SCRD (SmartCard Riset and Development) CSL

Review 3GPP TS 11.11, 11.14, 11.17, 23.038, 23.040, 03.48

Candidate

Nurmansyah Hazman

Dian permana

January 25, 2017

Introduction

- 3GPP TS 11.11 (3rd Generation Partnership Project; Technical Specification Group Terminals Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (Release 1999))
- 3GPP TS 11.14 (3rd Generation Partnership Project; Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (Release 1999))
- 3GPP TS 11.17 (3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Subscriber Identity Module (SIM) conformance test specification (Release 1999))

Introduction

- 3GPP TS 23.038 (3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Alphabets and language-specific information) (Release 8)).
- Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Technical realization of the Short Message Service (SMS) (3GPP TS 23.040 version 9.3.0 Release 9);
- 3GPP TS 03.48 (3rd Generation Partnership Project; Technical Specification Group Terminals; Security mechanisms for the SIM application toolkit; Stage 2 (Release 1999))

3GPP TS 11.11

Scope

- ✓ The requirements for the physical characteristics of the SIM, the electrical signals and the transmission protocols;

3GPP TS 11.11

Scope

✓ The requirements for the physical characteristics of the SIM, the electrical signals and the transmission protocols;

✓ The model which shall be used as a basis for the design of the logical structure of the SIM;

3GPP TS 11.11

Scope

- ✓ The requirements for the physical characteristics of the SIM, the electrical signals and the transmission protocols;
- ✓ The model which shall be used as a basis for the design of the logical structure of the SIM;
- ✓ The security features;

3GPP TS 11.11

Scope

- ✓ The requirements for the physical characteristics of the SIM, the electrical signals and the transmission protocols;
- ✓ The model which shall be used as a basis for the design of the logical structure of the SIM;
- ✓ The security features;
- ✓ The interface functions;

3GPP TS 11.11

Scope

- ✓ The requirements for the physical characteristics of the SIM, the electrical signals and the transmission protocols;
- ✓ The model which shall be used as a basis for the design of the logical structure of the SIM;
- ✓ The security features;
- ✓ The interface functions;
- ✓ The commands;

3GPP TS 11.11

Scope

- ✓ The requirements for the physical characteristics of the SIM, the electrical signals and the transmission protocols;
- ✓ The model which shall be used as a basis for the design of the logical structure of the SIM;
- ✓ The security features;
- ✓ The interface functions;
- ✓ The commands;
- ✓ The contents of the files required for the GSM application;

3GPP TS 11.11

Scope

- ✓ The requirements for the physical characteristics of the SIM, the electrical signals and the transmission protocols;
- ✓ The model which shall be used as a basis for the design of the logical structure of the SIM;
- ✓ The security features;
- ✓ The interface functions;
- ✓ The commands;
- ✓ The contents of the files required for the GSM application;
- ✓ The application protocol.

Physical characteristics

The physical characteristics of both types of SIM shall be in accordance with ISO/IEC 7816-1,2.

- Format and layout
- Temperature range for card operation

  The temperature range for full operational use shall be between $-25^{\circ}C$ and $+70^{\circ}$C with occasional peaks of up to $+85^{\circ}$C.
- Contacts

Logical Model

General Description

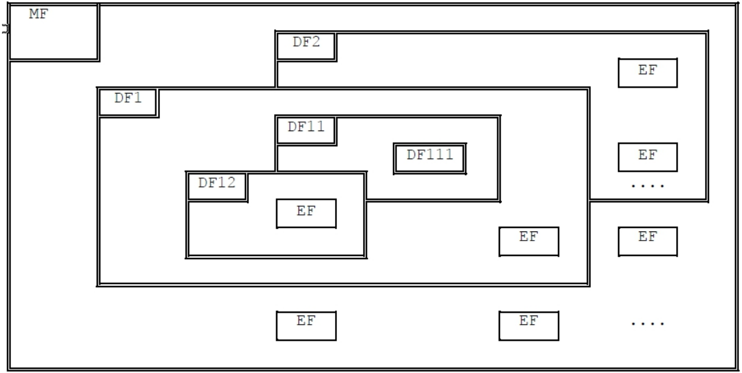


Figure: Organization of memory

Logical Model

File identifier

- ’3F’: Master File;
- ’7F’: 1st level Dedicated File;
- ’5F’: 2nd level Dedicated File;
- ’2F’: Elementary File under the Master File;
- ’6F’: Elementary File under a 1st level Dedicated File;
- ’4F’: Elementary File under 2nd level Dedicated File.

