**3GPP TSG-CT WG6 Meeting #112-e***draft***C6-220446**

**E-Meeting, 23rd – 26th August 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **Current version:** | **16.7.0** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps | **X** | ME | **X** | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** |  | | | | | | | | | |
| ***Source to TSG:*** | CT6 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 3 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | |  |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | During:   * **CT#88-e** meeting was approved the **CR0095** on 3GPP TS 31.101 which introduced dedicated AppCode on USIM AID coding dedicated to ’non-IMSI based SUPI Type’ * **CT6#98-e** meeting was approved the **CR0884** on 3GPP TS 31.102 which introduced ’either IMSI or NSI presence’ based on SUPI Type   Two USIMs shall be introduced (i.e. '3GPP USIM' and '3GPP USIM (non-IMSI SUPI Type)').  Test Cases shall be introduced to cover usage on EFSUPI\_NAI when Servise n° 130 is available. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | PIX to use on USIM AID:   * Clause 4.1, update definition of default USIM to clarify the PIX '3GPP USIM' to use in USIM AID * Clause 4.x added, define USIM AID using the PIX '3GPP USIM (non-IMSI SUPI Type)'   Specific USIM definition   * Clause 4.x and sub-clauses added * Clause 4.x.1 added, EFUST configuration (Service n° 130 available) * Clause 4.x.2 added, EFIMSI is not present * Clause 4.x.3 added, EFSUPI\_NAI configuration   SUPI Type NAI test cases added   * Clause 5.x added, cover the SUCI calculation by ME null-scheme using EFSUPI\_NAI | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | No test covering nor the specific USIM AppCode for ’non-IMSI based SUPI Type’ neither the EFSUPI\_NAI usage | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 3.7, 3.8, 4.1, 4.x (new) and sub-clauses, 5.3, 5.x (new) and sub-clauses | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Was | | | | | | | | |

\*\*\*\*\* Next change \*\*\*\*\*

# 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 in same release as the implementation release of the terminal under test applies.

[1] Void

[2] Void

[3] 3GPP TS 23.038: "Alphabets and language-specific information".

[4] 3GPP TS 31.102: "Characteristics of the USIM application".

[5] If the device under test is a

- R99 ME: ETSI TS 102 221 v3.18.0: "UICC-Terminal interface; Physical and logical characteristics",

- Rel-4 ME: ETSI TS 102 221 v4.16.0: "UICC-Terminal interface; Physical and logical characteristics",

- Rel-5 ME: ETSI TS 102 221 v5.10.0: "UICC-Terminal interface; Physical and logical characteristics",

- Rel-6 ME: ETSI TS 102 221 v6.15.0: "UICC-Terminal interface; Physical and logical characteristics",

- Rel-7 ME: ETSI TS 102 221 v7.17.0: "UICC-Terminal interface; Physical and logical characteristics",

- Rel-8 ME: ETSI TS 102 221 v8.5.0: "UICC-Terminal interface; Physical and logical characteristics",

- Rel-9 ME: ETSI TS 102 221 v9.2.0: "UICC-Terminal interface; Physical and logical characteristics"",

- Rel-10 ME: ETSI TS 102 221 v10.0.0: "UICC-Terminal interface; Physical and logical characteristics",

- Rel-11 ME: ETSI TS 102 221 v11.1.0: "UICC-Terminal interface; Physical and logical characteristics",

- Rel-12 ME: ETSI TS 102 221 v12.1.0: "UICC-Terminal interface; Physical and logical characteristics".

- Rel-13 ME: ETSI TS 102 221 v13.2.0: "UICC-Terminal interface; Physical and logical characteristics".

- Rel-14 ME: ETSI TS 102 221 v14.1.0: "UICC-Terminal interface; Physical and logical characteristics".

- Rel-15 ME: ETSI TS 102 221 v15.0.0: "UICC-Terminal interface; Physical and logical characteristics".

[6] 3GPP TS 22.011: "Service accessibility".

[7] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[8] 3GPP TS 22.024: "Description of Charge Advice Information (CAI)".

[9] 3GPP TS 23.086: "Advice of Charge (AoC) Supplementary Service – Stage 2".

[10] 3GPP TS 24.086: "Advice of Charge (AoC) Supplementary Service – Stage 3".

[11] 3GPP TS 22.101: "Service aspects; Service principles".

