TS 101 206-4 V1.2.1 (1998-01)

Technical Specification

Identification card systems; Telecommunications IC cards and terminals; Part 4: Application independent card related terminal requirements

European Telecommunications Standards Institute

Reference
RTS/PTS-00011 (b6100ior.PDF)

Keywords
Card

ETSI Secretariat

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

X.400
c= fr; a=atlas; p=etsi; s=secretariat

Internet
secretariat@etsi.fr
http://www.etsi.fr

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETR 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.fr/ipr).

Pursuant to the ETSI Interim IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETR 314 (or the updates on http://www.etsi.fr/ipr) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Project Pay Terminals and Systems (PTS).

TS 101 206-4 version 1.1.1 is the handover version to CEN for becoming EN 726-4.

TS 101 206-3, 4 and 7 version 1.2.1 represent an update of the documents handed over to CEN for becoming EN 726-3, 4, and 7. PTS has used version 1.2.1 rather than the handover version to CEN (version 1.1.1) for producing the conformance testing specification for EN 726-3, 4 and 7.

ETSI has produced a set of TSs which are not a copy of any CEN published EN. The TSs are complete and consistent documents with references among themselves. It has been made clear in these TSs that they are contributions to the CEN work for publication as EN (after re-editing the references). Once published by CEN as EN, ETSI will withdraw its TSs.

History of EN 726

EN 726 was prepared by ETSI STC TE9, adopted by CEN/TC 224 and submitted to the CEN formal vote.

EN 726 consists of seven parts covering Identification card systems; Telecommunications IC cards and terminals; as identified below:

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".

Overview of ETSI deliverables on EN 726 family

TS 101 206-1	"Identification card systems; Telecommunications IC cards and terminals; Part 1: System overview".
TS 101 206-3	"Identification card systems; Telecommunications IC cards and terminals; Part 3: Application independent card requirements".
TS 101 206-4	**"Identification card systems; Telecommunications IC cards and terminals; Part 4: Application independent card related terminal requirements".**
TS 101 206-7	"Identification card systems; Telecommunications IC cards and terminals; Part 7: Security module".

Overview of ETSI deliverables on EN 726 conformance testing family

TS 101 203-1/2/3	"Identification card systems; Telecommunications IC cards and terminals; Test methods and conformance testing for EN 726-3".

TS 101 204-1/2/3	"Identification card systems; Telecommunications IC cards and terminals; Test methods and conformance testing for EN 726-4".
TS 101 207-1/2/3	"Identification card systems; Telecommunications IC cards and terminals; Test methods and conformance testing for EN 726-7".

1 Scope

The present document specifies the application independent card related characteristics of card terminals able to process cards complying with TS 101 206-3 [1]. All common characteristics which are necessary for a standardized card use in the terminals are defined. The present document does not preclude letting terminals accept and process cards complying with other standards.

The application-specific characteristics are not defined in the present document. They are defined and described in the relevant application requirements.

The present document does not specify any internal realization of a card-terminal. It describes:

a) the requirements for the physical and environmental specifications on the card terminal, the electronic signals and transmission protocols;

b) the application independent logical model, which should be used as a basic design of the logical structure of card specific requirements supported by the terminal;

c) the description of the application independent functions and general scenarios to be used by most of the applications;

d) the error handling.

2 References

References may be made to:

a) specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or

b) all versions up to and including the identified version (identified by "up to and including" before the version identity); or

c) all versions subsequent to and including the identified version (identified by "onwards" following the version identity); or

d) publications without mention of a specific version, in which case the latest version applies.

A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] TS 101 206-3: "Identification card systems; Telecommunications IC cards and terminals; Part 3: Application independent card requirements".

[2] TS 101 206-7: "Identification card systems; Telecommunications IC cards and terminals; Part 7: Security module".

[3] EN 27816-1 (1989): "Identification cards - Integrated circuit(s) with cards contacts - Part 1 : Physical characteristics".

[4] EN 27816-2 (1989): "Identification cards - Integrated circuit(s) cards with contacts - Part 2 : Dimentions and location of the contacts".

[5] EN 27816-3 (1989): "Identification cards - Integrated circuit(s) cards with contacts - Part 3 : Electronic signals and transmission protocols".

[6] EN 27816-3 (1992/A1:1993) and ISO/IEC 7816-3 (1989/AM 1:1992): "Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols - Amendement 1: Protocol type T=1, asynchronous half duplex block transmission protocol".

