GemXplore 3G V2
3G and GSM Operation Modes

Reference Manual

GEMPLUS, B.P. 100, 13881 GEMENOS CEDEX, FRANCE.

Tel: +33 (0)4.42.36.50.00 Fax: +33 (0)4.42.36.50.90

Printed in France.

Document Reference: DOC107422A2

Document Version: 1.2

July 19, 2002

Contents

List of Figures

List of Tables

Introduction

This document describes the behavior of 3G/GSM sessions and 3G/GSM interworking for the GemXplore 3G V2 product. The GemXplore 3G V2 card behaves like a USIM (Universal Subscriber Identity Module) in a 3G handset and like a SIM (Subscriber Identity Module) in a GSM handset.

This document also describes the logical organization and the command set of the Universal Subscriber Identity Module (USIM) for the 3G application and the SIM part for the GSM application, as supplied by Gemplus card international and its affiliate companies.

The UICC USIM specification described in this document for 3G/GSM interworking fully complies with the reference recommendations documents, ETSI TS 102.221 version 4.2.0 and 3G TS 31.102 version 4.1.0 as established by the ETSI and 3GPP group respectively.

The SIM phase 2+ specification described in this document for 3G/GSM interworking fully complies with the reference recommendations document GSM 11.11 as established by the ETSI-GSM group.

This document is broadly divided into two parts:

- The first part describes the internal organization and functional mechanisms which help the user to understand the behavior of the SIM/USIM.
- The second part lists the operational administrative command sets, with their detailed syntax.

Who Should Read This Book

This manual assumes that you are familiar with smart cards, smart card reader technologies, and cryptography techniques. Reading the ISO/IEC 7816-3, ISO/IEC 7816-4 and EN726-3 standards will also prove useful.

How This Book Is Organized

This manual describes the operational and structural features of GemXplore 3G V2, the operating system used by Gemplus 3G V2 cards which known as the UICCs. GemXplore 3G V2 is fully compliant with 3GPP specifications. GemXplore 3G V2 operates over the entire 3V - 5V range in compliance with the ETSI TS 102 221 specification.

GemXplore 3G V2 Card Architecture

The hardware (that is, the chip) provides the card resources (for example, ROM, RAM, EEPROM, processing power).

GemXplore 3G V2 product is compliant with Java Card 2.1 for the operating system.

File Structure and Management

GemXplore 3G V2 manages file structures with up to four levels of directories which allows it to handle multi-level applications.

GemXplore 3G V2 uses three types of files:

- Transparent files to store non-formatted data (for example, secret codes).
- Linear fixed files to store formatted data (for example, Fixed Dialing Numbers).
- Cyclic files to store formatted data in chronological order (for example, Accumulated Call Meters).

Depending on the type of file, data may be read and updated using absolute or relative addressing methods.

File management features (file types, file selection, accessing data in a file, and file contents) are defined in the *3G TS 31.102 version 4.1.0*, the *ETSI TS 102.221 version 4.2.0* and *ETSI TS 102.222 version 3.2.0* specifications.

Data Security and Integrity

GemXplore 3G V2 offers enhanced data integrity features with, in particular, a back-up mechanism for sensitive data (secret code files, secret key files and file descriptors).

Security features (algorithms and processes, and file access conditions) are defined in the *3G TS 31.102 version 4.1.0*, the *ETSI TS 102.221 version 4.2.0* and *ETSI TS 102.222 version 3.2.0* specifications.

Communication Protocol

GemXplore 3G V2 cards send and receive data under the T=0 protocol, in accordance with the ISO 7816-3 standard.

Command Set

GemXplore 3G V2 offers a complete command set which is composed of three types of commands:

- Those defined in the *ETSI TS 102.221 version 4.2.0* and *ETSI TS 102.222 version 3.2.0* specification, referred to as 3GPP commands.
- Those defined in ETSI TS 11.11 specification, referred to as GSM commands.
- Those defined by Gemplus, referred to as administrative commands. These commands are divided into three groups: those based on ETSI/TE9 (EN 726-3) specifications, those based on the ISO 7816-4 standard, and Gemplus proprietary commands. The administrative command set is used for personalization purposes, and includes advanced commands (for example, **Create File** and **Delete**) allowing operators to format cards according to specific customer requirements.

3G and GSM Interworking

This section describes the different cases of interaction between an Identity Module (GSM-SIM or a 3G-USIM) and the GSM or 3G mobile equipment with a special focus on the different situations that can apply in a mixed GSM/3G network.

Conventions

The following conventions are used in this document:

Numeric values. By default, numeric values are expressed in decimal notation.

- Binary numbers are followed by the ‘b’ character. For example, the decimal value 13 is expressed in binary as **1101b**.
- Hexadecimal numbers are followed by the ‘h’ character. For example, the decimal value 13 is expressed in hexadecimal as **0Dh**.

RFU values. The value 00h is assigned to each RFU (Reserved for Future Use) byte.

Bit Numbering. A byte consists of 8 bits, b_7 to b_0, where b_7 is the most significant bit and b_0 the least significant bit, as shown below:

One byte	b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0

Byte numbering. A string of n bytes consists of n number of concatenated bytes: Bn-1 Bn-2 ...B1B0.
Bn is the most significant byte and B1 is the least significant byte:

String on n bytes	B_{n-1}	B_{n-2}	...	B_3	B_2	B_1	B_0

Not Used (NU). When NU is included in a command, the value 0 is masked in the operation system.

Contact our Hotline

If you don't find the information you need in this manual, or if you find errors, contact the Gemplus hotline by phone, fax, or email. In your email, please include the document reference number, your job function, and the name of your company. (You will find the document reference number at the bottom of the legal notice on the inside front cover.)

Corporate and EMEA

Hotline: +33 (0)4 42 36 50 50

Hot Fax: +33 (0)4 42 36 50 98

Email: hotline@gemplus.com

Americas

Hotline: 1 (877) 436-7233

Hot Fax: 1 (215) 390-1586

Email: hotlineusa@gemplus.com

From our Web Site

http://www.gemplus.com

1

File Structure

GemXplore 3G V2 cards have a hierarchical file structure. Four categories of files are handled by the operating system:

- Master File (MF)
- Application Dedicated Files (ADF)
- Dedicated Files (DFs)
- Elementary Files (EFs)

Each file contains a descriptor which holds information about the file's structure and attributes (for example, access conditions). File descriptors are managed internally by the operating system, but file information can be retrieved using the **Get Response** command after a **Select** command.

Each file is assigned a unique file identifier coded on two bytes. This identifier is used by the operating system for file selection. Files belonging to the same parent file cannot have the same identifier.

File	Code	Category
Master File	MF	The root of the file system which contains DFs, EFs, and defines Level 0.
Dedicated Files	DF	Functional grouping of files which can be the parent of DFs or EFs.
Application Dedicated Files	ADF	A DF that contains all the DFs and EFs which define 3G application.
Elementary Files	EF	System or application data units under an MF, DF, or ADF.

Table 1 - GemXplore 3G V2 File Categories

The following figure illustrates the relationship between the categories of files.

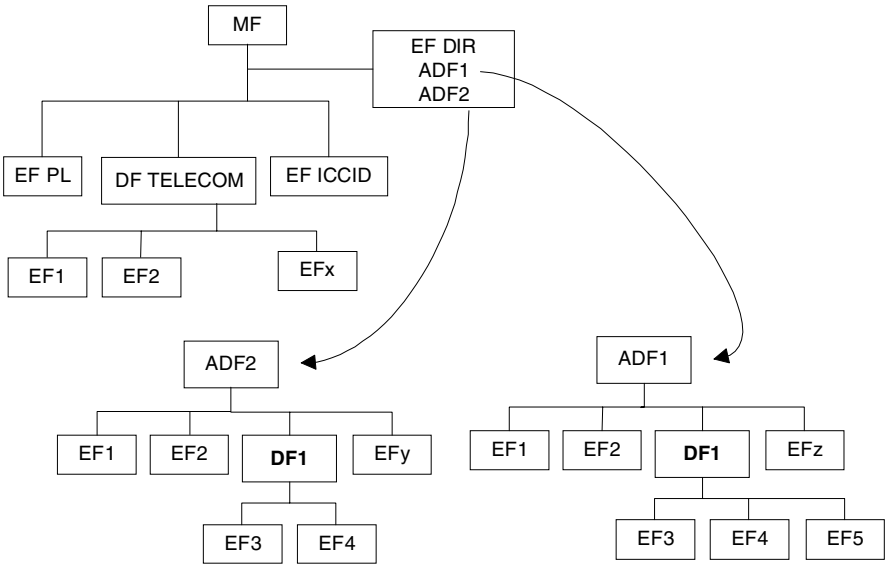

Figure 1 - GemXplore 3G V2 Card File Structure

Master File

All cards have one mandatory Master File (MF) which is the parent of the dedicated files and elementary files on the first level of the hierarchical file structure. The master file handles the allocation of the entire EEPROM memory. The MF contains dedicated files, elementary files or application dedicated files. The identifier of the master file is 3F 00h.

Application Dedicated Files

Application Dedicated Files (ADFs) contain all the DFs and EFs that are required by a particular application. The application's files are addressed through the ADF. The ADFs in turn are addressed through a special EF, EFDIR (2F 00h) located directly under the MF. In EFDIR, each application is identified by an Application ID (AID).

ADFs are visible only in a 3G session.

Dedicated Files

Dedicated files (DFs) are not only used to group elementary files but may also contain other nested DFs. A DF's memory allocation is defined when it is first created.

Note:

- The number of nested DF levels is limited to four including the MF level.
- The number of DFs in the card that can be managed by the OS is limited to 255.

Certain identifiers are reserved for specific DFs. On the first level, these specific DFs include DFTELECOM (7F 10h) which contains telecommunication service-related information. There are also a number of other reserved DF identifiers. See the *ETSI TS 102.221 version 4.2.0, ETSI TS 102.222 version 3.2.0* and *3G TS 31.102 version 4.1.0* specifications for further details.

Elementary Files

There are three types of elementary files (EFs): transparent elementary files, linear fixed elementary files, and cyclic elementary files. All elementary files are made up of both a descriptor and a body. The body is used to store special information or application data. The descriptor contains the system information for the parent file. In the rest of this manual, when reference is made to a file, no distinction will be made between the body and the descriptor.

The operating system supports the following elementary file structures:

- Transparent structure: the interface to the file shows a sequence of data units. Such files are referred to as transparent files.
- Record structure: the interface to the file shows a sequence of individually identifiable records. These files include linear fixed and cyclic files.

Note: The number of EFs under a DF (or the MF), that can be managed by the operating system is limited by the available memory in the parent DF and must not exceed 255.

Transparent Elementary Files

A transparent EF consists of a sequence of bytes. Access to the data is obtained by specifying an offset from the beginning of the body of the EF followed by a string length. See “Chapter 2 - Accessing Data”.

In the GemXplore 3G V2 a transparent EF can be created with a size limited only by the size of the remaining available memory.

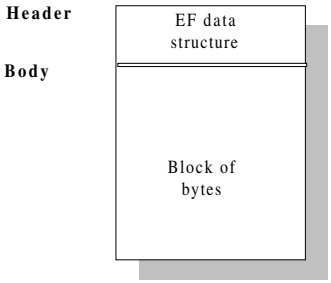

Figure 2 - Transparent EF Structure

The transparent files in GemXplore 3G V2 cards are used to store application data. However, they also include a number of specialized transparent files such as key files (EFKEY) and secret code files (EFPIN and EFADM). See “Specialized EF Structures” on page 6 for further details on these files.

Linear Fixed Elementary Files

Linear fixed elementary files are made up of a set of fixed-length records. Linear fixed files can contain up to 254 records, including any extensions, and the records can be up to 255 bytes long. “Figure 3 - Linear Fixed EF Structure” shows the structure of a linear fixed EF.

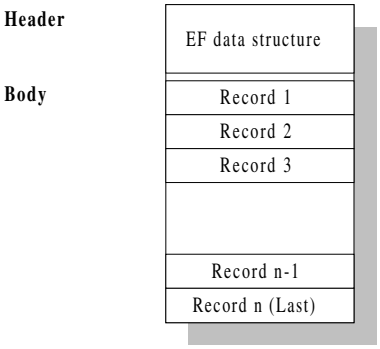

Figure 3 - Linear Fixed EF Structure

Records in linear fixed elementary files are accessed using either absolute or relative addressing, or by pattern seeking. See “Chapter 2 - Accessing Data”.

Cyclic Elementary Files

Cyclic elementary files contain a sequence of fixed-length records of equal length which are used to store data in chronological order. Cyclic elementary files can contain a maximum of 254 records. Each record can be up to 254 bytes long. The last record created is logically contiguous with the first record created. Access to the records in cyclic EFs is obtained using either absolute or relative addressing methods. See “Chapter 2 - Accessing Data”. The **Update Record** and **Increase** commands overwrite the oldest record (which then becomes record 1, all other record numbers being incremented by 1). As a result, the last updated record containing the newest data is record number 1, and the oldest data is held in the record number N.

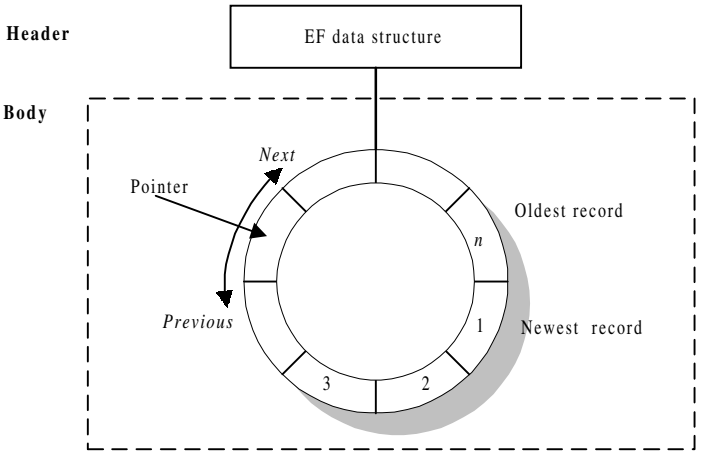

Figure 4 - Cyclic EF Structure Specialized EF Structures

Specialized EF Structures

GemXplore 3G V2 uses the following types of elementary files:

- Application Directory (EFDIR)
- Secret Code EFs (EFPIN and EFADM)
- Access Reference Rule EFs (EFARR)
- Key EFs (EFKEY)
- Authentication Configuration EFs (EFAUTHPARAM)
- EFSQN
- EFAUTHCOUNT
- EFMAP
- EFSMS SYSTEM
- EFSMS LOG

Each file type has a pre-defined structure.

EFDIR provides a list of applications contained in the card. All applications are addressed using this list.

EFPIN and EFADM contain the secret codes used to protect information in the card.

The security of the GemXplore 3G V2 is also provided through the association of the EFARR Access Rule Referencing Security Attributes. For more information on the Security Attributes, please read “Chapter 3 - 3G Data Security”.

EFKEY and EFAUTHPARAM are files related to 3G network authentication. For more information on this procedure, please read “Chapter 4 - 3G Network Security”.

EFSQN contains the 32 element array of the previously accepted sequence numbers.

EFAUTHCOUNT contains a counter whose value is decreased each time a **GSM Run Algorithm** or a 3G **Authentication** command is executed.

EFMAP contains information related to addressing for files that are mapped. For more information on this mechanism, please see “Chapter 11 - 3G and GSM Interworking”.

EFSMS SYSTEM contains system information. Synchronization counter used for OTA security, notification if a script has been executed successfully, unsuccessfully or downloading is in progress, and status for the script execution.

EFSMS LOG contains the addresses of servers, which have the permission to send executable scripts to the card.

Application Directory EF (EFDIR)

This file is a linear fixed EF and is located under the master file. It contains a list of applications in the card, each stored as an application identifier template. The application identifier template contains the AID value which must be presented to select the respective application and the Application Label. The use of the AID is the only way that an application DF (ADF) can be selected (as illustrated by the curved lines in "Figure 1 - GemXplore 3G V2 Card File Structure").

The file identifier is 2F00h. The short file identifier assigned to EFDIR is 30.

Byte Number	Description	Length
1	TAG 61 (Application Template)	1
2	Length	1
4	TAG 4F (Application Identifier Template)	1
5	Length	1
6 to 6+X	AID value	X= 1 to 16
7+X	TAG 50 (Application Label Template)	1
8+X	Length	1
9+X to 9+X+Y	Application Label Value	Y

Table 2 - EFDIR File Body Structure

The Application Label Value contains a string of bytes provided by the application provider coded using the GSM default alphabet or UCS2 Alpha Coding.

Application Identifier Value (TAG 4F):

The Application Identifier (AID) identifies an application in a card. An AID is divided in two parts:

- A Registered application provider Identifier (RID) coded on five bytes
- A Proprietary application Identifier Extension (PIX) containing between 7 and 11 bytes, and coded in BCD (22 digits maximum).

For 3G:

RID	Value	Length
3G	A0 00 00 00 87h	5

Table 3 - RID Value for 3G

Digit Number	PIX meaning (BCD coded)
1–4	3G application code
5–8	Country code
9–14	Application provider code
15 up to 22	Application provider field (optional)

Table 4 - PIX Data Format

For the USIM (3G application), the 3G application code is 1002h.

For more information on AID coding, refer to the 3G TS 31.110 specification (*"Numbering System for Telecommunication IC Card Applications"*).

EFARR

EFARR files are linear fixed files whose records contain access rule information for all files on the card, including EFARR files themselves. Each record represents a set of access rules.

GemXplore 3G V2 uses the access method based on referencing via the EFARR file ID and record number. In effect, for a given EF or DF, the file ID and record number of EFARR is indicated after tag 8B in the EF or DF's header.

- For an EF, if EFARR cannot be found in the current DF, a backtracking mechanism searches for it in the parent DF, up until an ADF or the MF is reached.
- For a DF, if EFARR cannot be found in the parent DF, a backtracking mechanism searches for it in the grandparent DF, up until an ADF or the MF is reached.
- For the MF or an ADF, the EFARR is searched for under the MF.

The EFARR file identifier is 2F 06h for files associated with the MF and 6F 06h for files associated with DFs or ADFs. The short file identifier assigned to EFDIR is 06.

Please refer to “Access Rules EFARR” on page 39 for details on the record structure of EFARR.

Secret Code EFs

There are two types of secret code EFs: EFPIN and EFADM. These secret code EFs are described as follows.

EFPIN

EFPIN files are transparent EFs which contain user-defined secret codes. A file’s access conditions may specify that one of these codes must be presented before carrying out certain operations. No more than four EFPIN files can be created in a given directory for each global and local PIN. The identifiers for global PINs $EF_{PIN_{1–4}}$ are 0101h, 0102h, 0103h and 0104h respectively, located under the MF. The identifiers for local PINs $EF_{PIN_{1–4}}$ are 0010h, 0020h, 0030h and 0040h respectively, located under the ADF, and which are used to define the access conditions for the files belonging to this application, or under the MF / a DF outside the ADF. Each EFPIN file contains only one single secret code.

Byte Number	Description							Length
1	RFU							
2	Presentation of PIN and Unblock PIN codes							1
	Bit7	**Bit6**	**Bit5**	**Bit4-3**	**Bit2**	**Bit1-0**		
	0	X	X	X	X	X	PIN enable/disable allowed	
	1	X	X	X	X	X	PIN enable/disable not allowed	
	X	0	X	X	X	X	PIN enabled	
	X	1	X	X	X	X	PIN disabled	
	X	X	0	X	X	X	Change not allowed	
	X	X	1	X	X	X	Change allowed	
	X	X	X	X	0	X	Coded in alphanumeric	
	X	X	X	X	1	X	PIN/Unblock PIN coded in BCD	
3	RFU							1
4–11	PIN code							8
12	Maximum value for the PIN ratification counter							1
13	Remaining number of PIN attempts before the code is blocked							1
14–21	Unblock PIN code							8
22	Remaining number of unblock PIN attempts before the code is blocked							1
23	Remaining number of unblock PIN attempts in the unblock mechanism							1

Table 5 - EFPIN File Body Structure

Byte 13. It is loaded with Byte 12 value when the PIN is correctly presented. The value is decreased by one each time the PIN is incorrectly presented. When this parameter reaches the null value, the PIN is blocked and the corresponding right cannot be granted anymore, even if the PIN is correctly presented after the ratification counter has reached the null value.

Byte 14–21. Contains the unblocking code. Correctly presenting this value resets Byte 13 and unblocks the PIN.

Byte 22. This is a counter which is decreased every time an unblocking code is presented incorrectly. If the unblocking code is presented correctly, this counter is reset to its maximum value (10). If the counter reaches 0, the **Unblock PIN** command can no longer be used on the code.

Byte 23. This is a counter which is decreased every time the unblock secret code procedure is called, whether successful or not. In other words, it limits the total number of unblocking attempts which can be performed over the card's life cycle, thus providing additional security where required. If the byte is originally initialized with an FFh value, the counter is not decreased and this mechanism is not active.

EFADM

EFADM files are transparent EFs which contain administrative secret codes. No more than four EFADM files can be created. The identifiers are 1000h, 1001h, 1002h and 1003h for EFADM1, EFADM2, EFADM3, and EFADM4, respectively.

Byte Number	Description	Length
1	RFU	1
2	Presentation of ADM and Unblock ADM codes **Bit7 Bit6 Bit5 Bit4-3 Bit2 Bit1-0** 0 X X X X X ADM enable/disable allowed 1 X X X X X ADM enable/disable not allowed X 0 X X X X ADM enabled X 1 X X X X ADM disabled X X 0 X X X Change not allowed X X 1 X X X Change allowed X X X X 0 X Coded in alphanumeric X X X X 1 X ADM/Unblock ADM coded in BCD	1
3	AC0 coding. Each bit, if set, the corresponding right is granted when ADM code is correctly verified. **B0=1, others are set to 0:** global PIN1 right is granted (3G) or chv1 right is granted (GSM) **B1=1, others are set to 0:** global PIN2 right is granted (3G) or chv2 right is granted (GSM) **B2=1, others are set to 0:** global PIN3 right is granted (3G) **B3=1, others are set to 0:** global PIN4 right is granted (3G) **B4=1, others are set to 0:** ADM1 right is granted (3G and GSM) **B5=1, others are set to 0:** ADM2 right is granted (3G and GSM) **B6=1, others are set to 0:** ADM3 right is granted (3G and GSM) **B7=1, others are set to 0:** ADM4 right is granted (3G and GSM)	1
4–11	ADM code	8
12	Maximum value for the ADM ratification counter	1
13	Remaining number of ADM attempts before the code is blocked	1

Table 6 - EFADM File Body Structure

Byte Number	Description	Length
14–21	Unblock ADM code	8
22	Remaining number of unblock ADM attempts before the code is blocked	1
23	Remaining number of unblock ADM attempts in the unblock mechanism	1

Table 6 - EF$_{ADM}$ File Body Structure (continued)

Byte 3. This byte indicates the rights that may also be granted when an ADM is correctly verified, even if the ADM bit of the ADM code being verified is not set in byte AC0.

Byte AC0 does not support the use of local PINs, as they are ADF dependant and related to applications. Rights granted for knowledge of a secret code in one ADF are revoked if you switch to a different ADF

Byte 13. It is loaded with Byte 12 value when the ADM is correctly presented. The value is decreased by one each time the ADM is incorrectly presented. When this parameter reaches the null value, the ADM is blocked and the corresponding right cannot be granted anymore, even if the ADM is correctly presented after the ratification counter has reached the null value.

Byte 14–21. Contains the unblocking code. Correctly presenting this value resets Byte 13 and unblocks the ADM.

Byte 22. This is a counter which is decreased every time an unblock secret code is presented incorrectly. If the unblock secret code is presented correctly, this counter is reset to its maximum value (10). If the counter reaches 0, the **Unblock PIN** command can no longer be used on the code.

Byte 23. This is a counter which is decreased every time the unblock secret code procedure is called, whether successful or not. In other words, it limits the total number of unblocking attempts which can be performed over the card's life cycle, thus providing additional security where required. If the byte is originally initialized with an FFh value, the counter is not decreased and this mechanism is not active.

Key EFs (EFKEY)

EFKEY files are transparent elementary files which cannot be extended, but can be created and updated by the operator.
The GSM **Run GSM Algorithm** command and 3GPP **Authenticate** command use secret key stored in the EFKEY. The EFKEY for GSM is created directly under the MF. As for 3G, the EFKEY must be created directly under the ADF.

An EFKEY file stores the cryptographic key used by the operating system and also contain other information concerning the key and its algorithm. The EFKEY file identifier is 0001h.

Byte Number	Description	Length
1	Algorithm identifier for the secret key	1
2–17	Secret key value	16
18–33	Secret Key mask	16
34	OPc indicator	1
35–50	OP or OPc secret key	16
51–66	OPc mask	16

Table 7 - EFKEY File Body Structure

Where:

Byte 1. This byte specifies the algorithm to be used with relevant key. If the identifier set to 00h, the card considers the corresponding key is not initialized and thus it cannot be used.

Identifier	Specified Algorithm
40h	COMP 128-1 (for GSM only)
41h	GSM XOR
42h	3G Dummy XOR
48h	3G Milenage

Byte 2–17. These bytes constitutes the value of the key.

Byte 34. Value = 00h, indicates byte 35-50 contains OPc value.
Value = 55h, indicates byte 35-50 contains OP value, and on-card OPc generation from the OS is required.

Byte 35–50. OP or OPc key value.

Authenticate Configuration (EF AUTHPARAM)

The EFAUTHPARAM file is a transparent file which contains the authenticate configuration. The file identifier is 2FE5h and is located under the MF.

Byte Number	Description	Length
1	**RES length**: INT(Desired Length/8)*8 + (8-(Desired Length MOD 8))	1
2	α value	1
3	β value	1

If any one of the following occurs, α and β will take the default value of 32:

- EFAUTHPARAM file is not found.
- The length of the file is less than the offset of α and β.
- When the values exceed the maximum allowable value of 43.

Table 8 - EFAUTHPARAM File Body Structure

If this file does not exist or if RES length is not valid, then the default RES size will be 64 bits for 3G Milenage algorithm and 128 bits for 3G Dummy XOR algorithm.

EFSQN

The EFSQN file is a linear fixed file which contain the computed SQN value after an successful authenticate command, which must be stored in the card EF. The file identifier is 6F1Dh and is located directly under the ADF file.

Record #	Description	Length
1	SQNMS	6
2	SQN0	6
.....		6
33	SQN31	6

Table 9 - EFSQN File Body Structure

EFAUTHCOUNT

The EFAUTHCOUNT is a transparent file that contain a counter with its value decreased each time a **GSM Run Algorithm** or a **3G Authenticate** command is executed.

When the file is present and valid, the operating system will verify if the counter has reached the blocking value 000000h before running the **GSM Run Algorithm** or the **3G Authenticate** command. The command will only be executed if the counter has not reached the blocking value. However, if the file is not present or is invalidated, then security mechanism is not activated, and the command can be run at anytime.

The file identifier is 6F1F and is located under the MF.

Byte #	Description	Length
1–3	Current value of the Run GSM Algorithm counter	3

Table 10 - EFAUTHCOUNT File Body Structure

EFMAP

EFMAP is linear fixed file located directly under the MF to facilitate file sharing. Each record should be three bytes long.

The file identifier is 6E01.

EFSMS SYSTEM

The EFSMS SYSTEM is a transparent file located under the MF.

This file contains the following information:

- Synchronization counter used for OTA security
- notification if a script has been executed successfully, unsuccessfully or downloading is in progress.
- status for the script execution.

Note: The access condition for “invalidate” must always set to never.

The file identifier is 5F11, with minimum nine bytes in length.

Byte #	Description	M/O	Length
1	SIM synchronisation counter	M	5
6	Absolute Offset of Command Number Field If this byte is 00h, the fields “Command Number” and “Error Status” will not be updated after a Update Record SMS session. If this byte is any value other than 00h, this value corresponds to the absolute offset of the Command Number field, and update is done in either success or failure case.	M	1
7	Number of bytes of the subsequent string for successful case notification	M	1
8	String #1 in packed format, used for notification for successful case	O	X
8+X	Number of bytes of the subsequent string for failure case notification	M	1
9+X	String #2 in packed format, used for notification for failure case	O	Y
9+X+Y	Number of bytes of the subsequent string for failure case notification	M	1

Table 11 - EFSMS SYSTEM File Body Structure

Byte #	Description	M/O	Length
10+X+Y	String #3 in packed format, used for notification for concatenation case	O	Z
10+X+Y+Z	Command Number when error occurs • if error occurs during 03.40 header or 03.48 header, the Command Number byte is set to 00h. • if error occurs during message command execution, the Command Number byte contains the number of the command that caused this error. • if no error occurs during message command execution, the Command Number byte contained the number of the last executed command. The first command is associated with the Command Number 01h. If either a GSM or OP interpreter applet is triggered without any command to process, then both the Command Number and the Error Status are set to 00h, that is, no command and no error status	O	1
11+X+Y+Z	Error Status during 03.48 header analysing and command execution. In the case of the 03.48 command analysing, both the Error Status and the Command Number will be equal to 00h.	O	2

Table 11 - EFSMS SYSTEM File Body Structure

Note: When creating a system file, the attributes of the file must be followed strictly according to the attributes stated in "Table 11 - EFSMS SYSTEM File Body Structure". The card will not verify whether the required attributes are attached to the file.

Caution: Byte 6 to 10+X+Y are dedicated only for Update Record SMS triggering.

EFSMS LOG

EFSMS LOG is a linear fixed file that contains the addresses of servers, which have the permission to send executable scripts to the card. The script will be executed if there is a matching address in this file. The number of records depends on the number of addresses to be stored.

The file identifier is 5F14, and is located under the DFTELECOM.

Byte #	Description	M/O	Length
1	Address length (number of useful semi-bytes)	M	1
2	Type of address (TON and NPI)	M	1
3-12	Address value (unused semi-bytes are set to Fh)	M	10

Table 12 - EFSMS LOG File Body Structure

When creating a EFSMS LOG, the attributes of the file must be followed strictly according to the attributes stated in "Table 12 - EFSMS LOG File Body Structure", in order to execute the downloaded script successfully. The card will not verify whether the required attributes are attached to the file.

The number of records at creation depends on the number of address to store. However, the size can be extended in the applicative phase through the Extend command.

If the EFSMS LOG does not exist under the DFTELECOM (7F10h) or the file is invalidated, the address is not checked.

