

Identification card systems — Inter-sector electronic purse —

Part 2: Security architecture

The European Standard EN 1546-2:1999 has the status of a
British Standard

ICS 35.240.15

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

BSI
Documents



Document Sharing Hub

National foreword

This British Standard is the English language version of EN 1546-2:1999.
The UK participation in its preparation was entrusted to Technical Committee IST/17, Identification cards and related devices, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled “International Standards Correspondence Index”, or by using the “Find” facility of the BSI Standards Electronic Catalogue.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the EN title page, pages 2 to 110, an inside back cover and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Committee and comes into effect on 15 January 2000

© BSI 01-2000

Amendments issued since publication

Amd. No.	Date	Comments

ISBN 0 580 35213 7

English version

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

Identifikationskartensysteme – Branchenübergreifende
elektronische Geldbörse – Teil 2: Sicherheits-Architektur

This European Standard was approved by CEN on 20 May 1999.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the Central Secretariat has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.



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

Central Secretariat: rue de Stassart, 36 B-1050 Brussels

Contents

Foreword	4
1 Scope	5
2 Normative references	5
3 Definitions, symbols and abbreviations	6
3.1 Definitions	6
3.1.1 Terms defined in prEN 1546-1	6
3.1.2 Terms specific to this part of EN 1546	7
3.2 Symbols	8
3.3 Abbreviations	8
3.4 Special notation	9
4 Security Architecture	10
4.1 Security requirements and characteristics	10
4.2 Error handling	11
4.3 Security relevant data elements	12
4.4 Security procedures	14
4.4.1 General notes	14
4.4.2 Load (optional)	16
4.4.3 Purchase	24
4.4.4 Purchase Cancellation/IEP Balance Recovery (optional)	29
Annex A (informative) Additional security procedures	32
A.1 IEP transactions	32
A.1.1 Currency Exchange	32
A.1.2 IEP Monitoring	34
A.1.3 Update IEP parameter	34
A.2 SAM transactions	36
A.2.1 Collection	36
A.2.2 SAM Monitoring	42
A.2.3 Update SAM parameter	42
A.2.4 Open SAM	46
A.2.5 Close SAM	47
Annex B (informative) Security requirements and security mechanisms	48
Annex C (informative) Key Management	51
C.1 General	51
C.2 Key Management for symmetric algorithms	51
C.2.1 IEP/PSAM communication	51
C.2.2 Partitioned master keys for the Purchase transaction	51
C.2.3 IEP/PPSAM communication	52
C.2.4 PSAM/PPSAM communication	52
C.2.5 LSAM/PPSAM communication	53
C.2.6 Key separation	53
C.2.7 Key modification	53
C.3 Key Management for asymmetric algorithms	54
C.3.1 General requirements for key certification	54
C.3.2 Key Management requirements	55
C.3.3 Topology of the IEP System	56
C.3.4 The operational requirements	56
C.3.5 The pre-operational requirements	57
C.3.6 The operational phase key modification requirements	58
C.3.7 Specification of PKCs	59
C.3.8 Key Management requirements for interactive Signatures	59
Annex D (informative) High-level overview of the Purchase transaction	60
Annex E (informative) Security protocols using DES	64

E.1	Specific notes for DES.....	64
E.1.1	Encipherment/Decipherment using DES.....	64
E.1.2	Authentication using DES	64
E.1.3	Implementation notes for DES	65
E.2	Data elements specific for DES.....	65
E.3	Security protocols	65
E.3.1	Load	65
E.3.2	Purchase	73
E.3.3	Collection.....	77
Annex F (informative)	Security protocols using RSA/DSS.....	83
F.1	Specific notes for RSA.....	83
F.1.1	Authentication using RSA	83
F.1.2	Public key certification using RSA.....	83
F.2	Specific notes for DSS.....	84
F.2.1	Authentication using DSS	84
F.2.2	Public key certification using DSS.....	85
F.3	Use of public key certificates in IEP Systems.....	86
F.4	Data elements specific for RSA/DSS	86
F.5	Implementation notes for RSA/DSS	86
F.6	Security protocols	87
F.6.1	Load	87
F.6.2	Purchase	96
F.6.3	Collection.....	101
Annex G (informative)	Purchase transaction using 3-step interactive Signatures	107
G.1	Data elements	107
G.2	Changes to subclause 4.4.3.....	107
G.3	Specific notes for interactive Signatures.....	107
G.4	Data elements specific to interactive Signatures	108
G.5	Security protocols.....	108
G.5.1	Purchase	108

Foreword

This European Standard has been prepared by Technical Committee CEN/TC 224 "Machine-readable cards, related device interfaces and operations", the Secretariat of which is held by AFNOR.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by January 2000, and conflicting national standards shall be withdrawn at the latest by January 2000.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom.

Annexes designated as "normative" are part of the body of the standard. Annexes designated "informative" are given for information only. In this standard, annexes A to G are informative.

This European Standard consists of the following parts, under the general title "Identification card systems - Inter-sector electronic purse" :

- *Part 1: Definitions, concepts and structures*
- *Part 2: Security architecture*
- *Part 3: Data elements and interchanges*
- *Part 4 : Data objects*

1 Scope

This part of EN 1546 defines the detailed security architecture for IEP systems as they are described in prEN 1546-1. It also describes the application protocols, the use of cryptographic algorithms and some underlying assumptions concerning the key management necessary to implement IEP systems with sufficient security levels.

The general architecture described here allows many types of implementation. It should be noted that the informative annexes of this standard focus on particular implementations.

As time progresses it is envisaged that other implementations may come into focus.

The security architecture defines the security procedures needed at the application level of the IEP system transactions described in prEN 1546-1, A.5 and A.6. This architecture relies on the basic assumptions stated in prEN 1546-1, 1.4.

Manual error recovery is outside the scope of this standard. Audit information needed for performing manual error recovery procedures is, however, covered by this standard.

The description in this part of the standard is in the form of ordered exchanges of data between distinct conceptual devices. Operational instructions performed by these devices produce the required ordered exchanges. Examples of meanings of the required operational instructions are presented as mathematical formulae in informative annexes. The transactions in this part of the standard are described as functional requirements. They define the order of cryptographic proofs and verifications and their related data elements necessary to achieve security in an IEP system.

An IEP system conforming to the security architecture defined in this part of EN 1546 may be implemented in physical devices using generally practised programming techniques. Optimization of computations and data exchanges which preserve the operational requirements of the ordered data exchanges may also be implemented.

The data elements and interchanges defined in this part of EN 1546 primarily address security issues. In order to fulfil requirements of the IEP System other than security, further data elements and interchanges may be added. The detailed formats of data elements and interchanges between IEPs and devices are described in EN 1546-3 (Data elements and interchanges).

2 Normative references

This **Error! Reference source not found.** incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this **Error! Reference source not found.** only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

prEN 1546-1, *Identification card systems - Inter-sector electronic purse - Part 1 : Definitions, concepts and structures.*

EN 1546-3, *Identification card systems - Inter-sector electronic purse - Part 3 : Data elements and interchanges.*

prEN 1546-4, *Identification card systems - Inter-sector electronic purse - Part 4 : Devices.*

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

ISO/CEI 9797, *Information technology - Security techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm.*

3 Definitions, symbols and abbreviations

3.1 Definitions

3.1.1 Terms defined in prEN 1546-1

This part of EN 1546 uses the following terms defined in prEN 1546-1:

- 1) activation;
- 2) aggregation;
- 3) authentication;
- 4) cancellation;
- 5) collection;
- 6) currency exchange;
- 7) deactivation;
- 8) electronic value;
- 9) error recovery;
- 10) identity;
- 11) inter-sector electronic purse (IEP);
- 12) IEP balance;
- 13) IEP monitor;
- 14) IEP system;
- 15) key management;
- 16) key management system;
- 17) load;
- 18) load agent;
- 19) load device;
- 20) load log;
- 21) load SAM;
- 22) negative file;
- 23) Personal Identification Number (PIN);
- 24) purchase;
- 25) purchase cancellation;
- 26) purchase device;
- 27) purchase log;

- 28) purchase SAM;
- 29) purse holder;
- 30) purse provider;
- 31) purse provider host;
- 32) purse provider SAM;
- 33) Secure Application Module (SAM);
- 34) SAM monitor;
- 35) security architecture;
- 36) service provider;
- 37) total;
- 38) value.

In order to emphasize terms specific to a general IEP system, throughout EN 1546, these terms commence with capital letters, e.g. Service Provider.

3.1.2 Terms specific to this part of EN 1546

For the purpose of this part of EN 1546, the following definitions apply:

3.1.2.1

completion code

a part of the response to any component on a given command. It indicates whether the command was successfully performed or not; in the latter case the completion code indicates the reason why it was not successful

3.1.2.2

disruption attack

systematic attempts to disturb the normal functioning of the IEP System by preventing transactions from being performed, e.g. debiting the balance of a component without allowing the associated balance of another component to be correspondingly credited

3.1.2.3

dual-mode authentication

this mode applies only to Incremental Purchase Transactions where the first debit-credit step is performed in Two-way Authentication mode and further steps are performed in One-way Authentication mode

3.1.2.4

incremental purchase transaction

a Purchase transaction performed in serial steps, each being a debit of the IEP and a credit of the PSAM

3.1.2.5

masquerading

pretending to be a genuine device, e.g. an IEP, by simulation. Can be prevented by use of secret information, e.g. keys within the genuine devices

3.1.2.6

message authentication code

a code, in a message between a sender and a receiver, used to validate the source and part or all of the text of a message. The code is the result of an agreed calculation

3.1.2.7

non-repudiation

providing cryptographic proof that neither the originator nor the receiver can repudiate having sent/received a given message with its original contents

3.1.2.8

one-way authentication

a transaction between two components where only one component is authenticated by the other, e.g. only the IEP is authenticated by the PSAM in Purchase transactions in this mode

3.1.2.9

replay

to obtain messages from a real IEP transaction and try to replay it later in order to duplicate a transaction or similar. Can be prevented by having some unique information only valid for a single transaction

3.1.2.10

signature

in this standard, (digital) signatures are used in the security protocols to authenticate both devices and the integrity of data

3.1.2.11

two-way authentication

a transaction between two components where each component is authenticated by the other

In order to emphasize terms specific to a general IEP system, throughout EN 1546, these terms commence with capital letters, e.g. Completion Code.

