SLOVENSKI STANDARD
SIST EN 726-3:2004

01-maj-2004

Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 3: Application independent card requirements

Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 3: Application independent card requirements

Identifikationskartensysteme - Anforderungen an Chipkarten und Endgeräte für Telekommunikationszwecke - Teil 3: Applikationsunabhängige Anforderungen an die Karte

Systemes de cartes d'identification - Cartes a circuit intégré et terminaux pour les télécommunications - Partie 3: Spécifications de la carte indépendantes des applications

Ta slovenski standard je istoveten z: **EN 726-3:1994**

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices

SIST EN 726-3:2004 **en**

EUROPEAN STANDARD **EN 726-3**

NORME EUROPÉENNE

EUROPÄISCHE NORM December 1994

ICS 33.120.00; 35.240.60

Descriptors: Telecommunications, IC cards, telecommunication terminals, specifications, characteristics

English version

Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 3: Application independent card requirements

Systèmes de cartes d'identification - Cartes à circuit intégré et terminaux pour les télécommunications - Partie 3: Spécifications de la carte indépendantes des applications

Identifikationskartensysteme - Anforderungen an Chipkarten und Endgeräte für Telekommunikationszwecke - Teil 3: Applikationsunabhängige Anforderungen an die Karte

This European Standard was approved by CEN on 1994-12-05. 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.

The European Standards exist 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, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

CEN

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 was prepared by ETSI STC TE9 and adopted by CEN/TC 224 "Machine-readable cards, related device interfaces and operations", the secretariat of which is held by AFNOR.

This document was submitted to the formal vote and the result of the formal vote was positive.

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 June 1995, and conflicting national standards shall be withdrawn at the latest by June 1995.

According to the CEN/CENELEC Internal Regulations, the following countries are bound to implement this European Standard :

Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

This European Standard consists of the following parts, under the general title "Identification card systems - Telecommunications integrated circuit(s) cards and terminals" :

- Part 1 : System overview ;
- Part 2 : Security framework ;
- Part 3 : Application independent card requirements ;
- Part 4 : Application independent card related terminal requirements ;
- Part 5 : Payment methods ;
- Part 6 : Telecommunication features ;
- Part 7 : Security module.

1 Scope

This part of EN 726 specifies the application-independent characteristics of multi-application IC-cards and plug-in modules for telecommunication applications in order to ensure interoperability for telecommunication cards with the various systems and terminals. Mono-application cards are considered to be a subset of multi-application cards. All common characteristics, necessary for the interactions between the card and the external world are defined.

This part of EN 726 does not preclude cards from other sectors from containing telecommunication application(s) based on this part of EN 726.

The application-specific characteristics are not defined in this part of EN 726. They are defined and described in the relevant application requirements.

This part of EN 726 does not specify any internal technical implementation. It describes:

- the requirements for the physical characteristics of the card, the electronic signals and the transmission protocols ;

- the application-independent logical model which should be used as a basis for the design of the logical structure of, optionally, several applications in the card ;

- the security facilities concerning the access to the different parts within the card and the possible interactions between these parts. Also the description of security functions which should be needed generally by the various applications. They shouldbe available as a common set ;

- the description of the application-independent functions between card and external world, should be used as a standardized common set for all basic functions used in international applications;

- the mapping of these application messages (commands and responses) under standardized protocols ;

- the contents of the master File ;

- the interoperability of IC cards ;

- the overall security aspects for card-manufacturers, application providers and card-issuers.

2 Normative references

This part of EN 726 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 listed hereafter. For dated references, subsequent amendments to, or revisions of any of these publications apply to this part of EN 726 only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

EN 726-1	Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 1 : System overview.
EN 726-2	Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 2 : Security framework[1)] .
EN 726-4	Identification card systems - Telecommunications intergrated circuits cards and terminals - Part 4 : Application independent card related terminal requirements.

