SLOVENSKI STANDARD
SIST EN 1546-1:2004

01-maj-2004

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

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

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

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

Ta slovenski standard je istoveten z: **EN 1546-1:1999**

ICS:

01.040.35	Informacijska tehnologija. Pisarniški stroji (Slovarji)	Information technology. Office machines (Vocabularies)
35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices

SIST EN 1546-1:2004 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 1546-1

August 1999

ICS 01.040.35; 35.240.15

English version

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

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

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

This European Standard was approved by CEN on 29 July 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 February 2000, and conflicting national standards shall be withdrawn at the latest by February 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.

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*

Introduction

EN 1546 defines interfaces and functionality for IEP (Inter-sector Electronic Purse) Systems to a level of detail necessary to make it possible for Purse Holders to use their IEPs in other IEP Systems, e.g. in other countries.

Similarly, EN 1546 supports the use of IEPs from several Purse Providers in the same equipment if so allowed by business agreements.

It is outside the scope of EN 1546 to define administrative procedures and organisational structures, although, in order to improve overall understanding, the business relationships are described for a general IEP System.

Wherever possible, EN 1546 references other existing ISO and CEN standards.

Not described are "indirect" participants like authorities enacting general and/or special legislation concerning IEP Systems, legal courts, and possibly clearing systems.

1 Scope

This part of EN 1546 gives an overview of an IEP System by describing the participants, physical devices and functions needed.

The models presented here are the most general ones, and simpler systems ("closed systems") can be designed by selecting subsets of the functionality described. However, this could also lead to limitations in interoperability.

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.

EN 30202-1, *Financial transaction cards - Security architectures of financial transaction systems using integrated circuit cards - Part 1 : Card life cycle (ISO 10202-1:1991).*

3 Terms and definitions

For the purposes of this standard, the following definitions apply :

3.1
acquirer
an organisation which collects and possibly aggregates transactions from several Purchase Devices and/or other Acquirer Hosts for delivery to one or more Purse Providers

3.2
acquirer host
the equipment used by the Acquirer in order to perform the IEP related tasks for the Acquirer

3.3
activation
a secure procedure under control of the Purse Provider, switching an IEP or a SAM to its active life state for normal operation

3.4
aggregation
for each Purse Provider and each currency, the process of adding several Totals into one overall Total. The result is a new Total with the Value equivalent to the sum of all the original Totals

3.5
authentication
a cryptographic process in which one entity proves its identity and the integrity of the data it may send to another entity

3.6
card issuer
the organisation responsible for the provision and distribution of ICCs for use in an IEP System

NOTE This definition of an IEP card issuer shall not be confused with the general use of that term in other card-based payment systems.

3.7
collection
the process of transferring data on transactions from PSAMs and/or Purchase Devices to Purse Provider Host(s) and PPSAM(s) directly or via Acquirers

3.8
currency exchange
an on-line transaction to the Purse Provider Host during which, the entire IEP Balance is exchanged from one currency to another

3.9
currency exchange log
a file in an IEP's non-volatile memory used to record information on at least the latest Currency Exchange transaction

3.10
deactivation
a secure procedure under control of the Purse Provider, switching an IEP or a SAM from its active life state to a permanently disabled state. Only reading of non-secret data is possible in the deactivated state

3.11
electronic value ; value
the (electronic) Value stored and exchanged in an IEP System. The Electronic Value represents real money in the specified currency

3.12
error recovery
procedures used for correcting certain errors observed during processing of normal transactions, e.g. Purchase transactions

3.13
IC card (ICC)
an Integrated Circuit Card with at least one IEP installed

3.14
IC embedder
the organisation integrating IC assemblies and plastic cards into ICCs. It could also personalise the IEP

3.15
IC manufacturer
the organisation manufacturing the ICs for ICCs

3.16
identity
a string of bits chosen to have a unique value and used for example to distinguish between instances of IEPs, SAMs and transactions

3.17
IEP balance
the current amount of Value in an IEP (in a specific currency). It is increased by Load (and Purchase Cancellation) transactions and decreased by Purchase transactions