3.2 Symbols

$\wedge$	Logical AND
$\vee$	Logical OR
$\in$	Belongs to
$\notin$	Does not belong to
k	Concatenation (of data elements)
$\{ \}$	Set (of data elements)
$()$ or $[]$	Ordered set (of data elements)
$:=$	Assignment
$::=$	Definition
$\overline{A}$	Vector (identifier for an ordered set of data elements)

3.3 Abbreviations

DES	Data Encryption Standard (cryptographic algorithm)
DSS	Digital Signature Standard (cryptographic algorithm)
IEP	Inter-sector Electronic Purse
LDA	Load Device Application
LSAM	Load SAM
PDA	Purchase Device Application
PIN	Personal Identification Number
PK	Public Key
PKC	Public Key Certificate

PSAM	Purchase SAM
PPSAM	Purse Provider SAM
RSA	Rivest, Shamir and Adleman (cryptographic algorithm)
SAM	Secure Application Module

3.4 Special notation

The notation used in the figures for the security protocols defined in subclause 4.4 is given below.

Each figure shows the components involved in a specific transaction, e.g. an IEP, a PDA and a PSAM are involved in a Purchase transaction.

For each device involved, two columns are defined. For the left-most column the following definitions apply:

- Cn: Denotes a command sent to another component;
- An: Denotes the action(s) to be performed by the receiving component;
- Rn: Denotes a response to be sent to the originator of the command.

In the next column the definition of what to do for a specific action is shown. Furthermore, parameters to be sent in a command or a response are listed. Only security related data elements are included in the figures.

Special notations related to this column are as follows (this specific notation is used mainly in the figures in the normative part of this standard) :

- compare() Compare the parameters listed in the brackets;
- decipher() Decipher the parameters listed in the brackets;
- encipher() Encipher the parameters listed in the brackets;
- parameters() Transmit the parameters listed in the brackets as a command;
- response() Transmit the parameters listed in the brackets as a response;
- select() Select the parameters listed in the brackets;
- sign() Sign the parameters listed in the brackets;
- verify() Verify the parameters listed in the brackets;
- write() Write/update the parameters listed in the brackets.

Specific descriptions of these operations are used in the annexes, which describe detailed examples of how to implement the transactions using various cryptographic algorithms:

- command() [] The command given by the name in the brackets is sent using the parameters listed in the square brackets;
- decipher(K) [] The decipher function is evaluated with the parameters listed in the square brackets using the key K;
- encipher(K) [] The encipher function is evaluated with the parameters listed in the square brackets using the key K;
- hash [] A hash function is evaluated with the parameters listed in the square brackets;

response()	The parameters in the brackets are sent out in a response (always including a Completion Code);
select() []	The information detailed in the brackets is selected from a set of data elements listed in the square brackets;
sign(K) []	The signature function is evaluated with the parameters listed in the square brackets using the key K;
verify(K) []	The verification function is evaluated with the parameters listed in the square brackets using the key K. In contrast to the general verify() function, this function is a specific cryptographic operation depending on the given algorithm;
write() []	The parameters listed in the square brackets are written to the file indicated in the normal brackets. Comments will indicate whether the data is appended to the file or used to update existing data.

4 Security Architecture

The Security Architecture as defined here is designed to protect against intentional fraud as well as some kinds of equipment malfunction. There is, however, no protection against human error when operating the equipment, e.g. keying in a wrong amount, as this cannot be detected by the equipment itself. These errors shall be handled by error procedures which possibly require human intervention.

Operational procedures and business contracts between the participants are not covered by this standard, although some of the underlying assumptions have been taken into consideration. However, this part of EN 1546 includes requirements for keeping information and proofs which are necessary for these procedures.

Trade-offs between security levels and the cost of implementing and operating IEP Systems are not explicitly covered.

Irrespective of the chosen Security Architecture, secret and public key cryptosystems may be involved and the necessary keys shall be generated and distributed in a controlled way to avoid their compromise. The basic assumptions concerning Key Management required to specify the Security Architecture are described in Annex C (informative), but implementation of any specific Key Management scheme is outside the scope of this part of EN 1546.

4.1 Security requirements and characteristics

The main requirements of the Security Architecture are to prevent:

- a) value being debited or credited in IEPs or SAMs in a way not intended by the Purse Provider;
- b) value being exchanged without agreement between the participants involved, e.g. the Purse Holder and the Service Provider;
- c) participants defrauding others without detection;

and to enable:

- d) the balanced exchange of Value;
- e) recovery procedures in the event of error;
- f) provision of adequate data to resolve conflicts.

More detailed security requirements for each transaction in IEP Systems are shown, for information, in Annex B.

The Security Architecture of IEP Systems has the following main characteristics, provided that the basic assumptions stated in prEN 1546-1, subclause 1.4 are fulfilled:

- a) in an IEP System, the Purse Provider carries the risk of fraud in the system and therefore defines the necessary security level by selecting a specific Security Architecture;
- b) parts of the overall security of an IEP System are based on contractual agreements between individual business partners. This is particularly important when delegation of tasks and responsibilities takes place;
- c) the Security Architecture provides protection against duplication and unauthorized modification of transactions, Masquerading and repudiation of transactions once they have been executed;
- d) a SAM is in general needed where critical security related functions, such as Authentication and Non-repudiation, need to be performed or when critical data, such as cryptographic keys and Negative File(s), need to be securely stored;
- e) end-to-end security protocols exist between the following component pairs, if present:
 - IEP ↔ PPSAM, e.g. for Load transactions;
 - IEP ↔ PSAM, e.g. for Purchase transactions;
 - LSAM ↔ PPSAM, e.g. for Load transactions;
- f) each IEP and SAM shall be uniquely identified;
- g) updates of data in two different components, e.g. the IEP Balance and the Total in the PSAM, are designed to minimize the risk of loss of synchronization. If a transaction is prematurely aborted, the two components may, where there are no security risks involved, enable a roll-back to cancel (or roll-forward to complete) any updates already made, but this may require human intervention;
- h) audit based on individual transactions is possible;
- i) functions are defined for maintaining at least limited Negative File(s) in some or all of the SAMs in the IEP System;
- j) the IEP is assumed to contain only one type of cryptographic algorithm.

4.2 Error handling

Error handling takes place in different devices, of which only some are trusted by the Purse Provider. Additionally, error handling takes place at different protocol layers. A simplified model showing two communicating devices, each consisting of a transport layer and an application layer as well as a local data store which can also cause errors, is shown in figure 1.

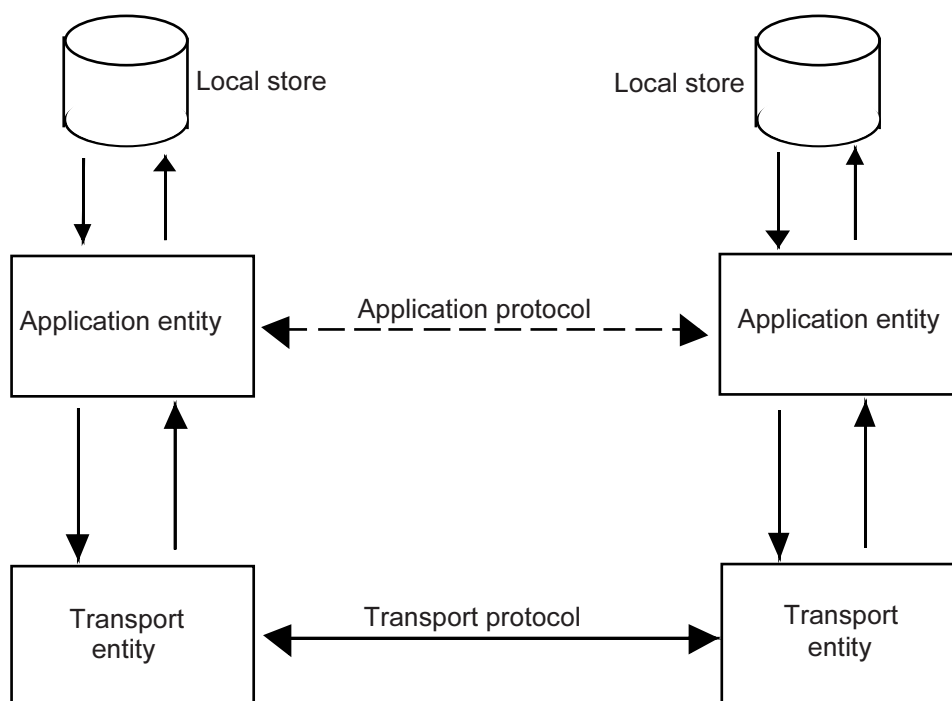


Figure 1 - Protocol layers in the IEP System

Only error handling at the application layer is within the scope of this part of EN 1546. Errors at a lower layer shall either be recovered at this layer or signalled to the application layer as unrecoverable.

From a security point of view, no critical error handling can be expected from devices not directly controlled by the Purse Provider. The error handling in such devices can, however, initiate secure error handling in the trusted devices.

A device controlling communication between two trusted devices, e.g. a Purchase Device establishing communication between an IEP and a PSAM, shall normally try to inform the other device in case one device rejects a command (or an unrecoverable error at a lower layer is detected). Likewise, such a controlling device shall instruct the failing device to terminate the current transaction if applicable. Finally, the controlling device should store information on the failure.

As a general principle, the security components defined shall always perform all actions prescribed when receiving a command. In case the power is removed or the component is reset, sufficient information shall be present to perform a full roll-back or roll-forward following the next power-on or after the reset respectively, in such a way that there are no security risks involved. This Error Recovery shall be performed before accepting other commands.

More detailed error handling is described in prEN 1546-4 and a list of Completion Codes is given in EN 1546-3.

4.3 Security relevant data elements

This part of EN 1546 defines security related aspects of all transactions in IEP Systems. For clarity, conceptual data elements are also defined, although they may not exist in actual implementations.

Data elements are stored in different components of the IEP System
(COMP ::= IEP/LSAM/PSAM/PPSAM).

Where applicable, possible values of the data elements are given in brackets.

Data elements which are specific to a certain algorithm are detailed in the informative Annexes E, F and G for the given algorithm.