Logical Model

Dedicated files

- ✓ DFGSM which contains the applications for both GSM and/or DCS 1800;
- ✓ DFTELECOM which contains telecom service features;
- ✗ DFIS41 which contains the applications for IS-41 as specified by ANSI T1P1;
- ✗ DFFP-CTS which contains the applications for the CTS fixed part (see TS 11.19 [34]).

Logical Model

Elementary files

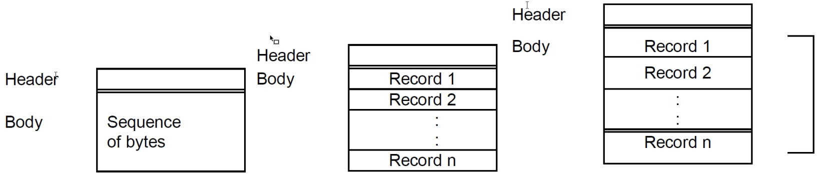
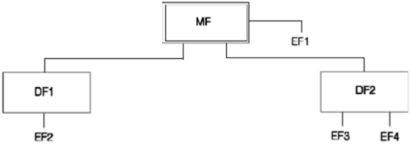
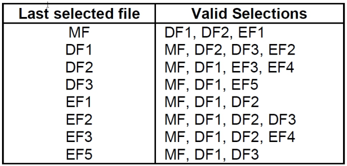


Figure: Structure of a transparent EF(Left), a linear fixed file (Center), a cyclic file (Right)

Logical Model

Methods for selecting a file





Last selected file	Valid Selections
MF	DF1, DF2, EF1
DF1	MF, DF2, DF3, EF2
DF2	MF, DF1, EF3, EF4
DF3	MF, DF1, EF5
EF1	MF, DF1, DF2
EF2	MF, DF1, DF2, DF3
EF3	MF, DF1, DF2, EF4
EF5	MF, DF1, DF3

Figure: Logical structure(Left), File selection(Right)

Security features

Authentication and cipher key generation procedure

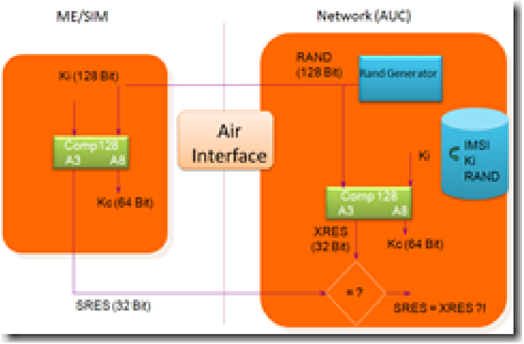


Figure: GSM Authentication

Description of the functions

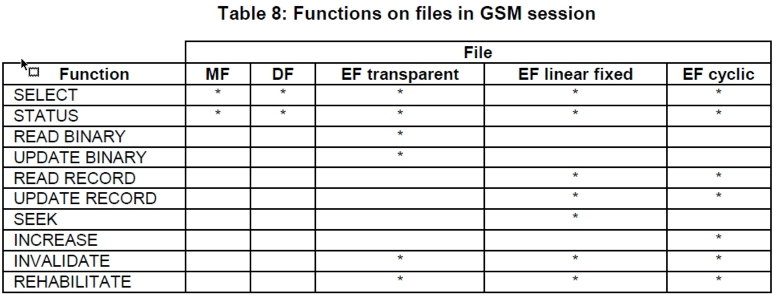


Table 8: Functions on files in GSM session

Function	File				
	MF	DF	EF transparent	EF linear fixed	EF cyclic
SELECT	*	*	*	*	*
STATUS	*	*	*	*	*
READ BINARY			*		
UPDATE BINARY			*		
READ RECORD				*	*
UPDATE RECORD				*	*
SEEK				*	
INCREASE					*
INVALIDATE			*	*	*
REHABILITATE			*	*	*

Description of the commands

Application Protocol Data Units

What is the Application Protocol Data Units ?