File IDs for Specialized EFs

File	ID	Content	File Location
EFCHV1	0000h	GSM card holder verification 1	MF
EFCHV2	0100h	GSM card holder verification 2	MF
EFGPIN1	0101h	3G Global PIN1 (GPIN1)–for 3G only	MF
EFGPIN2	0102h	3G Global PIN2 (GPIN2)–for 3G only	MF
EFGPIN3	0103h	3G Global PIN3 (GPIN3)–for 3G only	MF
EFGPIN4	0104h	3G Global PIN4 (GPIN4)–for 3G only	MF
EFUPIN	000Ah	Universal PIN–for 3G only	MF
EFLPIN1	0010h	Local PIN1 (LPIN1)–for 3G only	MF/DF/ADF
EFLPIN2	0020h	Local PIN2 (LPIN2)–for 3G only	MF/DF/ADF
EFLPIN3	0030h	Local PIN3 (LPIN3)–for 3G only	MF/DF/ADF
EFLPIN4	0040h	Local PIN4 (LPIN4)–for 3G only	MF/DF/ADF
EFADM1	1000h	Administrative code 1	MF
EFADM2	1001h	Administrative code 2	MF
EFADM3	1002h	Administrative code 3	MF
EFADM4	1003h	Administrative code 4	MF
EFKEY	0001h	Key file for 3G **Authenticate** command. Key file for GSM **Run GSM Algorithm** command.	ADF (3G) MF (GSM)
EFDIR	2F00h	3G application ID list	MF
EFARR	2F06h	3G Access Reference Rule	MF
EFAUTHPARAM	2FE5h	Authenticate configuration	MF
EFMAP	6E01h	File Sharing System File	MF
EFSQN	6F1Dh	Sequence number	MF
EFAUTHCOUNT	6F1Fh	Authentication counter	MF
EFSMS SYSTEM	5F11h	System information	MF
EFSMS LOG	5F14h	Addresses of Servers	DFTELECOM

Table 13 - Internal File Locations

2

Accessing Data

This chapter provides information on the following:

- Selecting files on a GemXplore 3G V2 card
- Activating, terminating, and resetting an application
- Data access methods for transparent, linear fixed, and cyclic EFs

Selecting Files

Access to the data in GemXplore 3G V2 cards is obtained by using logical addressing methods. Before handling the application data stored in an elementary file, its parent file and then the elementary file itself must be selected in order, in case of a FID selection. After an **Answer To Reset** (ATR) the currently selected file will be the master file. Any other file can then be selected on the basis of the following rules:

- Selecting the MF, ADF or a DF sets the current directory.
- After an MF, ADF or DF selection there is no current EF.
- Selecting an EF sets the current EF which must be a child of the current directory.

The following files can thus be selected from the last selected file:

- Any file which is an immediate child of the current directory.
- Any DF which is a sibling of the current file.
- An immediate child DF of the parent of the current DF.
- The parent of the current directory.
- The current DF.
- The MF.

When the file selection succeeds, the file pointer moves to the selected file, and file information can be retrieved by sending the **Get Response** command. If the Select command fails, the file pointer remains on the previously selected file.

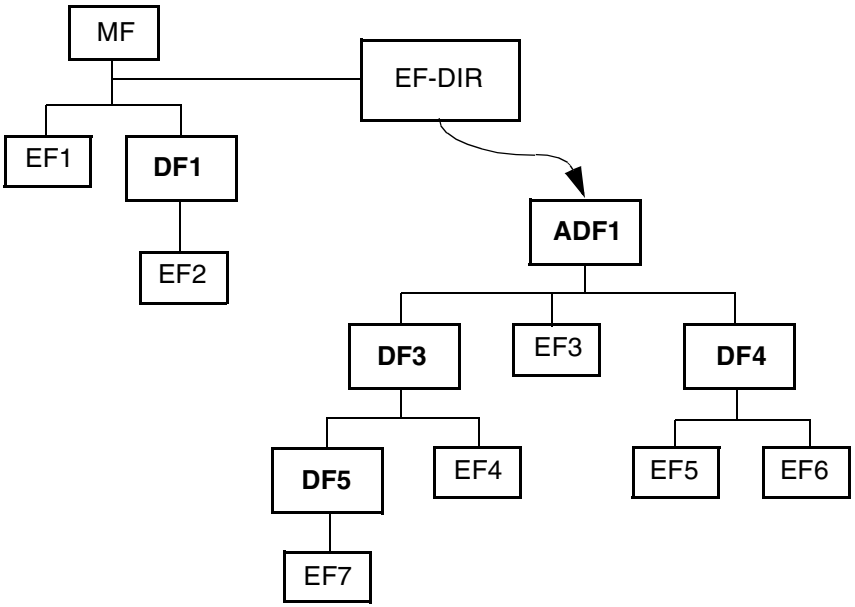

Figure 5 - Example of Card Structure

The following table gives the valid selections for the logical structure in “Figure 5 - Example of Card Structure” if the FID is used. Re-selection of the last selected file is also allowed but not shown.

Last Selected File	Valid Selections
MF	DF1, EF1, EF-DIR
DF1	MF, EF2
ADF1	MF, DF3, DF4, EF3
DF3	MF, ADF1, DF4, DF5, EF4
DF4	MF, ADF1, DF3, EF5, EF6
DF5	MF, DF3, EF7
EF1	MF, DF1, EF-DIR
EF2	MF, DF1

Table 14 - File Select by FID for “Figure 5 - Example of Card Structure”

Last Selected File	Valid Selections
EF3	MF, ADF1, DF3, DF4
EF4	MF, ADF1, DF3, DF5, DF4
EF5	MF, DF4, ADF1, EF6, DF3
EF6	MF, DF4, ADF1, EF5, DF3
EF7	MF, DF3, DF5

Table 14 - File Select by FID for "Figure 5 - Example of Card Structure" (continued)

File Selection Modes

GemXplore 3G V2 cards provide five file selection modes:

- Select by identifier (only for GSM commands)
- Select by DF name –AID (only for 3G commands)
- Select by path (only for 3G commands)
- Select by SFI (only for 3G commands)
- Select by child number (for Gemplus proprietary commands)

Select by Identifier

Any file except an ADF can be selected using its two byte identifier in accordance with the file selection rules described in "Selecting Files" on page 23.

In order to select unambiguously any file by its identifier, the file identifier must be defined during file creation. No two files belonging to the same parent may share the same file identifier.

When a DF is selected you can select a child file either by using its identifier or by using its child number.

With this method, it is possible to select a file which is:

- an immediate child of the current DF (down)
- a child DF of the parent of the current DF (horizontal)
- a DF which is a sibling of the current file (horizontal)
- the parent of the current directory (up)
- the current DF
- the MF (top)

For example, for the architecture shown in Table 14, “File Select by FID for “Figure 5 - Example of Card Structure””, on page 24 shows the files that may be selected from the current entity.

The following file identifiers are reserved:

3F 00h	Master file
3F FFh	Reserved (see referencing by path addressing mode)
FF FFh	Reserved
7F FFh	The active Application Dedicated File (ADF)

Select by DF name (AID)–for 3G mode only

This method enables you to select application directories by specifying their Application IDentifier (AID) string - DF name, coded on 1 to 16 bytes. In order to select unambiguously by the DF name, all DF names must be unique on the card.

However, this selection mechanism is used especially for ADF files, as ADFs can only be referenced by a DF name (providing the corresponding entry in EFDIR is found). A partial DF name is allowed during referencing.

Following are some limitations on selecting an ADF:

- An ADF can only be selected successfully via a DF name, provided the corresponding DF name (AID) is located in EFDIR.
- An ADF can also be selected via **Select** by identifier with FID = 7FFFh only if the ADF is in its active state.
- ADF is located physically directly under the MF, logically, there is no direct link among MF and any ADFs.

You are also able to select application directories by specifying a right-truncated DF name. For more information on application selection, refer to “Application Session Management” on page 28.

Select by Path

This selection mechanism enables you to select files which are remote in the file structure using just one command, in cases where several commands would be required with the “select by FID” method.

The path is a concatenation of the file identifiers (or active ADFs), always in the direction parent to child, from the MF or current DF and ending with the identifier of the intended file. If the identifier of the current DF is unknown, the value 3FFFh can be used at the beginning of the path. The identifier value 7FFFh can be used to automatically select the current active application.

The path of the file to be selected may correspond either to any of the following:

- A file selection starting from the MF:
  File selections starting from the MF are typically used to directly select files higher up or in a remote branch of the file structure. When selecting from the MF, the root directory (3F 00h) does not necessarily need to be specified in the path and you can if necessary specify the path starting from the second level of the file structure (for example, the Telecom directory can be specified as 3F00/7F10 or simply as 7F10). This enables you to specify file paths going four levels down in the file structure (including the root directory).
- A file selection starting from the current DF:
  File selections starting from the current DF are typically used to select a file located lower down in the file structure, in the same branch as the current DF.

Select by SFI

On GemXplore 3G V2, the data management commands (that is, **Read Binary, Update Binary, Read Record, Update Record, Increase** and **Search**) support Short File Identifiers (SFIs). SFIs provide a means of reading/updating EFs directly without having to select the EF explicitly with a **Select** command. This is done by passing the SFI in the command parameters.

The SFI is specified with an SFI TLV object associated with each EF. However, if no SFI object is found, the SFI corresponds to the five least significant bits of the EFs identifier (for example, the SFI of 6F 39h is 25 (that is, 11001b)). If the SFI TLV object exists, but is of zero length, then the EF does not support selection by SFI. SFI values must be within the range 1 to 30 (encoded in 5 bits).

When several files have the same SFI, the command is applied to the first file found in the card's memory (the first file created), but it is strongly recommended that all SFIs in the same current directory be different.

When a data management command (as shown above) contains a valid SFI, the command sets the file as the current EF and resets the current record pointer.

Note: An SFI cannot be used as the current EF or as a file identifier.

Select by Child Number

Any file located within a DF may be referenced by its child number coded on two bytes, from 0001h to FFFFh. The child number of the first child of a DF is 0001h. Value 0000h is reserved.

The child number is determined by the file creation order. If an EF is deleted under the current DF, the child number of other files will be changed.

Application Session Management

Since 3G cards support multiple applications, a session must be activated whenever an application is selected. The procedures for managing application sessions include activation, termination, and reset.

Activating/Resetting an Application Session

An application session is initiated by either one of the following:

- A **Select** by AID command with a complete or partial AID that is different from the AID of the currently active application and command parameters which specify that the "only occurrence" will be activated.
- A **Select** by AID command with a complete or partial AID and command parameters which specify that the "last occurrence" will be selected. If the last selected ADF corresponds to the 16-byte AID and is different from the current one, the selection is performed in activation mode.

Terminating an Application Session

An application session is terminated if any one of the following events occurs:

- A **Select** by AID command with a complete or partial AID that is different from the AID of the currently active application and command parameters which specify that a new application will be activated. The previously selected application is terminated.
- Re-selection of the current application by a **Select** command with a complete or partial AID matching the currently active application and command parameters which specify that the application will be terminated.
- A reset of the UICC, which involves termination of the current application.

Data Access Methods

You cannot handle the data stored in an elementary file unless it has been selected and the relevant access conditions of the elementary file have been met. The data access methods used are different depending on whether the file is a transparent, linear fixed or cyclic EF.

Access to Data in Transparent EFs

Access to data in transparent EFs is obtained by specifying an offset from the beginning of the file with a string length in the command. This allows bytes to be manipulated by blocks of arbitrary length. The operating system checks that the offset plus the length does not exceed the total file length. The first byte of the transparent EF has the relative address 0000h. The commands used to handle transparent EFs are: **Read Binary** and **Update Binary.** See “Chapter 9 - Operational Commands”.

Access to Data in Linear Fixed EFs

Access to data in linear fixed EFs is obtained using either relative or absolute addressing methods. The first record in a linear fixed EF is record 1. The commands used to handle linear fixed EFs are: **Read Record**, **Update Record** and **Search.** See “Chapter 9 - Operational Commands”.

Relative Addressing

The data in linear fixed EFs can be handled using relative addressing. In relative addressing, the commands use the following parameters:

- The position of the record relative to the currently selected record (current, previous or next mode).
  - If no record is currently selected, next mode points to the first record in the EF, and previous mode points to the last record in the EF.
  - If the last record is currently selected, next mode is not valid. If the first record is currently selected, previous mode is not valid.
- If no record is currently selected, the first or last record in the file will be chosen.

Absolute Addressing

In absolute addressing, the commands use the record number as a parameter.

You can also find data in linear fixed EFs using the **Search** command with a search pattern of up to 255 bytes. See “Search/Seek” on page 122.

Access to Data in Cyclic EFs

Access to data in cyclic EFs is obtained using either relative or absolute addressing methods. Record 1 in a cyclic EF is always the most recently updated record which means that the oldest record always has the highest record number.

Read Operations

- **Relative addressing**
  When a cyclic EF is selected, in 3G mode, there is no current record, where else, in GSM mode, the latest record is the current record. The data in a cyclic EF is read using the **Read Record** command with the following parameters:
  - The position of the record relative to the currently selected record (current, previous or next mode).
  - The first (that is, the most recent record) or the last record (that is, the oldest record).

  You can also reach data in cyclic EFs using the **Search** command with a search pattern of up to 255 bytes. See “Search/Seek” on page 122.
- **Absolute addressing**
  In absolute addressing, the **Read Record** command uses the record number as a parameter.

Update Operations

You can modify the data in a cyclic file by using the **Update Record** command which works exclusively in previous mode. When you run an **Update Record** command, the oldest record is overwritten and becomes record 1 (that is, the current record); all the other record numbers are incremented by 1.

You can also modify the data in cyclic files by using the **Increase** command. In this case, a constant value is added to the last written record. The result is then written in the oldest record, which becomes record 1. See “Chapter 9 - Operational Commands”.

3

3G Data Security

The data stored in 3G cards is protected by means of access conditions which define the type of authentication required before an operation can be performed on the card. There are two types of authentication:

- Passive authentication which consists in verifying secret codes.
- Active authentication which consists in comparing cryptograms generated by the card and the terminal using a random value, an algorithm and a secret key.

This chapter describes access conditions and passive authentication procedures. Active authentication is described in “Chapter 4 - 3G Network Security”.

Security Architecture

The security architecture of 3G cards provide active and passive authentication control over execution of commands and the access to files. The active access control is maintained by setting security attributes to each command and file access. Thus the security attribute of each instruction is checked against its security status before execution of each command giving complete access control.

Global and Local Secret Codes

A Global PIN is a PIN that uses a global key reference. It allows access to all files on the UICC that reference it in the access rules. This type of PIN has global access rights with respect to files. All operations performed on a PIN (enable/disable/change) that cover several ADFs/DF's affect the applications that use the PIN and the access rules that use the corresponding key reference.

From the security context point of view, GemXplore 3G V2 can be considered as a multi-verification capable UICC, supporting four-level one-user verification requirements ($GPIN_{1–4}$ and Universal PIN) and four-level two-user verification requirements ($LPIN_{1–4}$). These four $LPIN_{1–4}$ are supported per ADF/DF.

A local PIN (LPIN) is a PIN that uses a local key reference. It is only valid within the ADF/DF that specifies it in the FCP. In addition, GemXplore 3G V2 supports four global ADMs ($ADM_{1–4)}$.

Note: A local PIN file can be located under either a DF (if the DF is outside an ADF) or an ADF. However, for an ADF, the local PIN file must be located directly under it.

If the desired local PIN file is not found, backtracking is used to search for the local PIN file until the DF at level 1 is reached.

Access Conditions for GSM

A file, which is accessible in both GSM and 3G sessions (For example, in the MF: EF-PL in the UICC can be identical to EF-ELP in the SIM), can support independent GSM and 3G access conditions. The UICC does not check the consistency of the access conditions in both modes. Therefore it is possible that the same EF or DF has different security attributes in GSM and 3G operation mode.

The operating system stores the access rights to CHV/PIN, ADM which have already fulfilled, until the card session ends or the application is explicitly closed.

The purpose is not to ask twice for the same user identification (CHV/PIN and any secret code).

Access Condition Group 1–4 / 1–6

These bytes coded the access conditions (ACs) associated to each group of command. The ACs defined in these bytes only apply in GSM files in GSM session.

GSM Access Conditions Storage. Each GSM file has its own specific access condition for each command group. The relevant access condition of the current file must be fulfilled before the requested action can take place.

You can assign one or more of the following access conditions for each command group.

Identification Number (b7-b0)	Access Condition	Description
00000000	NEVER	The action cannot be performed over a SIM/ME interface. No bit should be set for the 'NEVER' access condition.
XXXXXXX1	ALWAYS	No restrictions on the command.
XXXXXX1X	CHV1	The command can be executed if one of the following conditions is met: • CHV value is correctly presented during the current session (using the **Verify CHV, Change CHV, Enable CHV, Disable CHV** or **Unblock CHV** commands), • CHV Enable/Disable flag is set to "Disabled" and CHV is not blocked, • **Unblock CHV** is successfully performed during the current session, • An ADM right is granted and the AC0 byte of this ADM body has set to "1" in b1 and b2 for CHV1 and CHV2 respectively.
XXXXX1XX	CHV2[1]	
[1]: CHV2 cannot be used on **Enable CHV** and **Disable CHV** commands.		
XXXX0XXX	-	RFU
XXX1XXXX	ADM 1	The administrative authority is responsible for allocating these levels and the respective requirements for their fulfilment. The management of these codes is the same as CHV1 and CHV2. One point to note, that is ADM1–4 are able to grant access conditions of the associate codes CHV1–2, ADM1–4. The access rights associated with the ADM code are defined when the EF$_{ADM}$ is created. If the ADM code is blocked, the associated rights, according to byte AC0, are lost.
XX1XXXXX	ADM 2	
X1XXXXXX	ADM 3	
1XXXXXXX	ADM 4	

Table 15 - Access Conditions and Identification Number

These access conditions are not hierarchical. That is to say, for example, that presenting CHV2 does not give the access rights associated with CHV1.
Once the appropriate CHV or ADM code has been presented correctly, the resulting access rights are granted and valid for the current session, unless the corresponding code becomes blocked.

Each group of functions requires a nibble to code its own access conditions. Similarly, a group of functions requires one nibble to code its relevant key number (zero to seven), if needed.

Access Conditions for a Dedicated File

AC Group	Dedicated Files
Group 1	RFU
Group 2	RFU
Group 3	Delete
Group 4	Create File / Extend

Table 16 - File-Related Commands for Dedicated Files

Access Conditions for Elementary Files

AC Group	Transparent Files	Linear Fixed Files	Cyclic Files
Group 1	Read Binary	Read Record/Seek	Read Record/Seek
Group 2	Update Binary	Update Record	Update Record
Group 3	RFU	RFU	Increase (if authorized on file)
Group 4	RFU	RFU	RFU
Group 5	Rehabilitate	Rehabilitate	Rehabilitate
Group 6	Invalidate	Invalidate	Invalidate

Table 17 - File-Related Commands for Elementary Files

Universal PIN

A Universal PIN is a PIN that is used in a multi-application environment to allow several applications to share one common PIN. The Universal PIN is a global access condition that has been assigned a key reference value '11h'. This key reference value shall not be used for anything else but to indicate the Universal PIN.

In order to give access to several applications on a multi-application UICC, a terminal conforming to the present document shall support the usage of the Universal PIN. A multi-application UICC according to the present document shall support the usage of a Universal PIN.

If an application allows the use of the Universal PIN as replacement PIN, the Universal PIN shall be part of the access condition for this application on a multi-application UICC that complies to the present document. In case of a single verification capable UICC the Universal PIN shall not be used.

The Universal PIN does not belong to any application, e.g. its verification status cannot be reset by the application activation or termination procedures.

The Universal PIN which is optional and exists only in 3G session, can be used to replace any Global PIN using Disable PIN (With Replacement) command. When a Global PIN is replaced by Universal PIN, any file that is protected by that PIN will now require Universal PIN to be verified prior to access. To distinguish whether to verify a Global PIN or Universal PIN for access to a file, two Security Environments are specified; SE01 and SE00. Essentially (though there are exceptions), when the current Security Environment is SE01 Global PIN has to be verified and when it is SE00 Universal PIN has to be verified. All files contain specification for two access rules; one for SE01 and another for SE00. Depending on the current Security Environment, the OS will go to the corresponding rule to check for access.

Application PIN

An Application PIN is a PIN that uses a global key reference. The Application PIN allows access to any file on the UICC where it is referenced in the access rules. i.e. this PIN has global access rights with respect to files. It becomes an application PIN based on where it is assigned, and it belongs to the corresponding application Security Environment. PIN assignment is done at the time an ADF is created. Its verification status can be reset by the application activation or termination procedure. An application, from the security context point of view, may consist of one or more ADFs/DFs.

In this case the ADFs/DFs are seen as one application from the security and access rules point of view. All operations performed on a PIN (enable/disable/replace) covering several ADFs/DFs affects the applications where the PIN is used and the access rules where the corresponding key reference is used.

Security Environment

The security environment is a mechanism to specify for the card system the security functions that are available to provide protection to commands for a specific application of the card according to ISO/IEC 7816-8. The security environment for a multi-application UICC is defined as a container for each activated application on the UICC. In case of a single application card the security environment is valid for the whole UICC. In the referenced format it is possible to indicate different access rules as a function of the SE that is in use.

The OS maintain two Security Environments information. The default Security Environment which is used when no application is active, and the Security Environment for current ADF used when there is an active application.

The table below is used to process the Security Environment.

<table>
<tr><th colspan="3" rowspan="2">PIN to verify</th><th colspan="2">Universal PIN status</th></tr>
<tr><th>Enabled</th><th>Not Enabled</th></tr>
<tr><td rowspan="3">Application PIN status</td><td colspan="2">Enabled</td><td>Application PIN SE01</td><td>Application PIN SE01</td></tr>
<tr><td rowspan="2">Not Enabled</td><td>UUP</td><td>Universal PIN SE00</td><td>No PIN SE00</td></tr>
<tr><td>DUUP</td><td>No PIN SE00</td><td>No PIN SE00</td></tr>
</table>

UUP: Use Universal PIN (usage qualifier set to ‘08’).
DUUP: Do not use Universal PIN (usage qualifier set to ‘00’).

Table 18 - PIN mapping into Security Environment.

Security Environment under an ADF

To derive this environment, below three items from the “Table 18 - PIN mapping into Security Environment.”are required to look into:

Application PIN status

This refers to the status (enabled / not enabled) of the ‘Application PIN’ that the current ADF is associated with.

Usage Qualifier

If the ‘Application PIN’ is replaced, usage qualifier is regards as UUP. Otherwise, it will regards as DUUP.

Universal PIN status

This column is to determine the Universal PIN is enabled or disabled and which security environment it should become, that is either SE00 or SE01.

Example:

An ADF is created with GPIN2 associated with it. If GPIN2 is disabled and replaced by the Universal PIN through **Disable PIN** command, then the parameters in "Table 18 - PIN mapping into Security Environment." should set as follow:

- Application PIN status: 'Not Enabled' and 'UUP' are set.
- Universal PIN status: 'Enabled' is set and Security Environment becomes SE00.

PIN/ADM EFs

In 3G mode, four application PINs ($GPIN_{1–4}$) and one Universal PIN, with global key references are available. In addition, the UICC also supports up to four local PINs ($LPIN_{1–4}$) for each DF/ADF.

In GSM mode, only CHV1 and CHV2 are available. They apply to files in DF-GSM and DF-TELECOM.

CHV1, CHV2, ADM and Global PIN File Identifiers. The ADM files used is the same as that of GSM. These files are shared between GSM and 3G session, and have the same file ID. These files are located under the MF. The file identifiers allocated for the CHV1, CHV2, Global PINs (GPINs), Universal PIN and ADMs are as follows.

GSM File Name	3G File Name	File Identifier
CHV1		0000h
CHV2		0100h
	Universal PIN	000Ah
	Global PIN1 [GPIN1]	0101h
	Global PIN2 [GPIN2]	0102h
	Global PIN3 [GPIN3]	0103h
	Global PIN4 [GPIN4]	0104h
ADM1	ADM1	1000h

Table 19 - File Identifier for ADMs and Global PINs

GSM File Name	3G File Name	File Identifier
ADM2	ADM2	1001h
ADM3	ADM3	1002h
ADM4	ADM4	1003h

Table 19 - File Identifier for ADMs and Global PINs (continued)

Local PIN File Identifiers. The local PINs are stored under a DF or ADF. The file structure is the same as global PINs (GPINs).

3G File Name	File Identifier
Local PIN1 (LPIN1)	0010h
Local PIN2 (LPIN2)	0020h
Local PIN3 (LPIN3)	0030h
Local PIN4 (LPIN4)	0040h

Table 20 - File Identifier for Local PINs

3G and GSM PINs Mapping

Mapping of PINs between GSM and 3G operation modes, so that activation, deactivation or changing of a PIN in one operation mode has the same effect in the other operation mode, based on these principles:

- Mapping of CHV1
  CHV1 in the SIM application can be mapped to any USIM application PIN with a global key reference (or to the Universal PIN), but to only one at a time.
- Mapping of CHV2
  CHV2 in the SIM application can be mapped to the corresponding local key reference belonging to the USIM application to which the CHV1 is mapped. In the 2G operation mode, this PIN is considered to be global, in the 3G operation mode, it is seen as a being local. If mapped, then, with respect to the requirement in TS GSM 11.11 for CHV2, this PIN cannot be disabled in either operation mode. The UICC will return an appropriate error condition in that case.
- Mapping of Local PINs (LPINs)
  A SIM does not support Local PINs, hence there is no correspondence in 2G operation mode. Local PINs cannot be mapped.
- Mapping of Administrative PINs (ADMs)
  The mapping of administrative PINs between the 2G and 3G operation modes is fully under the discretion of each network operator and card manufacturer.

Security Attributes for 3G

The security attributes are a set of access rules attached to a DF or EF; these access rules consist of an access mode and a security condition. The security conditions must be set for a file to be able to perform commands other than **Select**, **Status** and **Get File Info** on the file.

The access rules contain Access Mode Data Objects (AM_DO) and a Security Condition Data Object (SC_DO). The AM_DO defines for which group or type of command(s) the following security conditions apply. The interpretation of AM_DO is file dependent, the effect is different for DFs and EFs. This difference is demonstrated in the following sections.

Note: The default security conditions for any commands not referenced in any AM_DO in a file security attribute is set to NEVer.

The SC_DO indicates which security conditions (user PIN verification) must be satisfied before a command can be performed on a file.

Security Attributes are stored in EFARR files. Each access rule can be shared by other EFs/ DFs. The EFARR file identifier and record number are stored in the file header of ADFs, DFs and EFs. A file should specify a maximum of two access rules, one for SE00 and another for SE01.

Access Rules EFARR

An EFARR is a linear fixed file whose records contain access rule information. Each record represents a set of access rules.

Each EFARR contains access rules concerning:

- Itself (in the first and second record)
- The files located under the DF which is the parent of the EFARR itself.

Note: Limitation access rule format:

- Only the expanded format access rule is supported.
- Unused bytes in a record are set to ‘FF’.

Location

One (and only one) EFARR shall be located in the following locations

- under the MF
- under DFTELECOM
- under each ADF

The presence of an EFARR under other DFs is optional.

The File ID of the EFARR located under the MF (location of the MFs access condition) is 2F06h.

Note:

- EFARR can be located under any DF.
- If the desired EFARR file cannot be located at the current level, then backtracking is used.
- If the DF is under ADF, backtracking stopped once the ADF level is reached.
- If the DF is not under an ADF, backtracking stopped once the MF is reached.
- The EFARR for an ADF or MF is located under the MF.
- Searching for EFARR for a DF starts at the same level as the DF.
- Searching for EFARR for an EF starts under the current DF.
- EFARR cannot be a link file. Please refer to “File Sharing Mechanism” on page 59for the definition of link file.
- For an EFARR, record 1 is the SE01 access rule and record 2 is the SE00 access rule. If the access rules are different; if they are identical, record 1 contains the SE01 and SE00 access rule.
- Access Referencing Rule (ARR) in SE01 record should include any ADM/PIN except Universal PIN, and in SE00 record should contain any PIN/ADM except global PINs. In case local PIN/ADM is used, this local PIN/ADM should be in both records, although this is not checked by the OS.

Access Rule Record Format

Each record of an EFARR contains one or more Access Rules coded according to the Expanded format. All unused bytes in the record are set to FFh.

AM_DO	SC_DO	AM_DO	SC_DO	...

The expanded format of the access rule consists of one AM_DO followed by one or more SC_DO.

AM_DO Format

The AM_DO Data object contains either an Administrative rule, the AM byte (Tag 80) or a command access rule condition, any tag from 81 to 8F.

Administrative Rule (Tag 80)

Tag	Length	AM byte
80h	01h	see the following

Where:

AM byte indicates which administrative commands are controlled by the current access rule definition. The interpretation of the AM byte is file dependent; it is different for a DF and an EF:

AM byte:

b7	b6	b5	b4	b3	b2	b1	b0	DF Administration	EF Administration
0	1	0	0	0	0	0	0	RFU	RFU
0	0	1	0	0	0	0	0	RFU	RFU
0	0	0	1	0	0	0	0	Activate File	Activate File
0	0	0	0	1	0	0	0	Deactivate File	Deactivate File
0	0	0	0	0	1	0	0	Create File (DF)	RFU
0	0	0	0	0	0	1	0	Create File (EF)	Update binary, Update Record
0	0	0	0	0	0	0	1	Delete File (child)	Read Binary, Read Record, Search

General Rule for Tags 81 to 8F

For these tags the AM_DO represents a list of possible combinations of CLA - INS - P1 - P2 to be compared to the command APDU exchange. Depending on bits b3 to b0, the list contains only the indicated reference values.

AM_DO tag byte:

b7	b6	b5	b4	b3	b2	b1	b0	Command APDU Administration
1	0	0	0	1	-	-	-	CLA exists
1	0	0	0	-	1	-	-	INS exists
1	0	0	0	-	-	1	-	P1 exists
1	0	0	0	-	-	-	1	P2 exists

Note: In 3G V2, the OS only supports tag 84 for **Increase** command.

SC_DO Format

An SC_DO data object contains the security conditions to be fulfilled before executing the commands defined in the preceding AM_DO.

- If the access rule does not specify any condition, Tag 90 must be used.
- If the access rule specifies the command is never to be executed, Tag 97 must be used.
- If the access rule is to specify the command execution conditions, Tag A4 must be used.

SC_DO Rule (Tag 90)

Tag	Length
90h	00h

The access rights for the commands defined in the preceding AM_DO are ALW (always).

SC_DO Rule (Tag 97)

Tag	Length
97h	00h

The access rights for the commands defined in the preceding AM_DO are NEV (never).

SC_DO Rule (Tag A4)

Tag	Length	Key_DO			Usage Qualifier		
A4h	03h/06h	Tag	Length	Value	Tag	Length	Value

Key_DO (Tag 83)

The Key_DO, defining which Secret Code is to be verified

Tag	Length	Value
83h	01h	see the following

Where:

Value Defines the key reference according to the following table:

Value	Access Condition	Level	FID	File Location
01h	Application PIN 1 (GPIN1)	1	0101h	MF
02h	Application PIN 2 (GPIN2)	1	0102h	MF
03h	Application PIN 3 (GPIN3)	1	0103h	MF
04h	Application PIN 4 (GPIN4)	1	0104h	MF
11h	Universal PIN	1	000Ah	MF
0Ah	ADM1	5	1000h	MF
0Bh	ADM2	5	1001h	MF
0Ch	ADM3	5	1002h	MF
0Dh	ADM4	5	1003h	MF
81h	Local PIN 1 (LPIN1)	2	0010h	DF or ADF
82h	Local PIN 2 (LPIN2)	2	0020h	DF or ADF
83h	Local PIN 3 (LPIN3)	2	0030h	DF or ADF
84h	Local PIN 4 (LPIN4)	2	0040h	DF or ADF

Usage Qualifier (Tag 95)

The usage qualifier, defining the type of security mechanism to be used to verify the secret code defined in the preceding Key_DO. This is optional and will not be interpreted even if it is present under the EFARR.

Tag	Length	Value
95h	01h	see below

Where:

Value Indicates the type of security mechanism used to verify the Secret Code defined in the preceding Key_DO, as defined in the following table.

