

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

Part 7: Security module

The European Standard EN 726-7:1999 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 726-7:1999.

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 48, 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 Committee and comes into effect on 15 November 1999

© BSI 11-1999

ISBN 0 580 35472 5

Amendments issued since publication

Amd. No.	Date	Comments

ICS 35.240.15

Descriptors: telecommunications, IC cards, telecommunication terminals, safety, specifications

English version

Identification card systems — Telecommunications integrated circuit(s) cards and terminals — Part 7: Security module

Systèmes de cartes d'identification — Cartes à circuit intégré et terminaux pour les télécommunications —
Partie 7: Module de sécurité

Identifikationskartensysteme — Chipkarten und Endgeräte für Telekommunikationszwecke —
Teil 7: Sicherheitsmodul

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	8.2 Functions used to compute a cryptogram or message authentication codes (MAC)	11
1 Scope	3	8.2.1 COMPUTE LOAD KEY	11
2 Normative references	3	8.2.2 COMPUTE MAC	12
3 Definitions and abbreviations	3	8.2.3 COMPUTE CRYPTOGRAM	13
3.1 Definitions	3	8.3 Functions verifying cryptograms or message authentication codes (MAC)	14
3.2 Abbreviations	5	8.3.1 VERIFY MAC	14
4 Physical characteristics of the SM	6	8.3.2 UPDATE (SM)	15
5 Electronic signals and transmission protocols	6	8.3.3 INCREASE (SM)	15
6 Logical model for SM	6	8.3.4 DECREASE (SM)	16
7 General concepts	7	8.3.5 VERIFY CRYPTOGRAM	17
7.1 General security principles	7	8.4 Functions for downloading of keys from the SM to the UC	17
7.1.1 Access conditions	7	8.5 Functionality on SM-EW interface	17
7.1.2 Sequence control	7	8.6 Linking functions with keys	18
7.2 SM Life cycle	7	8.7 Limitations of the usage of keys	18
7.3 Configuration of the system	7	9 Data elements	18
7.4 SM security functions	9	9.1 Data for SM identification	18
8 Description of the functions of a SM	9	9.1.1 SM identifier	18
8.1 Functions without MAC	10	9.2 UC data	19
8.1.1 SELECT KEYSET	10	9.2.1 IC serial number of user card	19
8.1.2 DIVERSIFY KEYSET	10	9.2.2 Application Expiry date	19
8.1.3 ASK PARAMETER	10	9.2.3 Application Identifier (AID)	19
		9.2.4 Key file version	19
		9.2.5 Algorithm identifier	19
		9.2.6 Amount	19
		9.2.7 Value	20
		9.2.8 Type of units	20
		9.3 Status conditions returned by the SM	20
		9.3.1 Functions versus possible status responses	20
		Annex A (normative) The case of a SM in the form of an IC card	23
		Annex B (informative) Example of scenarios for SM in the form of an IC card	35
		Annex C (informative) Bibliography	48

1 Scope

This part of EN 726 specifies:

- the minimum security requirements for a Security Module (SM);
- the general card related functions embedded in the SM-terminal protocols including minimum data exchange; The data elements and cryptographic processing described in annex A for the case where the SM is an ICC should be supported if the SM is not an ICC or the configuration of the system, e.g. where the SM handles more than one terminal/user card. Configurations where the SM handles more than one terminal/user card are not fully specified in this standard. Further mechanisms may be required to enable these configurations;
- the necessary security services and mechanisms to provide application and cryptographic security information for the processing of telecommunication transactions.

considering several types of SMs at different locations in the system and different system configurations.

This part of EN 726 allows interaction between the Integrated Circuit Card (IC card) and the SM via the terminal in a way that may be functionally transparent to the terminal and possibly also the network(s). This provides the flexibility to use different techniques, commands and message formats at the terminal-SM interface.

This part of EN 726 supports IC cards with payment applications following EN 726-5 and all card applications following clauses 4 to 7 of this part of the standard. This part of EN 726 supports IC cards following EN 726-3:1994. Other telecommunication cards which are not in accordance with EN 726, e.g. simple memory cards, may also be supported by the SM described in this part.

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 726-2:1995, *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 726-5, *Identification card systems — Telecommunications integrated circuit(s) cards and terminals — Part 5: Payment methods.*

EN 24217, *Codes for the representation of currencies and funds.*
(ISO 4217:1990)

EN ISO/IEC 7816-4, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interchange.*
(ISO/IEC 7816-4:1995)

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)

ISO 10202-4, *Financial transactions cards — Security architecture of financial transaction systems using integrated circuit cards — Part 4: Secure application modules.*

3 Definitions and abbreviations

3.1 Definitions

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

3.1.1

access conditions (AC)

a set of security attributes associated to a file

3.1.2

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 and outside the IC card (external application).

3.1.3

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 or from several application providers

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 DF can be associated, optionally, an ASC-set (an application specific command set and/or an application specific program). 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

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

3.1.7

dedicated file (DF)

a file containing AC and allocatable memory. It may be the parent of elementary files and/or dedicated files

3.1.8

elementary file (EF)

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

- EF_{DIR} is an elementary file at the master file or at DF level, which contains a list of all, or part of, available applications in the card;
- EF_{ID} is an elementary file at the master file level, containing the identification number of the card
- EF_{ICC} is an elementary file at the master file level, containing general information concerning the IC and IC card;
- EF_{KEY_OP} is an elementary file containing operational keys;
- EF_{KEY_MAN} is an elementary file containing management keys;
- EF_{DIK_OP} is an elementary file containing diversified operational keys;
- EF_{DIK_MAN} is an elementary file containing diversified management keys.