[7] ISO/IEC 646 (1991): "Information technology - ISO 7-bit coded character set for information interchange".

[8] CCITT Recommendation T.50 (1988): "International alphabet n°5".

3 Definitions, abbreviations, symbols

3.1 Definitions

For the purposes of the present document, the following definitions apply:

Access Conditions (AC): A set of security attributes associated to a file.

Elementary File (EF): A file containing AC, data or program. It can not be the parent of another file.

EF_{CHV} is an elementary file containing the CardHolder Verification (CHV) information.

EF_{DIR} is an elementary file at the MF or at DF level, which contains a list of all, or part of, available applications in the card (see also ISO 7816-5).

EF_{ID} is an elementary file at the MF level, containing the identification number of the card.

EF_{IC} is an elementary file at the MF level, containing general information concerning the Integrated Circuit (IC).

EF_{KEY} is an elementary file containing keys linked to the AC.

InterFace Device (IFD): A terminal, communication device or machine to which the IC card is electrically connected during a session.

Master File (MF): The mandatory unique file representing the root of the file structure and containing AC and allocable memory. It may be the parent of elementary files and/or dedicated files.

nibble: Half a byte. The most significant nibble of a byte consists of bits $b_8b_7b_6b_5$ and the least significant of bits $b_4b_3b_2b_1$.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AC	Access Condition
ATR	Answer To Reset
BCD	Binary Coded Decimal
CEN	Comité Européen de Normalization
CHV	Card Holder Verification
EF	Elementary File
EN	European Norm
FFS	For Further Study
IC	Integrated Circuit
IFD	InterFace Device
ME	Mobile Equipment or portable battery operated equipment
MF	Master File
PIN	Personal Identification Number
SM	Security Module
STC	Technical Sub-Committee of ETSI
TC	Technical Committee
TE9	Terminal Equipment 9 (Technical Sub-Committee, STC, of ETSI)

3.3 Symbols

For the purposes of the present document, the following symbols apply:

N	Newton
V_{CC}	Supply Voltage
V_{PP}	Programming Voltage

4 Physical requirements for the card terminal

4.1 Mechanical interface between the IFD and the IC card

The mechanical interface between the Integrated Circuit card (IC card) and the InterFace Device (IFD) shall be in accordance with EN 27816-1 [3] and EN 27816-2 [4].

If the IFD accepts ID-1 cards with embossing, then the embossing shall be on the same side as the contacts. If the IFD supports IC cards combined with a magnetic stripe, the magnetic tracks shall always be on the opposite side of the contacts.

4.2 Contacting of the IC card

No short circuit or damage to the card or IFD shall take place when inserting or removing the card, even when it is pulled out with a speed < 1 m/s. Activation and deactivation of the contacts shall be in accordance with EN 27816-3 [5] and ISO/IEC 7816-3 [6].

No short circuit between any contacting elements in the terminal shall prevent normal operation of the terminal when removed.

The shape and the material of the contacting elements shall be such that no damage to the card is caused by them when applied to it.

The contact force of the contacting elements shall be large enough to ensure contact, even in extreme environmental conditions (e.g. shocks or vibrations) which can be application dependent.

However, under no circumstances shall the contact force be greater than 0,5 N per contact.

The shape of the contacts and the way of contacting shall be done in such a way that even polluted cards are contacted properly.

4.3 User/terminal interface

The method of inserting the card shall be by the short side first, where the contacts are situated, preferably with the contacts upwards. Therefore, for public terminals, a clear and unambiguous indication shall be given to the user to indicate the correct orientation for inserting the card.

The card shall always be accessible to the user.

Physical removal of the card at any time however, shall not leave the applications in the terminal in an invalid or unknown logical state.

NOTE: During write operations on the card, especially in the case of management operations, a clear indication shall be given to the user, not to remove his card from the terminal.

4.4 Magnetic stripe card reader

A combination with a magnetic stripe card reader function is optional.

4.5 Card Holder Verification (CHV) module

If required, a CHV module can be integrated in the terminal. This module shall allow the user to proof his/her identity by entering his/her CHV number and/or biometric information.

In case of a CHV-entry, the CHV may be entered on the keypad/keyboard of the card terminal or by means of a separate and secure PIN-pad.

