ETSI TS 131 104 V17.0.0 (2022-04)

Universal Mobile Telecommunications System (UMTS);
LTE;
Characteristics of the Hosting Party Subscription Identity Module (HPSIM) application
(3GPP TS 31.104 version 17.0.0 Release 17)

Reference
RTS/TSGC-0631104vh00

Keywords
LTE,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

Y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

Z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

The present document defines the Hosting Party Subscription Identity Module (HPSIM) application. This application resides on the UICC, an IC card specified in TS 31.101 [3]. In particular, TS 31.101 [3] specifies the application independent properties of the UICC/terminal interface such as the physical characteristics and the logical structure.

1 Scope

The present document applies to a H(e)NB supporting the HPSIM for H(e)NB Hosting Party authentication. The present document defines the HPSIM application, the UICC application residing in the Hosting Party Module for H(e)NB Hosting Party authentication and provisioning.

The present document specifies

- identification of the Hosting Party
- security mechanism, e.g. authentication based on EAP-AKA method
- support of information for the initial provisioning (e.g. O&M system contact)
- initialisation procedure on H(e)NB-UICC interface
- O&M procedure

2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.320: "Security of Home Node B (HNB)/ Home evolved Node B (HeNB)".

[3] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

[4] 3GPP TS 22.220: "Service requirements for Home Node B (HNB)/ Home eNode B (HeNB)".

[5] 3GPP TS 33.102: "3G Security; Security Architecture".

[6] ISO/IEC 7816-4: "Integrated circuit cards, Part 4: Organization, security and commands for interchange".

[7] 3GPP TS 31.102: "Characteristics of the USIM application".

[8] 3GPP TS 25.467: "UTRAN architecture for 3G Home NodeB (HNB)".

[9] IETF RFC 3629 (2003): "UTF-8, a transformation format of ISO 10646".

[10] ISO/IEC 8825-1 (2008): "Information technology – ASN.1 encoding rules : Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)"

[11] ETSI TS 101 220: "Smart Cards; ETSI numbering system for telecommunication application providers".

[12] Void.

[13] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[14] 3GPP TS 32.583: "Telecommunications management; Home Node B (HNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Procedure flows for Type 1 interface HNB to HNB Management System (HMS)".

[15] 3GPP TS 32.593: "Telecommunications management; Home Node B (HeNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Procedure flows for Type 1 interface HeNB to HeNB Management System (HeMS)".

[16] Void.

[17] 3GPP TS 36.413, "S1 Application Protocol".

[18] 3GPP TS 31.115: "Secured packet structure for (U)SIM Toolkit applications"

[19] 3GPP TS 31.116: "Remote APDU structure for (U)SIM Toolkit applications"

[20] 3GPP TS 31.111: "USIM application toolkit"

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1], TS 22.220 [4] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1] and TS 22.220 [4].

HPSIM: UICC application residing on the Hosting Party Module, providing necessary mechanism for H(e)NB Hosting Party authentication and provisioning.

3.2 Symbols

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

||	Concatenation
⊕	Exclusive or
f1	Message authentication function used to compute MAC
f1*	A message authentication code (MAC) function with the property that no valuable information can be inferred from the function values of f1* about those of f1, ... , f5 and vice versa
f2	Message authentication function used to compute RES and XRES
f3	Key generating function used to compute CK
f4	Key generating function used to compute IK
f5	Key generating function used to compute AK

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

FQDN	Fully Qualified Domain Name
HeMS	Home eNodeB Management System
HeNB	Home evolved NodeB
HeNB-GW	HeNB Gateway
HMS	HNB Management System
HNB	Home NodeB
HNB-GW	Home NodeB Gateway

HPSIM	Hosting Party Subscription Identity Module.
H(e)MS	HMS or HeMS
H(e)NB	HNB or HeNB
H(e)NB-GW	HNB-GW or HeNB-GW
K	Long-term secret Key shared between the HPSIM and the AuC
MME	Mobility Management Entity

3.4 Coding Conventions

The following coding conventions apply to the present document.

All lengths are presented in bytes, unless otherwise stated. Each byte is represented by bits b8 to b1, where b8 is the most significant bit (MSB) and b1 is the least significant bit (LSB). In each representation, the leftmost bit is the MSB.

The coding of Data Objects in the present document is according to TS 31.101 [3].

