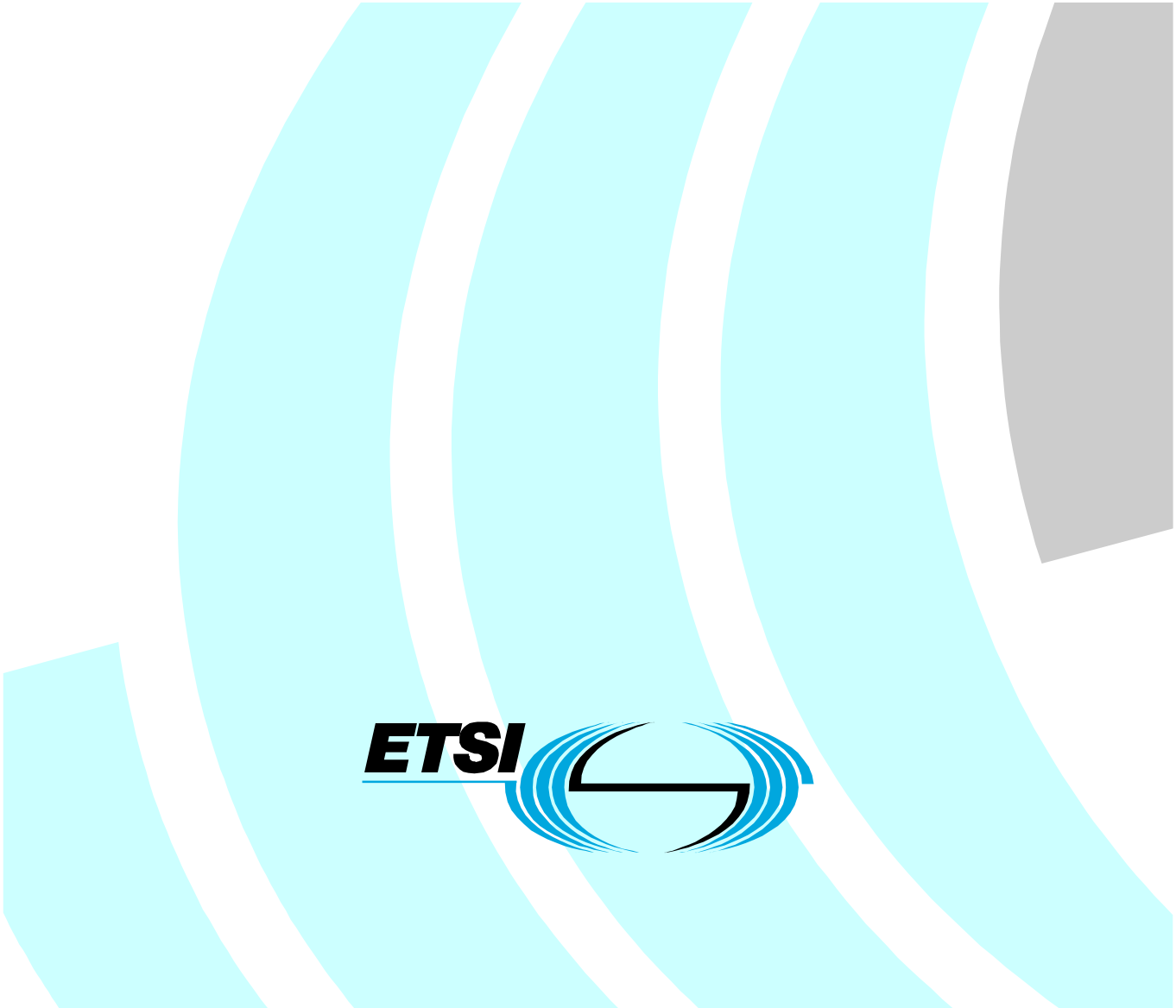
ETSI TS 102 222 V3.4.0 (2002-10)

Technical Specification

Integrated Circuit Cards (ICC); Administrative commands for telecommunications applications (Release 1999)



Reference
RTS/SCP-00011r2

Keywords
GSM, smart card, UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - 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

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 ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

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 ETSI 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 Technical Specification (TS) has been produced by ETSI Project Smart Card Platform (SCP).

The contents of the present document are subject to continuing work within SCP and may change following formal SCP approval. If EP SCP modifies the contents of the present document, it will be republished by ETSI with an identifying change of release date and an increase in version number as follows.

Version 3.x.y

where:

- 3 indicates Release 1999
- x the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- y the third digit is incremented when editorial only changes have been incorporated in the specification

1 Scope

The present document defines functions and syntax of a set of administrative commands for a telecommunication IC Card.

The commands defined in the present document are compliant to the commands defined in the ISO/IEC 7816 series where corresponding commands in ISO/IEC are available. The commands described in the present document are using parts of the functionality of the commands described in the ISO/IEC 7816-3 series. An IC Card supporting the command set based on the present document shall support the command as defined in the present document. However, it is up to the IC Card to provide more functionality than described in the present document.

The present document does not cover the internal implementation within the ICC and/or the external equipment.

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 and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] ISO/IEC 7816-3 (1997): "Information technology; Identification cards; Integrated circuit(s) cards with contacts; Part 3: Electronic signals and transmission protocols".

[2] ISO/IEC 7816-4 (1995): "Information technology; Identification cards; Integrated circuit(s) cards with contacts; Part 4: Interindustry commands for interchange".

[3] ISO/IEC 7816-8 (1999): "Identification cards; Integrated circuit(s) cards with contacts; Part 8: Security related interindustry commands".

[4] ISO/IEC 7816-9 (2000): "Identification cards; Integrated circuit(s) cards with contacts; Part 9: Additional interindustry commands and security attributes".

[5] ETSI TS 102 221: "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 5)".

[6] ETSI TS 151 011: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (3GPP TS 51.011 Release 4)".

