung, die von der Zahlungseinrichtung bearbeitet wird) zwischen Zahlungseinrichtungen und dem Zentralrechner des Börsenanbieters.

Für die Protokollierung und/oder statistische Zwecke kann der Börsenanbieter auch ausführliche Informationen über einzelne Transaktionen benötigen.

Die Entscheidung darüber, einzelne Transaktionen zu signieren und zu protokollieren wird vom PPSAM in Stufe A7 vorgenommen, beruhend auf Transaktionsdaten, z. B. IEP-Bezeichner und Beendigungscode, und Parametern im PSAM, die außerhalb des Anwendungsbereichs dieser Norm liegen.

4.4.3.5 Anonyme Transaktionsverfahren

In diesem Teil von EN 1546 beruhen die Sicherheitsprotokolle und die Funktionalität des IEP-Systems darauf, dass jede Transaktion einmalig ist. Diese Eigenschaft wird dadurch erreicht, dass jede IEP-Identität einmalig ist und ein zunehmender IEP-Transaktionszähler verwendet wird. Diese Daten müssen bei jeder Transaktion über die Schnittstelle gehen. Bei unverschlüsselten Daten können einzelne IEP-Transaktionen optional protokolliert werden.

Dieser Teil der EN 1546 schließt die Verwendung anonymer Zahlungstransaktionsverfahren nicht aus, bei denen die Daten, die die Einmaligkeit der Transaktion gewährleisten, so über die Schnittstelle gehen, dass ihre Identität nicht offengelegt wird. Das Verfahren, das die Anonymität gewährleistet, wird jedoch nicht beschrieben.