'XX': Single quotes indicate hexadecimal values. Valid elements for hexadecimal values are the numbers '0' to '9' and 'A' to 'F'.

4 Files

4.0 Overview

Clause 4 of the present document specifies the Efs for the H(e)NB session defining access conditions, data items and coding. A data item is a part of an EF which represents a complete logical entity.

4.1 Contents of the Efs at the MF level

There are four Efs at the Master File (MF) level. These Efs are specified in TS 31.101 [3].

4.2 Contents of files at the HPSIM ADF (Application DF) level

4.2.0 HPSIM ADF overview and card issuer-reserved file identifiers

The Efs in the HPSIM ADF contain service and network related information and are required for H(e)NB to operate in a 3GPP environment.

The File Ids '6F1X' (for Efs), '5F1X' and '5F2X' (for DFs) with X ranging from '0' to 'F' are reserved under the HPSIM ADF for administrative use by the card issuer.

4.2.1 EF_{ARR} (Access Rule Reference)

This EF contains the access rules for files located under the HPSIM ADF in the UICC. If the security attribute tag '8B' is indicated in the FCP it contains a reference to a record in this file.

Structure of EF_{ARR} at ADF-level

Identifier: '6F06'	Structure: Linear fixed	Mandatory
SFI: '06'		
Record Length: X bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to X	Access Rule TLV data objects	M	X bytes

This EF contains one or more records containing access rule information according to the reference to expanded format as defined in ISO/IEC 7816-4 [6]. Each record represents an access rule. Unused bytes in the record are set to 'FF'.

If the card cannot access EF_{ARR} , any attempt to access a file with access rules indicated in this EF_{ARR} shall not be granted.

4.2.2 EF_{IMSI} (IMSI)

This EF contains the International Mobile Subscriber Identity (IMSI).

An HPSIM shall be provisioned with an IMSI value as defined in TS 33.320 [2].

Identifier: '6F07'	Structure: transparent	Mandatory
SFI: '07'		
File size: 9 bytes	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1	Length of IMSI	M	1 byte
2 to 9	IMSI	M	8 bytes

For the content and coding, refer to TS 31.102 [7].

4.2.3 EF_{AD} (Administrative Data)

This EF contains information concerning the mode of operation according to the type of HPSIM, such as normal (to be used by Hosting Party for H(e)NB operation), type approval (to allow specific use of the H(e)NB during type approval procedures of e.g. the network equipment), manufacturer specific (to allow the H(e)NB manufacturer to perform specific proprietary auto-test in its H(e)NB during e.g. maintenance phases).

It also provides an indication of whether some H(e)NB features should be activated during normal operation.

Identifier: '6FAD'	Structure: transparent	Mandatory
SFI: '03'		
File size: 4+X bytes	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	H(e)NB operation mode	M	1 byte
2 to 3	Additional information	M	2 bytes
4	length of MNC in the IMSI	M	1 byte
5 to 4+X	RFU	O	X bytes

- H(e)NB operation mode:

  Contents:

  - mode of operation for the H(e)NB.

  Coding:

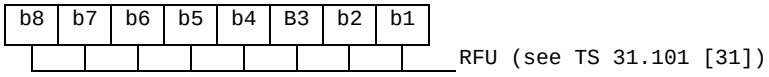
  - Initial value
    - '00' normal operation.
    - '80' type approval operations.
    - '01' normal operation + specific facilities.
    - '81' type approval operations + specific facilities.
    - '02' maintenance (off line).

- Additional information:

  Coding:

  - specific facilities (if b1=1 in byte 1);

    Bytes 2 and 3 (first byte of additional information):



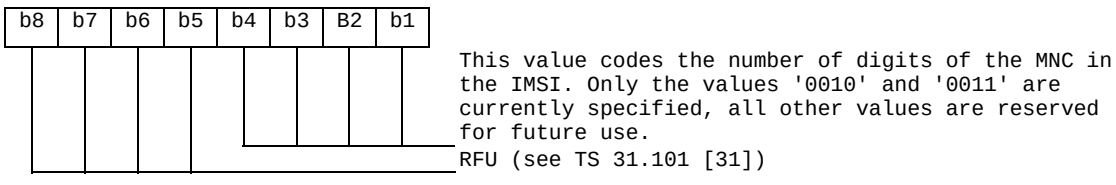
- Length of MNC in the IMSI:

Contents:

The length indicator refers to the number of digits, used for extracting the MNC from the IMSI

Coding:

Byte 4:



4.3 HPSIM file structure

This clause contains a figure depicting the file structure of the ADF_{HPSIM}.

