ETSI TS 131 105 V19.0.0 (2025-10)

TECHNICAL SPECIFICATION

5G;
Characteristics of the Slice Subscriber Identity Module application
(3GPP TS 31.105 version 19.0.0 Release 19)

Reference
RTS/TSGC-0631105vj00

Keywords
5G

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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 at 3GPP to ETSI numbering cross-referencing.

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.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

Introduction

The present document defines the Slice Subscriber Identity Module (SSIM) application. This application resides on the UICC as specified in TS 31.101 [2]. In particular, TS 31.101 [2] specifies the application independent properties of the UICC/terminal interface such as the physical characteristics and the logical structure.

TS 31.101 [2] is one of the core documents for this specification and is therefore referenced in many places in the present document.

UICC detection clause is removed as useless in case of SSIM, the UICC detection is following the USIM requirement as USIM always selected for primary authentication.

1 Scope

The present document defines the SSIM application for 3GPP telecom network operation related to Network Slice-Specific Authentication and Authorization procedure.

The present document specifies:

- specific command parameters;
- file structures;
- contents of EFs (Elementary Files);
- security functions;
- application protocol to be used on the interface between UICC (SSIM) and ME.

This is to ensure interoperability between a SSIM and an ME independently of the respective manufacturer, card issuer or operator.

The present document does not define any aspects related to the administrative management phase of the SSIM. Any internal technical realisation of either the SSIM or the ME is only specified where these are reflected over the interface. The present document does not specify any of the security algorithms which may be used.

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 TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

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

[4] 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)".

[5] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[6] 3GPP TS 33.501: "Security Architecture and procedures for 5G system".

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

[8] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[9] IETF RFC 2716: "PPP EAP TLS Authentication Protocol".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1] 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].

PIN/ADM: A terminal is required to evaluate the access condition and verify it in order to access the EF if the access condition is set to PIN or PIN2.

Slice SIM: UICC application residing on the UICC, providing necessary mechanism for Network Slice-Specific Authentication and Authorization (NSSAA).

3.2 Symbols

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

|| Concatenation

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].

AAA-S	Authentication, Authorization and Accounting Server
AID	Application Identifier
EF	Elementary File
EAP	Extensible Authentication Protocol
NSSAA	Network Slice-Specific Authentication and Authorization
PIN	Personal Identification Number
SD	Slice Differentiator
SSIM	Slice Subscriber Identity Module
SST	Slice/Service type
S-NSSAI	Single Network Slice Selection Assistance Information

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 [2].

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

4 Contents of the Files

This clause specifies the EFs for the 3GPP session defining access conditions, data items and coding. A data item is a part of an EF which represents a complete logical entity.

A file is associated with attributes that depending of the file type indicates how data is to be accessed e.g. file size, record length etc. Although in the present document some files and data items stored in a file are indicated as having a fixed length; when reading such structures the terminal shall derive the length of the data item from the attributes provided in the file information i.e. not use the fixed value specified for the file in the present document. Although the terminal is able to read the entire structure it should only use those elements in the data item which is recognised by the terminal.

For any EF, when the SFI is not indicated in the description of the file it is not allowed to assign an SFI. If in the description of the file an SFI value is indicated the file shall support SFI. The SFI value shall be assigned by the card issuer. It is mandatory for EFs stating an SFI value ('YY') in the description of their structure to provide an SFI. For files where in the file description the SFI is indicated as 'Optional' the file may support an SFI.

For an overview containing all files see figure 1.

4.1 Contents of the EFs at the MF level

The EFs at the Master File (MF) level are specified in TS 31.101 [2].

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

The EFs in the SSIM ADF contain service and NSSAA procedure information related.

The File Ids '6F1X' (for EFs), '5F1X' and '5F2X' (for DFs) with X ranging from '0' to 'F' are reserved under the SSIM 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 SSIM 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.

Table 4.2.1-1: Structure of EF_{ARR} at ADF-level

Identifier: '6F06'	Structure: Linear fixed	Mandatory
SFI: '06'		
Record Length: X bytes, (X > 0)	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 [3]. 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_{EAPID} (EAP Identifier)

This file shall be available.

This EF contains the EAP Identifier to be used in NSSAA procedure.

