ETSI TECHNICAL REPORT

ETR 115

January 1994

Second Edition

Source: ETSI TC-TE

Reference: DTR/TE-09002

ICS: 33.020, 33.040.40

Key words: TE, IC card

Terminal Equipment (TE); General concerns for the parties involved during the telecommunication integrated circuit card life cycle

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 92 94 42 00 - Fax: +33 93 65 47 16

Copyright Notification: No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 1994. All rights reserved.

New presentation - see History box

Whilst every care has been taken in the preparation and publication of this document, errors in content, typographical or otherwise, may occur. If you have comments concerning its accuracy, please write to "ETSI Editing and Committee Support Dept." at the address shown on the title page.

Contents

Blank page

Foreword

This ETSI Technical Report (ETR) has been produced by the Terminal Equipment (TE) Technical Committee of the European Telecommunications Standards Institute (ETSI).

ETRs are informative documents resulting from ETSI studies which are not appropriate for European Telecommunication Standard (ETS) or Interim European Telecommunication Standard (I-ETS) status. An ETR may be used to publish material which is either of an informative nature, relating to the use or an application on ETS or I-ETS, or which is immature and not yet suitable for formal adoption as an ETS or I-ETS.

Blank page

1 Scope

This ETSI Technical Report (ETR) gives guidance to the various parties involved in the issuing of Integrated Circuit (IC) cards and applications using IC cards. It is aimed at executives as well as system designers. It concerns matters of so general a nature that they cannot be included in the actual standards:

- European Standards (ENs) concerning requirements for IC cards and terminals for telecommunication use;

- European Telecommunication Standards (ETSs) and ENs concerning telecommunication applications using IC cards.

This ETR is applicable to IC cards and terminals for telecommunication use.

2 References

For the purposes of this ETR, the following references apply:

[1] prEN 726-1: "Identification Card Systems - Telecommunication Integrated Circuit Cards and Terminals - Part 1: System overview".

[2] prEN 726-2: "Identification Card Systems - Telecommunication Integrated Circuit Cards and Terminals - Part 2: Security framework".

[3] prEN 726-3: "Identification Card Systems - Telecommunication Integrated Circuit Cards and Terminals - Part 3: Application independent card requirements".

[4] prEN 726-4: "Identification Card Systems - Telecommunication Integrated Circuit Cards and Terminals - Part 4: Application independent card related terminal requirements".

[5] prEN 726-5: "Identification Card Systems - Telecommunication Integrated Circuit Cards and Terminals - Part 5: Payment methods".

[6] prEN 726-6: "Identification Card Systems - Telecommunication Integrated Circuit Cards and Terminals - Part 6: Telecommunication features".

[7] prEN 726-7: "Identification Card Systems - Telecommunication Integrated Circuit Cards and Terminals - Part 7: Security Module".

[8] ISO 7812 (1987): "Identification cards - Numbering system and registration procedure for issuer identifiers".

[9] ISO/IEC 7816: "Identification cards - Integrated circuit(s) cards with contacts -

ISO/IEC 7816-3 (1989): Electronic signals and transmission protocols. (including amendment 1, (1992): (Clause 9, Protocol type T=1, asynchronous half duplex block transmission protocol),

ISO/IEC 7816-4 (1992): Inter industry commands for interchange (CD),

ISO/IEC 7816-5 (1993): Registration system for applications in IC cards."

3 Definitions and abbreviations

3.1 Definitions

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

ROM mask: The software that is coded in the corresponding microprocessor's assembly language that is implemented into the Read Only Memory (ROM) of the silicon-chip at a very early stage of its manufacturing phase.

EF_{DIR}: An elementary file, which contains a list of all, or part of, available applications in the card.