3.1.9

file identifier (ID)

each file (MF, DF, EF) has an identifier consisting of 2 bytes

3.1.10

file qualifier

first byte of the file identifier

3.1.11

master file (MF)

the mandatory unique file representing the root of the file structure and containing AC and allocatable memory. It may be the parent of elementary files and/or dedicated files

3.1.12

operating system

that which is required to manage the logical resources of a system, including process scheduling and file management

3.1.13

path

concatenation of file identifiers without delimitation

3.1.14

secrets

algorithm(s), related key(s), security procedures and information

3.1.15

security module

a device containing logically and physically protected secrets — algorithm(s), related key(s), security procedures and information to protect applications in such a way that unauthorized access is not feasible. In order to achieve this the module may in addition be further physically, electrically and logically protected

3.1.16

security module provider

see ISO 10202-4

3.1.17

sequence control

a feature assuring that operations, invoked by commands, can only be performed by the SM in allowed, predefined order(s)

3.2 Abbreviations

AC	Access Condition
AID	Application Identifier
AUT	Authenticated
CHV	Card Holder Verification information
DF	Dedicated File
EF	Elementary File
EW	External World
IC	Integrated Circuit
ICC	Integrated Circuit Card
ID	Identifier of a file
IFD	Interface Device
INT.AUTH	Internal Authentication
INV	Invalidate
LEN	Length
MAC	Message Authentication
MF	Master File
NEV	Never
PRO	Protected
RAN	Random
REH	Rehabilitate
RFU	Reserved for Future Use
SM	Security Module
UC	User Card

4 Physical characteristics of the SM

If the SM is an IC card the physical characteristics shall be in accordance with clause 4 of EN 726-3:1994.
 For any other case the physical characteristics are out of the scope of this part of EN 726.

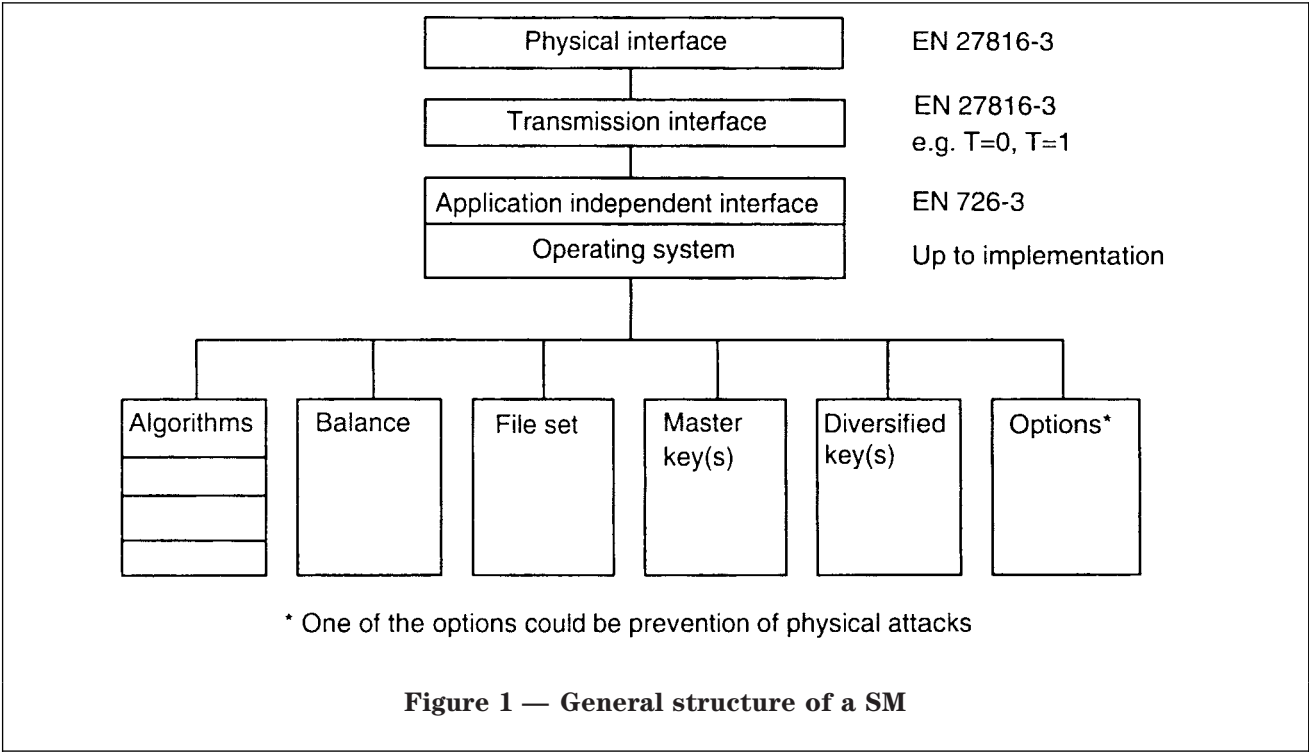
5 Electronic signals and transmission protocols