3 Definitions, symbols and abbreviations

3.1 Definitions

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

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

administrative command: command modifying the internal properties of the file system of an ICC

current directory: latest directory (Dedicated File (DF) or Master File (MF)) selected in the ICC

current EF: latest Elementary File (EF) selected in the ICC

current file: latest file (DF or EF) selected in the ICC

Dedicated File (DF): file containing Access Conditions (AC) and allocable memory

NOTE: It may be the parent of Elementary Files (EF) and/or Dedicated Files (DF).

directory: general name for MF or DF

Elementary File (EF): file containing Access Conditions (AC) and data

NOTE: It cannot be the parent of another file.

file IDentifier (ID): each file (DF, EF) has a file identifier consisting of 2 bytes

Master File (MF): mandatory unique DF representing the root of the file structure and containing Access Conditions (AC) and allocable memory

NOTE: It may be the parent of elementary files and/or dedicated files.

operating system: required to manage the logical resources of a system, including process scheduling and file management

operating system termination state: ICC in this state shall be permanently unusable for the cardholder

record: string of bytes handled as a whole by the ICC and terminal and referenced by a record number or a record pointer

record number: is sequential and unique within an EF

NOTE: It is managed by the ICC.

telecommunication card: ICC mainly used for telecommunication applications

3.2 Symbols

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

'	Single quotation is used to indicate hexadecimal notation.
'0' to '9' and 'A' to 'F'	The sixteen hexadecimal digits
b8 ... b1	Bits of one byte. b8 is the MSB, b1 the LSB

3.3 Abbreviations

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

AC	Access Condition
ADF	Application Dedicated File
ADM	ADMinistrative (Access condition to an EF which is under the control of the authority which creates this file)
ALW	ALWays
AM	Access Mode byte
AM_DO	Access Mode Data Object
APDU	Application Protocol Data Unit
ARR	Access Rule References
AT	Authentication Template
ATR	Answer To Reset
CCT	Cryptographic Checksum Template
CLA	CLAss
CRT	Control Reference Template
CT	Confidentiality Template
DF	Dedicated File (abbreviation formerly used for Data Field)
DST	Digital Signature Template
EF	Elementary File

FCP	File Control Parameters
GSM	Global System for Mobile communications
IC	Integrated Circuit
ICC	Integrated Circuit(s) Card
ID	IDentifier
IEC	International Electrotechnical Commission
INS	INStruction
ISO	International Organization for Standardization
Lc	Length of command data sent by the application layer
LCSI	Life Cycle Status Information
Le	Maximum length of data expected by the application layer
LSB	Least Significant Bit
M	Mandatory
MF	Master File
MSB	Most Significant Bit
O	Optional
PIN	Personal Identification Number
PS	PIN Status
PS_DO	PIN Status Data Object
RFU	Reserved for Future Use
SC	Security Condition
SC_DO	Security Condition Data Object
SE	Security Environment
SEID	Security Environment ID
SIM	Subscriber Identity Module
SM	Secure Messaging
SW1/SW2	Status Word 1/Status Word 2
TLV	Tag Length Value

4 Mapping principles

IC Cards compliant to the present document shall follow the rules of TS 102 221 [5] in clauses 7 and 10.

5 Security architecture

This clause describes the general coding of security attributes assigned to files by use of the CREATE FILE command.

5.1 Security attributes

The security attributes are attached to a DF/EF and they are part of the FCP given in the CREATE FILE command. A security attribute is constructed using two basic data elements, the AM information and the security condition information SC. This information can be indicated in a compact format or an expanded format see ISO/IEC 7816-9 [4]. The security attributes are indicated in the FCP using tag '8B', tag '8C' or tag 'AB' depending upon the format used, see ISO/IEC 7816-9 [4].

5.1.1 Access mode indication

The AM information indicates what operations are allowed on a DF/EF. The coding of the AM information is file dependent i.e. the content of the access mode byte or data object is different if a DF or an EF is created, see ISO/IEC 7816-9 [4]. The access mode information is indicated in the FCP of the CREATE FILE command.

The security conditions for bits not set to 1 in the AM byte are set to NEVer by default.

5.1.2 Security conditions

In order to perform other commands on a file than the SELECT and STATUS/GET RESPONSE the security condition for the file shall be met. A security condition data object contains the conditions to be met in order to perform certain commands on a selected ADF/DF/EF. The SC or SC_DO contains information on what type of verification is needed (usage qualifier). This is defined by tag '95' as defined in ISO/IEC 7816-9 [4]. The SC_DO also contains a reference pointer, in this case a key reference. The key reference is indicated using tag '83' as defined in ISO/IEC 7816-4 [2]. The key reference is used to indicate what key is to be verified in the VERIFY command as defined in ISO/IEC 7816-4 [2]. The SC information is indicated in the FCP of the CREATE FILE command.

5.1.3 Access condition mapping

The access coding mapping is application specific. The access coding mapping can be found in the annex A.

5.2 Access rules

The access rule defines the security conditions for access to a file for each command/command group indicated in the AM-byte/AM_DO. The security condition is indicated in the SC-byte(s)/SC_DO(s) following the AM-byte/AM_DO. The access rule is coded by using one ore more AM-bytes/AM_DOs each followed by one or more security conditions that are to be satisfied for the appropriate access.

The access rules may be coded in a compact or an expanded format. Furthermore, it is possible to combine one or more SCs to one AM such that at least one SC (the OR relation) shall be fulfilled before the command can be executed. It is possible to combine the SC such that more than one SC has to be fulfilled (the AND relation).

An access rule is a requirement that has to be met in order to perform operations on a file. An access rule contains an AM byte/AM_DO that indicates what commands can be performed and a SC byte/SC_DO that indicates what SC must be met to be able to perform the commands indicated in the AM byte/AM_DO. The content of each AM byte (in compact format) or AM_DO (in expanded format) shall be unique within the same access rule. SC_DOs OR and AND relations shall contain at least two access conditions.