Depending on the application, the CHV-entry may be numerical or alphanumeric. For telecommunication applications the CHV-data shall be coded in accordance with CCITT Recommendation T.50 [8] or ISO/IEC 646 [7]. If alphanumeric CHV-entry has to be performed, only terminals with a keyboard shall be used. In case of numerical CHV-entry, both keyboard and keypad (up to 12 numerical push buttons) can be used.

For public terminals the terminal shall be designed so that CHV entry cannot be easily observed.

The plain text CHV shall never leave the terminal, except when it is presented to the card.

4.6 Acceptance of memory cards

Terminals accepting memory cards are not excluded by the present document.

5 Electronic signals and transmission protocols

The electronic signals and asynchronous transmission protocols between the IFD and the IC card shall be in accordance with EN 27816-3 [6] and ISO/IEC 7816-3 [6]. IC cards conforming to the present document shall not be damaged.

The following, additional, requirements shall be applied in order to have simplified terminals and to ensure a proper operation in mobile equipment or portable battery operated equipment (ME) except for the supply current which is to be used in stationary equipment as well.

5.1 Supported transmission types

For the IFD, two types of transmission shall be considered:

a) the asynchronous transmission, used by the IC cards, with the possibility of having cards;

b) with an internal or external clock;

c) the synchronous transmission used by the memory cards.

Therefore, the IFD shall support the different types of reset behaviour for the cards using asynchronous transmission (see EN 27816-3 [5] clause 5 and subclause 6.1).

The IFD may support the reset procedure for the cards using synchronous transmission (see EN 27816-3 [5] clause 5 and subclause 6.2). If the IFD supports synchronous cards, the conditions for an asynchronous IC card shall be applied first.

The terminal shall support at least one of the protocols described in EN 27816-3 [5].

5.2 Supply voltage V_{CC}

According to the value given in EN 27816-3 and ISO/IEC 7816-3 [6] except for mobile equipment where the supply voltage V_{CC} shall be 5 V ± 10%.

5.3 Supply current

The terminal shall be able to supply at least 20 mA to the IC card. In portable battery operated equipment, the supply current shall be at least 10 mA.

Due to technology, spikes in the supply current can occur, the amplitude of which can be several times the average current. The power supply shall be able to counteract spikes up to a maximum charge of 40 nAs with no more than 400 ns duration and an amplitude of at most 200 mA.

5.4 Programming voltage

For card terminals accepting European telecommunication cards, the V_{PP} contact shall supply the same voltage as the V_{CC} contact (see also TS 101 206-3 [1] subclause 5.3).

If the IFD also supports memory cards, then different values for the programming voltage, in accordance with EN 27816-3 and ISO/IEC 7816-3 [6], shall be allowed.

5.5 Duty cycle

According to the values given in EN 27816-3 and ISO/IEC 7816-3 [6] except for mobile equipment where the duty cycle for asynchronous transmissions shall be taken between 40 % and 60 % (see also TS 101 206-3 [1], subclause 5.4).

5.6 Guard time

According to the values given in EN 27816-3 and ISO/IEC 7816-3 [6], except for mobile equipment where the guard time shall be in accordance with the definitions for guard time in TS 101 206-3 [1], subclause 5.5.

6 Security facilities

The security facilities, from the terminal point of view, are completely based on the security facilities defined for the IC card. As defined in TS 101 206-3 [1], clause 7, for each possible action, there are Access Conditions (AC) defined in the IC card.

The only exception concerns the internal authentication feature, where the card has to prove its authenticity to the terminal. In this case, it shall be the terminal that decides.

NOTE: It is recognized that it could be necessary to encrypt not only the data, but also the header of a command or a part of it.

6.1 Security Module (SM)

Depending upon the security policy, defined for the complete card system and the various applications using it, there are two possibilities to fulfil these requirements. These are stated in subclauses 6.1.1 and 6.1.2 of the present document.

6.1.1 Using a SM in the terminal

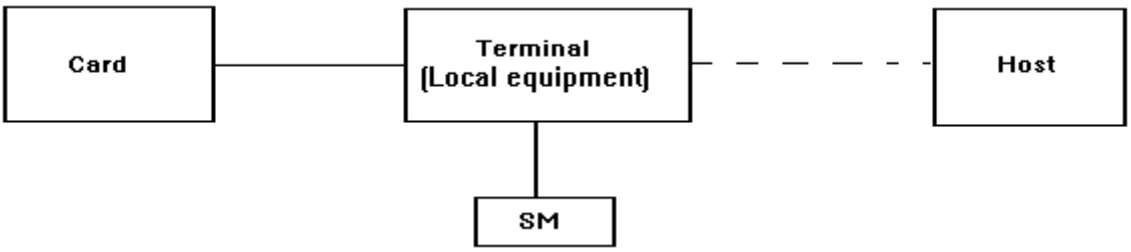


Figure 1: Off-line environment

The use of a SM, in the terminal or in the local equipment, may be necessary in an off-line environment (see figure 1) when secret key algorithms are used to fulfil the security policy. See TS 101 206-7 [2] for a description of the SM.