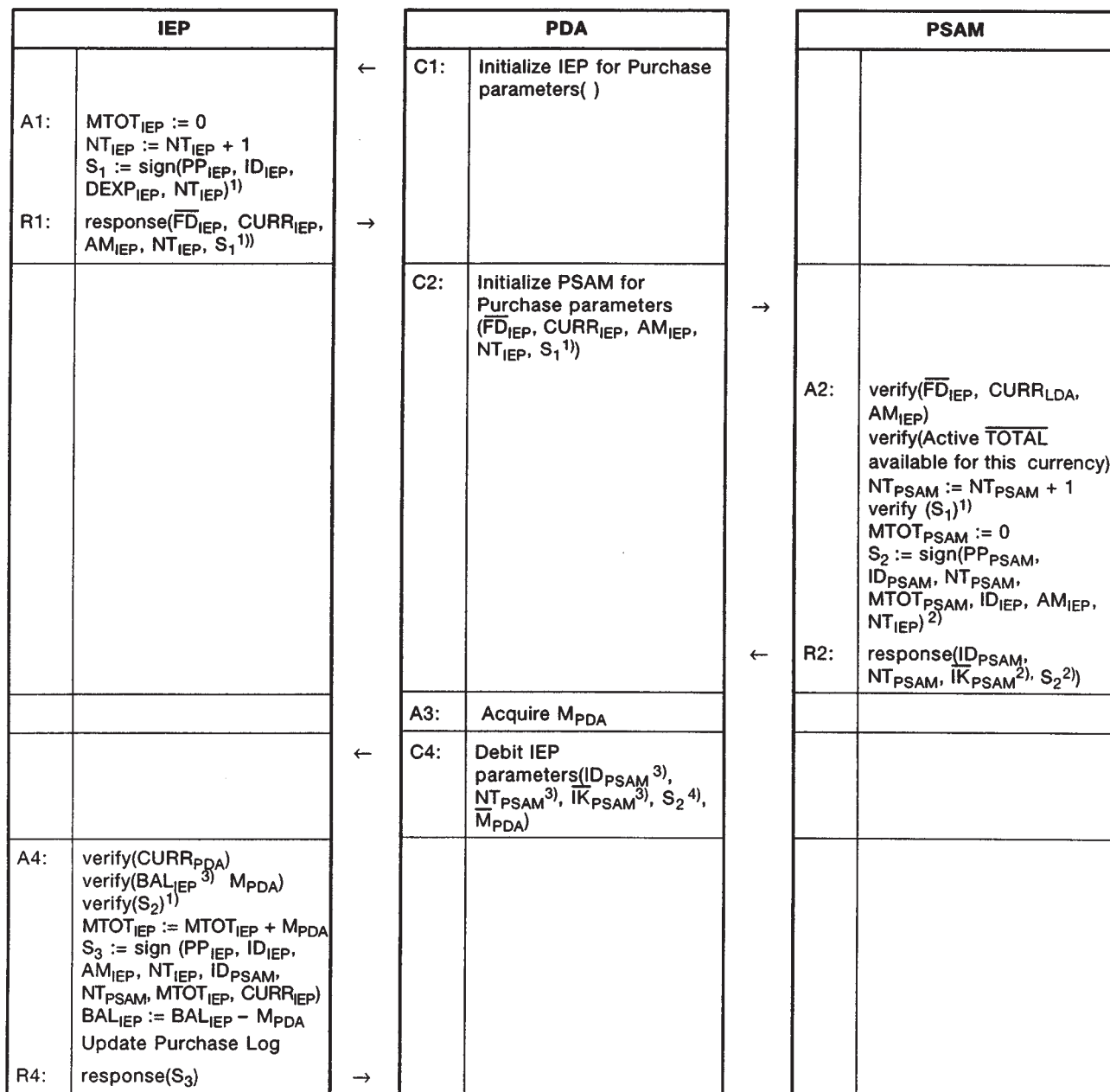


Bild 4 – Zahlungstransaktion (fortgesetzt)

- 1) Im Fall einer Zweiweg- oder Dualmodus-Authentisierung unter bestimmten Bedingungen ausgeführt/gesendet. Wird von der IEP zum PSAM durch die Verwendung eines AM_{IEP} angezeigt.
- 2) Im Fall einer Zweiweg- oder Dualmodus-Authentisierung. Wird von der IEP zum PSAM durch die Verwendung eines AM_{IEP} angezeigt.
- 3) Nur in der ersten Stufe bei aufeinander folgenden Stufen bei Zahlungstransaktionen mit fester Buchung gesendet.
- 4) Nicht benötigt für:
- Einweg-Authentisierung;
 - aufeinander folgende Stufen bei Zahlungstransaktionen mit fester Buchung unter Verwendung der Dualmodus-Authentisierung.