The CRT tags for SC_DOs are defined in ISO/IEC 7816-9 [4]. The SC required to perform commands indicated in the AM byte/AM_DO may be a simple condition or a logical OR or AND condition of several SC_DOs. The constructed TLV object containing AM bytes/AM_DOs and SC bytes/SC_DOs is an access rule. An access rule can be indicated in the FCP of the CREATE FILE command in one of the following ways:

- Tag '8C' Security attributes, compact format;
- Tag 'AB' Security attributes expanded format;
- Tag '8B' Security attributes. Referenced to expanded format.

The security attribute formats to be supported shall be defined by the application(s), e.g. see annex A.

5.2.1 Compact format

The compact format is indicated by tag '8C' in the FCP. In the compact format an access rule consists of an AM byte and one or more SC bytes as defined in ISO/IEC 7816-9 [4].

The AM byte conveys two types of information. The interpretation of the AM byte itself, this is coded on b8 and the number of SC bytes following, this is equal to the number of bits set to '1' in bits b7-b1 in the AM byte. If b8 in the AM byte is set to '1' an SC byte must be supplied for each bit set to '1' in the AM byte (excluding b8). If b8 in the AM byte is set to '1' the usage of bits b7-b4 is proprietary.

When multiple sets of AM byte and one or more corresponding SC bytes are present in the value field they present an OR condition.

5.2.2 Expanded format

The expanded format is indicated by tag 'AB' in the FCP. In the expanded format an access rule consists of one AM_DO followed by a sequence of SC_DOs. The contents of the AM_DO is defined by the tag that it is indicated with, see ISO/IEC 7816-9 [4]. Tag '80' indicates that the AM_DO contains an AM byte. The sequence of SC_DOs following the AM_DO is relevant for all commands specified in the AM_DO. The different SC_DOs can form an OR or and AND condition as defined in ISO/IEC 7816-9 [4]. The following tag 'AB' in the FCP can contain a lot of data if the rule is complex.

The structure of the security attribute in expanded format is as follows:

Tag	length	AM_DO tag	AM_DO	SC_DO tag	SC_DO	AM_DO tag	AM_DO	SC_DO tag	SC_DO
'AB'		See ISO/IEC 7816-9 [4]		See ISO/IEC 7816-9 [4]		See ISO/IEC 7816-9 [4]		See ISO/IEC 7816-9 [4]	

5.2.3 Referenced to expanded format

In case the access rule is very complex and it applies to more than one file referencing to the expanded format can be used to indicate the access rule see ISO/IEC 7816-9 [4]. The referenced format is indicated in the FCP following tag '8B'. The access rule is stored in a file, EF_{ARR}. This file is a linear fixed file. The structure of the EF_{ARR} file is as follows:

Record Number (ARR)	Record Content (Access Rule)
'01'	AM_DO | SC_DO_1 | SC_DO_2 | AM_DO | SC_DO_3 | SC_DO_4 ….
'02'	AM_DO | SC_DO_1 | AM_DO | SC_DO_5 | SC_DO_6 ….

Referencing EF_{ARR} is based on the file ID. If a file with the file ID indicated in tag '8B' cannot be found in the current DF, the parent DF shall be searched for EF_{ARR}. This process shall continue until the EF_{ARR} is found or until an ADF or the MF is reached. When an EF_{ARR} is referred to in the FCP template of an ADF, the MF shall be used for searching this EF_{ARR}.

NOTE: There may be several EF_{ARR} containing access rules under the same DF. They are distinguished and referred to by their respective file-IDs.

The structure of the access rule referencing DO is as follows:

Tag	Length	Value
'8B'	'03'	File ID, record number
'8B'	'02' + n x '02'	File ID, SE ID_{n1}, Record number X, SE ID_{n2}, Record number Y, …..

Each record in EF_{ARR} contains a sequence of AM_DOs followed by SC_DOs. The content of the record is the rule that applies for access to the selected file.

5.3 PIN status indication

The status of a PIN that is used by an application for user verification shall be indicated in the FCP of the CREATE FILE command for an ADF or DF. In case the PIN status of a PIN already used is indicated in the PIN status template of the CREATE FILE command and its value is different from the current status of the parent DF the value indicated in the PIN status DO shall be ignored and the PIN status of the parent DF is used.

The PIN status information is indicated in the FCP in the PS template DO using tag 'C6'. The PS template DO conveys two types of data, first the PS_DO indicated by tag '90' that indicates the status of the PIN(s) enabled/disabled. The PS_DO is followed by one or more key reference data objects indicated by tag '83'. The PIN status may be encoded over several bytes. For each bit set to '1' the corresponding key reference (PIN) is enabled. The PS_DO is coded using a bitmap list. Bit b8 in the most significant byte corresponds to the first key reference indicated in tag '83' following the PS_DO. Bits b7-b1 are mapped to consecutive key references indicated by tag '83'. A key reference data object may be proceeded by a usage qualifier data object. The usage qualifier data object indicated by tag '95' indicates whether an enabled PIN needs to be verified. If the usage qualifier data object is given in the FCP of the CREATE FILE command for a DF this allows the verification of the key reference to be neglected even if it is enabled. The content of the usage qualifier is defined in table 1. From table 1 for user PIN verification the value to be used is '08'. See TS 102 221 [5] for an use case of the usage qualifier.

Table 1: Usage qualifier coding

b8 b7 b6 b5 b4	b3 b2 b1	Meaning
0 0 0 0 0	0 0 0	do not use the verification requirement for verification
1 - - - -	- - -	- use verification (DST,CCT) - use encipherment (CT) - use external authentication (AT)
- 1 - - -	- - -	- use computation (DST,CCT) - use decipherment (CT) - use internal authentication (AT)
- - 1 - -		- use SM response (CCT, CT, DST)
- - - 1 -	- - -	- use SM command (CCT, CT, DST)
- - - - 1	- - -	- use user authentication, knowledge based i.e. PIN for verification (Key Reference data)
- - - - -	1 - -	- use user authentication, biometric based
- - - - -	- x x	- RFU (default = 00)

The PS template DO is constructed as indicated in tables 2 and 3.