[1)] At present at the stage of draft

ENV 1375-1	Identification card systems - Intersector integrated circuit(s) card additional formats - Part 1 : ID-000 card size and physical characteristics. [1)]
ENV 1375-2	Identification card systems - Intersector integrated circuit(s) card additional formats - Part 2 : ID-00 card size and physical characteristics. [1)]
EN 27810:1989	Identification cards - Physical characteristics.
EN 27811-1:1989	Identification cards - Recording technique - Part 1 : Embossing.
EN 27811-2:1989	Identification cards - Recording technique - Part 2 : Magnetic stripe.
EN 27812:1989	Identification cards - Numbering system and registration procedure for issuer identifiers.
EN 27816-1:1989	Identification cards - Integrated circuit(s) with cards contacts - Part 1 : Physical characteristics.
EN 27816-2:1989	Identification cards - Integrated circuit(s) cards with contacts - Part 2 : Dimentions and location of the contacts.
EN 27816-3:1992	Identification cards - Integrated circuit(s) cards with contacts - Part 3 : Electronic signals and transmission protocols.
EN 27816-3:1992/A1:1993	Identification cards - Integrated circuit(s) cards with contacts - Part 3 : Electronic signals and transmission protocols - Amendement 1 : Protocol type T=1, asynchronous half duplex block transmission protocol.
I-ETS 300045-1:1992	European digital cellular telecommunications system (phase 1) : Subscriber identity module - Module equipment (SIM - ME) interface specification (GSM 11.11).
ISO 639:1988	Code for the representation of names of languages.
ISO/IEC 646:1991	Information technology - ISO 7-bit coded character set for information interchange.
ISO 3166:1988	Codes for the representation of names of countries.
ISO/IEC 7816-4	Identification cards - Integrated circuit(s) cards with contacts - Part 4 : Interindustry commands for interchange [1)]
ISO/IEC 7816-5	Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers. [1)]
ISO 8859-1:1987	Information processing - 8-bit single-byte coded graphic character sets-Part 1 : Latin alphabet N°1.
ISO 9564-1:1991	Banking - Personal identification number management and security - Part 1 : PIN protection principes and techniques.
ISO 9564-2:1991	Banking - Personal identification number management and security - Part 2 : Approved algorithm(s) for PIN encipherment.

[1)] At present at the stage of draft

ISO 9807:1991	Banking and related financial services - Requirements for message authentication (retail).
ISO 9992-1:1991	Financial transaction cards - Messages between the integrated circuit card and the card accepting device - Part 1 : Concepts and structures.
ISO 9992-2	Financial transaction cards - Messages between the integrated circuit card and the card accepting device - Part 2 : Functions, messages (commands and responses), data elements and structures.[1)]
ISO 10202-0	Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Part 0 : System overview.[1)]
ISO 10202-1:1991	Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Part 1 : Card life cycle.
ISO 10202-2	Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Part 2 : Transaction process [1)].
ISO 10202-3	Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Part 3 : Cryptographic key relationships. [1)]
ISO 10202-4	Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Part 4 : Secure application modules. [1)]
ISO 10202-5	Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Part 5 : Use of algorinthms. [1)]
ISO 10202-6	Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Part 6 : Card holder verification. [1)]
CCITT Recommendation E.118:1988	Automated international telephone credit card system.
CCITT Recommendation T.50:1988	International alphabet n°5.

[1)] At present at the stage of draft

3 Definitions, abbreviations and symbols

3.1 Definitions

For the purposes of this part of EN 726, the following definitions apply.

3.1.1 access conditions (AC): A set of security attributes associated to a file.

3.1.2 allocable memory: Portion of memory contained in a file but not presently allocated.

3.1.3 application: An application consists of a set of security mechanisms, files, data, protocols (excluding transmission protocols) which are located and used in the IC card and outside the IC card (external application).

3.1.4 application session: A link between the card application part and the external world application part of the same application.

3.1.5 application specific command set (ASC): To a dedicated file (DF) can be associated an optional an application specific command set and/or an application specific program (ASC-set). This means that when selecting this application, the general command set is extended or modified by this specific command set. The ASC is valid for the whole subtree of this application unless there are other ASCs defined at the lower levels of this application.

3.1.6 application provider (AP): The entity which is responsible for the application after its allocation. One AP may have several applications in one card. The files allocated in the card corresponding to one application are called a card-application. There may exist several applications on a given card from the same application provider.

3.1.7 card: A multi-application card can be considered as a set of files, some of them shared by the different application providers and/or the card issuer, other files owned exclusively by the different application providers or the card issuer. Files can, e.g, be read, written or executed.

3.1.8 card session: A link between the card and the external world starting with the answer to reset (ATR) and ending with a subsequent reset or a de-activation of the card.

3.1.9 current directory: The latest directory (MF or DF) selected in the card.

3.1.10 current EF: The latest EF selected in the card.

3.1.11 current file: The latest file (MF, DF or EF) selected in the card.

3.1.12 dedicated file (DF): A file containing AC and allocable memory. It may be the parent of elementary files and/or dedicated files.

3.1.13 directory: General name for MF or DF.

3.1.14 elementary file (EF): A file containing AC, data or program. It can not be the parent of another file.