NOTE: Local equipment could be, for example a payphone connecting unit which is part of the subscriber line but which resides in the exchange which is a secure environment. The SM may therefore reside in the local equipment or in a remote location.

6.1.2 No SM in the terminal

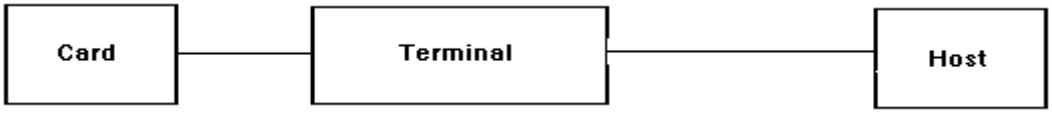


Figure 2: On-line environment

There is no need for a SM inside the terminal in a complete on-line environment (see figure 2).

7 Description of the functions

Refer to TS 101 206-3 [1] clause 8, for the description of the functions.

Not all the functions, possible in the IC card, need be supported in the terminal.

8 Commands

Refer to TS 101 206-3 [1] for the following items:

a) the mapping principles (subclause 9.1);

b) the coding of the commands for the byte protocol (T=0) or the block protocol (T=1) (subclause 9.2);

c) the Access Condition (AC) coding (subclause 9.5);

d) the coding of the contents of EF_{CHV} and EF_{KEY} (subclauses 10.1, 10.6 and 10.7);

e) the coding of the error conditions returned by the IC card (subclause 9.4).

Not all commands, possibly supported by the IC card, need be available in the terminal.

In all cases, the terminal-side of an application is the master in the IFD-IC card relation.

The terminal shall at minimum be able to distinguish between status responses from the card indicating successful and unsuccessful completion of the command. An unrecognized status response shall be treated as unsuccessful completion of the command.

9 Error handling

The error recovery procedures at the transport level, as stated in EN 27816-3 and ISO/IEC 7816-3 [6], shall be supported.

Unrecoverable errors should be signalled to the user. For terminals having alphanumeric displays, the error cause should be displayed in plain text (see table 1).

Table 1

Error conditions		Text displayed
SW1	**SW2**	
91	01	Card malfunction, contact application provider
98	08	Card blocked, contact application provider
98	04	Wrong CHV, X remaining attempts (note)
NOTE: When a wrong CHV was presented, displaying the remaining CHV-attempts should be optional. The remaining attempts shall be available after requesting the status of the corresponding EF_{CHV}.		

10 Functional requirements of the card terminal

10.1 Language for display messages

For public telecommunication terminals, at least 2 languages shall be supported, one of which should be English (for language selection, see subclause 10.3.5).

10.2 Display messages

There should be a set of basic messages, common to all public terminals, for user guidance. For example:

a) insert your card;

b) remove your card;

c) card refused (i.e. invalid, locked);

d) re-insert the card (i.e. after a recovered malfunction);

e) enter your Card Holder Verification number (CHV);

f) wrong Card Holder Verification number (CHV);

g) enter your old Card Holder Verification number (CHV);

h) re-enter Card Holder Verification number (CHV);

i) service locked;

j) service not available;

k) terminal out of service.

The user shall have the possibility to suppress the displaying of user related data.

10.3 Basic operations

10.3.1 Removal of the card

When the card is removed, all data related to the card within the terminal shall be erased, except for the data relevant to the transaction record in the terminal.

10.3.2 Escape possibility

At any time, the user at the terminal shall have the possibility to abort the current operation. The terminal shall reject the card and return to the idle state.

10.3.3 CHV-entry

During the entering of the CHV (between 4 and 8 characters), an indication of the number of characters entered should be visualized. However, the values of the entered CHV shall not be displayed in plain text nor be disclosed by audible feedback.