Table 2: PS Template DO structure

PS Template DO Tag	L	PS-DOTag	L	V PS-byte(s)	Key-reference Tag	L	V	Key-reference Tag	L	V
'C6'	L1	'90'	L2	see text above	'83'	'01'	see annex A	'83'	'01'	see annex A

Table 3: PS Template DO structure when usage qualifier used

PS Template DO Tag	L	PS-DO Tag	L	V PS-byte(s)	Usage Qualifier Tag	L	V	Key-reference Tag	L	V	Key-reference Tag	L	V
'C6'	L1	'90'	L2	see text above	'95'	'01'	see table 1	'83'	'01'	see annex A	'83'	'01'	see annex A

6 Description of the functions and commands

This clause gives a functional description of the commands, their respective responses, associated status conditions, error codes and their coding.

6.1 Coding of the commands

Table 4: Coding of the commands

Command	CLA	INS
CREATE FILE	'00'	'E0'
DELETE FILE	'00'	'E4'
DEACTIVATE FILE	'00'	'04'
ACTIVATE FILE	'00'	'44'
TERMINATE DF	'00'	'E6'
TERMINATE EF	'00'	'E8'
TERMINATE CARD USAGE	'00'	'FE'

The coding of the CLA-bytes shall be according to ISO/IEC 7816-4 [2], clause 5.4.1.

All bytes specified as RFU shall be set to '00' and all bits specified as RFU shall be set to 0.

These are the basic commands under the assumption of no secure messaging (SM). If SM is used, the Lc and data field must be adopted.

Other commands may be needed in order to execute the commands listed above (e.g. EXTERNAL AUTHENTICATE). If such commands are necessary, they shall be coded according to ISO/IEC 7816-4 [2] or ISO/IEC 7816-8 [3].

6.2 TLV objects

All TLVs described in the present document shall be supported by the ICC.

The sequence of mandatory TLV objects within the data field of any command specified in the present document shall be as in the description of the command.

According to the requirements of the application, the mandatory list of TLVs may be appended by one of the Tags '85' (Proprietary Information, see ISO/IEC 7816-4 [2]) or 'A5' (Proprietary Information Constructed, see ISO/IEC 7816-9 [4]).

Tag '85' or Tag 'A5' may be appended by other TLVs described in the present document or by any ISO/IEC or application dependent optional TLV object if necessary for a particular application.

6.3 CREATE FILE

6.3.1 Definition and scope

This function allows the creation of a new file under the current DF or ADF. The access condition for the CREATE FILE function of the current DF or ADF shall be fulfilled.

When creating an EF with linear fixed or cyclic structure the ICC shall directly create as many records as allowed by the requested file size.

After the creation of a DF, the current directory shall be on the newly created file. In case of an EF creation, the current EF shall be on the newly created file and the current directory is unchanged. After creation of an EF with linear fixed structure, the record pointer is not defined. After creation of an EF with cyclic structure, the current record pointer is on the last created record.

The memory space allocated shall be reserved for the created file.

This command can be performed only if logical channel 0 is selected and no other logical channel is open.

If an ADF is created, some instance has to take care of the administration of the application, e.g. updating the EF_{DIR} with the application ID. The CREATE FILE command does not take care of this administration by its own. The DF Name tag shall only provided in the command, if an ADF is created.

The CREATE FILE command shall initialize newly created EFs with 'FF'. The content of the whole newly created EF shall consist of bytes of this value. If, for another application, other default values are required, this default behaviour can be overwritten by specifying an appropriate TLV in the application dependent data TLV (tag '85' or 'A5') of the CREATE FILE command.

6.3.2 Command message

The CREATE FILE command message is coded according to table 5.

Table 5: CREATE FILE command message

Code	Value
CLA	As defined in ISO/IEC 7816-4 [2], b1and b2 set to 0
INS	'E0'
P1	'00'
P2	'00'
Lc	Length of the subsequent data field
Data field	Data sent to the ICC
Le	Not present

6.3.2.1 Parameters P1 and P2

P1 and P2 are set to '00' indicating: FileID and file parameters encoded in data.

6.3.2.2 Data field sent in the command message

6.3.2.2.1 Creating a DF

Table 6: Coding of the data field of the CREATE FILE command (in case of creation of a DF)

Value	M/O	Description	Length
'62'	M	Tag: FCP Template	1 byte
LL		Length (byte 3 to the end)	1 byte
'82'	M	Tag: File descriptor	1 byte
'02'		Length of file descriptor	1 byte
xx		File descriptor byte indicating DF, see table 7	1 byte
'21'	M	Data Coding Byte	1 byte
'83'	M	Tag: File ID	1 byte
'02'		Length of file ID	1 byte
xx xx		File ID	2 bytes
'84'	O	Tag: DF Name	1 byte
LL		Length of DF Name	1 byte
xx		DF Name	1 - 16 bytes
'8A'	M	Life Cycle Status Information (LCSI)	1 byte
'01'		Length of the LCSI	1 byte
xx		Life Cycle Status Information	1 byte
'8C' 'AB' '8B'	M	Tag: Security attributes: one of the following: Compact Expanded Referenced	1 byte
LL		Length of security attributes related data	1 byte
xx ... xx	M	Data for the security attributes	
'81'	M	Tag: Total file size	1 byte
X, X ≥2		Length of number	1 byte
xx ... xx		Number of data bytes	X bytes
"C6"	M	Tag: PIN Status Template DO	1 byte
LL		Length of PIN Status Template DO	1 byte
xx ... xx		PIN Status Template DO	X bytes
'85' or 'A5'	O	Tag: Proprietary, application dependent	1 byte
LL		Length of application dependent data	1 byte
		Application dependent data (see below)	
LL: indicates a length of a TLV object coded in one hexadecimal byte. xx: indicates one hexadecimal byte.			

Security attributes:

At least the key references that are used to allow access during the operational phase of the IC card are to be supplied in the security attributes.

Tag '81': Total file size:

Amount of physical memory allocated for the DF or ADF. The amount of memory specifies, how much memory will be available within the currently created DF or ADF to create EFs or other DFs. It shall include the memory needed for structural information for these EFs and DFs. The size of the structural information for the created DF shall not be included.

