SLOVENSKI STANDARD
SIST EN 726-2:1998

01-junij-1998

Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 2: Security framework

Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 2: Security framework

Identifikationskartensysteme - Chipkarten und Endgeräte für Telekommunikationszwecke - Teil 2: Sicherheitsgrundgerüst

Systemes de cartes d'identification - Cartes à circuit intégré et terminaux pour les télécommunications - Partie 2: Cadre général pour la sécurité

Ta slovenski standard je istoveten z: **EN 726-2:1995**

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices

SIST EN 726-2:1998 **en**

EUROPEAN STANDARD **EN 726-2**

NORME EUROPÉENNE

EUROPÄISCHE NORM November 1995

ICS 33.120.00; 35.240.60

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

English version

Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 2: Security framework

Systèmes de cartes d'identification - Cartes à circuit intégré et terminaux pour les télécommunications - Partie 2: Cadre général pour la sécurité

Identifikationskartensysteme - Chipkarten und Endgeräte für Telekommunikationszwecke - Teil 2: Sicherheitsgrundgerüst

This European Standard was approved by CEN on 1995-10-18. 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 has been prepared by the Technical Committee CEN/TC 224 "Machine-readable cards, related device interfaces and operations" of which the secretariat 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 May 1996, and conflicting national standards shall be withdrawn at the latest by May 1996.

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 the 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 a security framework for telecommunication use of IC cards. This specification does not describe any implementation details. It describes:

- a general security approach resulting in a methodology, different card phases for identifying security requirements and a description of security services which can be offered by the IC card;

- the implementation of the general security approach to the application independent IC card, resulting in a list of application independent security requirements, a selection of needed security services and a description of a common set of application independent security mechanisms;

- the implementation of the general security approach to applications using IC cards, resulting in a methodology which is used to design the set of security mechanisms for specific applications.

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 amendments 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: Systems overview
EN 726-3	1994	Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 3: Application independent card requirements
prEN 726-7	1994	Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 7: Security module
EN 27498	1989	Information Processing Systems - Open Systems Interconnection, Basic Reference Model
ISO 7498-2	1989	Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture
ISO/IEC 9798-2		Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment alogorithms
ISO 9798-3		Information technology - Security techniques - Entity authentication mechanisms - Part 3: Entity authentication using a public key algorithm
ISO 10202-1	1991	Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Part 1: Card life cycle

3 Definitions and abbreviations

3.1 Definitions

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

3.1.1 access control information: Information describing for each action which can be performed on a file in the card, the conditions to fulfil.

3.1.2 action: An action performed by an external application on a card means a command followed by a response.There are two kinds of actions: normal actions on files of the card (e.g. Read, Write, Select, Execute, Invalidate, Rehabilitate...) management actions on files of the card (e.g. Create, Delete, Extend...).

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 of the IC card (external application).

3.1.4 application privilege information: External application capabilities used to perform the rights of the external application.

3.1.5 application provider: The entity which is responsible for the application after its allocation. One application provider 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.

3.1.6 card: A multi-application card can be considered as a set of files, some of them shared by the different application provider and/or card issuer, others owned exclusively by application provider or issuer. Files can be read, written or executed. The files located in the card corresponding to one application provider are called card application.

3.1.7 card application: The card related part of one application.

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

3.1.9 card manufacturer: The card manufacturer is the entity which fabricates the card and performs the IC embedding.

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

3.1.11 external world: All application related entities outside the card.

3.1.12 kernel: Part of the card or external world, which contains application independent data/code, including the MF (in case of a card kernel) and the operating system.

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

3.1.14 protocol control information (PCI): Information exchange between application entities using transmission protocols to coordinate the joint operation.

3.1.15 tampering: An unauthorized modification which alters the proper functioning of the card in a manner which degrades the security it provides;

3.1.16 trusted authority: Independent authority in charge of imposing and monitoring the system from the security point of view.