✓ **An APDU** can be a command APDU or a response APDU

Table: A command APDU has the following general format

CLA	INS	P1	P2	P3	Data

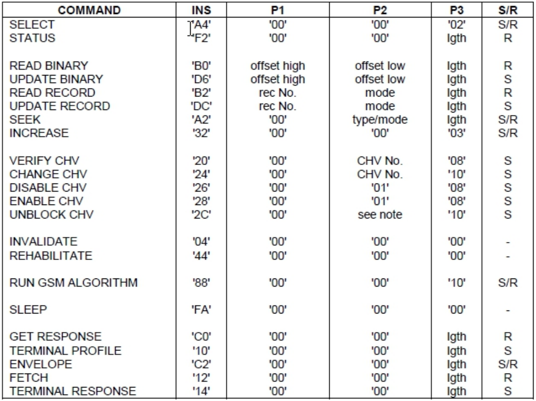
Table: The response APDU has the following general format:

Data	SW1	SW2

Description of the commands

Coding of the commands

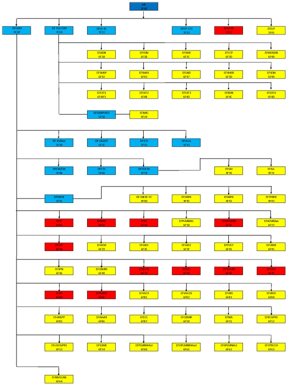
Table 9: Coding of the commands



COMMAND	INS	P1	P2	P3	S/R
SELECT	'A4'	'00'	'00'	'02'	S/R
STATUS	'F2'	'00'	'00'	lgth	R
READ BINARY	'B0'	offset high	offset low	lgth	R
UPDATE BINARY	'D6'	offset high	offset low	lgth	S
READ RECORD	'B2'	rec No.	mode	lgth	R
UPDATE RECORD	'DC'	rec No.	mode	lgth	S
SEEK	'A2'	'00'	type/mode	lgth	S/R
INCREASE	'32'	'00'	'00'	'03'	S/R
VERIFY CHV	'20'	'00'	CHV No.	'08'	S
CHANGE CHV	'24'	'00'	CHV No.	'10'	S
DISABLE CHV	'26'	'00'	'01'	'08'	S
ENABLE CHV	'28'	'00'	'01'	'08'	S
UNBLOCK CHV	'2C'	'00'	see note	'10'	S
INVALIDATE	'04'	'00'	'00'	'00'	-
REHABILITATE	'44'	'00'	'00'	'00'	-
RUN GSM ALGORITHM	'88'	'00'	'00'	'10'	S/R
SLEEP	'FA'	'00'	'00'	'00'	-
GET RESPONSE	'C0'	'00'	'00'	lgth	R
TERMINAL PROFILE	'10'	'00'	'00'	lgth	S
ENVELOPE	'C2'	'00'	'00'	lgth	S/R
FETCH	'12'	'00'	'00'	lgth	R
TERMINAL RESPONSE	'14'	'00'	'00'	lgth	S

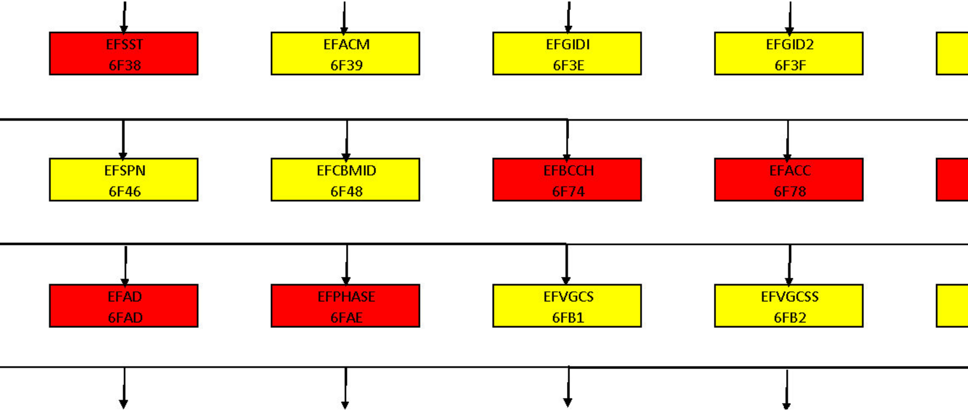
Contents of the Elementary Files (EF)