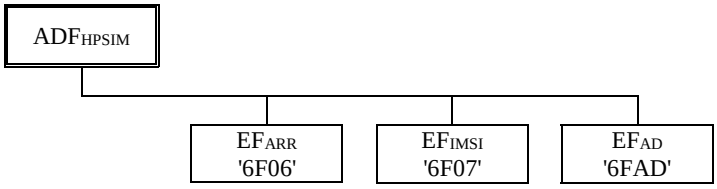


Figure 1: File identifiers and directory structure of the HPSIM

5 Application Protocol

5.0 Overview of HPSIM selection and HPSIM-related procedures

The requirements stated in the corresponding clause of TS 31.101 [3] apply to the HPSIM application. The ADF_{HPSIM} shall be selected using the AID and information in EF_{DIR}.

The procedures listed in clause "5.1 HPSIM management procedures" are required for execution of the procedures in the subsequent clause "HPSIM security related procedures". The procedures authentication procedure, IMSI request, which are listed in clause "HPSIM security related procedures" are mandatory.

5.1 HPSIM management procedures

5.1.1 Initialisation

5.1.1.1 HPSIM application selection

After UICC activation (see TS 31.101 [3]), the H(e)NB shall select an HPSIM application. If no HPSIM applications are found in the UICC, the H(e)NB shall abort the HPSIM initialisation procedure.

An HPSIM compliant to the present document shall have an AID with a PIX value starting with '3G application code' ='100A', see ETSI TS 101 220 [11].

After a successful HPSIM application selection, the selected HPSIM (AID) is stored on the UICC. This application is referred to as the last selected application. The last selected application shall be available on the UICC after a deactivation followed by an activation of the UICC.

If a HPSIM application is selected using partial DF name, the partial DF name supplied in the command shall uniquely identify a HPSIM application. Furthermore if a HPSIM application is selected using a partial DF name as specified in TS 31.101 [3] indicating in the SELECT command the last occurrence the UICC shall select the application stored as the last application. If, in the SELECT command, the options first, next/previous are indicated, they have no meaning if an application has not been previously selected in the same session and shall return an appropriate error code.

5.1.1.2 HPSIM initialisation

The HPSIM shall not indicate any language preference.

If the H(e)NB provides an user interface, the H(e)NB shall choose a language from EF_{PL} at the MF level according the procedure defined in TS 31.101 [3]. If the H(e)NB does not support the languages of EF_{PL}, the H(e)NB shall use its own internal default parameters.

If supported by H(e)NB, the H(e)NB runs the PIN verification procedure. If the procedure is not performed successfully, the HPSIM initialisation stops.

If both the application selection and the PIN verification procedures have been performed successfully then the HPSIM session starts. In all other cases the HPSIM session shall not start.

After the previous procedures have been completed successfully, the H(e)NB runs the following procedures:

- Administrative information request, by reading the EF_{AD}.
- IMSI request.

After the HPSIM initialisation has been completed successfully, the H(e)NB shall indicate this to the HPSIM by sending a particular STATUS command.

5.1.2 HPSIM Session termination

NOTE 1: This procedure is not to be confused with the deactivation procedure in TS 31.101 [3].

The HPSIM session is terminated by the H(e)NB as follows.

The H(e)NB shall indicate to the HPSIM by sending a particular STATUS command that the termination procedure is starting.

The H(e)NB deletes all the subscription related information elements from its memory.

NOTE 2: If the H(e)NB has already updated any of the subscriber related information during the session, and the value has not changed until session termination, the H(e)NB may omit the respective update procedure.

To actually terminate the session, the H(e)NB shall use one of the mechanisms described in TS 31.101 [3].

5.1.3 HPSIM application closure

After termination of the HPSIM session as defined in clause 5.1.2, the HPSIM application may be closed by closing the logical channels that are used to communicate with this particular HPSIM application.