3.2 Abbreviations

For the purposes of this ETR, the following abbreviations apply:

CHV	Card Holder Verification information
EF	Elementary File
EN	European Standard (Norme Européene)
ETR	ETSI Technical Report
ETS	European Telecommunication Standard
ETSI	European Telecommunications Standards Institute
IC	Integrated Circuit
IC card	Integrated Circuit card
I-ETS	Interim European Telecommunication Standard
MF	Master File
PIN	Personal Identification Number
ROM	Read Only Memory
SM	Security Module
TE	Terminal Equipment

4 Card and card life cycle

Five different phases in the card life cycle are distinguished:

- IC- and card-manufacturing phase (phase 1);
- card preparation (issuing) phase (phase 2);
- application preparation (phase 3);
- usage phase (phase 4);
- termination of use (phase 5).

Each of these phases is described by the activities taking place during that phase. The phases are described in the following subclauses.

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

4.1 IC- and card- manufacturing phase (phase 1)

Phase 1 is characterized by:

- the development of the operating system, and the transport of the operating system to the IC manufacturer;
- the implementation of the operating system;
- the production of the IC, and the transport of the IC to the card manufacturer;
- the production of the card, and the transport to the card issuer.

4.2 Card preparation (issuing) phase (phase 2)

Phase 2 is characterized by:

- the initialization and the pre-personalization of the card, the loading of the application independent data, functions and keys;
- the distribution of the cards to the application provider.

4.3 Application preparation (phase 3)

Phase 3 is characterized by:

- the allocation of the applications;
- the personalization of the applications, including the (remote) loading of an application and its keys in the card;
- the activation of an application.

Furthermore, there may be the generation of the transport code for the transport of the card to the user.

4.4 Usage phase (phase 4)

Phase 4 is characterized by:

- the use of the general card functions;
- the access to the applications;
- the use of the application management functions, e.g. blocking and unblocking of applications.

4.5 Termination of use (phase 5)

Phase 5 is characterized by at least one of the following:

- the termination of a card application;
- the deletion of a card application;
- the termination of the use of the IC on the card.

5 Other hardware items than the user IC card to be considered

The following hardware items are involved:

- production equipment (not standardized);
- personalization equipment (not standardized);
- card terminal;
- security module;
- network;
- other system components.

In figures 1 and 2, an overview of the card and its environment is shown. The fine lines indicate which items are covered by the different parts of prEN 726 [1] to [7].

NOTE 1: Figures 1 and 2 do not cover all the possible cases. For example, the "card-terminal-network-terminal-card" scenario is not shown in these figures.

NOTE 2: In figures 1 and 2, the security module can be placed anywhere in the system, depending upon the application.

Figure 1 shows an application working in an off-line system. The external world consists of a terminal.