The length of a CHV, presented to the IC card, shall be 8 bytes as defined in TS 101 206-3 [1], subclause 9.2.16. Therefore, an end-of-CHV character shall be entered by the user, to denote the end of the CHV-entry when the length of the entered CHV is shorter than 8 characters (for telecommunication terminals, this end-of-CHV character could be '#').

The terminal shall present the CHV in the requested format to the card:

a) 8-bytes long, containing the entered CHV;

b) left aligned;

c) padded at the right with binary 1.

Padded with binary 1 means that for the remaining bytes, or nibbles in case of a BCD-coded CHV, every bit shall be set to one.

When an enciphered CHV is required, the padding with binary 1, shall be done before the encipherment of the CHV.

For telecommunication applications, the CHV-data shall be coded in accordance with CCITT Recommendation T.50 [8] or ISO/IEC 646 [7], reserving 1 byte per CHV-character as in figure 3.

In all representations the leftmost bit represents the most significant bit while the rightmost bit represents the least significant bit of the least significant byte.

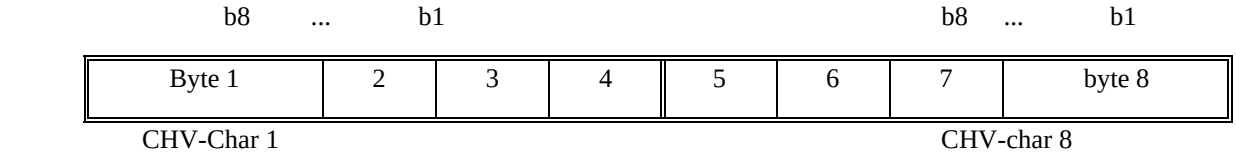


Figure 3: Coding in accordance with CCITT Recommendation T.50 [8]

For applications requiring a longer CHV, BCD coding is possible, reserving 1 nibble per CHV-character as in figure 4.

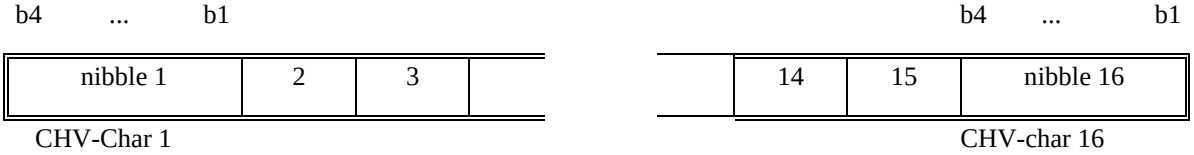


Figure 4: BCD coding

Care shall be taken to be consistent in using the right CHV-coding technique, once it is decided for a particular application which coding-technique shall be used.

A possible scenario for CHV-entry is given in annex A.

10.3.4 CHV-change

The user should be able to change his CHV only at those terminals that fulfil the requirements for CHV-entry and if those terminals support the CHV-change function.

To change the CHV, the old CHV should be entered first according to the procedure for CHV-entry (see subclause 10.3.3). Then, the new CHV shall be entered twice, also according the same procedure for CHV-entry. Only when the two entries of the new CHV match, shall the terminal activate the CHV-change in the card by sending the appropriate command to the card.

When there is a difference between the two new CHVs, the operation shall be aborted and the user shall be notified that the CHV-change operation was not successful. In this case, his old CHV shall still be valid.

A possible scenario for CHV-change is given in annex B.

NOTE: CHV-entry and CHV-change: in case of a mistyped digit/character, during the entering of the CHV, at least the escape possibility described in subclause 10.3.2 can be used. More convenient functions, i.e. editing, could be implemented.

10.3.5 Language choice/change

The order for language preferences may be indicated in the Master File (MF) of the IC card. After the Answer To Reset (ATR), the terminal shall read the MF and shall compare the list of language preferences from the IC card with the list of language preferences in the terminal. The language with the highest preference in the card and which is also available in the terminal, shall be chosen.

If there is no conformity in the list of language preferences from the terminal and the one from the IC card, or if there is no such list present in the MF of the IC card, then the language with the highest preference, as implemented in the terminal, shall be used.

However, the user should have the possibility to change the language used on the terminal, at least once at the beginning of the card session. For example by means of:

a) a special key;

b) a menu.

10.3.6 Selection of an application

In a mono-application terminal, the required application shall be selected automatically.

In a multi-application terminal, only the subset of the applications which are supported by both the terminal and the IC card, and which are not invalidated in the IC card, may be shown to the user. The possibility to show the complete directory may be supported by the terminal and should be preferred.