5.1.4 UICC presence detection

The H(e)NB checks for the presence of the UICC according to TS 31.101 [3] within all 30 s periods of inactivity on the UICC-Terminal interface. If the presence detection according to TS 31.101 [3] fails, then the H(e)NB shall follow the requirements listed in TS 33.220 [2] for the removal of the HPM within 5s after the presence detection has failed.

5.2 HPSIM security related procedures

5.2.1 Authentication procedure

The H(e)NB selects a HPSIM application and uses the AUTHENTICATE command (see clause 7.1).

5.2.2 IMSI request

Request: The H(e)NB performs the reading procedure with EF_{IMSI}.

5.3 Subscription related procedures

5.3.1 Location Information acquisition procedures

The support of Location Information acquisition procedures is optional for both the HPSIM and the H(e)NB. However, if implemented, it shall be according to the present clause.

For the purpose of Location Information acquisition, a H(e)NB shall support the PROVIDE LOCAL INFORMATION proactive command as specified below.

An HPSIM and a H(e)NB supporting Location Information acquisition procedure shall support the following mechanism defined in TS 31.111 [20].

- PROVIDE LOCAL INFORMATION, H(e)NB IP address (letter class "v").

Additionally, the HPSIM and H(e)NB may support one or both of the following mechanism defined in TS 31.111 [20].

- PROVIDE LOCAL INFORMATION, H(e)NB surrounding macrocells (letter class "w")

- Geographical Location Reporting (letter class "n").

The support of any other option of the PROVIDE LOCAL INFORMATION proactive command is not required.

The HPSIM retrieves location information using one or a combination of the USAT commands listed above.

The HPSIM shall only require location information after HPSIM initialisation procedure, and at regular intervals as Operator policy requires.

Note : IP address change procedures are defined in TS 32.583 [14] for HNB and in TS 32.593 [15] for HeNB.

6 Security features

6.0 Generic security

The security aspects of H(e)NB are specified in TS 33.320 [2]. Clause 6 of the present document gives information related to security features supported by the HPSIM with respect to user verification and file access conditions.

6.1 User verification and file access conditions

The User of the HPSIM is the H(e)NB Hosting Party.

The security architecture as defined in TS 31.101 [3] applies to the HPSIM and UICC with the following definitions and additions:

- The HPSIM application shall use a global key reference PIN1 as specified in TS 31.101 [3].
- The only valid usage qualifier is '08' which means user authentication knowledge based (PIN) as defined in ISO/IEC 7816-4 [6].

In order to restrict the access to the HPSIM, the PIN may be enabled.

7 HPSIM commands

7.0 Generic commands

The commands specified in TS 31.101 [3] are supported by HPSIM, with the restrictions identified in clause 7 of the present document.

7.1 AUTHENTICATE

7.1.1 Command description

The function can be used in the following security context:

- AKA security context during the procedure for authenticating the HPSIM to the Home Network and vice versa when AKA authentication data are available. The function shall be used whenever an AKA context shall be established, i.e. when the terminal receives a challenge from the AKA. A cipher key and an integrity key are calculated. For the execution of the command the HPSIM uses the subscriber authentication key K, which is stored in the HPSIM. The same AKA security context is used for HNB and H(e)NB authentication.

The function is related to a particular HPSIM and shall not be executable unless the HPSIM application has been selected and activated, and the current directory is the HPSIM ADF or any subdirectory under this ADF and a successful PIN verification procedure has been performed (see clause 6.1).

The HPSIM first computes the anonymity key AK = $f5_K$ (RAND) and retrieves the sequence number SQN = (SQN ⊕ AK) ⊕ AK.

Then the HPSIM computes XMAC = $f1_K$ (SQN || RAND || AMF) and compares this with the MAC which is included in AUTN. If they are different, the HPSIM abandons the function.

Next the HPSIM verifies that the received sequence number SQN is previously unused. If it is unused and its value is lower than SQN_{MS}, it shall still be accepted if it is among the last 32 sequence numbers generated. A possible verification method is described in TS 33.102 [5].

NOTE: This implies that the HPSIM has to keep a list of the last used sequence numbers and the length of the list is at least 32 entries.