Usage Qualifier Value

b7	b6	b5	b4	b3	b2	b1	b0	Meaning
0	0	0	0	0	0	0	0	Verification requirement not used for verification.
1	-	-	-	-	-	0	0	Use verification (DST,CCT) Use encipherment (CT) Use external authentication (AT)
-	1	-	-	-	-	0	0	Use computation (DST, CCT) Use decipherment (CT) Use Run GSM Algorithm (AT)
-	-	1	-	-	-	0	0	Use SM response (CCT, CT, DST)
-	-	-	1	-	-	0	0	Use SM command (CCT, CT, DST)
-	-	-	-	1	-	0	0	Use PIN for verification (Key Reference data user knowledge based)
-	-	-	-	-	1	0	0	Use user authentication (biometrics based)
other values								RFU

AND and OR Tag

Security Condition byte	Tag	Length	SC_DO	SC_DO
OR template	A0h	X	YY	YY
AND template	AFh	X	YY	YY

This tag is used to combine the SC_DOs in a rule.
An AND and OR operation must involve a minimum of the following parameters:

- Two SC_DOs or,
- one SC_DO and another AND/OR condition or,
- two AND / OR conditions.

The OS only supports an access rule with a maximum of two level when using AND/OR.

Note: SC_DO tags 90h (‘Always’ access condition) and 97h (‘Never’ access condition) cannot be encapsulated in an AND or OR tag.

Access Conditions for Files Accessible in Both GSM and 3G Sessions

If a EF or DF is accessible in both GSM or 3G sessions, both access conditions will be present in the file header. It is possible to have different security attributes in the same EF for GSM and 3G sessions, as the operating system does not check the consistency of the access conditions. However, the operator must be ensure that the security attributes for GSM and 3G sessions are the same if necessary.

Current Security Status

The FCP returned by **Select** or **Status** on a DF contains a PIN status template DO Tag C6. This TLV deal with the state “enable / disable” of the secret code files that located in the current MF/DF/ADF.

Tag	Length	Value		
C6	XXh	PS_DO	Key_DO	.....

The tag C6 indicates a constructed data object that is either empty (L=00h) or containing a PS_DO (tag 90) and one or more Key_DO.

The list of the Key_DO indicates the secret codes that belong to the current DF, MF or current ADF, according to the following rules:

Rule 1: the status of global PINs which are directly under the MF (if global PINs exist) is returned into the PS_DO byte. However, if selecting an ADF, only the associated global PIN is returned.

Rule 2: if the entity selected is an ADF or a DF under an ADF, the status of local PINs (if local PINs exist) which are directly under the activated ADF, is returned into the PS_DO byte.

Rule 3: if the entity selected is a DF under the MF or the MF itself, the status of local PINs (if local PINs exist) which are under the DF being selected, is returned into the PS_DO byte.

Rule 4: if the entity selected is the MF, the status of ADM secret codes (ADM 1-4), if they exist, are returned into the PS_DO byte.

PS_DO

A PS_DO object tag 90 indicates the state of each secret code belonging to the current MF/DF/ADF.

Tag	Length	PS byte
90	XXh	XX

The PS byte contains the state Enable / Disable of each secret code whose file belongs to the current MF/DF/ADF. Each bit set to 1 indicates that the corresponding secret code is enabled, and 0 indicates that the corresponding secret code is disabled.

The msb of the PS byte is relevant to the first secret code of the Key_DO list.

Security Status

The card security status presents the card's current state after the completion of a single command or a sequence of commands. It results from completing the procedure of proving knowledge of a secret code. It is updated after each completion of a PIN-related command.

The operating system is able to store the status of the rights granted for all global PINs; ADMs; Universal PIN; local PINs for ADF; local PINs for up to three levels of DF and the security environment of the current ADF.

Rules on Security Status

- The security status will be cleared after a card reset.
- After activation/reset of an ADF, the ADF security status is cleared.
- The global security status remains the same throughout the whole card session.
- The security status remains unchanged after a file selection. This is to eliminate multiple secret code presentation.
- A wrong presentation of a secret code does not affect the file-specific security status except if this wrong presentation blocks the secret code; in this case, the operating system automatically cancels the information of a previous correct presentation, if any, in the current session.

4

3G Network Security

Authentication

The purpose of this procedure is to authenticate the user and establish a new key between the USIM and the ME. During the authentication, the USIM verifies the freshness of the authentication vector that is used.

The authentication result can be divided into three cases:

- Authentication accept case: the USIM checks that XMAC = MAC and that the sequence number is correct, returns the RES, CK and IK parameters to the ME.
- MAC failure case: the USIM identifies the calculated XMAC value is different from the MAC and returns an error.
- SQN failure case: the USIM verifies that the SQN is not in the correct range, returns an authentication failure message, AUTS for re-synchronization.

Generally, the authentication process and response parameters can be illustrated in “Figure 6 - Authentication Process and Response Parameters”.

.

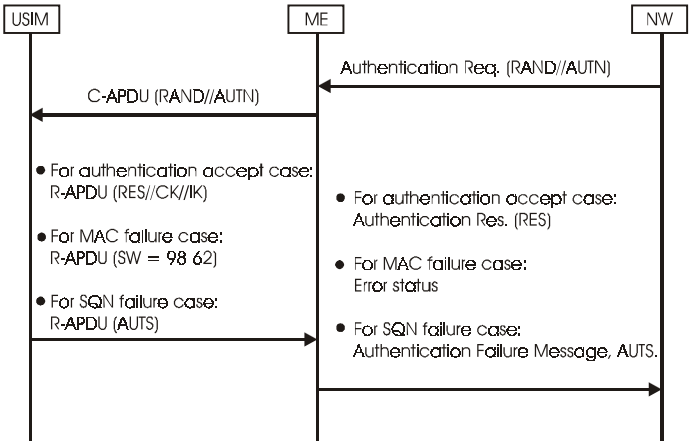

Figure 6 - Authentication Process and Response Parameters

In a 3G session, the algorithms supported on GemXplore 3G V2 are the 3G Dummy XOR algorithm and the 3G Milenage algorithm, described in subsequent sections.

Authentication function in USIM

Definitions

//	Concatenation
XOR	Exclusive OR
f1	Message authentication function used to compute XMAC
f2	Message authentication function used to compute RES
f3	Key generating function used to compute CK
f4	Message authentication function used to compute IK
f5	Message authentication function used to compute AK in normal procedures
K	Long-term secret key shared between the USIM and the AuC

The RAND and the AUTN field are all composed of 16 bytes each.

The AUTN field contains SQN, AMF and MAC, in the following order.

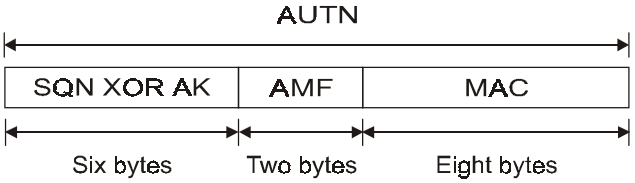

Figure 7 - The AUTN Field

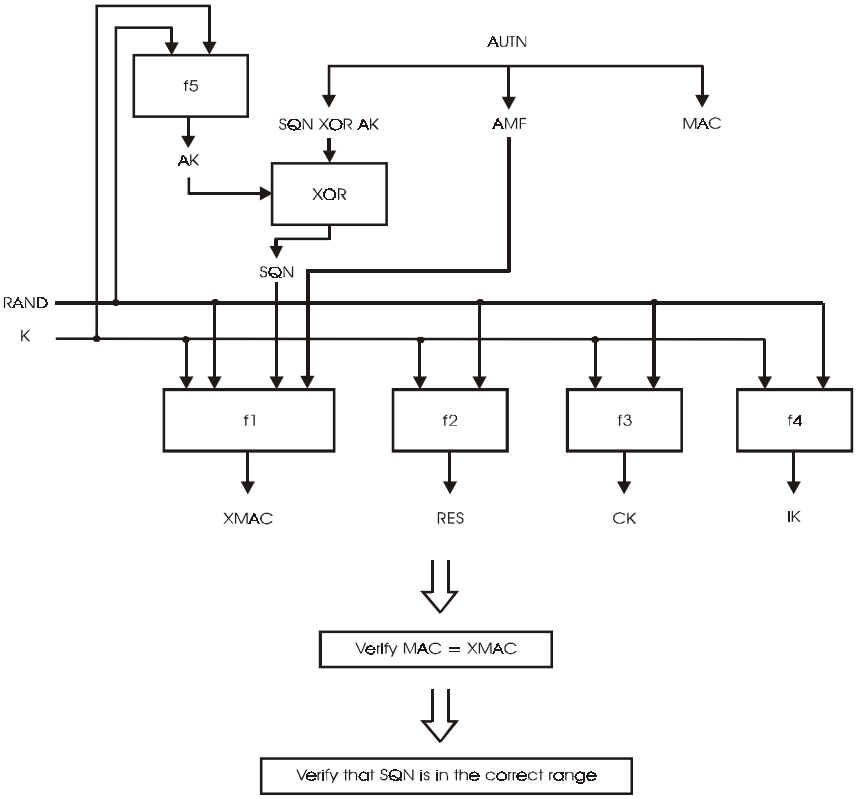

Figure 8 - User Authentication Function in USIM

3G Milenage Algorithm

In a 3G Context

1. Generate AK = f5 (RAND)
2. Derive SQN = (SQN XOR AK) XOR AK
3. Compute XMAC = f1 (RAND, AMF, SQN)
4. Compare XMAC = MAC,

   If XMAC ≠ MAC, return authentication failure message.

   If XMAC = MAC, go to Step 5.
5. Verify SQN is in the correct range,

   If SQN is out of range, generate AUTS message. See “The Synchronization Failure AUTS” on page 54.

   If SQN is in range, go to Step 6.
6. Generate successful message:

   RES = f2 (RAND)

   CK = f3 (RAND)

   IK = f4 (RAND)

   If service° 27 in EFUST is available, compute Kc

   Kc = C3(IK, CK) = IK[bits0..63] XOR IK[bits64..127] XOR CK[bits0..63] XOR CK[bits64..127]

In GSM Context and Service° 38 in EFUST Set to 1

1. Compute RES = f2 (RAND)
2. Compute IK = f4 (RAND)
3. Compute CK = f3 (RAND)
4. Compute Kc

   Kc = C3(IK, CK) = IK[bits0..63] XOR IK[bits64..127] XOR CK[bits0..63] XOR CK[bits64..127]
5. Compute SRES

   SRES = C2(RES) = RES[bits0..31] XOR RES[bits32..63]

3G Dummy XOR Algorithm

In a 3G Context

1. Compute XDOUT = K XOR RAND

   XDOUT[bits 0,1,..126,127] = K[bits 0, 1, ..126, 127] XOR RAND[bits 0,1,..126,127]

2. Generate AK = f5 (XDOUT)

   AK[bits 0,1,..46,47] = XDOUT[bits 24,25,..70,71]

3. Derive SQN = (SQN XOR AK) XOR AK

4. Compute CDOUT = SQN || AMF

   CDOUT[bits 0,1,..62,63] = SQN[bits0,1,..46,47] || AMF[bits0,1,..14,15]

5. Compute XMAC = f1 (RAND, CDOUT)

   XMAC[bits0,1,..62,63] = XDOUT[bits0,1,..62,63] XOR CDOUT[bits0,1,..62,63]

6. Compare XMAC = MAC

   If XMAC ≠ MAC, returns an authentication failure message.

   If XMAC = MAC, go to Step7.

7. Check if AMF = 0xFFFF,

   If AMF = 0xFFFF, generate AUTS message. See “The Synchronization Failure AUTS” on page 54

   If AMF ≠ 0xFF, go to Step 8.

8. Generate successful message:

   RES = f2 (XDOUT, n)
   RES[bits 0,1,..n-1,n] = XDOUT[bits 0,1,..n-1,n] (with 30<n<128)

   CK = f3 (XDOUT)
   CK[bits 0,1,..126,127] = XDOUT[bits 8,9,..126,127,0,1,..6,7]

   IK = f4 (XDOUT)
   IK[bits 0,1,..126,127] = XDOUT[bits 16,17,..126,127,0,1,..14,15]

   If service° 27 is available, compute Kc
   Kc = C3(IK, CK) = IK[bits0..63] XOR IK[bits64..127] XOR CK[bits0..63]XOR CK[bits64..127]

In a GSM Context and Service° 38 in EFUST Set to 1

1. Compute XDOUT = K XOR RAND

   XDOUT[bits 0,1,..126,127] = K[bits 0, 1, ..126, 127] XOR RAND[bits 0,1,..126,127]

2. Compute RES

   RES[bits 0,1,..n-1,n] = XDOUT[bits 0,1,..n-1,n] (with 30<n<128)

3. Compute IK

   IK[bits 0,1,..126,127] = XDOUT[bits 16,17,..126,127,0,1,..14,15]

4. Compute CK

   CK[bits 0,1,..126,127] = XDOUT[bits 8,9,..126,127,0,1,..6,7]

5. Compute Kc

   Kc = C3(IK, CK) = IK[bits0..63] XOR IK[bits64..127] XOR CK[bits0..63] XOR CK[bits64..127]

6. Compute SRES

   SRES = C2(RES) = RES[bits0..31] XOR RES[bits32..63] XOR RES[bits64..95] XOR RES[bits65..127]

The Synchronization Failure AUTS

If there is a synchronization error, SQN is not in range. In that case, the card should return the AUTS value as a response parameter. This value is called the synchronization failure message.

Definitions.

f1* message authentication function used to compute MAC-S.

f5* message authentication function used to compute AK in re-synchronization procedures.

SQNms is the highest SQN value stored in the USIM

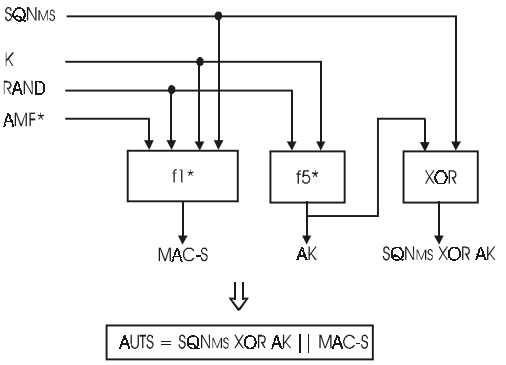

Figure 9 - Construction of the AUTS Parameter

For 3G Milenage Algorithm

MAC-S = f1* (AMF*, RAND, SQNMS)
(Where SQNMS is the highest SEQ number among the 32-element array stored in the USIM, AMF* = 0000h).

AK = f5* (RAND)

AUTS = (SQNMS XOR AK) || MAC-S

For 3G Dummy XOR Algorithm

AMF* = 0000h

Compute CDOUT = SQN||AMF*
CDOUT[bits0..63] = SQN[bits0..47] || AMF*[0..15]

Compute MAC_S = f1* (RAND, CDOUT)
MAC_S[bits0..63] = XDOUT[bits0..63] XOR CDOUT[bits0..63]

AK = AK

SQNMS = SQN

AUTS = (SQNMS XOR AK) || MAC-S

Sequence Number Management

The USIM keeps track internally of a 32-element array (that is, the 32 SEQ values) of previously accepted sequence numbers (SQN). Each element of the array contains a 43-bit SEQ value. The initial value for all array elements should be zero.

In its binary representation, the SQN extracted from the authentication token (AUTN) consists of two concatenated parts SQN=SEQ || IND. The SEQ is the batch number and IND is used to index into the array. IND represents the last 5 bits of the 6-byte SQN.

The SQN values are stored in the EFSQN (See “EFSQN” on page 16.) under the USIM.

Acceptance Rule

An SEQ extracted from an AUTN is deemed fresh if and only if the following three conditions are satisfied.

- SEQ>SEQ(IND) where SEQ(IND) is the value stored in the array element indexed using the IND component of the same SQN.
- SEQ-SEQMS < Δ
  where: $\Delta = 2^{\alpha}$
  SEQMS is the highest SEQ number among the 32-element array stored in the USIM.
  Value of α can be configured during personalization.
  If α = 43, this rule is always true.
- SEQMS - SEQ < L
  where: $L = 2^{\beta}$
  Value of β can be configured during personalization.
  If β = 43, this rule is always true.

The value of α and β will be stored in the EFAUTHPARAM and configured by using **Update Binary** command after the creation of the file.

If SEQ is not fresh then the re-synchronization procedure should be invoked.

List Update

If the SEQ number is accepted, it will overwrite the value that it was checked against in the array. Furthermore, the Operating System (OS) will also check if the newly accepted SEQ is greater than SEQMS (record 1 of EFSQN). If yes, the SEQMS is also updated.

Authentication Counter

The number of times authentication can be issued can be controlled through an authentication counter. The authentication counter is a three-byte counter stored in the EFAUTHCOUNT that is directly located under the MF. See “EFAUTHCOUNT” on page 17

The counter is active only if EFAUTHCOUNT exists and is activated.

Customizing RES Length

The RES length of the authenticate command can be customized and the desired size value stored in the EFAUTHPARAM, directly located under the MF. See “Authenticate Configuration (EF AUTHPARAM)” on page 16.

The size parameter is coded in bits. The valid range for 3G Milenage algorithm is from 32 to 64 bits and for 3G Dummy XOR algorithm is from 32 to 128 bits. If the value is out of range, or EFAUTHPARAM does not exist / is deactivated, then the default value is assumed (that is, eight bytes for 3G Milenage algorithm, 16 bytes for 3G Dummy XOR algorithm).

Customizing for the Milenage Algorithm:

- The behavior of the Milenage algorithm can be customized by changing the values of Ci, Ri and OPC.
- Ci and Ri values are customized during the personalization stage, after which further modification is not possible.
- The OPC value is stored in the key file. Modification of this value depends on the access condition of the key file. See “Key EFs (EFKEY)” on page 15.

5

Specific Applicative Card Mechanisms

File Sharing Mechanism

File sharing is required to share EFs that are both accessible in GSM and 3G mode so that data modified in the GSM mode is visible in the 3G mode and vice-versa. The file (link file) which is using the body of another file (data file) is indicated in the **Create File** command.

When creating a link file, the path of the data file should be specified.

Caution: Limitations on file sharing:

- Selecting a link EF will fail if the corresponding data file cannot be located.
- When attempted to delete a data file, it is logically deleted if there is any link file dependent on it.
- The data file will continue to exist in the memory until all the link files that dependent on it are deleted.
- The access condition follows that of the current EF.
- The current EF reference is not modified.
- The current DF reference is not modified.
- No nesting is possible, the path specified during creation of a link EF must refer to a data file.
- A link EF cannot be extended.

Backtracking Mechanism

This mechanism is used if, when executing a command, the correct PIN or EF$_{ARR}$ file is not found locally.

For Global PINs

Universal PIN, all global PINs and ADMs are directly located under the MF. An error occurs if the requested file is not found. Hence, global secret codes do not use backtracking.

For Local PINs

Backtracking applies to the local PIN EFs. However, rules apply to govern the searching of local PINs from one DF to its parent DF.

- If the current EF/DF is under an active ADF, then local PINs are searched directly under ADF.
- If the current EF/DF is not under an active ADF, then the local PINs are searched first directly in the current DF. Backtracking is used when one of the following conditions exist:
  - EFPIN is not found,
  - EFPIN is deactivated,

Backtracking stops once the MF has been reached.

For EFARR

EFARR is located by the following mechanism:

- For MF/ADF, the EFARR is located directly under the MF.
- For DF, the EFARR is first searched at the same level as the current DF (that is, the sibling of the DF, if the EFARR cannot be located, then backtracking is used).
- For EF, the EFARR is first searched under the current DF (that is, sibling of the EF, if the EFARR cannot be located, then backtracking is used).
- Backtracking is used when any one of the following arise:
  - EFARR is not found.
  - EFARR is deactivated.

Backtracking stops when the MF is reached or the ADF is reached.

6

Data Integrity

Sensitive Data Integrity

A specific mechanism guarantees the integrity of the sensitive data written in the EEPROM. This mechanism ensures that sensitive data is not altered or corrupted when the card is removed from the reader, and that data is not lost if the reader is switched off during a session.

Before sensitive data is modified, the operating system makes a backup copy of the current data. If the card is removed before modifications have been completed, or if the terminal is switched off, the previous card data is restored at the beginning of the next session, and the modifications are discarded.

A backup is carried out for all write operations involving sensitive data (that is, secret code EFs, secret key EFs, and file descriptors). The backup data is stored in special backup fields.

Cyclic EF Data Integrity

As a general rule, cyclic files are updated very frequently.

In order to anticipate any problems which may possibly arise from high update rates, and in particular EEPROM failures, the operating system uses a special protective mechanism.

This mechanism implements a file update process which avoids placing excessive stress on the record pointer and the checksum (both contained in the file descriptor).

The operating system manages all cyclic files in the same way, thus enhancing their life expectancy and, more generally, data integrity.

7

Communication Protocol

T=0 Protocol

In the T=0 protocol, the terminal always acts as the master, dictating instructions to the slave card as to whether it should be in reception or transmission mode. The T=0 standard does not allow for a simultaneous exchange between the card and the terminal. The one-way communication channel thus always originates from the terminal.

Incoming Commands

Incoming commands are those by which the terminal sends data to the card. These commands have the following structure:

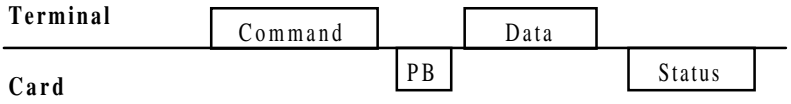

Figure 10 - Incoming Command Structure

Outgoing Commands

Outgoing commands are those whereby the terminal requests data from the card. They have the following structure:

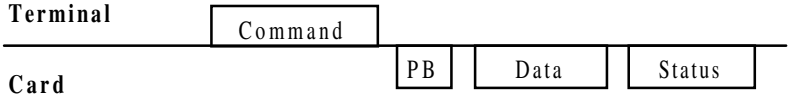

Figure 11 - Outgoing Command Structure

The T=0 standard is explained in full in the ISO 7816-3 Standard.

Protocol Parameter Selection (PPS)

Protocol Parameter Selection (also known as PTS - Protocol Type Selection) allows the Mobile Equipment (ME) to instruct the card to change the protocol (speed) used.

The PPS feature must be implemented on both the mobile equipment and the card, but can only be initiated by the mobile equipment.

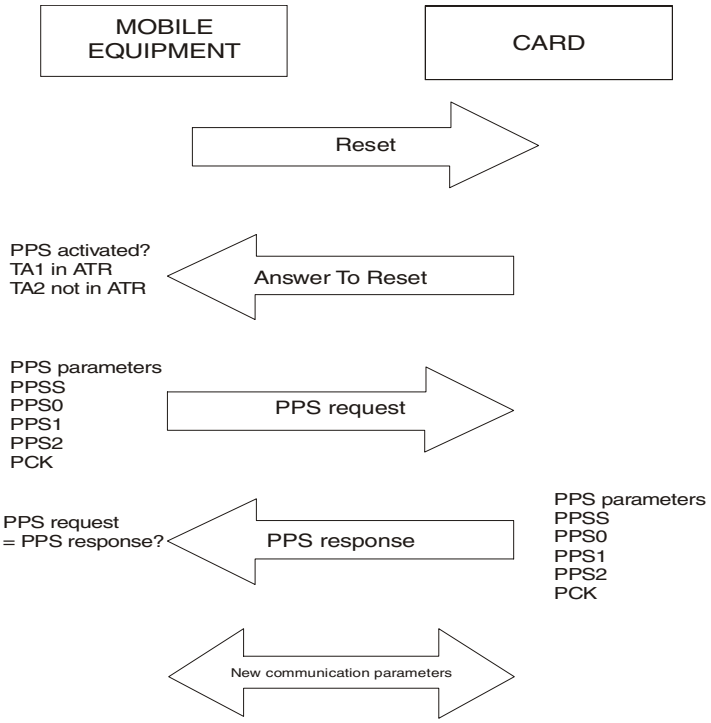

Figure 12 - Protocol Parameter Selection (PPS)

The TA1 values (that is, speed parameters) handled by GemXplore 3G V2 are defined in the following table.

TA1	F/D	Speed (baud)	Frequency (MHz)
11h	372	9,600	3.5712
94h	64	57,600	3.6864
95h	32	115,200	3.6864

Table 21 - Speed Parameters

This procedure involves the following steps:

1. PPS is initiated by the Mobile Equipment (ME) immediately after the **Answer To Reset** (ATR), provided the card is in negotiable mode (that is, TA2 not in the ATR and PPS not already accepted by the card during the current session).
2. The ME sends a PPS request and the card returns a PPS response. The PPS request and PPS response messages both contain one identifier character (PPSS), followed by a message format character (PPS0), three optional parameter characters (PPS1, PPS2 and PPS3), and a checksum (PCK).
3. The PPS is considered successful if the PPS response is exactly the same as the PPS request. In this case the card and the ME use the new settings to communicate.

   A PPS is also considered successful if the PPS response does not contain the PPS1 character used in the PPS request, the other characters being the same (excepting the checksum and PPS0 indicating no PPS1). In this case the card indicates that the default values will be used.

The following diagram gives examples of successful PPS procedures, illustrating these two cases. The first one initiates a specific mode (that is, the ME and the card communicate with the new parameters and no other PPS is allowed during the card session) whereas the second one leaves the card and the ME in negotiable mode (that is to say, the ME and the card communicate with the default parameters and PPS is still allowed). See “Appendix A - Answer To Reset” for further details.

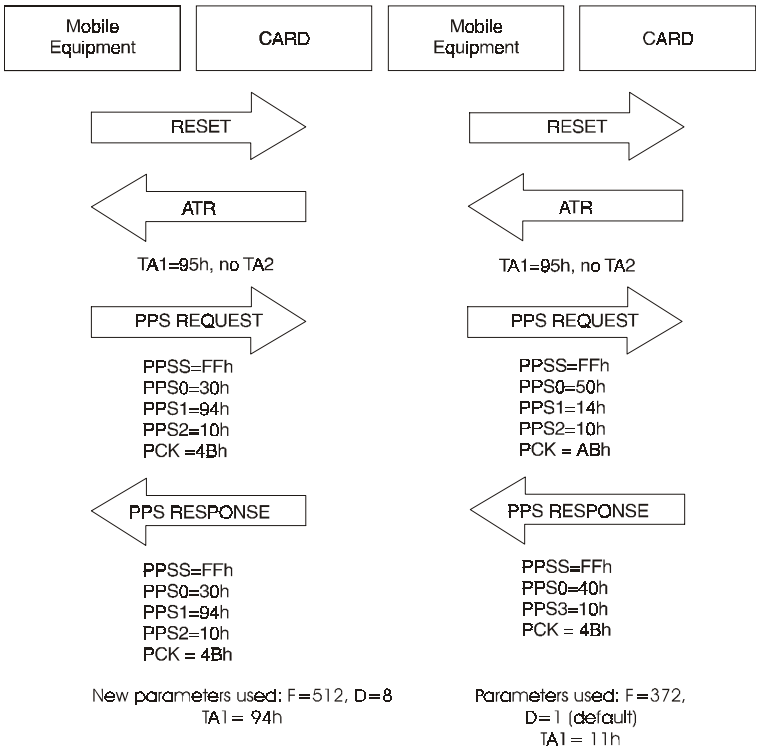

Figure 13 - Examples of Protocol Parameter Selection (PPS)

In the first case, the PPS request and the PPS response match exactly. As a result, the card and the ME are in a specific mode and any subsequent PPS will not be taken into account by the card.

In the second case, the parameters used are still the default ones because the card indicates that it does not handle the parameters requested by the ME. The ME is allowed to initiate another PPS without resetting the card.

8

GemXplore 3G V2 Command Format

GemXplore 3G V2 uses the APDU (Application Data Protocol Unit) command and response formats defined in the ISO 7816-4 standard. This ensures that the commands are compatible with the Gemplus Card Reader (GCR) Interface Driver Library. It should however be kept in mind that the GemXplore transport layer protocol is compliant with the ISO 7816-3 T = 0 standard. In this standard, APDUs are converted into TPDUs (Transport Data Protocol Units). The reader sends command TPDUs to the card, and the card returns response TPDUs to the reader.

In the T=0 protocol, the terminal always acts as the master, and the card as the slave, with the terminal indicating to the card whether it should be in reception or transmission mode. The T=0 standard does not allow for simultaneous exchanges between the card and the terminal. The one-way communication channel always originates from the terminal.

GemXplore 3G V2 handles commands in any of the following cases:

- **Case 1**
  No command or response data.
  Transported as a T=0 ISO-IN TPDU with the length = 0.
- **Case 2**
  Short format. No command data. Response data between 1 and 256 bytes.
  Transported as a T=0 ISO-OUT TPDU.
- **Case 3**
  Short format. Command data between 1 and 255 bytes. No response data.
  Transported as a T=0 ISO-IN TPDU.
- **Case 4**
  Short format. Command data between 1 and 255 bytes. Response data between 1 and 256 bytes.

  The command is transported as a T=0 ISO-IN TPDU and must be followed by a **Get Response** command transported as a T=0 ISO-IN TPDU. The Get Response mechanism is compliant with the ISO 7816-4 standard.

If commands are received in a different class, GemXplore 3G V2 returns a SW1 = 6Eh, SW2 = 00h status code and the command fails. If commands received include incorrect instructions, GemXplore 3G V2 returns a SW1 = 6Dh, SW2 = 00h status code and the command fails.

The APDU format defines the length of the data sent to the card (Lc) and the length of the data expected in response (Le). When the Lc and Le parameter values are different from 00h (that is, case 4 above), the response data (Le) can only be retrieved by sending the card a **Get Response** command.

Command Format

GemXplore 3G V2 handles commands in the following format:

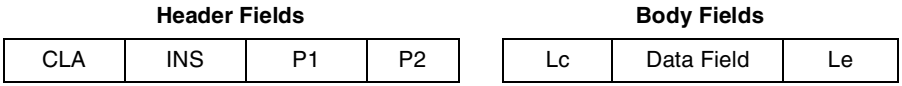

Figure 14 - GemXplore 3G V2 Command Format

Header Fields

The header fields are mandatory:

Field Name	Length in bytes	Description
CLA	1	Instruction class for 3G commands
INS	1	Instruction code. This is given in the command descriptions
P1	1	Parameter 1
P2	1	Parameter 2

Body Fields

The command body is optional. It may contain the following fields:

Field Name	Length in bytes	Description
Lc	1	Data length
Data	variable	Command parameters or data
Le	1	Expected length of data to be returned

Response Format

GemXplore 3G V2 transmits responses in the following format:

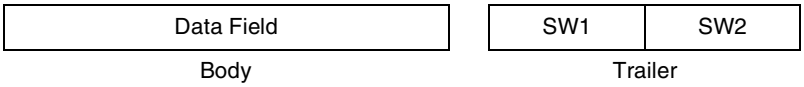

Figure 15 - GemXplore 3G V2 Response Format

The body is optional and holds the data returned by the card.

The trailer includes the two following mandatory bytes:

SW1: Status byte 1, which returns the command processing status

SW2: Status byte 2, which returns the command processing qualifications

Response Transmission

In order to allow response APDUs to be transmitted under the T=0 transport protocol, you execute the **Get Response** command (see “Get Response” on page 155). The **Get Response** command should be executed for all APDU case 4 format commands (for example, **Select**).

Detail of the T=0 Cases

The following table illustrates the commands sent by the terminal and the responses from the card.

