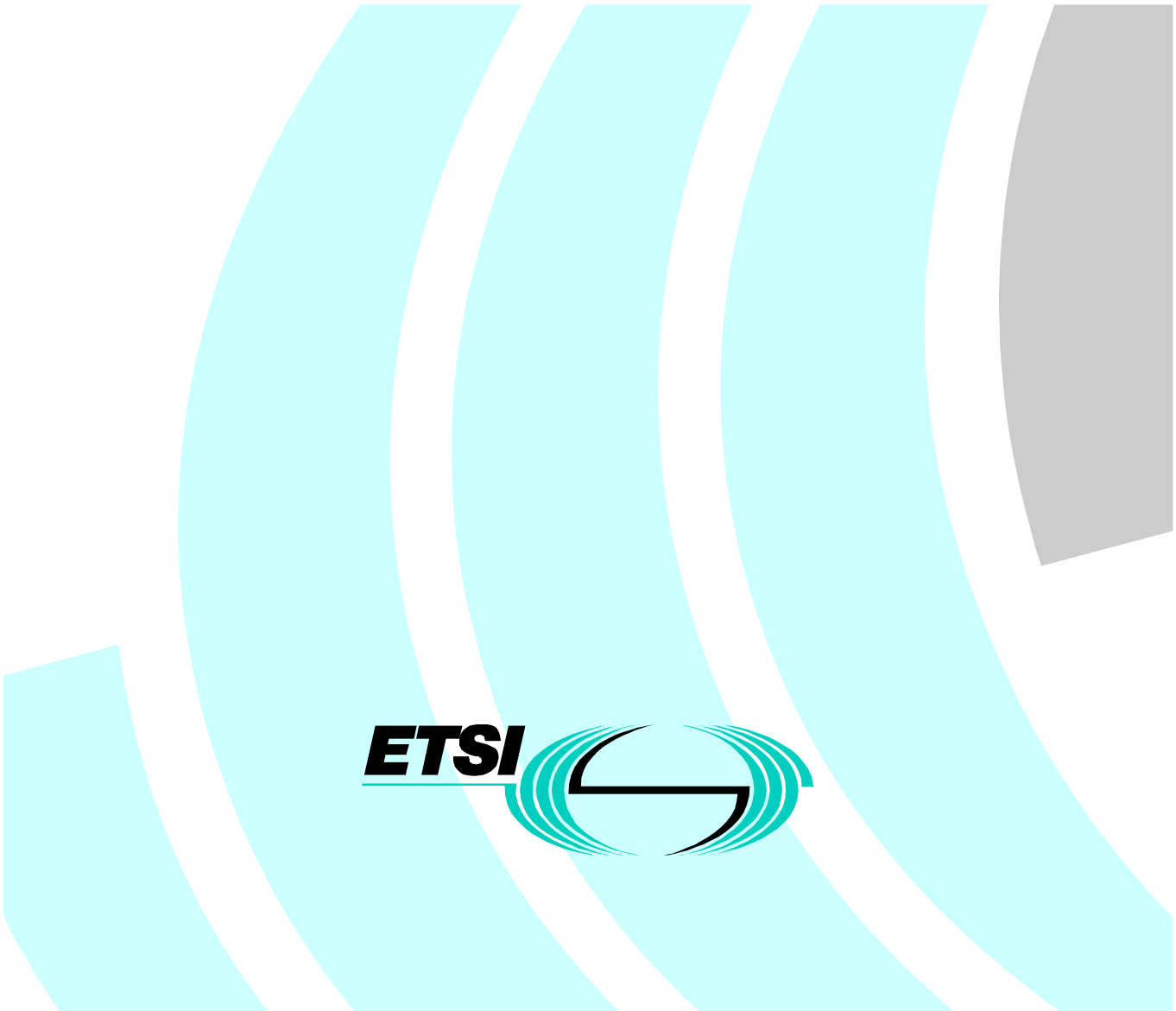
Draft ES 201 208 V1.2.1 (1999-01)

ETSI Standard

Identification card systems; Telecommunications IC cards and terminals; Additional Telecommunications Features (ATF)



Reference
RES/PTS-00004 (b6o00iop.PDF)

Keywords
Card

ETSI

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

Internet
secretariat@etsi.fr
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org

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 SR 000 314: *"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.org/ipr).

Pursuant to the ETSI 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 SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Standard (ES) has been produced by ETSI Project Pay Terminal and Systems (PTS), and is now submitted for the ETSI standards Membership Approval Procedure.

1 Scope

The present document specifies a group of Additional Telecommunications Features (ATF) in addition to those already specified in EN 726-6 [7]. The present document does not require all the ATF to be implemented; they may be implemented singly or in groups. Implementation of the telecommunications features in EN 726-6 [7] is not a pre-requisite for implementation of the ATF in the present document.

The ATF specified in the present document are listed below:

- Service Access Control (SAC);
- logging of call data;
- general identification/authentication;
- third party cards;
- last numbers storage;
- User Data Backup (UDB).

The present document applies to the User Cards (UC), card-related part of the terminals, Security Modules (SM) and to the interfaces between these entities.

Aspects included in the present document are:

- descriptions of features;
- logical structure of stored data;
- coding of data in data elements;
- functions and commands used by the ATF;
- procedures involved in interactions between the entities;
- security mechanisms;
- life cycle aspects of the ATF;
- usage of the ATF by applications;
- functions, external to the entities, which are required to support the ATF;
- application identifiers.

The present document does not specify the practical realization of the ATF in the entities.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, 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] CCITT Recommendation E.164: "The international public telecommunication numbering plan".

[2] CCITT Recommendation I.330 (1988): "ISDN numbering and addressing principles".

[3] EN 726-2 (1995): "Identification card systems - Telecommunication integrated circuit(s) cards and terminals - Part 2: Security framework".

[4] EN 726-3 (1994): "Identification card systems - Telecommunication integrated circuit(s) cards and terminals - Part 3: Application independent card requirements".

[5] EN 726-4 (1994): "Identification card systems - Telecommunication integrated circuit(s) cards and terminals - Part 4: Application independent card related terminal requirements".

[6] EN 726-5: "Identification card systems - Telecommunication integrated circuit(s) cards and terminals - Part 5: Payment methods".

[7] EN 726-6 (1995): "Identification card systems - Telecommunication integrated circuit(s) cards and terminals - Part 6: Telecommunication features".

[8] EN 726-7: "Identification card systems - Telecommunication integrated circuit(s) cards and terminals - Part 7: Security Module".

[9] EN 1038: "Identification card systems - Telecommunication applications - Integrated circuit(s) card payphone".

[10] EN 28601: "Data elements and interchange formats - Information interchange - Representation of dates and times".

[11] ISO 7816-1 (1987): "Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics".

[12] ISO 7816-2 (1988): "Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and location for the contacts".

[13] ISO 7816-3 (1990): "Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols".

[14] ISO 7816-4 (1995): "Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange".

[15] ISO 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for applications identifiers".

[16] ISO 7816-6: "Identification cards - Integrated circuit(s) cards with contacts - Part 6: Inter-industry data elements".

[17] ISO 8859-1: "Information technology - 8-bit single-byte coded graphic character sets - Part 1: Latin alphabet No. 1".

3 Abbreviations and symbols

3.1 Abbreviations

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

ACI	Access Control Information
AID	Application Identifier
ALW	Always (an access condition to an ICC file, see EN 726-3 [4])
ATF	Additional Telecommunications Feature
BAP	Backup-Application Provider
BCD	Binary Coded Decimal
CAD	Card Accepting Device
CHV	Card Holder Verification (e.g. a PIN or a biometric template)
CPS	Called Party Subaddress
DF	Dedicated File
EF	Elementary File
EF_{DIR}	EF containing a list of AIDs, i.e. applications supported by the ICC
EN	European Norm
HEX	Hexadecimal notation
HHMM	Hour, Minute
HHMMSS	Hour, Minute, Second
ICC	Integrated Circuit(s) Card
ID	Identification
ISDN	Integrated Services Digital Network
LNS	Last Numbers Storage
MMI	Man-Machine Interface
NEV	never (an access condition to an ICC file, see EN 726-3 [4])
Opt	Optional
PIN	Personal Identification Number
PRO	Protected (an access condition to an ICC file, see EN 726-3 [4])
PSTN	Public Switched Telephone Network
PTO	Public Telecommunications Operator
RFU	Reserved for Future Use (allocated only by the body responsible for maintaining the present document)
SAC	Service Access Control
SM	Security Module
UC	User Card (an ICC unless otherwise stated)
UDB	User Data Backup
YYMMDD	Year, Month, Date

3.2 Symbols

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

h	When used as a suffix, denotes a number expressed in hexadecimal format i.e. the sixteen hexadecimal digits "0" to "9" and "A" to "F".
n	A positive integer greater than zero.

4 General concepts

The present document complies with EN 726-6 [7], which describes:

- a possible method of using EF_{DIR} to determine which ATF are supported by the UC and to select the appropriate ATF;
- an informative logical model of the UC showing how each ATF may be associated with a DF and a group of EFs;
- normative conditions on the use of cohesive sets of keys and algorithms.

For each ATF (except the Third Party Card) an AID is required. The AID is preferably one issued by ETSI although other authorities may issue AIDs. The AID includes an application code and an application provider code. The ETSI application code is provided in the present document, and the appropriate application provider code can be obtained from the ETSI Secretariat.

5 Service Access Control (SAC)

5.1 Rationale

UC applications can generally be used in relation to a certain card related service (e.g. telephony). Not all users/subscribers will want to have the same access rights to particular services. Therefore a way to distinguish between different types of users/subscribers is needed.

5.2 Description

Based on the information provided by the ATF the application using the ATF may or may not allow access to services, e.g. international calling.

The following pre-conditions shall apply to the scope of this ATF:

- only applications requiring the use of a UC-related part of the terminal complying with EN 726-4 [5] are considered here. All other applications are out of scope;
- only applications requiring a UC which complies with EN 726-3 [4] are considered by the present document. All other applications are out of scope;
- the access control enforcement and actual service provision is out of scope here. It is assumed to be handled by the application involved.

Two access control schemes are specified, including:

- local access control for terminal resident applications;
- remote access control for remote equipment resident applications.

5.3 Functional model

5.3.1 Architecture and procedures

Figure 1 shows the model to be used for Service Access Control (SAC).

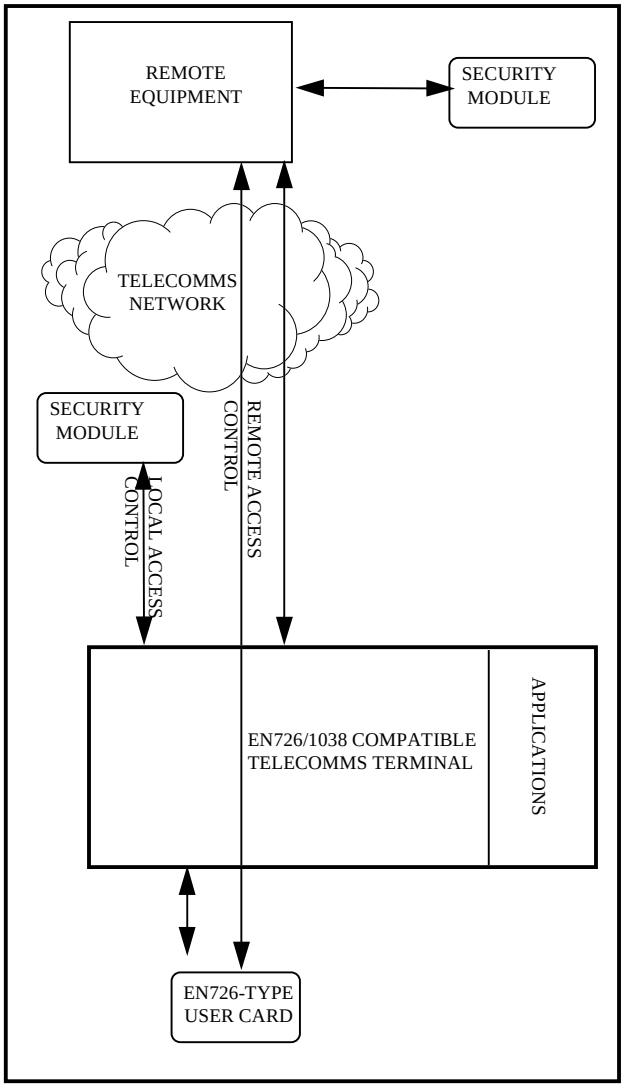


Figure 1: Reference model for Service Access Control (SAC)

Local access control shall be initiated by an application residing in the terminal; remote access control shall be initiated by an application residing in the remote equipment. In case of local access control the UC, terminal and local SM shall be involved. In case of remote access control the UC, terminal, remote equipment and remote SM shall be involved.

5.3.2 Functionality

Terminal functions:

For local access control the terminal shall contain access control decision functionality. It shall perform the following actions:

1) select the access control feature;

2) perform a CHV verification (optional);

3) retrieve and verify the access control information in a secure way;

4) take an access control decision and inform the initiating application about the result;

5) in case of a positive decision, provide the initiating application with data (e.g. CHV) which shall allow access to the part of that application residing on the UC.

For remote access control the terminal shall contain functionality to enable communication between the UC and the remote equipment. The flow of operation shall be controlled by the remote equipment.

UC functions:

When requested by the external world, the UC shall provide access control information and a related cryptogram to the external world. The EN 726-3 [4] READ STAMPED command shall be used for this purpose. If the AC CHV is set the UC shall verify the CHV successfully before this function may be used. If the AC PRO is set then the UC shall authenticate the origin of the command and check the integrity of the contents of the command given by the external world to the UC. The UC shall contain access control information, related secret keys related and a CHV. This data shall be contained in a DF_{SAC} and related files.

SM functions:

When requested by the external world, the SM shall provide a cryptogram to the UC, using the EN 726-7 [8] COMPUTE CRYPTOGRAM command. Before this is done the applicable keyset shall be diversified first. The EN 726-7 [8] DIVERSIFY KEY SET command shall be used for this purpose. On request of the external world the SM shall verify the access control information and related cryptogram provided by the UC. The EN 726-7 [8] VERIFY CRYPTOGRAM command shall be used for this purpose. The SM shall contain key sets related to UCs. This data shall be contained in a DF_{SAC} and related files.