ALG_{COMP}	Denotes the algorithm used by the component.
AM_{IEP}	Authentication Mode(s) required by the IEP for Purchase transactions (ONE_WAY/TWO_WAY/DUAL_MODE). Furthermore, it specifies whether S_1 is computed by the IEP ($S1_BIT$) and whether a signed acknowledgement is required (ACK_BIT).
BAL_{COMP}	Balance of the component.
$\overline{BAL}_{COMP}$	Data vector containing Balance and corresponding currency code.
BAL_{max_COMP}	Maximum balance of the component.
CC_{COMP}	Completion Code (as sent by the component).
CT	Completion status in the PSAM related to a Total (ACTIVE/OFF-LINE_COLLECTED/ON-LINE_COLLECTED).
$CURR_{COMP}$	Currency code of the component.
$DACT_{COMP}$	Activation date of the component.
$DATE_{COMP}$	Current date of the component.
$DDEA_{COMP}$	Deactivation date of the component.
$DEXP_{COMP}$	Expiry date for the component.
$\overline{FD}_{IEP}$	Fixed data vector transmitted by the IEP. It comprises the following data elements: PP_{IEP} , ID_{IEP} , ALG_{IEP} , $\overline{IK}_{IEP}$ and $DEXP_{IEP}$
$\overline{FD}_{LSAM}$	Fixed data vector transmitted by the LSAM. It comprises the following data elements: PP_{LSAM} , ID_{LSAM} , ALG_{LSAM} , $\overline{IK}_{LSAM}$ and $DEXP_{LSAM}$
$\overline{FD}_{PSAM}$	Fixed data vector transmitted by the PSAM. It comprises the following data elements: ALG_{PSAM} , $\overline{IK}_{PSAM}$ and $DEXP_{PSAM}$
ID_{COMP}	Identifier for the component.
$\overline{IK}_{COMP}$	Fixed data vector comprising key information (algorithm dependent) for the component. This data vector can be empty.
$\overline{IND}$	Fixed data vector of the PSAM containing the following data for individual transactions PP_{PSAM} , ID_{PSAM} , NC , NT_{PSAM} , $NI(NC)$, ID_{IEP} , NT_{IEP} , AM_{IEP} , $CURR(NC)$, $MTOT_{PSAM}$, CC_{PSAM} and transaction type (Purchase or Purchase Cancellation/IEP Balance Recovery).
M_{COMP}	Transaction amount from the component (determined by the PDA or LDA).
$\overline{M}_{COMP}$	Data vector comprising M and CURR.
$MTOT_{COMP}$	Amount of a transaction incremented in the components IEP and PSAM (for Incremental Purchase Transaction).
NC	Number of Collection (identifier for Totals of a given PSAM); reference to this Total in another data element X is made by $X(NC)$.
NF_{PSAM}	Negative File controlled by the PSAM.
NI	Number of Individual transactions related to a Total.
NT_{COMP}	Transaction Number of the component.
NU_{COMP}	Update number computed by the PPSAM and used in off-line PSAM parameter update.

NV	New value for a parameter (used in Update IEP/SAM Parameter).
PAR	Identifier of the parameter to be updated (used in Update IEP/SAM Parameter).
PEXP	Boolean used by the PSAM to control validation of expiry dates. It may be a fixed value stored in the PSAM or it may be computed during each transaction based on transaction parameters available to the PSAM.
PIND	Boolean stored in the PSAM or computed by the PSAM during transaction processing based on transaction parameters and parameters stored in the PSAM. It controls generation of individual transactions.
PP _{COMP}	Purse Provider ID stored in the component.
R	Random number computed by the PPSAM.
S _n	Signature.
STAT _{COMP}	Operational status of a component indicating whether it is open or closed for transactions.
TM	Total amount of a Total.
TOTAL	Data vector associated to a total amount of the PSAM for one Purse Provider and for one currency. It comprises the data elements: PP _{PSAM} , ID _{PSAM} , N, NI(NC), TM(NC), CURR(NC) and CT(NC).
VK _{COMP}	Key version used by the component.

4.4 Security procedures

4.4.1 General notes

The transactions considered in 4.4 have common features. For ease of description and to avoid repetition, these common features are described once in this subclause.

4.4.1.1 Verification of the internal status

For each transaction initiated by the device, the status of the secure component shall be active, except for the transactions update parameter (when for example DACT_{COMP} has to be set) and monitoring, i.e. the activation date shall be set but not the expiry date. The same remark is valid concerning the state open of SAMs.

4.4.1.2 Selection/generation of keys

For each cryptographic process (signing, verifying, enciphering, deciphering) the secure component has to select and/or generate one or more keys. How to perform this in detail depends on the type of algorithm and e.g. on the decision whether to use different keys for every session.

4.4.1.3 Transaction logs

Each secure component, administering one or more transaction logs, prepares a new entry for each transaction.

In the case of a Purchase transaction with several incremental steps, a single entry is prepared. This entry is then updated for each subsequent debit IEP command.

The following logs are used in this part of EN 1546: Purchase Log and Load Log.

4.4.1.4 Completion Codes

A Completion Code is put into each IEP response to any command. It contains information about the result of performing the command which is important for the controlling device in deciding how to proceed with the transaction. It is therefore especially important for error handling. Since the figures only describe error-free transaction execution, the Completion Code is only mentioned if it is used in the transaction for specific security reasons.

4.4.1.5 Challenges for Authentication

Authentication defined in this part of EN 1546 is based on two kinds of challenges to protect against Replay:

- counters for challenges generated by IEPs, PSAMs and LSAMs (chosen for easy generation and auditing);
- random numbers for challenges generated by PPSAMs (chosen for unpredictability).

The kind of PPSAM challenge chosen (either based on counters or random numbers) is not critical, as in both cases Replays are detectable.

Consequently, a particular PPSAM implementation can use challenges based either on counters or random numbers. It is, however, important from the IEP's viewpoint that both appear in the same format. A more detailed description of this is given in EN 1546-3.

4.4.1.6 Digital Signatures

A digital Signature satisfies the following properties:

- only the signer is able to compute a valid Signature on given data; it should be impossible for anybody else to (successfully) forge a Signature;
- the Signature can be verified by anybody. The verification process authenticates not only the given data but the origin of the data as well;
- an impartial third party on the basis of the signed data is able to resolve disputes concerning forgery.

True digital Signatures with these properties are inherent in asymmetric public key algorithms. With symmetric secret key algorithms, most of these properties can be simulated if tamper resistant hardware (SAMs) is available. However, the property of Signature verification by anybody is not implementable.

In this part of EN 1546, digital Signatures are used in the security protocols to authenticate devices and the integrity of data.

4.4.1.7 Discretionary data

Discretionary data added in a transaction can be cryptographically protected if the associated Signature already exists in the commands/responses of the transaction. In this case, either all or part of this discretionary data is appended to the data signed. The length of discretionary data shall be specified in the relevant command/response, see EN 1546-3 for details on this mechanism.

4.4.1.8 Purse Provider specific transactions

Some transactions, such as Collection, update SAM parameter and open/close SAM, could be considered as transactions specific to each Purse Provider, as they would have a less significant impact on interoperability than IEP related transactions. As such, these transactions are detailed in informative Annex A of this part of EN 1546, since it is recognized that Purse Providers might implement their own specific protocols; particularly when interoperability is not influenced. The protocols in the informative annex should as a minimum serve as a guideline for the level of security required in these transactions.

4.4.2 Load (optional)

The Load transaction, conducted by the LDA as an interaction between the IEP and the PPSAM, debits the PPSAM by the agreed amount and credits the IEP by the same amount.

Two solutions are defined for the Load transaction. Seen from the IEP, the initializing and crediting phases are the same for both these solutions:

- one solution, depicted in figure 2 and defined in 4.4.2.1, assumes that the Purse Provider is confident that conventional payment will be, or indeed has been, received and is an on-line end-to-end protocol involving only the IEP and the PPSAM. This solution supports a solution with only two on-line messages;
- the other solution, depicted in figure 3 and defined in 4.4.2.2, assumes that the Purse Provider has to rely on another business entity providing a guarantee that the Purse Provider will receive conventional payment. This protocol assumes an LSAM component is also present.

The communication path from the IEP to the LSAM shall be secured to guarantee that the IEP parameters cannot be modified.

4.4.2.1 Load without an LSAM

This protocol shows the Load IEP transaction without an LSAM. The agreed Load amount is captured by the LDA.

After initialization of the PPSAM and the IEP for the Load transaction the LDA generates a request for IEP Load to the PPSAM (including S_1). The PPSAM verifies (from additional data which could be received from the outside and by means outside the scope of this standard) that the conventional payment corresponding to the Load amount is, or will be, received by the Purse Provider. The Purse Provider shall be sure that the payer has agreed to pay for the loading of a given IEP.

The PPSAM authenticates the IEP and generates an IEP Load Certificate (S_2) and debits its Balance before transmitting S_2 to the IEP. The IEP verifies S_2 (which implies the Authentication of the PPSAM) before crediting its Balance with the Load amount and updating the Load Log. The IEP generates a signed acknowledgement whether loading was successful or not (S_3) which is transmitted to the PPSAM. This signed acknowledgement can be used for audit purposes.

This Load transaction implements Two-way Authentication between the PPSAM and the IEP and is designed to protect against the following threats:

- loading of IEPs other than the identified IEP (S_1);
- loading by false PPSAMs (S_2);
- repudiation of successful loading (S_3);
- Disruption Attacks such as unauthorized debiting of the PPSAM balance (S_1).