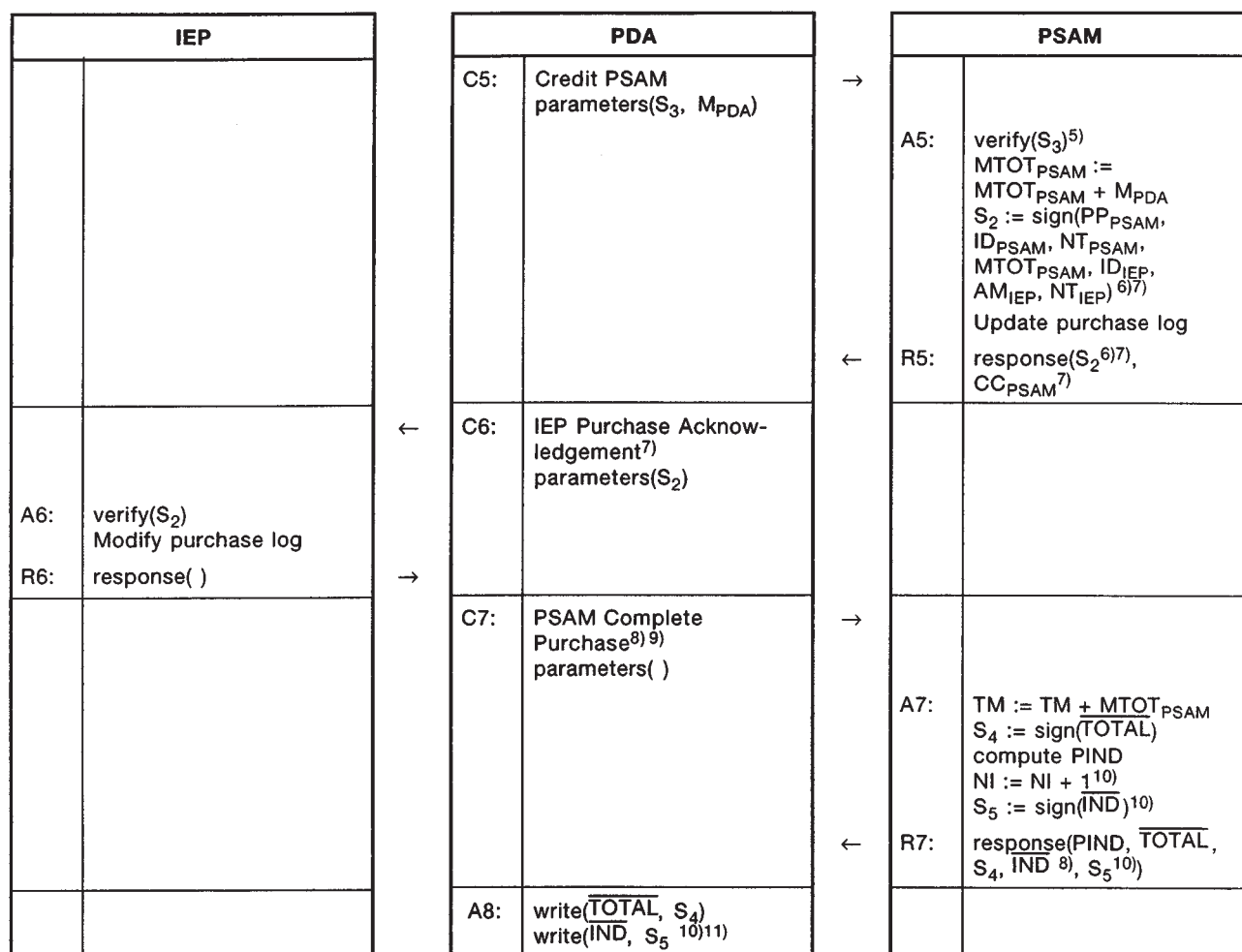


Bild 4 – Zahlungstransaktion (abgeschlossen)

ANMERKUNG 1 Es handelt sich hierbei um ein begriffliches Modell, das nicht als Beispiel einer Implementation gewertet werden sollte. Gültige Implementationen müssen den Sicherheitsanforderungen dieses Teils der EN 1546 Rechnung tragen.

ANMERKUNG 2 Bei Systemen mit entfernten PSAMs, ist eine Zahlungstransaktion mittels Zweiweg-Authentisierung und lediglich zwei Austauschvorgängen zwischen Terminal und entferntem Knoten möglich.

ANMERKUNG 3 Bei Systemen ohne Gesamtsummen, muss der Käufer einen Teil der Transaktionsdaten pflegen und testen, zum Beispiel die einmalige Transaktionsvorgangsnummer (NT_{PSAM}), um die Annahme doppelter Transaktionen zu vermeiden.

4.4.4 Zahlungsabbruch/IEP-Saldobereinigung (optional)

Diese Transaktion, die von der PDA als eine Interaktion zwischen der IEP und dem PSAM ausgeführt wird,

- bucht dem PSAM-Saldo den Betrag der letzten (und möglicherweise einzigen) Stufe der letzten Zahlungstransaktion ab und schreibt ihn dem IEP-Saldo gut, falls dies in beiden Geräten erfolgreich war (Abbruch);
- schreibt nur dem IEP-Saldo gut, wenn die letzte Stufe zwar in der IEP erfolgreich war, aber nicht im PSAM (IEP-Saldobereinigung).

Das Sicherheitsprotokoll ist in Bild 5 dargestellt.

5) Die Signatur muss unter Verwendung von $MTOT' = MTOT_{PSAM} + M_{PDA}$ überprüft werden (da $MTOT_{PSAM}$ nicht vor einer erfolgreichen Prüfung von S_3 aktualisiert werden darf).

6) Im Fall einer Zweiweg-Authentisierung gesendet.

7) Die IEP-Zahlungsqittung wird nur gesendet, wenn sie vom IEP angefordert wird: Das wird von der IEP zum PSAM durch die Verwendung eines AM_{IEP} angezeigt. Das PSAM übersetzt diese Information an die PDA durch Verwendung eines CC_{PSAM} .

8) Eine Endsumme summieren, sie zu senden und zu signieren kann nur so weit gesichert werden, wie es die PSAM-Realisierung zulässt.

9) Nicht verwendet bei Systemen ohne Endsumme.

10) Wird nur ausgeführt/gesendet, wenn $PIND = TRUE$ (einzelne zu erzeugende Transaktion).

11) Bei Systemen ohne Endsumme wird S_3 anstatt S_5 verwendet.

Nach der Initialisierung der Transaktion überprüft die IEP, ob die letzte Zahlungstransaktion erfolgreich war, ansonsten weist sie die Abbruch-/Fehlerbehebungsanforderung zurück. Sie prüft ebenfalls, ob der Höchstsaldo, den die IEP besitzen darf, gleich oder größer als die Summe aus dem aktuellen IEP-Saldo und dem zu stornierenden Betrag ist. Dies geschieht, um sicherzustellen, dass, falls in der Zwischenzeit ein Aufladen vorgenommen wurde (kein normales Ereignis), dann der Höchstsaldo durch den Abbruch trotzdem nicht überschritten werden würde. Wenn diese Überprüfungen erfolgreich sind, berechnet die IEP ein Abbruch-/Fehlerbehebungszertifikat (S_1), das aus den Transaktions- und den Authentisierungsparametern besteht, wobei die Transaktionsparameter dem Zahlungsprotokoll entnommen sind. Die IEP überträgt S_1 und die entsprechenden Parameter zum PSAM. Das PSAM prüft S_1 und bestätigt folgende Bedingungen:

- die empfangenen IEP-Parameter entsprechen einer Zahlungstransaktion, die noch im PSAM protokolliert ist;
- dass diese Zahlungstransaktion nicht vorhergehend zurückgenommen worden ist;
- ob die Zahlungstransaktion dem PSAM gutgeschrieben wurde oder nicht.