5.4 Data requirements

5.4.1 Application code

The application code 0001h shall be used for this ATF.

5.4.2 Stored data on the User Card (UC)

The following figure depicts how the data structure of the Service Access Control (SAC) information shall be stored on the UC.

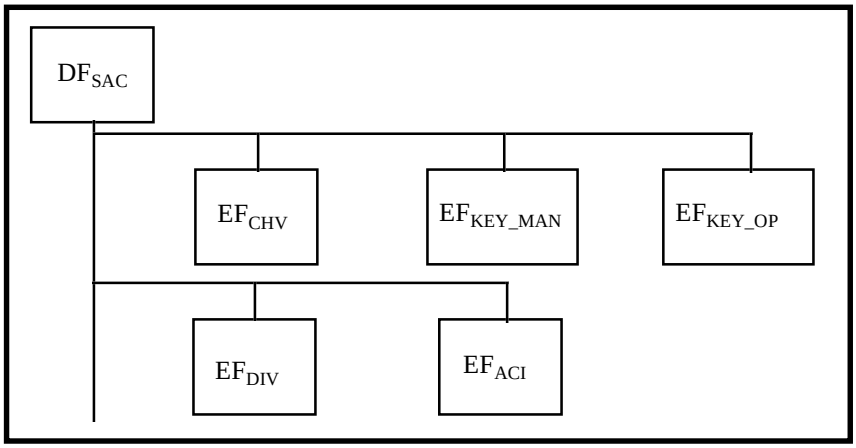


Figure 2: Data structure of access control feature on UC

- DF_{SAC} shall contain the access control application files based on a structure as specified by EN 726-3 [4]. Mandatory files are EF_{DIV}, EF_{ACI}, $EF_{Key\text{-}MAN}$ and $EF_{KEY–OP}$. File EF_{CHV} is optional.
- EF_{DIV} shall contain diversification information needed to derive the appropriate secret key in the SM.
- EF_{ACI} shall contain access control information, consisting of a classifier, service identifier and access parameter. The classifier shall specify if the access control information conforms to the present document or has a proprietary structure. The service identifier shall indicate the type of service it is applicable for. The access parameter shall indicate the access rights.
- EF_{KEY_OP} shall contain the key for calculating the cryptogram used to verify the authenticity of the ACI data.
- Optional file EF_{CHV}, if used, shall contain the CHV value needed to use the application.

Table 1: File attributes of EF_{DIV}

File size (memory to be allocated)	
File ID	
Access conditions UPDATE: READ: CREATE: WRITE: INVALIDATE: REHABILITATE:	 PRO CHV1/ALW PRO NEV PRO PRO
File status (refer to EN 726-3 [4] subclause 9.2.1).	
Length of the following data.	
Type of EF.	"01"
Length of records.	13 bytes

Table 2: Structure of a record in the file EF_{DIV}

Bytes	Description	Length
1-10	Diversification data	10 bytes
11-13 (note)	Expiry date	3 bytes
NOTE:	Byte 11-13, the expiry date, shall be BCD coded with format YYMMDD.	

Table 3: File attributes of EF_{ACI}

File size (memory to be allocated)	
File ID	
Access conditions UPDATE: READ: CREATE: WRITE: INVALIDATE: REHABILITATE:	 PRO CHV1/ALW PRO NEV PRO PRO
File status (refer to EN 726-3 [4] subclause 9.2.1).	
Length of the following data.	
Type of EF.	"01"
Length of records.	5 + X bytes

Table 4: Structure of a record in the file EF_{ACI}

Bytes	Description	Length
1 - 2	Classifier.	2 bytes
3 - 4	Service identifier.	2 bytes
4 - 5	Length of access rights.	1 byte
6- X	Access parameter.	X bytes

The classifier shall have the following structure and values:

- 00 00h = according to the present document;
- 00 01h = proprietary 1;
- 00 02h = proprietary 2;
- 00 03h to FF FFh = RFU.

For the 00 00h classifier, the service identifiers shall have the following structure and values:

- 00 00h = "payphone";
- 00 01h to FF FFh = RFU.

For the 00 00h service identifier (payphone), the access parameter shall have the following structure and values:

- a (range of) telephone number(s) permitted to be used by the payphone service. The numbers shall be coded in compliance with EN 726-5 [6].

The file may contain n records.

5.4.3 Stored data on the Security Module

The following figure depicts the data structure of the service access control information which shall be stored on the SM.

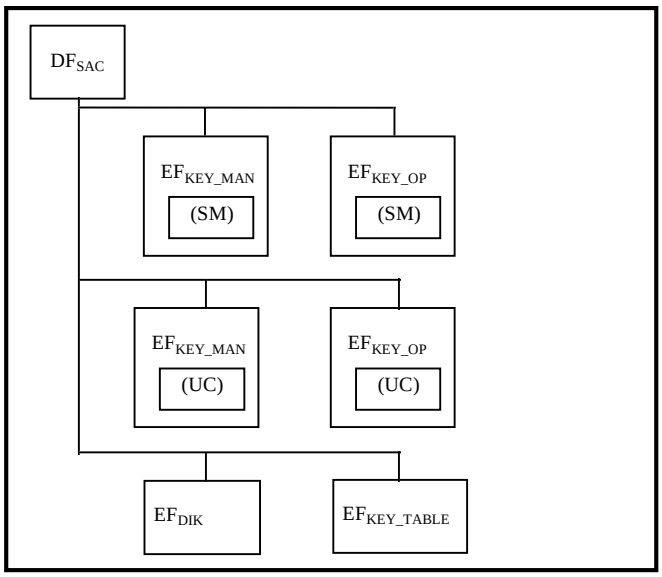


Figure 3: Data structure of access control feature on SM

- DF_{SAC} shall contain the access control application files which shall comply with the structure as specified by EN 726-7 [8]. $EF_{KEY\_OP(UC)}$ and EF_{DIK} are mandatory for this ATF.
- $EF_{KEY\_OP(UC)}$ shall contain the master key necessary to derive the relevant key for verifying the cryptogram coming from the UC, see EN 726-7 [8].
- EF_{DIK} shall contain the diversified keys after diversification, see EN 726-7 [8].
- All other files in figure 3 shall contain data as specified in EN 726-7 [8].

5.4.4 Interface data

The MMI shall comply with EN 726-4 [5].

The UC - terminal interface data shall comply with EN 726-3 [4].

UC - remote equipment interface data: On an application level the interface shall comply with EN 726-3 [4]. On a transport level the commands and responses may be grouped. The communication protocol and physical interface used depend on the applicable configuration (e.g. PSTN or ISDN).

The SM - terminal interface data shall comply with EN 726-3 [4] and EN 726-7 [8].

Terminal - remote equipment interface data: On a functional level this interface shall be able to transport signalling information for the general identification application applications and remote equipment handling functions in the terminal and the remote equipment. The communication protocol and physical interface used depend on the applicable configuration (e.g. PSTN or ISDN).

5.5 User procedure

The following user procedure shall be used:

1) if the user has not yet inserted the UC, the user shall be requested to insert it;

2) the user shall be requested to enter the relevant CHV (e.g. PIN), if required;

3) the user shall be informed about the status and result of the access control procedure.

If the access control feature is not supported by the terminal then the user shall be informed that the service requested cannot be provided by this terminal due to incompatible UC and terminal.

If the CHV entered is not correct then the situation shall be handled as specified in EN 726-3 [4] and EN 726-4 [5].

5.6 Security provisions

The following security provisions are mandatory:

- read access to the access control information stored in the UC shall allow CHV protection;
- access to secret keys stored in the UC shall not be possible from the external world after loading of these keys;
- access to key sets stored in the SM shall not be possible after loading of these keys;
- computation and verification of cryptograms shall be performed on data exchanged between the UC and the external world;
- random numbers shall be used in the computation of cryptograms.

6 Logging of call data

6.1 Rationale

For account based payment methods (e.g. auto-billing) a difference can exist between the charging/credit information available in a central billing system and the real costs/credit of a user/subscriber at a certain moment in time. A user/subscriber may require more up to date and off-line call cost information. Therefore local logging of call data is needed. In addition, the user might find it useful to have a personal log of other details of the last few transactions stored on the UC, as specified below. This ATF can be used with the payment applications specified in EN 726-3 [4].

6.2 Description

This feature shall allow a user/subscriber to store information on the UC concerning the latest n transactions and to review it in an off-line environment.

At the end of a telecommunications session, the terminal shall place transaction data into a special datafile on the UC, belonging to this ATF. If this ATF forms an integral part of another application, then an application code shall not be required for this ATF, because it will run under the application code of the parent application.

This feature can be activated or deactivated by the service provider during the administrative phase.

This feature can be used in conjunction with the auto-billing or the pre-payment application on the UC as specified in EN 726-5 [6].

6.3 Functional model

There are three mandatory functional scenarios associated with this application:

- updating the transaction log with call data in a terminal;
- reviewing the transaction log in an off-line environment;
- activating or deactivating of the feature by the service provider.

The transaction log shall be updated at the end of a call made from a terminal using the associated payment application in the UC.

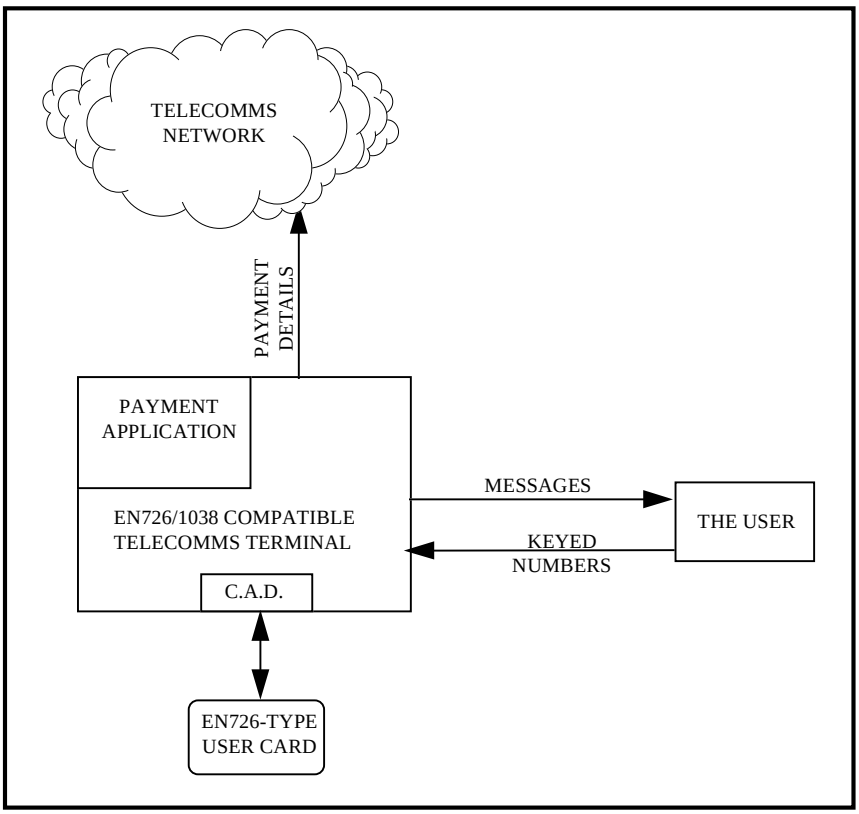


Figure 4: Functional model for updating the transaction log

The transaction log can be reviewed in an off-line environment. Activation or deactivation of the feature may also take place on an off line environment. It is not mandatory that this is done at a telecommunications terminal.

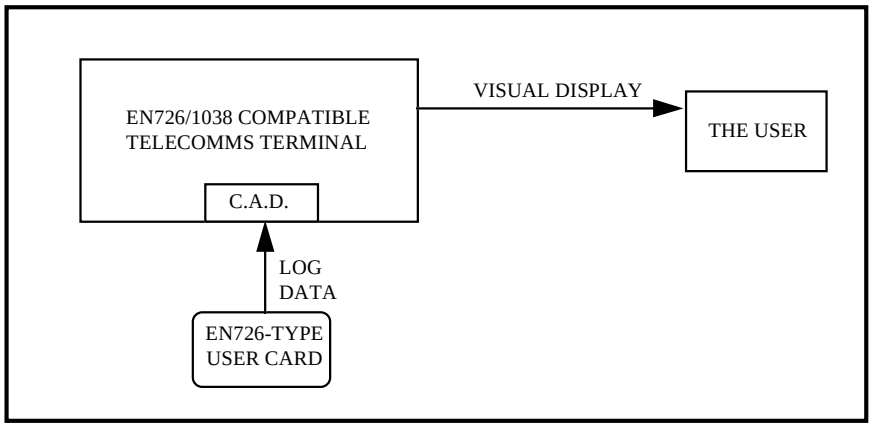


Figure 5: Functional model for viewing the transaction log

6.4 Data requirements

6.4.1 Application code

If this ATF forms an integral part of another application, then an application code shall not be required for this ATF, because it will run under the application code of the parent application. Otherwise, the application code shall be 0002h.

6.4.2 Specific files for the logging of call data

The logging of call data shall be associated with either an auto-billing or pre-payment application. One specific file for the logging of call data (EF_{CALL_DATA}) is mandatory and shall reside in the DF of the associated application ($DF_{AUTOBILLING}$ or $DF_{PRE\text{-}PAYMENT}$).

6.4.3 EF_{CALL_DATA}

Purpose:

This elementary file shall contain the following items needed for the logging of call data:

- date and time at which a call was made;
- telephone number which was dialled;
- duration of the call;
- cost incurred during the call;
- additional application-specific data.

File attributes:

When creating EF_{CALL_DATA} the following attributes are mandatory (also refer to EN 726-3 [4], subclause 9.2.3).

The file attributes may differ between a file associated with a pre-payment application and an auto-billing application.

