3GPP TSG-T (Terminals) Meeting #9
Hawaii, USA, 20 - 22 September, 2000

Tdoc TP-000148

Source: T3

Title: Change Requests to GSM 11.11 "SIM/ME interface specification"

Agenda item: 6.3.3

Document for: Approval

This document contains several change requests to GSM 11.11 v8.3.0 agreed by T3.

T3 Doc	Spec	CR	Rv	Rel	Subject
T3-000480	11.11	A125		R99	Addition of warning regarding network selection with access technology
T3-000479	11.11	A126		R99	Standardise the current GAIT commands and reserving these CLA/INS codes

3GPP TSG-T3 Meeting #15
San Diego, USA, August 16-18, 2000

***Document* T3-000480**
Revised from Tdoc T3-000453

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

GSM 11.11	**CR**	**A125**	Current Version:	8.3.0
GSM (AA.BB) or 3G (AA.BBB) specification number ↑		*↑ CR number as allocated by MCC support team*		

For submission to: TSG-T #09 — for approval ☒ — strategic □ *(for SMG use only)*
list expected approval meeting # here ↑ — For information □ — non-strategic □

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from:* ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM ☒ ME ☒ UTRAN / Radio □ Core Network □
(at least one should be marked with an X)

Source:	T3	**Date:**	18-08-00
Subject:	PLMN with access technology and PLMN selection with access technology.		
Work item:	TEI		

Category:	F	Correction	☒	**Release:**	Phase 2 □
	A	Corresponds to a correction in an earlier release	□		Release 96 □
(only one category	B	Addition of feature	□		Release 97 □
shall be marked	C	Functional modification of feature	□		Release 98 □
with an X)	D	Editorial modification	□		Release 99 ☒
					Release 00 □

Reason for change: This CR contains a warning with respect to PLMN with access technology and selection, as the status with this issue is still under discussion within 3GPP TSG SA.

Clauses affected: 10.3.35, 10.3.36, 10.3.37, 11.2.1, 11.4.10, 11.4.11, 11.4.12

Other specs affected:	Other 3G core specifications	□	→ List of CRs:
	Other GSM core specifications	□	→ List of CRs:
	MS test specifications	□	→ List of CRs:
	BSS test specifications	□	→ List of CRs:
	O&M specifications	□	→ List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

10.3.35 EF$_{PLMNwACT}$ (PLMN Selector with Access Technology)

Note: PLMN with access technology and PLMN selection with access technology are still under discussion by 3GPP TSG SA and may be subject to change.

This EF contains coding for n PLMNs, where n is at least eight. This information, determined by the user, defines the preferred PLMNs of the user in priority order. The EF also contains the Access Technologies for each PLMN in this list. The MS use this information to determine what type of channels to scan for when searching for a specific PLMN (see GSM 03.22 [45]).

<table>
<tr><td colspan="2">Identifier:'6F60'</td><td colspan="2">Structure: transparent</td><td>Optional</td></tr>
<tr><td colspan="2">File size: 4n (n ≥ 8) bytes</td><td colspan="3">Update activity: low</td></tr>
<tr><td colspan="5">Access Conditions:
READ CHV1
UPDATE CHV1
INVALIDATE ADM
REHABILITATE ADM</td></tr>
</table>

Bytes	Description	M/O	Length
1 – 3	1st PLMN (highest priority)	M	3 bytes
4	Access Technologies of 1st PLMN in PLMN selector with Access Technology	M	1 byte
5–7	2nd PLMN	M	3 bytes
8	Access Technologies of 2nd PLMN in PLMN selector with Access Technology	M	1 byte
(4n–3)--(4n–1)	nth PLMN (lowest priority)	O	3 bytes
4n	Access Technologies of nth PLMN in PLMN selector with Access Technology	O	1 byte

- PLMN

  Contents:

  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

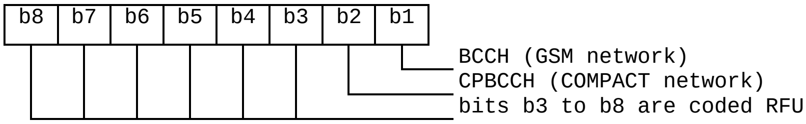
  Coding:

  according to TS 24.008 [47].

- Access Technologies

  Contents: The Access Technologies of a PLMN that the MS will assume when searching for a listed PLMN.