File identifiers and directory structures of GSM



Contents of the Elementary Files (EF)

File identifiers and directory structures of GSM



EFSST 6F38

EFACM 6F39

EFGIDI 6F3E

EFGID2 6F3F

EFSPN 6F46

EFCBMID 6F48

EFBCCH 6F74

EFACC 6F78

EFAD 6FAD

EFPHASE 6FAE

EFVGCS 6FB1

EFVGCSS 6FB2

SIM management procedures

SIM initialization

1. After SIM activation, the ME selects the Dedicated File DFGSM and optionally attempts to select EFECC If EFECC is available, the ME requests the emergency call codes.
2. The ME requests the Extended Language Preference. The ME only requests the Language Preference (EFLP) if at least one of the following conditions holds:
    - EFELP is not available;
    - EFELP does not contain an entry corresponding to a language specified in ISO 639[30];
    - the ME does not support any of the languages in EFELP.
3. If both EFs are not available or none of the languages in the EFs is supported then the ME selects a default language

SIM management procedures

SIM initialization

3. For a SIM of Phase 2 or greater, GSM operation shall only start if one of the two following conditions is fulfilled:
    - if EFIMSI and EFLOCI are not invalidated, the GSM operation shall start immediately;
    - if EFIMSI and EFLOCI are invalidated, the ME rehabilitates these two EFs.
4. When EFIMSI and EFLOCI are successfully rehabilitated, if the FDN capability procedure indicates that:
    - FDN is allocated and activated in the SIM; and FDN is set "enabled", i.e. ADN "invalidated" or not activated; and the ME supports FDN; or
    - FDN is allocated and activated in the SIM; and FDN is set "disabled", i.e. ADN "not invalidated"; or
    - FDN is not allocated or not activated;

SIM management procedures

SIM initialization

5 GSM operation shall start.

6 If the SIM service table indicates that the proactive SIM service is active, then from this point onwards, the ME, if it supports the proactive SIM service, shall send STATUS commands at least every 30s during idle mode as well as during calls, in order to enable the proactive SIM to respond with a command

3GPP TS 11.14

Scope

✓ The commands;

✓ The application protocol;

✓ The mandatory requirements on the SIM and ME for each procedure

Overview of SIM Application Toolkit

SIM Application Toolkit

- ✓ The SIM Application Toolkit provides mechanisms which allow applications, existing in the SIM, to interact and operate with any ME which supports the specific mechanism(s) required by the application.

Overview of SIM Application Toolkit

- Profile Download
- Proactive SIM
- Data download to SIM
- Menu selection
- Call control by SIM
- MO Short Message control by SIM
- Event download
- Security
- Multiple card
- Timer Expiration
- Bearer Independent Protocol

Profile Download

What is the profile download

- ✓ The **profile download** instruction is sent by the ME to the SIM as part of the SIM initialization procedure
- ✓ Profile downloading provides a mechanism for the ME to tell the SIM what it is capable of. The ME knows what the SIM is capable of through the SIM Service Table and EFPHASE.

Proactive SIM

Proactive SIM

- ✓ Proactive SIM gives a mechanism whereby the SIM can initiate actions to be taken by the ME
- ✓ The proactive SIM service provides a mechanism which stays within the protocol of T 0.