Wenn die ersten beiden Bedingungen erfüllt sind, akzeptiert das PSAM die Zahlungsabbruchtransaktion und berechnet ein Gutschrift-IEP-Zertifikat (S_2). Wenn eine (oder beide) dieser zwei Bedingungen ungültig ist, weist das PSAM die Abbruchtransaktion zurück.

Wenn die letzte Bedingung zeigt, dass die Transaktion dem PSAM gutgeschrieben wurde, bucht das PSAM ebenfalls den Gesamtbetrag in der entsprechenden Endsumme ab. Das PSAM überträgt S_2 und die entsprechenden Parameter an die IEP. Nach der Überprüfung von S_2 macht die IEP in ihrem Saldo die Gutschrift des Betrags der letzten Stufe der Zahlungstransaktion rückgängig.

Die Endsumme des PSAM und, falls erforderlich, die einzelnen Transaktionsparameter zur Speicherung in der PDA werden vom PSAM aktualisiert.

Dieses Protokoll ist vorgesehen zum Schutz vor:

- erfolgreichem Wiederholen von Zahlungsabbruch-/IEP-Saldobereinigungstransaktionen (S_1);
- Fehlfunktion von IEPs am Anfang der Transaktion (S_1);
- Unterbrechungs-Angriffen, wenn der PSAM-Saldo ohne Berechtigung verringert wird (S_1);
- unberechtigtem Rückgängigmachen von Gutschriften von IEPs (S_2).