[12] 3GPP TS 22.030: "Man-Machine Interface (MMI) of the User Equipment (UE)".

[13] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[14] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[15] 3GPP TS 44.018: "Mobile radio interface layer 3 specification; Radio Resource Control Protocol".

[16] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core Network protocols; Stage 3".

[17] 3GPP TS 24.080: "Mobile radio Layer 3 supplementary service specification; Formats and coding".

[18] 3GPP TS 22.086: "Advice of Charge (AoC) supplementary services; Stage 1".

[19] 3GPP TS 21.111: "USIM and IC card requirements".

[20] 3GPP TS 25.331 "Radio Resource Control (RRC); Protocol Specification".

[21] 3GPP TS 34.108 "Common test environments for User Equipment (UE) conformance testing".

[22] 3GPP TS 51.010‑1 "Mobile Station (MS) conformance specification; Part1: Conformance specification".

[23] 3GPP TS 23.140 Release 6 "Multimedia Messaging Service (MMS); Functional description; Stage 2".

[24] 3GPP TS 24.002 "GSM – UMTS Public Land Mobile Network (PLMN) Access Reference Configuration".

[25] 3GPP TS 23.060 "General Packet Radio Service (GPRS); Service description; Stage 2".

[26] 3GPP TS 24.301: "Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet Systems (EPS): Stage 3".

[27] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[28] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA) Radio Resource Control (RRC); Protocol specification".

[29] 3GPP TS 36.508: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Packet Core (EPC); Common test environments for User Equipment (UE) conformance testing"

[30] 3GPP TS 36.523-2 " Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Packet Core (EPC);User Equipment (UE) conformance specification Part 2: Implementation Conformance Statement (ICS) proforma specification"

[31] 3GPP TS 23.122: "Non-Access-Stratum functions related to Mobile Station (MS) in idle mode".

[32] 3GPP TS 31.103: "Characteristics of the IP Multimedia Services Identity Module (ISIM) application".

[33] 3GPP TS 34.229-1: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); User Equipment (UE) conformance specification; Part 1: Protocol conformance specification".

[34] 3GPP TS 22.220: "Universal Mobile Telecommunications System (UMTS); Service requirements for Home Node B (HNB) and Home eNode B (HeNB)".

[35] 3GPP TS 36.304: "Evolved Universal Terrestrial Radio Access (E-UTRA) User Equipment (UE); Procedures in idle mode ".

[36] 3GPP TS 24.368: "Non-Access Stratum (NAS) configuration Management Object (MO)"

[37] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[38] 3GPP 34.123-1: "User Equipment (UE) conformance specification; Part 1: Protocol conformance specification".

[39] 3GPP TS 31.101: " UICC-terminal interface; Physical and logical characteristics".

[40] 3GPP TS 38.508-1: "5GS; User Equipment (UE) conformance specification; Part 1: Common test environment".

[41] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[42] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[43] 3GPP TS 22.261: "Service requirements for the 5G system".

[44] 3GPP TS 38.331: "NR Radio Resource Control (RRC) protocol specification".

[45] 3GPP TS 33.102: "3G security; Security architecture".

[46] RFC 5480; "Elliptic Curve Cryptography Subject Public Key Information".

[47] RFC 4187; "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".

[48] Void

[49] 3GPP TS 23.501: "System architecture for the 5G System (5GS)".

[50] 3GPP TS 24.526: "User Equipment (UE) policies for 5G System (5GS)".

[51] 3GPP TS 23.501: "System architecture for the 5G System (5GS)".

[52] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS)".

[53] ISO/IEC 9646-7: "Information technology -- Open Systems Interconnection – Conformance testing methodology and framework -- Part 7: Implementation Conformance Statements".3 Definitions, symbols, abbreviations and coding

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

[yy] 3GPP TS 23.316: “Wireless and wireline convergence access support for the 5G System (5GS)”

\*\*\*\*\* Next change \*\*\*\*\*

## 3.7 Table of optional features

Support of several features is optional or release dependent for the terminal equipment. However, if an ME states conformance with a specific 3GPP release, it is mandatory for the ME to support all mandatory functions of that release, as stated in table A.1 with the exception of the functions:

- "Support of ACL"; and

- "Support of local phonebook";

The supplier of the implementation shall state the support of possible options in table A.1.

