# SLOVENSKI STANDARD
# SIST EN 1546-2:2004

**01-maj-2004**

---

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

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

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



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



**Ta slovenski standard je istoveten z:** **EN 1546-2:1999**

---

**ICS:**

| | | |
|---|---|---|
| 35.240.15 | Identifikacijske kartice in sorodne naprave | Identification cards and related devices |

**SIST EN 1546-2:2004** **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

**EN 1546-2**

July 1999

ICS 35.240.15

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

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 practiced 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 European Standard 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 European Standard 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.



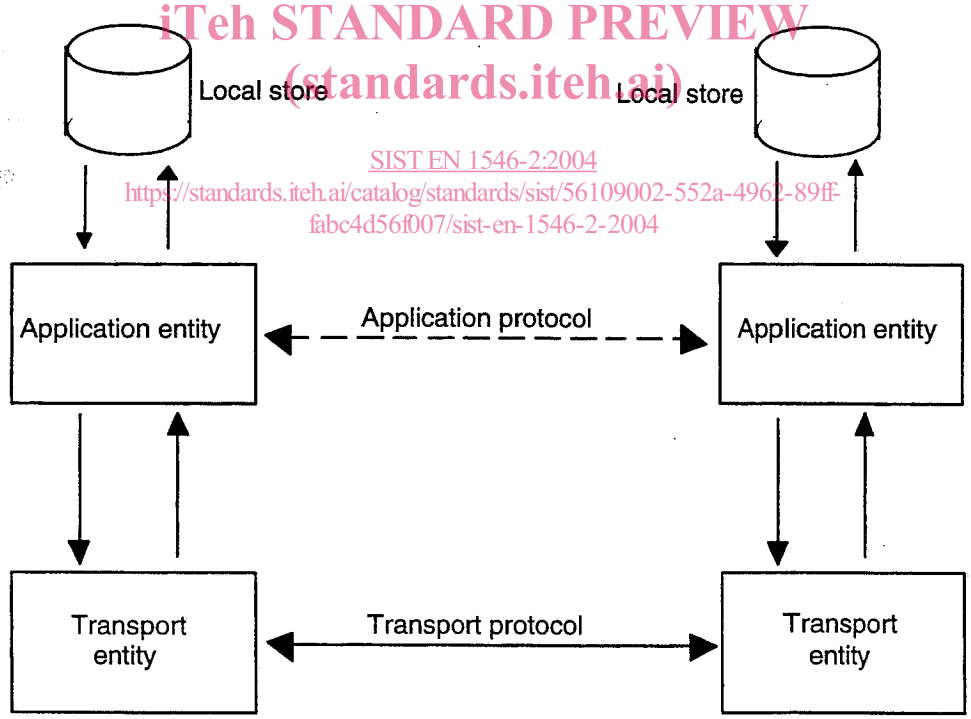


**Figure 1 - Protocol layers in the IEP System**

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. |
| $BALmax_{COMP}$ | 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 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. |
| $\overline{TOTAL}$ | Data vector associated to a total amount of the PSAM for one Purse Provider and for one currency. It comprises the data elements: $PP_{PSAM}$, $ID_{PSAM}$, NC, 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.