The procedure to present this list of applications, is to read out the elementary file EF_{DIR} at the MF level of the IC card. Out of the response of the card, only the verbal description (see TS 101 206-3 [1], subclause 6.3) of the relevant applications shall be displayed.

The selection of an application from this list by the user, can be done by a function key or by choosing from a menu. For the applications which do not appear in the EF_{DIR} at the MF level, it is up to the application part in the terminal to select the desired application in the card.

The card expiry date, given in the elementary file EF_{ID} at the MF level of the card, can be checked against the real time clock in the terminal/host.

10.4 Audio messages

The user guidance may be supported by audio messages.

At the end of the card session, the user should get an audio message, reminding the user to remove the card from the terminal.

Annex A (informative): A scenario for CHV-entry

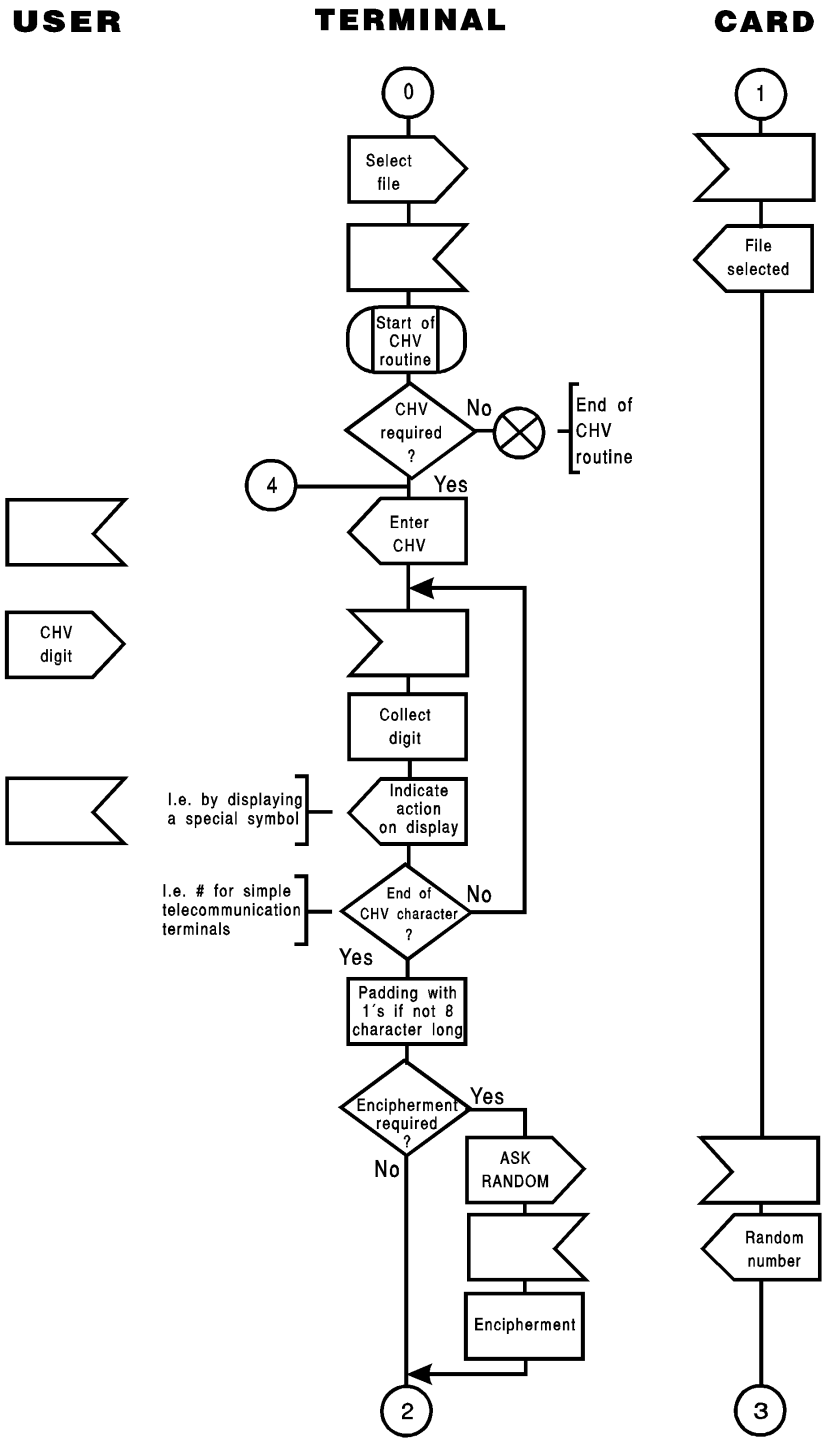
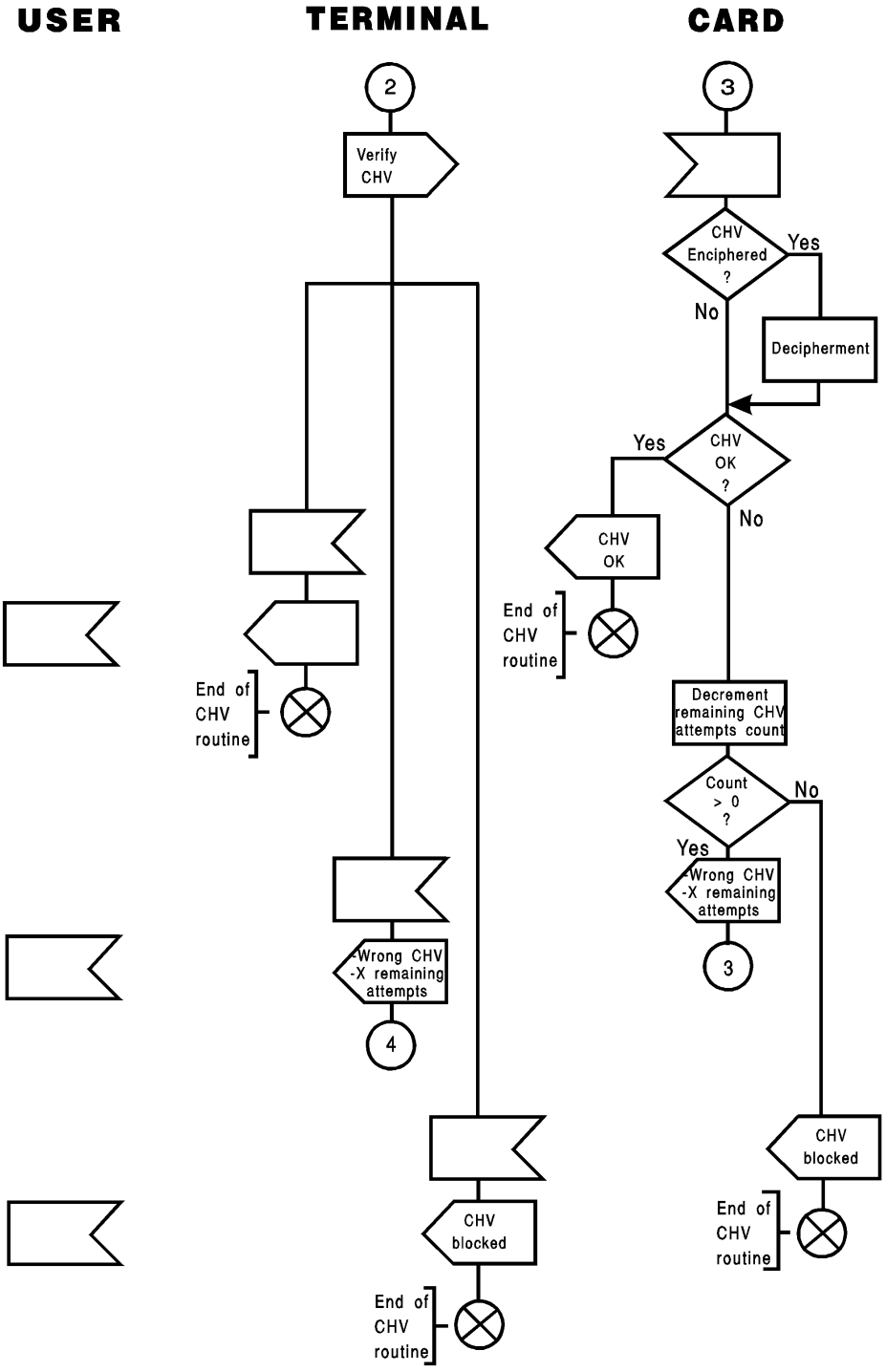


Figure A.1



NOTE: CHV required in the scenario means that the CHV-entry is needed and enabled (if this option is available).