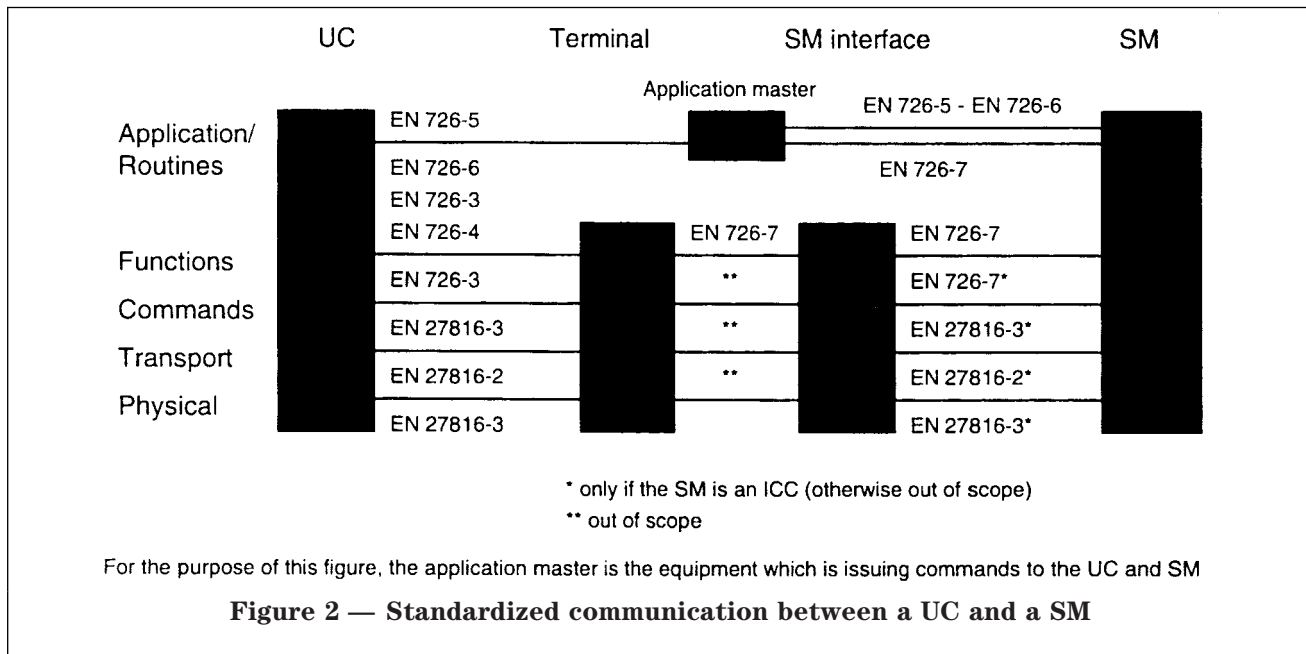
If the SM is an IC card the electronic signals and transmission protocol(s) shall be in accordance with clause 5 of EN 726-3:1994.
 For any other case the electronic signals and transmission protocol are out of the scope of this standard.

6 Logical model for SM

A SM following this standard contains:

- permanent secrets (master key(s));
- temporary secrets (diversified key(s));
- a balance (optional);
- an operating system to handle secure access to the secrets mentioned above. Additional options are possible as long as they do not interfere with the basic contents, but are out of the scope of this standard.





7 General concepts

7.1 General security principles

The SM provider shall be responsible for the life cycle of the SM.

Any aspect in the operation of a SM or data obtainable from a SM shall not compromise the security of the system.

Cryptographic keys used in the SM and the UC shall be managed in such a way that the security of any system using SMs or UCs is not compromised.

During the application life cycle the need to change keys in the UC may appear. To support this the SM may contain several keyset versions.

Interoperability of telecommunication SMs in Europe is based on the exchange of secret keys. The mechanisms for downloading keys into the SM are not described in this part of EN 726. The isolation of the key management systems between different operators requires the use of a trusted party.

7.1.1 Access conditions

For the functions described in this part of the standard no ACs have to be fulfilled in the SM, but the usage of the keys may be restricted. The SM uses diversified keys for functions in the UC where the ACs require a key operation. For the management of the SM by the External World, the ACs defined in EN 726-3:1994 shall apply only if the SM is an IC card.

The SM may also perform a key diversification for Application Specific functions in the UC which are not defined in EN 726-3:1994. In this case, the limits of the usage of the key(s) for this specific function shall be kept in the SM.

7.1.2 Sequence control

A sequence control can be achieved by using ACs of the UC on the SM. Sequence control functions where the SM checks if it is allowed to perform commands and status responses can optionally be added if needed in the application. The implementation is out of the scope of the standard. Nevertheless the following applies, if the command is allowed the operation will be performed and the results will be the outcome of the command. If the command is not allowed the operation will not be performed and the status conditions will contain “Command out of sequence”. The internal reaction of the SM is application dependent.