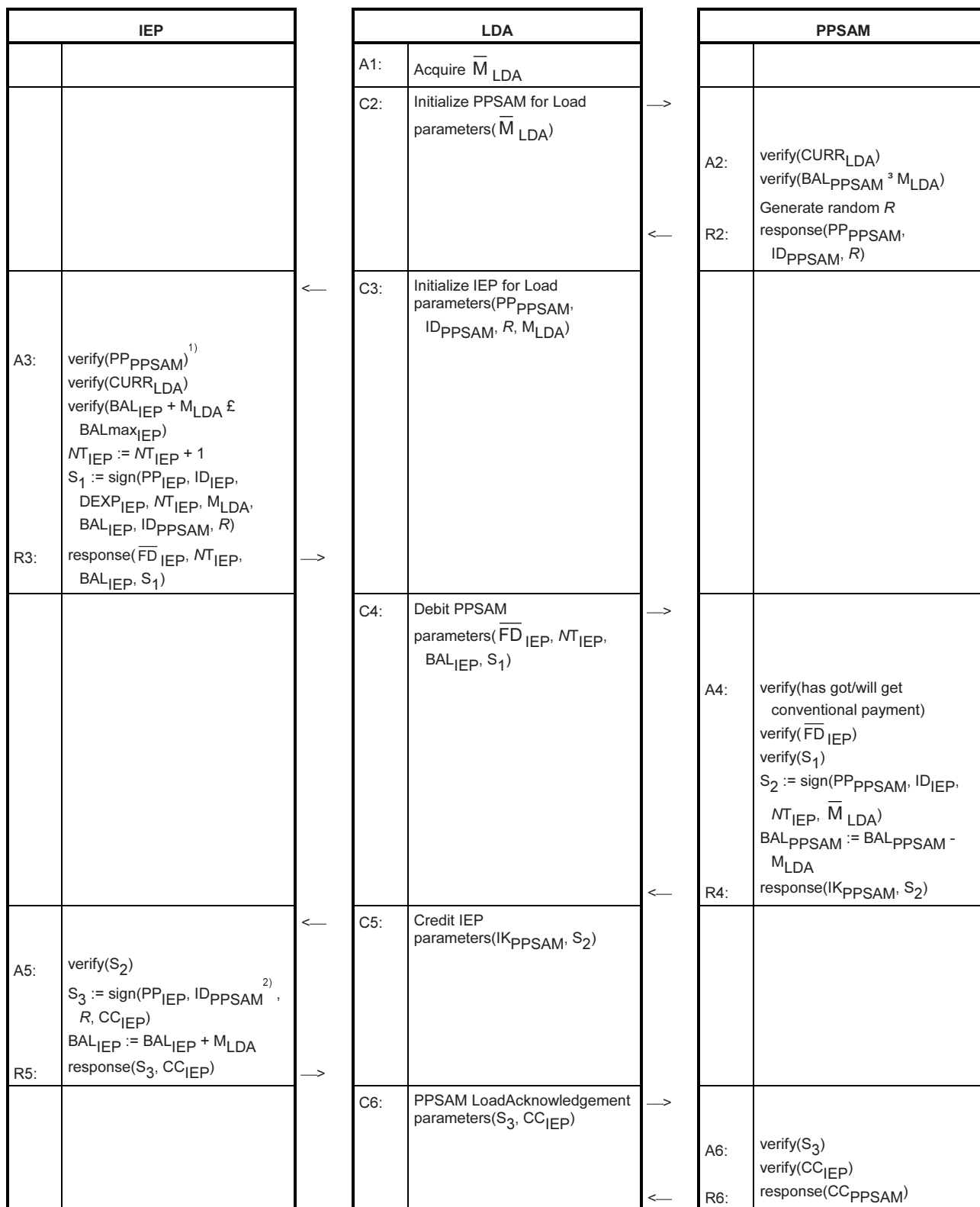


Figure 2 - Load transaction without an LSAM

¹⁾ This verification can be performed without transferring PPPPSAM across any interface to the card. For example, verification can be achieved by the subsequent verification of S_1 .

²⁾ Only added to enable consistent use of S_3 in Currency Exchange and update IEP parameter.
© BSI 01-2000

NOTE This is a conceptual model and should not be interpreted as an implementation example. Valid implementations should fulfil the security requirements defined in this part of EN 1546.

For example, this Load protocol supports Load transactions based on a single exchange, transporting the critical Load certificate S_2 . The initial challenge and the signed acknowledgement may, for example, be transmitted in the previous and next transaction respectively, or generated/verified locally.

4.4.2.2 Load with an LSAM

In the case of a Load transaction incorporating an LSAM, the Load Agent and the Purse Holder agree on the amount to be loaded.

After initialization of the PPSAM, the IEP and the LSAM for the Load transaction by the LDA (including the amount), the LDA initiates a debit PPSAM request which contains Authentication parameters of the IEP and the LSAM. After this debit request, the PPSAM generates an IEP Load certificate (S_3) and enciphers this so that only the LSAM can decipher it for transmission to the IEP. Additionally, the PPSAM transmits in its response, sufficient key information to enable the LSAM to verify S_3 and later on the received signature S_5 of the IEP for confirmation.

The encryption is necessary because the Load Agent should not be able to transmit S_3 to the IEP without giving it to the LSAM, and then repudiate the reception of the PPSAM's response. Upon receipt, the LSAM verifies S_3 before transmitting it to the IEP.

The IEP verifies S_3 before crediting its Balance by the Load amount and updating the Load Log. The IEP generates a signed acknowledgement of successful loading (S_5) which is transmitted to the LSAM. The LSAM, after verification of S_5 , computes an acknowledgement certificate (S_6) which is then sent to the PPSAM. The PPSAM after verifying S_6 computes a signed acknowledgement and certificate (S_7) which is verified by the LSAM and stored as further proof by the LDA.

This Load transaction implements Two-way Authentication between the PPSAM and the IEP and between the LSAM and the PPSAM. It is designed to protect against the following threats:

- only the IEP identified by the LSAM can be loaded (crediting of the same Load transaction amount to more than one IEP) (S_2);
- Masquerading (simulation of one IEP by another) (S_1);
- repudiation of successful Load transactions by the Load Agent, the Purse Provider and Purse Holder (S_3 encryption, S_7 , S_5);
- repudiation of unsuccessful loading by the Purse Provider (S_5);
- Disruption Attacks as systematic attempts to debit a PPSAM (S_1);
- malfunction of the IEP (S_1).

The relationship between the Purse Holder, the Load Agent and the Purse Provider are based on the following assumptions:

- generation of S_2 implies that the Load Agent has been paid by the Purse Holder;
- if the verification of S_1 or S_2 in the PPSAM fails, the Purse Provider shall not claim any money from the Load Agent;

- generation of S_3 and enciphering with the LSAM's key guarantees that neither the Purse Provider nor the Load Agent can repudiate having sent and received S_3 in the context of a successful Load transaction;
- S_6 is a signed acknowledgement by the LSAM of the successful or unsuccessful loading of the IEP.

Four cases are possible:

- if the IEP was correctly loaded and S_6 is received by the PPSAM, the Load Agent shall pay the Purse Provider the corresponding amount;
- if the IEP was not correctly loaded and S_5 is received by the LSAM and S_6 by the Purse Provider the latter does not require payment by the Load Agent and S_3 is invalidated in the LSAM. Instead the Load Agent repays the Purse Holder;
- if the IEP was correctly loaded and S_6 is not received by the PPSAM, the Purse Provider assumes a priori that the transaction was successful and the Load Agent shall pay the Purse Provider, if no other business arrangement is implemented;
- if the IEP was not correctly loaded and S_5 cannot be generated by the IEP, the Purse Holder shall reclaim the payment he made to the Load Agent from the Purse Provider and the Load Agent shall pay the Purse Provider.