Data downloading

Data downloading

✓ Data downloading to the SIM uses either dedicated commands (the transport mechanisms of SMS point-to-point and Cell Broadcast) or the Bearer independent protocol.Transferral of information over the SIM-ME interface uses the ENVELOPE command

The menu selection

What is The menu selection

✓ The menu selection mechanism is used to transfer the SIM application menu item which has been selected by the user to the SIM. The menu selection mechanism may also be used for requesting help information on the items of the SIM application menu

Timer Expiration

Timer Expiration

✓ The SIM is able to manage timers running physically in the ME with a proactive command. The Timer Expiration mechanism is used to inform the SIM when a timer expires.

Tag values

Table: BER-TLV tags in ME to SIM direction

SMS-PP download tag	1	D1
Cell Broadcast download tag	1	D2
Menu Selection tag	1	D3
Call control tag	1	D4
MO Short message control tag (	1	D5
Event download tag	1	D6
Timer expiration	1	D7
Reserved for TIA/EIA-136	1	DF

Tag values

Table: BER-TLV tags in SIM TO ME direction

Description	Length of tag	Value
Proactive SIM command tag	1	D0

Table: SIMPLE-TLV tags in both directions

8	7	6	5	4	3	2	1
CR	Tag Value						

Structure of SIM Application Toolkit communications

Table: BER-TLV data object

T	L	V	1..n SIMPLE-TLV objects

Table: SIMPLE-TLV data object

T	L	V	1..m element

T	L	V

3GPP TS 11.17

scope

✓ The present document provides the Conformance Test Specification for the Subscriber Identity Module defined in GSM 11.11 [1], GSM 11.12 [8] and GSM 11.18 [9].

Test Procedure

- Physical characteristics
- Electronic signals and transmission protocols
- Logical Model
- Security features
- Description of the functions
  Example :
  - SELECT function
  - STATUS function

3GPP TS 23.040

- SMS-DELIVER (in the direction SC to MS)

Example : EF SMS

```
0107912698461001292 40D91269806931074F30000611130010192820
4C464D009FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFF FFFFFFFFFFFFFFFFFFFFFFFFFF
```

SMS-DELIVER

Table: Basic elements of the SMS-DELIVER type

Abbr.	Reference	P1	P2
TP-MTI	TP-Message-Type-Indicator	M	2b
TP-MMS	TP-More-Messages-to-Send	M	b
TP-LP	TP-Loop-Prevention	O	b
TP-RP	TP-Reply-Path	M	b
TP-UDHI	TP-User-Data-Header-Indicator	O	b
TP-SRI	TP-Status-Report-Indication	O	b
TP-OA	TP-Originating-Address	M	2-12o
TP-PID	TP-Protocol-Identifier	M	o
TP-DCS	TP-Data-Coding-Scheme	M	o

SMS-DELIVER

TP-SCTS	TP-Service-Centre-Time-Stamp	M	7o
TP-UDL	TP-User-Data-Length	M	I
TP-UD	TP-User-Data	O	3)

- Provision; Mandatory (M) or Optional (O).
- Representation; Integer (I), bit (b), 2 bits (2b), Octet (o), 7 octets (7o), 2-12 octets (2-12o).
- Dependent on the TP-DCS.

Result

$SMSC\# + 628964011092$

$Sender : +6289603901473$

$TimeStamp : 03/11/1610 : 10 : 29$

$TP_PID : 00$

$TP_DCS : 00$

$TP_DCS - popis : UncompressedText, class : 0$

$Alphabet : Default$

$DIAN$

$Length : 4$

3GPP TS 23.038

Scope

- The present document defines the character sets, languages and message handling requirements for SMS, CBS and USSD and may additionally be used for Man Machine Interface (MMI) (3GPP TS 22.030 [2]).
- The specification for the Data Circuit terminating Equipment/Data Terminal Equipment (DCE/DTE) interface (3GPP TS 27.005 [8]) will also use the codes specified herein for the transfer of SMS data to an external terminal.