7.2 SM Life cycle

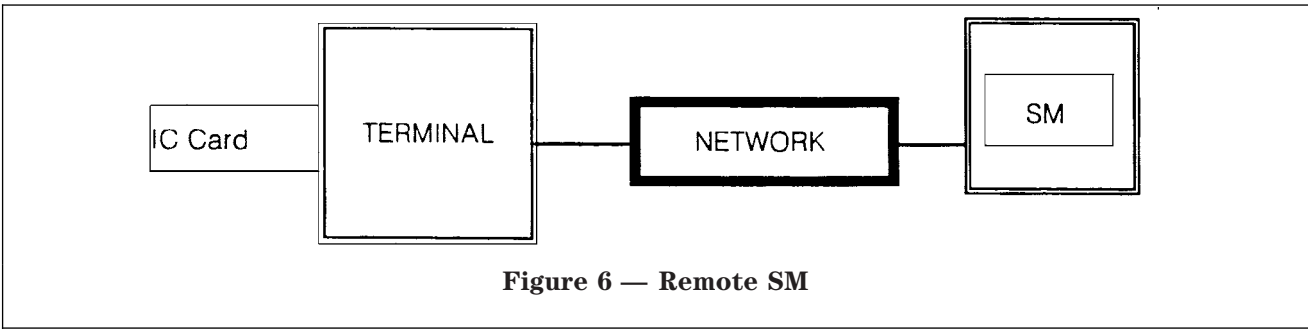
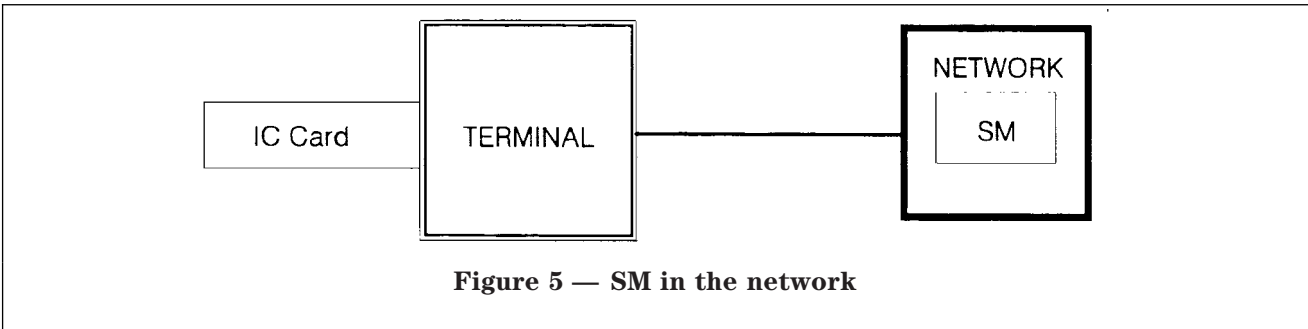
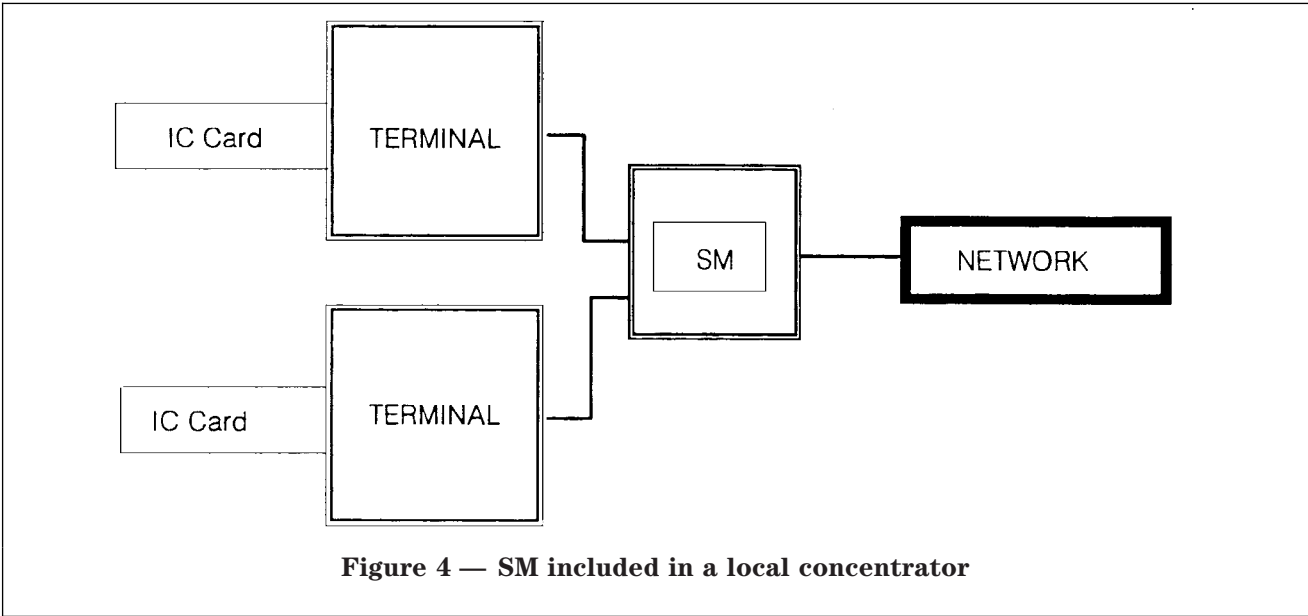
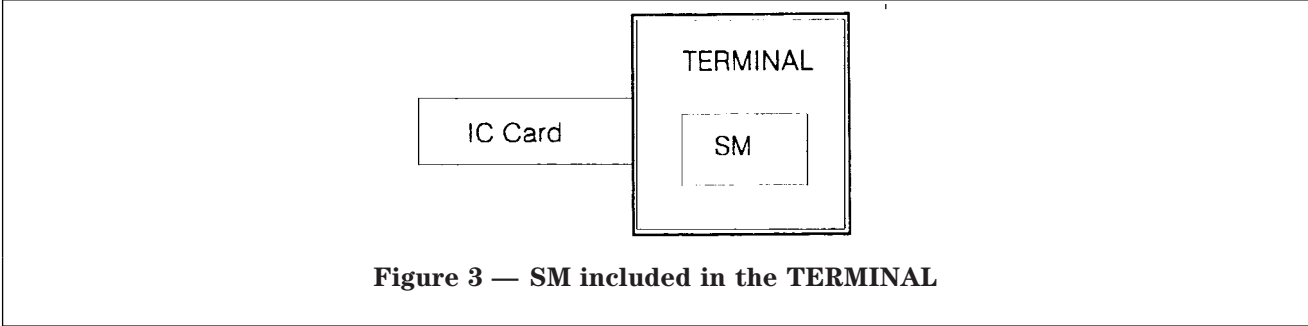
See ISO 10202-4.