Table A.1: Options

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Option | Status | Support | Mnemonic |
| 1 | Support of CS | O |  | O\_CS |
| 2 | Support of a feature requiring PIN2 entry (such as e.g. AoC or FDN) | O |  | O\_PIN2\_ENTRY\_FEAT |
| 3 | Support of UTRAN access | C001 |  | O\_UTRAN |
| 4 | Support of GERAN access | C002 |  | O\_GERAN |
| 5 | Support of Fixed Dialling Numbers | O |  | O\_FDN |
| 6 | Support of Advice of Charge Charging | O |  | O\_AoCC |
| 7 | Support of Higher priority PLMN selector with Access Technology service (Implementation is optional in Rel-6 and onwards) | C003 |  | O\_HPLMNwACT |
| 8 | Support of local phonebook | O  NOTE 1 |  | O\_Local\_PB |
| 9 | Support of global phonebook | C004 |  | O\_Global\_PB |
| 10 | Support of storing received Class 2 Short Messages in the USIM | O |  | O\_Store\_Received\_SMS |
| 11 | Support of MMS | O |  | O\_MMS |
| 12 | Support of usage of MMS related data stored on the USIM | C005 |  | O\_MMS\_USIM\_DATA |
| 13 | Supported of unselected user MMS connectivity parameters | O |  | O\_NO\_USER\_MMS\_CONF\_SELEC |
| 14 | Support of MMS notification storage on the USIM | O |  | O\_MMS\_NOTIF\_STORAGE |
| 15 | Support of ACL | O  NOTE 2 |  | O\_ACL |
| 16 | Support of SDN | O |  | O\_SDN |
| 17 | Support of numerical entry of PLMN codes in EF PLMNwACT | O |  | O\_EFPLMNwACT\_numerical entry |
| 18 | Terminal does support speech call | O |  | O\_Speech\_Calls |
| 19 | Terminal support PIN MMI strings | O |  | O\_PIN\_MMI\_Strings |
| 20 | Terminal does support eFDD | O |  | pc\_eFDD |
| 21 | Terminal does support eTDD | O |  | pc\_eTDD |
| 22 | Terminal does support CSG list handling (for E-UTRA) | O |  | pc\_Allowed\_CSG\_list |
| 23 | Terminal supports SM-over-IP-receiver | O |  | pc\_SM-over-IP receiver |
| 24 | Terminal supports reading SMS' stored in EF SMS on the USIM if USIM and ISIM are present | O |  | pc\_USIM\_EF\_SMS\_reading\_support\_if\_USIM\_ISIM both present |
| 25 | Terminal supports reading SMS' stored in EF SMS on the ISIM if USIM and ISIM are present | O |  | pc\_ISIM\_EF\_SMS\_reading\_support\_if\_USIM\_ISIM both present |
| 26 | Terminal can store more than 1000 text messages | O |  | O\_LARGE\_SMS\_STORAGE |
| 27 | Support for multiple PDN  connections | O |  | pc\_Multiple\_PDN |
| 28 | Terminal does support CSG (for UTRA) | O |  | pc\_CSG |
| 29 | Support of manual CSG selection | O |  | pc\_manual\_CSG\_selection |
| 30 | Support of PS | O |  | O\_PS |
| 31 | Terminal does support display | O |  | O\_Display |
| 32 | Terminal does support keypad | O |  | O\_Keypad |
| 33 | Terminal supports E-UTRA Disabling Allowed for EMM cause #15 | O |  | O\_EUTRA\_Disabling\_EMM\_cause#15 |
| 34 | Terminal supports Override NAS signalling low priority | O |  | O\_Override\_NAS\_signalling\_low\_priority |
| 35 | Terminal supports T3245 timer | O |  | O\_T3245 |
| 36 | Terminal supports Override Extended access barring | O |  | O\_Override\_EAB |
| 37 | Terminal does support NB-IoT | O |  | pc\_NB |
| 38 | MS maintains a list of PLMN-specific attempt counters | O |  | O\_PLMN\_specific\_attempt\_counters |
| 39 | Terminal does support deactivation of the UICC in PSM. | O |  | O\_PSM\_DEAC\_UICC |
| 40 | Terminal does support deactivation of the UICC during extended DRX | O |  | O\_eDRX\_DEAC\_UICC |
| 41 | Terminal does support the UICC suspension mechanism in PSM. | O |  | O\_PSM\_ SUSPEND\_UICC |
| 42 | Terminal does support the UICC suspension mechanism during extended DRX | O |  | O\_eDRX\_ SUSPEND\_UICC |
| 43 | UE supports 5G Core Network | O |  | pc\_5GC |
| 44 | Support of NR access | O |  | pc\_NR |
| 45 | Support of URSP by USIM | O |  | O\_URSP\_by\_USIM |
| xx | Terminal supports SUPI as Network Access Identifier (NSI, GLI or GCI) | O |  | O\_SUPI\_NAI |
| yy | Terminal supports GCI for 5G-CRG or FN-CRG | O |  | O\_GCI |
| C001 If terminal is 3G terminal then M else N/A  C002 If terminal is 2G terminal then M else O  C003 If Higher priority PLMN selector with Access Technology service is implemented according to Rel-6 or later then O else M  C004 If (A.1/18 is supported) AND (A.1/31 is supported) AND (A.1/32 is supported) AND (terminal is implemented according to Rel-6 or later) then M, else O  C005 If ((A.1/11 is NOT supported) OR (terminal is implemented according to R99)) then N/A else if terminal is implemented according to Rel-4 then O else M  C006 void  NOTE 1: The support of this feature was made optional by CR#0214. See conditions in TS 31.102 [4]  NOTE 2: The support of this feature was made optional by CR#0200. | | | | |