SMS Data Coding Scheme

Use of bits 3..0

Bit 1	Bit 0	Message Class
0	0	Class 0
0	1	Class 1 Default meaning : ME-specific
1	0	Class 2 (U)SIM specific message
1	1	Class 3 Default meaning

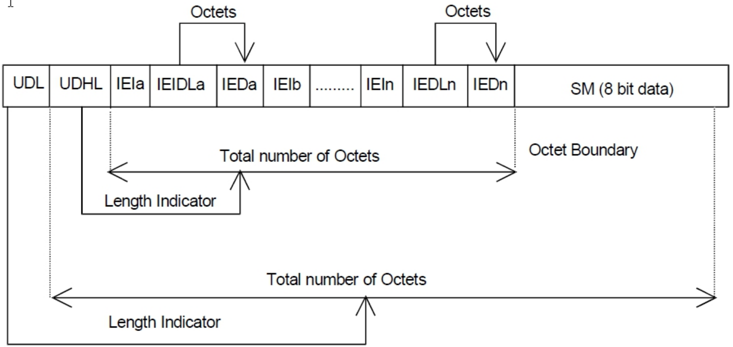
Bit 3	Bit 2	Character set
0	0	GSM 7 bit default alphabet
0	1	8 bit data
1	0	UCS2 (16bit)
1	1	Reserved

SMS Data Coding Scheme

NOTE : The special case of bits 7..0 being 0000 0000 indicates the GSM 7 bit default alphabet with no message class

Over The Air (OTA)

Implementation for SMS-PP



Octets

Octets

UDL | UDHL | IEIa | IEIDLa | IEDa | IEIb | .... | IEIn | IEDLn | IEDn | SM (8 bit data)

Total number of Octets

Octet Boundary

Length Indicator

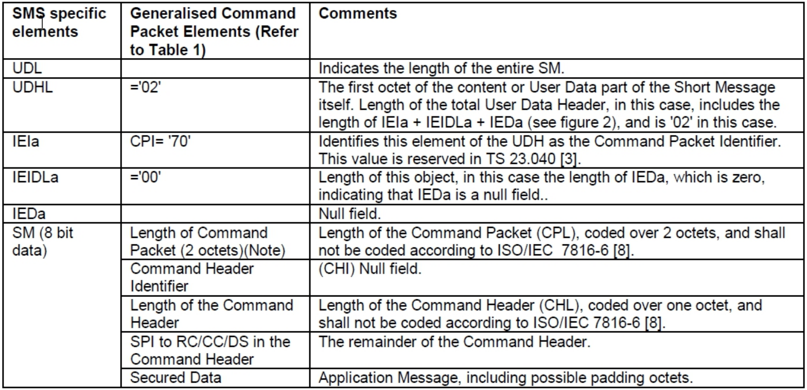
Total number of Octets

Length Indicator

Figure: Structure of User Data Header in the Short Message Point to Point

Over The Air (OTA)

A Command Packet contained in a Single Short Message Point to Point

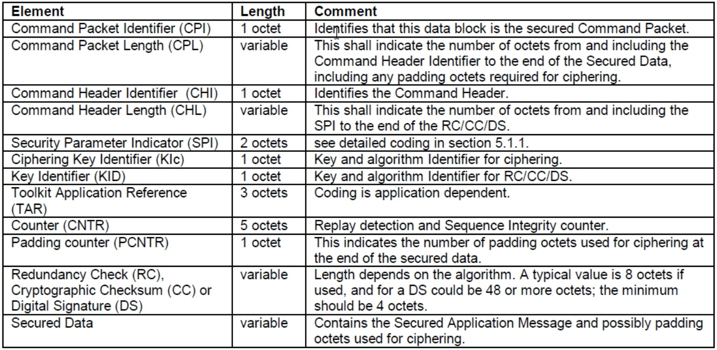


SMS specific elements	Generalised Command Packet Elements (Refer to Table 1)	Comments
UDL		Indicates the length of the entire SM.
UDHL	='02'	The first octet of the content or User Data part of the Short Message itself. Length of the total User Data Header, in this case, includes the length of IEIa + IEIDLa + IEDa (see figure 2), and is '02' in this case.
IEIa	CPI= '70'	Identifies this element of the UDH as the Command Packet Identifier. This value is reserved in TS 23.040 [3].
IEIDLa	='00'	Length of this object, in this case the length of IEDa, which is zero, indicating that IEDa is a null field..
IEDa		Null field.
SM (8 bit data)	Length of Command Packet (2 octets)(Note)	Length of the Command Packet (CPL), coded over 2 octets, and shall not be coded according to ISO/IEC 7816-6 [8].
	Command Header Identifier	(CHI) Null field.
	Length of the Command Header	Length of the Command Header (CHL), coded over one octet, and shall not be coded according to ISO/IEC 7816-6 [8].
	SPI to RC/CC/DS in the Command Header	The remainder of the Command Header.
	Secured Data	Application Message, including possible padding octets.