3.2 Abbreviations

For the purpose of this standard the following abbreviations apply:

AC Access Conditions

ACI Access Control Information

API Application Privilege Information

CHV Card Holder Verification

EF Elementary File

EW External World

IC Integrated Circuit

MF Master File

PIN Personal Identification Number

4 Reference model

This reference model has been included here because it is used as a model in the following clauses.

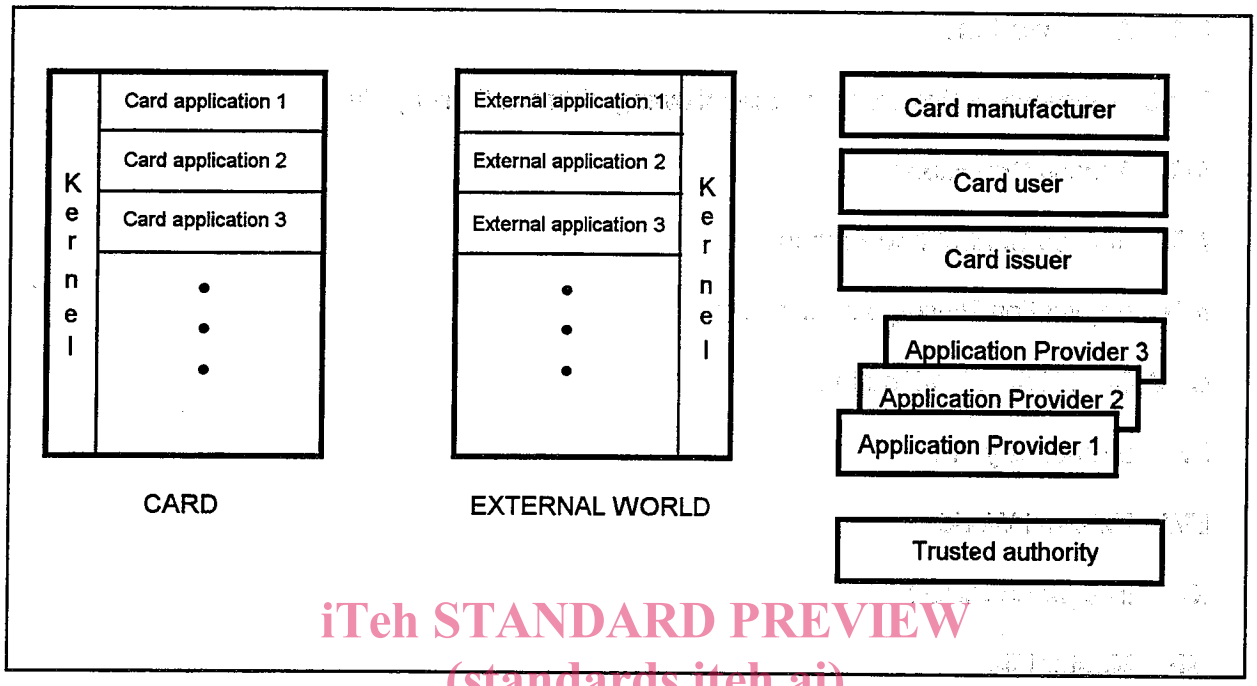

Figure 1: Reference model

The following entities are used in figure 1 to describe the reference model:

- the card, which consists of a kernel and one or several card applications (card application 1, card application 2, card application 3...);

- the external world, which may be either an on-line or an off-line system (see EN 726-1). The external world also consists of a kernel and one or several external applications (external application 1, external application 2, external application 3...). In this context, the kernel of the external world has the task e.g. to manage the transmission from and to the card and to support application independent actions. Security functionalities of the external world may reside in the security module(s);

- the card manufacturer (in this model, it means both the chip- and card manufacturer);

- the card-user;

- the card issuer, who can be the same as the application provider;

- one or several application providers;

- optionally, a trusted authority

5 General security approach

This clause describes the general approach for establishing security in an environment in which the card and card terminal are used.