Figure A.2

The scenario for the Enable/Disable CHV feature, is almost the same as the scenario for the CHV-entry, except that in the beginning of the scenario, a check shall be included to see whether enabling/disabling of the CHV is allowed.

Annex B (informative): A scenario for CHV-change

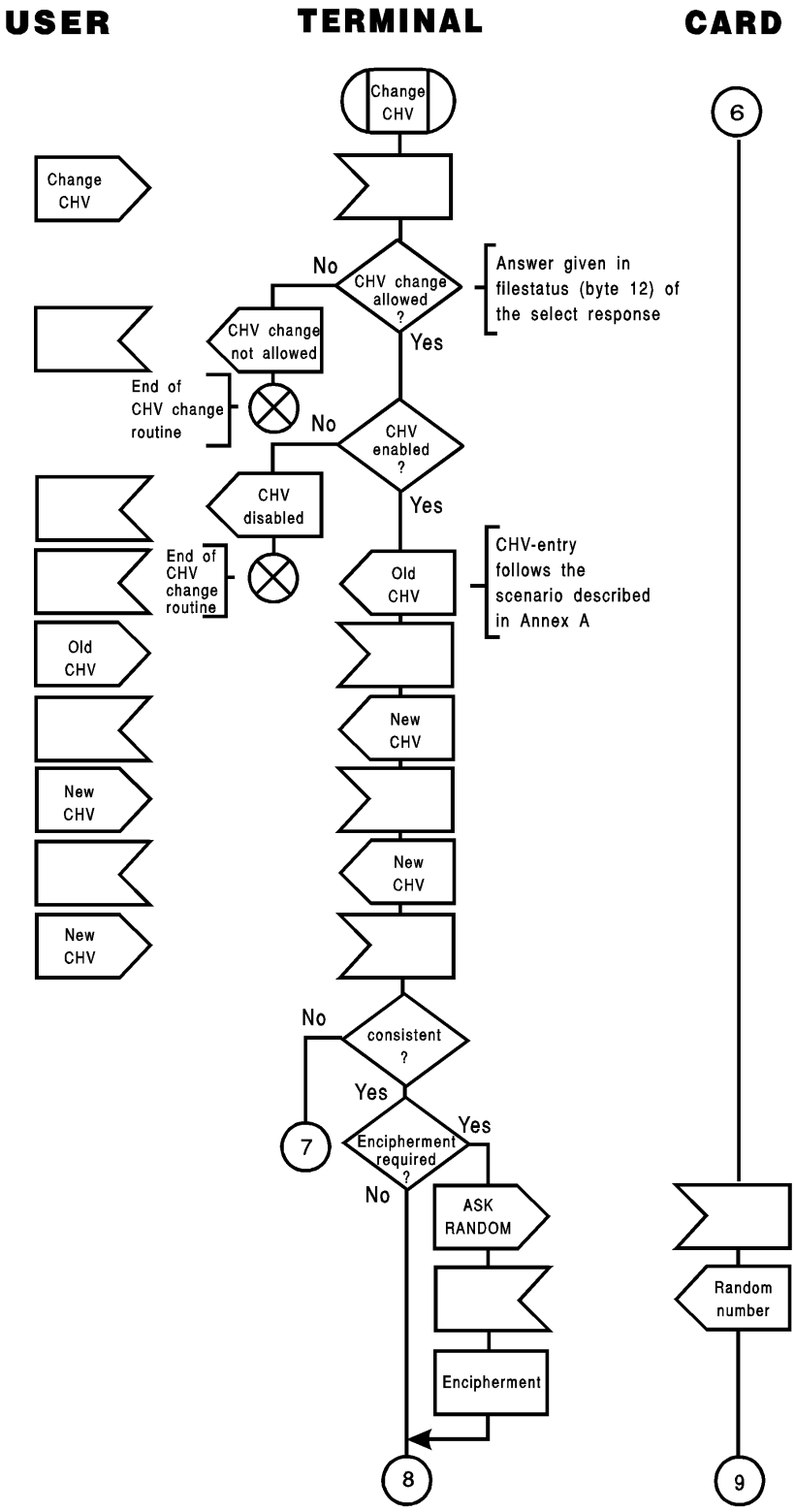


Figure B.1

History

Document history		
V1.1.1	August 1997	Identical with the document handed over to CEN. It was not published by ETSI.
V1.2.1	January 1998	Publication

ISBN 2-7437-1900-1
Dépôt légal : Janvier 1998