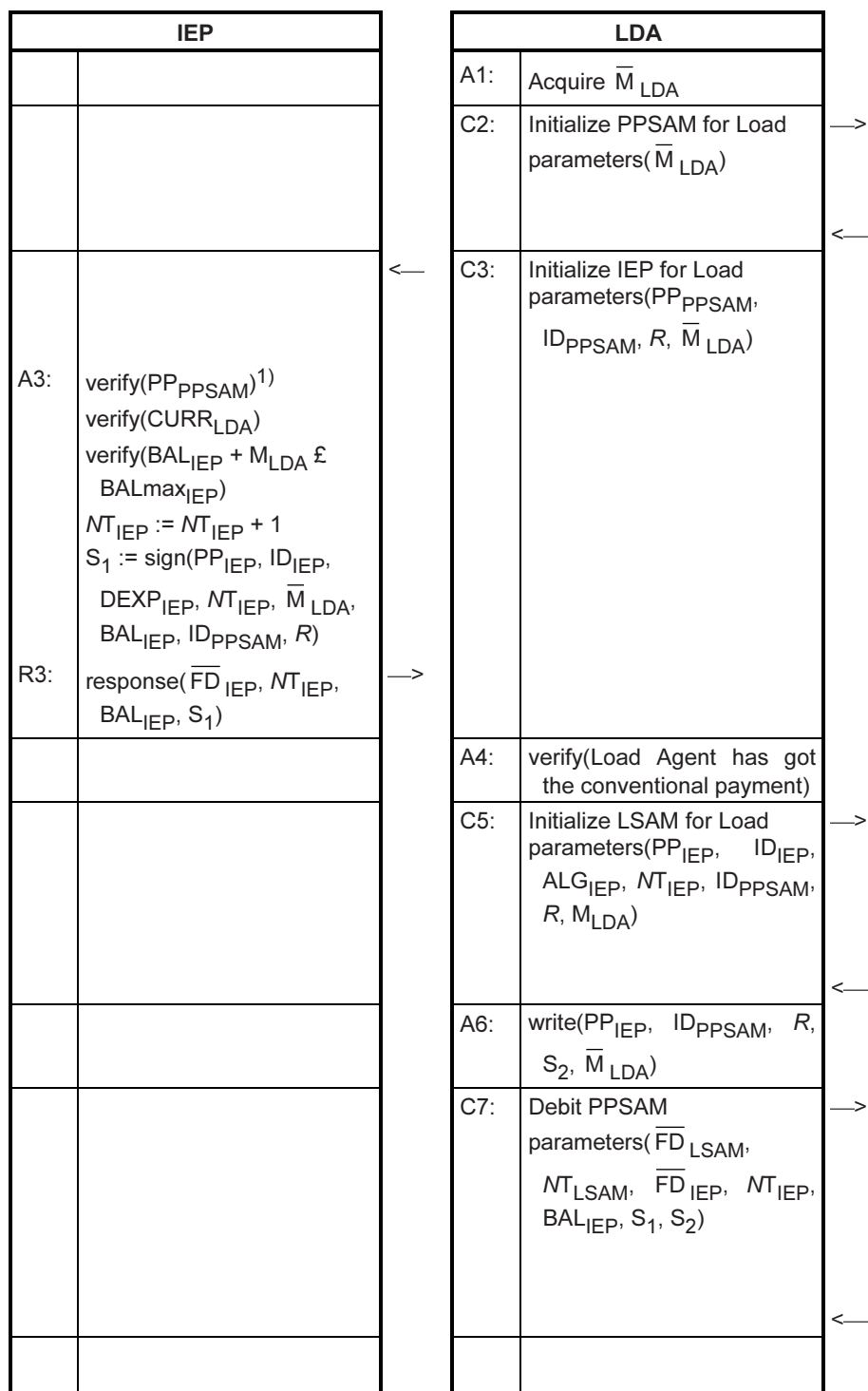


Figure 3 - Load transaction with an LSAM - left half

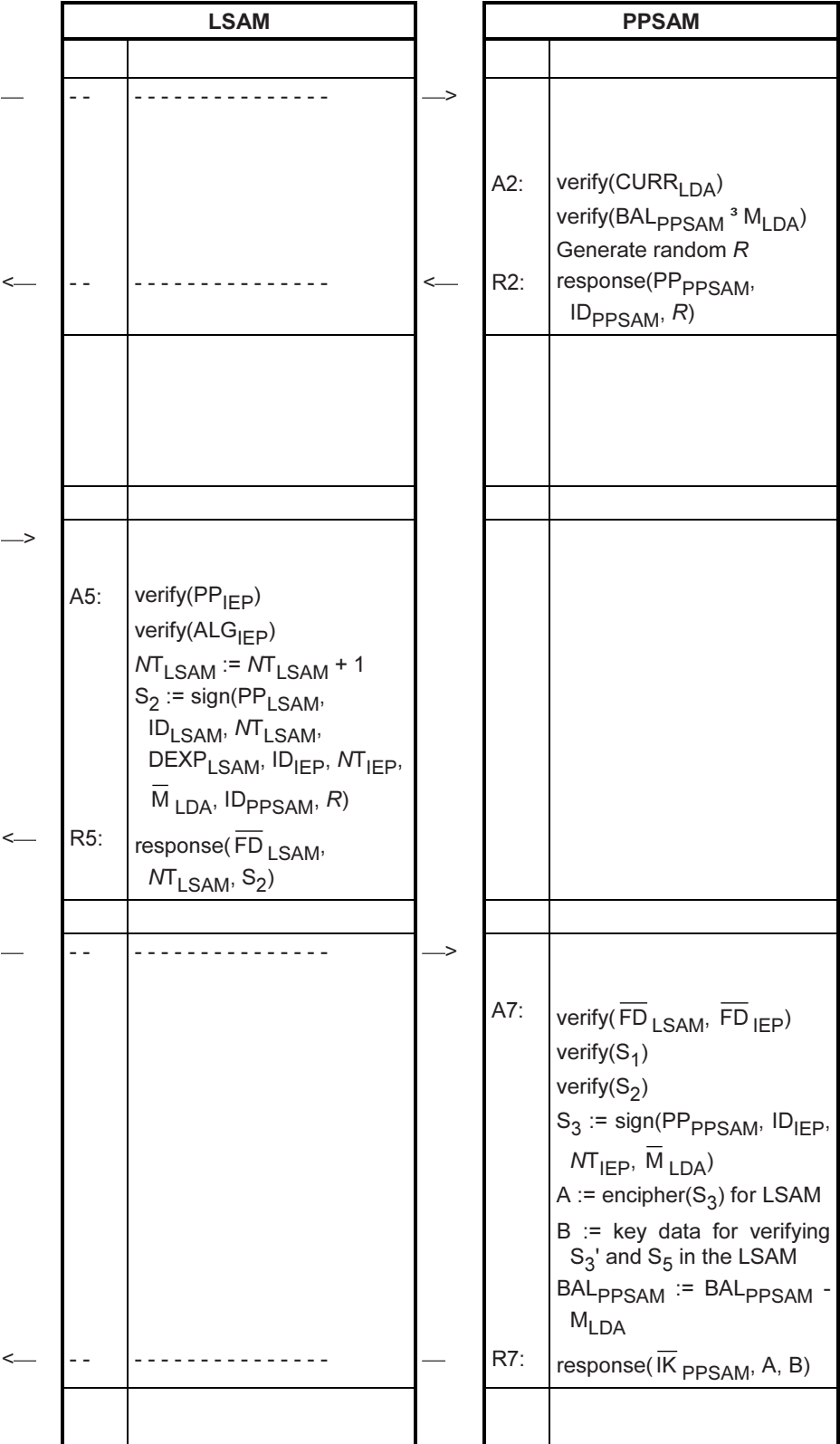


Figure 3 - Load transaction with an LSAM - right half (continued)

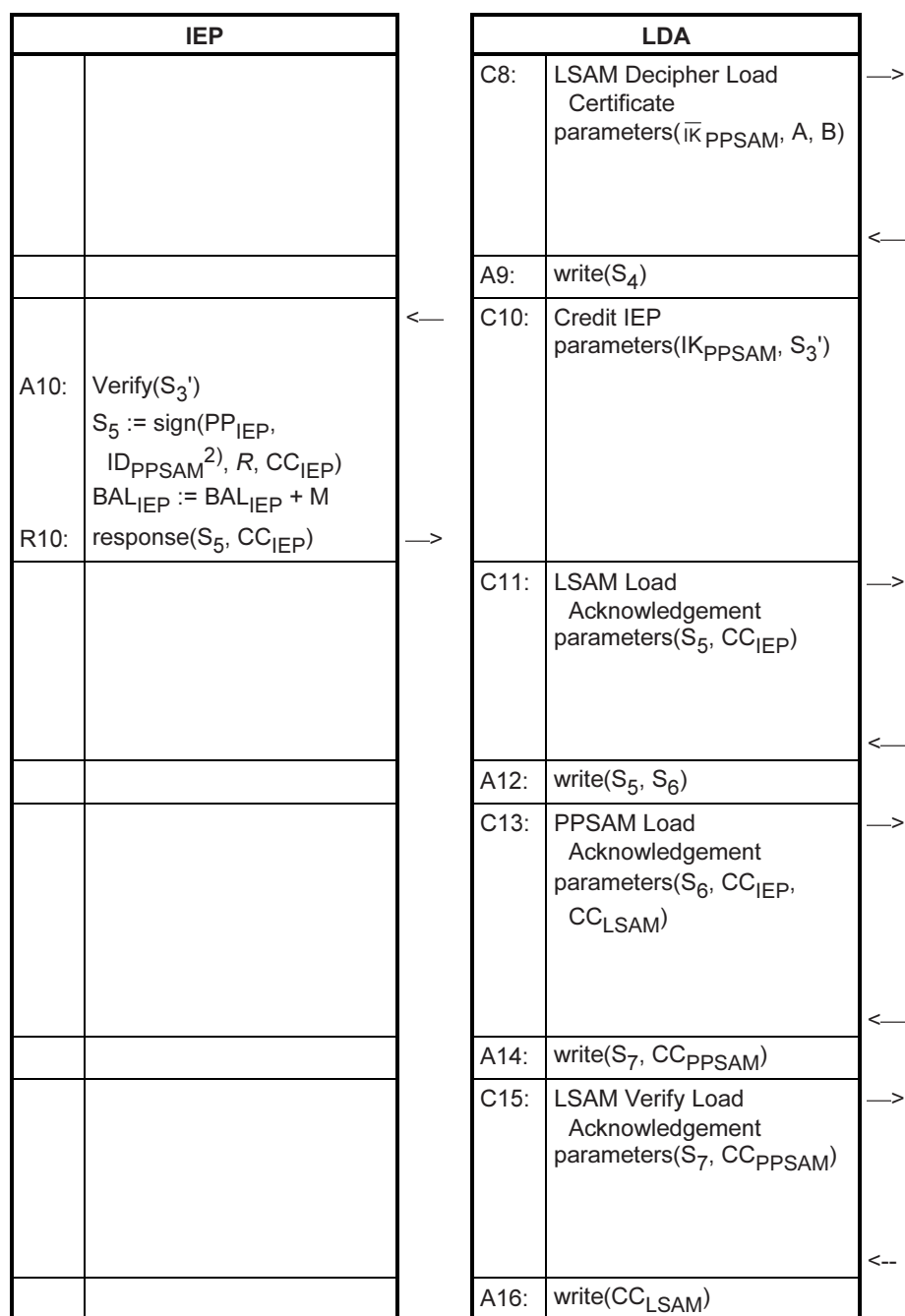
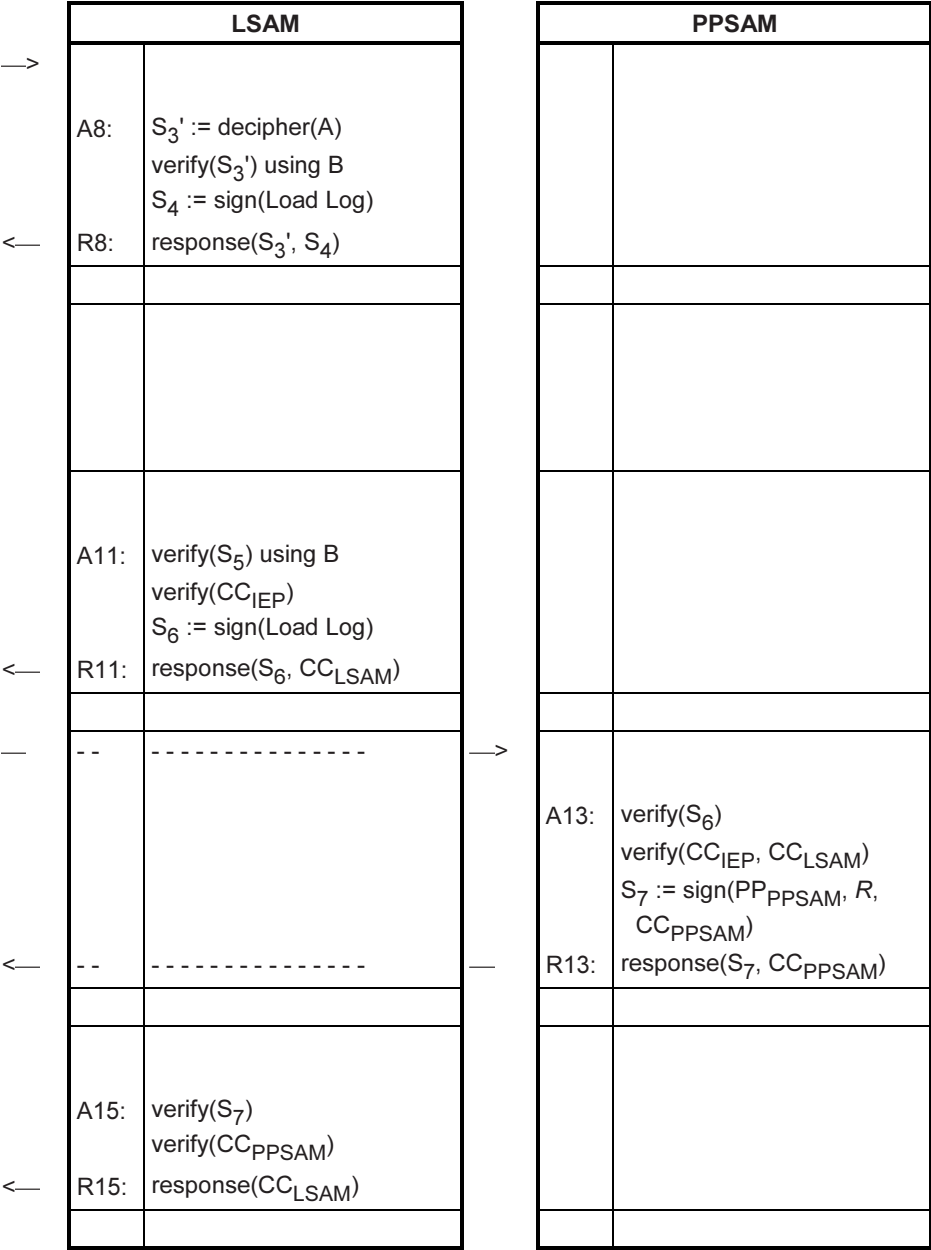


