**3GPP TSG-SA3 Meeting #123 Draft S3-253030-r1**

Goteborg, Sweden, 25 – 29 August 2025

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.514** | **CR** | **Draft CR** | **rev** | **-** | **Current version:** | **19.1.0** |  |
|  |
| *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 |  | ME |  | Radio Access Network |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Corrections to 33.514 based on GSMA NESASG agreements |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon, CAICT |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** | 2025-08-18 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-20 |
|  | *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 canbe 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:*** | According to GSMA NESASG agreements, several corrections to 33.514 are needed. Besides, the execution steps in 4.2.2.1 are not written in the view of tester like that in 4.2.2.2, making it hard for testers to conduct. |
|  |  |
| ***Summary of change:*** | 1. Correcting wrong font styles.
2. Complementing the missing referenced document in the main text.
3. Rephrasing execution steps in 4.2.2.1 in the view of tester.
 |
|  |  |
| ***Consequences if not approved:*** | Low quality of SCAS documents. Hard for testers to conduct. |
|  |  |
| ***Clauses affected:*** | 4.2.1.1, 4.2.1.2, 4.2.1.3, 4.2.2.1, 4.2.2.2 |
|  |  |
|  | **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:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of CHANGES\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 4.2.1.1 De-concealment of SUPI from the SUCI based on the protection scheme used to generate the SUCI

*Requirement Name:* De-concealment of SUPI from the SUCI based on the protection scheme used to generate the SUCI.

*Requirement Reference:* TS 33.501 [2], clause 5.8.2.

*Requirement Description:* The SIDF resolves the SUPI from the SUCI based on the protection scheme used to generate the SUCI as specified in TS 33.501 [2], clause 5.8.2.

*Threat References*: TR 33.926 [4], clause E.2.2.1, Incorrect SUCI de-concealment.

*Test Case:*

**Test Name:** TC\_DE-CONCEAL\_SUPI\_from\_SUCI\_UDM

**Purpose:**

Verify that the SIDF De-conceals the SUPI from the SUCI based on the protection scheme used to generate the SUCI.

**Procedure and execution steps:**

**Pre-Condition:**

- UDM network product is connected in simulated/real network environment including an AUSF and AMF.

- Tester shall have access to the subscription data stored in UDR.

- Tester shall record the SUPI from the UE.

**Execution Steps:**

Tester shall capture the entire authentication procedure between UE and AMF over N1, N12 and N13 interface using any network analyser.

1. Tester shall filter the Nudm\_UEAuthentication\_Get Response message sent from UDM to AUSF over N13 interface containing the SUPI.

2. Tester shall compare the SUPI gotten from UE and the SUPI retrieved from Nudm\_UEAuthentication\_Get Response message.

NOTE: The tester may filter the Nausf\_UEAutentication\_Authenticate Response message sent from the UDM/AUSF to the AMF over N12 interface containing the SUPI, if the UDM and AUSF network products are collocated without an open N13 interface.

**Expected Results:**

SIDF resolves the SUPI from the SUCI based on the protection scheme used to generate the SUCI.

**Expected format of evidence:**

Evidence suitable for the interface, e.g., evidence can be presented in the form of screenshot/screen-capture.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of 1st CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 2nd CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 4.2.1.2 Rejection of SUCIs using an ECIES protection scheme with an invalid public key.

*Requirement Name:* Rejection of SUCIs using an ECIES protection scheme with an invalid public key.

*Requirement Reference:* TS 33.501 [2], clause C.3.3 with reference to SECG SEC 1 [8] clause 2.3.4.

*Requirement Description:* Output: An elliptic curve point P, or "invalid" as specified in SECG SEC 1 [8], clause 2.3.4.

*Threat References*: TR 33.926 [4], clause E.2.2.6, Invalid public key.

*Test Case:*

**Test Name**: TC\_REJECT\_SUCI\_PROFILE\_B\_INVALID\_PUBKEY\_UDM

**Purpose:**

Verify that the SIDF rejects the SUCI if it uses an ECIES protection scheme and contains an invalid point as the UE’s public key for Profile B.

**Procedure and execution steps:**

**Pre-Condition:**

- The tester has access to the public information of the SUCI profile (e.g., profile type, public key …) of the UDM/SIDF under test.

- The tester has configured the UDM to use Profile B.

- The tester has access to a SUPI of provisioned subscriber.

**Execution Steps**

1. The tester selects an invalid point (NOTE 1) and uses the point as a public key to encrypt the SUPI based on the encryption defined in Annex C of 33.501 [2] and SECG SEC 1 [8] (NOTE 2).

2. The tester sends the SUCI to the Nudm\_UEAuthentication\_Get service of the UDM/ SIDF under test.

NOTE 1: An example invalid point for Profile B (of order 47) is: 0x049af0190d4e237c462c94c447052c770f6d348866f1dbbe29a0ee889f18835d6a973457a6730323716ef2c8a3723793be64b54cec40eb86ab194057c95baf8cfe.