Case 1			
P3 = 0	**Terminal**		**Card**
	[CLA INS P1 P2 P3]	=>	
		<=	SW from card
Case 2			
P3=0	**Terminal**		**Card**
(Licc[1] ≠ 256)	[CLA INS P1 P2 00]	=>	
		<=	6CLicc[1]
	[CLA INS P1 P2 Licc[1]]	=>	
		<=	INS [Data(Licc[1])] 90 00
	[Other command]	=>	
		<=	[normal exe]
P3=Licc[1]	**Terminal**		**Card**
(P3=0 and Licc[1]=256)	[CLA INS P1 P2 Licc[1]]	=>	
		<=	INS [Data(Licc[1])] 90 00
	[Other command]	=>	
		<=	[normal exe]

P3<Licc[1]	Terminal		Card
	[CLA INS P1 P2 P3]	=>	
		<=	INS [Data(P3)] 61 < Licc[1]-P3>
	00 C0 00 00 YY	=>	
		<=	C0 [Data(YY)] 61 ZZ
	00 C0 00 00 ZZ	=>	
		<=	C0 [Data(YY)] 90 00
	00 C0 00 00 Le> Licc[1]or Le=0	=>	
		<=	6C Licc[1]
		=>	
	[Other command] (even during chaining)	<=	[normal exe]
P3>Licc	**Terminal**		**Card**
	[CLA INS P1 P2 P3]	=>	
		<=	6C Licc[1]
	[CLA INS P1 P2 Licc[1]]	=>	
		<=	INS [Data(Licc[1])] 90 00
	[Other command]	=>	
		<=	[normal exe]
Case 3			
P3 <> 0	**Terminal**		**Card**
	[CLA INS P1 P2 P3]	=>	
		<=	INS
	[Data(P3)]	=>	
		<=	SW from card

Case 4			
All P3	**Terminal**		**Card**
	[CLA INS P1 P2 Lc]	=>	
		<=	INS
	[Data (Lc)]	=>	
		<=	61 Licc[1]
	00 C0 00 00 XX	=>	
		<=	C0 [Data(XX)] 61 YY
	00 C0 00 00 YY	=>	
		<=	C0 [Data(YY)] 90 00
	00 C0 00 00 Le>Licc[1]	=>	
		<=	6C Licc[1]
	[Other command]	=>	
	(even during chaining)	<=	[normal exe]

Licc[1]: means the remaining size. If Le is equal to zero or greater than the remaining size, status code 6CXX will be returned.

Table 22 - T = 0 Command Response Sequences

9

Operational Commands

This section describes the GemXplore 3G V2 commands compliant with those described in the *ETSI TS 102 221 version 4.2.0* specifications, referred to as the Operational commands.

Administrative commands that compliant with those described in the *ETSI TS 102 222 version 3.2.0* specifications and proprietary Gemplus commands are described in “Chapter 10 - Administrative Commands”.

Other commands (test commands) are outside the scope of this document. For details on these commands please contact your local Gemplus representative.

GemXplore 3G V2 Commands

Command Name	Mode	Code							Type
		Header				Body			
		CLA	INS	P1	P2	Lc	Data	Le	
Select	**3G**	00h	A4h	Smode	Smode	00h-10h	Data	*	ISO-IN
	GSM	A0h	A4h	Smode	00h	02h	Data	16h/0Fh	ISO-IN
Status	**3G**	80h	F2h	00h/01h/02h	Smode	-	-	*	ISO-OUT
	GSM	A0h	F2h	00h	00h	-	-	16h	ISO-OUT
Read Binary	**3G**	00h	B0h	OffHigh/SFI	OffLow	-	-	01h-FFh	ISO-OUT
	GSM	A0h	B0h	OffHigh	OffLow	-	-	01h-FFh	ISO-OUT
Update Binary	**3G**	00h	D6h	OffHigh/SFI	OffLow	00h-FFh	Data	-	ISO-IN
	GSM	A0h	D6h	OffHigh	OffLow	00h-FFh	Data	-	ISO-IN
Read Record	**3G**	00h	B2h	Record	Mode	-	-	01h-FFh	ISO-OUT
	GSM	A0h	B2h	Record	Address Mode	-	-	01h-FFh	ISO-OUT
Update Record	**3G**	00h	DCh	Record no.	Mode	01h-FF	Data	-	ISO-IN
	GSM	A0h	DCh	Record no.	Address Mode	01h-FF	Data	-	ISO-IN
Search Seek	**3G**	00h	A2h	Record no.	Mode	*	Pattern	*	ISO-IN
	GSM	A0h	A2h	00h	Mode	*	Pattern	00h/01h	ISO-IN
Increase	**3G**	80h	32h	00h/SFI	00h	01h-80h	Data	01h-FFh	ISO-IN
	GSM	A0h	32h	00h	00h	03h	Data	01h-FFh	ISO-IN
Verify PIN Verify CHV	**3G**	00h	20h	00h	PIN no.	08h/00h	PIN no.	-	ISO-IN
	GSM	A0h	20h	00h	Secret Code	08h	Secret Value	-	ISO-IN
Change PIN	**3G**	00h	24h	00h	PIN no.	10h	PIN values	-	ISO-IN
Change CHV	**GSM**	A0h	24h	00h	Secret Code.	10h	Secret values	-	ISO-IN

Command Name	Mode	Code							Type
		Header				Body			
		CLA	INS	P1	P2	Lc	Data	Le	
Disable PIN	**3G**	00h	26h	Replacement	PIN no.	08h	PIN Value	-	ISO-IN
Disable CHV	**GSM**	A0h	26h	00h	Secret Code	08h	Secret Value	-	ISO-IN
Enable PIN	**3G**	00h	28h	00h	PIN no.	08h	PIN Value	-	ISO-IN
Enable CHV	**GSM**	A0h	28h	00h	Secret Code	08h	Secret Value	-	ISO-IN
Unblock PIN	**3G**	00h	2Ch	00h	PIN no.	10h/00h	PIN Value	-	ISO-IN
Unblock CHV	**GSM**	A0h	2Ch	00h	Secret Code	10h	Secret Value	-	ISO-IN
Deactivate File	**3G**	00h	04h	Smode	00h	0xh	Data	-	ISO-IN
Invalidate	**GSM**	A0h	04h	00h	00h	00h	-	-	ISO-IN
Activate File	**3G**	00h	44h	Smode	00h	0xh	Data	-	ISO-IN
Rehabilitate	**GSM**	A0h	44h	00h	00h	00h	-	-	ISO-IN
Authenticate	**3G**	00h	88h	00h	Smode	*	Authenticate data	-	ISO-IN
Run GSM Algorithm	**GSM**	A0h	88h	00h	00h	10h	Random Value	-	ISO-IN
Manage Channel	**3G**	00h	70h	Operation Code	Channel no.	-	-	00h/01h	ISO-OUT
	GSM	-	-	-	-	-	-	-	-
Get Challenge	**3G**	00h	84h	00h	00h	-	-	01h–08h	ISO-OUT
	GSM	-	-	-	-	-	-	-	-
Get Response	**3G**	00h	C0h	00h	00h	-	-	00h/ SW2	ISO-OUT
	GSM	A0h	C0h	00h	00h	-	-	00h-FFh	ISO-OUT

* The length of data/response bytes (Lc/Le) varies.

SELECT

These commands are used to select an entity. The entity can be an EF, DF, MF or ADF.

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Lc	Data	Le
00h	A4h	Smode1	Smode2	Lc	Data	Le

for GSM:

CLA	INS	P1	P2	Lc	Data	Le
A0h	A4h	Smode1	00h	02h	Data	Le

Where

Smode 1 (3G): The selection mode (identifier, child number, path).

bit7 to bit5: RFU (set to 0)

bit 4 to bit 0: refer to the coding as follows:

b4	b3	b2	b1	b0	Action and Data
0	0	0	0	0	Select MF, DF or EF by File Identifier (FID)
0	0	0	0	1	Select child DF of the current DF
0	0	0	1	1	Select parent DF of the current DF (no data)
0	0	1	0	0	Select by DF name–Application Identifier (AID)
0	1	0	0	0	Select by path from MF
0	1	0	0	1	Select by path from current DF
1	0	0	0	1	Select by child number of the current DF, starts at 0001h (Gemplus proprietary).

Smode 1 (GSM): 0000 0000b: Select by FID. Refer to the notes below.

0001 0000: Select by child number of current DF, starts at 0001h (Gemplus proprietary)

Note: If P1=00, P2 set to 0Ch (no data returned) and the data field is empty, then MF is set as the current directory.

To avoid ambiguities when P1=00, the following search order applies when selecting a file with FID as a parameter:

1. Immediate children of the current DF
2. The parent DF
3. The immediate children of the parent DF

Smode 2 (3G) The command selection mode (application session or selection by AID control).

b7	b6	b5	b4	b3	b2	b1	b0	Meaning
0	**X**	**X**	**0**	**-**	**-**	**-**	**-**	**Application session control:**
0	0	0	0	-	-	-	-	Activation / Reset
0	1	0	0	-	-	-	-	Termination
0	**-**	**-**	**0**	**X**	**X**	**-**	**-**	**File Control Information (FCP) required:**
0	-	-	0	0	1	-	-	Return FCP template
0	-	-	0	1	1	-	-	No FCP returned
0	**-**	**-**	**0**	**-**	**-**	**X**	**X**	**Selection by AID control1:**
0	-	-	0	-	-	0	0	First or only occurrence
0	-	-	0	-	-	0	1	Last occurrence

:[1]: Only applies to ADF activation.

Lc / Data **for 3G:**

00h–for selecting parent DF of current DF

02h–file identifier or child number

01h to 10h–AID (full or partial)

02h, 04h, 06h, 08h or 0Ah–path

for GSM:

02h–file identifier or child number

Response

The response is returned in the following format:

Response	SW1	SW2

After a **Select** command, you can use the **Get Response** command to obtain data returned by the **Select** command.

The expected length of the data to be returned by the **Get Response** command must be lower than or equal to the length of the available data which is indicated in the status code returned by the **Select** command.

The information available for the **Get Response** command is detailed in subsequent tables.

Note: This information remains available until a command other than **Get Response** is used after a **Select** command.

3G Response

Response After 3G Selection of Dedicated Files.

The response data holds the FCP template of the selected file. The FCP template varies depending on the type of file selected.

Byte No.	Description
1	FCP template tag = 62h
2 to 3	Length of data expected in BER -TLV = L
3–(2+L) or 4–(3+L)	FCP template

FCP Template Description for 3G Selection of Dedicated Files.

Byte No.	TAG	Description
3 to 6 or 4 to 7	82h	File Descriptor
7 to 10 or 8 to 11	83h	File Identifier
11 to 19 or 12 to 20	A5h	Proprietary Information
20 to 22 or 21 to 23	8Ah	Life Card Status Integer
23 to 22+X or 24 to 23+X where X = 5 or 8	8Bh	Security Attributes
23+X to 22+X+(Y+2) or 24+X to 23+X+(Y+2)	C6h	PIN Status Template DO (Length = Y)

File Descriptor Description for 3G Selection of Dedicated Files.

Byte No.	Description
1	Tag = 82h
2	Length = 02h
3	**File Descriptor Byte:** b7 = RFU b6 = 0–Not Shareable file = 1–Shareable file b5b4b3 = 111–File type DF b2b1b0 = 000–EF structure, no information given
4	Data coding byte = 21h

File Identifier Description for 3G Selection of Dedicated Files.

Byte No.	Description
1	Tag = 83h
2	Length = 02h
3–4	File Identifier

Proprietary Information Description for 3G Selection of Dedicated Files.

Byte No.	Description
1	Tag = A5h
2	Length = 07h
3	UICC Characteristics Tag = 80h
4	Length = 01h
5	**Bit 7:** 0 – RFU **Bit 6** **Bit 5** **Bit 4** **Description** 0 0 1 Class A - Min: 4.5V to Max: 5.5V 0 1 0 Class B - Min: 2.7V to Max: 3.3V 1 0 0 Class C - Min: 1.62V to Max: 1.98V **Clock stop mode not allowed:** **Bit 3** **Bit 2** **Description** 0 0 Never 0 1 Unless at high level 1 0 Unless at low level 1 1 RFU **Clock stop mode allowed:** **Bit 3** **Bit 2** **Description** 0 0 No preferred level 0 1 High level preferred 1 0 Low level preferred 1 1 RFU **Bit 1:** 0 - RFU **Bit 0:** 1 - Clock stop mode allowed 0 - Clock stop mode not allowed
6	Amount of available EEPROM memory Tag = 83h
7	Length - 02h
8 to 9	Number of data bytes

Life Card Status Integer Description for 3G Selection of Dedicated Files.

Byte No.	Description				
1	Tag = 8Ah				
2	Length = 01h				
3	**Bits 7 -6 - 5 - 4:** 0000 - RFU				
	Bit 3	**Bit 2**	**Bit 1**	**Bit 0**	**Description**
	0	0	0	0	No information given
	0	0	0	1	Creation state
	0	0	1	1	Initialization state
	0	1	-	1	Operational state - activated
	0	1	-	0	Operational state - deactivated
	1	1	-	-	Termination state

Security Attribute description for 3G Selection of Dedicated Files.

Case 1: security attributes length = 5 bytes.

Byte No.	Description
1	Tag = 8Bh (for referenced to expanded format)
2	Length = 03h
3–4	EF$_{ARR}$ file ID
5	EF$_{ARR}$ record number

Case 2: security attributes length = 8 bytes.

Byte No.	Description
1	Tag = 8Bh (for referenced to expanded format)
2	Length = 06h
3–4	EF$_{ARR}$ file ID
5	SEID #01
6	EF$_{ARR}$ record number for SEID #01
7	SEID #00
8	EF$_{ARR}$ record number for SEID #00

PIN Status Template DO Description for 3G Selection of Dedicated Files.

Byte No.	Description
1	Tag = C6h
2	Length = Y bytes
3	PS_DO tag = 90h
4 /4–5	Length = 01h/02h
5 / 6	PS_DO byte
6 / 7	Usage qualifier DO tag = 95h
7 / 8	Length = 01h
8 / 9	Usage qualifier
9 / 10	Key reference tag = 83h
10 / 11	Length = 01h
11 / 12	Key reference
...	...
	Key reference tag = 83h
	Length = 01h
Y+2	Key reference

Note: PS_DO for MF

The pins included in the template consist of Global PINs, ADMs and Local PINs that is located directly under the MF.

PS_DO for DF/ADF under ADF

The pins included consists of the Global PINs and Local PINs under ADF. Global PINs that are not associated to ADF will not be returned.

PS_DO for DF outside ADF

When ADF is active:

The pins included consist of the associated Global PIN and all Local PINs directly under the current DF only.

When ADF is not active:

The pins included consist of the Global PINs and all Local PINs directly under the current DF only.

In general, the PIN status will be included in the template only when the following conditions are satisfied:

- ADM/PIN EF is activated

Response After 3G Selection of Application Dedicated Files.

Byte No.	TAG	Description
3 to 6 or 4 to 7	82h	File Descriptor
7 to 6+(L+2) or 8 to 7+(L+2)	84h	DF Name (AID), Length = L
9+L to 20+L or 10+L to 21+L	A5h	Proprietary Information
21+L to 23+L or 22+L to 24+L	8Ah	Life Card Status Integer
24+L to 23+L +X or 25+L to 24+L+X where X = 5 or 8	8Bh	Security Attributes
24+L +X to 23+L +X+(Y+2) or 25+L +X to 24+L +X+(Y+2)	C6h	PIN Status Template DO Length = Y

Table 23 - FCP Template Description for Selection of ADF

Byte No.	Description
1	Tag = 82h
2	Length = 02h
3	**File Descriptor Byte:** b7 = RFU b6 = 00–Not Shareable file = 01–Shareable file b5b4b3 = 111–File type DF b2b1b0 = 000–EF structure, no information given
4	Data coding byte = 21h

Table 24 - File Descriptor Description for Selection of ADF

Byte No.	Description
1	Tag = 84h
2	Length = 01h to 10h = L
3 to 2+L	DF Name

Table 25 - DF Name (AID) Description for Selection of ADF

Byte No.	Description
1	Tag = A5h
2	Length = 0Ah
3	UICC Characteristics Tag = 80h
4	Length = 01h
5	**Bit 7:** 0 – RFU **Bit 6** **Bit 5** **Bit 4** **Description** 0 0 1 Class A - Min: 4.5V to Max: 5.5V 0 1 0 Class B - Min: 2.7V to Max: 3.3V 1 0 0 Class C - Min: 1.62V to Max: 1.98V **Clock stop mode not allowed:** **Bit 3** **Bit 2** **Description** 0 0 Never 0 1 Unless at high level 1 0 Unless at low level 1 1 RFU **Clock stop mode allowed:** **Bit 3** **Bit 2** **Description** 0 0 No preferred level 0 1 High level preferred 1 0 Low level preferred 1 1 RFU **Bit 1:** 0 - RFU **Bit 0:** 1 - Clock stop mode allowed 0 - Clock stop mode not allowed
6	Application minimum clock frequency Tag = 82h
7	Length = 01h

Table 26 - Proprietary Information Description for Selection of ADF

Byte No.	Description	
8	0Ah - FEh:	Corresponding to 1 - 25.4 MHz with resolution of 0.1MHz
	FFh:	No application minimum clock frequency indicated
9	Amount of available EEPROM memory Tag = 83h	
10	Length = 02h	
11–12	Number of data bytes	

Table 26 - Proprietary Information Description for Selection of ADF (continued)

Byte No.	Description				
1	Tag = 8Ah				
2	Length = 01h				
3	**Bits 7 -6 - 5 - 4:** 0000 - RFU				
	Bit 3	**Bit 2**	**Bit 1**	**Bit 0**	**Description**
	0	0	0	0	No information given
	0	0	0	1	Creation state
	0	0	1	1	Initialization state
	0	1	-	1	Operational state - activated
	0	1	-	0	Operational state - deactivated
	1	1	-	-	Termination state

Table 27 - Life Card Status Integer Description for Selection of ADF

Byte No.	Description
1	Tag = 8Bh (for referenced to expanded format)
2	Length = 03h
3–4	EF$_{ARR}$ file ID
5	EF$_{ARR}$ record number

Table 28 - Security Attribute (5-byte) Description for Selection of ADF

Byte No.	Description
1	Tag = 8Bh (for referenced to expanded format)
2	Length = 06h
3–4	EF$_{ARR}$ file ID
5	SEID #01
6	EF$_{ARR}$ record number for SEID #01
7	SEID #00
8	EF$_{ARR}$ record number for SEID #00

Table 29 - Security Attribute (8-byte) Description for Selection of ADF

Byte No.	Description
1	Tag = C6h
2	Length = Y bytes
3	PS_DO tag = 90h
4	Length = 01h / 02h
5 / 5–6	PS_DO byte(s)
6 / 7	Usage qualifier DO tag = 95h
7 / 8	Length = 01h
8 / 9	Usage qualifier
9 / 10	Key reference tag = 83h
10 / 11	Length = 01h
11 / 12	Key reference
...	...
	Key reference tag = 83h
	Length = 01h
Y+2	Key reference

Table 30 - PIN Status Template DO Description for Selection of ADF

Response After 3G Selection of an Elementary File.

Byte No.	TAG	Description
3 to 9 or 4 to 10	82h	File Descriptor
10 to 13 or 11 to 14	83h	File Identifier
14 to 21 or 15 to 22	A5h	Proprietary Information
22 to 24 or 23 to 25	8Ah	Life Card Status Integer
25 to 24+X or 26 to 25+X where X = 5 or 8	8Bh	Security Attributes
25+X to 28+X or 26+X to 29+X	80h	File Size
29+X to 32+X or 30+X to 33+X	81h	Total File Size
33+X to 35+X or 34+X to 36+X	88h	Short File Identifier (optional)

Table 31 - FCP Template Description for Selection of an EF

Byte No.	Description
1	Tag = 82h
2	Length = 02h or 05h
3	**File Descriptor Byte:** b7 = RFU b6 = 0–Not Shareable file = 1–Shareable file b5b4b3 = 000–File type is operational EF **Bit2 Bit1 Bit0 Description** 0 0 1 Transparent EF 0 1 0 Linear EF 1 1 0 Cyclic EF
4	Data coding byte = 21h
5 to 6[1]	Record length byte 5: 00h, byte 6: XXh length of record
7	Number of records

Table 32 - File Descriptor Description for Selection of an EF

[1] Byte 5 to 7 are mandatory for linear fixed and cyclic files, otherwise they are not applicable.

Byte No.	Description
1	Tag = 83h
2	Length = 02h
3–4	File Identifier

Table 33 - File Identifier Description for Selection of an EF

Byte No.	Description
1	Tag = A5h
2	Length = 06h
3	UICC Characteristics Tag = 80h
4	Length = 01h
5	**Bit 7:** RFU **Bit 6 Bit 5 Bit 4 Description** 0 0 1 Class A - Min: 4.5V to Max: 5.5V 0 1 0 Class B - Min: 2.7V to Max: 3.3V 1 0 0 Class C - Min: 1.62V to Max: 1.98V **Clock stop mode not allowed:** **Bit 3 Bit 2 Description** 0 0 Never 0 1 Unless at high level 1 0 Unless at low level 1 1 RFU **Clock stop mode allowed:** **Bit 3 Bit 2 Description** 0 0 No preferred level 0 1 High level preferred 1 0 Low level preferred 1 1 RFU **Bit 1:** 0 - RFU **Bit 0:** 1 - Clock stop mode allowed 0 - Clock stop mode not allowed

Table 34 - Proprietary Information Description for Selection of an EF

Byte No.	Description
6	Special File Info Tag = C0h
7	Length = 01h
8	b7: 0 Low update activity : 1 High update activity b6: 0 Non readable and cannot be updated when invalidated : 1 Readable and can be updated when invalidated

Table 34 - Proprietary Information Description for Selection of an EF (continued)

Byte No.	Description				
1	Tag = 8Ah				
2	Length = 01h				
3	**Bits 7 -6 - 5 - 4:** 0000 - RFU				
	Bit 3	**Bit 2**	**Bit 1**	**Bit 0**	**Description**
	0	0	0	0	No information given
	0	0	0	1	Creation state
	0	0	1	1	Initialization state
	0	1	-	1	Operational state - activated
	0	1	-	0	Operational state - deactivated
	1	1	-	-	Termination state

Table 35 - Life Card Status Integer Description for Selection of an EF

Byte No.	Description
1	Tag = 8Bh (for referenced to expanded format)
2	Length = 03h
3–4	EF$_{ARR}$ file ID
5	EF$_{ARR}$ record number

Table 36 - Security Attribute (5-byte) Description for Selection of an EF

Byte No.	Description
1	Tag = 8Bh (for referenced to expanded format)
2	Length = 06h
3–4	EF$_{ARR}$ file ID
5	SEID #01
6	EF$_{ARR}$ record number for SEID #01
7	SEID #00
8	EF$_{ARR}$ record number for SEID #00

Table 37 - Security Attribute (8-byte) Description for Selection of an EF

Byte No.	Description
1	Tag = 80h
2	Length = 02h
3–4	Number of allocated data bytes in the file, excluding structural information

Table 38 - File Size Description for Selection of an EF

Byte No.	Description
1	Tag = 81h
2	Length = 02h
3 to 4	Number of allocated data bytes in the file, including structural information, if any.

Table 39 - Total File Size Description for Selection of an EF

Byte No.	Description
1	Tag = 88h
2	Length = 00h or 01h
3	SFI

Table 40 - Short File Identifier (SFI) Description for Selection of an EF

Note: If the TLV is not present, the SFI value is the five least significant bits of the FID.

If the TLV is present but empty, the SFI is not supported for the selected file.

If the length of the TLV is 1, the SFI is indicated in the five most significant bits of the TLV value field.

Tip: To improve the Select command performance, it is advisable to create local PIN file(s) and EFarr immediately under the ADF or DF. This is to shorten the file scanning time while preparing PS_DO response.

GSM Response

Byte No.	Description
1–2	RFU
3–4	Total amount of available EEPROM space
5–6	File identifier of the selected DF
7	Type of file: 01h for MF and 02h for DF
8–12	RFU
13	Number of remaining bytes (byte 14 to the end)
14	File characteristics: **Bit 7:** 0 = CHV1 enabled and 1 = CHV1 disabled **Bit 6–5:** RFU **Bit 4:** 3V technology card identification: 0 = 5V only card 1 = 3V technology card **Bits 3-2-0:** see the following **Bit 0 / Bit 2 / Bit 3 / Description** 1 / 0 / 0 / Clock stop allowed, no preferred level. 1 / 1 / 0 / Clock stop allowed, high level preferred. 1 / 0 / 1 / Clock stop allowed, low level preferred. 0 / 0 / 0 / Clock stop not allowed. 0 / 1 / 0 / Clock stop not allowed unless at high level. 0 / 0 / 1 / Clock stop not allowed unless at low level. **Bit 1:** minimum frequency: 0 = 13/8 MHz and 1 = 13/4 MHz
15	Number of DFs which are direct children of the current directory

Byte No.	Description
16	Number of EFs attached to the selected directory
17	Number of secret codes (CHV and ADM, and their respective Unblock codes) Examples: If there are CHV1, UNBLOCK CHV1, ADM2, UNBLOCK ADM2, the value for this byte is 04h.
18	RFU
19	CHV1 Status: Bit 7: 0 = code not activated and 1 = code activated Bits 6–4: RFU Bits 3–0: number of consecutive incorrect presentations remaining
20	UNBLOCK CHV1 Status: same bit assignment as for CHV1 code
21	CHV2 Status: same bit assignment as for CHV1 code
22	UNBLOCK CHV2 Status: same bit assignment as for CHV1 code

The different states of bytes 19–22 are described as follows for each case.

- Case 1: CHV1 and CHV2 present:

19	CHV1 Status
20	UNBLOCK CHV1 Status
21	CHV2 Status
22	UNBLOCK CHV2 Status

- Case 2: CHV1 and CHV2 not present: bytes 19–22 set to 00h.
- Case 3: only CHV1 present:

19	CHV1 Status
20	UNBLOCK CHV1 Status
21	00h
22	00h

- Case 4: only CHV2 present:

19	00h
20	00h
21	CHV2 Status
22	UNBLOCK CHV2 Status

Note: To determine whether the code is blocked in the above four cases, CHV1 or CHV2 file must be valid.

When an EF Is Selected.

Byte No.	Description
1–2	RFU
3–4	File size: Transparent EF: size of the body part Linear fixed or cyclic EFs: (record length) x (number of records)
5–6	File identifier
7	Type of file: 04h for EF
8	For transparent EFs and linear fixed EFs, this byte is RFU. For cyclic EFs, only bit 6 is used. The other bits are RFU. Bit 6: 0 = Increase command forbidden 1 = Increase command allowed on the file
9–11	General access conditions of the entities attached to the selected file - Transparent files: Read/Update/RFU/RFU/Rehabilitate/Invalidate - Linear fixed files: Read-Seek/Update/RFU/RFU/Rehabilitate/Invalidate - Cyclic files: Read-Seek/Update/Increase if authorized/RFU/Rehabilitate/Invalidate
12	File status: Bits 7 to 3: RFU Bit 2: 0 = not readable or cannot be updated when invalidated 1 = readable and can be updated when invalidated Bit 1: RFU Bit 0: 0 = invalidated 1 = not invalidated

Byte No.	Description
13	Number of remaining bytes (byte 14 to the end) = 02h
14	Structure of the EF: 00h transparent 01h linear fixed 03h cyclic
15	Record length (linear fixed or cyclic structure) 00h for transparent files

Note:

- **Bytes 3-4**: contain the body size of an EF. In the case of a formatted EF, the size is equal to the record length multiplied by the record number.
- **Bytes 9-11**: This field contains the lowest access condition to access the current entity. The level of access conditions in ascending order is: ALWAYS, CHV1, CHV2, ADM0, ADM1, ADM2, ADM3 and NEVER. The following table gives the corresponding access condition value.

Level	Access condition
0	Always
1	CHV1
2	CHV2
3	RFU
4	RFU
5	RFU
6	RFU
7	RFU
8	RFU
9	RFU
10	ADM1
11	ADM2
12	ADM3
13	ADM4
14	RFU
15	Never

Status Codes.

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
61h	XXh	9Fh	XXh	Command executed successfully with xxh bytes available for the **Get Response** command
90h	00h			Command executed successfully.
62h	83h			Selected File is deactivated
64h	00h			No active application. **Termination** is impossible.
67h	00h	67h	00h	Wrong Lc
69h	84h	94h	02h	Wrong child number
69h	86h			No active application exist previously or supplied AID mismatched for Activation or Reset using Last mode.
6Ah	82h	94h	04h	File not found
6Bh	00h	6Bh	00h	Incorrect P1 or P2 parameter
6Ch	XXh			Normal ending of the command with XXh bytes set to Le for next issuance of **Select** command.
6Fh	00h	92h	40h	DF or EF integrity error
6Fh	06h			FCP formatting aborted
6Fh	20h	6Fh	00h	Shared file (data file) not found

STATUS

This command returns information about the currently selected directory. It can be used at any time during a card session. There are no access conditions defined for this command.

The information returned is identical to that returned in response to **Select** command followed by a **Get Response** command. The application can send a **Status** command requesting fewer bytes than are available (coded in Le).

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Le
80h	F2h	Smode1	Smode2	Le

for GSM:

CLA	INS	P1	P2	Le
A0h	F2h	00h	00h	Le

Where:

Smode 1 (3G) bit7 to bit2: RFU (set to 0)

bit 1 to bit 0: refer to the following coding:

b1	b0	Action and Data
0	0	No indication
0	1	Current application is initialized in the ME
1	0	ME will initiate the termination of the current application
Any other values		RFU

Smode 2 (3G) bit7 to bit4: RFU (set to 0)

bit 3 to bit 0: refer to the following coding:

b3	b2	b1	b0	Action and Data
0	0	0	0	Response parameters and data identical to the response parameters and data of SELECT command
0	0	0	1	DFNAME of the currently selected application returned
1	1	0	0	No data returned
Any other value				RFU

Le Length of response bytes expected.

Response

The response is returned in the following format:

Response	SW1	SW2

3G Response

Response When Smode 2 = 00h, for Dedicated Files.

