SLOVENSKI STANDARD
SIST EN 726-5:2004

01-maj-2004

Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 5: Payment methods

Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 5: Payment methods

Systemes de carte d'identification - Cartes a circuit intégré et terminaux pour les télécommunications - Partie 5: Méthodes de paiement

Ta slovenski standard je istoveten z: **EN 726-5:1999**

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices

SIST EN 726-5:2004 **en**

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 726-5

January 1999

ICS 35.240.15

English version

Identification card systems

Telecommunications integrated circuit(s) cards and terminals

Part 5: Payment methods

Systèmes de carte d'identification – Cartes à circuit intégré et terminaux pour les télécommunications – Partie 5: Méthodes de paiement

Identifikationskartensysteme – Anforderungen an Chipkarten und Endgeräte im Telekommunikationsbereich – Teil 5: Bezahlungsmethoden

This European Standard was approved by CEN on 1999-01-01.

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, the Czech Republik, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, and the 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

Page

Foreword 4

1 Scope 5

2 Normative references 5

3 Definitions, abbreviations and symbols 6
3.1 Definitions 6
3.1.1 application 6
3.1.2 application provider 6
3.1.3 autobilling 6
3.1.4 card 6
3.1.5 card issuer 6
3.1.6 closed system 6
3.1.7 elementary file (EF) 7
3.1.8 external application 7
3.1.9 external world 7
3.1.10 key set linked to SM 7
3.1.11 master file (MF) 7
3.1.12 off-line 7
3.1.13 on-line 7
3.1.14 open system 7
3.1.15 pre-payment 8
3.1.16 pre-payment application provider 8
3.1.17 telecommunication unit 8
3.1.18 Telecu 8
3.1.19 trusted authority 8
3.2 Abbreviations and symbols 9

4 General concepts 10
4.1 The payment application situated in the concept of card architecture 10
4.2 Selection of a payment method 11
4.3 Key management and the use of algorithms 11

5 Pre-payment 12
5.1 General concepts 12
5.2 The participants in the system 15
5.2.1 The pre-payment application provider 15
5.2.2 The cardholder 15
5.2.3 An application provider offering a service 15
5.2.4 Clearing and settlement 16
5.3 Security provisions for the pre-payment application 16
5.3.1 Security services to be used 17
5.4 Data requirements specific for pre-payment 18
5.4.1 $DF_{PRE-PAYMENT}$ 19
5.4.2 EF_{PAY} 19
5.4.3 EF_{AMOUNT} 21
5.5 General scenario for pre-payment application 22
5.5.1 Security in the external world for payment 23
5.5.2 Reload value in the card 23

6 Autobilling 23
6.1 General concepts 23
6.2 The participants in the system 24

6.2.1 The autobilling application provider 24
6.2.2 The cardholder 24
6.2.3 An application provider offering a service 24
6.3 Security provisions for the autobilling application 24
6.3.1 Security services to be used 25
6.4 Data requirements specific for autobilling 26
6.4.1 $DF_{AUTOBILLING}$ 27
6.4.2 EF_{AUTO} 27
6.5 General scenario of the autobilling application 28
6.5.1 Security in the external world 29
6.5.2 Load/reload the expiry date of the application 30

Annex A (normative) Selecting payment applications 31

Annex B (normative) Scenario for the pre-payment application (diagram) 32

Annex C (informative) Scenario for the pre-payment application in conjunction with the security module 34

Annex D (normative) Scenario for the autobilling application (diagram) 35

Annex E (informative) Scenario for the autobilling application in conjunction with the security module 36

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 July 1999, and conflicting national standards shall be withdrawn at the latest by July 1999.

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.

1 Scope

This part of EN 726 specifies payment methods for telecommunication applications, using IC cards. These payment methods are not necessarily linked to the applications which use them, and they can be used by more than one application.

This part of EN 726 gives guidance on the interface between the IC card and the external world, using the tools given in EN 726-3:1994 and EN 726-7.

This part of EN 726 considers an open system, in which the payment methods will be used. A closed system is a special case of the open system.

This part of EN 726 describes the following methods of payment :

- pre-payment ;

- autobilling.