Over The Air (OTA)

Generalised Secured Packet structure

Structure of the Command Packet

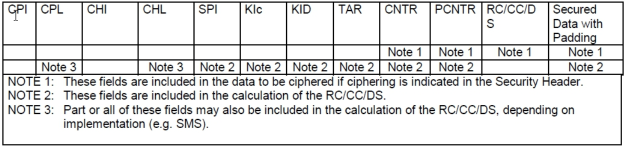


Element	Length	Comment
Command Packet Identifier (CPI)	1 octet	Identifies that this data block is the secured Command Packet.
Command Packet Length (CPL)	variable	This shall indicate the number of octets from and including the Command Header Identifier to the end of the Secured Data, including any padding octets required for ciphering.
Command Header Identifier (CHI)	1 octet	Identifies the Command Header.
Command Header Length (CHL)	variable	This shall indicate the number of octets from and including the SPI to the end of the RC/CC/DS.
Security Parameter Indicator (SPI)	2 octets	see detailed coding in section 5.1.1.
Ciphering Key Identifier (KIc)	1 octet	Key and algorithm Identifier for ciphering.
Key Identifier (KID)	1 octet	Key and algorithm Identifier for RC/CC/DS.
Toolkit Application Reference (TAR)	3 octets	Coding is application dependent.
Counter (CNTR)	5 octets	Replay detection and Sequence Integrity counter.
Padding counter (PCNTR)	1 octet	This indicates the number of padding octets used for ciphering at the end of the secured data.
Redundancy Check (RC), Cryptographic Checksum (CC) or Digital Signature (DS)	variable	Length depends on the algorithm. A typical value is 8 octets if used, and for a DS could be 48 or more octets; the minimum should be 4 octets.
Secured Data	variable	Contains the Secured Application Message and possibly padding octets used for ciphering.

Over The Air (OTA)

Generalised Secured Packet structure

Linear Representation of Command Packet



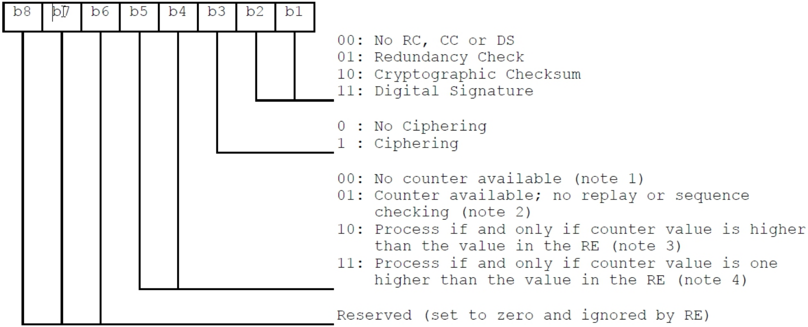
CPI	CPL	CHI	CHL	SPI	KIc	KID	TAR	CNTR	PCNTR	RC/CC/DS	Secured Data with Padding
								Note 1	Note 1	Note 1	Note 1
	Note 3		Note 3	Note 2	Note 2	Note 2	Note 2	Note 2	Note 2		Note 2

NOTE 1: These fields are included in the data to be ciphered if ciphering is indicated in the Security Header.
NOTE 2: These fields are included in the calculation of the RC/CC/DS.
NOTE 3: Part or all of these fields may also be included in the calculation of the RC/CC/DS, depending on implementation (e.g. SMS).