7.3 Configuration of the system

The general card related functions at the SM-terminal interface including minimum data exchange shall not be affected. The user card-terminal interface shall not be affected by type of implementation of the SM.

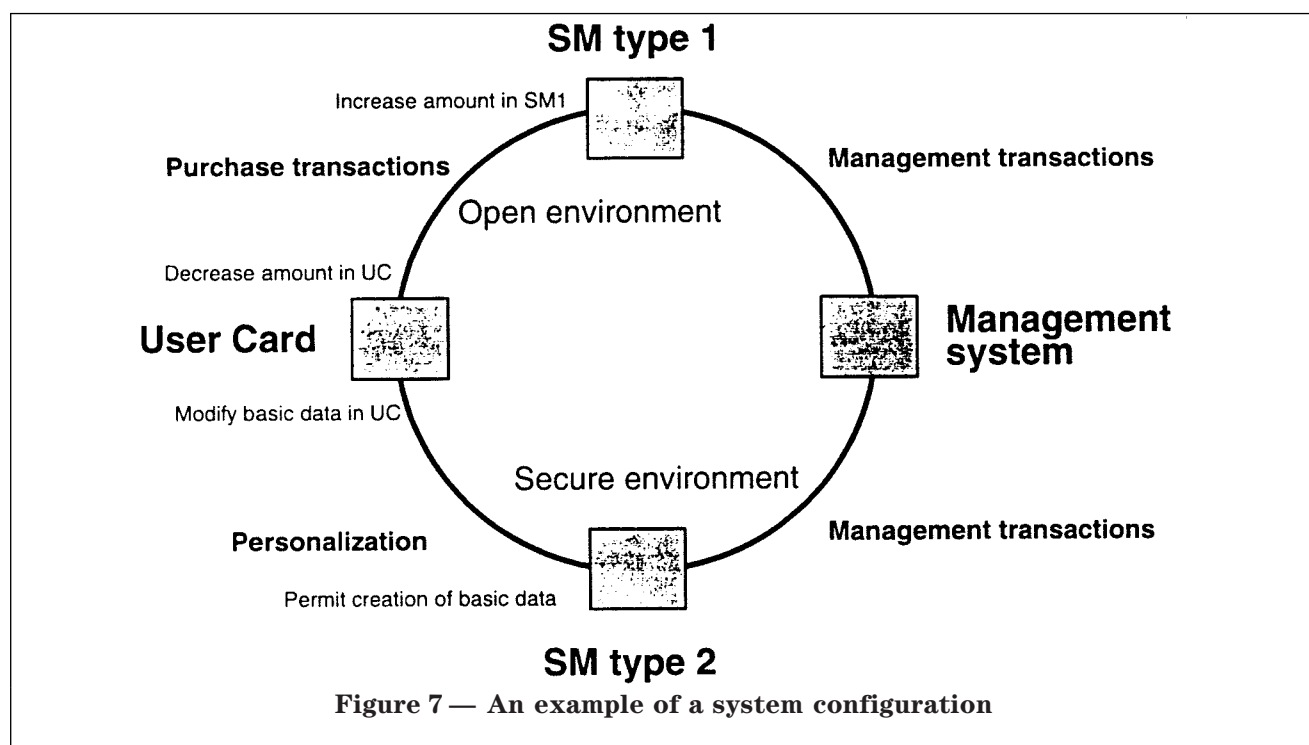
Four possible configurations of the SM are shown in Figures 3 to 6.

In the interests of completeness all four locations are shown. However, it is probable that for the more distant locations a higher level transport protocol may be appropriate. Such high level transport protocols are outside the scope of this standard.



A distinction between normal operations (transfer of sensitive data such as payment transactions) and more sensitive operations (such as creation of sensitive data) may be necessary. In this case, two kinds of SM may exist. SM1 situated in an open environment only allowing normal operations and SM2 (and terminal) located in a secure environment and allowing in addition e.g. personalization.