3.18
inter-sector electronic purse (IEP)
an application in an ICC able to store and process Electronic Value according to EN 1546

3.19
IEP monitor
a device, possibly hand-held, by which public information in the IEP, such as the IEP Balance and log information, can be read out

3.20
IEP system
the term refers to all described participants, devices, and functions covered by EN 1546

3.21
installation
the process where an IEP or SAM application and its associated parameters are loaded into an ICC

3.22
key management
the techniques used in the IEP System for the generation, distribution, storage, updating and destruction of cryptographic keys and related keying material. The recommendations made in this standard provide for both manual and automated techniques to securely exchange keys and keying material between the various IEP System components, either directly or indirectly using common Key Management centres to whom responsibility has been delegated by the Purse Provider(s)

3.23
key management system
the actual implementation of Key Management in an IEP System

3.24
load
the transaction performed using a Load Device whereby Value from the PPSAM is transferred to an IEP. In return either the Load Agent or the Purse Provider receives payment from the Purse Holder. The term Load includes subsequent Loads of an IEP (reloads)

3.25
load agent
the organisation providing Load Devices to be used by Purse Holders. Additionally, the Load Agent may receive payment from Purse Holders in exchange for Load transactions

3.26
load device
a physical device operated by a Load Agent and used jointly by a Purse Holder and the Load Agent to transfer Value from the PPSAM to the (Purse Holder's) IEP

3.27
load log
a file in an IEP's non-volatile memory used to record information on at least the latest Load transaction

3.28
load SAM (LSAM)
a logical module that provides security in Load Device(s) operated by a Load Agent receiving payment directly

3.29
negative file
a file that contains zero or more ranges of identifiers for IEPs that are not allowed to perform transactions in the IEP System. If present, the file should be available for SAMs at transaction time

3.30
personal identification number (PIN)
data which may be required by the application to be presented to the card by its user before data can be processed

3.31
purchase
the transaction performed using a Purchase Device whereby Value is transferred from an IEP to a PSAM. In return the Purse Holder receives a Service from the Service Provider

3.32
purchase cancellation
a transaction made at a Purchase Device in order to cancel the latest Purchase transaction for the involved IEP and PSAM

3.33
purchase device
a physical device operated by a Service Provider and used jointly by a Purse Holder and the Service Provider to transfer Value from the Purse Holder's IEP to the PSAM associated with the Purchase Device

3.34
purchase log
a file in an IEP's non-volatile memory used to record information on at least the latest Purchase transaction

3.35
purchase SAM (PSAM)
a SAM issued under the responsibility of the Purse Provider, installed in connection with Purchase Device(s) and providing the necessary security for Purchase-related transactions and the Collection process

3.36
purse holder
a person in possession of an (ICC with an) IEP. Not necessarily the same person for the whole lifetime of the IEP

3.37
purse provider
the organisation responsible for the overall functionality and security of an IEP System. Also the organisation which is entitled to receive funds in exchange for Load transactions and credits the Service Providers according to the transactions made in their Purchase Devices

3.38
purse provider host
a data processing system possessing the necessary functionality to perform the Purse Provider's IEP functions in a secure way by using the PPSAM

3.39
purse provider SAM (PPSAM)
the SAM of the Purse Provider providing the necessary functionality for the secure functioning of the IEP System as seen from the Purse Provider's viewpoint, i.e. secure Activation, Load, Collection and auditing functions

3.40
secure application module (SAM)
a logical device used to provide security for insecure environments. It is protected against tampering, and stores secret and/or critical information. Several types of SAMs are defined for the IEP System

3.41
SAM issuer
the certified organisation responsible for issuing SAMs, e.g. Purchase SAMs, for use in an IEP System

3.42
SAM monitor
a device by which public information in the SAM, such as Totals, can be read out

3.43
security architecture
the utilisation of detailed security mechanisms, including cryptographic algorithms and the Key Management appropriate to comply with the security requirements of the IEP System