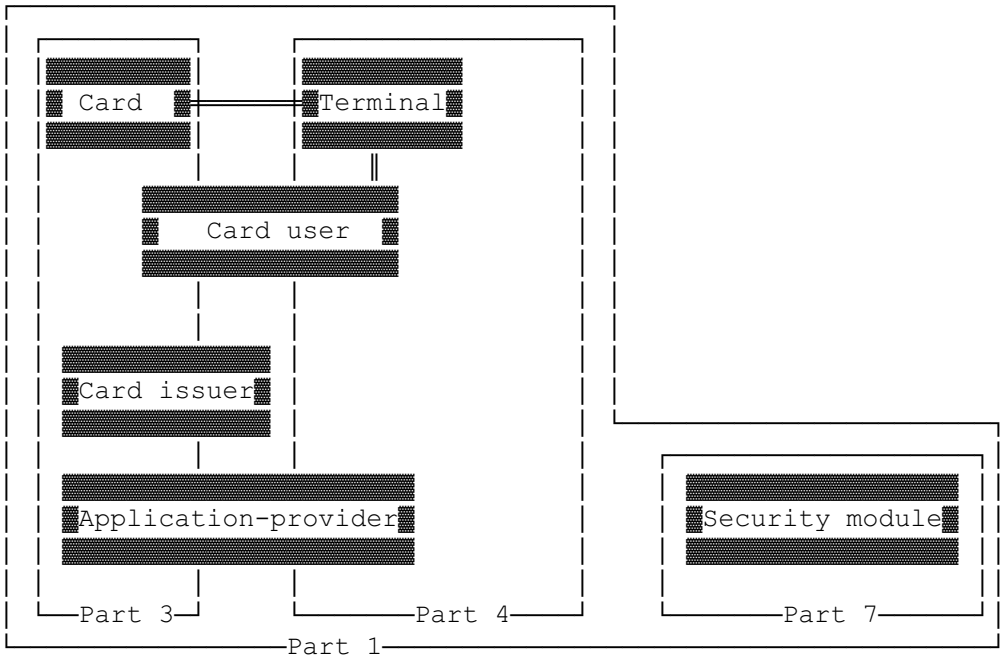
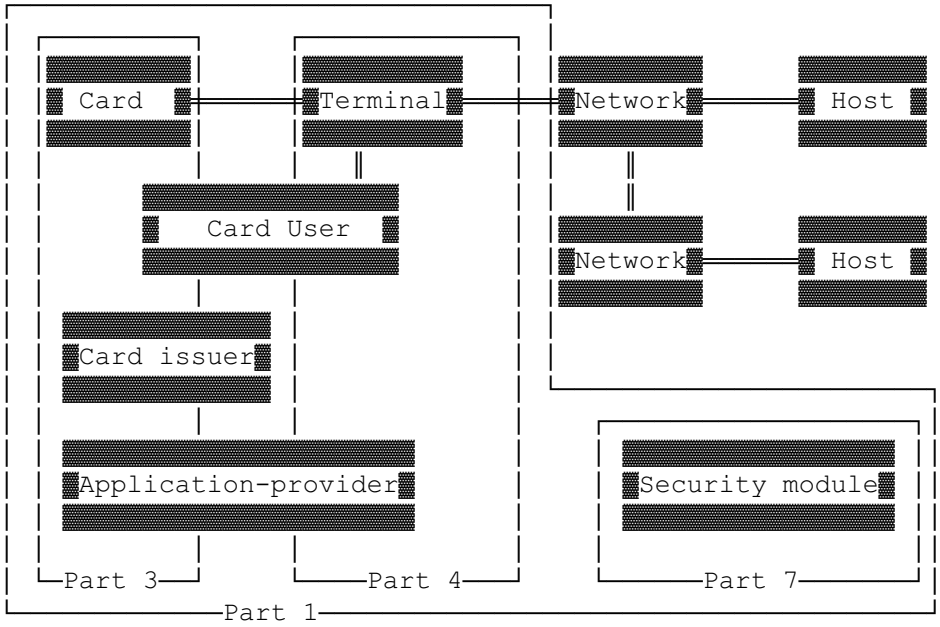


Figure 1: An application working in an off-line system

Figure 2 shows an application working in an on-line system. The external world can consist of a terminal, the network and a host.



NOTE: During the life cycle of a multi-application card, both the on-line and the off-line case can occur. An application-provider can offer his applications both to be used with on-line or off-line systems, depending on choices (e.g., the network cost or the cost of having the terminal in a secured environment).

Figure 2: An application working in an on-line system

5.1 Production equipment

Equipment for production of ICs and IC cards is company dependent.

Figure 3 gives an overview of the processes involved in the production of an IC card.