## 3.8 Applicability table

Table B.1: Applicability of tests

| Item | Description | Tested feature defined in Release | Test sequence(s) | R99 ME | Rel-4 ME | Rel-5 ME | Rel-6 ME | Rel-7 ME | Rel-8 ME | Rel-9 ME | Rel-10 ME | Rel-11 ME | Rel-12 ME | Rel-13 ME | Rel-14-ME | Rel-15 ME | Rel-16 ME | Network Dependency | Support | Additional test case execution recommendation |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | UE identification by short IMSI | R99 | 5.1.1 | M | M | M | M | M | C049 | C049 | C049 | C049 | C049 | C049 | C049 | C049 | C049 | UMTS System Simulator or System Simulator only |  | AER005 |
| 2 | UE identification by short IMSI using 2 digit MNC | R99 | 5.1.2 | M | M | M | M | M | C049 | C049 | C049 | C049 | C049 | C049 | C049 | C049 | C049 | UMTS System Simulator or System Simulator only |  | AER005 |
|  | … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 170 | Support for URSP by USIM | Rel-16 | 16.1.1 | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | C058 | NG-SS |  |  |
| 171 | Support for URSP by ME | Rel-16 | 16.1.2 | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | C058 | NG-SS |  |  |
| 172 | Support of signalled URSP | Rel-16 | 16.1.3 | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | C058 | NG-SS |  |  |
| xxx | SUCI calculation by ME using null scheme - SUPI Type NAI | Rel-16 | 5.3.x | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | Cxxx | NG-SS |  |  |

Table B.1: Applicability of tests (continued)