3.44
service
any kind of service and/or goods delivered by a Service Provider to a Purse Holder and paid for in a Purchase transaction

3.45
service provider
the organisation delivering Service(s) to a Purse Holder to be paid for using an IEP. The Service Provider operates one or more Purchase Devices

3.46
settlement
a process performed by the Purse Provider or Acquirer on behalf of the Purse Provider. Based on data from Purchase and Load transactions, payment is effected from the Purse Provider to the Service Providers and in some cases from the Load Agents to the Purse Provider

3.47
total
a summary of individual Purchase transactions. It contains (at least) the total number of transactions and the total amount of these transactions. A Total can only contain information for one Purse Provider and for transactions made in one currency

3.48
value
see Electronic Value

3.49
verification
a process where it is determined whether the presenter of an ICC or SAM is an authorised user, e.g. by use of a PIN or by biometric measures

In order to emphasise terms specific to a general IEP System, throughout this European Standard, these terms commence with capital letters, e.g. Service Provider.

4 Abbreviations

IC	Integrated Circuit
ICC	IC Card
IEP	Inter-sector Electronic Purse
LSAM	Load SAM
PIN	Personal Identification Number
PSAM	Purchase SAM
PPSAM	Purse Provider SAM
SAM	Secure Application Module

5 Overview of an IEP System

5.1 Main system characteristics

The IEP System has the following main characteristics :

— it is based on a Security Architecture which protects against misuse ;

— an IEP is installed in a microprocessor based ICC (Integrated Circuit Card), with or without contacts ;

— an IEP is prepaid. The electronic Value contained in the IEP is the counterpart of a bank deposit ;

— it is possible to use the IEP in many different types of Purchase Devices in different sectors. This includes various types of self-service equipment. Expected applications include pay-phones, parking meters, public transport, toll roads, automatic vending machines, canteens, shops etc.;

— as a consequence of these types of applications, the Value stored in the IEP is expected to be limited by the Purse Holder, the Purse Provider, and perhaps by legislation ;

— use of an IEP is anonymous in the sense that no direct link is necessary between the IEP and a bank account or other person-related information, although such links are not excluded ;

— Purchase Devices normally operate off-line from central computer systems when handling Purchase transactions ;

— Load Devices operate directly connected to the Purse Provider Host (on-line) when handling Load transactions ;

— in some systems, more functions may be combined in one physical unit, e.g. an IEP can function as a PSAM and/or PPSAM.

5.2 Basic assumptions

This standard, defining IEP Systems at the application level, is based on the following basic assumptions which are the foundation for all descriptions and requirements :

5.2.1 Physical security

The functionality of the IEPs and SAMs essential to the security of IEP Systems is implemented in tamper resistant environments. This means that sensitive data, cryptographic keys, executable code etc. can be securely stored and only accessed via the IEP and SAM applications themselves under the defined access conditions.

Reverse engineering of IEPs and SAMs, in order to duplicate or simulate these devices, is not economically feasible.

5.2.2 Available technology

The necessary technology will be commercially available to support, in particular :

— symmetric and asymmetric cryptographic algorithms implementable in ICCs with sufficient performance ;

— general functions common to all applications implemented in ICCs as defined by ISO and CEN where applicable.

5.2.3 Cryptography

The symmetric and asymmetric cryptographic algorithms likely to be used in IEP Systems offer sufficient protection against practical cryptanalysis over the planned life time of the IEP Systems.

5.2.4 Manufacturing and personalisation

The life cycles of IEPs and SAMs during the manufacturing and personalisation phases (see A.4.7 (IEP Life Cycle)) are secure. This means that the IC Manufacturers, IC Embedders, Card Issuers and SAM Issuers will fulfil the security requirements of the Purse Provider.

5.2.5 Legal regulations

Restrictions due to legislation such as export rules, patents or others are not major barriers to the implementation of IEP Systems.

Initiators of a prepaid cards project involving more than one good or Service Provider should inform their central bank at the earliest possible stage (as concluded in the report to the council of the European Monetary Institute on prepaid cards, May 1994).