  Coding:



A '1' in a bit position indicates that the Access Technology corresponding to that bit position is supported and a '0' that it is not supported. The RFU bits are coded with '0' in the bit positions.

The default coding of the Access Technologies field shall be '01'.

A user initiated update of a PLMN shall automatically initiate an update of the associated Access Technologies field, according to the Access Technologies identified by the MS for the respective PLMN. If no Access Technologies are identified, the default coding value shall apply for the associated Access Technologies field.

If storage for fewer than the maximum possible number n is required, the excess bytes shall be set to 'FF'.

For instance, using 246 for the MCC and 81 for the MNC for a GSM-only PLMN, and if this is the first and only PLMN in the list, the contents reads as follows:

Bytes 1-3: '42' 'F6' '18'

Byte 4 : '01'

Bytes 5-7: 'FF' 'FF' 'FF'

Byte 8 : 'FF'

etc.

10.3.36 EF$_{\text{OPLMNwACT}}$ (Operator controlled PLMN Selector with Access Technology)

Note: PLMN with access technology and PLMN selection with access technology are still under discussion by 3GPP TSG SA and may be subject to change.

This EF contains coding for n PLMNs, where n is at least eight. This information, determined by the operator, defines the preferred PLMNs of the operator in priority order. The EF also contains the Access Technologies for each PLMN in this list. The MS uses this information to determine what type of channels to scan for when searching for a specific PLMN (see GSM 03.22 [45]).

Identifier: '6F61'	Structure: transparent	Optional
File size: 4n (n ≥ 8) bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 – 3	1st PLMN (highest priority)	M	3 bytes
4	Access Technologies of 1st PLMN in Operator controlled PLMN selector with Access Technology	M	1 byte
5–7	2nd PLMN	M	3 bytes
8	Access Technologies of 2nd PLMN in Operator controlled PLMN selector with Access Technology	M	1 byte
(4n–3)--(4n–1)	nth PLMN (lowest priority)	O	3 bytes
4n	Access Technologies of nth PLMN in Operator controlled PLMN selector with Access Technology	O	1 byte

- PLMN

Contents:

Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

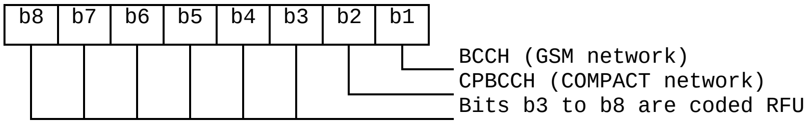
Coding:

according to TS 24.008 [47].

- Access Technologies

Contents: The Access Technologies of a PLMN that the MS will assume when searching for a listed PLMN.

Coding:



A '1' in a bit position indicates that the Access Technology corresponding to that bit position is supported and a '0' that it is not supported. The RFU bits are coded with '0' in the bit positions.

The default coding of the Access Technologies field shall be '01'.

If storage for fewer than the maximum possible number n is required, the excess bytes shall be set to 'FF'.

For instance, using 246 for the MCC and 81 for the MNC for a GSM-only PLMN and if this is the first and only PLMN in the list, the contents reads as follows:

Bytes 1-3: '42' 'F6' '18'

Byte 4 : '01'

Bytes 5-7: 'FF' 'FF' 'FF'

Byte 8 : 'FF'

etc.

10.3.37 $EF_{HPLMNACT}$ (HPLMN Access Technology)

Note: PLMN with access technology and PLMN selection with access technology are still under discussion by 3GPP TSG SA and may be subject to change.

This EF contains the Access Technology for the HPLMN (see EF_{IMSI}). The MS uses this information to determine what type of channels to scan for when searching for the HPLMN and in what priority order. (see GSM 03.22 [45]).

If this EF does not exist on the SIM then the MS shall assume that HPLMN use BCCH.

Identifier: '6F62'	Structure: transparent	Optional
File size: n bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1	Access Technology 1 of HPLMN	O	1 byte
2	Access Technology 2 of HPLMN	O	1 byte
n	Access Technology n of HPLMN	O	1 byte

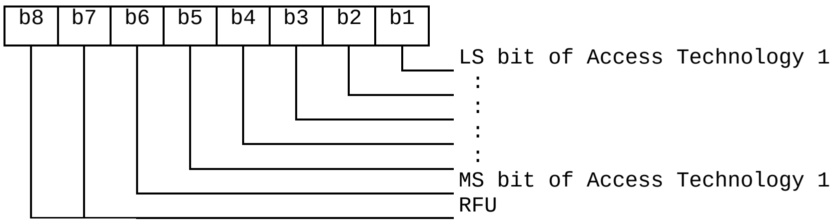
- Access Technology

Contents: The Access Technology of the HPLMN that the MS will assume when searching for the HPLMN, in priority order. The first Access Technology in the list has the highest priority.