For SMs covering more sensitive operations, specific security tools are necessary as physical protection. These requirements are out of the scope of this standard.



7.4 SM security functions

A SM contains:

- secrets which allow the terminal to access protected parts of the UC;
- secrets which allow the authenticity of the UC to be checked;
- optionally, a balance that can be increased and decreased in a secure manner in the SM, coupled with a corresponding reverse operation in the UC.

A SM shall be logically and physically protected against attacks aimed at exposing or abusing secrets during the whole life cycle of the SM.

All functions shall be independent of transmission protocols. These may be different at the terminal-UC and at the terminal-SM interface.

In order to fulfill the AC = AUT or PRO of files in the UC, any related functions in the UC and the SM shall use the same keys and algorithms.

For the purpose of this part of EN 726 the functionality is based on:

- symmetric algorithms;
- diversified keys.

However, the use of asymmetric or hybrid cryptosystems may be defined later.

8 Description of the functions of a SM

This clause only describes the additional specific functions necessary for a SM. If the SM is an IC card the remaining part of this clause and annex A apply. Additional functions to support other applications outside the scope of EN 726 are not precluded. Any such function shall not conflict with the content of EN 726. The command header and trailer referred to in this chapter are data elements used to control the processing of data by the SM in accordance with the function specified.

8.1 Functions without MAC

8.1.1 *SELECT KEYSET*

The purpose of this function is to unambiguously address a specific keyset in the SM, that shall be used at least for the next cryptographic computation, corresponding to the specific command, file, AC and application of the UC. In case a UC following EN 726-3:1994 is used, the SM shall select a keyset corresponding with the key master version indicated by the UC.

Input: a/ command header;
 b/ key qualifier.

Table 1 — Key qualifier (in case of a MF of the UC)

Bytes	Description	Length
1 to 4	IC card manufacturing references (coded in accordance with EN 726-3:1994)	4 bytes
5	Card personalizer ID (coded in accordance with EN 726-3:1994)	1 byte
6 to 7	File ID of the EF _{KEY}	2 bytes
8	Keyfile version (coded in accordance with EN 726-3:1994)	1 byte

Table 2 — Key qualifier (in case of a DF in the UC)

Bytes	Description	Length
1 – X	AID (coded in accordance with to EN 726-3:1994)	1 to 16 bytes
(X + 1) – (X + 2)	File ID of the EF _{KEY}	2 bytes
X + 3	Keyfile version (coded in accordance with EN 726-3:1994)	1 byte

Output: a/ data : none;
 b/ status.

8.1.2 *DIVERSIFY KEYSET*

The purpose of this function is to derive temporary keys from all the master keys contained in the previously selected keyset using application specific diversification data. The temporary keys are written in a specific temporary file. After key diversification, this temporary file becomes relevant for the DF in the UC.

This diversified keyset is kept in the SM and is valid until the next diversification using the same master keyset takes place.

NOTE To increase the prevention of misuse of diversified keys sequence control can be used.

All secret keys, diversified as well as master keys, shall never be allowed to be read out from the SM.

Pre-conditions: before the DIVERSIFY KEYSET function is performed, the relevant keyset shall be selected by use of the SELECT KEYSET function.

Input: a/ command header;
 b/ diversification data;
 c/ algorithm ID.

Table 3 — Diversification data

Bytes	Description	Length
1 – X	Diversification data (application dependent)	1 to 16 bytes

Output: a/ data : none;
 b/ status.

8.1.3 *ASK PARAMETER*

The purpose of this function is to transfer a parameter from the SM to the terminal.

This parameter is given to the terminal and used inside the SM to compute the next incoming cryptogram.

This parameter shall be valid until the next function requiring a challenge is performed in the SM except in the case of VERIFY MAC.

Types of parameters:

- 1) challenge (random);
- 2) challenge (counter).

Several counters for providing challenges, related in different keysets, may exist. In case of multiple counters the counter related to the previously selected keyset shall be used to provide the challenge, else a common SM-counter shall be used.

NOTE 1 It is proposed not to specify the counter structure for the case where the SM is an ICC in order to allow flexibility in the way the system works.

NOTE 2 For some applications a counter, e.g. a transactions number, may be used instead of a random number. In the case of the SM not being an IC-card, functionality is equivalent to what is described in A.5.3.1.

Input: a/ command header;
b/ type of parameter;
c/ length.

Output: a/ parameter;

Table 4 — Parameter

Bytes	Description	Length
1 – X	Challenge	X bytes

b/ status.

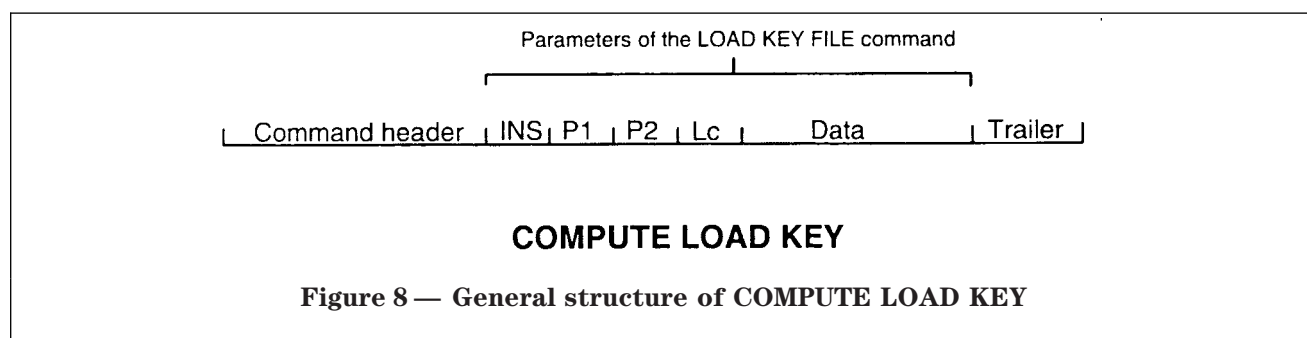
8.2 Functions used to compute a cryptogram or message authentication codes (MAC)