Figure 3 - Load transaction with an LSAM - left half (continued)



NOTE 1 This verification can be performed without transferring PP_{PPSAM} across any interface to the card. For example, verification can be achieved by the subsequent verification of S_1 .

NOTE 2 Only added to enable consistent use of S_5 in Currency Exchange and update IEP parameter.

Figure 3 - Load transaction with an LSAM - right half (concluded)

NOTE This is a conceptual model and should not be interpreted as an implementation example. Valid implementations should fulfil the security requirements defined in this part of EN 1546. For example, this Load protocol supports Load transactions based on a single exchange in the same way as described in the note following figure 2.

4.4.3 Purchase

The Purchase transaction, conducted by the PDA as an interaction between the IEP and the PSAM, debits the IEP Balance by the agreed Purchase amount and credits the PSAM by the same amount. The Purchase transaction protocol is shown in figure 4 (detailed) and in Annex D (overview).

For the Purchase transaction, this standard includes the following options:

- one-way, Two-way or Dual-mode Authentication between the IEP and the PSAM offering protection against different types of threats (defined in 4.4.3.1);
- additional Signature (S_1 in figure 4) offering protection against additional threats (defined in 4.4.3.1);
- signed acknowledgement (steps C6-R6 in figure 4) offering different Error Recovery facilities (defined in 4.4.3.2);
- incremental steps offering a fast repeated debit/credit phase (steps A3-R5 in figure 4) of the Purchase transaction, useful for some services, e.g. telecommunication (defined in 4.4.3.3);
- one-way Authentication with individual transaction Collection not requiring a tamper resistant implementation of the PSAM.

For example, it is possible to implement an IEP System without a physical PSAM, or with a combined PDA-PSAM, or with a PSAM which does not accumulate Totals.

The actual messages exchanged between devices in an implementation are further described in EN 1546-3 which provides normative descriptions of the messages between IEP and PDA only.

Some systems may not implement physically tamper-resistant PSAMs. In this case, the authenticity of the software, keys and, when applicable, Totals etc. will need to be protected procedurally.

The possibility of combinations between these options is described in the following table:

Table 1 - Summary of options for the Purchase transaction

Authentication type	S_1	Signed acknowledgement	Incremental Steps
One-way	No	No	No
One-way	No	No	Yes
Two-way	No	No	No
Two-way	No	No	Yes
Two-way	No	Yes	No
Two-way	No	Yes	Yes
Two-way	Yes	No	No
Two-way	Yes	No	Yes
Two-way	Yes	Yes	No
Two-way	Yes	Yes	Yes
Dual-mode	No	No	Yes
Dual-mode	Yes	No	Yes

4.4.3.1 Security features of the Purchase transaction

The Purchase transaction can be implemented using One-way, Dual-mode or Two-way Authentication. Dual-mode means that the first step has to be performed using Two-way, the following ones using One-way Authentication.

The IEP either supports One-way, Dual-mode or Two-way Authentication. The Authentication mode required by the IEP is defined in the response to the initializing command. The PSAM should be able to handle all modes for interoperability reasons.

In the case of One-way Authentication, the IEP is debited after identification of the PSAM. In the case of Two-way Authentication, the IEP is only debited after it has authenticated the PSAM by optionally signing S_1 and verifying S_2 . Two-way Authentication without S_1 is also possible. In all cases the IEP computes a cryptographic proof (S_3) of its debit which is authenticated by the PSAM, the Purchase amount only being credited to the PSAM after successful Authentication of the proof of debit.

One-way Authentication (using only S_3) of the IEP by the PSAM is designed to protect against the following threats:

- false (simulated) IEPs;
- replays of Purchase transactions to PSAMs;
- masquerading (simulation of one IEP by another);
- crediting of the same Purchase transaction to more than one PSAM.

Two-way Authentication (using S_2 and S_3) is designed to additionally protect against the following threats:

- debiting by false or malfunctioning PSAMs or applications;
- disruption Attacks (systematic attempts to debit IEPs).

Thanks to S_1 it is impossible to obtain a genuine S_2 from a genuine PSAM without having a genuine IEP. Consequently, it is not possible to build a fake PDA which could fraudulently debit any Two-way Authentication IEP of known Identity and NT_{IEP} .

With a PSAM implemented in software not contained in a tamper resistant device, e.g. ICC, it can only securely accumulate a Total Value by keeping details of all transactions. The Purchase transaction with this implementation of the PDA-PSAM component supports only One-way Authentication (S_3).

4.4.3.2 Signed acknowledgement to the IEP

Recovery after error(s) in the Purchase transaction may be based on the logs of the IEP and the PSAM or on a signed acknowledgement to the IEP.

4.4.3.3 Incremental steps

A Purchase transaction can be executed as a single step Purchase amount or in several incremental step amounts. For each incremental step needed, the sequence [A3, C4, A4, R4, C5, A5, R5] is repeated.

Having received R5, the PDA decides on how to proceed. The following three possibilities exist:

- at A3 in the case of an incremental Purchase and there is a further step to perform;
- at C6 if the transaction should be terminated and AM_{IEP} in R1 indicated the need for a signed acknowledgement;

- at C7 if the transaction should be terminated and no such signed acknowledgement is required.
- The incremental step option has the following security characteristics:
 - if One-way or Two-way Authentication is used, then the security is equal to the corresponding Authentication mode for the single step transaction;
 - if Dual-mode Authentication is used, the security is at least equivalent to the single step Purchase transaction using One-way Authentication.

In the case of an Incremental Purchase Transaction, the IEP is debited and the PSAM credited by the incremental amounts defined, using either One-way or Two-way Authentication for each incremental step as specified by AM. However, for some implementations, e.g. in the telecommunication sector, the PSAM may be credited only once (in the last step) with the total amount debited in the IEP during the transaction. In this case, in the Credit PSAM command, only the Signature (S_3) of the last step is transmitted and $\bar{M}$ is replaced by $\overline{MTOT}$ computed by the PDA.

In the case of Two-way Authentication, the PSAM computes S_2 which serves either as an Authentication parameter which the IEP verifies before debiting its balance (for all incremental steps except the last) or as an acknowledgement for the IEP after the last step if this is required. In an incremental transaction without acknowledgement, the last S_2 need not be computed by the PSAM if the PDA knows in A3 that it is in fact the last step, e.g. the Purse Holder has hung up in the case of a telephone call.

In the case of Dual-mode Authentication, the PSAM need only compute S_2 for the first step (when receiving the Initialize PSAM for Purchase command) and for the last incremental step if the PDA can specify the last step to the PSAM.

4.4.3.4 Signing and logging individual transactions

This part of EN 1546 is generally based on the exchange between Purchase Devices and the Purse Provider's Host of Totals (one Total per Purse Provider per currency handled by the Purchase Device).

For auditing and/or statistical purposes Purse Providers may also require detailed information on individual transactions.

The decision on signing and logging individual transactions is taken by the PSAM in step A7 based on transaction data, e.g. IEP identifier and Completion Code, and parameters in the PSAM outside the scope of this standard.

4.4.3.5 Anonymous transaction schemes

In this part of EN 1546, the security protocols and the functionality of the IEP System are based on ensuring that each transaction is unique. This property is maintained by identifying each IEP uniquely and by maintaining an increasing IEP transaction counter. This data shall pass across the interface for each transaction. If the data is in clear, then individual IEP transactions may be optionally audited.

This part of EN 1546 does not preclude the use of anonymous Purchase transaction schemes where the data that ensures transaction uniqueness is passed across the interface in a manner which does not reveal the Identity. However, the process whereby anonymity is ensured is not described.