Table 4.2.2-1: EF_{EAPID} file structure

Identifier: '6F01'	Structure: transparent	Mandatory
SFI: '01'		
File size: X bytes	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to X	EAP ID TLV data object	M	X bytes

EAP ID

Contents:

- EAP ID used for the NSSAA procedure

Coding: the coding of EAP ID TLV data object is described hereafter.

Table 4.2.2-2: EAP ID TLV data object coding

Length	Description	Value	Status
1 byte	EAP ID Tag	80	M
1 byte	Length (see note 1)	Z	M
Z bytes	EAP Identifier	--	M
Note 1: coded according to ISO/IEC 8825-1 [4].			

4.2.3 EF_{NSSAI} (S-NSSAI List)

This file shall be available.

This EF contains one or more records, each indicating the S-NSSAI supported by the SSIM application.

Table 4.2.3-1: EF_{NSSAI} file structure

Identifier: '6F02'	Structure: linear fixed	Mandatory
SFI: '02'		
Record length: 4 bytes	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to 4	S-NSSAI	M	4 bytes

S-NSSAI

Contents:

- S-NSSAI for which the SSIM application is used for NSSAA procedure

Coding:

- S-NSSAI shall be coded on 32 bits as specified in TS 23.003 [5], SD reserved value "no SD value associated with the SST" defined as hexadecimal FFFFFF shall be used to pad value to 32 bits.

4.2.4 $EF_{EAPSTATUS}$ (EAP Authentication Status)

This file shall be available.

This EF contains the authentication status corresponding to the EAP client supported by the SSIM application for ongoing NSSAA procedure(s) associated with S-NSSAI(s).

This EF contains the same number of records as EF_{NSSAI}.

Table 4.2.4-1: $EF_{EAPSTATUS}$ file structure

Identifier: '6F03'	Structure: linear fixed		Mandatory
SFI: '03'			
Record length: 5 bytes		Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to 4	S-NSSAI	M	4 bytes
5	Authentication status	M	1 byte

S-NSSAI

Contents:

- S-NSSAI associated to ongoing NSSA procedure.

Coding:

- S-NSSAI shall be coded on 32 bits as specified in TS 23.003 [5], SD reserved value "no SD value associated with the SST" defined as hexadecimal FFFFFF shall be used to pad value to 32 bits.

Authentication Status

Contents:

- Status of the corresponding EAP authentication.

Coding:

- Authentication status is coded in one byte as below.

Table 4.2.4-2: Authentication status values

Value	Meaning
'00'	No authentication started
'01'	Authenticating
'02'	Authenticated
'03'	Held (Authentication failure)

4.3 SSIM file structure

This clause contains a figure depicting the file structure of the ADF_{SSIM}. ADF_{SSIM} shall be selected using the AID and information in EF_{DIR}.

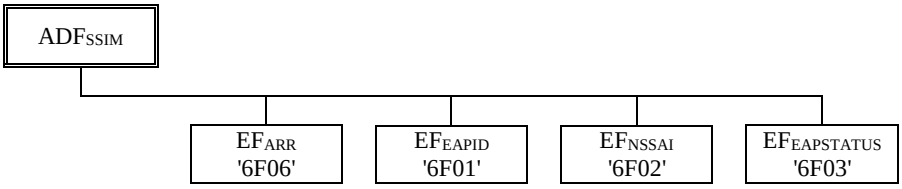

Figure 1: File identifiers and directory structures of SSIM

5 Application protocol

The requirements stated in the corresponding clause of TS 31.101 [2] apply to the SSIM application.

The procedures listed in clause "SSIM management procedures" are required for execution of the procedures in the subsequent clauses "SSIM security related procedures". The procedures listed in clauses "SSIM security related procedures" are mandatory.

5.1 SSIM management procedures

5.1.0 SSIM identification

When a Network Slice-Specific Authentication and Authorization procedure starts as specified in TS 33.501 [6] on a S-NSSAI, the ME shall use the appropriate SSIM (clause 5.1.1) based on following criteria:

1) the AID is present in EF_{DIR} and identified with '3GPP SSIM' App Code as defined in Annex E,

2) the S-NSSAI of the NSSAA procedure listed in the application as described in S-NSSAI list request, clause 5.1.5

5.1.1 SSIM initialisation

5.1.1.1 SSIM application selection

The ME shall select an SSIM application using the SELECT by DF name as defined in TS 31.101 [2].