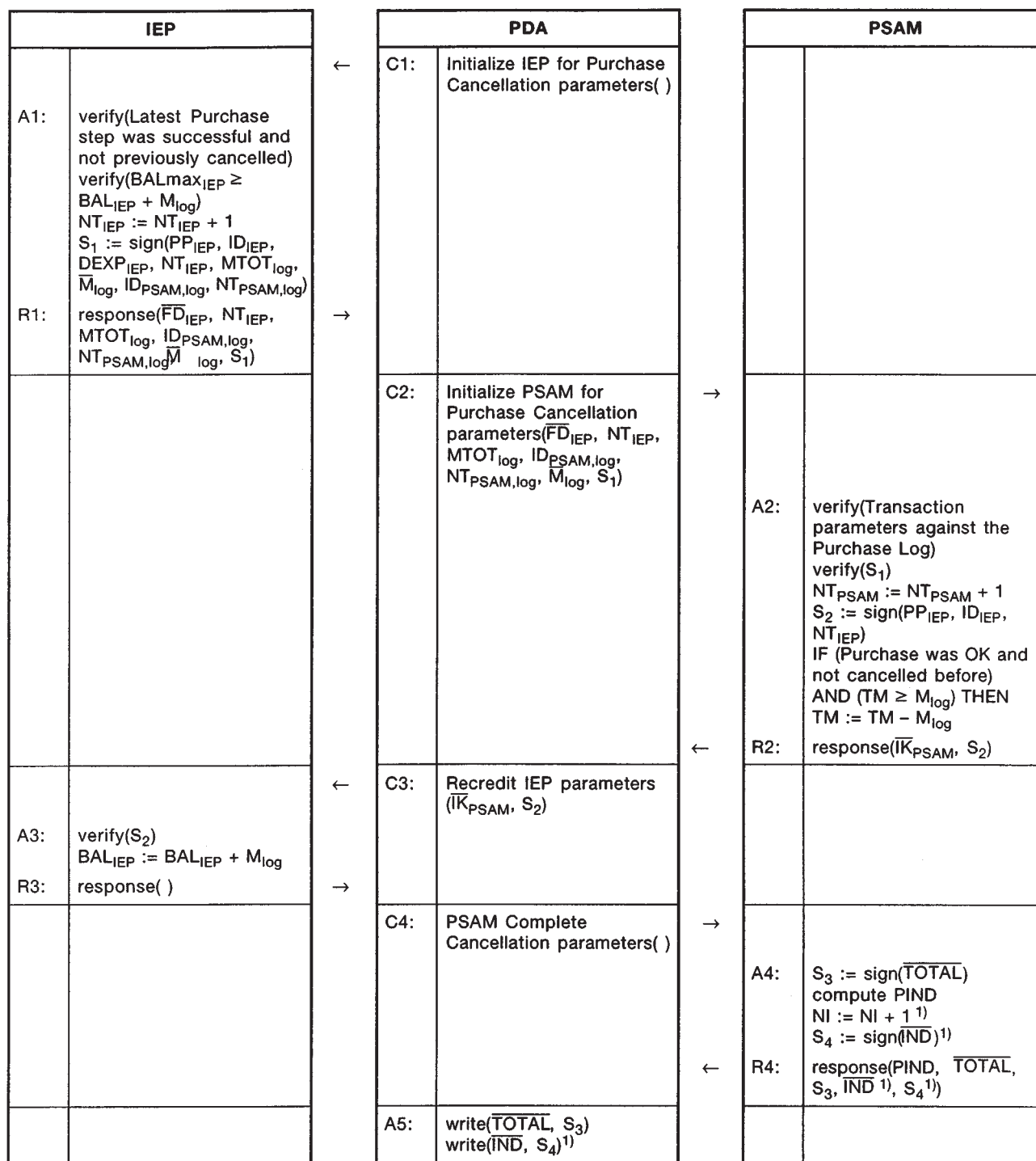


Bild 5 – Zahlungsabbruch/IEP-Saldbereinigungstransaktion

ANMERKUNG Es handelt sich hierbei um ein begriffliches Modell, das nicht als Beispiel einer Implementation gewertet werden sollte. Gültige Implementationen müssen den Sicherheitsanforderungen dieses Teils der EN 1546 Rechnung tragen.

1) Wird nur ausgeführt/gesendet, wenn PIND = TRUE (einzelne zu erzeugende Transaktion).

Anhang A (informativ) Zusätzliche Sicherheitsprozeduren

A.1 IEP-Transaktionen

A.1.1 Währungsumrechnung

Die Währungsumrechnungstransaktion, die von einer Aufladeeinrichtung oder einer Sondereinrichtung als eine Interaktion zwischen der IEP und dem PPSAM durchgeführt wird, rechnet den gesamten IEP-Saldo von einer Währung in einen gleichwertigen Saldo in einer anderen Währung um, wie es in Bild A.1 festgelegt ist.

Diese Transaktion umfasst drei einfachere, primitivere Prozesse, nämlich Zahlung (bei der IEP-Saldo in der aktuellen Währung auf Null gesetzt wird), IEP-Parameter-Aktualisierung, z. B. wird die $CURR_{IEP}$ geändert, und einem Ladevorgang in der neuen Währung.

Es wird vorausgesetzt, dass der Börseninhaber bereits mit dem Wechselkurs einverstanden ist, bevor die Transaktion gestartet wird, oder spätestens bevor der Befehl Umrechnen der IEP-Währung zur IEP gesendet wird.

Diese Transaktion verwendet die Einweg-Authentisierung des PPSAM und eine signierte Quittung von der IEP. Zusätzlich beginnt die IEP mit dem Signieren (unter anderen Daten) ihres Saldos und ihrer Transaktionsnummer (S_1). Die IEP-Parameter und S_1 werden dann an das PPSAM zur Überprüfung gesendet. Wenn diese Überprüfung erfolgreich ist, berechnet das PPSAM ein Zertifikat (S_2), das es der IEP ermöglicht, ihren Saldo in die neue Währung umzuwandeln.

Nachdem die Umrechnung durchgeführt worden ist, wird eine signierte Quittung an das PPSAM gesendet – selbst in dem Fall, wenn die Umrechnung nicht erfolgreich war. Diese Quittung garantiert eine spätere Authentisierung der IEP durch das PPSAM und kann für Zwecke der Protokollierung verwendet werden.

Das Protokoll ist zum Schutz gegen folgende Gefahren vorgesehen:

- Währungsumrechnung durch falsche PPSAMs (S_2);
- Währungsumrechnung in anderen IEPs (S_1 und S_2);
- Wiederholen von alten Währungsumrechnungszertifikaten an die IEP (S_1 und S_2);
- Unsicherheit im PPSAM, ob die Umrechnung erfolgreich war oder nicht (S_3).

ANMERKUNG Vorgänge mit mehreren Währungen können entweder durch die Verwendung entsprechend vieler IEP-Anwendungen durchgeführt werden oder durch Kombination der Währungen innerhalb der IEP-Anwendung.