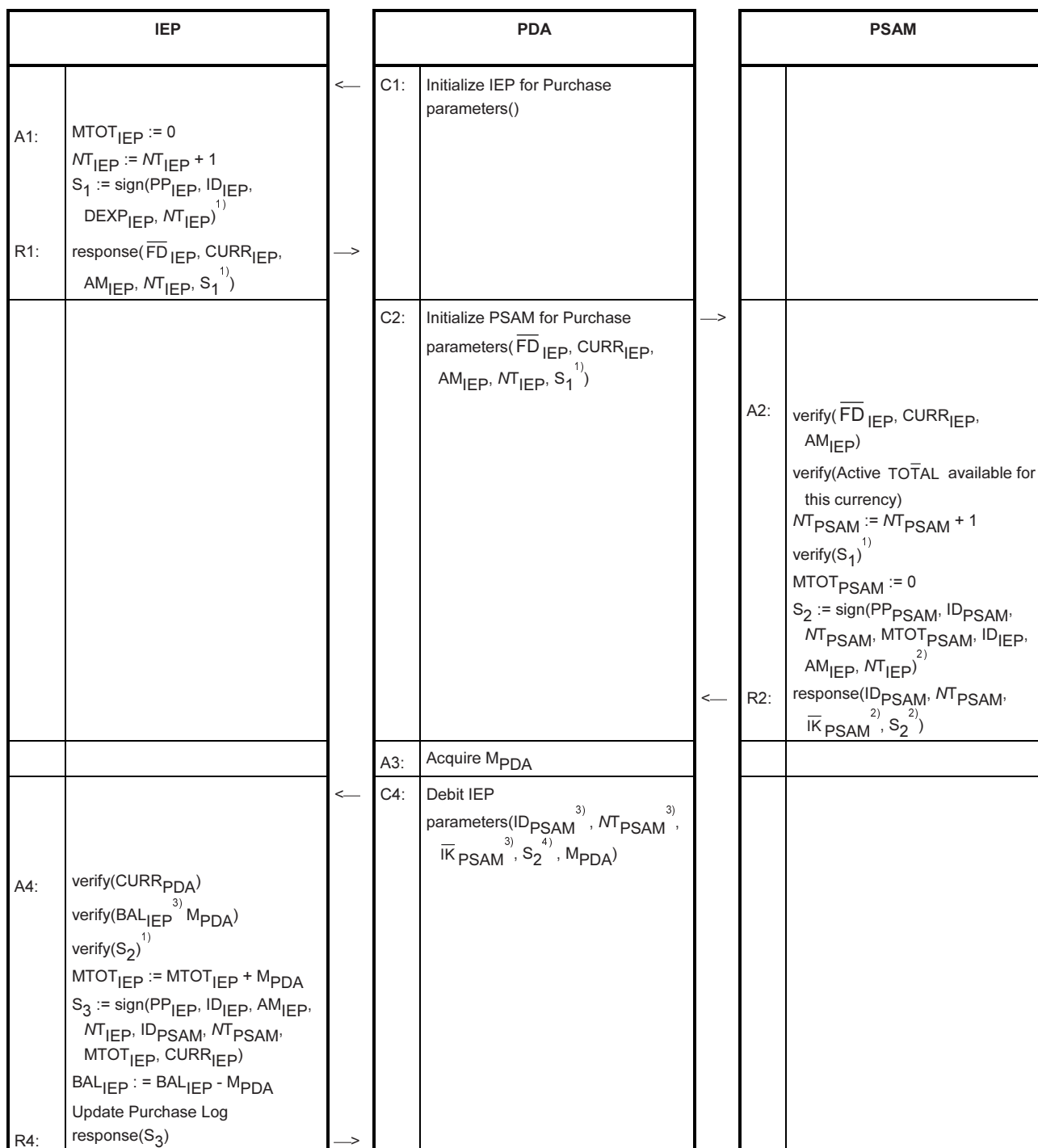


Figure 4 - Purchase transaction

¹⁾ Conditionally performed/sent in case of Two-way or Dual-mode Authentication. This is indicated by the IEP to the PSAM by use of AM_{IEP} .

²⁾ In case of Two-way or Dual-mode Authentication. This is indicated by the IEP to the PSAM by use of AM_{IEP} .

³⁾ Only sent in the first step of Incremental Purchase Transactions.

⁴⁾ Not needed for :

- One-way Authentication ;
- subsequent steps in Incremental Purchase Transactions using Dual-mode Authentication.

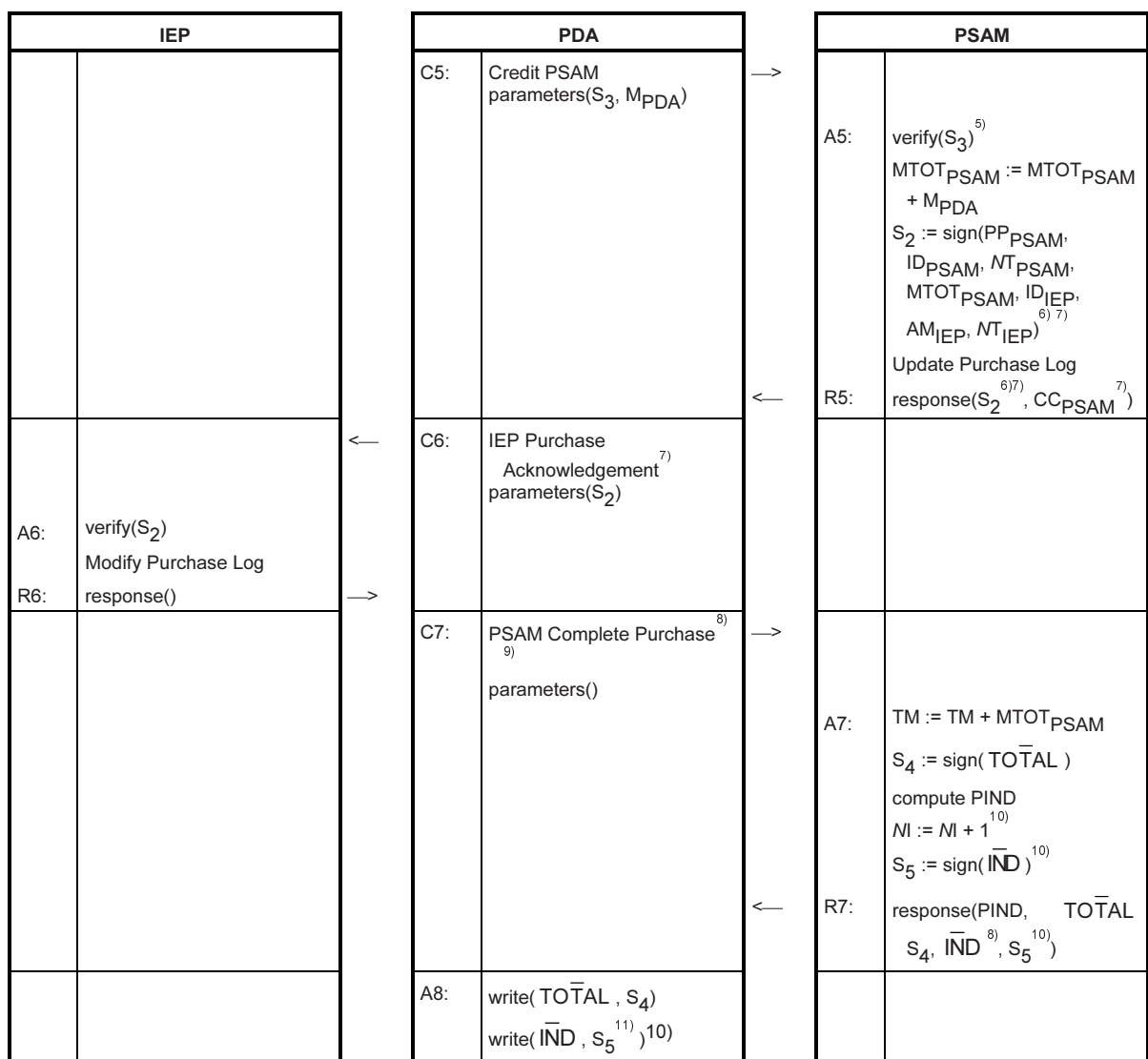


Figure 4 - Purchase transaction (concluded)

⁵⁾ The signature shall be verified using $MTOT' = MTOT_{PSAM} + M_{PDA}$ (as $MTOT_{PSAM}$ shall not be updated before a successful verification of S_3).

⁶⁾ Sent in case of Two-way Authentication.

⁷⁾ The IEP Purchase acknowledgement is only sent if required by the IEP. This is indicated by the IEP to the PSAM by use of AM_{IEP} . The PSAM translates this information to the PDA by use of CC_{PSAM} .

⁸⁾ Maintaining a Total Value and transmitting and signing it can be secured only to the extent that this is permitted by the PSAM implementation.

⁹⁾ Not used for systems without Totals.

¹⁰⁾ Only performed/sent if PIND = TRUE (individual transaction to be generated).

¹¹⁾ For a system without Totals, S_3 is used instead of S_5 .

NOTE 1 - This is a conceptual model and should not be interpreted as an implementation example. Valid implementations should fulfil the security requirements defined in this part of EN 1546.

NOTE 2 - In systems with remote PSAMs, a Purchase transaction is possible using Two-way Authentication and only two exchanges between terminal and remote node.

NOTE 3 - For a system without Totals, in order to prevent duplicated transactions from being accepted, the acquirer has to maintain and test some transaction data, e.g. the unique transaction sequence number (NT_{PSAM}).

4.4.4 Purchase Cancellation/IEP Balance Recovery (optional)

This transaction, conducted by the PDA as an interaction between the IEP and PSAM:

- debits the PSAM Balance and credits the IEP Balance by the amount of the latest (and possibly the only) step of the latest Purchase transaction if this was successful in both devices (Cancellation);
- only credits the IEP Balance if the latest step was successful in the IEP but unsuccessful in the PSAM (IEP Balance Recovery).

The security protocol is shown in figure 5.

After initialization of the transaction, the IEP verifies that the latest Purchase transaction was successful, otherwise it rejects the cancellation/recovery request. It also verifies that the maximum balance that the IEP is allowed to hold is equal to or greater than the sum of the current IEP Balance and the amount to be cancelled. This is to ensure that if a Load was made in the meantime (not a normal event) then the maximum balance would still not be violated by the cancellation. If these verifications are successful, the IEP computes a cancellation/recovery request certificate (S_1) comprising the transaction and Authentication parameters, the transaction parameters taken from the Purchase Log. The IEP transmits S_1 and the corresponding parameters to the PSAM. The PSAM verifies S_1 and validates the following conditions:

- the IEP parameters received correspond to a Purchase transaction still logged in the PSAM;
- that this Purchase transaction has not previously been cancelled;
- whether the Purchase transaction was credited or not to the PSAM.

If the first two conditions are fulfilled, the PSAM accepts the Purchase Cancellation transaction and computes a credit IEP certificate (S_2). If one (or both) of these two conditions is invalid the PSAM rejects the Cancellation transaction.