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

If a SSIM application is selected using partial DF name, the partial DF name supplied in the command shall uniquely identify a SSIM application. Furthermore, if a SSIM application is selected using a partial DF name as specified in TS 31.101 [2] indicating in the SELECT command the last occurrence the UICC shall select the SSIM application stored as the last SSIM 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 SSIM initialisation

The SSIM shall not indicate any language preference. It shall use the language indicated by any other application currently active on the UICC or by default, choose a language from EF_{PL} at the MF level according to the procedure defined in TS 31.101 [2].

If the ME does not support the languages of EF_{PL}, then the ME shall use its own internal default selection.

The ME then runs the:

- user verification procedure.
- EAP Identifier request.

If all these procedures have been performed successfully then the Network Slice-Specific Authentication and Authorization procedure shall start. In all other cases Network Slice-Specific Authentication and Authorization procedure shall not start.

After the SSIM initialisation has been completed successfully, the ME is ready for an SSIM session and shall indicate this to the SSIM by sending a particular STATUS command as defined in TS 31.101 [2].

5.1.2 SSIM session termination

NOTE 1: This procedure is not to be confused with the deactivation procedure in TS 31.101 [2].

The SSIM session is terminated by the ME as follows.

The ME deletes all these NSSAA procedure related information elements from its memory.

NOTE 2: If the ME has already updated any of the NSSAA procedure related information during the NSSAA procedure, and the value has not changed until SSIM session termination, the ME may omit the respective update procedure.

To terminate the session, the ME shall then use one of the mechanisms described in TS 31.101 [2].

5.1.3 SSIM application closure

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

5.1.4 EAP Identifier request

The ME performs the reading procedure with EF_{EAPID}.

5.1.5 S-NSSAI list request

The ME performs the reading procedure with EF_{NSSAI}.

5.1.6 S-NSSAI Authentication status verification procedure

After NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT NAS message received from AMF and when receiving the following CONFIGURATION UPDATE COMMAND NAS message from AMF including one or more S-NSSAI(s) in IE Allowed NSSAI (respectively IE Partially Allowed NSSAI) not currently in Allowed NSSAI (respectively Partially Allowed NSSAI) stored in the ME non-volatile memory, the UE shall check that each corresponding new S-NSSAI is supported by the SSIM and the EAP Authentication Status in the corresponding record of $EF_{EAPSTATUS}$ is 'Authenticated' to store each new S-NSSAI in the Allowed NSSAI (respectively Partially Allowed NSSAI) in the ME non-volatile memory.

5.2 SSIM security related procedures

5.2.1 Authentication procedure

The ME selects a SSIM application (see 5.1) and uses the AUTHENTICATE command (see 7.2). The response is sent to the ME (in case of the T=0 protocol when requested by a subsequent GET RESPONSE command).

6 Security features

6.0 General

The security aspects of NSSAA procedure are specified in TS 33.501 [6]. This clause gives information related to security features supported by the SSIM with respect to user verification and file access conditions.

6.1 User verification and file access conditions

The security architecture as defined in TS 31.101 [2] applies to the SSIM and UICC with the following definitions and additions:

- The SSIM application shall use a global key reference as PIN1 as specified in TS 31.101 [2].
- The only valid usage qualifier is '08' which means user authentication knowledge based (PIN) as defined in ISO/IEC 7816-4 [3].

7 SSIM commands

7.0 Introduction

The status conditions and the commands specified in TS 31.101 [2] are supported by SSIM application, with the restrictions identified in the following clauses.

7.1 Status Conditions returned by the SSIM

7.1.0 General

Status of the card after processing of the command is coded in the status bytes SW1 and SW2. This clause specifies the coding of the status bytes in the following tables, in addition to the ones defined in TS 31.101 [2].

7.1.1 Security management

Table 7.1.1-1: Security management error Status Words

SW1	SW2	Error description
'98'	'62'	- Authentication error (EAP Failure Packet received)

7.1.2 Application errors

Table 7.1.2-1: Application error Status Words

SW1	SW2	Error description
'62'	'00'	- No information given, state of non-volatile memory unchanged (EAP Packet silently ignored)

7.1.3 Status Words of the Commands

The provisions of TS 31.101 [2] clause 10.2.2 apply with the exceptions in the following table which shows the possible status conditions returned (marked by an asterisk *).