The numeric KEY values assigned in tables 5 and 6 are consistent with those defined in EN 726-5 [6] subclause 5.4.1.

Table 5: File attributes of EF_{CALL_DATA} in a pre-payment application

File size (memory to be allocated)	
File ID	"1300"
Access conditions UPDATE: READ: CREATE: WRITE: INVALIDATE: REHABILITATE:	 PRO, KEY 1 CHV1 PRO/KEY 3 NEV PRO/KEY 1 PRO/KEY 4
File status (refer to EN 726-3 [4] subclause 9.2.1)	
Length of the following data	
Type of EF (note)	"03"
Length of records	X + 26 bytes
NOTE: Type of EF = "03" means cyclic EF.	

Table 6: File attributes of EF_{CALL_DATA} in an auto-billing application

File size (memory to be allocated)	
File ID	"3200"
Access conditions UPDATE: READ: CREATE: WRITE: INVALIDATE: REHABILITATE:	 PRO/KEY 1 CHV1 PRO/KEY 2 NEV PRO/KEY 1 PRO/KEY 3
File status (refer to EN 726-3 [4] subclause 9.2.1)	
Length of the following data	
Type of EF (note)	"03"
Length of records	X + 26 bytes
NOTE: Type of EF = "03" means cyclic EF.	

Structure of the file:

The total record length: X + 26 bytes. The file shall contain n records.

Table 7: Structure of a Record in the file EF_{CALL_DATA}

Bytes	Description	Length
1 - 3	Date of call	3 bytes
4 - 5	Time of call	2 bytes
6	Length of number (note 3)	1 byte
7	Type of number/numbering plan (note 3)	1 byte
8 - 17	Number dialled	10 bytes
18 - 23	Duration of call	6 bytes
24 - 26	Call cost	3 bytes
	Optional application dependent data	X bytes
NOTE 1: The date of call shall BCD coded in the format YYMMDD. NOTE 2: The time of call shall be BCD coded in the format: HHMM. NOTE 3: These number dialled shall be coded as defined in EN 726-6 [7], subclause 5.4.3. NOTE 4: The duration of call shall be BCD coded and has the following format: EN 28601 [10] NOTE 5: The call cost, if available, shall be stored and interpreted as specified in the respective payment application. If the call cost is not available the field shall be filled with FFh.		

6.5 Operational procedures

There are three operational scenarios which may be provided for the logging of call data:

- usage with a pre-payment application;
- usage with an auto-billing application;
- reviewing the transaction log.

6.5.1 Pre-payment application:

The pre-payment application shall be used as defined in EN 726-5 [6] subclause 5.5, with the addition of the following procedure at the end of a call:

- when a call ends, the external world shall check that the UC is still present and that the logging ATF is active. Then EF_{CALL_DATA} shall be selected. A transaction log shall be produced in the external world and stored in the UC.

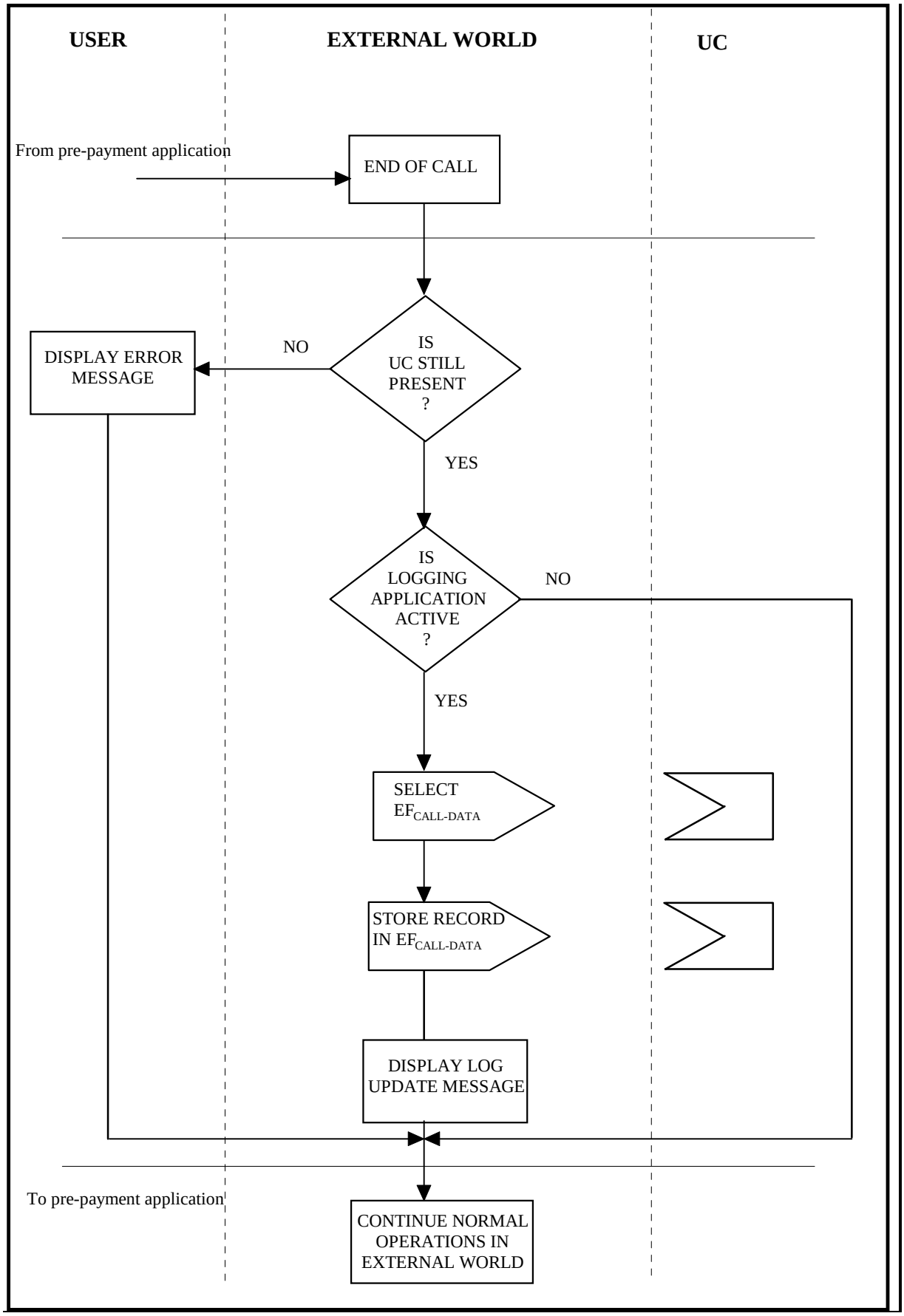


Figure 6: Scenario for the logging of call data with a pre-payment application

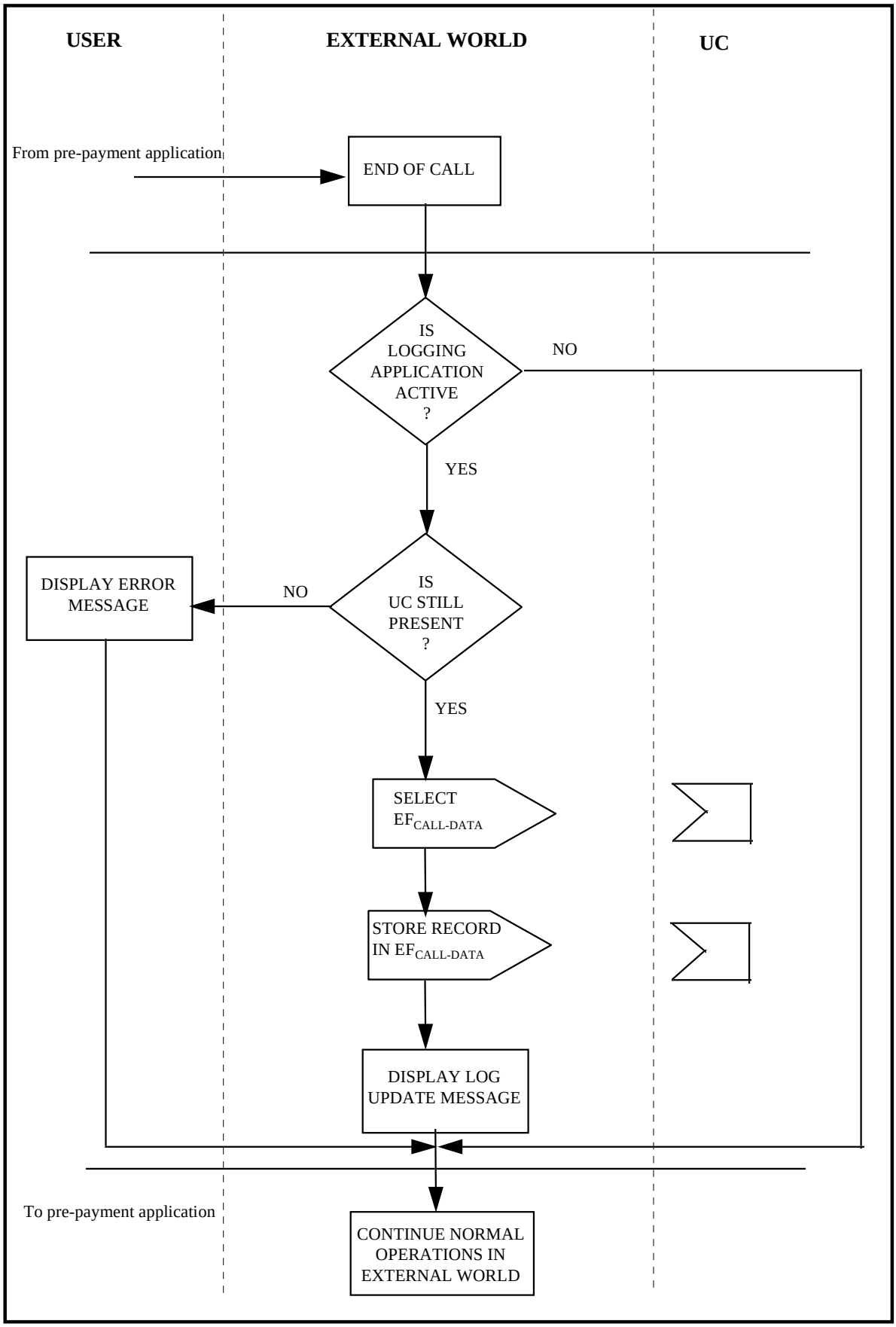


Figure 6 (concluded): Scenario for the logging of call data with a pre-payment application

6.5.2 Auto-billing application

The auto-billing application shall be used as defined in EN 726-5 [6] subclause 6.5, with the addition of the following procedures at the start and end of a call:

- when a call starts, if the logging application is active, the user shall be prompted to leave the UC in the terminal until the end of the call, to enable logging to take place;

- when a call ends, the external world shall check that the UC is still present and that the logging application is active. Then EF_{CALL_DATA} shall be selected. A transaction log shall be produced in the external world and stored in the UC.

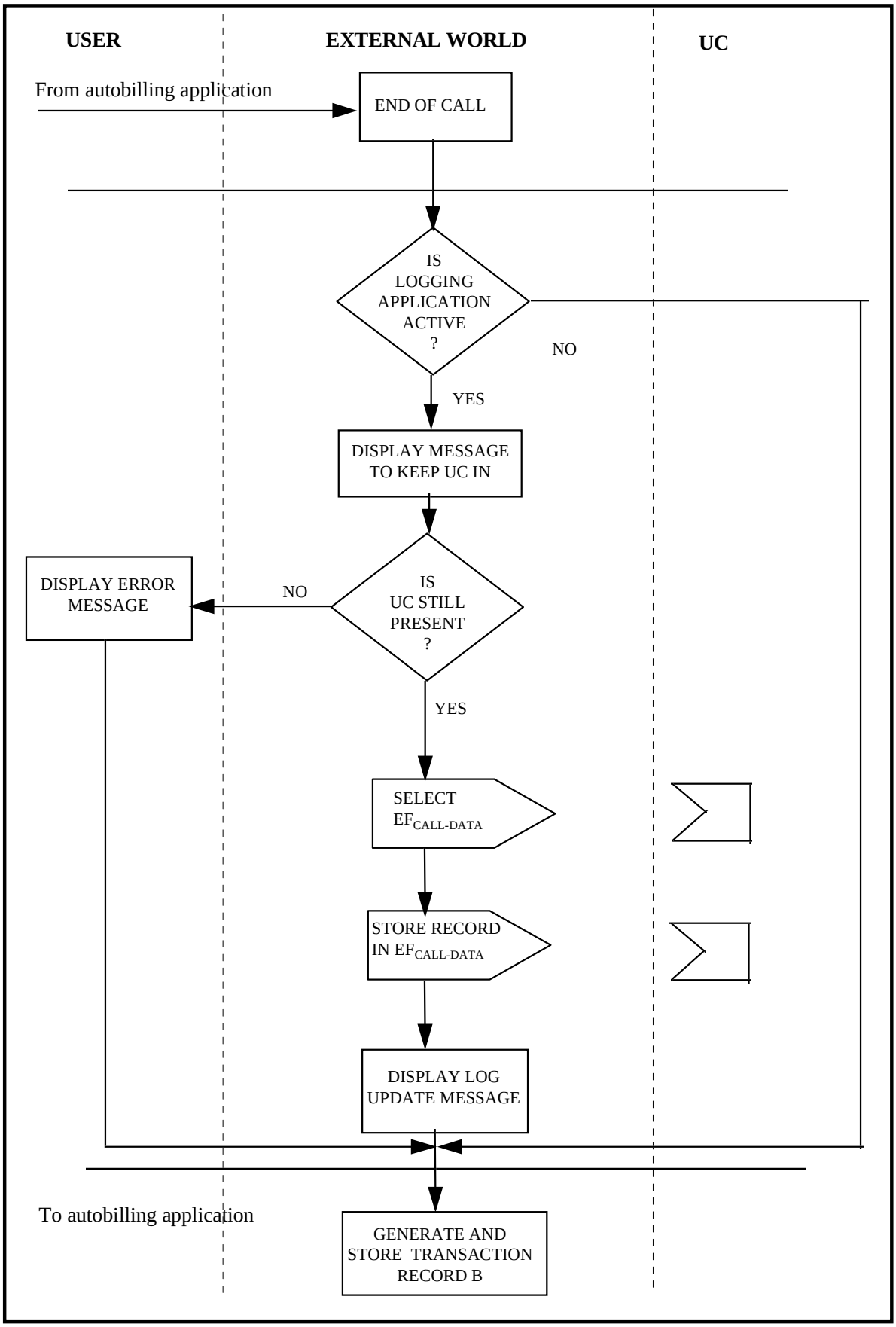


Figure 7: Scenario for the logging of call data with an auto-billing application

6.5.3 Reviewing the transaction log

The relevant pre-payment or auto-billing application shall be selected by the external world. If the logging of call data application is active, the user shall be able to request one or more of the transaction records to be displayed.