If TESA 7 is used, a cryptogram is computed according to Tesa 7 mode “authentication” (see A.3.1 and A.3.2 of EN 726-2:1995) and message authentication (MAC) is computed according to Tesa 7 mode “MAC” (see A.2.3 and A.2.4 of EN 726-2:1995)

NOTE In other parts of this standard the result of the MAC computation may be also referred as “cryptogram”.

8.2.1 COMPUTE LOAD KEY

The purpose of this function is to provide an enciphered key and the related cryptogram to the UC. The SM shall perform an encipherment of the key (indicated in the input parameters) of the previously selected keyset. The key used to perform the encipherment shall be indicated in the command header of COMPUTE LOAD KEY. The enciphered key, the contents of the data field and the challenge previously given by the UC shall be used to provide a cryptogram. The input data for this function contains the necessary parameters used in the UC for verifying the cryptogram.



Pre-conditions: the challenge used to compute the cryptogram shall be obtained from the UC by an ASK RANDOM function and transmitted by the terminal to the SM using a GIVE RANDOM;
the keyset shall be selected using the SELECT KEYSET function. The relevant key file shall be the one containing the keys after diversification.

Input: a/ command header/trailer (COMPUTE LOAD KEY);
b/ data (parameters of the following UC command);

Table 5 — Data

Bytes	Description	Length
1	INS byte of the following LOAD KEY FILE command sent to the UC (coded in accordance with EN 726-3:1994)	1 byte
2	P1 of the following LOAD KEY FILE command sent to the UC (coded in accordance with EN 726-3:1994)	1 byte
3	P2 of the following LOAD KEY FILE command sent to the UC (coded in accordance with EN 726-3:1994)	1 byte
4	L _c of the following LOAD KEY FILE command sent to the UC (coded in accordance with EN 726-3:1994)	1 byte
5	Key file version (only present if key number 1)	1 byte
6	Key length	1 byte
7	Algorithm identifier	1 byte

c/ key number (indicated in the command header of the LOAD KEY command (P2));

d/ EF_{KEY} type (EF_{KEY_MAN} or EF_{KEY_OP}) indicated in the command header of the LOAD KEY FILE command (P1).

Output: a/ response data;

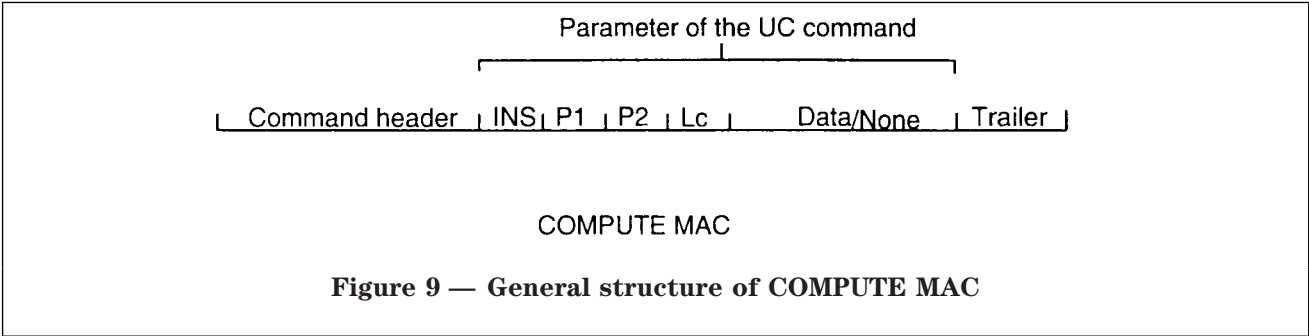
Table 6 — Response data

Bytes	Description	Length
1 to 16	Enciphered key	16 bytes
17 to 24	MAC	8 bytes

b/ status.

8.2.2 COMPUTE MAC

For functions in the UC which need a MAC in order to fulfill the ACs, the general function COMPUTE MAC shall be used in the SM to calculate the MAC. The input data for this function contains the necessary parameters used in the UC for verifying the MAC (command header and data).



Pre-conditions: the challenge used shall be obtained from the UC by an ASK RANDOM function and transmitted by the terminal to the SM using a GIVE RANDOM;

the keyset shall be selected using the SELECT KEYSET function. The relevant key file shall be the one containing the keys after diversification.