Some card implementations support dynamic allocation of memory (memory is allocated for the whole UICC), and therefore will ignore this TLV object.

By specifying a value other than '0000' it is possible, to indicate the requested amount of physical memory for the content of a DF or an ADF. This amount is taken from the memory allocated for the current DF.

The behaviour of the ICC for a value equal to '0000' is for further study.

Tag '82': File Descriptor with Data Coding Byte

The File Descriptor Byte shall be coded according to table 7.

Table 7: File descriptor byte

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	X	-	-	-	-	-	-	**File accessibility**
0	0	-	-	-	-	-	-	Not shareable file
0	1	-	-	-	-	-	-	Shareable file
0	-	X	X	X	-	-	-	**File type**
0	-	0	0	0	-	-	-	Working EF
0	-	0	0	1	-	-	-	Internal EF
0	-	0	1	0	-	-	-	RFU
0	-	0	1	1	-	-	-	
0	-	1	0	0	-	-	-	
0	-	1	0	1	-	-	-	
0	-	1	1	0	-	-	-	
0	-	1	1	1	-	-	-	DF or ADF
0	-	-	-	-	X	X	X	**EF structure**
0	-	-	-	-	0	0	0	No information given
0	-	-	-	-	0	0	1	Transparent
0	-	-	-	-	0	1	0	Linear fixed
0	-	-	-	-	0	1	1	RFU
0	-	-	-	-	1	0	0	
0	-	-	-	-	1	0	1	
0	-	-	-	-	1	1	0	Cyclic
0	-	-	-	-	1	1	1	RFU
1	X	X	X	X	X	X	X	RFU

The data coding byte can be used differently according to table 86 in ISO/IEC 7816-4 [2]. For the present document, the value '21' (proprietary) shall be used and shall not be interpreted by the ICC.

Tag '84': DF Name:

This TLV shall only be provided if an ADF is created. The DF name is a string of bytes which is used to uniquely identify a dedicated file in the card.

Tag '8A': Life Cycle Status Information LCSI

Table 8: Coding of Life Cycle Status Integer

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	No information given
0	0	0	0	0	0	0	1	Creation state
0	0	0	0	0	0	1	1	Initialization state
0	0	0	0	0	1	-	1	Operational state - activated
0	0	0	0	0	1	-	0	Operational state - deactivated
0	0	0	0	1	1	-	-	Termination state
≠ 0				X	X	X	X	Proprietary
Any other value								RFU

This TLV specifies the status of the file after creation.

The initialization state can be used to set the file into a specific security environment for administrative purposes. See ACTIVATE command.

Tag "C6": PIN Status Template DO

The PIN Status Template DO shall be coded according to clause 5.3.

6.3.2.2.2 Creating an EF

Table 9: Coding of the data field of the CREATE FILE command (in case of the creation of an EF)

Value	M/O	Description	Length
'62'	M	Tag: FCP Template	1 byte
LL		Length (next byte to the end)	1 byte
'82'	M	Tag: File descriptor File descriptor byte followed by data coding byte or File descriptor byte followed by data coding byte and record length, coded on 2 bytes	1 byte
LL		Length of the data (indicating 2 or 4 bytes)	1 byte
xx	M	File Descriptor Byte, see table 7	1 byte
'21'	M	Data Coding Byte	1 byte
xx xx	O	only available, if a record structured file (i.e. for linear fixed or cyclic file) is created	2 bytes
'83'	M	Tag: File ID	1 byte
'02'		Length of the File ID	1 byte
xx xx		File ID	2 bytes
'8A'	M	Life Cycle Status Information (LCSI)	1 byte
'01'		Length of the LCSI	1 byte
xx		Life Cycle Status Information	1 byte
'8C' 'AB' '8B'	M	Tag: Security attributes: one of the following: Compact Expanded Referenced	1 byte
LL		Length of security attributes related data	1 byte
xx ... xx	M	Data for the security attributes	
'80'	M	Tag: File size	1 byte
'02'		Length of the number of bytes	1 byte
xx xx		Number of data bytes	2 bytes
'88'	O	Tag: Short File Identifier	1 byte
LL		Length of Short File Identifier	1 byte
xx		Short File Identifier	1 byte
'A5'	O	Tag proprietary, application dependent	1 byte
LL+3		Length of application dependent data	1 byte
		Application dependent data (see below)	
'C0'		Tag: Special file information (file status byte) (within proprietary tag)	1 byte
'01'		Length	1 byte
xx		Special file information (file status byte)	1 byte
xx ... xx		Additional application dependent data (see annex)	LL bytes

Tag '80' File size:

File size indicates the number of bytes allocated for the body of the file (i.e. it does not include structural information). In the case of an EF with linear or cyclic structure, it is the record length multiplied by the number of records of the EF.

Tag '82': File Descriptor

The File Descriptor Byte shall be coded according to table 7.

The data coding byte can be used differently according to table 86 in ISO/IEC 7816-4 [2]. For the present document, the value '21' (proprietary) shall be used and shall not be interpreted by the ICC.

The record length shall be present if a record structured file (i.e. for linear fixed or cyclic files) is selected. In this case it indicates the length of the records on 2 bytes. Most significant byte comes first in the value field.

Tag '8A': Life Cycle Status Information LCSI

Table 10: Coding of Life Cycle Status Integer

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	No information given
0	0	0	0	0	0	0	1	Creation state
0	0	0	0	0	0	1	1	Initialization state
0	0	0	0	0	1	-	1	Operational state - activated
0	0	0	0	0	1	-	0	Operational state - deactivated
0	0	0	0	1	1	-	-	Termination state
≠ 0				X	X	X	X	Proprietary
Any other value								RFU

This TLV specifies the status of the file after creation.

The initialization state can be used to set the file into a specific security environment for administrative purposes. See ACTIVATE command.