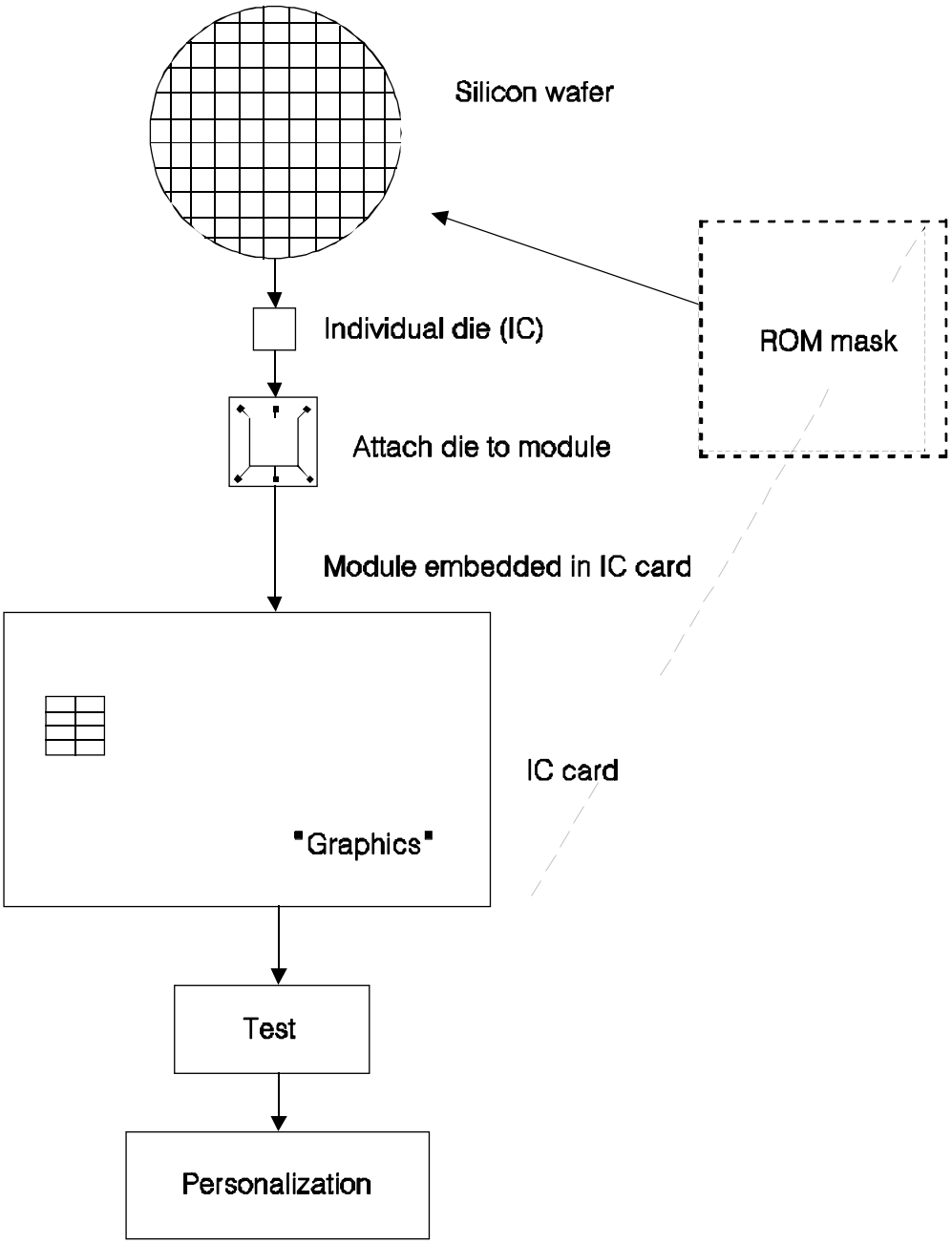


Figure 3: Processes involved in the production of an IC card

5.2 Personalization equipment

Equipment which adds card specific and customer specific data (could also include application specific data). The equipment that carries out this process is volume and company dependent.

5.3 Card terminal

A device which, besides the telecommunication application support, is typically designed to allow IC card insertion, providing physical voltage and signal supply for the IC card, and communication protocol support. Optionally, other user interfaces may be found such as display, keyboard, etc. Transparent terminals provide the possibility to perform communication between the IC card and a connected host without application data modification (see prEN 726-4 [4]).

5.4 Security Module (SM)

A device which contains security functions allowing:

- the terminal to access protected parts of the user card;

- checking of the authenticity of the user card;

- optionally, the provision of a balance that can be increased and decreased in a secure way in the Security Module (SM) with a reverse operation in the user card;

- computation and verification of cryptograms.

When using IC cards there is generally a need for proving the authenticity of the user card and, in some cases, also for proving the authenticity of the system as seen by the user card. In the case of transactions there is also a need to store a balance in a secure way in the system as an intermediate storage until the balance is transferred to a management centre or clearing centre. The fulfilment of these functions requires a secure environment, since it involves the use of secret keys, algorithms and secure storage locations. These requirements can be solved by a SM. The SM needs, therefore, to be logically and physically protected against attacks to expose or abuse secrets.