|  |  |  |
| --- | --- | --- |
| C001 | (NOT A.1/3) AND A.1/4 | -- (NOT O\_UTRAN) AND O\_GERAN |
| C002 | A.1/1 AND A.1/3 | -- O\_CS AND O\_UTRAN |
| … |  |  |
| C057 | IF A.1/43 AND A.1/44 AND A.1/31 THEN M ELSE N/A | -- pc\_5GC AND pc\_NR AND O\_Display |
| C058 | IF A.1/43 AND A.1/44 AND A.1/45 THEN M ELSE N/A | -- pc\_5GC AND pc\_NR AND O\_URSP\_by\_USIM |
| Cxxx | IF A.1/43 AND A.1/44 AND A.1/xx AND A.1/yy THEN M ELSE N/A | -- pc\_5GC AND pc\_NR AND O\_SUPI\_NAI AND O\_GCI |
| O.1 | IF C002 THEN "Expected Sequence A" M ELSE IF C001 THEN "Expected Sequence B" M |  |
| AER001 | IF (A.1/20 OR A.1/21) AND ((A.1/3 OR A.1/4) AND (NOT A.1/18) THEN R ELSE A | -- (pc\_eFDD OR pc\_eTDD) AND (O\_UTRAN OR O\_GERAN) AND (NOT O\_Speech\_Calls) |
| AER002 | IF (A.1/20 OR A.1/21) AND (A.1/3 OR A.1/4) THEN R ELSE A | -- (pc\_eFDD OR pc\_eTDD) AND (O\_UTRAN OR O\_GERAN) |
| AER003 | IF (test 8.2.3 has been PASSED) THEN R ELSE A |  |
| AER004 | IF (test 8.2.5 has been PASSED) THEN R ELSE A |  |
| AER005 | IF (NOT A.1/3) AND A.1/4 AND (NOT A.1/1) THEN R ELSE A | -- (NOT O\_UTRAN) AND ((O\_GERAN AND (NOT O\_CS)) |
| AER006 | If A.1/38 is supported set the implementation specific counter to small value to reduce the test execution time. |  |
| AER007 | If A.1/39 is supported, in addition to the test case initial conditions, any specific information or particular UE configurations required to ensure that the UE performs UICC deactivation in PSM shall be provided by the UE manufacturer. |  |
| AER008 | If A.1/40 is supported, in addition to the test case initial conditions, any specific information or particular UE configurations required to ensure that the UE performs UICC deactivation in eDRX shall be provided by the UE manufacturer |  |
| AER009 | The value of timers T3324 (T3324\_V) and T3412 (T3412\_V) shall be provided by the UE manufacturer and shall be set to a value suitable for executing the test cases. |  |
| AER010 | The value of eDRX (eDRX\_V) and PTW (PTW\_V) parameters shall be provided by the UE manufacturer and shall be set to a value suitable for executing the test cases. |  |
| NOTE 1: Definition of applicability for this test case is FFS.  NOTE 2: For Rel‑13, if the UE supports NB-IoT, this test case shall be verified by accessing the NB System Simulator (NB-SS). | | |

\*\*\*\*\* Next change \*\*\*\*\*

## 4.1 Definition of default values for USIM-Terminal interface testing (Default UICC)

A USIM containing the following default values is used for all tests of this present document unless otherwise stated.

USIM AID value shall follows the PIX coding for '3GPP USIM' from ETSI TS 101 220 [xx] annex E.

The service "Non-Access Stratum configuration by USIM" shall not be available unless otherwise specified.

For each data item, the logical default values and the coding within the elementary files (EF) of the USIM follow.

NOTE 1: Bx represents byte x of the coding.

NOTE 2: Unless otherwise defined, the coding values are hexadecimal.

\*\*\*\*\* Next change \*\*\*\*\*

## 4.x Definition of 5G-NR UICC – non-IMSI SUPI Type

The 5G-NR test cases require a different configuration than the one described in clause 4.1. For that purpose, a default 5G-NR UICC is defined. In general, the values of the 5G-NR UICC are identical to the default UICC, with the following exceptions:

USIM AID value shall follows the PIX coding for '3GPP USIM (non-IMSI SUPI Type)' from ETSI TS 101 220 [xx] annex E.

### 4.x.1 EFUST (USIM Service Table)

Settings from clause 4.9 (Default 5G-NR UICC) of the present document apply with the following changes:

Logically:

|  |  |  |
| --- | --- | --- |
| Service n°130 | Support for SUPI of type NSI or GLI or GCI | available |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Coding:** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** |
| Binary: | xxxx xx1x | xxxx xxxx | xxxx 1x00 | xxxx x1xx | xxxx xx11 | xxxx xxxx | xxxx xxxx | xxxx xxxx |
|  | **B9** | **B10** | **B11** |  | **B16** | **B17** |  |  |
|  | xxxx xxxx | xxxx xxxx | xx11 xxxx | ..... | xxx0 111x | xxxx xx1x |  |  |

### 4.x.2 EFIMSI (IMSI)

This file shall not be available.

### 4.x.3 EFSUPI\_NAI (SUPI as Network Access Identifier)

This file shall be available.