If the HPSIM detects the sequence numbers to be invalid, this is considered as a synchronisation failure and the HPSIM abandons the function. In this case the command response is AUTS, where:

- $AUTS = Conc(SQN_{MS}) \,||\, MACS$;
- $Conc(SQN_{MS}) = SQN_{MS} \oplus f5^*_K(RAND)$ is the concealed value of the counter SQN_{MS} in the HPSIM; and
- $MACS = f1^*_K(SQN_{MS} \,||\, RAND \,||\, AMF)$ where:
- *RAND* is the random value received in the current user authentication request;

If the sequence number is considered in the correct range, the HPSIM computes RES = $f2_K$ (RAND), the cipher key CK = $f3_K$ (RAND) and the integrity key IK = $f4_K$ (RAND) and includes these in the command response. Note that if this is more efficient, RES, CK and IK could also be computed earlier at any time after receiving RAND.

The use of AMF is HN specific and while processing the command, the content of the AMF has to be interpreted in the appropriate manner. The AMF may e.g. be used for support of multiple algorithms or keys or for changing the size of lists, see TS 33.102 [5]. The AMF contains the EPS AKA indication bit, see TS 33.401 [13]. This bit is not interpreted by HPSIM.

7.1.2 Command parameters and data

Editor's note : HPSIM does not need to support ODD instruction code.

Code	Value
CLA	As specified in TS 31.101 [3]
INS	'88'
P1	'00'
P2	See table below
Lc	See below
Data	See below
Le	'00', or maximum length of data expected in response

Parameter P2 specifies the authentication context as follows:

Coding of the reference control P2:

Coding b8-b1	Meaning
'1-------'	Specific reference data (e.g. DF specific/application dependant key)
'-XXXX---'	'0000'
'-----XXX'	Authentication context: 001 AKA

All other codings are RFU.

Parameter P1 is used to control the data exchange between the terminal and the UICC as defined in TS 31.101 [3].

Parameter P2 is set to '81'.

Command parameters/data:

Byte(s)	Description	Length
1	Length of RAND (L1)	1
2 to (L1+1)	RAND	L1
(L1+2)	Length of AUTN (L2)	1
(L1+3) to (L1+L2+2)	AUTN	L2

The coding of AUTN is described in TS 33.102 [5]. The most significant bit of RAND is coded on bit 8 of byte 2. The most significant bit of AUTN is coded on bit 8 of byte (L1+3).

Response parameters/data, case 1, command successful:

Byte(s)	Description	Length
1	"Successful 3G authentication" tag = 'DB'	1
2	Length of RES (L3)	1
3 to (L3+2)	RES	L3
(L3+3)	Length of CK (L4)	1
(L3+4) to (L3+L4+3)	CK	L4
(L3+L4+4)	Length of IK (L5)	1
(L3+L4+5) to (L3+L4+L5+4)	IK	L5

The most significant bit of RES is coded on bit 8 of byte 3. The most significant bit of CK is coded on bit 8 of byte (L3+4). The most significant bit of IK is coded on bit 8 of byte (L3+L4+5).

Response parameters/data, case 2, synchronization failure:

Byte(s)	Description	Length
1	"Synchronisation failure" tag = 'DC'	1
2	Length of AUTS (L1)	1
3 to (L1+2)	AUTS	L1

The coding of AUTS is described in TS 33.102 [5]. The most significant bit of AUTS is coded on bit 8 of byte 3.

7.1.3 Status Conditions Returned by the HPSIM

7.1.3.0 Status Condition structure

Status of the card after processing of the command is coded in the status bytes SW1 and SW2. Clause 7.1.3 of the present document specifies coding of the status bytes in the following tables.

7.1.3.1 Security management

SW1	SW2	Error description
'98'	'62'	- Authentication error, incorrect MAC

7.1.3.2 Status Words of the Commands

The following table shows for each command the possible status conditions returned (marked by an asterisk *).

Commands and status words

Status Words	AUTHENTICATE
90 00	*
91 XX	*
93 00	
98 50	
98 62	*
62 00	*
62 81	
62 82	
62 83	
62 F1	*
62 F3	*
63 CX	
63 F1	*
64 00	*
65 00	*
65 81	*
67 00	*
67 XX – (see note)	*
68 00	*
68 81	*
68 82	*
69 81	
69 82	*
69 83	
69 84	*
69 85	*
69 86	
6A 80	
6A 81	*
6A 82	
6A 83	
6A 86	*
6A 87	
6A 88	*
6B 00	*
6E 00	*
6F 00	*
6F XX – (see note)	*
NOTE: Except SW2 = '00'.	