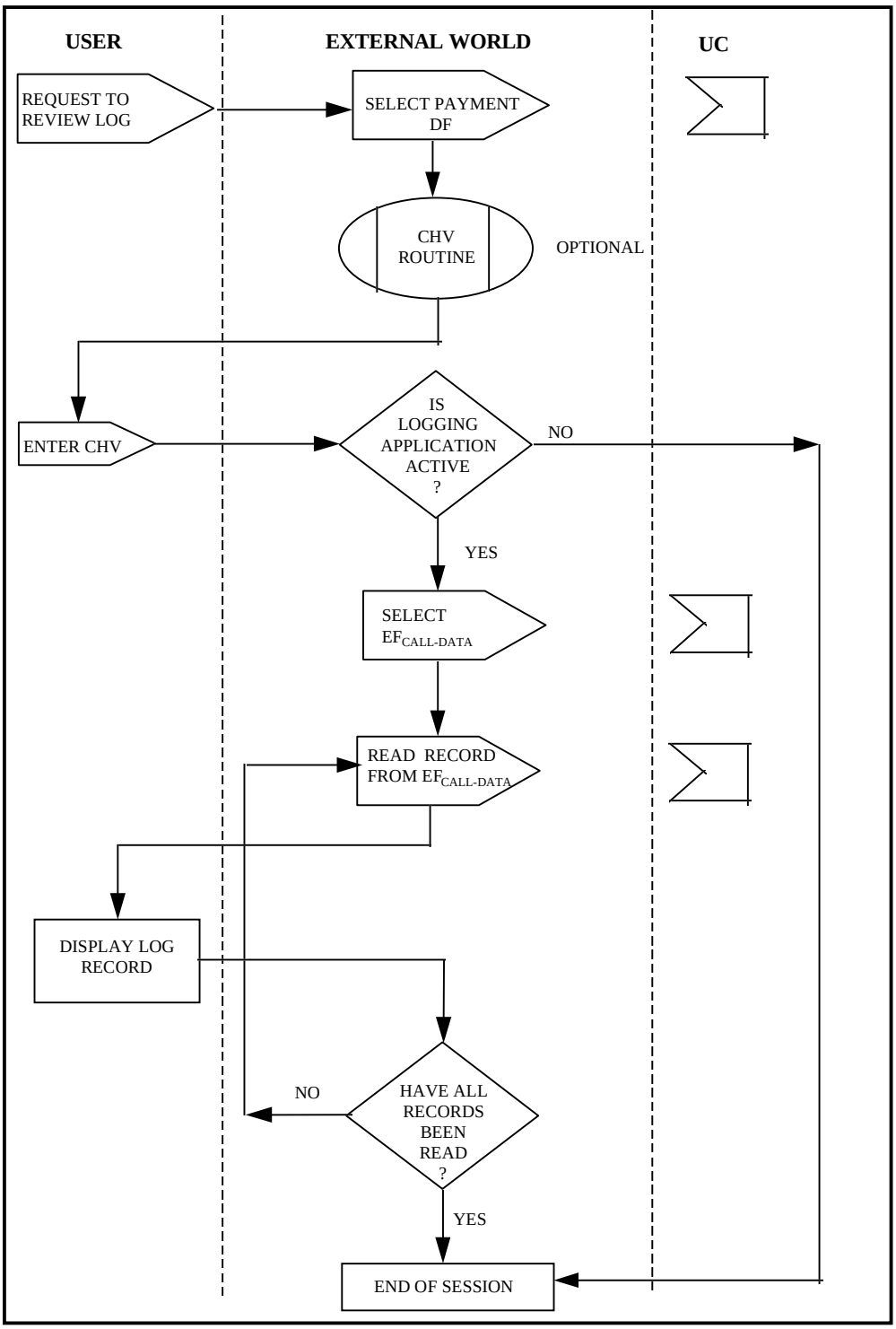


Figure 8: Scenario for reviewing the transaction application

6.6 Security provisions

The logging of call data application may be loaded in the relevant payment DF only by the payment application provider. The application may be invalidated or rehabilitated by an application provider.

The information stored in the transaction log shall be considered to be secure. The access condition for reading a record shall be CHV1 and for updating a record the access condition shall be PRO.

Based on the requirements of EN 726-2 [3] the following services are mandatory:

a) access control service;

b) authentication service, i.e.:

- card user to UC authentication;
- external world to UC authentication (for activation and deactivation of the application).

7 General-purpose identification/authentication

7.1 Rationale

Identification of the user by the service provider, and vice-versa, is a prerequisite for several telecommunication applications. For example, identification of the user can be needed for non-billing purposes such as access to closed user group. A general-purpose way of identification is therefore needed.

7.2 Description

This feature enables a service provider application to verify a user's identification. The feature also enables a user application to identify a service provider application and to verify the provider's application identification. This feature can be used as a prerequisite to get access to a certain telecommunication (e.g. telephony) or value added service (e.g. information service).

The following assumptions are made concerning the scope of this ATF:

- only applications requiring the use of a UC-related part of the terminal complying with EN 726-4 [5] are considered here, all other applications are out of scope;
- only applications where a UC complying with EN 726-3 [4] is required are considered by the present document; all other applications are out of scope;
- only applications residing in a terminal or UC, and where a SM complying with EN 726-7 [8] is required, are considered by the present document. All other applications are out of scope.

Two optional scenarios of general-purpose identification/authentication are specified. Whichever of these options are implemented, the method of implementation specified herein is normative:

- local identification/authentication;
- remote identification/authentication.

7.3 Functional model

7.3.1 Architecture and procedures

Figure 9 shows the functional model to be used for this ATF.

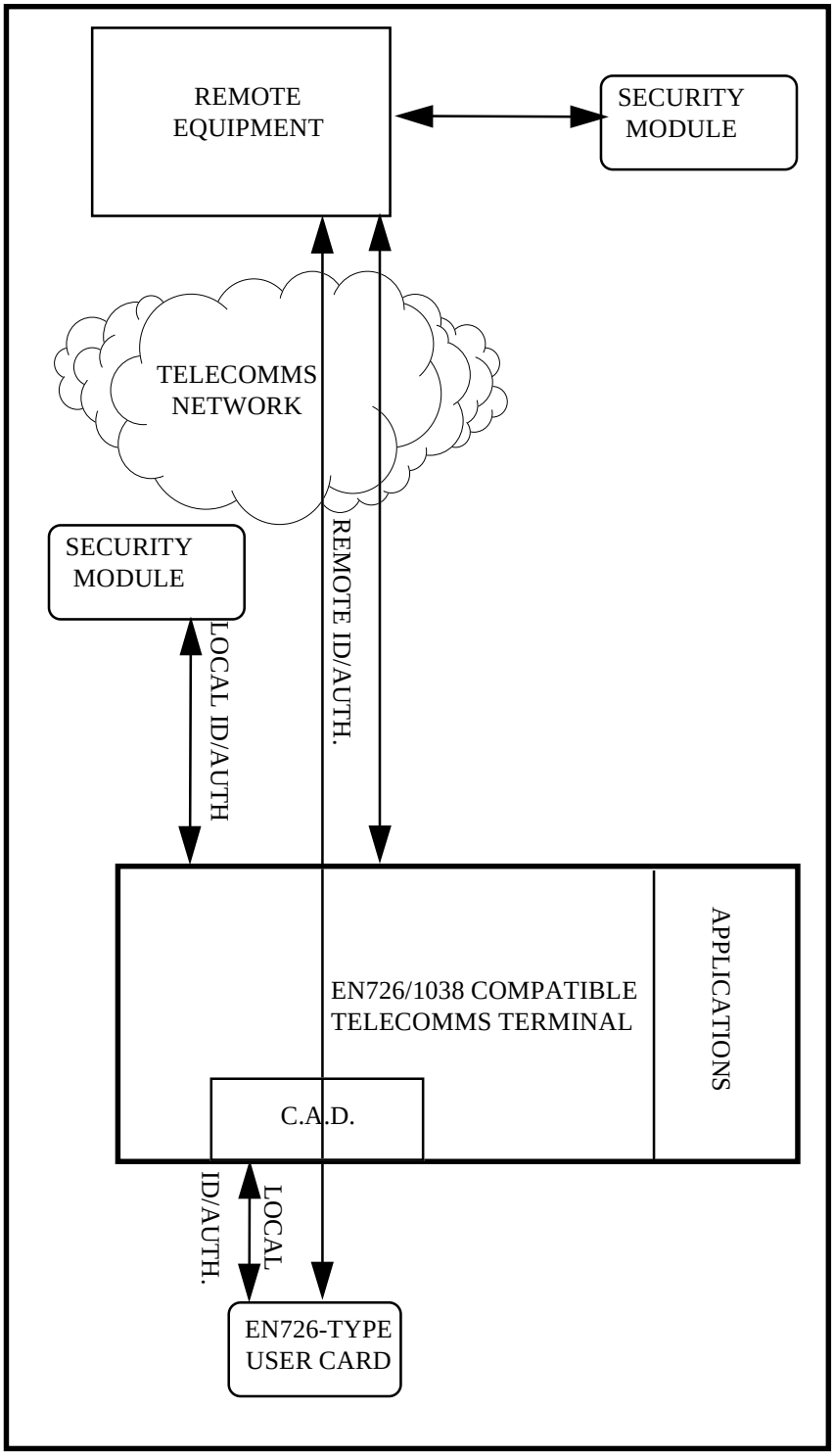


Figure 9: Reference model for general-purpose identification/authentication

Local Identification shall be initiated by an application residing in the terminal. Remote identification shall be initiated by an application residing in the remote equipment. In case of local identification/authentication the UC, terminal and local SM shall be involved. In the case of remote identification/authentication the UC, terminal, remote equipment and remote SM functionality shall be involved.

7.3.2 Functionality

Terminal functionality:

For local identification/authentication, the terminal shall contain functionality to perform the identification/authentication process. It shall perform the following actions:

1) select identification feature;
2) perform CHV verification;
3) retrieve and verify identification data;
4) store results and inform the initiating application about the result.

For remote identification, the terminal shall contain functionality to control communication between the general-purpose identification/authentication application in the remote equipment and the UC. The sequence of operations shall be controlled by the remote equipment.

UC functionality:

Firstly, the UC shall verify the CHV successfully. Then, when requested by the external world using the EN 726-3 [4] READ STAMPED command, the UC shall provide a user identifier and related cryptogram to the external world. However, if the AC AUTH is set on the UC, then before the files can be read the UC shall verify a cryptogram coming from the external world using the EN 726-3 [4] EXTERNAL AUTHENTICATION command. The UC shall contain an identifier, secret keys related to that identifier and a CHV. This data shall be contained in DF_{GIA} and related files.

SM functionality:

On request of the external world the SM shall provide a cryptogram to the UC, which shall be computed using a random obtained from the UC using the ASK RANDOM command. The EN 726-7 [8] COMPUTE CRYPTOGRAM command shall be used for this purpose. Before this is done the applicable keyset shall be diversified first. The EN 726-7 [8] DIVERSIFY KEY SET command shall be used for this purpose. On request of the external world the SM shall verify the identifier and related cryptogram provided by the UC. The EN 726-7 [8] VERIFY CRYPTOGRAM command shall be used for this purpose. The SM shall contain key sets related to UCs. This data shall be contained in a DF_{GIA} and related files.

7.4 Data requirements

7.4.1 Application code

The application code 0003h shall be used for this.

7.4.2 Stored data in the UC

The identification/authentication data coming from the UC on this interface shall be structured as shown in figure 10.

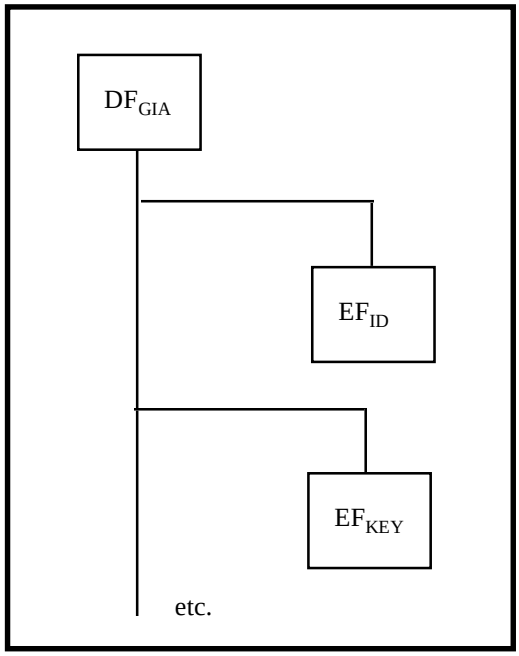


Figure 10: Data structure of application on User Card (UC)

- DF_{GIA} shall contain the application files for this feature. Mandatory files are EF_{ID} and EF_{key}.
- EF_{ID} shall contain the identification data.
- EF_{KEY} shall contain the secret key used for cryptographic computations.