Table 7.1.3-1: Commands and status words

Status Words	AUTHENTICATE
90 00	*
91 XX	*
93 00	
98 50	
98 62	*
98 64	*
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'.	

7.2 AUTHENTICATE

7.2.1 Command description

The function is used to transfer the EAP packets of the NSSAA procedure from the ME to the SSIM application (i.e. the SSIM application that supports the S-NSSAI requiring the NSSAA procedure).

The SSIM application provides a response EAP packet (as defined in RFC 3748 [8]) or a warning status word according to the EAP method being used.

The SSIM application maintains the EAP authentication status as described for the particular EAP method used.

The function is related to a particular SSIM application and cannot be executable unless this SSIM application is initialised following the SSIM initialisation defined in clause 5.1.1.

NOTE: EAP Identity is provided by the SSIM application.

The following EAP packets are allowed input packets for this command:

- EAP packets with code field equal to 1 "Request", 3 "Success" or 4 "Failure"

- EAP packets with code equal to 2 "Response" for EAP type 1 "Identity" (Code and type values as defined in RFC 3748 [8]).

The command and response data may contain specific EAP method related data as an additional input/output parameter (e.g. gmt_unix_time for EAP-TLS implementations as defined in RFC 2716 [9]).

The AUTHENTICATE command shall use ODD INS code only, the EAP input and response data shall be encapsulated in BER TLV data objects, as specified in TS 31.101 [2].

Input:

- S-NSSAI associated to EAP Packet;

- EAP Packet;

- EAP method related data.

Output:

- Either none (i.e. if authentication successful: EAP success packet received).

Or:

- S-NSSAI associated to EAP Packet;

- EAP Response Packet;

- EAP method related data.

7.2.2 Command parameters and data

Table 7.2.2-1: Command parameters

Code	Value
CLA	As specified in TS 31.101 [2]
INS	As specified in section 11.1.16 of TS 31.101 [2], ODD INS code only
P1	See Table 7.2.2-2 below
P2	00
Lc	Length of command data
Data	See below
Le	Length of the response data

Table 7.2.2-2: Coding of the reference control P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
			0	0	0	0	0	Parameter P1 = 'XXX0 0000' indicates that no information on the algorithm is given. The algorithm is known from EAP packets embedded into EAP command/response data.
x	x	x						As specified in TS 31.101 [2]

Command data:

Table 7.2.2-3: Command data, 'First block of authentication data' (b8b7b6 of P1 set to '100')

Byte(s)	Description	Length
1	BER-TLV Tag, encapsulation data (‘53’ for not structured data as defined in TS 31.101 [2] clause 11.1.16)	1
2 to L+2	BER-TLV length	1 ≤ L ≤ 4 (Note)
L+3 to L+6	S-NSSAI	4
L+7 to Lc	EAP command data (see table 7.2.2-5), possibly segmented	Lc - 5 - L
Note: Length is coded as specified in TS 31.101 [2] clause 11.3		

S-NSSAI shall be coded on 32 bits.

- As specified in TS 23.003 [5], SD reserved value "no SD value associated with the SST" defined as hexadecimal FFFFFF shall be used to pad value to 32 bits.

If command data does not fit in one APDU, subsequent AUTHENTICATE commands with b8b7b6 of P1 set to '000' shall have the following Command data:

Table 7.2.2-4: Command data, 'Next block of authentication data' (b8b7b6 of P1 set to '000'), only if EAP command data is segmented in more than one chained blocks

Byte(s)	Description	Length
1 to Lc	Next block of EAP command data (see table 7.2.2-5)	Lc

Table 7.2.2-5: Coding of EAP command data

Byte(s)	Description	Status	Length
1 to J	EAP packet (coded as defined for the method of EAP used as defined in RFC 3748 [8])	M	J bytes
J+1 to J+K+1	EAP method related data (specified by each application specific document defining a particular EAP method implementation)	O	K bytes
NOTE: The length of an EAP packet is contained within the packet and can therefore be retrieved from it.			

7.2.3 Response data

This clause describes the response data.

Response data:

Table 7.2.3-1: Response data, 'First block of authentication response data' (b8b7b6 of P1 set to '101')

Byte(s)	Description	Length
1	BER-TLV Tag, encapsulation data (‘53’ for not structured data as defined in TS 31.101 [2] clause 11.1.16)	1
2 to L+2	BER-TLV length	1 ≤ L ≤ 4 (Note)
L+3 to L+6	S-NSSAI	4
5 to Le - 4	EAP Packet Response Data (see table 7.2.3-3), possibly segmented	Le - 4
Note: Length is coded as specified in TS 31.101 [2] clause 11.3		

S-NSSAI shall be coded on 32 bits.