Byte No.	Description
1	FCP template tag = 62h
2 to 3	Length of data expected coding in BER TLV = L
3 to (2+L) or 4 to (3+L)	FCP template

Byte No.	TAG	Description
3 to 6 or 4 to 7	82h	File Descriptor
7 to 10 or 8 to 11	83h	File Identifier
11 to 19 or 12 to 20	A5h	Proprietary Information
20 to 22 or 21 to 23	8Ah	Life Card Status Integer
23 to 30 or 24 to 31	8Bh	Security Attributes
31 to 32+Y or 32 to 33+Y	C6h	PIN Status Template DO (Length = Y)

Table 41 - FCP Template Description for DF

Byte No.	Description	
1	Tag = 82h	
2	Length = 02h	
3	**File descriptor byte**	
	Bit 7	0 **-** RFU
	Bit 6	0 = File not shared 1 = File shared
	Bits 5 - 4 - 3	File Type 111 = DF
	Bits 3 - 2 - 0	EF structure 000 = No information given
4	Data coding byte = 21h	

Table 42 - File Descriptor Description for DF

Byte No.	Description
1	Tag = 83h
2	Length = 02h
3 - 4	File Identifier

Table 43 - File Identifier Description for DF

Byte No.	Description				
1	Tag = 8Ah				
2	Length = 01h				
3	**Bits 7 -6 - 5 - 4** RFU, set to 0				
	Bit 3	**Bit 2**	**Bit 1**	**Bit 0**	**Description**
	0	0	0	0	No information given
	0	0	0	1	Creation State
	0	0	1	1	Initialization State
	0	1	-	1	Operational State - activated
	0	1	-	0	Operational State - deactivated
	1	1	-	-	Termination State

Table 44 - Life Card Status Description for DF

Byte No.	Description
1	Tag = A5h
2	Length = 07h
3	UICC Characteristics Tag = 80h
4	Length = 01h
5	**Bit 7** RFU, set to 0 **Bit 6** **Bit 5** **Bit 4** **Description** 0 0 1 Class A - Min: 4.5V to Max: 5.5V 0 1 0 Class B - Min: 2.7V to Max: 3.3V 1 0 0 Class C - Min: 1.62V to Max: 1.98V **Clock stop mode allowed:** **Bit 3** **Bit 2** **Description** 0 0 No preferred level 0 1 High level preferred 1 0 Low level preferred 1 1 RFU **Clock stop mode not allowed:** **Bit 3** **Bit 2** **Description** 0 0 Never 0 1 Unless at high level 1 0 Unless at low level 1 1 RFU **Bit 1** RFU, set to 0 **Bit 0** Clock stop mode: 1 = allowed, 0 = not allowed
6	Amount of available EEPROM memory Tag = 83h
7	Length = 02h
8–9	Number of data bytes

Table 45 - Proprietary Information Description for DF

Byte No.	Description
1	Tag = 8Bh (for Referenced Format)
2	Length = 06h
3 - 4	EFARR File ID
5	SEID #00
6	EFARR Record Number for SEID #00
7	SEID #01
8	EFARR Record Number for SEID #01

Table 46 - Security Attributes Description for DF

Byte No.	Description
1	Tag = C6h
2	Length = Y bytes
3	PS_DO tag = 90h
4	Length = 01h / 02h
5 / 6	PS_DO byte
6 / 7	Usage qualifier DO tag = 95h
7 / 8	Length = 01h
8 / 9	Usage qualifier
9 / 10	Key reference tag = 83h
10 / 11	Length = 01h
11 / 12	Key reference
...	...
	Key reference tag = 83h
	Length = 01h
2+Y	Key reference

Table 47 - PIN Status Template DO Description (DFs)

Response When Smode 2 = 00h, for Application Dedicated Files .

Byte No.	TAG	Description
3 to 6 or 4 to 7	82h	File Descriptor
7 to 10 or 8 to 11	83h	File identifier
11 to 12+L or 12 to 13+L	84h	DF Name (AID) Length = L
13+L to 24+L or 14+L to 25+L	A5h	Proprietary Information
25+L to 27+L or 26+L to 28+L	8Ah	Life Card Status Integer
28+L to 35+L or 29+L to 36+L	8Bh	Security Attributes
36+L to 37+L+Y or 37+L to 38+L+Y	C6h	PIN Status Template DO (Length = Y)

Table 48 - FCP Template Description for ADF

Byte No.	Description
1	Tag = 82h
2	Length = 02h
3	**File descriptor byte** **Bit 7** 0 - RFU **Bit 6** 0 = File not shared 1 = File shared **Bits 5 - 4 - 3** File Type 111 = ADF **Bits 3 - 2 - 0** EF structure 000 = No information given
4	Data coding byte = 21h

Table 49 - File Descriptor Description for ADF

Byte No.	Description
1	Tag = 83h
2	Length = 02h
3–4	File Identifier

Table 50 - File Identifier Description for ADF

Byte No.	Description
1	Tag = 84h
2	Length = 01h to 10h = L
3 to 2+L	DF Name

Table 51 - Application Dedicated Identifier Description for ADF

Byte No.	Description
1	Tag = A5h
2	Length = 0Ah
3	UICC Characteristics Tag = 80h
4	Length = 01h
5	**Bit 7** RFU, set to 0 **Bit 6 Bit 5 Bit 4 Description** 0 0 1 Class A - Min: 4.5V to Max: 5.5V 0 1 0 Class B - Min: 2.7V to Max: 3.3V 1 0 0 Class C - Min: 1.62V to Max: 1.98V **Clock stop mode allowed:** **Bit 3 Bit 2 Description** 0 0 No preferred level 0 1 High level preferred 1 0 Low level preferred 1 1 RFU **Clock stop mode not allowed:** **Bit 3 Bit 2 Description** 0 0 Never 0 1 Unless at high level 1 0 Unless at low level 1 1 RFU Bit 1 RFU, set to 0 Bit 0 Clock stop mode: 1 = allowed, 0 = not allowed

Table 52 - Proprietary Information Description for ADF

Byte No.	Description
6	Application minimum clock frequency Tag = 82h
7	Length = 01h
8	0Ah-FEh: corresponding to 1-25.4MHz with resolution of 0.1MHz FFh: no application minimum clock frequency indicated
9	Amount of available EEPROM memory Tag = 83h
10	Length = 02h
11–12	Number of data bytes

Table 52 - Proprietary Information Description for ADF (continued)

Byte No.	Description				
1	Tag = 8Ah				
2	Length = 01h				
3	**Bits 7 -6 - 5 - 4** RFU, set to 0				
	Bit 3	**Bit 2**	**Bit 1**	**Bit 0**	**Description**
	0	0	0	0	No information given
	0	0	0	1	Creation State
	0	0	1	1	Initialization State
	0	1	-	1	Operational State - activated
	0	1	-	0	Operational State - deactivated
	1	1	-	-	Termination State

Table 53 - Life Card Status Description for ADF

Byte No.	Description
1	Tag = 8Bh (for Referenced Format)
2	Length = 06h
3 - 4	EF$_{ARR}$ File ID
5	SEID #00
6	EF$_{ARR}$ Record Number for SEID #00
7	SEID #01
8	EF$_{ARR}$ Record Number for SEID #01

Table 54 - Security Attributes Description for ADF

Byte No.	Description
1	Tag = C6h
2	Length = Y bytes
3	PS_DO tag = 90h
4	Length = 01h / 02h
5 / 6	PS_DO byte
6 / 7	Usage qualifier DO tag = 95h
7 / 8	Length = 01h
8 / 9	Usage qualifier
9 / 10	Key reference tag = 83h
10 / 11	Length = 01h
11 / 12	Key reference
...	...
	Key reference tag = 83h
	Length = 01h
2+Y	Key reference

Table 55 - PIN Status Template DO Description for ADF

Response When Smode 2 = 01h.

Byte No.	Description
1	Tag = 84h
2	Length = 01h to 10h = L
3 to 2+L	DF Name

Note: If no active ADF is selected, 6A82h is returned.

GSM Response

<table>
<tr><th>Byte No.</th><th>Description</th></tr>
<tr><td>1–2</td><td>RFU</td></tr>
<tr><td>3–4</td><td>Total amount of available EEPROM space</td></tr>
<tr><td>5–6</td><td>File identifier of the selected DF</td></tr>
<tr><td>7</td><td>Type of file: 01h for MF and 02h for DF</td></tr>
<tr><td>8–12</td><td>RFU</td></tr>
<tr><td>13</td><td>Number of remaining bytes (byte 14 to the end)</td></tr>
<tr><td>14</td><td>File characteristics:
Bit 7: 0 = CHV1 enabled and 1 = CHV1 disabled
Bit 6–5: RFU
Bit 4: 3V technology card identification:
0 = 5V only card
1 = 3V technology card
Bits 3-2-0: see the following
Bit 0 Bit 2 Bit 3 Description
1 0 0 Clock stop allowed, no preferred level.
1 1 0 Clock stop allowed, high level preferred.
1 0 1 Clock stop allowed, low level preferred.
0 0 0 Clock stop not allowed.
0 1 0 Clock stop not allowed unless at high level.
0 0 1 Clock stop not allowed unless at low level.
Bit 1: minimum frequency: 0 = 13/8 MHz and 1 = 13/4 MHz</td></tr>
<tr><td>15</td><td>Number of DFs which are direct children of the current directory</td></tr>
<tr><td>16</td><td>Number of EFs attached to the selected directory</td></tr>
<tr><td>17</td><td>Number of secret codes (CHV and ADM, and their respective Unblock codes)
Examples:
If there are CHV1, UNBLOCK CHV1, ADM2, UNBLOCK ADM2, the value for this byte is 04h.</td></tr>
<tr><td>18</td><td>RFU</td></tr>
<tr><td>19</td><td>CHV1 Status:
Bit 7: 0 = code not activated and 1 = code activated
Bits 6–4: RFU
Bits 3–0: number of consecutive incorrect presentations remaining</td></tr>
</table>

Byte No.	Description
20	UNBLOCK CHV1 Status: same bit assignment as for CHV1 code
21	CHV2 Status: same bit assignment as for CHV1 code
22	UNBLOCK CHV2 Status: same bit assignment as for CHV1 code

Byte 17: this field contains the number of codes CHV1, CHV2, ADM1 to ADM4 present and activated with EF not invalidated under the MF.

The different states of bytes 19–22 are described as follows for each case.

- Case 1: CHV1 and CHV2 present:

19	CHV1 Status
20	UNBLOCK CHV1 Status
21	CHV2 Status
22	UNBLOCK CHV2 Status

- Case 2: CHV1 and CHV2 not present: bytes 19–22 set to 00h.
- Case 3: only CHV1 present:

19	CHV1 Status
20	UNBLOCK CHV1 Status
21	00h
22	00h

- Case 4: only CHV2 present:

19	00h
20	00h
21	CHV2 Status
22	UNBLOCK CHV2 Status

Note: To determine whether the code is blocked in the above four cases, CHV1 or CHV2 file must be valid.

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	**SW2**	**SW1**	**SW2**	
90h	00h	90h	00h	Command executed successfully
61h	XXh	9Fh	XXh	Command executed successfully with XXh bytes available for the **Get Response** command
64h	00h			No active application and P1 = 01h or 02h
67h	00h	67h	00h	Incorrect parameter Le
6Bh	00h	6Bh	00h	Incorrect P1 or P2 parameter
6Fh	00h	92h	40h	DF or EF integrity error
6Fh	06h			FCP formatting aborted

READ BINARY

This command is used to read a string of bytes from the currently selected transparent EF or from the transparent EF selected using its Short File Identifier (SFI), if the **Read** access condition for the selected EF is satisfied.

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Le
00h	B0h	OffHigh or SFI	OffLow	Le

for GSM:

CLA	INS	P1	P2	Le
A0h	B0h	OffHigh	OffLow	Le

Where:

P1 (3G) If bit 7 is set to 1, SFI referencing is used. Bit 4 to bit 0 are the SFI (in the range 1 to 30), and P2 is the offset of the first byte to read.
If bit 7 is set to 0, bits 6 to 0 are the offset of the first byte to read.

P2 (3G) If bit 7 in P1 is set to 1, this parameter contains the offset from the beginning of the file coded on one byte.
If bit 7 in P1 is set to 0, this parameter contains the low offset. (The offset is defined on two bytes, and offset low corresponds to the LSB of the offset.)

P1, P2 (GSM) b7 to b0 of each P1 and P2 byte is the offset from the first byte to read.
P1 is the high part of the offset and P2 is the low part of the offset.

In both 3G and GSM, the first byte of a transparent EF is at offset 00h; a null offset (P1 P2 = 0000h) indicates that the read will be carried out from the beginning of the EF.

Le The length of the data requested (1-256 bytes).

For 3G: Le = 00 indicates any number of bytes in the range 1 to 256 to be read
For GSM: Le = 00 indicates 256 bytes to be read.

Response

The response is returned in the following format:

Response	SW1	SW2

Where:

Response	The data read in the current EF
SW1, SW2	The status codes

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
90h	00h	90h	00h	Command executed successfully
6Ch	XXh			Command executed successfully and Le = 0. XXh is the number of bytes available between the offset position and the end of the file (maximum of 255 bytes).
67h	00h	67h	00h	Incorrect parameter Le
6Ah	86h			Incorrect parameter P1 and P2 in SFI mode. SFI is not within the range from 1 to 30
69h	81h	94h	08h	Current EF is inconsistent with the command (not a transparent EF)
69h	82h	98h	04h	Access condition not fulfilled
69h	86h	94h	00h	No EF selected
6Ah	82h			File not found in SFI mode
6Bh	00h	6Bh	00h	Incorrect P1 or P2 parameter
6Fh	00h			File integrity error
69h	84h	98h	10h	Current file is deactivated

UPDATE BINARY

This command is used to update a string of bytes in the currently selected transparent EF or in the transparent EF selected using its Short File Identifier (SFI) coded in P1.

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Lc	Data
00h	D6h	OffHigh or SFI	OffLow	Lc	Data

for GSM:

CLA	INS	P1	P2	Lc	Data
A0h	D6h	OffHigh	OffLow	Lc	Data

Where:

P1 (3G) If bit 7 is set to 1, SFI referencing is used. Bit 4 to bit 0 are the SFI (in the range 1 to 30), and P2 is the offset of the first byte to update.
If bit 7 is set to 0, bits 6 to 0 are the offset of the first byte to update.

P2 (3G) If bit 7 in P1 is set to 1, this parameter contains the offset from the beginning of the file coded on one byte.
If bit 7 in P1 is set to 0, this parameter contains the low offset. (The offset is defined on two bytes, and offset low corresponds to the LSB of the offset.)

P1, P2 (GSM) b7 to b0 of each P1 and P2 byte is the offset from the first byte to update.
P1 is the high part of the offset and P2 is the low part of the offset.

Lc The length of the data to be updated (in the range 0 to 255 bytes)

Data The data to be updated in the selected transparent EF

The first byte of a transparent EF is at offset 00h; a null offset (P1 P2 = 0000h) indicates that the Update will be carried out from the beginning of the EF.

Response

SW1	SW2

The card updates the EF, and returns SW1 and SW2 status codes.

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
90h	00h	90h	00h	Command executed successfully
67h	00h	67h	00h	Incorrect parameter Le
69h	82h	98h	04h	Access condition not fulfilled
69h	81h	94h	08h	File is inconsistent with the command (not a transparent EF)
69h	86h	94h	00h	No EF selected
6Ah	82h			File not found in SFI mode
6Ah	86h			incorrect parameter P1 and P2 in SFI mode. SFI is not within the range from 1 to 30
6Bh	00h	6Bh	00h	Incorrect P1 or P2 parameter
6Fh	00h			File integrity error.
69h	84h	98h	10h	Current file is deactivated

READ RECORD

This command is used to read the contents of a record in a current linear fixed or cyclic EF. EFs can be selected by using Short File Identifier (SFI) coding in P2. If the **Read Record** command contains a valid SFI, the record pointer moves to the specified record and resets it as the current record. Any subsequent records can be read individually without SFI after a successful **Read Record** command.

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Le
00h	B2h	Record number	Addressing mode	Le

for GSM:

CLA	INS	P1	P2	Le
A0h	B2h	Record number	Addressing mode	Le

Where::

Record number — The record number or the offset.

Addressing mode (3G) — The addressing mode with or without the SFI. (The five msb of this field indicate the SFI of the file to be read. If these bits are set to 0, the command is applied to the current EF.) The coding of the addressing mode is described in the following table.

Rn(P1)	Addressing Mode (P2)								Description
	7	6	5	4	3	2	1	0	
	0	0	0	0	0	-	-	-	Currently Selected EF
	x	x	x	x	x	-	-	-	SFI (1 to 30)
00h	x	x	x	x	x	0	1	0	Next record
00h	x	x	x	x	x	0	1	1	Previous record
00h	x	x	x	x	x	1	0	0	Current record
Rec#	x	x	x	x	x	1	0	0	Absolute record. The record number is given in P1. P1=00h, denoting the current record and P1=XXh for the absolute mode.
Offset	x	x	x	x	x	1	1	1	Current mode with relative offset (variable length)

Addressing mode (GSM) The addressing mode (see the following table).

P1	P2	Address Mode
xx	02h	Next record
xx	03h	Previous record
00	04h	Current record
Rec #	04h	Absolute record Rn
Offset	07h	Current by offset (variable length)

Where:

xx is a value between 00h and FFh

Next record	The current record position is incremented before the read operation. If no current record is selected before the execution of the Read command, the first record of the EF is selected and becomes the current record which is then read. If the last record of a linear fixed EF is currently selected, the command has no effect, and an error message is returned. If the last physical record of a cyclic EF is currently selected, the next logical record will be the first physical record and is read.
Previous record	The current record position is decremented before the read operation. If no current record is selected before the execution of the Read command, the last record of the EF is selected and becomes the current record which is then read. If the first record of a linear fixed EF is currently selected, the command has no effect, and an error message is returned. If the first physical record of a cyclic EF is currently selected, the previous logical record will be the last physical record and is read.
Current record	The read operation is executed on the current record, the position of the current record is not affected. If no record is selected before this command, the card returns an error message.
Absolute record	The read operation is executed on the record defined by Rn, the position of the current record is not affected.
Current by offset	The read operation is executed on the current record starting from offset Rn and on Le bytes. A 00h offset means to read from the beginning of the record. If no record is selected before this command, the card returns an error message. The offset must be lower than the record length, and the offset (Rn) plus the length (Le) must be lower than or equal to the record length, otherwise the card returns an error.

Note: Current and absolute modes do not modify the current record pointer before execution of the read.
Previous and next modes modify the current record pointer.
Execution of the Read Record command does not modify the security context, whether the command was successful or not.

Le	The expected data length (in the range 1 to 255 bytes).

Response

The response is returned in the following format:

Response	SW1	SW2

Where:

Rdata The contents of the record

SW1, SW2 The status codes

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
6Ch	xxh	67h	00h	For mode 07, verify (offset + length to read) is lower than or equal to the record size
90h	00h	90h	00h	Command executed successfully
61h	xxh			Command executed successfully with xxh bytes available for the **Get Response** command
69h	86h	94h	00h	No EF selected
69h	84h	94h	02h	Mode and current pointer are inconsistent For linear fixed EFs: - Mode is Previous, but first record is currently selected - Mode is Next, but last record is currently selected - Mode is Current, but no record is currently selected
69h	81h	94h	08h	File is inconsistent with the command (not a formatted EF)
69h	82h	98h	04h	Read access condition not fulfilled
6Ah	82h			File not found in SFI mode
6Ah	83h	94h	02h	Incorrect P1 parameter: - Mode = Absolute and P1 > record quantity in EF
6Bh	00h	6Bh	00h	Incorrect P2 parameter: - Mode = Next or Previous and P1 is not equal to 0 - Mode ≠ Next, Previous, Current or Current by Offset
6Ah	86h			Incorrect parameter P1, P2 in SFI mode (SFI is not within the range from 1 to 30)
69h	84h	98h	10h	Current file is deactivated/invalidated

UPDATE RECORD

This command is used to update (erase then write) the contents of the current linear fixed or cyclic EF. The EF can be selected by using Short File Identifier (SFI) coding in P2. For a cyclic file, this function should be used only if the EF has assigned an **Update** access condition, and this condition is fulfilled.

If the **Update Record** command contains a valid SFI, the record pointer moves to the specified record and resets it as the current record. Any subsequent records can be read individually without SFI after a successful **Update Record** command.

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Lc	Data
00h	DCh	Record Number	Addressing mode	Lc	Data

for GSM:

CLA	INS	P1	P2	Lc	Data
A0h	DCh	Record Number	Addressing mode	Lc	Data

Where:

Record number	The record number or the offset.
Addressing mode (3G)	The addressing mode with or without the SFI. (The five msb of this field indicate the SFI of the file to be updated. If these bits are set to 0, the command is applied to the current EF.) The coding of the addressing mode is described in the following table.

This table defines the available address mode options:

Rn(P1)	Addressing Mode (P2)								Description
	0	0	0	0	0	-	-	-	Currently Selected EF
	x	x	x	x	x	-	-	-	SFI (1 to 30)
00h	x	x	x	x	x	0	1	0	Next record
00h	x	x	x	x	x	0	1	1	Previous record
00h	x	x	x	x	x	1	0	0	Current record
Rec#	x	x	x	x	x	1	0	0	Absolute record The record number is given in P1. P1=00h, denoting the current record and P1=XXh for the absolute mode.
Offset	x	x	x	x	x	1	1	1	Current mode with relative offset (variable length)

Addressing mode (GSM) The addressing mode (see the following table).

P1	P2	Address Mode
xx	02h	Next record
xx	03h	Previous record
00	04h	Current record
Rec #	04h	Absolute record Rn
Offset	07h	Current by offset (variable length)

Where:

xx is a value between 00h and FFh

For Linear Fixed EFs:

Next mode	The current record position is incremented before the update operation. If no record is currently selected, the first record is selected and updated. If the last record is currently selected, the command has no effect, and an error message is returned.
Previous mode	The current record position is decremented before the update operation. If no record is currently selected, the last record is selected and updated. If the first record is currently selected, the command has no effect, and an error message is returned.
Current mode	The current record is updated; the current record position is not affected. If no linear fixed record is selected before this command, the card returns an error message.
Absolute mode	The record defined by Rn is updated; the current record position is not affected.
Current by offset	The update operation is executed on the current record starting from offset Rn and on Le bytes. A 00h offset means to update from the beginning of the record. If no record is selected before this command, the card returns an error message. The offset must be lower than the record length, and the offset (Rn) plus the length (Le) must be lower than or equal to the record length, otherwise the card returns an error.

For Cyclic EFs:

Previous mode	Once the file is full, the oldest record is systematically updated, regardless of the position of the currently selected record. The updated record becomes the current record.

Note: Only previous mode is available with cyclic EFs.

Lc	The length of the record to be updated (1-255 bytes).
Data	The data to be used for the update.

Response

The card updates the EF if the conditions described above are met, and returns the SW1 and SW2 status bytes.

SW1	SW2

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
90h	00h	90h	00h	Command executed successfully
		67h	00h	For mode 07, verify (offset + length to update) is lower than or equal to the record size.
69h	86h	94h	00h	No EF selected
69h	84h	94h	02h	Mode and current pointer are not consistent For linear fixed EFs: - Mode is Previous, but the first record is currently selected - Mode is Next, but the last record is currently selected - Mode is Current, but no record is currently selected For Cyclic File: - Mode = Previous.
69h	81h	94h	08h	File is inconsistent with the command (not formatted EF)
69h	82h	98h	04h	Access condition not fulfilled
6Ah	82h			File not found in SFI mode
6Ah	83h	6Bh	00h	Incorrect parameter P1 - Mode = Absolute and P1 > record quantity in EF.
6Ah	86h			Incorrect parameter P1, P2 in SFI mode (SFI is not within the range from 1 to 30)
6Bh	00h	6Bh	00h	Incorrect P2 parameter: - Mode = Next or Previous and P1 is not equal to 0 - Mode ≠ Next, Previous, Current or Current by Offset
69h	84h	98h	10h	Current file is deactivated/invalidated

SEARCH/SEEK

This command is used to search(3G) / seek(GSM) for a character string of up to 255 bytes, in the currently selected linear fixed or cyclic EF or an EF addressed using the Short File Identifier (SFI).

The operating system handles EFs and their extensions as a single logical entity.

If the pattern search succeeds, the first record containing the character string becomes the current record. If the search fails, the current record stays unchanged.

The matching record's numbers are returned.

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Lc	Data	Le
00h	A2h	Record number (Rn)	Smode	Lc	Pattern	Le

for GSM:

CLA	INS	P1	P2	Lc	Data	Le
A0h	A2h	00h	Smode	Lc	Pattern	Le

Where:

Rn	The record number. If P1 is not specified and the search is to be started from P1, then if there is a record pointer pointing to a record in the current record EF, this pointer will be used as the default starting point.
Smode	The Search/Seek Record mode as described in subsequent tables.

Simple Search Mode Coding for 3G:

b7	b6	b5	b4	b3	b2	b1	b0	Meaning
0	0	0	0	0	-	-	-	Currently selected EF
X	X	X	X	X	-	-	-	Short File Identifier
1	1	1	1	1	-	-	-	RFU
-	-	-	-	-	0	X	X	RFU
-	-	-	-	-	1	0	0	**Simple Search** Start forward search from record Rn indicated in P1
-	-	-	-	-	1	0	1	**Simple Search** Start backward search from record Rn indicated in P1
-	-	-	-	-	1	1	0	**Enhanced Mode** See subsequent table for the first byte coding in the data field for enhanced mode.

3G Coding of the First Byte in the Data Field in Enhanced Mode:

b7	b6	b5	b4	b3	b2	b1	b0	Meaning
0	0	0	0	-	-	-	-	RFU
-	-	-	-	0	-	-	-	Offset; the following byte indicates the absolute position within the record from which to start the search
-	-	-	-	1	-	-	-	Offset, indicated as a character. The first occurrence of the character within the records after which the search starts is indicated in the following byte.
-	-	-	-	-	0	X	X	RFU
-	-	-	-	-	1	0	0	Start forward search from record Rn indicated in P1
-	-	-	-	-	1	0	1	Start backward search from record Rn indicated in P1
-	-	-	-	-	1	1	0	Start forward search from **next record**
-	-	-	-	-	1	1	1	Start backward search from **previous record**

P2 value for GSM:

P2	Description
x0h	Search from the first to the last record in the EF
x1h	Search from the last to the first record in the EF
x2h	Search from the next record to the last record in the EF. If no record is selected, **Seek** searches from the first record in the EF
x3h	Search from previous record to the first record in the EF. If no record is selected, **Seek** searches from the last record in the EF
0xh - type 1	The record pointer is set to the record that contains the pattern, but no output is available. Compatible with GSM 11.11 phase 1
1xh - type 2	The record pointer is set to the record containing the pattern. The output is the record number

Lc — The length of the pattern you want to search. The pattern length is limited to 255 bytes, and 253 bytes for 3G enhanced mode.

Pattern — For 3G:

- for simple search: search string
- for enhanced search: search indication (two bytes) followed by search string.
- for proprietary search: proprietary data.

Le — For 3G:

00h: 61hXXh is returned with XX indicated the available data.

Other values: Up to Le bytes are returned.

For GSM:

Empty for type 1, 01h for type 2.

Response

The response is returned in the following format:

Response	SW1	SW2

Where:

Response	Contains the record number(s) found with the search pattern
SW1, SW2	The status codes

The data returned by the **Search Record** command (that is, the status codes and the numbers of the matching records if the search succeeds) is obtained by using **Get Response**. See "Get Response" on page 155.

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
61h	XXh			Command executed successfully with XXh byte(s) available for the **Get Response** command
90h	00h	90h	00h	Normal ending of the command (type 1 only) in GSM and for 3G with byte(s) available in the data out
		9Fh	01h	Normal ending of the command with 1 byte available for the **Get Response** command (type 2 only)
69h	86h	94h	00h	No EF selected
69h	84h			Mode and current pointer not consistent: Invalid data. - Mode is Previous, but the first record is currently selected - Mode is Next, but the last record is currently selected - Only apply to 3G, mode is current, but no record is currently selected
6Ah	83h	94h	04h	Pattern not found / first occurrence of delimiter not found
69h	81h	94h	08h	File is inconsistent with the command
69h	82h	98h	04h	Access condition not fulfilled
6Ah	82h			File not found using SFI
6Ah	86h			SFI out of range
67h	00h	67h	00h	Incorrect length (Lc) parameter
6Bh	00h	6Bh	00h	Incorrect P1 or P2 parameter A check for Enhance mode parameters
69h	84h	98h	10h	Current file is deactivated(3G) or invalidated (GSM)

INCREASE

The **Increase** command gets the value sent by the terminal and adds it to the value of the last increased or updated record of the current cyclic elementary file or a cyclic EF addressed using the Short File Identifier (SFI). The result is then stored in the oldest written record which becomes the current record (with logical number 1).

This command can only be used on cyclic files to which an Increase access condition has been assigned and fulfilled.

If the result exceeds the maximum record value (all bytes set to FFh), the record is not updated.

The data returned by the **Increase** command is obtained by using **Get Response.**

If, in 3G mode, a non-selected file is the object of a successful command, it becomes selected.

The maximum record length is limited to 127 bytes.

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Lc	Data	Le
80h	32h	SFI / 00h	00h	Lc	Value	Le

for GSM:

CLA	INS	P1	P2	Lc	Data	Le
A0h	32h	00h	00h	03h	Value	Le

Where:

P1(3G) if bit 7 is set to 1, the five least significant bits contain the SFI (from 1 to 30) of the cyclic file whose value is to be increased.

if this field is set to 00h, the current file's value is increased

Lc The length of the value to be added to the record, range from 1 to 127 bytes for 3G and three bytes for GSM.

Value 1 to 127 byte(s) of value(s) to be added for 3G and three bytes for GSM.

Le The length of the expected response.

Response

The card returns the response in the following format:

Rec_val	Add_val	SW1	SW2

Field	Byte(s)	Description
Rec_val	1–X	Value of the increased record
Add_val	X+1–X+Lc	Value which has been added
SW1, SW2	2 bytes	Status bytes

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
90h	00h			Command executed successfully.
61h	XXh	9Fh	XXh	Command executed successfully with xxh bytes available for the **Get Response** command
65h	00h			Length of data bytes not available in response (Length > 256 bytes)
67h	00h	67h	00h	Incorrect length (Lc) parameter
69h	81h	94h	08h	In 3G / GSM session: - The file is not a cyclic EF In 3G session only: - Record length of the cyclic file is > 127.
69h	82h	98h	04h	Access condition not fulfilled
69h	86h	94h	00h	No EF is selected
6Bh	00h	6Bh	00h	Incorrect P1 or P2 parameter
6Fh	00h	92h	40h	File integrity error
69h	84h	98h	10h	EF deactivated(3G) or invalidated (GSM)
98h	50h	98h	50h	Value cannot be added, maximum record value has been reached

VERIFY PIN / CHV

This command is used to check that the cardholder or administrator knows the appropriate PIN or ADM secret code.

When the secret code is verified, the rights attached to it are granted. This command is also used to return the value of the security counter attached to the code specified in the P2 parameter.

If the code is not correct, the ratification counter is decreased. When the ratification counter reaches zero, the secret code is blocked and any rights associated with it are lost.

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Lc	Data
00h	20h	00h	PIN #	08h/00h	data

for GSM:

CLA	INS	P1	P2	Lc	Data
A0h	20h	00h	Secret Code #	08h	data

Where:

PIN# / Secret Code #

The codes must be specified in hexadecimal notation. The following are the values used to identify the code to be verified.

P2 Value	Secret PIN (3G)	Secret Code (GSM)
01h	Application PIN 1	CHV 1
02h	Application PIN 2	CHV 2
03h	Application PIN 3	N.A.
04h	Application PIN 4	N.A.
11h	Universal PIN	N.A.
0Ah	ADM 1	ADM 1
0Bh	ADM 2	ADM 2
0Ch	ADM 3	ADM 3
0Dh	ADM 4	ADM 4
81h	Local PIN 1	N.A.
82h	Local PIN 2	N.A.
83h	Local PIN 3	N.A.
84h	Local PIN 4	N.A.

Lc

The length of the PIN value, either 08h or 00h in 3G or 08h in GSM.

When Lc=00h in 3G, the retry counter value of PIN indicating in P2 and the status code 63hCXh are returned in response. The ‘X’ indicates the number of further allowed retries.

data

The PIN value / Secret code value.

Response

The card returns the SW1 and SW2 status codes.

SW1	SW2

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
90h	00h	90h	00h	Command executed successfully.
6Ah	88h	98h	02h	CHV / ADM / PIN is deactivated. DF or EF integrity error.
69h	84h	98h	08h	CHV / ADM / PIN file disabled.
63h	CXh	98h	04h	Unsuccessful CHV / ADM / PIN verification, at least one attempt left. X indicates the number of retries left in 3G.
69h	83h	98h	40h	CHV / ADM / PIN blocked.
67h	00h	67h	00h	Incorrect length (Lc) parameter.
6Bh	00h	6Bh	00h	Incorrect P1 or P2 parameter.
6Fh	00h	6Fh	00h	Memory error.