8 HPSIM remote management

8.1 General functionality

To support HPSIM remote management the H(e)NB and the HPSIM shall support the Profile Download mechanism as specified in TS 31.111 [20] and a subset of USAT functionality that is described in the following clauses.

An HPSIM shall support "Additional TERMINAL PROFILE after UICC activation" as defined in TS 31.111 [20] and allow the H(e)NB to send multiple Terminal Profile downloads.

8.2 Remote application and file management

HPSIM remote management shall use RAM/RFM over HTTP mechanism described in TS 31.115 [18], TS 31.116 [19].

8.3 Bearer Independent Protocol

The H(e)NB shall support BIP in UICC client mode, and indicate it in TERMINAL PROFILE command as specified in TS 31.111 [20]. After HPSIM management procedures, the UICC shall open a BIP channel in UICC client mode and send a polling message to a remote server for registration.

8.4 Proactive Polling

The H(e)NB shall support the proactive polling mechanism defined in TS 31.101 [3].

8.5 Polling a remote server

It is assumed that the UICC will send a polling message to a remote server at regular intervals, in order to check for updates. The UICC will send a TIMER MANAGEMENT command with appropriate value, in order to be informed when the next polling message shall be sent.

Annex A (informative): EF changes via remote management or USAT application

This annex defines if changing the content of an EF by the network (e.g. remote management) or by a USAT Application is advisable. Updating of certain Efs remotely could result in unpredictable behaviour of the H(e)NB; these are marked "Caution" in the table below. Certain Efs are marked "No"; under no circumstances should remote changes of these Efs be considered.

File identification	Description	Change advised
'2F00'	Application directory	Caution
'2F05'	Preferred languages	Yes
'2F06'	Access rule reference	Caution
'2FE2'	ICC identification	No
'6F06'	Access rule reference (under ADF_{HPSIM})	Caution
'6F07'	IMSI	Caution
'6FAD'	Administrative Data	Caution

Annex B (informative): Suggested content of the Efs at pre-personalization

If Efs have an unassigned value, it may not be clear from the main text what this value should be. This annex suggests values in these cases.

File Identification	Description	Value
'2F00'	Application directory	Card issuer / operator dependent
'2F05'	Preferred languages	'FF..FF'
'2F06'	Access rule reference	Card issuer / operator dependent
'2FE2'	ICC identification	Card issuer / operator dependent
'6F06'	Access rule reference (under ADF_{HPSIM})	Card issuer / operator dependent
'6F07'	IMSI	Operator dependent
'6FAD'	Administrative Data	Operator dependant

Annex C (informative): List of SFI values

This annex lists SFI values assigned in the present document.

C.1 List of SFI Values at the HPSIM ADF Level

File Identification	SFI	Description
'6F06'	'06'	Access Rule Reference
'6F07'	'07'	IMSI
'6FAD'	'03'	Administrative Data

All other SFI values are reserved for future use.

Annex D (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2012-06	CT-56	CP-120405				Specification approved at TSG CT. First publication as v11.0.0	11.0.0
2012-07	-	-				Correction of formatting errors noticed at CT-56 (removal of hanging paragraphs). Indication of correct letter classes for proactive commands mentioned in clause 5.3.1	11.0.1
2012-09	CT-57	CP-120621	001			Correction of reference to ASN.1 coding specification	11.1.0
2013-12	CT-62	CP-130790	002	1		Correction to delete a duplicate reference	11.2.0
2014-10	SA-65					Automatic upgrade to Rel-12	12.0.0
2015-03	CT-67	CP-150157	004	1		Allocation of 3G application code for the HPSIM	12.1.0
2015-12	SA-70					Automatic upgrade to Rel-13	13.0.0
2017-03	SA-75	-	-	-		Automatic Upgrade to Rel-14	14.0.0
2018-07	SA-80					Automatic Upgrade to Rel-15	15.0.0
2020-07	CT#88e	-	-	-		Update to Rel-16 version (MCC)	16.0.0
2020-09	CT#89	CP-202130	0005	1		Update of spec. reference	16.1.0
2022-04	-	-	-	-	-	Update to Rel-17 version (MCC)	**17.0.0**

History

Document history		
V17.0.0	April 2022	Publication