Coding:

For each 1 byte list element

Byte 1:



Byte:

Bits:	b6	b5	b4	b31	b3	b2	b1	
	0	0	0	0	0	0	1	BCCH
	0	0	0	0	0	1	0	CPBCCH

The default coding of the Access Technology field shall be '000001'.

The RFU bit positions shall be set to '0'.

11.2.1 SIM initialization

After SIM activation (see subclause 4.3.2), the ME selects the Dedicated File DF_{GSM} and optionally attempts to select EF_{ECC} If EF_{ECC} is available, the ME requests the emergency call codes.

The ME requests the Extended Language Preference. The ME only requests the Language Preference (EF_{LP}) if at least one of the following conditions holds:

- EF_{ELP} is not available;
- EF_{ELP} does not contain an entry corresponding to a language specified in ISO 639[30];
- the ME does not support any of the languages in EF_{ELP}.

If both EFs are not available or none of the languages in the EFs is supported then the ME selects a default language. It then runs the CHV1 verification procedure.

If the CHV1 verification procedure is performed successfully, the ME then runs the SIM Phase request procedure.

For a SIM requiring PROFILE DOWNLOAD, then the ME shall perform the PROFILE DOWNLOAD procedure in accordance with GSM 11.14 [27]. When BDN is enabled on a SIM, the PROFILE DOWNLOAD procedure is used to indicate to the SIM whether the ME supports the "Call Control by SIM" facility. If so, then the SIM is able to allow the REHABILITATE command to rehabilitate EF_{IMSI} and EF_{LOCI}.

If the ME detects a SIM of Phase 1, it shall omit the following procedures relating to FDN and continue with the Administrative Information request. The ME may omit procedures not defined in Phase 1 such as HPLMN Search Period request.

For a SIM of Phase 2 or greater, GSM operation shall only start if one of the two following conditions is fulfilled:

- if EF_{IMSI} and EF_{LOCI} are not invalidated, the GSM operation shall start immediately;
- if EF_{IMSI} and EF_{LOCI} are invalidated, the ME rehabilitates these two EFs.

  MEs without FDN capability but with Call control by SIM facility shall not rehabilitate EF_{IMSI} and/or EF_{LOCI} if FDN is enabled in the SIM and therefore have no access to these EFs. GSM operation will therefore be prohibited;

  MEs without FDN capability and without Call control by SIM facility shall not rehabilitate EF_{IMSI} and/or EF_{LOCI} and therefore have no access to these EFs. GSM operation will therefore be prohibited.

  It is these mechanisms which are used for control of services n°3 and n°31 by the use of SIMs for these services which always invalidate these two EFs at least before the next command following selection of either EF.

NOTE: When FDN and BDN are both enabled, and if the ME supports FDN but does not support the Call control by SIM facility, the rehabilitation of EF_{IMSI} and EF_{LOCI} will not be successful because of a restriction mechanism of the REHABILITATE command linked to the BDN feature.

When EF_{IMSI} and EF_{LOCI} are successfully rehabilitated, if the FDN capability procedure indicates that:

i) 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

ii) FDN is allocated and activated in the SIM; and FDN is set "disabled", i.e. ADN "not invalidated"; or

iii) FDN is not allocated or not activated;

then GSM operation shall start.

In all other cases GSM operation shall not start.

Afterwards, the ME runs the following procedures:

- Administrative Information request;
- SIM Service Table request;
- IMSI request;
- Access Control request;
- HPLMN Search Period request;
- Investigation PLMN scan request;
- PLMN selector request;
- HPLMN Access Technology request;
- PLMN Selector with Access Technology request;
- OPLMN Selector with Access Technology request;
- Location Information request;
- Cipher Key request;
- BCCH information request;
- CPBCCH information request;
- Forbidden PLMN request;
- LSA information request;
- CBMID request;
- Depersonalisation Control Keys request;
- Network's indication of alerting request.