Input: a/ command header/trailer (COMPUTE MAC);

b/ data (parameters of the following UC command);

Table 7 — Data

Bytes	Description	Length
1	INS byte of the following command sent to the UC (coded in accordance with EN 726-3:1994)	1 byte
2	P1 of the following command sent to the UC (coded in accordance with EN 726-3:1994)	1 byte
3	P2 of the following command sent to the UC (coded in accordance with EN 726-3:1994)	1 byte
4	L _c of the following command sent to the UC (coded in accordance with EN 726-3:1994)	1 byte
5 – (4 + X)	The data field of the following command sent to the UC (coded in accordance with EN 726-3:1994)	X bytes

c/ key number (indicated in the command header if SM is an IC card).

Output: a/ MAC (UC command header, data);

Table 8 — Cryptogram

Bytes	Description	Length
1 – X	MAC	X bytes

b/ status.

NOTE The length X depends on the cryptographic algorithm application. In case of TESA 7 X = 8.

For the following functions in the UC, the COMPUTE MAC function is applicable when AC = PRO:

CREATE FILE
DELETE FILE
EXTEND
EXECUTE
UPDATE BINARY
UPDATE RECORD
CREATE RECORD
INVALIDATE
REHABILITATE
WRITE BINARY
WRITE RECORD
DECREASE
CREATE RECORD

The purpose of these functions is to prove that the SM has been involved in a given transaction and that the function it was to perform has been accomplished.

8.2.3 COMPUTE CRYPTOGRAM

This function shall be used to compute the cryptogram used in the user card in the EXTERNAL AUTHENTICATION command.

Pre-conditions: the challenge used shall be obtained from the UC by an ASK RANDOM function and transmitted by the terminal to the SM using a GIVE RANDOM;

the keyset shall be selected using the SELECT KEYSET function. The relevant key file shall be the one containing the keys after diversification.

Input: a/ command header/trailer (COMPUTE CRYPTOGRAM);

b/ key number (indicated in the command header if SM is an IC card).

Output: a/ cryptogram;

Table 9 — Cryptogram

Bytes	Description	Length
1 – X	MAC	X bytes

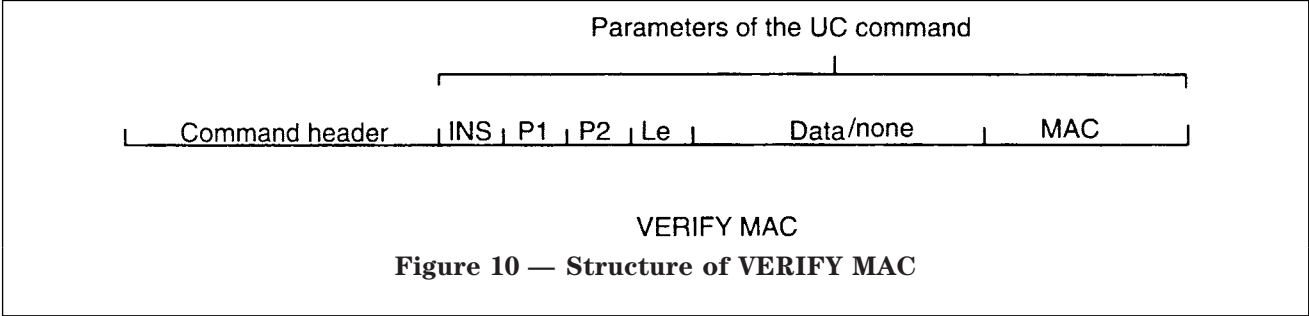
b/ status.

8.3 Functions verifying cryptograms or message authentication codes (MAC)

If Tesa 7 is used, a cryptogram is computed according to Tesa 7 mode “authentication” (see A.3.1 and A.3.2 of EN 726-2:1995) and message authentication (MAC) is computed in accordance with Tesa 7 mode “MAC” as described in A.2.3 and A.2.4 of EN 726-2:1995. In other parts of this standard the result of the MAC computation may be also referred as “cryptogram”.

8.3.1 VERIFY MAC

The purpose of this function is to verify a MAC performed in the UC. The SM shall check if the indicated key is allowed to perform this function.



- Pre-conditions:

the challenge used shall be obtained from the SM using an ASK PARAMETER function and transmitted to the UC using a GIVE RANDOM;

the keyset shall be selected using the SELECT KEYSET function. The relevant key file shall be the one containing the keys after diversification.
- Input:

a/ command header/trailer (VERIFY MAC);

b/ Key number (indicated in the command header);

c/ data (parameters of the previous UC command/response).

Table 10 — Data

Bytes	Description	Length
1	INS byte of the previous command sent to the UC (coded in accordance with EN 726-3:1994)	1 byte
2	P1 of the previous command sent to the UC (coded in accordance with EN 726-3:1994)	1 byte
3	P2 of the previous command sent to the UC (coded in accordance with EN 726-3:1994)	1 byte
4	The L _e of the previous command sent to the UC (coded in accordance with EN 726-3:1994)	1 byte
5 – (4 + X)	The data field of the previous response sent by the UC (coded in accordance with EN 726-3:1994)	X bytes

- Output:

a/ data : none;

b/ status.

For the following functions in the UC which provide MACs, the VERIFY MAC function is applicable:

- READ BINARY STAMPED

READ RECORD STAMPED

The cryptogram shall be in accordance with EN 726-3:1994. The key indicated in the command header of the VERIFY MAC function, shall be the same as the one used to compute the MAC in the UC.