

Identification card systems — Telecommunications integrated circuit(s) cards and terminals —

Part 5: Payment methods

The European Standard EN 726-5 :1999 has the status of a
British Standard

ICS 35.240.15

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW



Document Sharing Hub

National foreword

This British Standard is the English language version of EN 726-5:1999.
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 22, 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 Board and comes into effect on 15 September 1999

© BSI 09-1999

ISBN 0 580 35120 3

Amendments issued since publication

Amd. No.	Date	Comments

ICS 35.240.15

Descriptors: IC cards, terminal telecommunications, specifications

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

This European Standard was approved by CEN on 1 January 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.

CEN

European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

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

© 1999 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

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.

Contents

	Page
Foreword	2
1 Scope	3
2 Normative references	3
3 Definitions, abbreviations and symbols	3
4 General concepts	4
4.1 The payment application situated in the concept of card architecture	4
4.2 Selection of a payment method	4
4.3 Key management and the use of algorithms	6
5 Pre-payment	7
5.1 General concepts	7
5.2 The participants in the system	9
5.3 Security provisions for the pre-payment application	9
5.4 Data requirements specific for pre-payment	9
5.5 General scenario for pre-payment application	12
6 Autobilling	13
6.1 General concepts	13
6.2 The participants in the system	13
6.3 Security provisions for the autobilling application	13
6.4 Data requirements specific for autobilling	13
6.5 General scenario of the autobilling application	15
Annex A (normative) Selecting payment applications	17
Annex B (normative) Scenario for the pre-payment application (diagram)	18
Annex C (informative) Scenario for the pre-payment application in conjunction with the security module	20
Annex D (normative) Scenario for the autobilling application (diagram)	21
Annex E (informative) Scenario for the autobilling application in conjunction with the security module	22

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 given in others parts of EN 726.

3.1.1

application

an application consists of a set of security mechanisms, files, data and 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

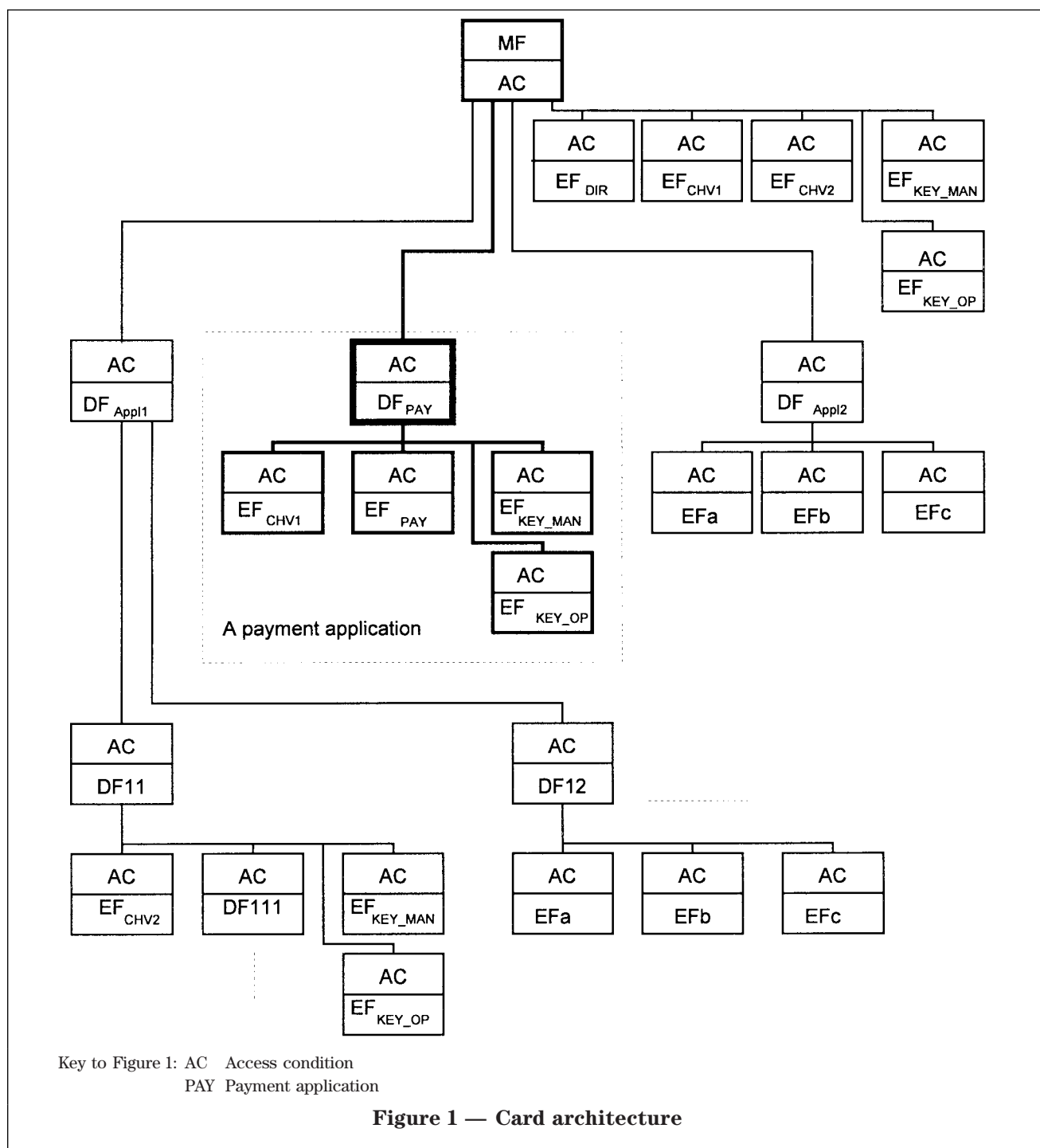
4.1 The payment application situated in the concept of card architecture

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

4.2 Selection of a payment method

If only one payment method is supported by the external world this payment application may be directly selected.

In order to determine which different payment methods are supported by the IC-card, the external application may read out EF_{DIR} at master file level (see EN 726-3:1994), which contains the standardized application identifiers of the various applications supported by the IC card.



After reading EF_{DIR}, the external application shall compare the list of available payment applications in the IC card with the list of payment applications the external application supports. If more than one option is possible, the user shall have the possibility to select a payment application.

After selecting the payment application, the path for selecting it in the IC card is found in EF_{DIR}, together with its standardized application identifier.

For each payment application, there shall be defined a unique, standardized application identifier in accordance with EN 726-3:1994 and EN ISO/IEC 7816-5. The general scenario to select a payment application is described in annex A.

4.3 Key management and the use of algorithms

For each payment application, it is mandatory that the card application and the corresponding external application use the corresponding keys and algorithms. For a certain payment application in the card, correlated keys must be shared between both the cards and the external world.

Only one EF_{KEY-OP} or EF_{KEY-MAN} may be linked to fulfil the access conditions for one file. If another keyset or algorithm shall be used, for example by another network provider, another application (including application identifier) has to be defined.