Logically: 00-00-5E-00-53-00@5gc.mnc012.mcc345.3gppnetwork.org

Username: 00-00-5E-00-53-00

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Realm: 5gc.mnc012.mcc345.3gppnetwork.org**Coding:** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** |
| Hex | 30 | 30 | 2D | 30 | 30 | 2D | 35 | 45 |
| **B9** | **B10** | **B11** | **B12** | **B13** | **B14** | **B15** | **B16** |
| 2D | 30 | 30 | 2D | 35 | 33 | 2D | 30 |
| **B17** | **B18** | **B19** | **B20** | **B21** | **B22** | **B23** | **B24** |
| 30 | 40 | 35 | 67 | 63 | 2E | 6D | 6E |
| **B25** | **B26** | **B27** | **B28** | **B29** | **B30** | **B31** | **B32** |
| 63 | 30 | 31 | 32 | 2E | 6D | 63 | 63 |
| **B33** | **B34** | **B35** | **B36** | **B37** | **B38** | **B39** | **B40** |
| 33 | 34 | 35 | 2E | 33 | 67 | 70 | 70 |
| **B41** | **B42** | **B43** | **B44** | **B45** | **B46** | **B47** | **B48** |
| 6E | 65 | 74 | 77 | 6F | 72 | 6B | 2E |
| **B49** | **B50** | **B51** | **B52** | **B53** | **B54** | **B55** | **B56** |
| 6F | 72 | 67 |  |  |  |  |  |

### 4.x.4 EF5GS3GPPLOCI (5GS 3GPP location information)

Settings from clause 4.9.3 of the present document apply.

### 4.x.5 EFSUCI\_Calc\_Info (Subscription Concealed Identifier Calculation Information EF)

Logically:

Protection Scheme Identifier List data object

Protection Scheme Identifier 1 – ECIES scheme profile B

Key Index 1: 1

Protection Scheme Identifier 2 – ECIES scheme profile A

Key Index 2: 2

Protection Scheme Identifier 3 – null-scheme

Key Index 3: 0

Home Network Public Key List data object

Home Network Public Key 1 Identifier: 27

Home Network Public Key 1:

- 04 72 DA 71 97 62 34 CE 83 3A 69 07 42 58 67 B8 2E 07 4D 44 EF 90 7D FB 4B 3E 21 C1 C2 25 6E BC D1 5A 7D ED 52 FC BB 09 7A 4E D2 50 E0 36 C7 B9 C8 C7 00 4C 4E ED C4 F0 68 CD 7B F8 D3 F9 00 E3 B4

Home Network Public Key 2 Identifier: 30

Home Network Public Key 2:

- 5A 8D 38 86 48 20 19 7C 33 94 B9 26 13 B2 0B 91 63 3C BD 89 71 19 27 3B F8 E4 A6 F4 EE C0 A6 50

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Coding:** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** |
| Hex | A0 | 06 | 02 | 01 | 01 | 02 | 00 | 00 |
|  | **B9** | **B10** | **B11** | **B12** | **B13** | **B14** | **B15** | **B16** |
| A1 | 6B | 80 | 01 | 1B | 81 | 41 | 04 |
| **B17** | **B18** | **B19** | **B20** | **B21** | **B22** | **B23** | **B24** |
| 72 | DA | 71 | 97 | 62 | 34 | CE | 83 |
| **B25** | **B26** | **B27** | **B28** | **B29** | **B30** | **B31** | **B32** |
| 3A | 69 | 07 | 42 | 58 | 67 | B8 | 2E |
| **B33** | **B34** | **B35** | **B36** | **B37** | **B38** | **B39** | **B40** |
| 07 | 4D | 44 | EF | 90 | 7D | FB | 4B |
| **B41** | **B42** | **B43** | **B44** | **B45** | **B46** | **B47** | **B48** |
| 3E | 21 | C1 | C2 | 25 | 6E | BC | D1 |
| **B49** | **B50** | **B51** | **B52** | **B53** | **B54** | **B55** | **B56** |
| 5A | 7D | ED | 52 | FC | BB | 09 | 7A |
| **B57** | **B58** | **B59** | **B60** | **B61** | **B62** | **B63** | **B64** |
| 4E | D2 | 50 | E0 | 36 | C7 | B9 | C8 |
| **B65** | **B66** | **B67** | **B68** | **B69** | **B70** | **B71** | **B72** |
| C7 | 00 | 4C | 4E | ED | C4 | F0 | 68 |
| **B73** | **B74** | **B75** | **B76** | **B77** | **B78** | **B79** | **B80** |
| CD | 7B | F8 | D3 | F9 | 00 | E3 | B4 |
| **B81** | **B82** | **B83** | **B84** | **B85** | **B86** | **B87** | **B88** |
| 80 | 01 | 1E | 81 | 20 | 5A | 8D | 38 |
| **B89** | **B90** | **B91** | **B92** | **B93** | **B94** | **B95** | **B96** |
| 86 | 48 | 20 | 19 | 7C | 33 | 94 | B9 |
| **B97** | **B98** | **B99** | **B100** | **B101** | **B102** | **B103** | **B104** |
| 26 | 13 | B2 | 0B | 91 | 63 | 3C | BD |
| **B105** | **B106** | **B107** | **B108** | **B109** | **B110** | **B111** | **B112** |
| 89 | 71 | 19 | 27 | 3B | F8 | E4 | A6 |
| **B113** | **B114** | **B115** | **B116** | **B117** |
| F4 | EE | C0 | A6 | 50 |