Table 8: EF_{ID}, a subsidiary of DF_{GIA}

File size (memory to be allocated)	
File ID	
Access conditions	
UPDATE:	PRO
READ:	CHV1/CHV1&AUT
CREATE:	PRO
WRITE:	NEV
INVALIDATE:	PRO
REHABILITATE:	PRO
File status (refer to EN 726-3 [4], subclause 9.2.1)	
Length of the following data	
Type of EF	"01"
Length of records	13 bytes

Table 9: Structure of a record in the file EF_{ID}

Bytes	Description	Length
1-10 (note 1)	Identification data	10 bytes
11-13 (note 2)	Expiry date	3 bytes
NOTE 1: Bytes 1 - 10: The Identification data shall be BCD coded and shall be determined by the application provider.		
NOTE 2: Byte 11-13: The expiry date shall be BCD coded with format YYMMDD.		

7.4.3 Stored data in the Security Module

The identification/authentication data stored in the SM on this interface shall be structured as shown in figure 11.

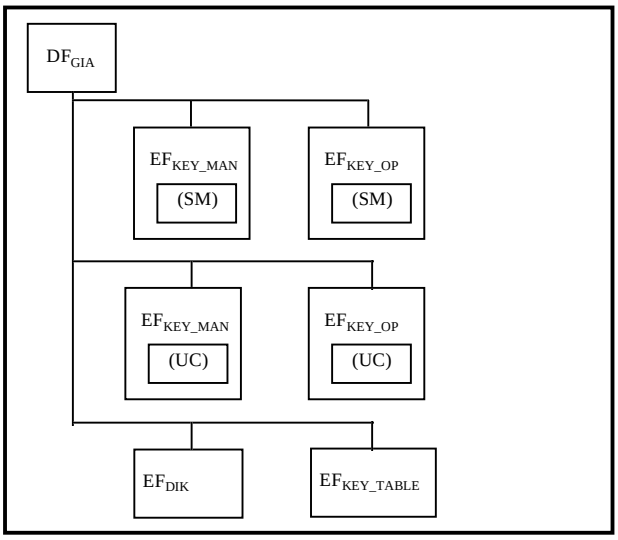


Figure 11: Data structure of application on SM

- DF_{GIA} shall contain the access control application files as specified by EN 726-7 [8]. $EF_{KEY\_OP(UC)}$ and EF_{DIK} are mandatory for this feature;
- $EF_{KEY\_OP(UC)}$ shall contain the master key necessary to derive the relevant key for verifying the cryptogram coming from the UC, as specified by EN 726-7 [8];
- EF_{DIK} shall contain the diversified keys after diversification, see EN 726-7 [8];
- all other files shall contain data as specified in EN 726-7 [8].

7.4.4 Interface data

The MMI shall conform to EN 726-4 [5].

The UC - terminal interface data shall conform to EN 726-3 [4].

Terminal - remote equipment interface data: for the transport of data and information the commands and responses may be grouped. This interface shall be able to transport signalling information for the general identification applications and remote equipment handling functions in the terminal and the remote equipment. The communications protocol and physical interface used depend on the applicable configuration (e.g. PSTN or ISDN) and are outside the scope of the present document.

The SM - terminal interface data shall conform to EN 726-3 [4] and EN 726-7 [8].

7.5 User procedure

The following user procedure shall be used:

1) if the UC is not inserted the user shall be requested to insert it;
2) the user shall be requested to enter the relevant CHV (e.g. PIN), if required;
3) the user shall be informed about the status and result of the identification/authentication.

If the CHV entered is not correct then the situation shall be handled as specified in EN 726-3 [4] and EN 726-4 [5].

7.6 Security provisions

- read access to the identifier stored in the UC can be CHV protected;
- access to secret keys stored in the UC shall not be possible from the external world after loading of these keys;
- access to key sets stored in the SM shall not be possible after loading of these keys;
- computation and verification of cryptograms can be performed on data exchanged between the UC and the external world;
- random numbers can be used for computation of cryptograms.

8 Third party cards

8.1 Rationale

The convergence of telecommunications, entertainment and financial applications means that IC Card terminals will need to accept UCs from service providers who are not PTOs.

Multi-application ICC UCs are not always viable, so it might be necessary to remove the EN 726-type UC during a call and to replace it with another UC to use and/or pay for a third-party service.

8.2 Description

This feature shall fall within the scope of the present document only if the UC used to establish and to pay for the call is one of the following:

- the auto-billing payment application on an EN 726-type UC;
- the prepayment application on an EN 726-type UC, but only if the call carries a fixed fee.

During a call, the user shall receive an audible or screen-based message from the service provider asking for the insertion of the 3rd party UC. The user shall then be required to remove the EN 726-type UC and replace it with the 3rd party UC. The EN 726-compatible terminal shall operate in a manner such that removal of the EN 726-type UC shall not cause the call to be terminated.

Details of the 3rd party UC application are outside the scope of the present document.

When the service provider's transaction is completed, the user shall be requested to remove the 3rd party UC and to terminate the call.

The use of other types of UC to establish the call or to obtain the 3rd party service is outside the scope of the present document.

8.3 Functional model

For the cases where this feature is to be used in publicly available EN 726-compatible terminals, the 3rd party ICC shall conform to the ISO/IEC 7816 series of standards [11] to [16], so that the terminal can interact with the appropriate application on the 3rd party ICC. The use of other types of 3rd party UC is outside the scope of the present document.

For the case where this feature is to be used in public payphones, the application on the 3rd party ICC shall operate as specified with the hardware functionality specified in EN 1038 [9].

This feature shall fall within the scope of the present document only if the 3rd party UC is supported by an application in the EN 726-compatible terminal, i.e. the terminal is able to recognize the 3rd party UC, to select the appropriate application on the UC and possesses (or is capable of obtaining a download of) the software required to handle the application on the 3rd party UC.

This feature shall operate according to the functional model in figure 12, which represents the minimum functional requirements.

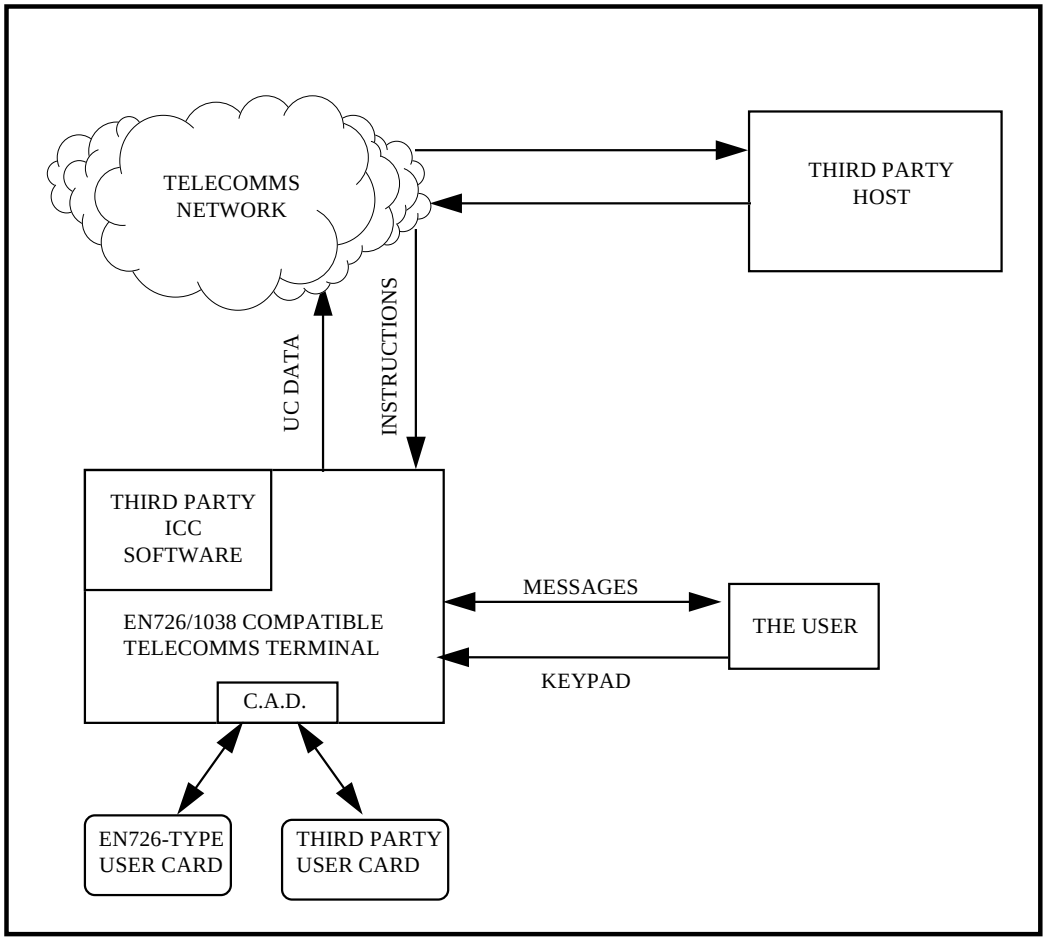


Figure 12: Minimum functional model for third party cards

8.4 Data requirements

All transactions generated concerning the EN 726-type UC shall be retained in the terminal's memory when the EN 726-type UC is replaced by the 3rd party UC. At the end of the EN 726-5 [6] type of call, these transactions shall be processed as per the requirements of EN 726-5 [6].

8.5 Operational procedures

The 3rd party UC feature shall be able to be used in conjunction with the fixed number dialling and short dialling features, as described in EN 726-6 [7], while the EN 726-type UC is still inserted in the terminal. For example, the EN 726-6 [7] short dialling feature can be used to call the 3rd party.

For 3rd party calls which are initiated using the prepayment application on the EN 726-type UC, the telecommunications terminal shall permit the user to remove the EN 726-type UC without terminating the call, but only if the call to the 3rd party service provider carries a fixed fee. For calls to the third party which carry a time-dependent fee, removal of the EN 726-type UC shall cause the call to be terminated as soon as any payment already deducted from the EN 726-type UC has been used up.

The scenarios in figure 13 show the operational procedures which shall be followed when this feature is used in conjunction with an EN 726-type UC and EN 726-type telecommunications terminal.