Four different positions of the SM in the system have been identified. The four positions are indicated in figures 4 to 7. The physical appearance of the SM may vary depending on its location in the system and the requirements (e.g. number of terminals to be handled by the SM). It may have the form of an IC card. The application provider is responsible for the SM. If more than one application provider agree to share a SM, special care needs to be taken to prevent unwanted interference between the applications and disclosure of the individual secrets.

Special precautions need to be taken during all phases of the lifetime of a security module as it contains secrets necessary to run the application. Special care is to be taken during phases 1, 2 and 3 where the SM is most vulnerable.

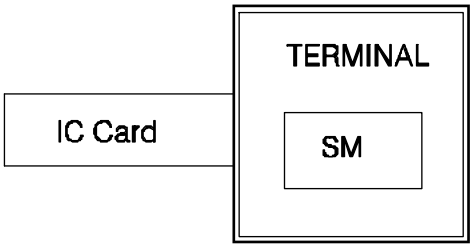


Figure 4: SM included in the terminal

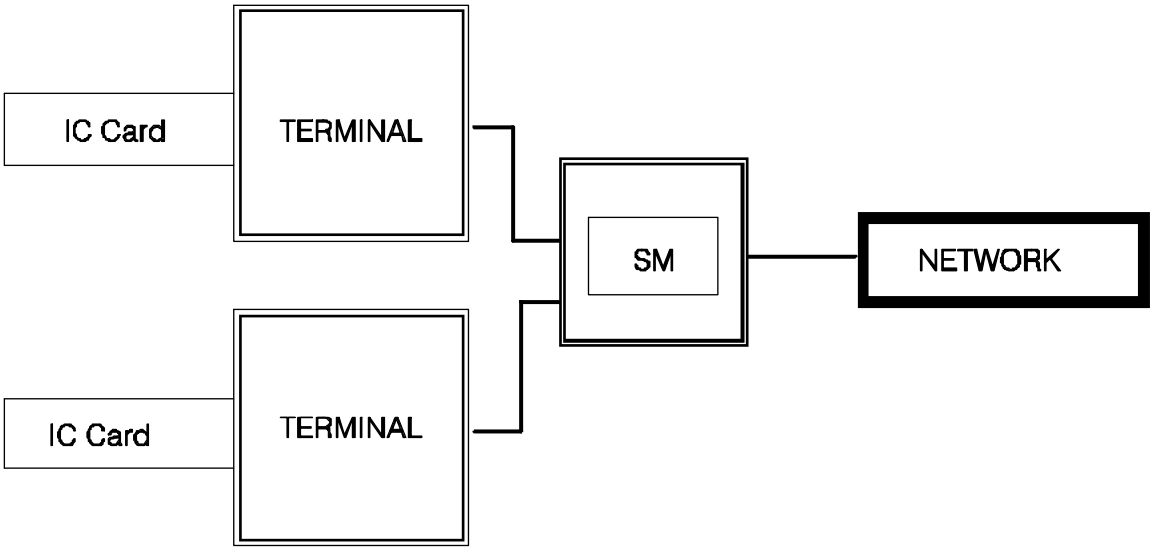


Figure 5: SM included in a local concentrator

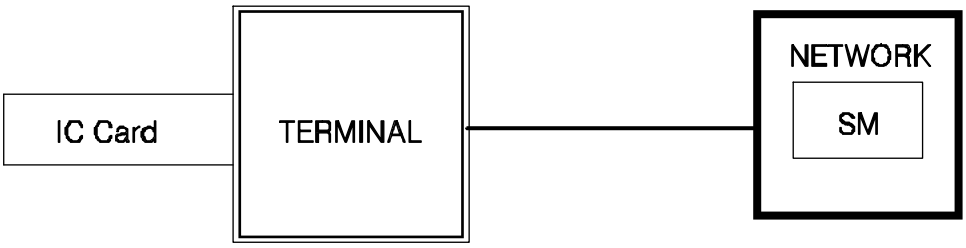


Figure 6: SM in the network

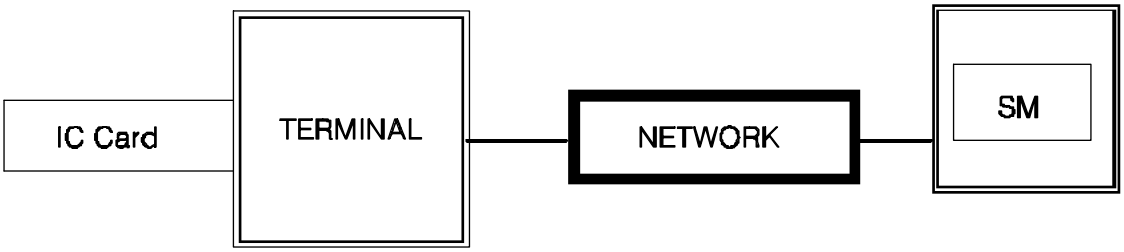


Figure 7: Remote SM

5.5 Network

The telecommunication network and/or other networks (e.g. for management purposes) are used to link card terminals with the remaining part of the system necessary to operate the application(s).

5.6 Other system components (PCs, Host, etc.)

The system necessary to operate an application consists of the user card, the card terminal and one or more components placed either as part of the telecommunication network or outside the network. The components will usually be computers (e.g. Personal Computers (PCs)) with the task of controlling and/or co-ordinating the use of the application. The communication between the terminal and the other system components is usually provided by means of telecommunication links (see figure 2).

6 Parties involved

The following parties are involved:

- ROM Mask provider;
- chip manufacturer;
- chip embedder;
- personalization agency;
- application provider;
- application loader;
- card issuer;
- service provider;
- clearing centre;
- card user;
- trusted authority;
- conformance testing agency.