Tag '88' Short File Identifier:

The short file identifier is coded from bits b8 to b4. Bits b3,b2,b1 = 000.

The following 3 cases shall be supported by the ICC if the ATR indicates that the ICC supports selection by SFI:

- Tag '88' is missing in the CREATE FILE command: The lower five bits of the file ID are used as the short file identifier by the EF;
- Tag '88' is available in the CREATE FILE command, there is no value part in the TLV: Short file identifier not supported by the EF;
- Tag '88' is available in the CREATE FILE command, there is a short file identifier value in the TLV: Short file identifier is supported by the EF.

Tag 'C0' Special File Information (file status byte) within the proprietary TLV (tag 'A5').

Table 11: Coding of the Special File Information

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	X	0	0	0	0	0	0	Low update activity
1	X	0	0	0	0	0	0	High update activity
X	0	0	0	0	0	0	0	Not readable or updatable when deactivated
X	1	0	0	0	0	0	0	Readable and updatable when deactivated
Any other value								RFU

6.3.3 Response message

6.3.3.1 Data field returned in the response message

The data field of the response message is not present.

6.3.3.2 Status conditions returned in the response message

The following status conditions shall be returned by the ICC.

Table 12: CREATE FILE successful status conditions

SW1	SW2	Meaning
Normal processing		
'90'	'00'	- normal ending of the command
'63'	'0X'	- command successful but after using an internal update retry routine 'X' times
Errors		
'62'	'83'	- in contradiction with activation status
'65'	'81'	- memory problem
'67'	'00'	- incorrect length field
'69'	'82'	- security status not satisfied
'69'	'85'	- Condition of use not satisfied: - more than 1 logical channel open - selected logical channel not channel 0
'6A'	'84'	- not enough memory space
'6A'	'89'	- file ID already exists
'6A'	'8A'	- DF name already exists (only for creation of a DF and if a DF Name TLV is used)
'6B'	'00'	- incorrect parameter P1 or P2
'6D'	'00'	- command not supported or invalid
'6E'	'00'	- wrong instruction class given in the command
'6F'	'00'	- technical problem with no diagnostic given
'6F'	'FX'	- technical problem, X (proprietary) provides diagnostic

6.4 DELETE FILE

6.4.1 Definition and scope

This command initiates the deletion of a referenced EF immediately under the current DF, or a DF with its complete subtree.

The access condition for the DELETE FILE function of the current DF shall be fulfilled.

After successful completion of this command, the deleted file can no longer be selected. The resources held by the file shall be released and the memory used by this file shall be set to the logical erased state. It shall not be possible to interrupt this process in such a way that the data can become recoverable.

This command can be performed only if logical channel 0 is selected and no other logical channel is open.

If an ADF is deleted, some instance has to take care of the administration of the application, e.g. deleting the application ID entry in the EF_{DIR}. The DELETE FILE command does not take care of this administration by its own.

6.4.2 Command message

The DELETE FILE command message is coded according to table 13.

Table 13: DELETE FILE command message

Code	Value
CLA	As defined in ISO/IEC 7816-4 [2], b1 and b2 set to 0
INS	'E4'
P1	'00'
P2	'00'
Lc	Length of the subsequent data field
Data field	Data sent to the ICC
Le	Not present

6.4.2.1 Parameters P1 and P2

P1 and P2 are set to '00', indicating the selection by file identifier as defined in ISO/IEC 7816-4 [2] for SELECT FILE command.

6.4.2.2 Data field sent in the command message

Table 14: Coding of the data field of the DELETE FILE command

Bytes	Description	Length
1 – 2	File ID (optional)	2 bytes

6.4.3 Response message

6.4.3.1 Data field returned in the response message

The data field of the response message is not present.

6.4.3.2 Status conditions returned in the response message

The following status conditions shall be returned by the ICC.

Table 15: DELETE FILE status conditions

SW1	SW2	Meaning
Normal processing		
'90'	'00'	- normal ending of the command
Errors		
'63'	'0X'	- command successful but after using an internal update retry routine 'X' times
'65'	'81'	- memory problem
'67'	'00'	- incorrect length field
'69'	'82'	- security status not satisfied
'69'	'85'	- Condition of use not satisfied: - more than 1 logical channel open - selected logical channel not channel 0
'6B'	'00'	- incorrect parameter P1 or P2
'6D'	'00'	- command not supported or invalid
'6E'	'00'	- wrong instruction class given in the command
'6F'	'00'	- technical problem with no diagnostic given
'6F'	'FX'	- technical problem, X (proprietary) provides diagnostic

6.5 DEACTIVATE FILE

The support of this command is mandatory for an ICC compliant to the present document.

Refer to TS 102 221 [5] for the specification of the command.

6.6 ACTIVATE FILE

The support of this command is mandatory for an ICC compliant to the present document.

Refer to TS 102 221 [5] for the specification of the command.

This command initiates the transition of a file from:

- the initialization state; or
- the operational state (deactivated).

To the operational state (activated).

6.7 TERMINATE DF

6.7.1 Definition and scope

The TERMINATE DF command initiates the irreversible transition of the currently selected DF into the termination state (coding see LCSI coding in ISO/IEC 7816-9 [4]).

Following a successful completion of the command, the DF is in terminated state and the functionality available from the DF and its subtree is reduced. The DF shall be selectable and if selected the warning status SW1/SW2='6285' (selected file in termination state) shall be returned.

Further possible actions are not defined.

The intend of DF termination is generally to make the application unusable by the cardholder.

The command can be performed only if the security status satisfies the security attributes defined for this command.

This command can be performed only if logical channel 0 is selected and no other logical channel is open.

NOTE: An appropriate security rule is to be setup and fulfilled in order to execute this command.

6.7.2 Command message

The TERMINATE DF command message is coded according to table 16.

Table 16: TERMINATE DF command message

Code	Value
CLA	As defined in ISO/IEC 7816-4 [2], b1 and b2 set to 0
INS	'E6'
P1	'00'
P2	'00'
Lc	Not present
Data field	Not present
Le	Not present

6.7.2.1 Parameters P1 and P2

P1 and P2 are set to '00'.