Note: PLMN with access technology and PLMN selection with access technology are still under discussion by 3GPP TSG SA and may be subject to change.

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. The SIM may send proactive commands (see GSM 11.14 [27]), including a command to change the interval between STATUS commands from the ME, when in idle mode. In-call requirements for STATUS for SIM Presence Detection are unchanged by this command.

After the SIM initialization has been completed successfully, the MS is ready for a GSM session.

11.4.10 PLMN Selector with Access Technology

Note: PLMN with access technology and PLMN selection with access technology are still under discussion by 3GPP TSG SA and may be subject to change.

Requirement: Service n°43"allocated and activated".

Request: The ME performs the reading procedure with $EF_{PLMNwACT}$.

Update: The ME performs the updating procedure with $EF_{PLMNwACT}$.

11.4.11 OPLMN Selector with Access Technology

Note: PLMN with access technology and PLMN selection with access technology are still under discussion by 3GPP TSG SA and may be subject to change.

Requirement: Service n°44 "allocated and activated".

Request: The ME performs the reading procedure with $EF_{OPLMNwACT}$.

Update: The ME performs the updating procedure with $EF_{OPLMNwACT}$.

11.4.12 HPLMN Access Technology

Note: PLMN with access technology and PLMN selection with access technology are still under discussion by 3GPP TSG SA and may be subject to change.

Requirement: Service n°45 "allocated and activated".

Request: The ME performs the reading procedure with $EF_{HPLMNACT}$.

3GPP T3 Meeting #14
San Diego, USA, 16 - 18 August, 2000

Tdoc T3-000479

CHANGE REQUEST No :	**A126**	*Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.*	
Technical Specification GSM:	11.11	Version:	8.3.0

Submitted to	TSG-T #9	For approval	X	without presentation ("non-strategic")	X
list plenary meeting no. here ↑		for information		with presentation ("strategic")	

PT SMG CR cover form. Filename: crf26_3.doc

Proposed change affects: SIM ☒ ME ☒ Network □
(at least one should be marked with an X)

Work item:

Source: T3 **Date:** 18/08/2000

Subject: Standardise the current GAIT commands and reserving these CLA/INS codes

Category:	F	Correction	X	**Release:**	Phase 2	
	A	Corresponds to a correction in an earlier release			Release 96	
(one category	B	Addition of feature			Release 97	
and one release	C	Functional modification of feature			Release 98	
only shall be	D	Editorial modification			Release 99	X
marked with an X)					Release 00	

Reason for change: Incomplete set of commands

Clauses affected: Annex H

Other specs affected:	Other releases of same spec		→ List of CRs:
	Other core specifications		→ List of CRs:
	MS test specifications / TBRs		→ List of CRs:
	BSS test specifications		→ List of CRs:
	O&M specifications		→ List of CRs:

Other comments:

help.doc

<---------- double-click here for help and instructions on how to create a CR.

H.2 Authentication Functionality

H.2.1 A-KEY (ANSI-41 Authentication Key)

The A-Key is only accessible to the algorithm used for Key generation. The A-Key may be programmed into the SIM directly by the service provider, or it may be programmed into the SIM through a specific over the air procedure. The A-Key is not accessible by the mobile equipment, therefore the method of storage on the SIM is not specified in this document. The SIM command A-KEY_VALIDATION is used to store the A-Key on the SIM.

H.2.2 SSD (Shared Secret Data)

The Shared Secret Data is accessible only to the Authentication and the Key Generation functions. SSD is not accessible by the mobile equipment, therefore the method of storage on the SIM is not specified in this document.

An additional Status Code is defined for SSD updating as follows:

98, 34 Error, Update SSD order sequence not respected (should be used if SSD Update commands are received out of sequence).