Over The Air (OTA)

Coding of the SPI

FirstOctat



00: No RC, CC or DS
01: Redundancy Check
10: Cryptographic Checksum
11: Digital Signature

0 : No Ciphering
1 : Ciphering

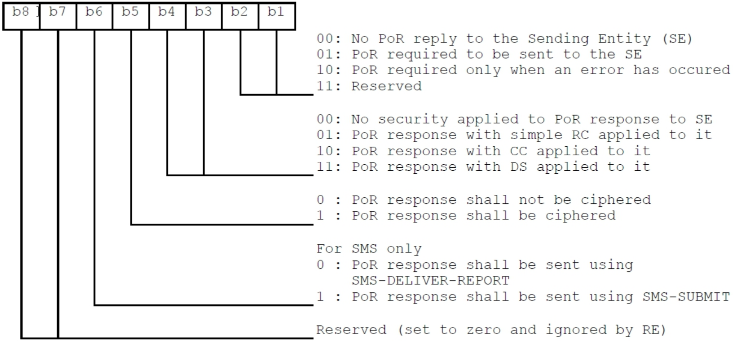
00: No counter available (note 1)
01: Counter available; no replay or sequence checking (note 2)
10: Process if and only if counter value is higher than the value in the RE (note 3)
11: Process if and only if counter value is one higher than the value in the RE (note 4)

Reserved (set to zero and ignored by RE)

Over The Air (OTA)

Coding of the SPI

secondOctat



00: No PoR reply to the Sending Entity (SE)
01: PoR required to be sent to the SE
10: PoR required only when an error has occured
11: Reserved

00: No security applied to PoR response to SE
01: PoR response with simple RC applied to it
10: PoR response with CC applied to it
11: PoR response with DS applied to it

0 : PoR response shall not be ciphered
1 : PoR response shall be ciphered

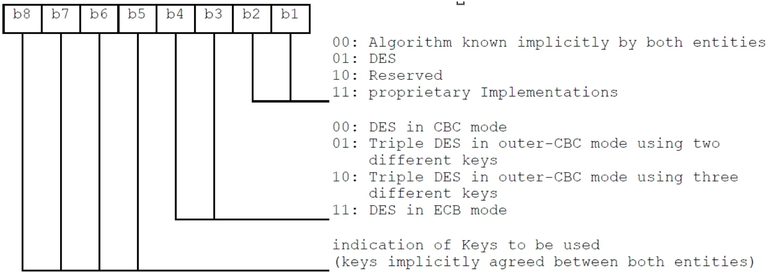
For SMS only
0 : PoR response shall be sent using SMS-DELIVER-REPORT
1 : PoR response shall be sent using SMS-SUBMIT

Reserved (set to zero and ignored by RE)

Over The Air (OTA)

Coding of the KIc

The KIc is coded as below



00: Algorithm known implicitly by both entities
01: DES
10: Reserved
11: proprietary Implementations

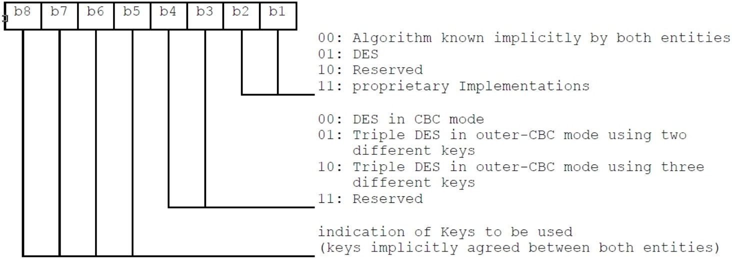
00: DES in CBC mode
01: Triple DES in outer-CBC mode using two different keys
10: Triple DES in outer-CBC mode using three different keys
11: DES in ECB mode

indication of Keys to be used
(keys implicitly agreed between both entities)

Over The Air (OTA)

Coding of the KID

The KID is coded as below



00: Algorithm known implicitly by both entities
01: DES
10: Reserved
11: proprietary Implementations

00: DES in CBC mode
01: Triple DES in outer-CBC mode using two different keys
10: Triple DES in outer-CBC mode using three different keys
11: Reserved

indication of Keys to be used
(keys implicitly agreed between both entities)

Thanks

I would like to thank people that, with precious hints, help me:

- Novia causal
- Beta Team
- Rumadi