CHANGE PIN / CHV

This command is used to replace an existing PIN or ADM secret code with a new code. If the old secret code specified in the command parameters is correct, it is replaced by the new one. An incorrect specification of the secret code decrements the ratification counter. If the counter reaches 0, the secret code is blocked and any rights associated with it are lost.

Successful execution grants right attached to the PIN/ADM.

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Lc	Data
00h	24h	00h	PIN #	10h	Old_PIN New_PIN

for GSM:

CLA	INS	P1	P2	Lc	Data
A0h	24h	00h	Secret Code #	10h	Old_code New_code

Where:

PIN# / Secret Code #

The codes must be specified in hexadecimal notation. The following are the values used to identify the code to be verified.

P2 Value	Secret PIN (3G)	Secret Code (GSM)
01h	Application PIN 1	CHV 1
02h	Application PIN 2	CHV 2
03h	Application PIN 3	N.A.
04h	Application PIN 4	N.A.
11h	Universal PIN	N.A.
0Ah	ADM 1	ADM 1
0Bh	ADM 2	ADM 2
0Ch	ADM 3	ADM 3
0Dh	ADM 4	ADM 4
81h	Local PIN 1	N.A.
82h	Local PIN 2	N.A.
83h	Local PIN 3	N.A.
84h	Local PIN 4	N.A.

Old_PIN / code — The current PIN / Secret code value

New_PIN / code — The new PIN / Secret code value

Response

The card returns the SW1 and SW2 status codes.

SW1	SW2

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
90h	00h	90h	00h	Command executed successfully.
63h	CXh	98h	04h	Unsuccessful CHV / ADM / PIN verification, at least one attempt left. X indicates the number of retries left in 3G.
6Ah	88h	98h	02h	CHV / ADM / PIN is deactivated / invalidate. DF or EF integrity error.
69h	84h	98h	08h	CHV / ADM / PIN file change not allowed, PIN disabled.
69h	83h	98h	40h	CHV / ADM / PIN blocked.
67h	00h	67h	00h	Incorrect length (Lc) parameter.
6Bh	00h	6Bh	00h	Incorrect P1 or P2 parameter.
6Fh	00h	6Fh	00h	Memory error.

DISABLE PIN / CHV

This command is used to disable a PIN or secret code after a correct code presentation. For 3G, this command also allows using Universal PIN to replace the disabled PIN / code, if it is activated and enabled. After the successful execution of this command and if no replacement has been done, all processes and file accesses that were conditional on entering the PIN / Secret code correctly can then be accessed freely with no restriction, and without the requirement to enter the PIN / Secret code. Otherwise, Universal PIN has to be verified first.

If the PIN / Secret code specified in the command parameters is correct, the rights attached to the code will be granted freely (that is, not restricted by an access condition). The action of incorrect specification of secret code decrements the ratification counter. If the counter reaches 0, the secret code is blocked and any rights associated with it are lost.

Caution: In 3G session: Only replacement of the disabled PIN / code with Universal PIN is supported.

In GSM session: CHV2 cannot be disabled.

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Lc	Data
00h	26h	Replacement	PIN #	08h	PIN value

for GSM:

CLA	INS	P1	P2	Lc	Data
A0h	26h	00h	Secret Code #	08h	Secret Code

Where:

P1(3G)	b7	b6	b5	b4b3b2b1b0	
	0	0	0	0 0 0 0 0	Verification data present in data field.
	0	0	0	0 0 0 0 0	Reserved by ISO/IEC 7816-8.
	1	-	-	- - - - -	Verification data present, and use reference data number as verification replacement.
	-	X	X	- - - - -	‘00’ (other values are RFU).
	-	-	-	1 0 0 0 1	Global key reference for Universal PIN.

PIN# / Secret Code #

The codes must be specified in hexadecimal notation. The following are the values used to identify the code to be verified.

P2 Value	Secret PIN (3G)	Secret Code (GSM)
01h	Application PIN 1	CHV 1
02h	Application PIN 2	CHV 2
03h	Application PIN 3	N.A.
04h	Application PIN 4	N.A.
11h	Universal PIN	N.A.
0Ah	ADM 1	ADM 1
0Bh	ADM 2	ADM 2
0Ch	ADM 3	ADM 3
0Dh	ADM 4	ADM 4
81h	Local PIN 1	N.A.
82h	Local PIN 2	N.A.
83h	Local PIN 3	N.A.
84h	Local PIN 4	N.A.

Response

The card returns the SW1 and SW2 status codes.

SW1	SW2

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
90h	00h	90h	00h	Command executed successfully.
6Ah	88h	98h	02h	• CHV / ADM / PIN is deactivated / invalidated. • DF or EF integrity error. • Apply to 3G only: Universal PIN does not exist / deactivated.
62h	00h	98h	08h	PIN already disabled.
63h	CXh	98h	04h	Unsuccessful CHV / ADM / PIN verification, at least one attempt left. X indicates the number of retries left in 3G.
69h	83h	98h	40h	CHV / ADM / PIN blocked.
67h	00h	67h	00h	Incorrect length (Lc) parameter.
6Bh	00h	6Bh	00h	Incorrect P1 or P2 parameter.
6Fh	00h	6Fh	00h	Memory problem.
6Fh	15h	98h	08h	CHV / ADM / PIN disable is not allowed.

ENABLE PIN / CHV

This command is used to enable a PIN or secret code which has been disabled by the **Disable PIN / CHV** command. On enabling a code value, all the commands using the PIN / secret code as an access condition will again be restricted.

If the PIN / secret code specified in the command parameters is correct, the PIN / secret code is enabled. The action of specification of the wrong code decrements the ratification counter. If the counter reaches 0, the PIN / secret code is blocked and any rights associated with it are lost.
When a replaced PIN is enabled successfully, the replacement information is removed. Successful execution grants rights attached to the PIN/ADM.

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Lc	Data
00h	28h	00h	PIN #	08h	PIN value

for GSM:

CLA	INS	P1	P2	Lc	Data
A0h	28h	00h	Secret Code #	08h	Secret Code

Where:

PIN# / Secret Code #

The codes must be specified in hexadecimal notation. The following are the values used to identify the code to be verified.

P2 Value	Secret PIN (3G)	Secret Code (GSM)
01h	Application PIN 1	CHV 1
02h	Application PIN 2	CHV 2
03h	Application PIN 3	N.A.
04h	Application PIN 4	N.A.
11h	Universal PIN	N.A.
0Ah	ADM 1	ADM 1
0Bh	ADM 2	ADM 2
0Ch	ADM 3	ADM 3
0Dh	ADM 4	ADM 4
81h	Local PIN 1	N.A.
82h	Local PIN 2	N.A.
83h	Local PIN 3	N.A.
84h	Local PIN 4	N.A.

Response

The card returns the SW1 and SW2 status codes.

SW1	SW2

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
90h	00h	90h	00h	Command executed successfully.
6Ah	88h	98h	02h	CHV / ADM / PIN is deactivated. DF or EF integrity error.
62h	00h	98h	08h	PIN was enabled.
63h	CXh	98h	04h	Unsuccessful CHV / ADM / PIN verification, at least one attempt left. X indicates the number of retries left in 3G.
69h	83h	98h	40h	CHV / ADM / PIN blocked.
67h	00h	67h	00h	Incorrect length (Lc) parameter.
6Bh	00h	6Bh	00h	Incorrect P1 or P2 parameter.
6Fh	00h	6Fh	00h	Memory problem.
6Fh	15h	98h	08h	Enable not authorized.

UNBLOCK PIN / CHV

This command unblocks a PIN/ADM secret code which has been blocked by a given number (N) of consecutive wrong PIN/ADM code presentations. It does this by resetting the code's ratification counter to its maximum value (N). This command can be performed whatever the state of the PIN/ADM code (blocked or not blocked, disabled or enabled).

If the PIN/ADM unblocking code presented is correct:

- The value specified for the PIN/ADM code in the command parameters is assigned to the blocked PIN/ADM code.
- The number of remaining **Unblock PIN** attempts for the blocked PIN/ADM code is reset to its initial value.
- The PIN/ADM is enabled and the associated rights are granted.

If the PIN/ADM unblocking code presented is not correct, the number of remaining **Unblock PIN** attempts for the blocked PIN/ADM is decremented. After a definable number of incorrect PIN/ADM unblocking code presentations (not necessarily in the same card session), the PIN/ADM can no longer be unblocked, regardless of card sessions.

Note: Specifying the wrong PIN/ADM unblocking code has no effect on the status of the PIN/ADM code itself.

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Lc	Data
00h	2Ch	00h	PIN #	00h/10h	Unblock_PIN/ New_PIN

for GSM:

CLA	INS	P1	P2	Lc	Data
A0h	2Ch	00h	Secret Code #	10h	Unblock Code/ New_Code

Where:

PIN# / Secret Code #

The codes must be specified in hexadecimal notation. The following are the values used to identify the code to be verified.

P2 Value	Secret PIN (3G)	Secret Code (GSM)
00h	N.A.	CHV 1 (GSM 11.11 standard)
01h	Application PIN 1	CHV 1 (Gemplus proprietary)
02h	Application PIN 2	CHV 2
03h	Application PIN 3	N.A.
04h	Application PIN 4	N.A.
11h	Universal PIN	N.A.
0Ah	ADM 1	ADM 1
0Bh	ADM 2	ADM 2
0Ch	ADM 3	ADM 3
0Dh	ADM 4	ADM 4
81h	Local PIN 1	N.A.
82h	Local PIN 2	N.A.
83h	Local PIN 3	N.A.
84h	Local PIN 4	N.A.

Lc

When Lc=00h in 3G, the retry counter value of PIN indicating in P2 and the status code 63hCXh are returned in response. The ‘X’ indicates the number of further allowed retries.

Response

The card returns the SW1 and SW2 status codes.

SW1	SW2

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
90h	00h	90h	00h	Command executed successfully.
6Ah	88h	98h	02h	CHV / ADM / PIN is deactivated. DF or EF integrity error.
69h	83h	98h	40h	CHV / ADM / PIN blocked.
63h	CXh	98h	04h	Unsuccessful CHV / ADM / PIN verification, at least one attempt left. X indicates the number of retries left in 3G.
67h	00h	67h	00h	Incorrect length (Lc) parameter.
6Bh	00h	6Bh	00h	Incorrect P1 or P2 parameter.
6Fh	00h	6Fh	00h	• Memory problem. • Decrements number of unblock mechanism (if ≠ FFh). • Reset error counter of Unblock PIN / ADM, reset retry counter of PIN / ADM to its maximum value. • Update PIN / ADM and counters with their new values, enable EFPIN or EFADM.
6Fh	17h	6Fh	00h	Number of unblock mechanism is equal to 00h.

DEACTIVATE / INVALIDATE FILE

This command initiates a reversible deactivation (3G) / invalidation (GSM) of an EF. Deactivating / invalidating a file restricts the commands that can be applied to it; the **Select** and **Activate File** commands are the only commands that can operate on the file when deactivated / invalidated.
The Deactivate / Invalidate File access condition for the EF must be satisfied for this command to be performed, the LCSI under the file header will be updated accordingly upon execution.

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Lc	Data
00h	04h	Smode	00h	Lc	Data

for GSM:

CLA	INS	P1	P2	Lc
A0h	04h	00h	00h	00h

Where:

Smode **Bits 7 -6 - 5** RFU, set to 0

Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
0	0	0	0	0	Select EF by FID
0	1	0	0	0	Select by path from MF
0	1	0	0	1	Select by path from DF
1	0	0	0	1	Select child number of current DF (starts at 0001h)

Note: In 3G mode, if P1=P2=00h and the data field is empty, the command will be applied on the current EF.

Lc	02h–if select by file identifier or child number 02h, 04h, 06h, 08h or 0Ah–if select by path
Data	• ID of the entity to be selected. • Child number of entity to be selected (first one is #0001). • Path.

Response

The card returns the SW1 and SW2 status codes.

SW1	SW2

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
90h	00h	90h	00h	Command executed successfully
69h	86h	94h	00h	Command not allowed due to no EF is selected
69h	82h	98h	04h	Access condition not fulfilled
62h	83h	98h	10h	Current file is already deactivated / invalidate
6Ah	82h			File not found
67h	00h	67h	00h	Incorrect length (Lc) parameter
6Bh	00h	6Bh	00h	Incorrect P1 or P2 parameter
6Fh	00h	6Fh	00h	EF or DF integrity error

ACTIVATE / REHABILITATE FILE

The **Activate** (3G) / **Rehabilitate** (GSM) command combines the file selection and reactivate mechanisms in one single command. It reactivates a deactivated EF.

A successful execution of a file restores the use of the commands previously restricted by the **Deactivate / Invalidate** command, and this file has to be the currently selected file for GSM mode, but not necessary for 3G mode.

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Lc	Data
00h	44h	Smode	00h	Lc	data

for GSM:

CLA	INS	P1	P2	Lc
A0h	44h	00h	00h	00h

Where:

Smode Bits 7 -6 - 5 RFU, set to 0

Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
0	0	0	0	0	Select EF by FID
0	1	0	0	0	Select by path from MF
0	1	0	0	1	Select by path from DF
1	0	0	0	1	Select child number of current DF (starts at 0001h)

Note: For 3G, if P1=P2=00h and the data field is empty, then the command applies to the current EF.

Lc	02h–if select by file identifier or child number 02h, 04h, 06h, 08h or 0Ah–if select by path
Data	• ID of the entity to be selected. • Child number of entity to be selected (first one is #0001). • Path.

Response

The card returns the SW1 and SW2 status codes.

SW1	SW2

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
90h	00h	90h	00h	Command executed successfully
69h	86h	94h	00h	Command not allowed due to no EF is selected
62h	00h	98h	10h	Current file is already valid
69h	82h	98h	04h	Access condition not fulfilled
6Ah	82h			File not found
67h	00h	67h	00h	Incorrect Lc parameter
6Bh	00h	6Bh	00h	Incorrect P1 or P2 parameter
6Fh	00h	6Fh	00h	EF or DF integrity error

AUTHENTICATE / RUN GSM ALGORITHM

For 3G session–Authenticate:

In 3G mode, this command is used during the procedure for authenticating the USIM to its HE and vice versa. In addition, a cipher key and an integrity key are calculated. For the execution of the command the USIM uses the subscriber authentication key K, which is stored in the USIM.

The function is related to a particular USIM and should not be executable unless the USIM has been selected as the current application (current ADF) and the current directory is under or equal to the ADF and a successful PIN verification (if enabled) procedure has been performed. An application needs to be selected prior to the execution of the command.

Either one of the following algorithms can be used:

- The Milenage algorithm (under an active ADF).
- The 3G Dummy XOR algorithm.

For more information on 3G network authentication, refer to “Chapter 4 - 3G Network Security”.

The USIM also manages the two services present in the EFUST and related to GSM interworking:

- Service° 27 (GSM access): When activated, the USIM calculates the GSM response parameter Kc.
- Service° 38 (GSM security context): When activated, the USIM is able to calculate the GSM response parameters SRES and Kc from RAND.

For GSM session–Run GSM Algorithm :

During GSM network phase, this command is used during the procedure which authenticates the SIM card to the GSM network and calculates the call ciphering key Kc. It executes an algorithm which uses a 16-byte random number and a subscriber authentication key Ki that is stored in the SIM. The response data (4-byte SRES and 8-byte Kc, the call ciphering key) is obtained using the **Get Response** command.

Either one of the following algorithms can be used:

- the standard COMP128 version of A3A8 algorithm (only authorized under the DFGSM,
- the Milenage algorithm (under an DFGSM),
- the GSM XOR algorithm
- the 3G Dummy XOR algorithm.

If the algorithm is the standard COMP128 or Milenage, the command is authorized only if the current directory is the DFGSM (ID is 7F20h under MF) or a sub-DF of the DFGSM. If the algorithm is the XOR, the command is authorized everywhere in the file system.

If the MF selects DFDCS1800 (7F21h), either one of the following two cases is possible:

1. The DCS1800 simulation mechanism is enabled, the card internally selects the DFGSM (7F20h) and the use of the comp128 algorithm is allowed.
2. The DCS1800 simulation mechanism is disabled, the card selects the real DFDCS1800 (if it exists) and the use of comp128 algorithm and Milenage algorithm are forbidden.

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Lc	Data	Le
00h	88h	00h	P2	11h/22h	Data	Le

for GSM:

CLA	INS	P1	P2	Lc	Data	Le
A0h	88h	00h	00h	11h	Data	Le

Where:

P2 The authentication context:
81h: 3G context
80h: GSM context

Input Data in 3G Context

Byte No.	Length	Description
1	1 byte	Length of RAND (L1 = 10h)
2 to 17	16 bytes	RAND
18	1 byte	Length of AUTN (L2 = 10h) (for 3G context)
19 to 34	16 bytes	AUTN = SQN ⊕ AK || AMF || MAC (for 3G context) SQN = six bytes AMF = two bytes MAC = eight bytes

Note: AUTN is present only if a 3G context is used.

Input Data in GSM Context

Byte No.	Length	Description
1	1 byte	Length of RAND (L1 = 10h)
2 to 17	16 bytes	RAND

Response

The card returns the SW1 and SW2 status codes.

Response	SW1	SW2

The data returned by the **Authenticate** command is obtained by using **Get Response**. See“Get Response” on page 155.

The data returned depends on the success or failure of the 3G security context as shown in the following tables:

3G Response Message:

Case 1: Command Successful, 3G Context.

Byte No.	Length	Description
1	1 byte	“Successful 3G authentication” tag = DBh
2	1 byte	Length of RES (L3)
3 to (L3+2)	L3	RES The size of RES value is customized through EFAUTHPARAM.
(L3+3)	1 byte	Length of CK (L4=10h)
(L3+4) to (L3+L4+3)	16 bytes	CK
(L3+L4+4)	1 byte	Length of IK (L5=10h)
(L3+L4+5) to (L3+L4+L5+4)	16 bytes	IK
(L3+L4+L5+5)	1 byte	Length of Kc (8 bytes) (if service° 27 is available)
(L3+L4+L5+6) to (L3+L4+L5+13)	8 bytes	Kc (if service° 27 is available)

Note: The most significant bit of RES is coded on bit 7 of byte 3
The most significant bit of CK is coded on bit 7 of byte L3+4
The most significant bit of IK is coded on bit 7 of byte L3+L4+5

Case 2: Synchronization Failure, 3G Context.

Byte No.	Length	Description
1	1 byte	“Synchronization failure” tag = DCh
2	1 byte	Length of AUTS = 0Eh
3 to 16	L1 bytes	AUTS = $SQN_{MS} \oplus AK \parallel MAC–S$

Case 3: GSM Security Context, Command Successful.

Byte No.	Length	Description
1	1 byte	04h (length of SRES)
2 to 5	4 byte	SRES
6	1 byte	08h (Length of Kc)
7 to 14	8 bytes	Kc

GSM Response Message:

Byte No.	Length	Description
1 to 4	4 byte	SRES
5 to 12	8 bytes	Kc

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
61h	XXh	9Fh	XXh	Command executed successfully with XXh bytes available for **Get Response**
64h	00h			No ADF is active (for 3G session)
6Fh	01h	94h	08h	Context error: • Authentication counter is zero. • Key algorithm identifier not correct. • EF (for example: EFKEY, EFust) is deactivated. • EF not found. • EF size incorrect. • EF type incorrect. • Current DF not under the ADF.
69h	82h	98h	04h	No PIN1 presented successfully before the command
67h	00h	67h	00h	Incorrect Lc parameter. RAND size not equal to 10h.
6Bh	00h	6Bh	00h	Incorrect P1 or P2 parameter
98h	62h			MAC ≠ XMAC
98h	64h			Service° 38 not present for GSM context.

MANAGE CHANNEL

This command is only available in 3G mode and is managed by JCRE. It is used to open and close logical channels. The open function opens a new logical channel other than the basic channel ‘0’, and channel number to be opened is assigned by card. The close function explicitly closes a logical channel, and once this channel has been closed successfully, it can be reassigned.

The basic logical channel ‘0’ is always available and cannot be closed.

Format

This command is formatted as follows:

for 3G only:

CLA	INS	P1	P2	Le
00h	70h	P1	P2	Le

Where:

P1 Logical channel operation code.

bit 6–bit 0: RFU. The value set to ‘0’.

bit 7: value set to ‘0’ to open logical channel.
value set to ‘1’ to close logical channel.

P2 Channel selection.

bit 7–bit 2: RFU. The value set to ‘0’.

bit 1 and bit 0:
‘00’– If P1=00h, logical channel will be internally assigned by the UICC.
If P1≠ 00h means this is reserved.
‘01’– Logical channel number 1 is selected.
‘10’– Logical channel number 2 is selected.
‘11’– Logical channel number 3 is selected.

Le Le = 01h, if P1P2 = 00h 00h
Le = 00h, if P1P2 ≠ 00h 00h

Response

The card returns the SW1 and SW2 status codes.

Response	SW1	SW2

Where:

Response — Logical channel number opened if both P1 and P2 set to 00h.

Status Codes

The following status codes may be returned after this command:

3G (only)		Description
SW1	SW2	
90h	00h	Command executed successfully
67h	00h	Incorrect Le parameter
6Ah	86h	Incorrect parameter P1 or P2
6Fh	00h	No more channel available

GET CHALLENGE

This command is only available in 3G mode and is used to request the card to issue a challenge. The challenge is a random number which internally computed by the card.

Format

This command is formatted as follows:

for 3G only:

CLA	INS	P1	P2	Le
0xh	84h	00h	00h	Le

Where:

Le 01–08h.

Response

The card returns the SW1 and SW2 status codes.

Response	SW1	SW2

Where:

Response Random Number.

Status Codes

The following status codes may be returned after this command:

3G (only)		Description
SW1	SW2	
90h	00h	Command executed successfully
67h	00h	Incorrect Le parameter
6Bh	00h	Incorrect parameter P1 or P2

GET RESPONSE

This command returns the data generated by the operating system after the successful execution of either a **Select,** an **Run GSM Algorithm** (GSM) **/** an **Authenticate** (3G), a **Seek–type 2** (GSM) **/ Search** (3G), an **Increase** or an **Envelope** command.

The **Get Response** command must be performed immediately after the command for which response data is to be retrieved. The data will be lost once another command is issued.

The **Get Response** command is managed by the JCRE and the T=0 protocol.

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Le
00h	C0h	00h	00h	00h/SW2

for GSM:

CLA	INS	P1	P2	Le
A0h	C0h	00h	00h	Le

Where:

CLA — The class byte; the command is performed whatever the value for the class.

Le — The number of bytes expected in the response. The length of the expected data must be less than or equal to the length of the available data as follows:

Response

The card returns the SW1 and SW2 status codes.

Response	SW1	SW2

Where:

Response The data requested by the command

Content of the response field in 3G context:

Previous Command	Number of Available Bytes
Authenticate	Result of the authenticate command
Envelope	between 1 and 256 bytes
Search	Record number(s)
Select	File Control Parameter
Increase	(X+Lc) bytes which X is the length of the record up to maximum 253 bytes. • (1 to X) for the value of the increased record • (X+1) to (X+Lc) for the value which has been added
Status	FCP of current directory

Content of the response field in GSM context:

Previous Command	Number of Available Bytes
Run GSM Algorithm	0Ch bytes will be returned
Envelope	between 1 and 256 bytes
Seek (type 2)	01 byte (record number)
Select	• 0Fh for an EF • 16h for a DF
Increase	(X+3) bytes which X is the length of the record up to maximum 253 bytes. • (1 to X) for the value of the increased record • (X+1) to (X+3) for the value which has been added

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
90h	00h	90h	00h	Command executed successfully.
67h	00h	67h	00h	Incorrect length (Le) parameter.
6Bh	00h	6Bh	00h	Incorrect P1 or P2 parameter.
67h	00h	6Fh	00h	No data available.

SLEEP

This command is only available in GSM mode, as specified by the GSM 11.11 recommendation. It does not have any specific action on the SIM card as the components used have an internal wait mode which is effective automatically between each command as long as the I/O line remains idle.

Format

This command is formatted as follows:

for GSM only:

CLA	INS	P1	P2	Lc
A0h	FAh	00h	00h	00h

Response

The card returns the SW1 and SW2 status codes.

SW1	SW2

Status Codes

The following status codes may be returned after this command:

GSM (only)		Description
SW1	SW2	
90h	00h	Command executed successfully
67h	00h	Incorrect Lc parameter
6Bh	00h	Incorrect parameter P1 or P2
6Fh	00h	Memory problem

10

Administrative Commands

GET FILE INFO

This command can be used after a **Select** command to obtain special Gemplus proprietary information about the currently selected file. This causes the response data for **Get Response** to be lost.

There is no restriction on the number of times this command can be passed consecutively.

There are no access conditions defined for this command.

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Le
00h	A6h	00h	00h	Le

for GSM:

CLA	INS	P1	P2	Le
A0h	A6h	00h	00h	Le

Where:

Le (3G) The number of bytes expected:

- Up to 16 bytes for an EF, except EFPIN, EFADM and EFKEY
- Up to 17 bytes for a DF or ADF
- Up to 19 bytes for a PIN file
- Up to 20 bytes for a ADM file
- Up to 15 bytes for a Key file

Le (GSM) Maximum up to 16 bytes expected for a DF or an EF.

Response

The card returns the response in the following format:

Response	SW1	SW2

Where:

Response The current entity related data

SW1, SW2 The status codes

The tables below detail the data returned by the **Get File Info** command.

3G Response

If the current entity is a DF:

Byte No.	Description
1	Type of file (01h for MF, 02h for DF and 03h for ADF)
2–7[1]	Path name (without MF ID)
8–9	File ID of selected DF
10–11	EFARR ID
12	Record Number
13	Number of DFs under current DF
14	Number of EFs under current DF
15	PIN1 needed before Authenticate (always true), bit 0 set to 1
16–17	Total amount of available EEPROM space

[1]: If the current entity is the current active ADF, then 7FFFh is returned as part of the path name.

If the current entity is an EF (other than an EFPIN, EFADM or EFKEY file):

Byte No.	Description
1	Type of file = 04h (EF)
2–7	Path name (without MF ID)
8–9	File ID of selected EF
10–11	EF ARR ID
12	Record Number
13–16	RFU

If the current entity is an EFPIN file:

Byte No.	Description
1	Type of file = 04h (EF)
2–7	Path name (without MF ID)
8–9	File ID of selected EF
10–11	EF ARR ID
12	Record Number
13	RFU
14	Special file information **Bits 7-6-5:** RFU **Bit 4:** 1=disable/enable not authorized on PIN 0=disable/enable authorized on PIN **Bit 3:** 1=PIN disabled 0=PIN enabled **Bit2:** 1=PIN change not authorized 0=PIN change authorized **Bit1-0:** RFU
15	Number of remaining PIN attempts
16	PIN activation byte
17	Presentation type of PIN / UNBLOCK PIN
18	Number of remaining UNBLOCK PIN attempts
19	Number of remaining UNBLOCK PIN mechanisms

If the current entity is an EF$_{ADM}$ file:

Byte No.	Description
1	Type of file = 04h (EF)
2–7	Path name (without MF ID)
8–9	File ID of selected EF
10–11	EF ARR ID
12	Record Number
13	RFU
14	Special file information **Bits 7-6-5:** RFU **Bit 4:** 1=disable/enable not authorized on ADM 0=disable/enable authorized on ADM **Bit 3:** 1=ADM disabled 0=ADM enabled **Bit2:** 1=ADM change not authorized 0=ADM change authorized **Bit1-0:** RFU
15	Number of remaining ADM attempts
16	ADM activation byte
17	Presentation type of ADM / UNBLOCK ADM
18	Number of remaining UNBLOCK ADM attempts
19	Number of remaining UNBLOCK ADM mechanisms
20	Rights granted by the ADM code Bit 7 ADM4 Bit 6 ADM3 Bit 5 ADM2 Bit 4 ADM1 Bit 3 PIN4 Bit 2 PIN3 Bit 1 PIN2 Bit 0 PIN1

If the current entity is an EFKEY file:

Byte No.	Description
1	Type of file = 04h (EF)
2–7	Path name (without MF ID)
8–9	File ID of selected EF
10–11	EFARR ID
12	EFARR record number
13	Length of secret key
14	Algorithm Identifier of key **0x40:** COMP128 (GSM) **0x41:** GSM XOR **0x42:** 3G Dummy XOR **0x48:** 3G Milenage
15	RFU

GSM Response

If the current entity is a DF:

Byte No.	Description
1	Type of file (01h for MF and 02h for DF)
2–7	Path name (without MF ID)
8–9	File ID of selected DF
10–15	Access Conditions: byte 2: NU byte 3: NU byte 4: Delete / Create File byte 5: Extend byte 6: NU byte 7: NU
16–17	Total amount of available EEPROM space

If the current entity is an EF (other than an EFCHV, EFADM or EFKEY file):

Byte No.	Description
1	Type of file = 04h (EF)
2–7	Path name (without MF ID)
8–9	File ID of selected EF
10–15	Access Conditions: byte 2: Read byte 3: Update byte 4: RFU byte 5: RFU byte 6: Rehabilitate byte 7: Invalidate

If the current entity is an EFCHV file:

Byte No.	Description
1	Type of file = 04h (EF)
2–7	Path name (without MF ID)
8–9	File ID of selected EF
10–15	Access Conditions: byte 2: Read byte 3: Update byte 4: RFU byte 5: RFU byte 6: Rehabilitate byte 7: Invalidate
16	Special file information **bits 7–5:** 1 = disable / enable not authorized on CHV 0 = disable / enable authorized on CHV **bit 4:** 1 = CHV disabled 0 = CHV enabled **bit 3:** 1 = CHV change not authorized 0 = CHV change authorized **bits 1–0:** RFU
17	Number of remaining CHV attempts
18	CHV activation byte

Byte No.	Description
19	Presentation type of CHV / UNBLOCK CHV
20	Number of remaining UNBLOCK CHV attempts
21	Number of remaining UNBLOCK CHV mechanisms

If the current entity is an EF$_{ADM}$ file:

Byte No.	Description
1	Type of file = 04h (EF)
2–7	Path name (without MF ID)
8–9	File ID of selected EF
10–15	Access Conditions: byte 2: Read byte 3: Update byte 4: RFU byte 5: RFU byte 6: Rehabilitate byte 7: Invalidate
16	Special file information **Bits 7-6-5:** RFU **Bit 4:** 1=disable/enable not authorized on ADM 0=disable/enable authorized on ADM **Bit 3:** 1=ADM disabled 0=ADM enabled **Bit2:** 1=ADM change not authorized 0=ADM change authorized **Bit1-0:** RFU
17	Number of remaining ADM attempts
18	ADM activation byte
19	Presentation type of ADM / UNBLOCK ADM
20	Number of remaining UNBLOCK ADM attempts
21	Number of remaining UNBLOCK ADM mechanisms
22	Rights granted by the ADM presentation **Bit 7:** ADM4 **Bit 6:** ADM3 **Bit 5:** ADM2 **Bit 4:** ADM1 **Bit 3–2:** RFU **Bit 1:** CHV2 **Bit 0:** CHV1

If the current entity is an EFKEY file:

Byte No.	Description
1	Type of file = 04h (EF)
2–7	Path name (without MF ID)
8–9	File ID of selected EF
10–15	Access Conditions: byte 2: Read byte 3: Update byte 4: RFU byte 5: RFU byte 6: Rehabilitate byte 7: Invalidate
16	RFU
17	Algorithm identifier of key

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
90h	00h	90h	00h	Command executed successfully
67h	00h	67h	00h	Incorrect Le parameter
6Bh	00h	6Bh	00h	Incorrect P1 or P2 parameter
6Fh	00h	92h	40h	DF and EF integrity error

CREATE FILE

This command is used to create a GSM and 3G file (ADF–3G only, DF or an EF) under the current directory. The file that has been created becomes the currently selected file.