~~H.2.3 Validation and Storage of entered A-Key~~

~~The SIM only stores the A-Key after successful verification (see Common Cryptographic Algorithms, Revision C, October 27, 1998, TR45AHAG [43]). The following parameters are specified:~~

~~COMMAND~~	~~CLASS~~	~~INS~~	~~P1~~	~~P2~~	~~P3~~
~~A-KEY_VALIDATION~~	~~'A0'~~	~~'86'~~	~~'00'~~	~~'00'~~	~~'12'~~

~~Command parameters/data:~~

~~Byte(s)~~	~~Description~~	~~Length~~
~~1- 13~~	~~Authentication digits string (first digit in Most-Significant nibble of byte 1, last digit in Least-Significant nibble of Byte 12, for a total of 26 digits)~~	~~13~~
~~14~~	~~Use ME ESN = '00'~~	~~1~~
~~15-18~~	~~ESN~~	~~4~~

~~The following table specifies the coding of the status words SW1 and SW2 returned from the SIM~~

~~SW1~~	~~SW2~~	~~Description~~
~~'90'~~	~~'00'~~	~~- Normal ending of the command~~
~~'98'~~	~~'04'~~	~~- Unsuccessful verification.~~

H.3 Authentication commands

Description

It is necessary to provide six interfaces to the CAVE Algorithm and Secret Data areas, as listed below:

- Generation of Authentication Signature data, and generation of ciphering keys.
- Validation and storage of entered A-Key's
- Ask Random task (generates RANDBS)
- Update Shared Secret Data (Generates SSD_A_NEW, SSD_B_NEW and AUTHBS values)
- Confirm Shared Secret Data (Updates SSD values)
- CMEA Encryption of voice channel data digits

NOTE: For each task, the expected normal (i.e. success) status code is listed in the status word description. A list of possible error codes that apply to all tasks can be found in the SIM Status Codes.

The interpretation of these instruction codes (INS in the table below) is valid only for class A0.

Task Name	**CLA**	**INS**	**P1**	**P2**	**Lc**
Internal_Authenticate	'A0'	'88'	'00'	'00'	'0F'
AKEY_validation	'A0'	'86'	'00'	'00'	'12'
Ask_Random	'A0'	'8A'	'00'	'00'	'04'
Update_SSD	'A0'	'84'	'00'	'00'	'0C'
Confirm_SSD	'A0'	'82'	'00'	'00'	'03'
CMEA_encrypt	'A0'	'8C'	'00'	'00'	'nn'

H.3.1 Generation of Authentication Signature Data and Ciphering Keys

This task produces an Authentication response, and shall be used during mobile Registrations, Originations, Terminations, R_Data messages, SPACH Confirmations, and for the Unique Challenge-Response Procedure. If Byte 0, Bit 1 is set, the SIM should also generate key bits after completing the Authentication function. Some of those ciphering octets may be passed back to the ME for use with supplementary crypto mechanisms which reside in the ME. This task requires the following input parameters:

Task Name	CLA	INS	P1	P2	Lc
Internal Authenticate	'A0'	'88'	'00'	'00'	'0F'

Data Bytes:

Byte 0 Process Control Byte

Bit 0 0=RANDs, 1= RANDU

Bit 1 Generate Key Bits flag (0= No, 1= Yes)

Bit 2 Load Internal key flag

(0= pass all generated key bytes to handset, 1= load first 8 bytes of generated keys internally to SIM, pass all remaining key bytes to ME)

Bits 3-7 Unused, future expansion

Bytes 1-4 RANDs (for Registrations, Originations, and Terminations)

or

(1-3) RANDU (for Unique Challenge-Response Procedures)

(4) = 0 (MIN2 will be filled in by SIM)

Byte 5 Digits Length (in bits, =0, 4, 8, 12, 16, 20 or 24,

= 4 x number of digits in bytes 6-8)

Bytes 6-8 =0,0,0 (for Registrations, Terminations, Unique Challenge Response Procedures)

= Last Dialed Digits, unused bits filled with 0's (for Originations). If more than 6 digits are dialed, these are the last 6 digits in the origination string. If less than 6 digits are dialed, MIN1 will be filled in by the SIM for the unused bits.

Byte 9 Use ME ESN (=‘00’)

Bytes 10-13 ESN

Byte 14 Key_size (=0 if Byte 0, Bit 1= 0, =8 (or more) if Byte 0, Bit 1 = 1)

The output of this task shall be:

Status Bytes: SW1 (=‘9F’ if success)

SW2 (=‘nn’ if success)

(‘nn’ is 03+Key_size if Byte 0, Bit 2 above =0, 03+Key_size-08 if Byte 0, Bit 2 above =1)

H.3.2 Validation and Storage of Entered A-Key's

With manual entry of the A-key, the input A-Key must be validated prior to its storage in the SIM. If successful, the A-key is saved in the SIM and the COUNTsp and Shared Secret Data (SSD) are reset to zero. This task requires the following input parameters:

Task Name	CLA	INS	P1	P2	Lc
AKEY_validation	'A0'	'86'	'00'	'00'	'12'

Data Bytes:

Bytes 0-12 Authentication digits string (first digit in Most-Significant nibble of byte 0, last digit in Least-Significant nibble of Byte 12, for a total of 26 digits)

Byte 13 Use ME ESN (='00')

Bytes 14-17 ESN

The output of this task shall be:

Status Bytes: SW1 (='90' if success)

SW2 (='00' if success)

H.3.3 Ask Random Task

This task is used to generate the RANDBS random value. This task must be executed prior to updating the Shared Secret Data (SSD). The value RANDSeed must be generated by the ME prior to calling this task. This task requires the following input parameters:

Task Name	**CLA**	**INS**	**P1**	**P2**	**Lc**
Ask_Random	‘A0’	‘8A’	‘00’	‘00’	‘04’

Data Bytes:

Bytes 0-3 RANDSeed

The output of this task shall be:

Status Bytes: SW1 (=‘9F’ if success)

SW2 (=‘04’ if success)

H.3.4 Update Shared Secret Data

This task is used to generate the preliminary new Shared Secret Data (SSD_A_NEW, SSD_B_NEW) and the AUTHBS value. The Ask Random Task (see above) must be executed prior to this routine. The task requires the following input parameters:

Task Name	CLA	INS	P1	P2	Lc
Update_SSD	‘A0’	‘84’	‘00’	‘00’	‘0C’

Data Bytes:

Bytes 0-6 RANDSSD

Byte 7 Use ME ESN (=‘00’)

Bytes 8-11 ESN

The output of this task shall be:

Status Bytes: SW1 (=‘90’ if success, =‘98’ if failure)

SW2 (=‘00’ if success, =‘04’ if failure)

H.3.5 Confirm Shared Secret Data

This task is used to validate the new Shared Secret Data (SSD_A_NEW, SSD_B_NEW) by comparing the internally computed AUTHBS with the AUTHBSs received from the system. If successful, the SSD_A and SSD_B values will be updated to match the SSD_A_NEW and SSD_B_NEW values, respectively The task requires the following input parameters:

Task Name	**CLA**	**INS**	**P1**	**P2**	**Lc**
Confirm_SSD	‘A0’	‘82’	‘00’	‘00’	‘03’

Data Bytes:

Bytes 0-2 AUTHBSs

The output of this task shall be:

Status Bytes: SW1 (=‘90’ if success)

SW2 (=‘00’ if success)

H.3.6 CMEA Encryption of Voice Channel Data Digits

This task is used when the MS is on a Voice Channel, to encrypt and decrypt some portions of digital messages transmitted to the BS. These will occur for the following messages:

- Called Address Message (in response to a hookflash, up to 4 bytes per word, 4 words, total of 16 bytes)

Task Name	**CLA**	**INS**	**P1**	**P2**	**Lc**
CMEA_encrypt	‘A0’	‘8C’	‘00’	‘00’	‘nn’

(‘nn’ is hex value of data length n)

Data Bytes:

Bytes 0 - (n-1) The n-byte data to be encoded, max. size = 32 bytes.

The output of this task shall be:

Status Bytes: SW1 (=‘9F’ if success)

SW2 (=‘nn’ if success) (‘nn’ is hex value of data length n)

H.3.7 SIM Status Codes

The following status codes, returned by the SIM in response to the execution of any of the tasks specified in this document, are valid. The first hex value is returned in SW1, the second hex value in SW2.

Success Codes:

90, 00 Generic success code

9F, xx Success, xx bytes of data available to be read via “Get_Response” task.

Error Codes:

92, 40 Error, memory problem

94, 08 Error, file is inconsistent with the command

98, 04 Error, no CHV1 has been presented successfully

98, 34 Error, Update SSD order sequence not respected (should be used if SSD Update commands are received out of sequence).

67, xx Error, incorrect parameter P3 (ISO code)

6B, xx Error, incorrect parameter P1 or P2 (ISO code)

6D, xx Error, unknown instruction code given in the command (ISO code)

6E, xx Error, wrong instruction class given in the command (ISO code)

6F, xx Error, technical problem with no diagnostic given (ISO code)

6F, 00 Error, invalid input parameters to authentication computation