- EF_{CHV} is an elementary file containing the Cardholder verification information (CHV).

- EF_{DIR} is an elementary file at the MF or at DF level, which contains a list of all, or part of, available applications in the card (see also ISO 7816-5).

- EF_{ID} is an elementary file at the MF level, containing the identification number of the card.

- EF_{IC} is an elementary file at the MF level, containing general information concerning the integrated circuit (IC).

- EF_{ICC} is an elementary file at the MF level, containing general information concerning the ICC.

- EF_{KEY_OP} is an elementary file containing operational keys.

EF_{KEY_MAN} is an elementary file containing management keys.

- EF_{LANG} is an elementary file at the MF level, containing the language preferences.

- EF_{NAME} is an elementary file at the MF level, containing the cardholder name.

3.1.15 file identifier (ID): Each file (MF, DF, EF) has a file identifier consisting of 2 bytes.

3.1.16 file qualifier: First byte of the file identifier.

3.1.17 keyfile version: Indicates the absolute version number of the keyfile (coded in BCD).

3.1.18 master file (MF): The mandatory unique file representing the root of the file structure and containing AC and allocable memory. It may be the parent of elementary files and/or dedicated files.

3.1.19 operating system: That which is required to manage the logical resources of a system, including process scheduling and file management.

3.1.20 padding: One or more bits appended to a message in order to cause the message to contain the required number of bits or bytes.

3.1.21 path: Concatenation of file identifiers without delimitation.

3.1.22 pattern: Is a string of bytes.

3.1.23 record: Astring of bytes handled as a whole by the card and referenced by a record number or a record pointer.

3.1.24 record number: Is sequential and unique within an EF. It is managed by the card.

3.2 Abbreviations

For the purposes of this part of EN 726, the following abbreviations apply.

AC	Access Condition
ALW	Always
APDU	Application Protocol Data Unit
ASC	Application Specific Command set
ATR	Answer to reset
AUT	Authenticated
CHV	Card holder verification information
DECT	Digital European Cordless Telephone
DF	Dedicated File
EF	Elementary File
etu	Elementary time unit
IC	Integrated Circuit
ID	Identifier
MF	Master File
MII	Major Industry Identifier
NEV	Never
PIN	Personal Identification Number
PRO	Protected
PTS	Protocol type select (response to the ATR)
RFU	Reserved for Future Use

3.3 Symbols

For the purposes of this part of the standard, the following symbols apply.

nAs	nano Ampere per second
ns	nano second

mA	Milliampere
MHz	Megahertz
V_{CC}	Supply voltage
V_{PP}	Program voltage

3.4 Notations

'0' to '9' and 'A' to 'F': the sixteen hexadecimal digits

4 Physical characteristics of the card

The physical characteristics for ID-1 cards shall be in accordance with EN 27816-1:1989 and EN 27816-2:1989.

Nevertheless, EN 726 is not limited to ID-1 size card but shall also cover other card formats as defined in ENV 1375-1 and ENV 1375-2.

The following additional requirements shall be applied in order to ensure proper operation in portable battery and line powered operated equipment as well as in stationary equipment.

4.1 Layout

The position of the contacts for cards used in Europe shall be as follows :

- if no embossing and no magnetic stripe, contacts on any side ;
- if embossing, contacts on same side ;
- if magnetic stripe, contacts on other side ;
- if embossing & magnetic stripe, contacts on embossing side.

The identification number and the card sequence number (if it exists) as defined in EF_{ID} (see clause 10) may be present on the outside of the card (if embossed, then in accordance with EN 27811).

4.2 Temperature range for card operation

The temperature range for full operational use shall be between - 25 °C and + 65 °C with occasional peaks of up to 70 °C.

"Occasional" means not more than 4 hours each time and not over 100 times during the life time of the card.

For multi-application cards, which may also be used in portable battery operated equipment, the temperature range for operational use shall be between - 25 °C and + 70 °C with occasional peaks of up to + 85 °C.

"Occasional" means not more than 4 hours each time and not over 100 times during the life time of the card.

5 Electronic signals and transmission protocols

Electronic signals and transmission protocols shall be in accordance with EN 27816-3.
The following additional requirements shall be applied in order to have simplified terminals and to ensure a proper operation in Mobile Equipment, including portable battery operated, line powered equipment as well as in stationary equipment.

5.1 Supply voltage

The card shall be operated with a supply voltage V_{CC} of 5 V ± 10 %.