### 4.x.6 EFRouting\_Indicator (Routing Indicator EF)

Settings from clause 4.9.5 of the present document apply.

\*\*\*\*\* Next change \*\*\*\*\*

## 5.3 Handling subscription identifier privacy for 5G - SUPI type IMSI

…

\*\*\*\*\* Next change \*\*\*\*\*

## 5.x Handling subscription identifier privacy for 5G - SUPI type NAI

### 5.x.1 SUCI calculation by ME using null scheme

#### 5.x.1.1 Definition and applicability

If the operator's decision is that ME shall calculate the SUCI, the home network operator shall provision a list of the Protection Scheme Identifiers in the USIM that the operator allows. The list of Protection Scheme Identifiers in the USIM may contain one or more Protection Scheme Identifiers in the order of their priority. The ME shall read the SUCI calculation information from the USIM, including the SUPI, the Home Network Public Key, the Home Network Public Key Identifier, and the list of Protection Scheme Identifiers. The ME shall select the protection scheme from its supported schemes that has the highest priority in the list obtained from the USIM.

The ME shall calculate the SUCI using the null-scheme if the highest priority of the protection schemes listed in the USIM is the null-scheme.

#### 5.x.1.2 Conformance requirement

1) SUCI calculation procedure shall be performed by the ME if Service n°124 is "available" and Service n°125 is not "available" in EFUST

2) SUPI is available in EFSUPI\_NAI if Service n°130 is "available" in EFUST

3) A subscriber identifier is in the form of a SUPI in NAI format

4) The SUPI may contain:

- a network-specific identifier, used for private networks as defined in TS 22.261 [43] or

- a GLI and an operator identifier of the 5GC operator, used for supporting FN-BRGs, as further described in TS 23.316 [yy] or

- a GCI and an operator identifier of the 5GC operator, used for supporting FN-CRGs and 5G-CRG, as further described in TS 23.316 [yy].

5) As part of the SUCI calculation performed by the ME, the ME performs the reading procedure for EFSUCI\_Calc\_Info.

6) The ME shall calculate the SUCI using the null-scheme if highest priority of the protection schemes listed in the USIM is the null-scheme.

Reference:

- TS 31.102 [4], clauses 4.4.11.8, 4.4.11.10, 4.4.11.11, 5.2.33, 5.3.47 and 5.3.51;

- TS 33.501 [41], clause Annex C;

- TS 23.003 [19], clause 28.2, 28.7.2.

- TS 24.501 [42], clause 5.5.1.2, 5.5.1.2.4.

#### 5.x.1.3 Test purpose

1) To verify that the READ EFSUCI\_Calc\_Info, EFRouting\_Indicator and EFSUPI\_NAI commands are performed correctly by the ME.

2) To verify that the ME performs the SUCI calculation procedure using null-scheme.

#### 5.x.1.4 Method of test

##### 5.x.1.4.1 Initial conditions

The NG-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001.

- Access control: unrestricted.