5.1 Methodology

The methodology consists of three steps (see ISO 7498-2). In the first step requirements are formulated that shall be fulfilled by the system in order to operate in a secure way. In the next step security services are identified that can enforce each requirement. Finally the security mechanisms shall be specified which realize the security services identified in the previous step.

5.2 Identifying security requirements

In order to identify all the security requirements related to card and card-terminal, which shall be fulfilled by the system in order to operate in a secure way, 5 different phases in the card lifecycle are distinguished (see ISO 10202-1). Each of these phases is described by the activities taking place during that phase.

NOTE: During the lifecycle of the card, phases can occur more than once for each card.

5.2.1 Manufacturing of IC and IC card (phase 1)

Phase 1 is characterized by:

- the IC (Integrated circuit) semi-conductor design and the software development of the operating system;

- the transport of the operating system to the IC-manufacturer;

- the IC semi-conductor manufacturing;

- the IC assembling and the transport of the IC to the card manufacturer;

- the IC embedding in the card, and the transport of the IC card to the card issuer.

5.2.2 Card preparation phase (phase 2)

Phase 2 is characterized by:

- the card personalisation: allocation and personalisation of the MF (Master File), the loading of the application independent data, functions and keys;

- the activation of the MF;

- the distribution of the cards to the application suppliers.

The card issuer shall be responsible for the card preparation phase.

5.2.3 Application preparation (phase 3)

Phase 3 is characterized by 5 subphases:

- the allocation of the applications, under the responsibility of the card issuer. This involves the allocation of memory areas in the IC data memory;

- the allocation of some keys for exclusive use in certain functions (application dependent);

- the personalisation of the applications. This process involves the loading of application related keys and data in the allocated memory areas (including remote loading);

- the activation of an application;

- the transport of the IC card to the user.

The personalisation and the activation of applications are done under the responsibility of the application provider, who may be the card issuer.

5.2.4 Usage phase (phase 4)

Phase 4 is characterized by:

- the use of the general card functions to access to the applications. During this use, the card is under the control of the card user;

- deactivation and reactivation of an application, under the control of the application provider;

- deactivation and reactivation of the files at the MF-level, under the control of the card issuer;

- changing the key-version for an application, under the responsibility of the application provider;

- changing the key-version at the MF level, under the control of the card issuer.

5.2.5 Termination of use (phase 5)

Phase 5 is characterized by:

- the termination of a card application, under the responsibility of the application provider. A terminated application cannot be reactivated anymore;

- the termination of the use of the whole card, under the responsibility of the card issuer.

5.3 General security services

This subclause describes all possible security services the IC card can offer.

Only technical security services relevant to the IC card and the external world are described here. Organizational/procedural security measures and other methods necessary to fulfil the security principles are out of the scope of this standard.

5.3.1 Access control service

The access control service provides protection against unauthorized operations on information or processes in the card.

The protection is provided for operations such as: reading, writing, deletion, creation and execution.

5.3.2 Authentication service

The following authentication services are distinguished:

(a) Data origin authentication, providing corroboration that the identity of the source of data received is as claimed:

1) the card provides the proof that it is the origin of the data send;

2) the card authenticates the origin of the received data.

(b) Party to party authentication, providing corroboration that the identity of a party in an association is as claimed:

1) card application to card user authentication (e.g. name or logo);

2) card user to card authentication;

3) card user to external world authentication via the card;

4) card application to external world authentication and kernel to external world authentication;

5) external world to card authentication;

6) card application to card application authentication. (between two applications in the same card via the external world).

5.3.3 Confidentiality service

The confidentiality service provides protection against unauthorized availability or disclosure of information.

The following confidentiality services are distinguished:

(a) data in transfer, i.e. data sent to and from the card;

(b) stored data, i.e. data stored in the card.

This data can be:

- user data;

- protocol control information (PCI) e.g. commands, addresses.

5.3.4 Integrity service