6.7.2.2 Data field sent in the command message

The data field of the command message is not present.

6.7.3 Response message

6.7.3.1 Data field returned in the response message

The data field of the response message is not present.

6.7.3.2 Status conditions returned in the response message

The following status conditions shall be returned by the ICC.

Table 17: TERMINATE DF status conditions

SW1	SW2	Meaning
Normal Processing		
'90'	'00	- normal ending of the command
Errors		
'65'	'81'	- memory problem
'67'	'00'	- incorrect length field
'69'	'82'	- security status not satisfied
'69'	'85'	- Condition of use not satisfied: - more than 1 logical channel open - selected logical channel not channel 0
'6B'	'00'	- incorrect parameter P1 or P2
'6D'	'00'	- command not supported or invalid
'6E'	'00'	- wrong instruction class given in the command
'6F'	'00'	- technical problem with no diagnostic given
'6F'	'FX'	- technical problem, X (proprietary) provides diagnostic

6.8 TERMINATE EF

6.8.1 Definition and scope

The TERMINATE EF command initiates the irreversible transition of the currently selected EF into the termination state (coding see LCSI coding in ISO/IEC 7816-9 [4]).

The command can be performed only if the security status satisfies the security attributes defined for this command.

This command can be performed only if logical channel 0 is selected and no other logical channel is open.

6.8.2 Command message

The TERMINATE EF command message is coded according to table 18.

Table 18: TERMINATE EF command message

Code	Value
CLA	As defined in ISO/IEC 7816-4 [2], b1 and b2 set to 0
INS	'E8'
P1	'00'
P2	'00'
Lc	Not present
Data field	Not present
Le	Not present

6.8.2.1 Parameters P1 and P2

P1 and P2 are set to '00'.

6.8.2.2 Data field sent in the command message

The data field of the command message is not present.

6.8.3 Response message

6.8.3.1 Data field returned in the response message

The data field of the response message is not present.

6.8.3.2 Status conditions returned in the response message

The following status conditions shall be returned by the ICC.

Table 19: TERMINATE EF status conditions

SW1	SW2	Meaning
Normal Processing		
'90'	'00	- normal ending of the command
Errors		
'65'	'81'	- memory problem
'67'	'00'	- incorrect length field
'69'	'82'	- security status not satisfied
'69'	'85'	- Condition of use not satisfied: - more than 1 logical channel open - selected logical channel not channel 0
'6B'	'00'	- incorrect parameter P1 or P2
'6D'	'00'	- command not supported or invalid
'6E'	'00'	- wrong instruction class given in the command
'6F'	'00'	- technical problem with no diagnostic given
'6F'	'FX'	- technical problem, X (proprietary) provides diagnostic

6.9 TERMINATE CARD USAGE

6.9.1 Definition and scope

The TERMINATE CARD USAGE command initiates the irreversible transition of the ICC into the termination state. Use of this command gives an implicit selection of the MF.

The termination state should be indicated in the ATR (see ISO/IEC 7816-4 [2]) using the coding shown in table 2 of ISO/IEC 7816-9 [4].

Following a successful completion of the command, no other than the STATUS command shall be supported by the ICC.

The intend of ICC termination is generally to make the ICC unusable by the cardholder.

The command can be performed only if the security status satisfies the security attributes defined for this command.

NOTE: An appropriate security rule is to be setup and fulfilled in order to execute this command.

6.9.2 Command message

The TERMINATE CARD USAGE command message is coded according to table 20.

Table 20: TERMINATE CARD USAGE command message

Code	Value
CLA	As defined in ISO/IEC 7816-4 [2], b1 and b2 set to 0
INS	'FE'
P1	'00'
P2	'00'
Lc	Not present
Data field	Not present
Le	Not present

6.9.2.1 Parameters P1 and P2

P1 and P2 are set to '00'.

6.9.2.2 Data field sent in the command message

The data field of the command message is not present.

6.9.3 Response message

6.9.3.1 Data field returned in the response message

The data field of the response message is not present.

6.9.3.2 Status conditions returned in the response message

The following status conditions may be returned by the ICC.

Table 21: TERMINATE CARD USAGE status conditions

SW1	SW2	Meaning
Normal Processing		
'90'	'00	- normal ending of the command
Errors		
'65'	'81'	- memory problem
'67'	'00'	- incorrect length field
'69'	'82'	- security status not satisfied
'69'	'85'	- Condition of use not satisfied: - more than 1 logical channel open - selected logical channel not channel 0
'6B'	'00'	- incorrect parameter P1 or P2
'6D'	'00'	- command not supported or invalid
'6E'	'00'	- wrong instruction class given in the command
'6F'	'00'	- technical problem with no diagnostic given
'6F'	'FX'	- technical problem, X (proprietary) provides diagnostic

Annex A (normative): Application specific data for TS 102 221 application

A.1 Access condition mapping

For access condition mapping, refer to clause "Access condition mapping" in TS 102 221 [5].

A.2 Proprietary tag coding

For coding of the proprietary tag 'A5', refer to clause "Proprietary information" in TS 102 221 [5].

A.3 Security attribute formats

For definition of the security attribute formats refer to clause "Security architecture" in TS 102 221 [5].

Annex B (informative): Security attributes mechanisms and examples

B.1 Coding

Two codings are defined:

- a compact coding based on bitmaps;
- an expanded coding which is an extension of the compact coding with intermediate scope containing bitmap and TLV list management.

The security conditions for bits not set to 1 in the AM byte are set to NEVer by default.

B.2 Compact format

The compact format access rule is indicated by tag '8C' in the FCP. An access rule in this format is encoded with:

- an AM byte as defined in ISO/IEC 7816-9 [4];
- one or more SC bytes as defined in ISO/IEC 7816-9 [4].

B.2.1 AM byte

The AM byte conveys two types of information:

- interpretation of the AM byte itself;
- number of SC bytes in the access rule.