The MF is also created using the same command. However, it has to be created first, followed by the EFARR, otherwise, no other file creation is possible.
The creation of the MF does not start at a fixed location in the EEPROM due to the fragmentation mechanism. The sequence of creation of the MF then EFARR is known as Create Initial Sequence.

Note: During the Create Initial Sequence, following precautions need to be taken:

- During the EFARR creation, the file access condition in Security Environment SE01 and SE00 that specify in first and second records in the EFARR respectively, must be set to always.
- GSM access conditions for EFADM4 will be taken care at the time of creation in Tag 90.

This determines the end of the initialization phase for 3G-GSM file system. The files to be created here after are not restricted by any process, except certain exceptional cases for the ADF creation that need the existing of EFDIR.

Caution: Maximum number of DF:

- The OS supports up to 255 DFs including MF.
- The MF has DF sequence number of 0x01.

Maximum number of EF:

- The OS supports up to 255 EFs under a DF.

Maximum DF level:

- The OS supports up to four DF level including MF.

Maximum record length:

- The OS supports maximum record length of 254 for Cyclic file.
- The OS supports maximum record length of 255 for Linear fixed file except EFARR which has a maximum record length of 254.

Maximum number of record:

- The OS supports up to 254 records for both Cyclic and Linear fixed files.

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Lc	Data
00h	E0h	00h	00h	Lc	Data

for GSM:

CLA	INS	P1	P2	Lc	Data
A0	E0h	00h	00h	Lc	Data

Where:

Lc	The length of the subsequent data field. Refer to the following for the variable length.
Data	The data defining the file. Refer to the following for the detail contents.

Template Tag = 62h

For a MF / DF / ADF creation:

Byte No.	Description
1	Tag = 62h (M)
2	Length = 20+ (LC6+2) + (LA5+2) + (L84+2)
3	File Descriptor Byte (FDB) Tag = 82h (M)
4	Length = 2
5	File Descriptor Byte value: 38h / 78h for MF / DF / ADF **Value: b7 b6 b5 b4 b3-b0 Meaning** 38h 0 0 1 1 1000 The MF / DF / ADF is not a shareable file 78h 0 1 1 1 1000 The MF / DF / ADF is a shareable file You can differentiate between the MF and DF through the file identifier. For file identifier 3F00h, is exclusively reserved for MF. An ADF can only be created during a 3G session, for creating an ADF, a DF AID Tag is mandatory to specify its file type.

Table 56 - For MF/ADF/DF Creation

Byte No.	Description
6	Data Coding Byte = 21h
7	Memory Amount Tag = 81h (M)
8	Length = 2
9–10	The value specifies the amount of memory to be allocated to the DF = xxh xxh
11	File Identifier Tag = 83h (M)
12	Length = 2
13–14	File identifier = yyh yyh
15	Life Cycle Status Information (LCSI) Tag = 8Ah (M)
16	Length = 01h
17	LCSI value = X5h: **b7–b4 b3 b2 b1 b0 State** xxxx 0 1 0 1 Operational state activated xxxx 0 1 0 0 Operational state deactivated File can only be created when the operational state is set to active.
18	Security Attribute Tag = 8Bh – for referenced format (M). (Please see the details in the following pages)
19	Length = 3 / 4 / 6
20–21	EFARR file identifier
22[1]	Record Number–SEXX (Please see the details in the following pages)
23	PIN Status Template DO Tag = C6h (M).
24	Length = LC6
25– 24+LC6	PIN Status Template DO.(Tag = 90h) (Please see the details in the following pages)

Table 56 - For MF/ADF/DF Creation (continued)

Byte No.	Description
25+LC6	Proprietary status tag = A5h (O)
26+LC6	Length = LA5
27+LC6 28+LC6 29+LC6 – 32+LC6	GSM Access Condition Tag = 90h (O) Length = 04h AC1, AC2, AC3, AC4. See “Security Architecture” on page 31 If this object is not present, then AC1–AC4 is filled with zero (that is, access is NEVER)
33+LC6	DF AID Tag = 84h (O) – Only applies to ADFs
34+LC6	Length = L84 (In 3G, it is variable, 01h –10h)
35+LC6– 34+LC6+ L84	DF AID

[1]: The length of this field is either 1, 2 or 4 bytes.

Table 56 - For MF/ADF/DF Creation (continued)

Note:

- All mandatory tags are identified with (M) next to the tag. The presence of objects marked ‘O’ are optional.
- It is not possible to create file with file identifier 7FFFh, 3FFFh and FFFFh, as they are reserved file identifier.
- If the FID is 7F10 or 7F20, they will be treated as special DF (DF$_{TELECOM}$ and DF$_{GSM}$ respectively).
- If the FDB is not 38h or 78h, an error is returned.
- The Memory Amount Tag for DF is ignored, even though it is mandatory in the template.
- An ADF can only be created during a 3G session, and here the FID object is mandatory.

Security Attribute Tag (Tag: 8Bh)

This object contains the security attribute for 3G access. The object size can be either 03h or 04h or 06h. For 03h object size, only SE01 is supported. In case of both SE01 and SE00 are supported, SE01 must be prior SE00.

PIN Status Template DO (Tag: C6h)

This object contains the PIN status information for a DF or ADF, and PINs which are used for accessing to the DF or ADF and its children. The content of this object is as follows:

Byte No.	Description
1	PS_DO Tag = 90h (M)
2 / 2-3	Length = L90 (either 01h or 02h)
3 / 4	PS_DO
4 / 5	Usage Qualifier DO Tag = 95h (O)
5 / 6	Length = 01h
6 / 7	Usage Qualifier
7 / 8	Key Reference Tag = 83h
8 / 9	Length = 01h
9 / 10	Key Reference (PIN)
10 / 11	Key Reference Tag = 83h
11/ 12	Length = 01h
12 / 13	Key Reference (PIN)
	.....
LC6	.....

Note:

- The PIN Status Template is ignored during creation of MF or DF, even though it is mandatory in the template.
- The PIN Status Template is applicable only for the creation of ADF.
- The PS_DO object and the Usage Qualifier objects are ignored.
- There should be only one global PIN reference (any global PIN except Universal PIN). In case there is more than one global PIN reference, only the first encountered is used and the subsequence global PIN reference is ignored.

For a EF creation .

Byte No.	Description
1	Tag = 62h (M)
2	Length = 22 + L82 + LA5 + L88(if exists)
3	File Descriptor Byte (FDB) Tag = 82h (M)
4	Length L82
5–4+L82	File Descriptor Byte value. See subsequent section for the details.
5+L82	Number of bytes to be allocated to the EF = 80h (M)
6+L82	Length = 02h
(7+L82)–(8+L82)	Amount of memory to be allocated to the EF = xxh xxh
9+L82	File Identifier Tag = 83h (M)
10+L82	Length = 02h
11+L82–12+L82	File identifier = yyh yyh
13+L82	Life Cycle Status Information (LCSI) Tag = 8Ah (M)
14+L82	Length =01h
15+L82	LCSI value = X5h **b7-b4** **b3-b0** **State** xxxx 0101 Operational state activated xxxx 0100 Operational state deactivated File can only be created when the operational state is set to active. **b7-b5** **b4** **b3-b0** **Specific for Cyclic Files only (only for GSM session)** xxx 0 xxxx Increase forbidden for cyclic files only xxx 1 xxxx Increase allowed for cyclic files only
16+L82	Security Attribute Tag = 8Bh – for referenced format (M)
17+L82	Length L8B = 03h / 04h / 06h
18+L82 – 19+L82	EF$_{ARR}$ file identifier = zzh zzh
20+L82[1]	Record Number–SEXX (Please see the details in the following pages)

Table 57 - For an EF Creation

Byte No.	Description
21+L82	**Proprietary status tag = A5h (O)**
22+L82	Length = LA5 = L90 + (L91+2) + (Laa+2) + (Lco+2)
23+L82	GSM Access Condition Tag = 90h (O)
24+L82	Length = L90 = 6
25+L82– 24+L82+L90	AC1 to AC6 If this object is not present, AC1–AC6 will be filled with zero, that means access is never. See “Chapter 3 - 3G Data Security” for details regarding access conditions.
25+L82+L90	File Sharing Information Tag = 91h (O)
26+L82+L90	Length = L91 = xxh
26+L82+L90– 25+L82+L90+ L91	Path of the target EF (the path format is similar to Select by path from MF). The following rules for file sharing are applied: • File sharing applies only to EF creation. • EFMAP, EFDIR, EFARR, EFAUTH and EFAUTHPARAM must not be link EFs. • The link EF type and data EF type must be the same. • For linear fixed and cyclic link EFs, the record length specified in the template is ignored. • The link EF must have a size of 0.
26+L82+L90+ L91	EFARR Access Rule Tag = AAh (O)
27+L82+L90+ L91	Length = LAA = xxh
28+L82+L90+ L91– 27+L82+L90+ L91+LAA	EFARR security value. While creating the EFARR file, the access rule for the EFARR (SE01) has to be created and stored in the first record of the file.
28+L82+L90+ L91+LAA	EFARR Access Rule Tag = ABh (O) Access rule for SE00 is defined in Tag ABh object. It will be stored in record 2 of the EFARR.
29+L82+L90+ L91+LAA	Length = LAB = xxh

Table 57 - For an EF Creation (continued)

<table>
<tr><th>Byte No.</th><th>Description</th></tr>
<tr><td>30+L82+L90+ L91+LAA– 29+L82+L90+ L91+LAA+ LAB</td><td>EFARR security value.
If record number for SE01 and SE00 is not 1 or 2 respectively, the creation fail and status 6B00h will be returned.
If record number for SE01 or SE00 is 00h, their respective EFARR Access Rule Tag (AAh or ABh) is ignored.
If these information are not present after the file creation, we cannot update EFARR in order to attribute other file security attributes.</td></tr>
<tr><td>30+L82+L90+ L91+LAA+LA B</td><td>Special File Information Tag = C0h (O)</td></tr>
<tr><td>31+L82+L90+ L91+LAA +LAB</td><td>Length LC0= 01h</td></tr>
<tr><td>32+L82+L90+ L91+LAA+LA B</td><td>Special File Information:
<table><tr><th>b7</th><th>b6</th><th>b5-b4</th><th>b3</th><th>b2-b0</th><th>Descriptions</th></tr><tr><td>0</td><td>x</td><td>xx</td><td>x</td><td>xxx</td><td>Low update activity</td></tr><tr><td>1</td><td>x</td><td>xx</td><td>x</td><td>xxx</td><td>High update activity</td></tr><tr><td>x</td><td>0</td><td>xx</td><td>x</td><td>xxx</td><td>Non readable and cannot be updated when Invalidated</td></tr><tr><td>x</td><td>1</td><td>xx</td><td>x</td><td>xxx</td><td>Readable and can be updated when invalidated</td></tr><tr><td>x</td><td>x</td><td>xx</td><td>0</td><td>xxx</td><td>EF not sharable (cannot be linked)</td></tr><tr><td>x</td><td>x</td><td>xx</td><td>1</td><td>xxx</td><td>EF sharable</td></tr></table></td></tr>
<tr><td>21+L82+LA5 (if exists)</td><td>SFI Tag = 88h (O)</td></tr>
<tr><td>22+L82+LA5</td><td>Length = L88 = 00h or 01h</td></tr>
<tr><td>23+L82+LA5</td><td>Value of SFI</td></tr>
</table>

[1]: The length of this field is either 1, 2 or 4 bytes.

Table 57 - For an EF Creation (continued)

Caution: EFMAP / EFDIR / EFARR:

- It must be a Linear fixed file and must not be a link file.
- The record length for must EFMAP be 03h.

EFKEY / EFPIN / EFADM:

- It must be a transparent file.

EFARR:

- When create an EFARR, either tag AAh or ABh must be present.
- EFARR is a Linear fixed file and its maximum record length is 254 bytes.

Security Attribute Tag (Tag: 8Bh)

This object contains the security attribute for 3G access. The object size can be either 03h or 04h or 06h. For 03h object size, only SE01 is supported. In case of both SE01 and SE00 are supported, SE01 must be prior SE00.

Length	Value					
03h	FID	FID	SE01 Rec#	-	-	-
04h	FID	FID	SEID#01/#00	SE01/SE00 Rec#	-	-
06h	FID	FID	SEID#01	SE01 Rec#	SEID #00	SE00 Rec#

File Descriptor Byte (Tag: 82h)

File Type	FDB (Length)	Byte1 (Tag Value)				Byte2 (Format Type)	Byte3&4 (Record Length)
		b7-b3	b2	b1	b0		
Linear Fixed	04h	00000	0	1	0	21h	nnh nnh
Cyclic	04h	00000	1	1	0	21h	nnh nnh
Transparent	02h	00000	0	0	1	21h	
File is not sharable:		b6 of byte1 = 0					
File is sharable:		b6 of byte1 = 1					

Most significant byte of record length is ignored by OS and only 2nd byte of record length is stored.

The maximum length for linear fixed file is 255 and for cyclic file is 254, hence, the most significant byte should not be used.

Table 58 - File Descriptor Byte

Note:

- All objects marked as ‘M’ are mandatory and must be present. The presence of objects marked ‘O’ are optional.
- An object should not be repeated.
- All mandatory objects must be placed first in a file creation.
- If optional objects are not present, the default value will be used.
- For fixed size object, the length value is checked.
- The validity of the object values is not checked except for certain specified conditions.

Response

The card returns SW1 and SW2 status codes.

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
90h	00h	90h	00h	Command executed successfully
6Fh	00h	92h	40h	Verify DF or EF integrity error
6Ah	89h	92h	20h	File identifier already exists in the current DF
62h	83h	98h	10h	Current DF has been invalidated / deactivated
67h	00h	67h	00h	Incorrect length (Le) parameter
6Bh	00h	6Bh	00h	Incorrect P1 or P2 parameter. Template format error. For Linear Fixed and Cyclic EFs: • Record length = 00h. • File size is not a multiple of the record length. • Number of records > 254. • For cyclic EF, record length > 254. • Link EF with non zero file size.
6Ah	82h			EF_{DIR} not found
6Ah	84h	92h	10h	Not enough memory in the memory space
69h	82h	98h	04h	Access condition not fulfilled

3G		GSM		Description
SW1	SW2	SW1	SW2	
6Fh	09h	6Fh	00h	For DF creation, verify there are no more than 255 DFs already existing. For EF creation, verify there are no more than 255 EFs already existing under the current DF
6Fh	1Dh	6Fh	00h	Verify there is no more than three DF levels before DF creation
6Fh	20h	6Fh	00h	Creation not allowed: • MF not created. • EFARR not created (in 3G session). • FID is reserved. • File type is wrong. • File cannot be a link EF. • File size is wrong. • ADF created at wrong level. • Data EF path specified not found. • Link EF and Data EF do not have the same type. • Data file is not sharable. • No space left in EFMAP. • AID already exists in EFDIR. • No space left in EFDIR. • EFMAP record length not equal to 3.

EXTEND

This command is used to extend the size of the specified elementary file (except cyclic files). The file to be extended must be a child of the current DF, but not necessarily the currently selected file. To extend a file requires knowledge of a secret code that satisfies access conditions set during file creation.

The extended file inherits the rights of the original file.

Note: You cannot extend DFs, the MF, Cyclic EFs, EFKEY files, EFPIN files, EFADM files, or invalidated files.

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Lc	Data
00h	D4h	00h	00h	03h	Data

for GSM:

CLA	INS	P1	P2	Lc	Data
A0h	D4h	00h	00h	03h	Data

Where:

Data The data defining the extension:

Byte 1-2: Identifier of the file to be extended.

Byte 3: Specifies the size or the number of records of the extension.
Transparent EF: size of extension (max = 255)
Linear Fixed EF: number of records (max = 254)

Response

The card returns the SW1 and SW2 status codes.

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
90h	00h	90h	00h	Command executed successfully
6Fh	00h	6Fh	00h	Memory problem, Null Size, Number of Records > 254. Cannot extend EF.
67h	00h	67h	00h	Incorrect length (Lc) parameter
6Bh	00h	6Bh	00h	Incorrect P1 or P2 parameter
69h	81h	94h	08h	File inconsistent with the command
69h	82h	98h	04h	Access condition not fulfilled.
6Ah	82h	94h	04h	File not found
6Ah	84h	92h	10h	Not enough memory.
69h	84h	98h	10h	In contradiction with invalidation status.

DELETE

This command is used to delete any DFs or EFs in the file structure, including DFs which still contain other files and EFs with extensions. Executing this command can be unlimited, depends on the application.
You can delete a file only in the base channel which is the logical channel 0, regardless of whether it is the last created file. Before deleting a file, its parent file must be selected and the access condition located in the parent file satisfied.
The same as other files, there is no restriction of deleting a shared file which its body is shared with some other file, if the access condition has satisfied.

However, in 3G session, for an ADF, the file must be explicitly selected before, and the file identifier must be 7FFFh in the **Delete** command. The corresponding entry in the EFDIR for the deleted ADF is cleared automatically.

When an entity is deleted, the links to the parent are cut, the same for the links from the parent to the deleted entity.

Following points need to be take note when executing the **Delete** command:

Note:

- This command cannot use to delete the MF.
  It is also not possible to delete a file which is currently selected or whose DF parents are selected in another context. However, you can delete an invalidated file.
- If a data file to be deleted is verified as shared file, all its dependencies will be checked for their existence in the EFmap, and then they are logically deleted. That mean, the files (dependencies) are still exist in the memory but can only be accessed by the link files and not its file identifier. The logically deleted data file is automatically physical deleted, when all its dependencies are deleted.
  The same mechanism apply for deleting a DF with data file appears in between with its dependencies. Deleting a DF automatically deletes all the files it contains

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Lc	Data
00h	E4h	00h	00h	02h	Data

for GSM:

CLA	INS	P1	P2	Lc	Data
A0h	E4h	00h	00h	02h	Data

Where:

Data The file identifier.

Response

The card returns SW1 and SW2 status codes.

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
90h	00h	90h	00h	Command executed successfully
6Fh	00h	6Fh	00h	DF or EF integrity error. Memory problem.
6Fh	1Ch	-	-	Verify the file to be deleted exists and it is not the MF
69h	82h	98h	04h	Access conditions not fulfilled
67h	00h	67h	00h	Incorrect length (Lc) parameter
64h	00h	-	-	Verify the Application is Activated to Delete (ADF).
6Ah	82h	94h	04h	File not found
6Bh	00h	6Bh	00h	Incorrect P1 or P2 parameter
-	-	94h	08h	File is inconsistent

LOCK

This command is used to lock the access conditions (ACs) of the current DF or EF. In 3G mode, when this command is issued, it sets all the access conditions in the file as Never, by setting the EFARR record number to 00h in the header of the current file.

There are no access conditions defined for this command.

Format

This command is formatted as follows:

for 3G:

CLA	INS	P1	P2	Lc	Data
00h	76h	00h	00h	02h	Data

for GSM:

CLA	INS	P1	P2	Lc	Data
A0h	76h	P1	00h/FFh	02h	Data

Where:

Coding of P1 (for GSM):

b7	b6	b5	b4	b3	b2	b1	b0	Meaning
0	**0**	**X**	**X**	**X**	**X**	**X**	**X**	**Change Access Condition (AC) to "Never" (apply only to GSM)**
0	0	1	-	-	-	-	-	Change AC group 6 to "Never"
0	0	-	1	-	-	-	-	Change AC group 5 to "Never"
0	0	-	-	1	-	-	-	Change AC group 4 to "Never"
0	0	-	-	-	1	-	-	Change AC group 3 to "Never"
0	0	-	-	-	-	1	-	Change AC group 2 to "Never"
0	0	-	-	-	-	-	1	Change AC group 1 to "Never" if P2 = FFh
1	1	1	1	1	1	1	1	Change AC group 4 to ADM 4 in GSM AC

Group	Command Ac for DF	Command Ac for EF
Group 6	Invalidate	Invalidate
Group 5	Rehabilitate	Rehabilitate
Group 4	Create File	Extend
Group 3	Delete	Increase for EF cyclic only / RFU only
Group 2	RFU	Update
Group 1	RFU	Read / Seek

Response

The card returns the SW1 and SW2 status codes.

Status Codes

The following status codes may be returned after this command:

3G		GSM		Description
SW1	SW2	SW1	SW2	
90h	00h	90h	00h	Command executed successfully
6Fh	00h	6Fh	00h	DF or EF integrity error
6Ah	82h	94h	04h	The file is not selected
67h	00h	67h	00h	Incorrect length (Lc) parameter
6Bh	00h	6Bh	00h	Incorrect P1 or P2 parameter

11

3G and GSM Interworking

The chapter describes the interworking between a SIM (Subscriber Identity Module) application and a USIM (Universal Subscriber Identity Module) application on a UICC (Universal Integrated Circuit Card).

A SIM application and a USIM application which are implemented together on a single UICC can never be active at the same time. Their activity solely depends on the type of ME (Mobile Equipment) in which they are inserted. A 2G ME will always activate the SIM application, while a 3G ME only uses the USIM application. The result is a direct way of interworking does not exist.

However, both applications may share certain elements, either to enable an intended basic subscription mode of the UICC (single or double subscription) or to optimize memory consumption, but still both applications have to be virtually independent from a functional point of view. This means that a 2G ME can interwork with the SIM application without any influence from the USIM, while a 3G ME finds all the mandatory characteristics of the USIM application.
Naturally, independence ends if one application changes shared data which is later accessed by the other application because the UICC was inserted into another type of ME.

Activation of GSM and 3G Operation Modes

After a cold reset has been performed during UICC activation, the ATR sent by the UICC is compliant to 3G TS 31.101. No particular operation mode is active at this stage. The selection and activation of either GSM operation mode (SIM application) or 3G operation mode, is implicitly done by the ME when sending the first command. The following table describes the different possible cases.

ICC / ME Combination	Class Byte of First Command	Resulting Operation Mode	Remark
UICC with or without a SIM application in a 3G or GSM/3G dual mode ME	'00' or '80	3G	The USIM application should reject commands with class byte = 'A0'. First command right after ATR can be **Select** or **Status**.
UICC with a SIM application in a GSM ME	'A0'	GSM	The SIM application may reject commands with class byte = '00' or '80'. First command right after ATR can be **Select**, **Status** or **Get Response**.
UICC without a SIM application in a GSM ME	'A0'	No operation!	All further commands with class byte = 'A0' will be rejected.

A 3G or GSM/3G dual mode ME will only send commands with class byte = '00' or '80'. A GSM will only send commands with class byte = 'A0'. The operation mode selection takes place regardless of the result of the first command.

File Sharing Mechanism

File sharing is achieved through EFMAP file (See "EFMAP" on page 17), a linear fixed record file of record length three bytes under the MF.

This file is introduced for file mapping purposes, and as a result of the need to have a shared file body between 3G and GSM files in a UICC. See the "File Mapping (Sharing)" section for more details.

Before going in depth, the convention is that an EF that has a body is referred to as a data EF, and the EF without a body is referred to as a link EF.

Example:

EF1 is a link file (located under any of the DFs) that is mapped into the data file EF3 (located under an ADF). Bit 4 of the “Type” byte in the EF3 file has to be set to 1 at the time of creation in order to make its body sharable.

When EF1 is created, a special tag 91 has to be included into the proprietary tag A5. Tag 91 contains the path (from the MF) of the targeted data in EF3.

File Mapping (Sharing)

Many of the files of a SIM (as listed in GSM TS 11.11) and of a USIM (as listed in 3G TS 31.102) not only have the same name and file identifier (although under different DFs), but they also have the same size and content parameters. These files can be shared by both applications (SIM and USIM) in order to allow memory efficiency and to speed up the pre-personalization process.

Therefore files should be mapped as far as possible, and in all cases where basic properties are equal and identical contents do not conflict with access by either a 2G or a 3G ME or with intended subscription differences when separate IMSIs are used.

Note: Mapping is not possible, when the content is clearly subscription dependent like in the case of IMSI, Kc, KcGPRS or MSISDN in a double subscription UICC.

The Table 59, “SIM/USIM File Mapping Table”, on page 188 gives an overview of the SIM and USIM files that potentially can be mapped. However, a case by case decision should be conducted by the network operator or the card manufacturer for each UICC implementation.

Constraints to Sharing Files

File Type and File Sharable Setting. To be linked both files must be of the same type. The data file must be marked as sharable when creating the file, through File Sharing Information tag 91h.

Access Conditions. Linked files may have different access conditions. Only the currently selected file’s access conditions are checked.

Extend. Link EFs cannot be extended.

Phone book Synchronization . If EFADN under DFTELECOM is mapped into another EFADN (probably in a DFPHONEBOOK), then any update on this EFADN has to be tracked, that is, the EFPBC under the same DFPHONEBOOK is updated. However, there could be more than one EFPBC file in the DFPHONEBOOK. The EFPBC to use is defined in EFPBR.

Therefore the following conditions apply for phone book synchronization:

- Current session is GSM session.
- If EF being selected is EFADN under DFTELECOM and the EF is mapped, then the EFPBC file is also searched.
- If the EFADN under DFTELECOM is updated, the corresponding record in EFPBC is updated to 1.

SIM Application DF / EF	USIM Application DF / EF	Mapping Possible	
		Single Subscription UICC	Double Subscription UICC
GSM / IMSI	USIM / IMSI	yes	no
GSM / HPLMN	USIM / HPLMN	yes	yes, 1)
GSM / ACM	USIM / ACM	yes	yes, 1)
GSM / ACMmax	USIM / ACMmax	yes	yes, 1)
GSM / PUCT	USIM / PUCT	yes	yes, 1)
GSM / GID1	USIM / GID1	yes	yes, 1)
GSM / GID2	USIM / GID2	yes	yes, 1)
GSM / SPN	USIM / SPN	yes	yes, 1)
GSM / CBMI	USIM / CBMI	yes	
GSM / CBMIR	USIM / CBMIR	yes	
GSM / CBMID	USIM / CBMID	yes	yes, 1)
GSM / ACC	USIM / ACC	yes	no
GSM / FPLMN*	USIM / FPLMN	yes	yes, 1)
GSM / LOCI	USIM / LOCI	yes	
GSM / LOCIGPRS	USIM / PSLOCI	yes	

Table 59 - SIM/USIM File Mapping Table

SIM Application DF / EF	USIM Application DF / EF	Mapping Possible	
		Single Subscription UICC	Double Subscription UICC
GSM / AD	USIM / AD	yes	
GSM / eMLPP	USIM / eMLPP	yes	yes, 1)
GSM / AAeM	USIM / AAeM	yes	yes, 1)
GSM / DCK	USIM / DCK	yes	yes, 1)
GSM / CNL	USIM / CNL	yes	yes, 1)
GSM / PLMNwACT	USIM / PLMNwACT	yes	
GSM / OPLMNwACT	USIM / OPLMNwACT	yes	yes, 1)
GSM / HPLMNwACT	USIM / HPLMNwACT	yes, 3)	
GSM / RPLMNACT	USIM / RPLMNACT	no	
GSM / SUME	TELECOM / SUME	yes	
GSM / Kc	USIM / GSM / Kc	yes	no
GSM / KcGPRS	USIM / GSM / KcGPRS	yes	no
GSM / CPBCCH	USIM / GSM / CPBCCH	yes	
GSM / INVSCAN	USIM / GSM / INVSCAN	yes	yes, 1)
TELECOM / SMS	USIM / SMS	yes	
TELECOM / SMSP	USIM / SMSP	yes	yes, 1)
TELECOM / SMSS	USIM / SMSS	yes	
TELECOM / SMSR	USIM / SMSR	yes	
TELECOM / SDN	USIM / SDN	yes	yes, 1)
TELECOM / FDN	USIM / FDN	yes	
TELECOM / BDN	USIM / BDN	yes	
TELECOM / CMI	USIM / CMI	yes	
TELECOM / MSISDN	USIM / MSISDN	yes	no
TELECOM / EXT2	USIM / EXT2	yes	
TELECOM / EXT3	USIM / EXT3	yes	yes, 1)

Table 59 - SIM/USIM File Mapping Table (continued)

SIM Application DF / EF	USIM Application DF / EF	Mapping Possible	
		Single Subscription UICC	Double Subscription UICC
TELECOM / EXT4	USIM / EXT4	yes	
TELECOM / ADN	... / PHONEBOOK / ADN	yes, required, 2)	
TELECOM / EXT1	... / PHONEBOOK / EXT1	yes, required, 2)	
TELECOM / ECCP	... / PHONEBOOK / CCP1	yes, required, 2)	
GSM / MEXE / all files	USIM / MEXE / all files	yes	yes, 1)
GSM / SoLSA / all files	USIM / SoLSA / all files	yes	yes, 1)

*: Mapping is possible only if the file size is 12 bytes.

Note:

1. No mapping, if subscription specific differences are required.
2. SIM file to be mapped with related USIM file either in DF PHONEBOOK under DF USIM or in DF PHONEBOOK under DF TELECOM.
3. Only if the same settings apply to 2G and 3G operation.

Table 59 - SIM/USIM File Mapping Table (continued)

IMSI, Secret Code and Authentication Algorithm

In the HLR (Home Location Register) or AuC (Authentication Centre), a single subscription is identified by a particular IMSI (International Mobile Subscriber Identity), which is connected to a particular secret key (“Ki” for 2G and “K” for 3G) and to one type of authentication algorithm (“A3/A8” for 2G, “f1–f5” for 3G). At no time, a single IMSI may be connected to more than one secret key or algorithm. This is valid for both 2G and 3G context. Further, it applies that:

- Length and Format ($IMSI_{2G}$) = Length and Format ($IMSI_{3G}$)
- Length (Ki) = Length (K)
- 2G-Type Algorithm = Part of 3G Algorithm + Conversion Functions c2, c3.

For the third equation see 3G TS 31.102 and 3G TS 33.102. This 2G behavior of the 3G algorithm is the same as the virtual 2G mode described in Table 59, “SIM/USIM File Mapping Table”, on page 188. If it is always active either in a SIM application or in a 2G HLR/AuC, it follows that it should be called a fixed virtual 2G mode. Then, in fact, it would be a 2G algorithm.