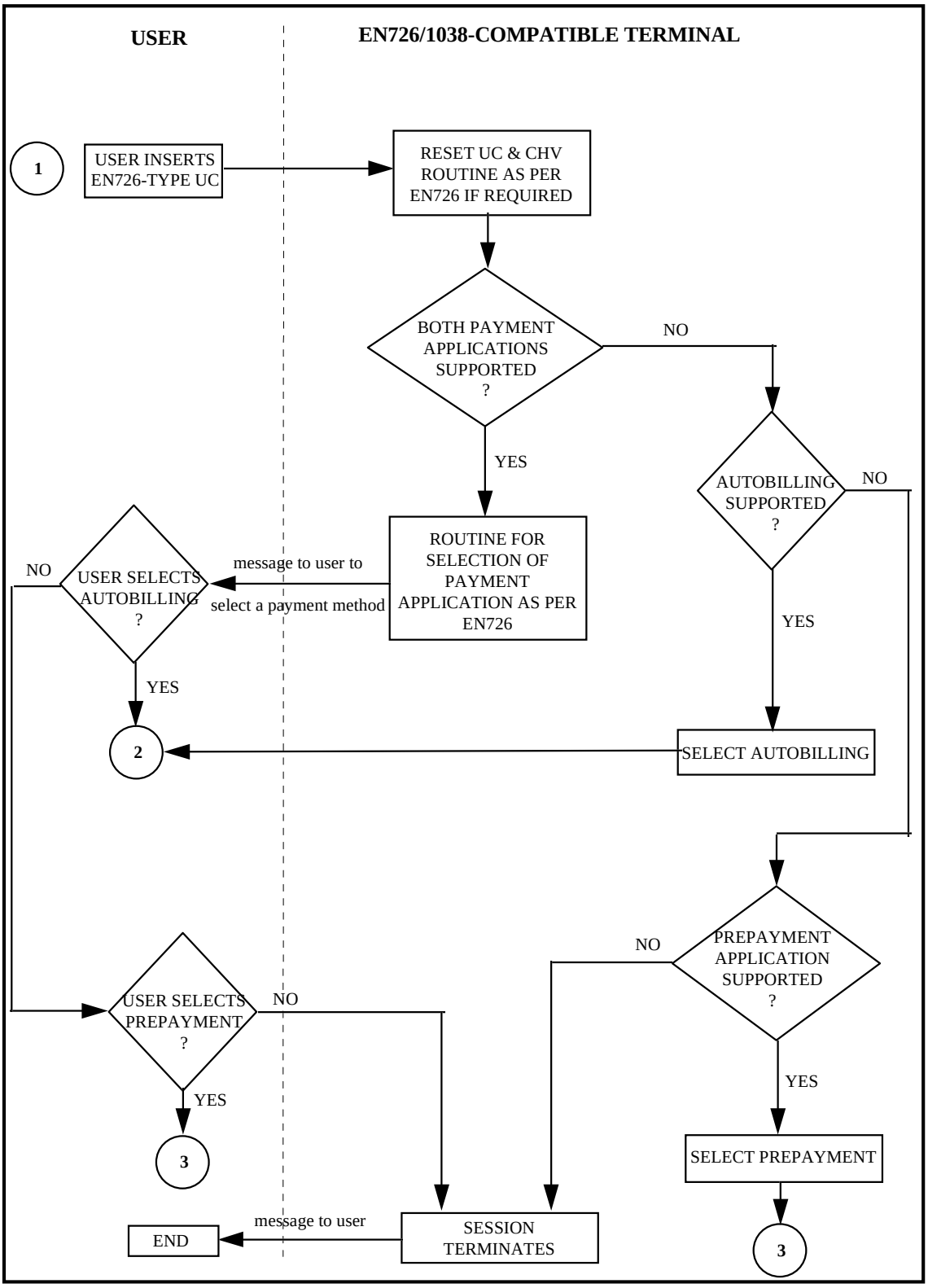


Figure 13: Selection of a payment application on the EN 726-type UC

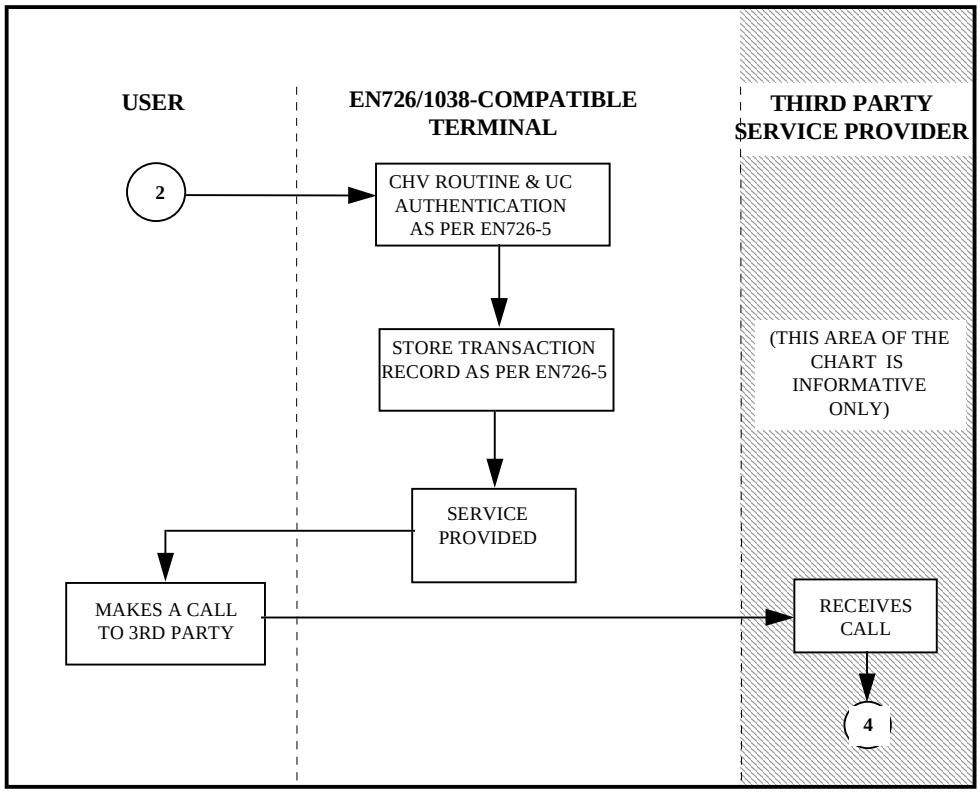


Figure 14: Scenario for the use of third party cards ATF with the EN 726-6 [7] auto-billing payment application

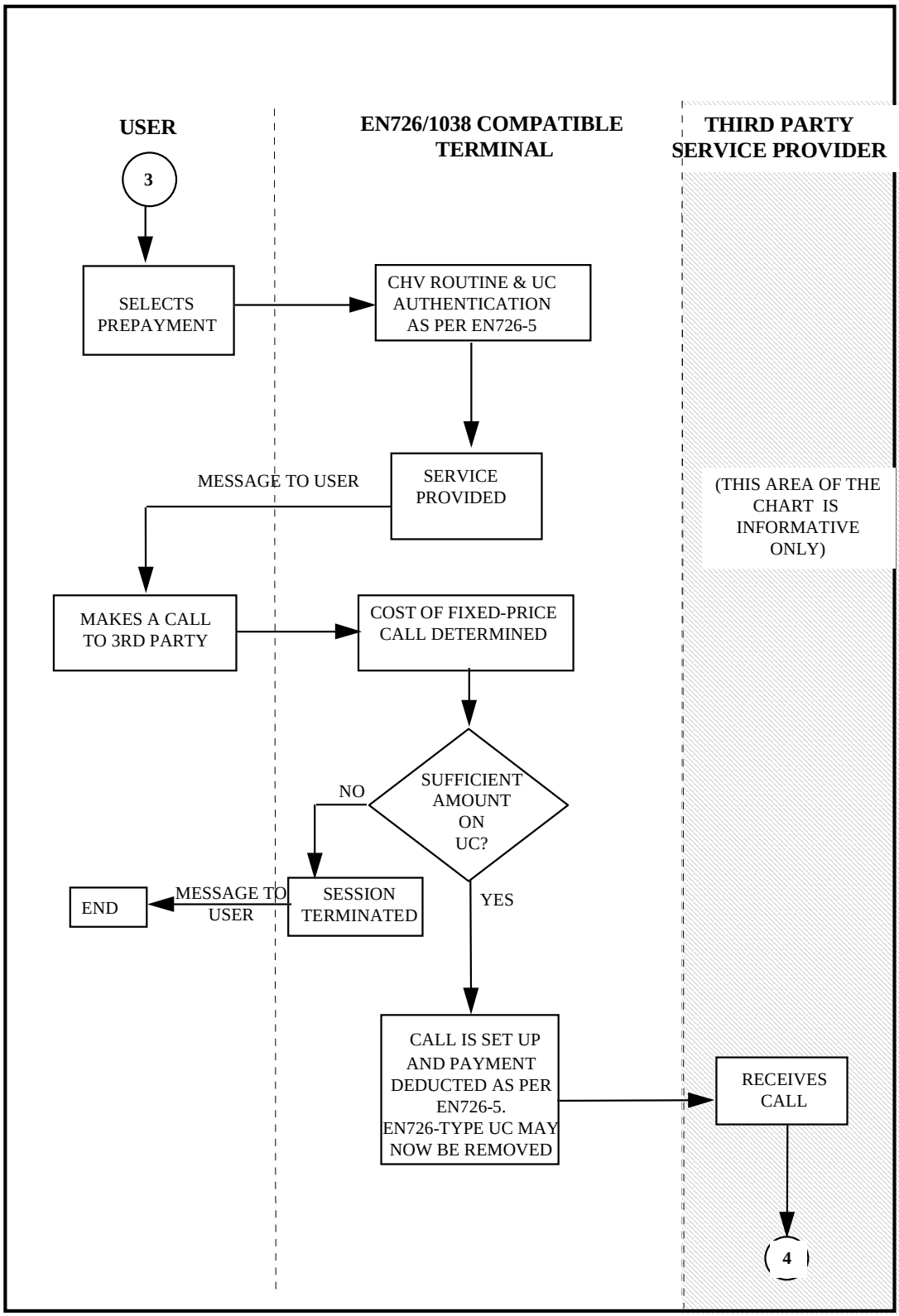


Figure 15: Scenario for the use of third party cards ATF with the EN 726-5 [6] prepayment application

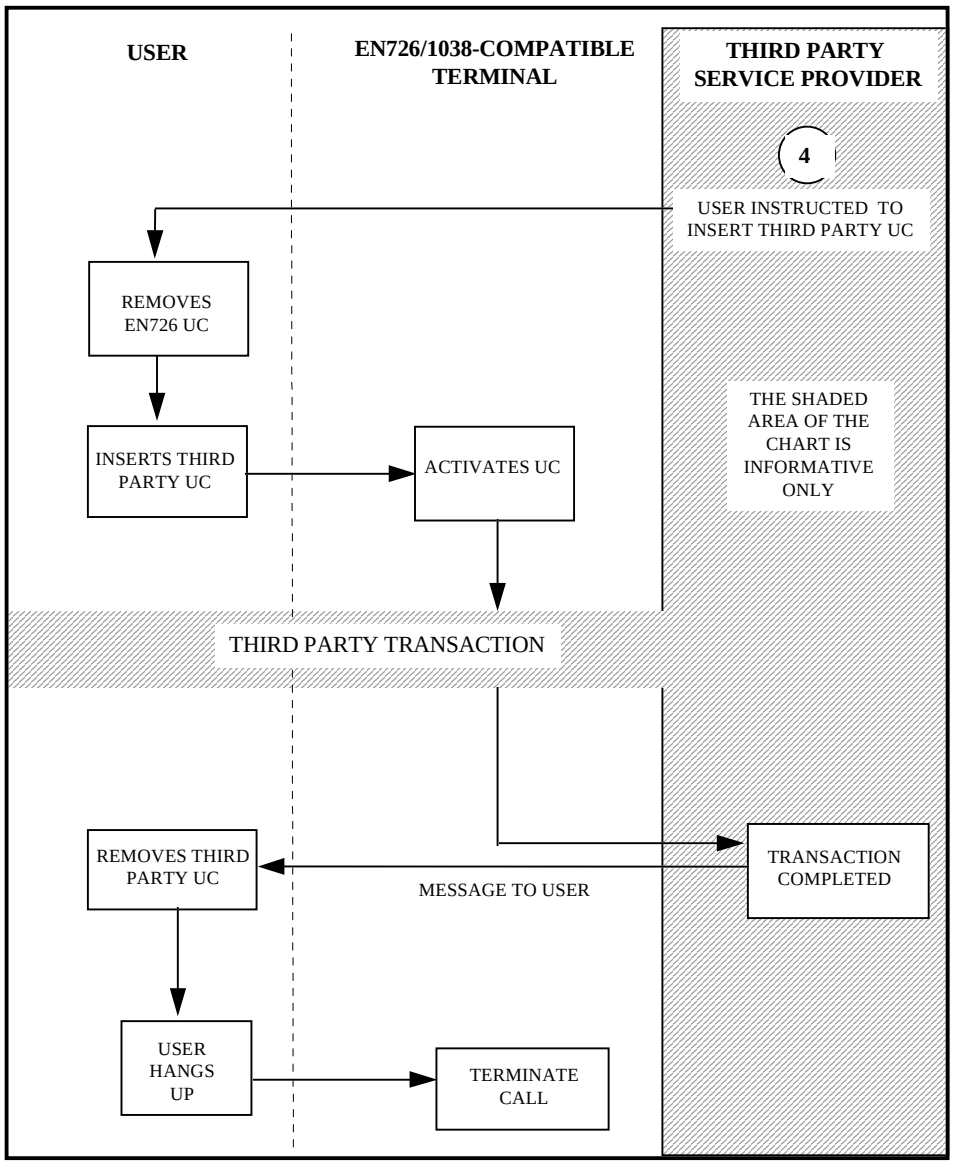


Figure 16: Common scenario for the use of third party cards ATF with the EN 726-type UC

8.6 Security provisions

When the prepayment application on the EN 726-type UC is used to initiate the call, the security requirements of that application in EN 726 shall apply until the EN 726-type UC is removed.

If the auto-billing payment application is used, then the following security provisions shall be mandatory:

- the security status of the EN 726-type UC and all diversified keys relevant to the EN 726-type UC shall be retained until the user terminates the EN 726 session e.g. UC removed or application terminated by the terminal;
- when the 3rd party part of the session is terminated, all security status and diversified keys relevant to the 3rd party UC shall be deleted from the memory of the EN 726-compatible terminal. When the EN 726-type session is terminated, the security status and derived keys relevant to the EN 726-type UC shall be managed as per the requirements of EN 726.

If the 3rd party application is downloaded to the user terminal during the 3rd party session, then the security status relevant to that application is outside the scope of the present document. It may be determined by the application provider.

9 Last numbers storage

9.1 Rationale

If a called number is busy, the user can make several calls before trying that number again. In this case, the last dialled number feature in EN 726-6 [7] is not helpful, but if a list of the most recently dialled numbers were stored it would be very useful.

9.2 Description

This feature allows the user to store in the UC the last n different numbers dialled out from a terminal, and it allows the redialling of any of these numbers automatically (after selecting the feature), even from another terminal, in another country, area or network. The last number dialled out shall be automatically stored in the UC.

This feature also allows network and bearer capabilities and/or extensions like called party subaddress to be associated with recorded numbers.

9.3 Functional model

The external application shall determine if the UC is able to support the last dialled numbers ATF. One way to do this is for the external application to read out EF_{DIR} at the master file level of the UC. It shall be left to the user to choose whether to use the EF_{DIR} method or not.

When a dialled number is given to the UC by the terminal, it shall consist of the national code, the area code, and the local number, in that order. Even if some or all of these were not dialled by the user, they shall be added on by the terminal.

For each of the n last dialled numbers, the terminal shall present to the user either the dialled number or the corresponding alphanumeric ID (if available) in reverse chronological order (i.e. most recently used number presented first). The user can then select one of the entries by its dialled number or by its alphanumeric ID, and the number then shall be automatically dialled by the terminal.

When the terminal dials out a number from the last numbers storage list on the UC, the terminal shall add or delete digits according to the type of number stored and the location from which the call is being made.

The MMI in the terminal shall be able to select this feature, to scroll the display, to select the desired number, and to validate it before dialling. Details of implementation of this MMI are outside the scope of the present document.

In the case where short dialling application (as described in EN 726-6 [7]) already exists on the EN 726-type UC, EF_{LND} shall be replaced by EF_{LNS}, (see subclause 9.4.2).

9.4 Data requirements

9.4.1 Application code

If this ATF forms an integral part of another application, then an application code is not required for this ATF, because it will run under the application code of the parent application. Otherwise, the application code shall be 0004h.

9.4.2 Specific files for Last Numbers Storage (LNS)

Figure 17 shows the file structure for this ATF.