- As specified in TS 23.003 [5], SD reserved value "no SD value associated with the SST" defined as hexadecimal FFFFFF shall be used to pad value to 32 bits.

If response data does not fit in one response APDU, subsequent AUTHENTICATE commands with b8b7b6 of P1 set to '001' shall have the following Response data:

Table 7.2.3-2: Response data, 'Next block of authentication response data' (b8b7b6 of P1 set to '001'), only if EAP response data is segmented in more than one chained blocks

Byte(s)	Description	Length
1 to Le	Next block of EAP Packet Response Data (see table 7.2.3-3)	Le - 4

Table 7.2.3-3: Coding of EAP Response data

Byte(s)	Description	Status	Length
1 to L	EAP packet	M	L bytes
L+1 to L+N+1	EAP method related data (specified by each application specific document defining a particular EAP method implementation)	O	N bytes
NOTE: The length of an EAP packet is contained within the packet and can therefore be retrieved from it.			

Annex A (informative): EF changes via Data Download or USAT applications

This annex defines if changing the content of an EF by the network (e.g. by sending an SMS), or by a USAT Application, is advisable. Updating of certain EFs "over the air" could result in unpredictable behaviour of the UE; these are marked "Caution" in the table below. Certain EFs are marked "No"; under no circumstances should "over the air" changes of these EFs be considered.

Table A-1: File change advised

File identification	Description	Change advised
'6F01'	EAP Identifier	Caution
'6F02'	S-NSSAI List	Caution
'6F03'	EAP Authentication Status	Caution
'6F06'	Access rule reference (under ADF_{SSIM})	Caution

Annex B (informative): Suggested contents 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.

Table B-1: Suggested content

File Identification	Description	Value
'6F01'	EAP Identifier	AAA-Server dependent
'6F02'	S-NSSAI List	Slices configuration dependent
'6F03'	EAP Authentication Status	'FFFFFFFF00' (No authentication started)
'6F06'	Access rule reference (under ADF_{SSIM})	Card issuer/SSIM owner dependent

Annex C (normative): List of SFI Values

This annex lists SFI values assigned in the present document.

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

Table C.1-1: SFI list

File Identification	SFI	Description
'6F01'	'01'	EAP Identifier
'6F02'	'02'	S-NSSAI List
'6F03'	'03'	EAP Authentication Status
'6F06'	'06'	Access rule reference (under ADF_{SSIM})

Annex D (informative): Tags defined in 31.105

Table D-1: Allocated Tags

Tag	Name of Data Element	Usage
'80'	EAP Identifier	EF_{EAPID}

Annex E (normative): Allocated 3GPP PIX numbers

The provisions of 3GPP TS 31.101 [2] annex O apply.

Annex F (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2023-08	CT6#116	C6-230423				Proposed skeleton of 31.105	0.0.0
2023-08	CT6#116					From C6-230423 with agreed pCRs C6-230483 and C6-230506	0.1.0
2023-11	CT6#117	C6-230721				From version 0.1.0 with agreed pCRs C6-230633, C6-230635 and C6-230713	0.2.0
2023-12	CT#102	CP-233095				TS presented for information and approval	1.0.0
2023-12	CT#102					TS approved in TSG#102	18.0.0
2024-06	CT#104	CP-241214	0001	1	F	Annex E to refer directly to TS 31.101 Annex O	18.1.0
2024-06	CT#104	CP-241214	0002	3	F	Clarification of ODD instruction chaining mechanism ('First block' vs 'Next block')	18.1.0
2024-09	CT#105	CP-242085	0003	-	D	Editorial Correction to SSIM file structure	18.2.0
2024-12	CT#106	CP-243157	0004	-	F	Contents of the EFs at the MF level	18.3.0
2024-12	CT#106	CP-243157	0005	-	F	Read EFEAPSTATUS for authentication procedure	18.3.0
2025-10	-	-	-	-	-	Update to Rel-19 version (MCC)	**19.0.0**

History

Document history		
V19.0.0	October 2025	Publication