There are three possible options for the UICC:

1. **Separate IMSI and Separate Secret Key**
   This case applies if the network operator for some reason wants to administrate the 2G and the 3G subscription, and the usage of a 2G or 3G ME is fully independent. The two subscriptions can be maintained in either a single 2G or 3G HLR/AuC or in different dedicated 2G and 3G HLR/AuCs. As for USIM and SIM applications, it also follows there is a need to keep separate IMSIs, $IMSI_{3G} \neq IMSI_{2G}$. IN ADDITION, the secret keys have to be different as well, K ≠ Ki. The algorithms in the UICC have to correspond to the algorithms associated with the IMSIs in the HLR/AuCs. The USIM application needs a 3G algorithm, while for the SIM application it can be one of the following:
   - A 2G algorithm on its own.
   - A 3G algorithm in fixed virtual 2G mode. In that case, the UICC needs to implement a 3G algorithm only, which from the SIM application is executed in 2G mode. The HLR/AuC must support this option accordingly.
2. **Separate IMSI and Shared Secret Key**
   From a functional point of view, this option is identical to option 1, except that the UICC saves 128 bits for the storage of a second secret key. On the other hand, the deliberate assignment of the same secret key to two different IMSIs would require particular solutions during secret key generation and pre-personalization.
3. **Shared IMSI & Shared Secret Key**
   This case applies if the network operator wants to have a single subscription for a user, independent of the usage of a 2G or 3G ME. Consequently the UICC has to carry the same identification details, IMSI and secret key in both SIM and USIM applications. On the network side, there is a single entry consisting of one IMSI and one secret key in either a 2G or a 3G HLR / AuC, in which $IMSI_{3G} = IMSI_{2G}$ and K= Ki. In a 2G HLR, the algorithm has to be a 3G-type in fixed virtual 2G mode (a 3G algorithm does not fit into a 2G HLR and a 2G algorithm does not fit with the USIM application on the UICC) while in a 3G HLR, the algorithm is a 3G-type. On the UICC side, there is not much choice. The USIM application essentially needs a 3G algorithm while for the SIM application, it can only be a 3G-algorithm in (fixed) 2G mode, as there is no 2G-type in the network. Again this has the advantage of having only one shared 3G algorithm on the UICC, from which the SIM application is executed in 2G mode.

The fourth theoretical combination, namely shared IMSI and separate secret keys, is not a valid option as a single IMSI cannot be associated with more than one secret key simultaneously.

GemXplore 3G V2 supports any of the above combinations.

Note: For security reason, Ki should not be shared between 3G and GSM modes. Two separate files with the same contents should be created. This is to avoid creating another EF that sharing the contents of EFki, but with a with lower access condition.

3G ME and UICC Interworking

To support a GSM / 3G dual mode ME in a GSM radio access network, the USIM may provide functions for GSM backward compatibility. Two particular USIM services are defined for such purposes:

1. **Service nº27**: “GSM Access”. This service is essential when a GSM Base Station Subsystem (BSS) is involved. The USIM additionally generates the GSM ciphering key Kc required by the GSM air interface. From the security point of view, this behavior can be characterized as “3G + Kc mode” (see subsequent paragraphs for more details). Furthermore, the USIM supports some additional GSM data storage elements that are necessary for GSM radio access.
2. **Service nº38**: “GSM Security Context”. This service is required when a GSM Visitor Location Register / Serving GPRS Support Node (VLR/SGSN) and / or a GSM Home Location Register / Authentication Centre (HLR) / (AuC) is involved. The USIM performs GSM Authentication and Key Agreement (AKA) that accepts GSM input data and generates GSM output data. From the security point of view, this behavior can be characterized as “virtual GSM mode” (see subsequent paragraphs for more details).

   A GSM VLR / SGSN is not compatible with a 3G BSS. Hence when a GSM VLR / SGSN is involved, then a GSM BSS is always part of the transmission chain and service nº27 is additionally required, as services nº27 and nº38 have to be available at the same time.

If services nº27 and nº38 are not supported by the USIM (which the ME can detect from the USIM Service Table during the USIM activation procedure) network access is impossible in a mixed GSM/3G environment, even when a SIM application is available on the UICC. A 3G ME only accesses the USIM application on the UICC.

From the security point of view, the compatibility services are connected to up to three different operation modes:

1. **Normal 3G Mode**: The results of the 3G algorithm are sent to the ME without any change. The USIM receives RAND and AUTN and responds with RES, CK and IK. This mode applies if service nº27 is not available.
2. **3G + Kc Mode**: The GSM ciphering key Kc (derived from CK, IK) is additionally included in the response. The USIM receives RAND and AUTN and responds with

RES, CK, IK and Kc. This requires conversion function C3 to be supported by the USIM. If service nº27 is available in the USIM, this mode is always active and the ME picks the relevant values from the USIM response according to the present network situation.

3. **Virtual GSM Mode**: The USIM receives a GSM authentication request with RAND and returns a GSM authentication response with SRES (derived from RES) and ciphering key Kc (derived from CK, IK). This requires a particular algorithm execution mode plus conversion functions C2 and C3 to be supported by the USIM. If service nº38 is available in the USIM, this mode is not always active. The ME may switch the USIM from normal 3G mode or 3G + Kc mode to virtual 2G mode by sending a particular command parameter according to the present network situation.

The service nº27 and nº38 are both optional. Network operators can decide whether to include them into their USIMs and hence to allow network access with a lower security level.

FDN/BDN Synchronization between GSM and 3G

FDN/BDN synchronization is required to ensure that operating system behavior during GSM / 3G sessions is consistent. For example, if in GSM mode FDN is enabled, this behavior should be inherited in a 3G session.

However this feature is optional. This mechanism is activated or deactivated at the personalization stage.

The following rules apply for synchronization:

- Synchronization occurs if there is a change in session only. GSM to 3G or 3G to GSM.
- Synchronization occurs if the appropriate service is allocated in EFSST or EFUST.
- For GSM, synchronization occurs during reset.
- For GSM, the mode is always synchronized with the last active ADF.
- For 3G, synchronization occurs during activation of the ADF.
- Synchronization occurs only for the first select of the ADF.
- Changing the configuration in the EFEST in the current ADF does not affect the other ADFs.

Example

Assuming a previous GSM mode and a current 3G mode immediately after reset.

- Select ADF1: synchronization occurs with previous GSM session. EFEST is updated accordingly.

- Select ADF2: synchronization occurs with previous GSM session. EFEST is updated accordingly.
- Select ADF1: nothing happens.
- Update EFEST.
- Select ADF2: Nothing happens.
- Select ADF1.

RESET.

- GSM synchronization occurs with the new EFEST setting in ADF1.

A

Answer To Reset

When a terminal powers up a GemXplore 3G V2 card, the card returns a standard **Answer To Reset** (**ATR**). The terminal can retrieve further information by using the **Get Response** command.

Byte	Value	Description
TS	3Bh	Direct convention
T0	9Fh	TA1 and TD1 present
TA1	95h	Clock rate conversion factor Fi, Baud rate adjustment factor Di
TD1	80h	TD2 only present
TD2	1Fh	TA3 only present, Global interface byte following
TA3	C3h	**Class AB: Clock Stop Mode Supported**
T1	80h	Historical byte (COMPACT-TLV)
T2	31h	Card data services
T3	E0h	Select by AID supported; select by partial AID supported; EF_{DIR} present
T4	73h	Card capabilities (data length 3)
T5	FEh	SFI supported
T6	21h	Data coding byte
T7	1Bh	No extended Lc and Le; four Logical Channels
T8	B3h	Tag L proprietary
T9	E2h	FMN: Operating system family name (defines the USIM family)
T10	01h	PRV: Program version

Table 60 - GemXplore 3G V2 Card Answer To Reset

Byte	Value	Description
T11	74h	Chip Reference
T12	83h	Tag L Proprietary
T13	00h	Card Life Status
T14	90h	SW1 returned after the ATR
T15	00h	SW2 returned after the ATR
TCK	TBA	Check byte

Table 60 - GemXplore 3G V2 Card Answer To Reset (continued)

Card Life Status

Name	Value	Description
Card OP Ready	01h	Card Manager is Initialized. Native operating system is no longer available
Card Initialized	07h	Card Manufacturer Initialization and Personalization
Card Secured	0Fh	Card is in Post Issuance
Card Locked	7Fh	Only Card Manager is selectable
Card Terminated	FFh	Card is mute and erased

B

Memory Requirements

The memory required to create an application can be calculated using the information given as follows.

File Type	Length (bytes)
MF	20
DF	20
ADF	20
Transparent EFs	20 + bodysize
EF$_{PIN}$ or EF$_{ADM}$	20 + bodysize
EF$_{KEY}$	20 + bodysize
Linear fixed EF	20 + number of records * record length
Cyclic EF	20 + number of records * record length

Table 61 - Memory requirements

C

3G Data Structure

This section describes the structure of a standard GemXplore 3G V2 card, obtained after the pre-personalization process. This standard structure contains both the files defined in the 3G TS 31.102 standard and those required by the operating system.

GemXplore 3G V2 cards store data in the following ways:

- The MF which contains the cardholder related information and system data
- The USIM ADF which contains the specific 3G data used for administrative, authentication and network management purposes
- The Telecom DF which contains the 3G data which can be shared with other telecommunications applications or end-user services

Standard UICC File Structure

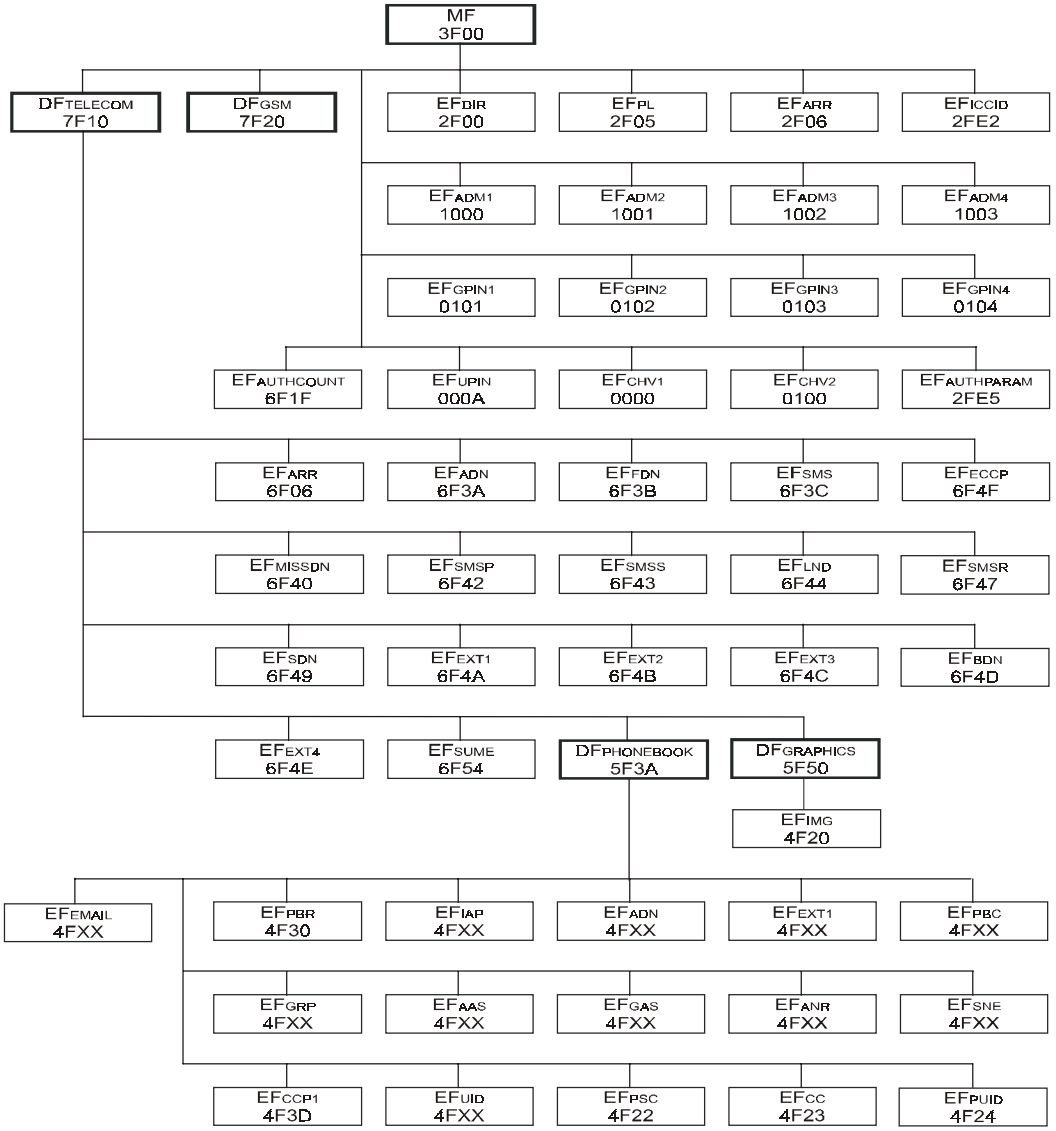

Figure 16 - File Identifier and Directory Structures of UICC

ADFUSIM File Structure

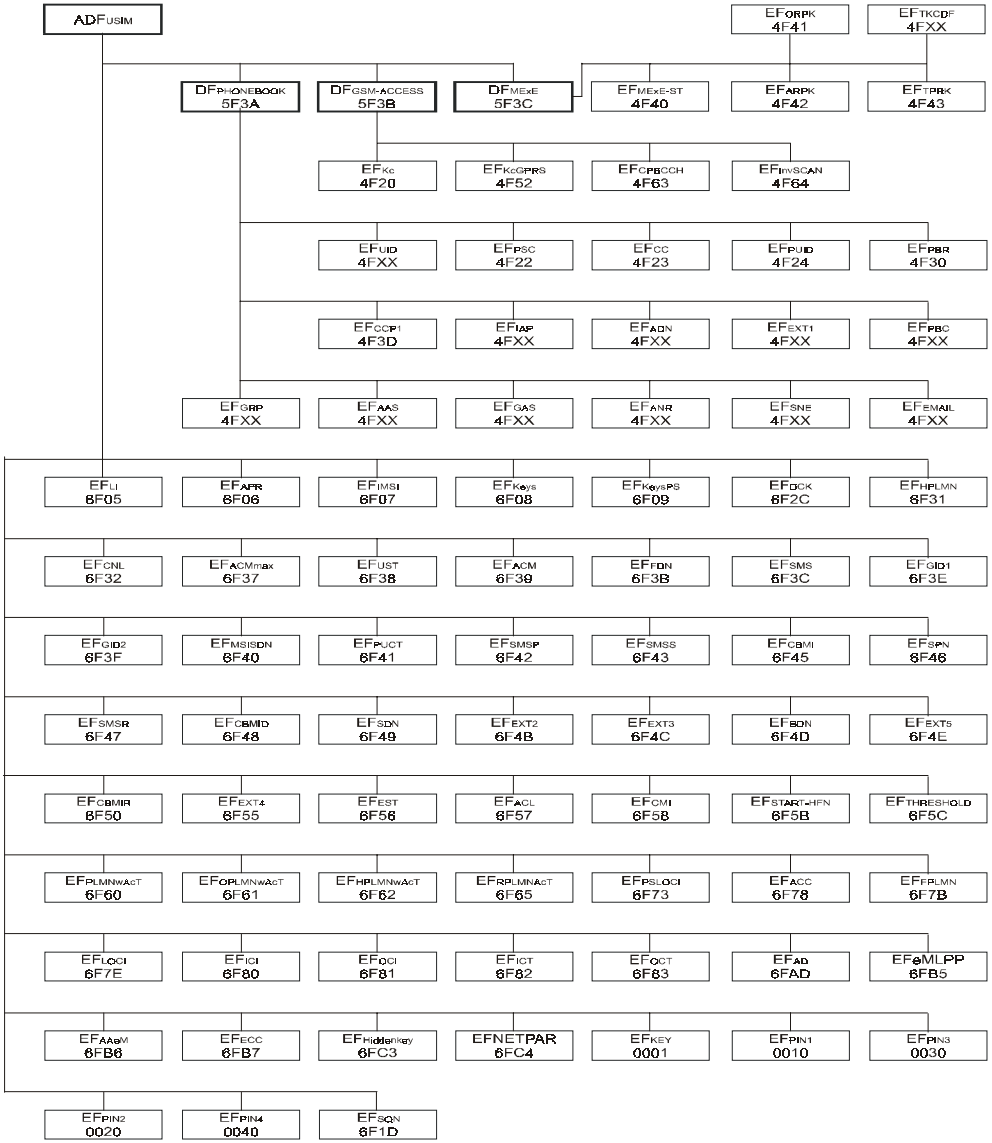

Figure 17 - File Identifiers and Directory Structures of USIM

Master File

The master file contains information from different stages of the card life cycle as well as from system EFs.

Identifier	Information	Type
6Fh1Fh	EFAUTHCOUNT (optional)	System
6Eh01h	EFMAP	System
5Fh11h	EFSMS SYSTEM	System
2FhE2h	EFICCID - Card serial number	ETSI TS 102.221
2Fh06h	EFARR	ETSI TS 102.221
00h0Ah	EFUPIN–Universal PIN (3G only)	System
00h00h	EFCHV1–GSM card holder verification 1	System
01h00h	EFCHV2–GSM card holder verification 2	System
01h01h	EFGPIN1 (3G ONLY)	System
01h02h	EFGPIN2 (3G ONLY)	System
01h03h	EFGPIN3 (3G ONLY)	System
01h04h	EFGPIN4 (3G ONLY)	System
10h00h	EFADM1	System
10h01h	EFADM2	System
10h02h	EFADM3	System
10h03h	EFADM4	System
2Fh00h	EFDIR	ETSI TS 102.221
2FhE5h	EFAUTHPARAM (optional)	System
2Fh05h	EFPL Preferred Languages	ETSI TS 102.221

Table 62 - MF File Contents

See *"Chapter 1 - File Structure"* for more details on the system files. Other files may be added to meet specific operator needs.

ADFUSIM

The ADFUSIM directory contains application information for 3G networks.

ADFUSIM contains its own EFARR which is used to obtain the access rights for its child EFs and DFs. Below is a list of the EFs in the ADFUSIM directory.

Identifier	Information	Type
00h01h	Key	System
6Fh06h	ARR	3G TS 31.102
00h10h	EFLPIN1 (3G ONLY)	System
00h20h	EFLPIN2 (3G ONLY)	System
00h30h	EFLPIN3 (3G ONLY)	System
00h40h	EFLPIN4 (3G ONLY)	System
6Fh05h	LI (Language Indication)	3G TS 31.102
6Fh07h	IMSI	3G TS 31.102
6Fh08h	Keys	3G TS 31.102
6Fh09h	KeysPS	3G TS 31.102
6Fh1Dh	EFSQN	System
6Fh60h	PLMNWACT (User controlled PLMN selector with Access Technology)	3G TS 31.102
6Fh31h	HPLMN (Home PLMN Search Period)	3G TS 31.102
6Fh37h	ACMmax	3G TS 31.102
6Fh38h	UST (USIM Service Table)	3G TS 31.102
6Fh39h	ACM (Accumulated Call Meter)	3G TS 31.102
6Fh3Eh	GID1	3G TS 31.102
6Fh3Fh	GID2	3G TS 31.102
6Fh46h	SPN	3G TS 31.102
6Fh41h	PUCT (Price/Unit and Currency Table)	3G TS 31.102
6Fh45h	CBMI (Cell Broadcast Message id selection)	3G TS 31.102
6Fh78h	ACC (Access Control Class)	3G TS 31.102

Table 63 - ADFUSIM File Contents

Identifier	Information	Type
6Fh7Bh	FPLMN (Forbidden PLMNs)	3G TS 31.102
6Fh7Eh	LOCI (Location Information)	3G TS 31.102
6FhADh	AD (Administrative Data)	3G TS 31.102
6Fh48h	CBMID (CBMI for Data Download)	3G TS 31.102
6FhB7h	ECC (Emergency Calling Code)	3G TS 31.102
6Fh50h	CBMIR (CBMI Range selection)	3G TS 31.102
6Fh73h	PSLOCI (Packet Switched Location Information)	3G TS 31.102
6Fh3Bh	FDN (Fixed Dialling Numbers)	3G TS 31.102
6Fh3Ch	SMS (Short Messages)	3G TS 31.102
6Fh40h	MSISDN	3G TS 31.102
6Fh42h	SMSP (Short Message Service Parameters)	3G TS 31.102
6Fh43h	SMSS (Short Message Status)	3G TS 31.102
6Fh49h	SDN (Service Dialling Numbers)	3G TS 31.102
6Fh4Bh	Ext2 (Extension 2)	3G TS 31.102
6Fh4Ch	Ext3 (Extension 3)	3G TS 31.102
6Fh47h	SMSR (SMS status report)	3G TS 31.102
6Fh80h	ICI (Incoming Call Information)	3G TS 31.102
6Fh81h	OCI (Outgoing Call Information)	3G TS 31.102
6Fh82h	ICT (Incoming Call Timer)	3G TS 31.102
6Fh83h	OCT (Outgoing Call Timer)	3G TS 31.102
6Fh4Eh	Ext5 (Extension 5)	3G TS 31.102
6Fh4Fh	CCP2 (Capability Configuration Parameter 2)	3G TS 31.102
6FhB5h	EMLPP (Enhanced Multi Level Precedence and Pre-emption)	3G TS 31.102
6FhB6h	AAEM (Automatic Answer for eMLPP Service)	3G TS 31.102
6FhC3h	Hiddenkey	3G TS 31.102
6Fh56h	EST (Enabled Service Table)	3G TS 31.102

Table 63 - ADFUSIM File Contents (continued)

Identifier	Information	Type
6Fh57h	ACL (Access Point Name Control List)	3G TS 31.102
6Fh2Ch	DCK (Depersonalization Control Keys)	3G TS 31.102
6Fh32h	CNL (Co-operative Network List)	3G TS 31.102
6Fh5Bh	START-HFN (Initialization values for Hyperframe number)	3G TS 31.102
6Fh5Ch	THRESHOLD (Maximum value of START)	3G TS 31.102
6Fh61h	OPLMNWAcT (Operator controlled OPLMN selector With Access Technology)	3G TS 31.102
6Fh62h	HPLMNWAcT (Preferred HPLMN selector With Access Technology)	3G TS 31.102
6Fh65h	RPLMNAcT (Registered PLMN last used Access Technology)	3G TS 31.102
6FhC4h	NETPAR (Network Parameters	3G TS 31.102
5Fh3Bh	DF GSM - ACCESS	3G TS 31.102
4Fh20h	Kc (GSM Ciphering Key)	3G TS 31.102
4Fh52h	KcGPRS (GSM Ciphering Key GPRS)	3G TS 31.102
4Fh63h	CPBCCH (CPBCCH information)	3G TS 31.102
4Fh64h	INVSCAN (Investigation scan)	3G TS 31.102

Table 63 - ADFUSIM File Contents (continued)

Telecom DF

This DF contains information relevant to the services offered by a given operator.

DFTELECOM contains its own EFARR which is used to obtain the access rights for its child EFs and DFs. Below is a list of the directory files and elementary files in the Telecom DF.

Identifier	Information	Type
6Fh06h	ARR	3G TS 31.102
6Fh3Ch	EFSMS (mandatory)	System
5Fh14h	EFSMS LOG (optional)	3G TS 31.102
5Fh3Ah	DF Phonebook	3G TS 31.102
4Fh30h	PBR (Phone Book Reference File)	3G TS 31.102
4Fh25h	IAP (Index Administration Phone book)	3G TS 31.102
4Fh3Ah	ADN (Abbreviated Dialling Numbers)	3G TS 31.102
4Fh4Ah	EXT1 (Extention 1)	3G TS 31.102
4Fh09h	PBC (Phone Book Control)	3G TS 31.102
4Fh26h	GRP (Grouping File)	3G TS 31.102
4Fh4Bh	AAS (Additional information Alpha String)	3G TS 31.102
4Fh4Ch	GAS (Grouping information Alpha String)	3G TS 31.102
4Fh11h	ANR (Additional Number)	3G TS 31.102
4Fh19h	SNE (Second Name Entry)	3G TS 31.102
4Fh3Dh	CCP1 (Capability Configuration Parameter 1)	3G TS 31.102
4Fh50h	EMAIL	3G TS 31.102
5Fh50h	DF Graphics	3G TS 31.102
4Fh20h	IMG	3G TS 31.102
4Fh01h	Image Instance Data Files	3G TS 31.102

Table 64 - DFTELECOM File Contents

D

Differences between 3G and GSM

OTA

The differences between OTA in a GSM session to OTA in a 3G session concerns the status codes returned. The status codes affected are:

- 9EXX is converted to 6200.
- 9FXX is converted to 61XX.
- In 3G mode, status code for wrong length is changed to 6CXX for the Get Response where XX is the remaining length given by the shuttle.
- While interpreting the SMS command scripts, no session check is done, and a GSM command can be embedded into the message in a 3G session and vice versa.

STK

The operating system has implemented the `Package usim.acess`, as the means for applets to access USIM data and the file system of a USIM application defined in the 3GPP 31.101 specification.

However, the access domain definition for 3G has not yet been defined in the standard. The access domain currently follows that of GSM defined in 03.48. Therefore, files which have free access condition or those protected by GPIN1–GPIN2, ADM1–ADM4 can be accessed by a toolkit applet.

Terminology

Abbreviations

3GPP	3rd Generation Partnership Project
AC	Access Condition
ADF	Application Dedicated File
ADM	Administrative secret code
AID	Application Identifier
AKA	Authentication and Key Agreement
ALW	ALWays
AM_DO	Access Mode Data Objects
APDU	Application Protocol Data Unit
ARR	Access Reference Rule
ATR	Answer To Reset.
AuC	Authentication Centre
BSS	Base Station Subsystem
CLA	Class
DF	Dedicated File

DO	Data Object
EEPROM	Electrically Erasable PROgrammable Memory
EF	Elementary File
FCI	File Control Information
FCP	File Control Parameters
FDB	File Descriptor Byte
FID	File Identifier
HE	Host Environment
HLR	Home Location Register
ID	Identifier
IMSI	International Mobile Subscriber Identity
INS	Instruction Code
Lc	Data field length
LCSI	Life Cycle Status Information
Le	Length expected
ME	Mobile Equipment
MF	Master File
MMI	Man Machine Interface
NEV	Never
NU	Not Used
OS	Operating System
P1 / P2	Parameter 1 / Parameter 2 of the command header
PIN	Personal Identification Number

PPS	Protocol and Parameter Selection
RFU	Reserved for Future Use
SC_DO	Security Condition Data Object
SFI	Short File Identifier
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SM	Secure Messaging
SW1 / SW2	Status Word 1 / Status Word 2
SRES	Signed RESponse
TE	Terminal Equipment
TLV	Tag Length Value
TPDU	Transfer Protocol Data Unit
UICC	Universal Integrated Circuit Card
USAT	USIM Application Toolkit
USIM	Universal Subscriber Identity Module
VLR	Visitor Location Register
VM	Virtual Machine

Glossary

3GPP	The standard organization for third generation
3G Session	The part of the card session dedicated to 3G operation.
Access Condition (AC)	Security attribute assigned to a file. The access condition defines which code must be verified or authentication procedure performed before access to the file data is granted. A file can be assigned a different access condition for each command concerning it.
Application	An application consists of a set of security mechanisms, files, data and protocols, excluding transmission protocols.
Application Protocols	The set of procedures required by the application.
Atomicity	Mechanism which guarantees the consistency of sensitive data in EEPROM against power losses or any similar problems while the card is updating memory.
Authentication	Procedure used to prove that the card is a genuine 3G card by means of an algorithm, a random value and a secret key.
Card Session	A link between the card and the interface device starting with the **Answer To Reset** and ending with a subsequent reset or a deactivation of the card.
Current Directory	The last directory (MF, DF or ADF) selected in the card.
Current File	The last DF or EF to be selected on the card.
Data File	A data file is a file with its own body which the contents is sharable with other file (Link File) via a linking mechanism. See also the definition of link file.
Data Object	Information coded as TLV objects that consist of a tag, length and a value part.
Dedicated File (DF)	EFs are grouped logically in DFs. A DF is a logical entity which groups a number of files (up to 255) including other DFs. A DF does not contain application-related data, but only stores information concerning the files under it.

Directory	Generic name for the Master File (MF) or a Dedicated File (DF).
EFADM	Elementary file containing an administrative secret code.
EFPIN	Elementary file containing a Card Holder Verification code.
EFKEY	Elementary files containing keys.
Elementary File (EF)	Set of data units or records which share the same file identifier. An EF cannot be the parent of another file. There are three types of EFs: Transparent EFs (previously called a binary data field), where data can be manipulated in strings of bytes of variable length (maximum length is 256 bytes), located anywhere within the EF. Linear Fixed EFs (previously called a formatted data field), where the data is stored in series of strings of fixed length called records. Linear Fixed EFs offer more extensive data addressing possibilities than transparent EFs. Cyclic EFs are made of fixed length records. The length is determined when the file is created and is stored in the file descriptor. Records are referenced in the inverse order of creation so that the last record to be written is always record number 1. When the file is full, the oldest record is replaced by the new record.
Entity	General term used to refer to dedicated files, elementary files and the master file.
Filter	Coding loaded in the EEPROM that modifies the standard behavior of the operating system.
GSM Session	The part of the card session dedicated to the GSM operation.
Identifier	Two-byte tag used to identify each logical entity in the card (that is, EFs and DFs).
International Mobile Subscriber Identity Code (IMSI)	3G subscribers are identified by a unique IMSI code which is an individual number permanently assigned to the subscriber. The IMSI code allows the system to identify the country and home PLMN of the user.

Initialization	First stage of the card-issuing process. The main goal of this process is to initialize the card's EEPROM and customize the card for the operator in terms of administrative management of the card.
Ki	Unique 16-byte secret key used for authentication. Each card has a different Ki.
Link File	A link file is a file without its own body but instead obtains its content from another file (Data File) by means of a linking mechanism and a mapping file. See also the definition of link file.
Master File (MF)	This file is unique and mandatory. It has its own security attributes and may contain DFs and/or EFs. After a reset or power up, this file is automatically selected by the operating system.
Mobile Station	Term used to define the mobile equipment (that is, a terminal + a SIM card).
Not Used (NU)	The data is stored in the card but is not used by the operating system.
Null	A value of 00h.
Padding	One or more bits appended to a message in order to ensure that it contains the required number of bits or bytes.
Personalization	Second stage of the card-issuing process. In this step the card is personalized with card holder related information and the supplementary service combination (abbreviated dialing numbers, short message storage, etc.).
Personalization Center	Center in which the following functions are performed: Card programming. Data connection to the subscription management system.
Ratification Counter	Counter assigned to each PIN and ADM code in the card. It records the number of consecutive times the code has been incorrectly entered. If the ratification counter reaches 0 after a pre-determined number of attempts (chosen when the secret code is first created), the secret code is blocked. If the secret code is entered correctly before it is blocked, the ratification counter is reset to its initial value, otherwise it must be unblocked using the **Unblock PIN** command. The purpose of the ratification counter is to prevent exhaustive secret code attacks.

Record	String of bytes which can be handled as a whole by the operating system and referenced absolutely by a record number and relatively to the current record.
Record Number	Number assigned sequentially to each record in a linear fixed or cyclic EF by the operating system. Each record number in a linear fixed or cyclic EF is unique.
Record Pointer	The pointer which addresses one record in an EF.
Reserved for Future Use (RFU)	The data contained in the bit is stored in the operating system, but is not used by the operating system. Commands must set RFU bits to 0.
Right	Authorization granted when an authentication procedure has been successfully completed or a secret code has been verified. Rights give the application access to the data stored in the card memory.
Secret Code	A number stored in a secure manner in the card. A secret code gives access rights. The user or the application must present a secret code correctly to the card in order to be granted one or more access rights.
Secret Key	Value of variable length used in an algorithm to perform authentication.
Security Policy	Different access conditions that apply to a GemXplore™ entity.
Session	Period of time between two card resets, or between power up and power down.
Set of Records	A linear fixed EF is created with a number of consecutive fixed length records in its body, known as the set of records.
Terminal	Any end-user terminal, for example a fax or mobile phone, which can be used on the network.
Unblocking PIN Code	Eight-byte code used to unblock a PIN secret code.
Unblocking ADM Code	Eight-byte code used to unblock an ADM secret code.
UICC	The platform on which a USIM operates.

USAT	The SIM toolkit for third generation
USIM	The 3G application.

Index

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

P

R

S

T

U

V