One organisation may perform the tasks of several of the parties involved.

This is not intended to be an exhaustive list of all the involved parties.

Table 1: Participation of involved parties in different card phases

Parties involved	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5
ROM Mask Provider	X				
Chip Manufacturer	X				
Chip Embedder	X	X			
Personalization Agency		X	X		
Application Provider			X	X	X
Application Loader			X		X
Card Issuer		X	X	X	X
Service Provider				X	
Clearing Centre				X	X
Card User				X	X
Trusted Authority	X	X	X		
Conformance Testing Agency	X	X	X		

Table 2: Relationships between different hardware items and the involved parties

	Production Equipment	Personalization Equipment	Card Terminal	Security Module and user card	Network	Other system components
ROM Mask Provider				NOTE 1 (X)		
Chip Manufacturer	X			NOTE 1 (X)		
Chip Embedder	X			NOTE 1 (X)		
Personalization Agency		X		NOTE 1 (X)		
Application Provider		X	X	X	X	X
Application Loader		X	X	X	X	X
Card issuer			X	X	X	
Service Provider			X		X	X
Clearing Centre					X	X
Card User			X	NOTE 2 (X)		
Trusted Authority		X		X		
Conformance Testing Agency	NOTE 3 (X)	NOTE 3 (X)	X	X	NOTE 3 (X)	NOTE 3 (X)

NOTE 1: Only applicable to the SM if it is an IC card.

NOTE 2: Only applicable for the user card.

NOTE 3: IC card standards are not applicable as a reference for conformance testing.

6.1 ROM Mask Provider

The task of the ROM Mask Provider is to create the code to be inserted in the ROM mask.

The code provided consists of an operating system including memory management functions, necessary security facilities and data structures and a communication handler for the card interface with the outside world. The capabilities of the card depend upon these items.

6.1.1 Operating system

The operating system manages the operation of the processor and the memory in the card and supports the performance of the application(s).

The operating system performs in accordance with ISO/IEC 7816 Parts 3 and 4 [9] and prEN 726 Part 1 [1], Part 2 [2] and Part 3 [3].

The capabilities of the operating system should be indicated, e.g. by giving a profile type as specified in prEN 726-3 [3], subclause 10.4.