5.2 Supply current

The current consumption shall not exceed 20 mA at any frequency accepted by the card. If the card is expected to be used in mobile equipment including portable battery operated as well as line powered equipment, the current consumption shall not exceed 10 mA at any frequency.

Due to technology, spikes in the supply current can occur, the amplitude of which can be several times the average current. Under no circumstances, during operation, shall the card draw spike charges of over 40 nAs with no more than 400 ns duration and an amplitude of at most 200 mA.

5.3 Programming voltage

A programming voltage different from V_{CC} shall be generated internally.

NOTE : For the European telecommunication cards, the V_{PP} contact shall supply the same voltage as the V_{CC} contact (see also EN 726-4).

Special conditions may apply to mobile equipment. (see relevant specifications I-ETS 300045-1:1992 and DECT specifications)

5.4 Duty cycle

Duty cycle for asynchronous operation shall be between 40 % and 60 % of the period during stable operation.

5.5 Guardtime

For the transmission between the card and the terminal there are two extra guardtimes with regard to the time duration of the character. The character duration shall be fixed to 12 elementary time units (etu). The extra guardtime for the transmission from the terminal to the card shall be fixed by TC1, parameter N in the answer-to-reset, which shall have a value of 255 (except for T=0), 0 or 4. The guardtime for the transmission from the card to the terminal is indicated in the PTS2 and shall have a value of 255, 0 or 12.

5.6 Low consumption mode

Cards may have a low power consumption mode, especially for mobile equipment, indicated in the clockstop byte in EF_{ICC}.

6 Logical model for IC cards

The logical organisation of data in a card, which defines the memory management of the card is shown in figure 1.

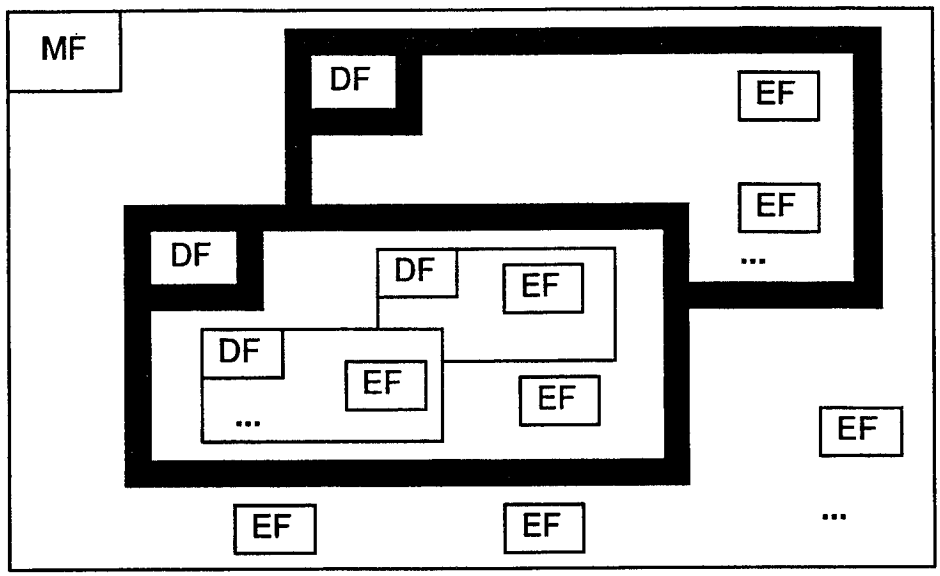

Figure 1 : Data structure model for an IC card

6.1 File identifier

See ISO/IEC 7816-4.

The file ID shall be chosen at the creation of the concerned file and shall be different for two files under the same parent. It is up to the operating system to ensure this requirement.

6.2 Elementary file (EF) structures

Based on ISO/IEC 7816-4, the following different elementary file (EF) structures are defined:

6.2.1 Transparent EF

An EF with a transparent structure consists of a sequence of bytes. A sequence of bytes to be read, written or updated are referenced by a relative address (offset) and a length indication (in bytes). The first byte of an EF with transparent structure has the relative address '00'. The total data length of the EF is indicated in the header of the EF.

6.2.2 EFs containing programs

If a transparent EF containing a program is created, the card issuer shall take all necessary steps to ensure that there is no possibility of interference between applications

For the set of commands, two possibilities appear:

- the general set of commands is sufficient and there is no need to associate this DF with an ASC-set;

- the general set of commands is not sufficient and there is a need to associate an ASC-set with this DF. This ASC-set shall be defined and agreed upon.

Programs contained in an EF are more related to the application with regard to some specific user-characteristics.