The default 5G-NR UICC non-IMSI SUPI Type is used with the following exception:

**EFSUCI\_Calc\_Info (Subscription Concealed Identifier Calculation Information EF)**

Logically:

Protection Scheme Identifier List data object

Protection Scheme Identifier 1 – null-scheme

Key Index 1: 0

Protection Scheme Identifier 2 – ECIES scheme profile B

Key Index 2: 1

Protection Scheme Identifier 3 – ECIES scheme profile A

Key Index 3: 2

Home Network Public Key List data object

Home Network Public Key 1 Identifier: 27

Home Network Public Key 1:

- 04 72 DA 71 97 62 34 CE 83 3A 69 07 42 58 67 B8 2E 07 4D 44 EF 90 7D FB 4B 3E 21 C1 C2 25 6E BC D1 5A 7D ED 52 FC BB 09 7A 4E D2 50 E0 36 C7 B9 C8 C7 00 4C 4E ED C4 F0 68 CD 7B F8 D3 F9 00 E3 B4

Home Network Public Key 2 Identifier: 30

Home Network Public Key 2:

- 5A 8D 38 86 48 20 19 7C 33 94 B9 26 13 B2 0B 91 63 3C BD 89 71 19 27 3B F8 E4 A6 F4 EE C0 A6 50

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Coding:** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** |
| Hex | A0 | 06 | 00 | 00 | 02 | 01 | 01 | 02 |
|  | **B9** | **B10** | **B11** | **B12** | **B13** | **B14** | **B15** | **B16** |
| A1 | 6B | 80 | 01 | 1B | 81 | 41 | 04 |
| **B17** | **B18** | **B19** | **B20** | **B21** | **B22** | **B23** | **B24** |
| 72 | DA | 71 | 97 | 62 | 34 | CE | 83 |
| **B25** | **B26** | **B27** | **B28** | **B29** | **B30** | **B31** | **B32** |
| 3A | 69 | 07 | 42 | 58 | 67 | B8 | 2E |
| **B33** | **B34** | **B35** | **B36** | **B37** | **B38** | **B39** | **B40** |
| 07 | 4D | 44 | EF | 90 | 7D | FB | 4B |
| **B41** | **B42** | **B43** | **B44** | **B45** | **B46** | **B47** | **B48** |
| 3E | 21 | C1 | C2 | 25 | 6E | BC | D1 |
| **B49** | **B50** | **B51** | **B52** | **B53** | **B54** | **B55** | **B56** |
| 5A | 7D | ED | 52 | FC | BB | 09 | 7A |
| **B57** | **B58** | **B59** | **B60** | **B61** | **B62** | **B63** | **B64** |
| 4E | D2 | 50 | E0 | 36 | C7 | B9 | C8 |
| **B65** | **B66** | **B67** | **B68** | **B69** | **B70** | **B71** | **B72** |
| C7 | 00 | 4C | 4E | ED | C4 | F0 | 68 |
| **B73** | **B74** | **B75** | **B76** | **B77** | **B78** | **B79** | **B80** |
| CD | 7B | F8 | D3 | F9 | 00 | E3 | B4 |
| **B81** | **B82** | **B83** | **B84** | **B85** | **B86** | **B87** | **B88** |
| 80 | 01 | 1E | 81 | 20 | 5A | 8D | 38 |
| **B89** | **B90** | **B91** | **B92** | **B93** | **B94** | **B95** | **B96** |
| 86 | 48 | 20 | 19 | 7C | 33 | 94 | B9 |
| **B97** | **B98** | **B99** | **B100** | **B101** | **B102** | **B103** | **B104** |
| 26 | 13 | B2 | 0B | 91 | 63 | 3C | BD |
| **B105** | **B106** | **B107** | **B108** | **B109** | **B110** | **B111** | **B112** |
| 89 | 71 | 19 | 27 | 3B | F8 | E4 | A6 |
| **B113** | **B114** | **B115** | **B116** | **B117** |
| F4 | EE | C0 | A6 | 50 |

The UICC is installed into the ME.

##### 5.x.1.4.2 Procedure

a) The UE is switched on.

b) The UE sends REGISTRATION REQUEST to the NG-SS indicating the 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "SUCI".

1. Upon reception of REGISTRATION ACCEPT message with a 5G-GUTI, the UE sends REGISTRATION COMPLETE message to the NG-SS.

#### 5.x.1.5 Acceptance criteria

1) After step a) the ME shall readEFSUPI\_NAI, EFRouting\_Indicator and EFSUCI\_Calc\_Info.

2) In step b) the UE shall include the SUCI as coded below in the 5GS mobile identity IE in the REGISTRATION REQUEST.

SUPI format: 1

Routing indicator: 17

Protection scheme id: 00

Home network public key Id: 0

Scheme output: 00-00-5E-00-53-00@5gc.mnc012.mcc345.3gppnetwork.org

\*\*\*\*\* End of changes \*\*\*\*\*