For some applications specific needs are to be met. The operating system may therefore need to be modified to get specific applications working in the card. On the one hand, the application supplier should try to use the facilities (subset or full set of features given in the above mentioned standards, maybe even expanded by further features) generally available in the operating system as much as possible, before asking for new features, on the other hand the producer of the operating system should make the operating system flexible enough so that new features are allowed to be implemented without too much trouble and thereby too high a price.

Provisions for algorithms and key management should be given. Multi-application cards need special considerations for the security issues.

For the memory management, the tree structure as described in prEN 726-3 [3] should be supported. This is particularly important if more than one application is likely to be implemented in the card. If more than one application may be considered active at the same time, logical channel support should be implemented.

Provision needs to be made for the use of storage areas outside the ROM area (e.g. EPROM and EEPROM) by the operating system for application specific commands, error correction and other functionalities that may need corrections and/or amendments.

Test methods need to be specified and the performance of such tests documented.

6.1.2 Communication handler

The communication handler takes care of the transmission of messages between the external world and the processor in the card (see prEN 726-3 [3]). The messages can be either messages concerning the transmission, application messages or messages for the operating system. The communication protocols need to be in accordance with prEN 726-3 [3] and ISO/IEC 7816-3 [9].

6.2 Chip manufacturer

The chip manufacturer produces the Integrated Circuit (IC) that will later be embedded in the IC card and loads the ROM mask code into the ROM.

It is important to design the IC in such a way that access to secret information stored in the IC and processed by the processor is not feasible by external means such as an electron microscope or subjecting the IC to conditions outside its normal operating state.

For security reasons procedures should be established for providing a complete logging of all the ICs produced. The logging should include the individual IC numbers and the transport keys given to the ICs by the chip manufacturer. All ICs should be stored under proper secure conditions.

Special test facilities built into the ICs should be protected to prevent misuse.

Programming aids for the ROM mask provider should be provided.

A well defined specification of the ICs capabilities (e.g. the processor) should be available.

Test methods should be specified and the performance of such tests documented.

Rejected ICs need to be destroyed in a secure manner.

6.3 Chip embedder

The chip embedder integrates the IC into a card body thereby producing the IC card.

The chip embedder should keep a log of all received ICs and all produced IC cards for security reasons and store all ICs and IC cards under proper secure conditions.

The chip embedder should provide information about printing capabilities, tolerances, choices of colours and durability of the printing.

Test methods should be specified and the performance of such tests documented.

Rejected cards need to be destroyed in a secure manner.

6.4 Personalization agency

This agency personalizes the IC cards on behalf of the card issuer and prepares the cards for actual use. In the personalization process the IC cards are loaded with the information necessary for using the card, e.g. card number, card profile, keys, PINs, expiry date and card holder name (see prEN 726-3 [3]). Applications may also be loaded if a business agreement is made to do so.

For security reasons the personalization agency should keep a log of all received and personalized IC cards and should store all IC cards under proper secure conditions. In order to comply with national data protection acts the same applies for any information on card user, etc., that is used in the personalization process.

If a directory (EF_{DIR}) is generated, it needs to be in conformance with ISO/IEC 7816-5 [9].

If additional printing and or embossing of the card is to be applied, it should usually be carried out by the personalization agency.

6.5 Application provider

The application provider offers applications in which the card is used and where a part of the application is placed in the IC card either as a data file, as an executable file or as a combination thereof.

The application provider provides the whole application, not only the part placed in the IC card.

If special needs are relevant, e.g. for the network, agreements need to be made.

The application provider proves through the use of a trusted party, that the application can coexist in the relevant IC cards without influencing the operating system or other applications that may exist in the IC card. An application should not influence or compromise any other application or file in the IC card. However, if a business agreement exists it may be possible for applications to use the facilities offered by other applications in the same IC card.

For cost reasons the general features of an IC card should be examined and used in preference to special features. The latter will complicate the card, add to the price and limit the possibilities of adding applications to a general multi-application card.

The application needs to be easily recognisable by the use of the ISO registration scheme given in ISO/IEC 7816-5 [9].