For the purpose of this standard the functionality is based on :

- symmetric algorithms ;

- diversified keys.

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 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 726-2	Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 2 : Security framework
EN 726-3:1994	Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 3 : Application independent card requirements
EN 726-4	Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 4 : Application independent card related terminal requirements
EN 726-7	Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 7 : Security module
EN 24217	Codes for the representation of currencies and funds (ISO 4217:1990)
EN ISO/IEC 7816-5	Identification cards - Integrated circuit(s) cards with contacts - Part 5 : Numbering system and registration procedure for application identifiers (ISO/IEC 7816-5:1994)

3 Definitions, abbreviations and symbols

3.1 Definitions

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

They complete those gived in others parts of EN 726.

3.1.1 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 (card application) and outside of the IC card (external application). The owner of the IC card application may be different from the owner of the external world application.

3.1.2 application provider

The entity which is responsible for the application after its allocation, (the external application or for both). One application provider may have several application(s) in one card.

3.1.3 autobilling

A payment method using an IC card, where information is collected from the IC card, which allows the identification of an account that will be billed later.

3.1.4 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 for example be read, written or executed.

3.1.5 card issuer

The card issuer is responsible for the common data of the IC card, the allocation of memory space for the applications and supplies application provider with the necessary tools for loading the required application.

3.1.6 closed system

For the purpose of this part of EN 726 a closed system is defined as a system, containing one of the following possibilities :

- one issuer/one application provider where they are one entity or different entities ;
- multiple issuer/one application provider ;
- one issuer/multiple application providers.

3.1.7 elementary file (EF)

An optional file containing AC, data or a program and no other file, as :

- EF_{CHV1}, EF_{CHV2} are elementary files containing the cardholder verification information ;

- EF_{DIR} is an elementary file at the MF or at DF level, which contains a list of all or of a part of available applications in the card ;

- EF_{KEY-OP} is an elementary file containing operational keys ;

- $EF_{KEY-MAN}$ is an elementary file containing management keys.

3.1.8 external application

Entity, located in the external world, which communicates with the related card application during the session.

3.1.9 external world

All application related entities outside the IC card.

3.1.10 key set linked to SM

Relevant EF_{KEY-OP}(SM) and $EF_{KEY-MAN}$(SM).

3.1.11 master file (MF)

The unique mandatory file containing AC and optionally DF's and/or EF's.

3.1.12 off-line

A terminal, or terminal and connecting unit (including a security module), which can handle an application stand-alone during a transaction. From time to time however, an information exchange will take place with the system.

3.1.13 on-line

A connection to the system is needed during each transaction.

3.1.14 open system

For the purpose of this part of EN 726 an open system is defined as one containing :

- multiple issuers/multiple application providers with the need of clearing/settlement.

3.1.15 pre-payment

A payment method using an IC card, where the card contains a pre-payment application. The pre-paid value is stored in the card and offers access to other applications. Pre-paid value means that the payment is received in advance.

3.1.16 pre-payment application provider

The pre-payment application provider is the entity who supplies the pre-payment application.

3.1.17 telecommunication unit

A telecommunication unit represents a certain amount of service from a specified service provider.

NOTE : A telecommunication unit may represent monetary unit(s) but also a charge pulse of for example the telephone network.

3.1.18 Telecu

A common agreed European Telecommunication unit.

3.1.19 trusted authority

Independent authority in charge of approving, imposing and monitoring the system from the security point of view.

3.2 Abbreviations and symbols

AC	Access condition
ALW	Always
AUT	Authenticated
APDU	Application Protocol Data Unit
CH	Command header
CHV	Card holder verification
DF	Dedicated file
EF	Elementary file
ENC	Enciphered
IC	Integrated Circuit
ICC	Integrated Circuit Card
ID	Identifier of a file
INV	Invalidate
KSM	Key set linked to SM
MF	Master File
NEV	Never
PRO	Protected
REH	Rehabilitate
SM	Security Module

'0' to '9' and 'A' to 'F' : The sixteen hexadecimal digits.