EXAMPLE 1 : In some applications, this could be in an IC card calculation of the limit based on some specific user-characteristics saved in the card.

Programs controlled by the specific ASC-set are more related to the application only.

EXAMPLE 2 : A specific cryptographic algorithm used to authenticate the application

6.2.3 EF with linear fixed structure

An EF of this structure consists of a sequence of records with fixed length. The first record in this EF is defined as record # 1. The following are indicated in the header of this structure:

- the total data length;

- number of records created;

- length of record.

There are three methods to access records within an EF of this type:
- using the record number;

- when positioned on the current record (known by the operating system), it shall be possible to perform an action on the current, the next (except for last record), the previous (except for the first record), the first or the last record existing in the EF;

- by pattern seek starting from the beginning forward, from the end backward, from the next record forward and from the previous record backward.

It is not possible to create more than 255 records in one file.

6.2.4 EF with linear variable structure

An EF of this structure consists of a sequence of records with variable length. The first record in this EF is defined as record # 1.

The following items are indicated in the header of this structure:

- the total data length;

- the number of records created;

Each record has it is own length indication, which cannot be changed after creation of the record.

The access to this type of EF is the same as for EFs with a linear fixed structure.

It is not possible to create more than 255 records in one file.

6.2.5 Cyclic EF

An EF of this structure consists of a sequence of records with identical length, organized as a ring. At creation time, all the records shall be filled with '00'.

In each file of cyclic structure the card maintains a reference to the last written record. In an EF of cyclic structure, the record number one (#1) is the last written record. The oldest written record, has the highest record number.

For writing operations, the only way of addressing a record is PREVIOUS. Only the record with the highest record number can be overwritten.

For increase and decrease operations the value to be modified is in the current record number 1, and the result of the computation shall be written in the oldest record. After an increase or decrease operation, the updated record shall become the current record number 1.

For reading operations, the ways of addressing a record are FIRST, LAST, NEXT, PREVIOUS, CURRENT or record number.

After the selection of a cyclic EF, the record pointer is automatically set on the last written record.

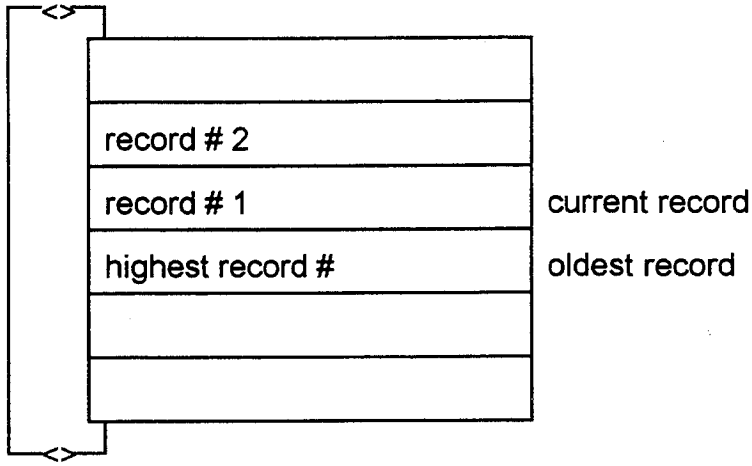

Figure 2 : Cyclic EF organization

It is not possible to create more than 255 records in one file.

6.2.6 EFs containing ASC-set

An EF containing an Application Specific Command Set (ASC) is a kind of filter which redirects commands and/or starts programs using procedures not defined in the general command set. An ASC can extend or modify the meaning of the general command set.

An ASC can only be associated to a given DF containing an application and becomes available when working on its subtree. When creating a DF, an information shall be given to the card indicating whether an EF containing an ASC-set may be available or not.

Only one ASC-set can be associated to a DF.

6.3 Contents of EF_{DIR}

EF_{DIR} may exist on any level. EF_{DIR} may have cross-references to DFs at any level according to business agreements.

The EF_{DIR} at the MF-level, contains for each non-hidden application the following information:

- application identifier;

- verbal description (Application label) of the application coded in ISO 8859-1:1987 (maximum 16 characters);

- path (Discretionary data) (sequence of 2 bytes file-IDs).

The coding of the contents of EF_{DIR} shall be in accordance with ISO/IEC 7816-5

6.4 Methods for selecting a file

See ISO/IEC 7816-4.

When the channel-mechanism shall be used to select files, the operating system shall have to remember the Current File, the Current Directory and the Current EF for each channel that is used.

With this channel mechanism, an exclusive select of the file (for one channel) shall be introduced. This is to prevent different applications to access data at the same time.