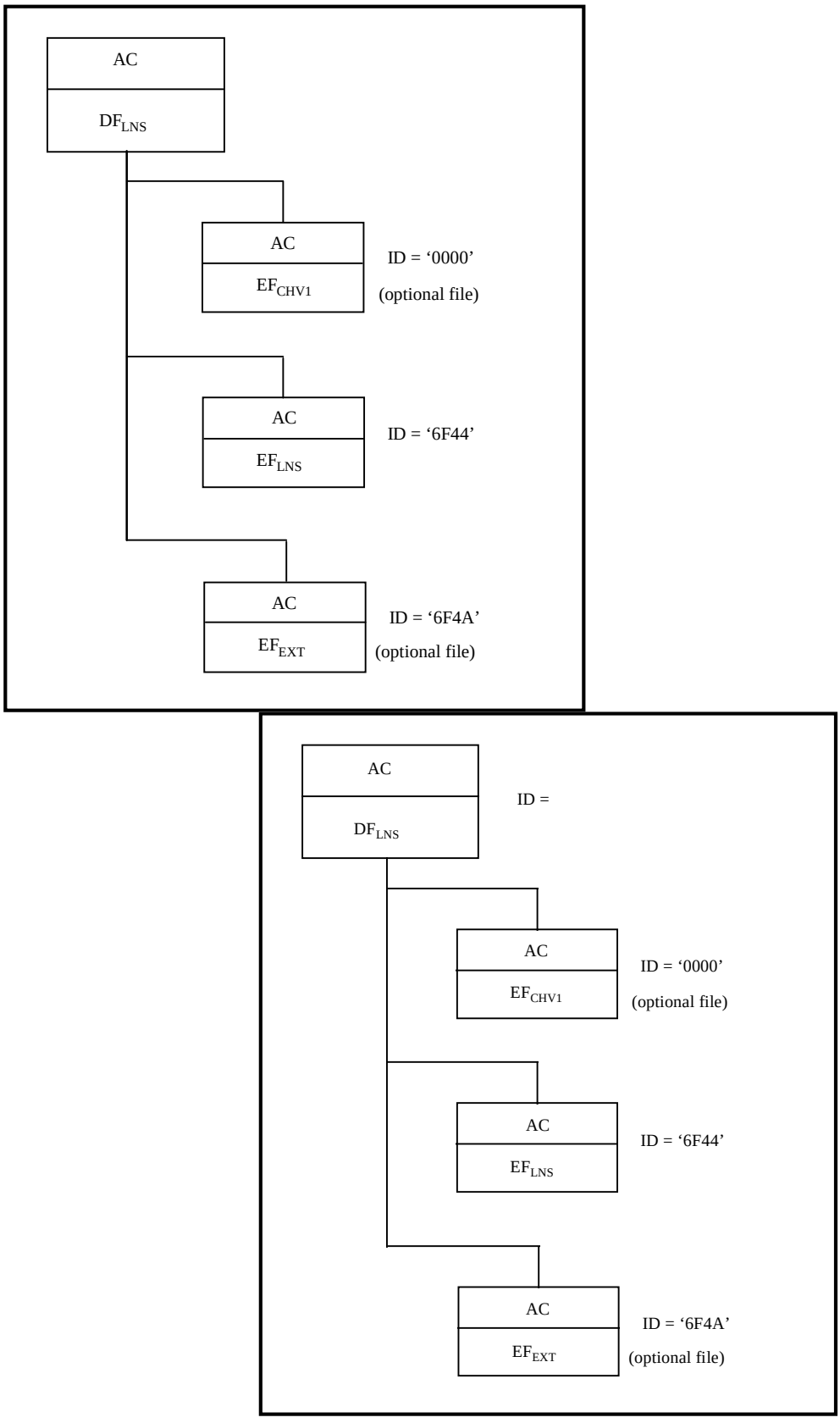


Figure 17: File structure for the Last Numbers Storage (LNS)

9.4.2.1 Description of the application DF_{LNS}

Purpose:
DF_{LNS} shall represent the Last Numbers Storage (LNS) application and shall contain all the EFs concerned with this application.

File attributes and file structure:

DF_{LNS} shall have the following attributes:

Table 10: File attributes of DF_{LNS}

File Size (memory to be allocated)	
File ID	
Access conditions CREATE	 PRO
File Status (refer to EN 726-3 [4] subclause 9.2.1)	
Type of file	"02" (DF)
Application identifier length	16 bytes
Application identifier (AID) (according to ISO/IEC 7816-5 [15])	

9.4.2.2 File for Last Numbers Storage: EF_{LNS}

Purpose:
EF_{LNS} shall contain the following items needed for the Last Numbers Storage (LNS) feature:

- length of numbers;
- type of numbers and numbering plan ID;
- telephone or terminal numbers of the n last correspondents. 20 BCD digits for each, stored on 10 bytes (unused nibbles shall be coded as Fh);
- a network/bearer capability identifier;
- an extension identifier;
- (optional) an alphanumeric ID associated with the number: up to X bytes in length. The value of X may vary from one UC to another, but within one EF_{LNS} it shall be identical for each record in the data field. The value of X shall be determined from the response of the UC to the SELECT command.

File attributes:
EF_{LNS} shall have the following attributes and structure:

Table 11: File attributes of EF_{LNS}

File size (memory to be allocated)	
File ID	"6F44"
Access conditions: UPDATE: READ: WRITE: CREATE:	 CHV1/ALW CHV1/ALW NEV PRO
File status (refer to EN 726-3 [4], subclause 9.2.1)	
Type of file	EF
Type of EF (note)	"03"
Length of records	X + 13 bytes
NOTE: Type of EF = "03" means that the file shall be a cyclic EF.	

Structure of the file:
The file shall contain n records. Each record shall be coded as shown in table 12. The length of each record shall be x + 13 bytes.

Table 12: Structure of a record in EF_{LNS}

Bytes	Description	Length
1	Length of dialled number	1 byte
2	Type of number and numbering plan	1 byte
3 to 12	Dialled number	10 bytes
13	Extension Record ID	1 byte
14 to 13 + x	Alphanumeric ID	X bytes

Coding:
Byte 1 shall be coded in BCD format.

Byte 2: the coding of the type of number/numbering plan shall be as shown in table 13.

Table 13: Coding of the type of numbering plan

Numbering plan identification	
Bits 4 3 2 1	
0 0 0 0	Numbering plan unknown
0 0 0 1	ISDN/telephony numbering plan (CCITT Recommendation E.164 [1])
0 0 1 1	Data numbering plan (ITU-T Recommendation X.121)
0 1 0 0	Telex numbering plan (ITU-T Recommendation F.69)
1 0 0 0	National numbering plan
1 0 0 1	Private numbering plan
1 1 1 1	Reserved for extension
	All other values are reserved.

Table 14: Coding of type number

Coding of type number	
Bits 8 7 6 5	
0 0 0 1	International number
0 0 0 0	Not international (unknown type). The terminal does not necessarily support the full functionality of last numbers storage in this case.
Others	RFU

Table 15: Coding for the dialled number

Number digits	
Bits 4 3 2 1 or 8 7 6 5	Number digit value
0 0 0 0	0
0 0 0 1	1
0 0 1 0	2
0 0 1 1	3
0 1 0 0	4
0 1 0 1	5
0 1 1 0	6
0 1 1 1	7
1 0 0 0	8
1 0 0 1	9
In accordance with CCITT Recommendations E.164 [1] and I.330 [2], only the decimal digits 0-9 shall be used in number information	
1 0 1 0	*
1 0 1 1	#
1 1 0 0	a
1 1 0 1	b
1 1 1 0	c
1 1 1 1	used as end mark in case of an odd number information

Bytes 3 to 12 of each record in EF_{LNS} shall contain two decimal digits in each byte. Unused nibbles shall be set to Fh.

The coding shall be as per the example below, where the coded numbers are shown in hexadecimal format for clarity.

EXAMPLE: Telephone number to be transmitted: 12345.

Byte 5	Byte 4	Byte 3	Byte 2	byte 1
F F	**F F**	**F 5**	**4 3**	**2 1**
b8.....b1	b8.....b1	b8.....b1	b8.....b1	b8.....b1

Figure 18: Coding of number digits

Byte 13, Coding of Extension Identifier byte: this byte shall be coded in binary and gives the associated record number in file EF_{EXT}. If no record is associated, this field shall be filled with "FF".

Bytes 14 to 13 + x: Alphanumeric ID (optional). The coding shall be in accordance with ISO 8859-1 [17]. The parity bit (bit 8) in ASCII characters set to 0 shall indicate no parity.

9.4.2.3 File for capability/configuration parameters: EF_{CCP}

Purpose:
This elementary file shall store the parameters of required network and bearer capabilities and configuration associated with a call established using one of the n last numbers dialled out.

File attributes:
EF_{CCP} shall have the following attributes:

Table 16: File attributes of EF_{CCP}

File size (memory to be allocated)	
File ID	6F3D
Access conditions: UPDATE: READ: WRITE: CREATE: INVALIDATE: REHABILITATE:	 CHV1/ALW CHV1/ALW NEV PRO PRO PRO
File status (refer to EN 726-3 [4], subclause 9.2.1)	
Length of the following data	
Type of file	EF
Type of EF (note)	"01"
Length of records	14 bytes
NOTE: Type of EF = "01" means that the file shall be linear with a fixed structure.	

Structure of the file:
The length of each record shall be 14 bytes.

The file shall contain n records.

Table 17: Structure of the file EF_{CCP}

Bytes	Description	Length
1 - 10	Network/bearer capability	10 bytes
11 - 14	User interface configuration	4 bytes

Coding:
Coding of each record of EF_{CCP} is outside the scope of the present document.

9.4.2.4 File for extension: EF_{EXT}

Purpose:
This elementary file shall contains the items needed for the Last Numbers Storage containing additional information such as Called Party Subaddress (CPS) (for ISDN use) or supplementary services which may be associated to the last numbers dialled, stored in EF_{LNS}.

File attributes:
EF_{EXT} shall have the following attributes:

Table 18: File attributes of EF_{EXT}

File size (memory to be allocated)	
File ID	6F3E
Access conditions: UPDATE: READ: WRITE: CREATE: INVALIDATE: REHABILITATE:	 CHV1/ALW CHV1/ALW NEV PRO PRO PRO
File status (refer to EN 726-3 [4], subclause 9.2.1)	
Length of the following data	
Type of file	EF
Type of EF	"01"
Length of records	13 bytes
NOTE: Type of EF = "01" means that the file shall be linear with fixed structure.	

Structure of the file:
The total record length: 13 bytes.

The file may contain n records.

Table 19: Structure of the file EF_{EXT}

Bytes	Description	Length
1	Type of record	1 byte
2 - 12	Extension information	11 bytes
13	Further extension ID	1 byte

Coding:
Byte 1 shall be the type of record, as shown in table 20:

Table 20: Coding of byte 1 of the file EF_{EXT}

Byte 1	
"00"	Unspecified
"01"	Called Party Subaddress (CPS)
"02"	Overflow data
	All other values are reserved for future use

Bytes 2-12 shall be extension information, i.e. overflow data or Called Party Subaddress (CPS), depending on record type.

Case 1: Extension record is Called Party Subaddress (CPS):

For a CPS two extension records shall be used, which shall be chained by the identifier field (byte 13). The extension record containing the first part of the CPS shall point to the record which contains the second part of the subaddress.

Case 2: Extension record is Overflow data:

The first byte of the extension data shall give the number of bytes of the remainder of the last number dialled and associated codes. The coding of remaining bytes shall be in BCD. Unused nibbles at the shall be set to Fh. If the number of overflow digits exceeds the capacity of the overflow record, it shall be possible to chain another record inside the EF_{EXT} by the identifier in byte 13.

Byte 13 (further extension ID):

Contents: Identifier of the next extension record to enable storage information longer than 11 bytes.

Coding: record number of the next record. "FF" identifies the end of the chain.

9.5 Operational procedures

9.5.1 Select Last Numbers Storage (LNS) feature

The user may choose whether or not to use the Last Numbers Storage feature to initiate a new call. However, this feature may only be selected if the Last Numbers Storage application is present in the UC and supported by the external world.

It shall be up to the external application to select the last numbers storage application as described in subclause 9.3. Then the external application can select the elementary file EF_{LNS}.

9.5.2 Select correspondent by LNS feature

After selecting EF_{LNS}, and after fulfilling all access conditions by the user, the contents of the file may be read by the external world. The external world then, depending on the way the feature is being performed (see subclause 9.3), can convert the choice of the user into the number to be dialled out, as described in subclause 9.3 as well. It may also be possible to add functionality described in the associated record(s) of network and bearer capabilities, and extensions like Called Party Subaddress (CPS).

9.5.3 Store the last number dialled

It may be possible that for a certain external application, during or at the end of the call, the last number dialled out is automatically stored in the UC in the file EF_{LNS} after all access conditions were fulfilled.

The procedure to evaluate, convert and store this last number dialled in the UC shall be as follows:

When updating a record in order to store the last number dialled, the external application shall convert the dialled subscriber number into the format defined for EF_{LNS} (refer to subclause 9.4.2.2 for the file format). For this purpose, the external world shall take into account:

- depending on the type of the call, all the prefixes added to the subscriber number;
- the country, area and network of the accessed terminal.

Since it is not allowed to have the same last number dialled stored more than once and the IC card cannot check when updating a record whether a certain entry already exists in EF_{LNS}, it is necessary that the external world first checks this by seeking in the file EF_{LNS}. After this check, if the number is not already on the list, the external world can store the new last number dialled by updating the record with the highest record number in EF_{LNS}. If the last number dialled is already stored the records shall be re-organized by the external world with the last number dialled as the current record.

As a cyclic file, EF_{LNS} shall have records of identical length and organized as a ring (refer to figure 19).

The number of records in EF_{LNS} shall be equal to the length of the last numbers dialled list (n numbers).

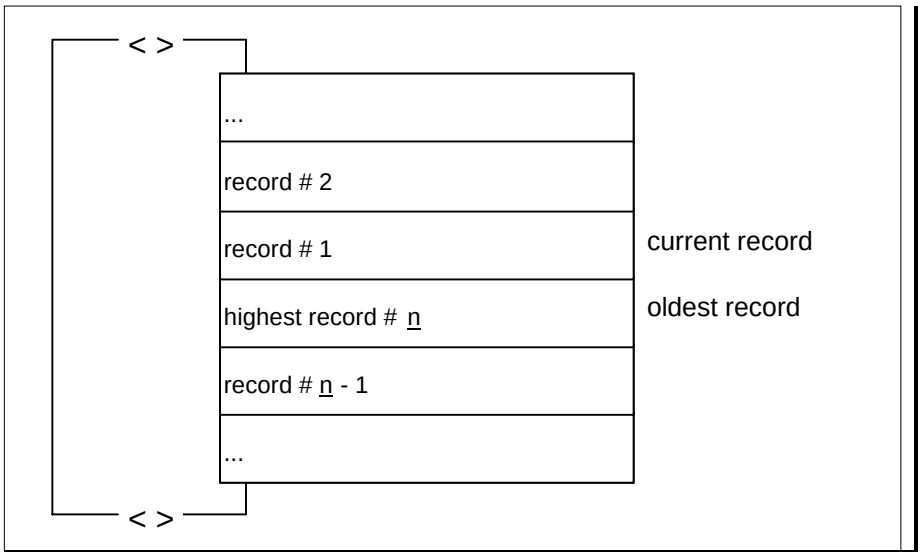


Figure 19: **Cyclic file organization**

In this file, record number one (# 1) shall be the last written record. The oldest written record shall have the highest record number.