If the last condition shows that the transaction was credited to the PSAM, the PSAM also debits the total amount in the corresponding Total. The PSAM transmits S_2 and the corresponding parameters to the IEP. After verification of S_2 the IEP recredits its Balance with the amount of the latest Purchase transaction step.

The PSAM Total and, if required, individual transaction parameters for storage at the PDA are updated by the PSAM.

This protocol is designed to protect against:

- successful Replay of Purchase Cancellation/IEP Balance Recovery transactions (S_1);
- malfunction of IEPs at the beginning of the transaction (S_1);
- disruption Attacks where the PSAM Balance is decreased without authorization (S_1);
- unauthorized recrediting of IEPs (S_2).

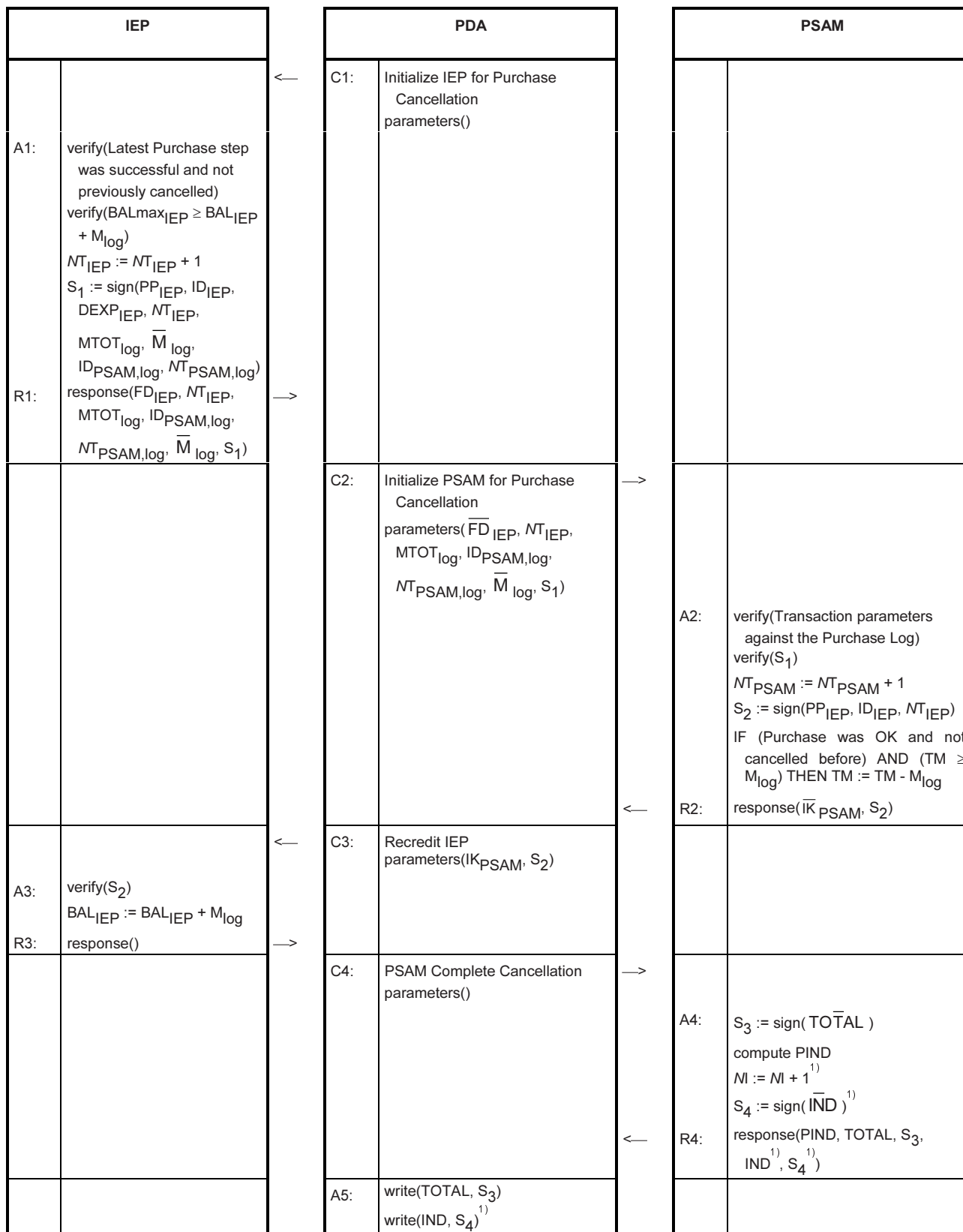


Figure 5 - Purchase Cancellation/IEP Balance Recovery transaction

¹⁾ Only performed/sent if PIND = TRUE (individual transaction to be generated).

NOTE This is a conceptual model and should not be interpreted as an implementation example. Valid implementations shall fulfil the security requirements defined in this part of EN 1546.

Annex A (informative)

Additional security procedures

A.1 IEP transactions

A.1.1 Currency Exchange

The Currency Exchange transaction, conducted by a Load Device or a special device as an interaction between the IEP and the PPSAM, changes the entire IEP Balance from one currency to an equivalent balance in another currency as defined in figure A.1.

This transaction integrates three simpler primitive processes, namely Purchase (where the IEP's balance is reduced to zero in the current currency), IEP parameter updates, e.g. $CURR_{IEP}$ is altered, and a Load in the new currency.

It is assumed that the Purse Holder has already agreed upon the exchange rate before starting the transaction or at the latest before the exchange IEP currency command is sent to the IEP.

This transaction uses One-way Authentication of the PPSAM and signed acknowledgement by the IEP. Additionally, the IEP begins by signing (among other data) its Balance and transaction number (S_1). The IEP parameters and S_1 are then sent to the PPSAM for verification. If this verification is successful, the PPSAM computes a certificate (S_2) which enables the IEP to change its Balance into the new currency.

After the exchange has been performed, a signed acknowledgement is sent to the PPSAM - even in the case when the exchange was unsuccessful. This acknowledgement assures a posteriori Authentication of the IEP by the PPSAM and can be used for auditing purposes.

The protocol is designed to protect against the following threats:

- Currency Exchange by false PPSAMs (S_2);
- Currency Exchange in other IEPs (S_1 and S_2);
- Replay of old Currency Exchange certificates to the IEP (S_1 and S_2);
- uncertainty in the PPSAM whether the exchange was successful or not (S_3).

NOTE Multiple currency operations may be performed either by using as many IEP applications as currencies or by combining the currencies within the IEP application.

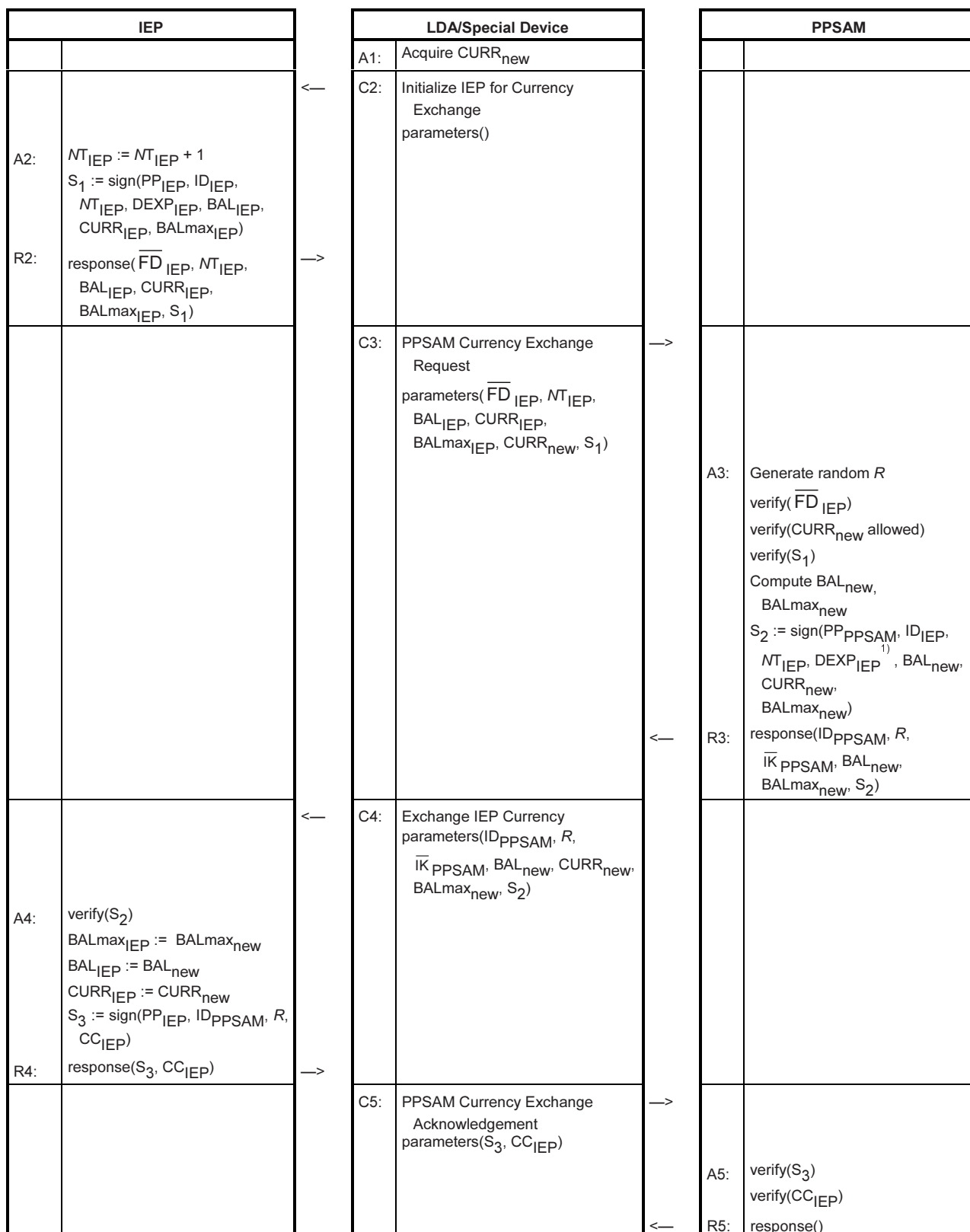


Figure A.1 - Currency Exchange transaction

¹⁾ Only added to define S₂ identical to S₁.