If b8 in the AM byte is set to '0' the AM byte is followed by a number of SC bytes equal to the number of bits set to '1' in the AM byte (excluding b8). Each SC bytes codes the conditions relevant to a set of commands, in the same order (b7 to b1) as in the AM byte. When b8 is set to '1' the usage of b7-b4 is proprietary.

When multiple sets of an AM byte and one or more corresponding SC bytes are present in the value field of the DO, tag '8C' they represent an OR condition.

B.2.2 SC byte

The SC byte specifies which security mechanisms are necessary to conform to the access rules, see ISO/IEC 7816-9 [4]. The 4 most significant bits (b8-b5) indicates the required security condition. A SE may be specified in bits b4–b1. If a SE is specified the mechanisms that may be defined in it for external authentication, user authentication and command protection shall be used, if indicated by bits b4-b1.

If bit b8 is set to '1' all conditions in bits b7-b5 shall be satisfied. If bit b8 is set to '0' at least one of the conditions set in bits b7-b5 shall be satisfied. If b7 is set to '1', the CRT of the SE indicated in bits b4-b1 describes whether secure messaging shall apply to the command APDU, the response APDU or both.

B.2.3 Examples

For EFs with the access condition ALW for READ and UPDATE the security attribute would look as follows:

Tag	L	AM	SC	SC
'8C'	'03'	'03'	'00'	'00'

For EFs with the access condition ALW for READ the security attribute would look as follows:

Tag	L	AM	SC
'8C'	'02'	'01'	'00'

This rule is applicable to EF_{ICC}, e.g. for EF_{DIR} the access rule would be as follows. The ADM condition is indicated by a user authentication. The key reference is implicitly known.

Tag	L	AM	SC	SC
'8C'	'03'	'03'	'90'	'00'

B.3 Expanded format

In the expanded format AM_DOs and SC_DOs are used to create the access rules. The compact format access rule is indicated by tag 'AB' in the FCP. An access rule in this format is encoded with:

- n AM_DO followed by a sequence of;
- C_DOs.

B.3.1 AM_DO

The AM_DO is defined in ISO/IEC 7816-9 [4]. The content of the AM_DO is defined by the tag value. Tag '80' indicates that the AM_DO contains an AM byte. Tags '81'-'8F' indicates that the AM_DO contains a command description. Tag '9C' indicates that the AM_DO contains a proprietary state machine description.

When multiple sets of AM_DOs and one or more corresponding SC_DOs are present in the value field of the DO following tag '8B' they represent an OR condition.

B.3.2 SC_DO

The SC_DO is defined in ISO/IEC 7816-9 [4]. The SC_DO definition contains an OR and an AND template. Several SC_DOs may be attached to a particular operation.

- If the SC_DOs are encapsulated in an OR template, then only one of the security conditions has to be fulfilled for the operation to be allowed.
- If the SC_DOs are not to be encapsulated in an OR template or if the SC_DOs are encapsulated in an AND template, then all security conditions shall be fulfilled before the operation is allowed.

B.3.3 Access rule referencing

Access rules in expanded format (AM_DOs and SC_DOs) may be stored in a linear fixed/variable EF, each record contain on ore more rules, as defined in ISO/IEC 7816-9 [4]. The access rule file may be an internal file, referenced implicitly, or may be referenced explicitly, e.g. by a file ID. The access rule stored in a file is indicated by tag '8B' in the FCP. The value of this DO contains at least one record number, called ARR. The record can contain:

- a single byte containing the record number of the rule, valid if the access rule is (implicitly) known;
- three bytes containing two bytes with the File ID of the access rule file followed by one byte with the record number for the access rule;
- if the value field is coded with a length of 2 + n x 2, for n > 1, it contains the File ID and one or more SEID/ARR pairs, where the SEID codes the SE number on one byte. For each SE, the access rules indicated in the ARR following its SE# are valid.

B.3.4 Examples

The access rule for EF_{PL} would look as follows. The READ and SEARCH access condition is ALWays. The UPDATE access condition is Application1 PIN or Application2 PIN.

Tag	L	AM_DO Tag	L	V	OR Tag	L	SC_DO Tag	L	Key Ref Tag	L	V	Usage Qualifier Tag	L	V	SC_DO Tag	L	Key Ref Tag	L	V	Usage Qualifier Tag	L	V	AM_DO Tag	L	V	SC_DO Tag	L
'AB'	'1B'	'80'	'01'	'02'	'A0'	'10'	'A4'	'06'	'83'	'01'	'01'	'95'	'01'	'08'	'A4'	'06'	'83'	'01'	'02'	'95'	'01'	'08'	'80'	'01'	'01'	'90'	'00'

Annex C (informative): Change history

The table below indicates all changes that have been incorporated into the present document since it was created by EP SCP.

Change history								
Date	**Meeting**	**EP SCP Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**
2000-05	SCP-01	9-00-0149	-		-	Final draft approved for publication		3.0.0
2000-11	SCP-03	9-00-0437	002		F	Alignments with TS 102 221 regarding CREATE FILE command. Note that CR 002 includes corrections which had originally been agreed in CR 001 in T3-000347.	3.0.0	3.1.0
		9-00-0438	003		F	Alignments with TS 102 221 regarding access conditions		
		9-00-0439	004		F	Alignments with TS 102 221 concerning editorial changes		
		9-00-0436	005		F	Administrative command: proprietary information added		
2001-05	SCP-05	SCP-010120	006		F	Correction of the annex applying to the SIM	3.1.0	3.2.0
		SCP-010144	007		F	Allocation of memory for a file		
2001-10	SCP-07	SCP-010305	008		F	Correction of the CREATE FILE command	3.2.0	3.3.0
2002-09	SCP-11	SCP-020256	009		F	Clarification of the SFI management by the CREATE FILE command	3.3.0	3.4.0

History

Document history		
V3.0.0	May 2000	Publication
V3.1.0	January 2001	Publication
V3.2.0	May 2001	Publication
V3.3.0	October 2001	Publication
V3.4.0	October 2002	Publication