4 General concepts

4.1 The payment application situated in the concept of card architecture

Figure 1 shows a possible structure of an IC card including a payment application.

Key to figure 1 : AC Access condition
PAY Payment application

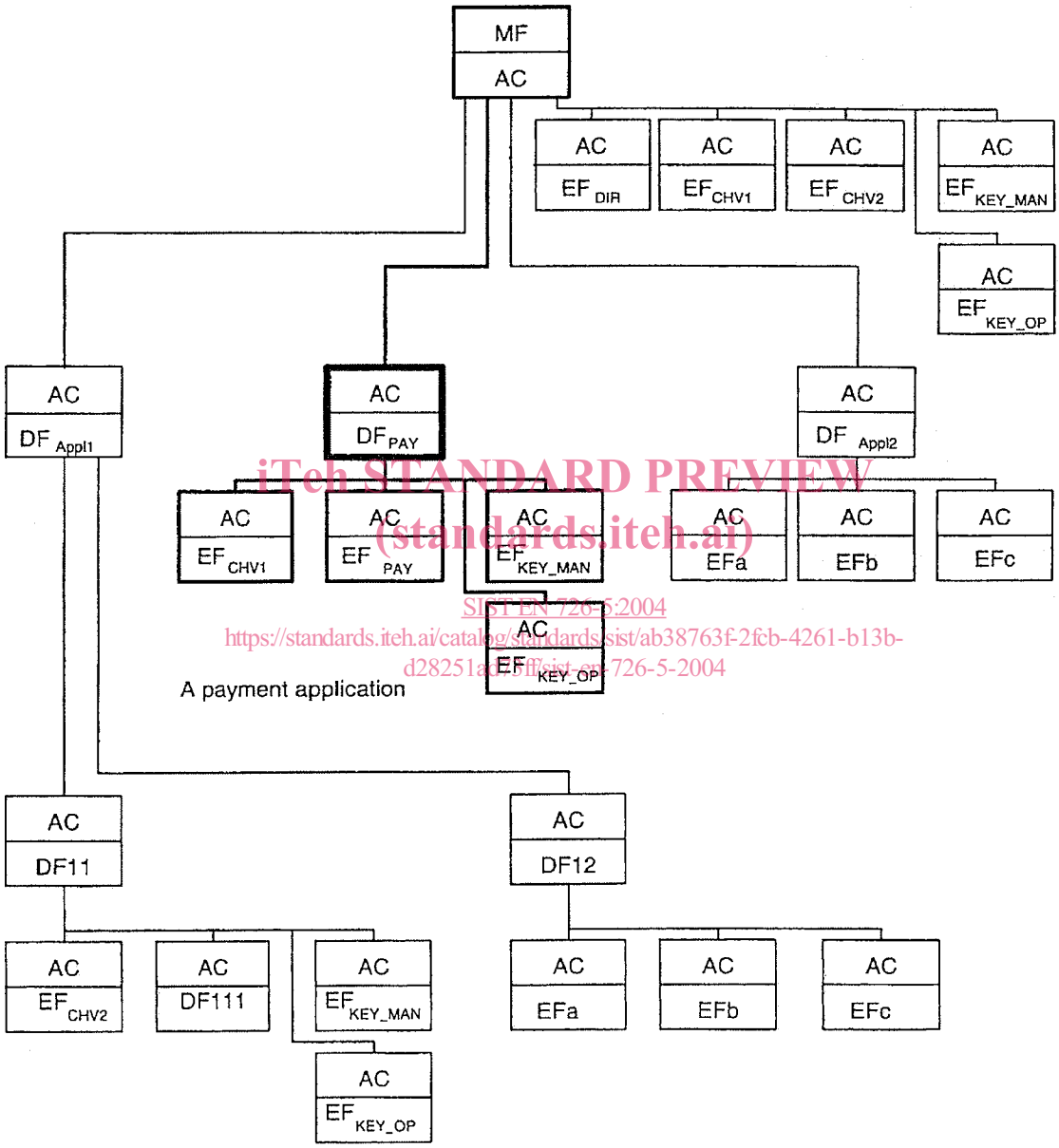

Figure 1 : Card architecture