For writing operations (i.e. to store the last number dialled, in this case), the only way of addressing a record shall be by using the command PREVIOUS. Only the record with the highest record number can be overwritten.

After a writing operation, the updated record shall be the current record number one (# 1).

9.6 Security provisions

A PIN (AC = CHV) may be used in that application to assure that only the authorized user may access the last numbers list stored in the card.

10 User Data Backup (UDB)

10.1 Rationale

A user who has stored data on his UC, e.g. telephone numbers, personal data etc., can lose or accidentally destroy the UC or can corrupt the data on it. It would be useful to be able to reload the lost data from a centralized backup store. Two functions are needed: backup (copy UC data to a backup store) and restore (reload a UC from the backup store).

10.2 Description

This feature enables the data in certain UC files to be saved into a remote backup store during a backup session, under the control of the user. The user may also copy these files to the same or another UC from the backup store during a reload session. In order to provide this service, the backup application provider shall be able to read and to reload all UC files which satisfy both of the following conditions:

- the access conditions for READ and UPDATE are ALWAYS or CHV1;
- the files IDs are specified in the file structure described in subclause 10.4 of the present document.

The use of this feature for files for which READ and/or UPDATE access are not ALWAYS or CHV1 (e.g. when the use of cryptographic algorithms and secret keys is required) is outside the scope of the present document.

10.3 Functional model

10.3.1 Entities involved

For the realization of the User Data Backup feature, the following logical entities shall be involved, but these entities need not be physically separate:

- the Backup-Application Provider (BAP). The BAP shall manage the backup store and shall inform the UC issuer how to implement the UDB application on the UC. The BAP shall be informed by the UC issuers on which UCs the User Data Backup application is implemented. The BAP shall be aware of the file structure of DFs of all the applications which use data that can and may be transferred to the backup-store;
- the UC issuer shall adapt the UC of the cardholder who requests the UDB application and shall provide up-to-date information to the BAP;
- the UC application provider(s) shall decide which data may be transferred to the backup store and under what circumstances.

10.3.2 Functional requirements in the different components

Three components shall be involved in the User Data Backup (UDB) application:

- the backup store;
- the terminal;
- the old UC and, optionally, the new UC.

The implementation of the User Data Backup application on the UC shall be done by the UC issuer. This implementation shall include an indication in the UC of the following elements:

- from which application the data may be transferred to the backup store;
- the data files which may be transferred to the backup store. The path to the data files which can be backed up may be recorded in the UC. If this is not the case, the terminal shall know the path;
- the expire date of the UDB feature of each application. Each application which can be backed up may have a specified expire date for the UDB feature, and if so this expire date shall be recorded in the UC. If the application to be backed up does not have such an expire date, then the expire date used shall be that of the UC;
- the contact details (e.g. telephone number) of the entity offering the UDB service.

The minimum functionality for the terminal to support the backup-application shall be as follows:

- a UDB session shall be allowed to be started only during another application;
- after a certain application is started, the terminal shall check in the $EF_{UDBINDEX}$ if the UDB for the current application is permitted on the UC and if the expire date for the UDB for the current application has not been passed. A UDB session may now be started but only by the user. If the check is unsuccessful, a UDB session shall not be permitted;
- after the user has started the UDB session, the user shall be prompted to choose between backup or reload;
- in the case of a backup session, the terminal shall read and memorize the identification number of the UC (bytes 1-10 in EF_{ID}). The path of those files and records to be backed up may either be recorded in the UC or be already known by the terminal. If the terminal does not know the files to be backed up, it shall select the $EF_{UDBINDEX}$ and shall seek the application identifier of the application to be backed up. If the application is found in the $EF_{UDBINDEX}$, the terminal shall memorize the backup store number contained therein. Then the EF_{UDB} file ID also defined in the $EF_{UDBINDEX}$ shall be selected. In the EF_{UDB} all files shall be defined which are allowed to be backed up;
- in case of a reload session, the user shall be asked to give the identification number of the UC which originated the backup data. Optionally, the user can indicate by a one-touch action that this number is the same as the identification number of the UC inserted, in which case the terminal shall read and memorize the identification number of the UC (bytes 1-10 in EF_{ID}). The terminal shall memorize the identification number of the UC which originated the backup data;
- the terminal shall contact the BAP;
- the method of information interchange between the terminal and BAP is out of the scope of the present document;
- the information interchange shall not be permitted until the CHV1 AC associated with the files to be read or updated has been satisfied, if required.

The backup store is a database which shall be accessible from every terminal which supports the UDB application. The database shall include the following functionality as a minimum requirement:

- the UC identification number (refer to EN 726-3 [4] subclause 10.5) shall be associated with each record;
- each record shall be subdivided into several fields. Each field shall contain the data necessary to support the backup of one application;
- each record shall contain an expire date; furthermore each field may contain its own expire date;
- before access to a record is given, the backup store shall check that:
  - the expire date has not been passed;
  - the UC is not blocked;
  - the CHV1 AC for the file has been satisfied, if required;

- the backup store knows the data structure of the applications on the UC which are supported by this backup-application. No information about this data structure shall be given by the terminal to the backup store.

10.4 Data requirements

10.4.1 Application code

The application code for this feature shall be 0005h.

10.4.2 Specific files for the user data backup-application

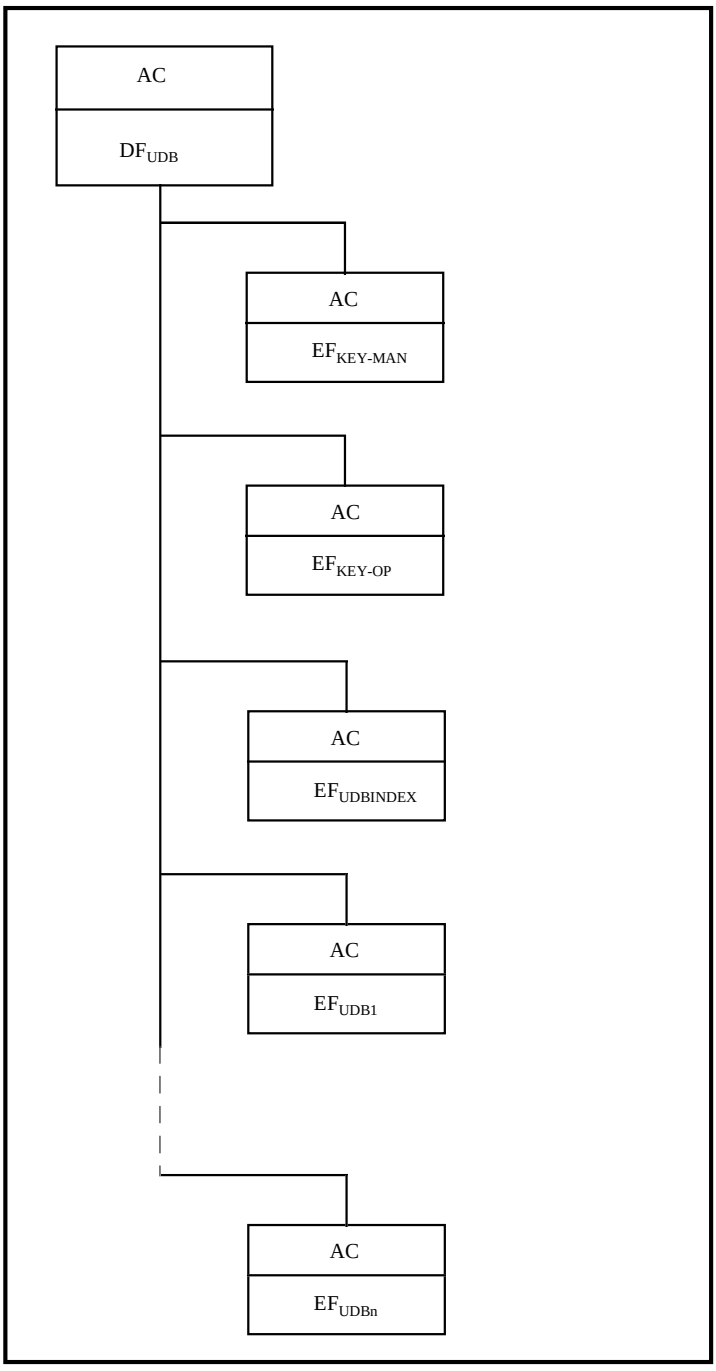


Figure 20: **Tree structure for the user data backup application**

10.4.3 Description of DF_{UDB}

DF_{UDB} shall have the following attributes (also refer to EN 726-3 [4], subclause 9.2.3.):

Table 21: **File attributes of DF_{UDB}**

File size (memory to be allocated)	
File ID	
Access conditions CREATE: INVALIDATE: REHABILITATE:	 PRO PRO PRO
File status (refer to EN 726-3 [4] subclause 9.2.1.)	
Length of the following data	
Type of file	DF
Application identifier length	
Application identifier (AID), according to ISO/IEC 7816-5 [15]	

10.4.4 Index file for user data backup: $EF_{UDBINDEX}$

Purpose:
An $EF_{UDBINDEX}$ shall be located in the user data backup directory DF_{UDB}. This EF shall contain the following records for each application which can use the User Data Backup (UDB) feature:

- the AID;
- the file ID of the related $EF_{UDBx;}$
- the number or address of the backup store for this application.

Each record in $EF_{UDBINDEX}$ may also contain the expire date for the User Data Backup (UDB) feature related to the application. If not, then the UC expire date shall be read from elsewhere in the UC (see EN 726-3 [4]).

Table 22: **File attributes of $EF_{UDBINDEX}$**

File size (memory to be allocated)	
File ID	
Access conditions: UPDATE: READ: CREATE: WRITE: INVALIDATE: REHABILITATE:	 PRO ALW PRO PRO PRO PRO
File status (refer to EN 726 subclause 9.2.1)	
Length of the following data	
Type of EF	LINEAR FIXED
Length of records	

Structure of the file:

Table 23: Structure of each record of $EF_{UDBINDEX}$

Bytes	Description	Length
1	AID	16 bytes
17	Length of backup store telephone number	1 byte
18	Type of number/numbering plan of backup store number	1 byte
19	backup store telephone number	10 bytes
29	File ID of related EF_{UDBn}	2 bytes
33	optional: expiry date	3 bytes

The coding of the backup store telephone number and type of number/numbering plan shall conform to EN 726-6 [7] subclause 5.4.3.

The expiry date shall be coded as YYMMDD in BCD format.

10.4.5 File for User Data Backup: EF_{UDB}

Purpose:
A separate EF_{UDB} is associated with each application. This means that for each application "n" that is supported by the data-backup application, an EF_{UDBn} shall be created.

Each record of this EF shall contain the following items needed for the User Data Backup (UDB) feature:

- the number of records of this file to be transferred (the value of 1 shall be used for binary files);
- the length of the records to be transferred;
- the path of the file to be transferred.

File attributes:
When creating EF_{UDB} the following attributes shall be taken into account (also refer to EN 726-3 [4], subclause 9.2.3).

Table 24: File attributes of EF_{UDB}

File size (memory to be allocated)	
File ID	
Access conditions: UPDATE: READ: CREATE: WRITE: INVALIDATE: REHABILITATE:	 PRO ALW PRO PRO PRO PRO
File status (refer to EN 726 subclause 9.2.1)	
Length of the following data	
Type of EF	LINEAR FIXED
Length of records	

Structure of the file:

Table 25: Structure of EF_{UDB}

Bytes	Description	Length
1	Number of records to be transferred	1 byte
2	length of the records to be transferred	1 byte
3	path of the file to be transferred	x bytes

10.5 Operational procedures

10.5.1 Invoking a backup/reload session

Invoking a backup/reload session may only occur during another application, i.e. when the access conditions to that other application are fulfilled. The way this invoking is handled by the human-terminal interface is out of the scope of the present document.

The user can choose between backup and reload. At the beginning of each session, the user shall be prompted to introduce a CHV (not necessarily the same CHV as stored on the UC) and, optionally any other means of verifying the identity of the user. The CHV shall be verified by the remote database. How this procedure is implemented is out of the scope of the present document.

After a successful check, permission shall be given to the terminal to proceed with the backup or reload operations as described as follows.

10.5.2 Make a backup (to a remote database) from the inserted ICC

The user shall be asked to introduce his UC CHV, if required to read the UC files and if not already introduced above. The terminal shall execute the backup session and shall advise the user whether the backup has been successful or not.

10.5.3 Reload the data in the backup store to an ICC

Two cases are possible: the data in the backup store are stored under the same ID as the ID of the inserted UC, or not.

After choosing "reload", the user shall be asked whether the ID is the same or not.

Data in the backup store are stored under the same ID as the ID of the inserted UC

The user can confirm this by a one-touch action. The terminal shall start the reload session, shall prompt the user to introduce his UC CHV, if required to update the UC files and if not already introduced above, and shall advise the user whether the reload session was successful or not.

Data in the backup store are stored under another ID than the ID of the inserted UC

The user can confirm this by a one-touch action. The terminal shall start the reload session, shall prompt the user to introduce the ID under which the data are stored and the UC CHV, if required and if not already introduced above. The terminal shall advise the user afterwards whether the reload session was successful or not.

10.6 Security provisions

From the security point of view, the user data backup application shall be independent from the application using the user data backup application, because they do not belong to the same DF in the UC.

Executing a reload/backup session on a stolen or found UC shall be prohibited by an on-line CHV or other identification mechanism.

History

Document history				
V1.1.1	May 1997	Membership Approval Procedure	MV 9730:	1997-05-27 to 1997-07-25
V1.1.1	August 1997	Publication		
V1.2.1	January 1999	Membership Approval Procedure	MV 9913:	1999-01-26 to 1999-03-26