The opening, termination and blacklisting of use of a card for a specific application needs to be considered (see prEN 726-3 [3]).

The legal aspects of responsibility for the application should be considered and it should be emphasized that several parties may be involved in the full implementation of an application.

6.6 Application loader

An application loader places the application in the IC card and provides for its use in the system. The application loader acts under the responsibility of the card issuer.

The application loader ensures availability of the application in terminals and/or system.

The application needs to be loaded by the use of keys provided by the card issuer. The application loader reports to the card issuer on cards loaded, according to an agreement between the card issuer and the application loader.

Special security conditions should be fulfilled by the application loader and agreed upon by the card issuer.

Downloading of applications to an IC card through a network should be done in a secure way that needs to be negotiated with the card issuer and maybe also other parties involved.

6.7 Card issuer

The card issuer is responsible for the IC card. The card issuer needs to be recognisable both visually on the front or back of the IC card and electrically in the IC at the Master File (MF) level. The identification of the card issuer shall be in accordance with ISO 7812 [8] and ISO/IEC 7816-6 [9].

The physical appearance of the IC card, the printing, advertising, etc. on the IC card is the responsibility of the card issuer.

The card issuer should guarantee that there is no influence from one application to the other or on the operating system. Only where business agreements exist, will one application be able to communicate with and influence on another application.

The opening, terminating and blacklisting of cards needs to be considered.

The card issuer may delegate responsibility to an application loader for the loading of applications on his behalf and for ensuring that the applications are supported by terminals and system.

6.8 Service provider

The service provider should have a business agreement with the application provider(s) in order to be able to offer the service.

The service provider should make terminal(s)/system access available in order to provide the service.

The service provider needs to train his staff in how to provide the service.

6.9 Clearing centre

Where payment is involved in an application, settlement of the payment will have to take place between the service provider and the application provider. This is usually done by means of a clearing centre.

The legal responsibilities of the clearing centre should be determined.

The security aspects for the clearing centre should be determined.

The availability of access to the clearing centre should be determined (up-time/down-time).

6.10 Card user

The card user receives his/her card from the card issuer or a company to which the card issuer has delegated the responsibility for issue of the card. Agreements between the card user and the application providers should be established.

The card user should be informed by the card issuer on legal rights and responsibilities.

The card user should be informed on how to use the card and the applications available on the card. This includes the use of Personal Identification Numbers (PINs), Card Holder Verification (CHV) information and the possibility of changing PINs.

The card user should be informed on how to handle the card (bending, temperature exposure, etc.).

Potential card users should be informed properly of possibilities and responsibilities before they apply for a card.

6.11 Trusted authority

An independent body having the task of administering security issues such as key distribution and management in a secure way.

6.12 Conformance Testing Agency

A test house having the authority to perform conformance testing on different parts of the system (hardware and/or software) according to an agreed test plan.

7 Patents, legal rights, etc.

It is important to investigate the influence of taken or pending patents on any hardware, software, algorithms etc. involved in a system as early as possible in the planning phase.

The need for auditability of a system should be considered.

Responsibility should be established for every step of a project and responsibilities determined for all participating parties.

Legal rights should be considered as well as national regulations. Please note that rights and rules may be different from country to country. Prediction of how the regulations apply to cryptography may be difficult.

8 Security aspects

The security aspects need to be considered from several points of view. The parties involved, the card life cycle, supporting systems and administrative routines need to be considered. The security requirements are often different for different applications.

It is recommended that a security analysis be made for every application. It is important to decide whether the specified security functions in the standards are sufficient or if additional measures need to be taken.

The specified security functions in the standards should normally be accompanied by appropriate administrative routines. Sloppy or missing administrative routines can make it possible to bypass the security functions in the card.

Special attention should be paid to the key management, since e.g. the authentication procedures rely on a sound key management.

It is important to agree upon areas of responsibility between the parties involved, especially if several service providers are allowed to install their applications in a multi-application card.

History

Document history	
December 1993	First Edition
January 1994	Second Edition
March 1996	Converted into Adobe Acrobat Portable Document Format (PDF)