NOTE 2: An example SUCI encrypted with the invalid point (above) for the MCC|MNC (274012) and MSIN (001002086) for Profile B (Annex C of 33.501 [2]) is: suci-0-274-012-0-2-2-049af0190d4e237c462c94c447052c770f6d348866f1dbbe29a0ee889f18835d6a973457a6730323716ef2c8a3723793be64b54cec40eb86ab194057c95baf8cfe8cf9a0959454b74e31a331018b.

**Expected Results:**

The UDM/SIDF rejects the SUCI, and the UDM sends a Nudm\_UEAuthentication\_Get Response message with an HTTP status code "403 Forbidden" and may include additional error information in the response body (in "ProblemDetails" element) as specified in TS 29.503 [9], clause 5.4.2.2.2, 2b.

NOTE 3: Values for "ProblemDetails" may be AUTHENTICATION\_REJECTED or INVALID\_SCHEME\_OUTPUT as specified in TS 29.503 [9], clause 6.3.3.2.4.2.2-2.

**Expected format of evidence:**

Evidence suitable for the interface, e.g., evidence can be presented in the form of packet trace (e.g., pcap file).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of 2nd CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 3rd CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 4.2.1.3 Rejection of SUCIs using an uncompressed point with Profile B.

*Requirement Name:* Rejection of SUCIs using an uncompressed point with Profile B.

*Requirement Reference:* TS 33.501 [2], clause C.3.4.0.

*Requirement Description:* Profile B shall use point compression to save overhead as specified in TS 33.501 [2], clause C.3.4.0.

*Threat References*: TR 33.926 [4], clause E.2.2.6, Invalid public key.

*Test Case:*

**Test Name:** TC\_REJECT\_SUCI\_PROFILE\_B\_NO\_COMPRESSION\_UDM

**Purpose:**

Verify that the SIDF rejects the SUCI if it uses the ECIES Profile B protection scheme and contains an uncompressed point as the UE's public key.

**Procedure and execution steps:**

**Pre-Condition:**

Tester shall have access to the HN’s public key for SUCI decryption with Profile B.

**Execution Steps**

1. The tester shall generate a SUCI for a registered SUPI with the protection scheme output for Profile B. The ephemeral public key of the UE should be in the uncompressed point format specified in SECG SEC 1 [8] clause 2.3.3. The remaining parts of the protection scheme output retain their format specified in SECG SEC 1 [8].

NOTE 1: The uncompressed point format shall have a size of 65 bytes, and the most significant byte shall be 0x04. The compressed point format shall have a size of 33 bytes, with 0x02 or 0x03 as the most significant byte. Test data in TS 33.501 [2], clause C.4.4.1.

2. The tester shall send the SUCI to the Nudm\_UEAuthentication\_Get service of the UDM/ SIDF under test.

**Expected Results:**

The SIDF rejects the SUCI, and the UDM sends a Nudm\_UEAuthentication\_Get Response message with an HTTP status code "403 Forbidden" and may include additional error information in the response body (in "ProblemDetails" element) as specified in TS 29.503 [9], clause 5.4.2.2.2, 2b.

NOTE 2: Values for "ProblemDetails" may be AUTHENTICATION\_REJECTED or INVALID\_SCHEME\_OUTPUT as specified in TS 29.503 [9], clause 6.3.3.2.4.2.2-2.

**Expected format of evidence:**

Evidence suitable for the interface, e.g., evidence can be presented in the form of packet trace (e.g., pcap file).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of 3rd CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 4th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 4.2.2.1 Synchronization failure handling

*Requirement Name*: Synchronization failure handling

*Requirement Reference:* TS 33.501 [2], clause 6.1.3.3.2.

*Requirement Description*: When the UDM/ARPF receives an Nudm\_UEAuthentication\_Get Request message with a "synchronisation failure indication" it acts as described in TS 33.102 [7], clause 6.3.5 where ARPF is mapped to HE/AuC. The UDM/ARPF sends an Nudm\_UEAuthentication\_Get Response message with a new authentication vector for either EAP-AKA' or 5G-AKA depending on the authentication method applicable for the user to the AUSF as specified in TS 33.501 [2], clause 6.1.3.3.2.

*Threat References*: TR 33.926 [4], clause E.2.2.2, Synchronization failure.

*Test Case*:

**Test Name:** TC\_SYNC\_FAILURE\_HANDLING\_UDM

**Purpose:**

Verify that synchronization failure is recovered correctly in the home network.

**Pre-Conditions:**

Test environment with an AUSF. The AUSF or AMF may be simulated.

**Execution Steps:**

1. The tester sends an Nudm\_UEAuthentication\_Get Request message to the UDM under test with a "synchronisation failure indication" and parameters RAND and AUTS.

2. The UDM/ARPF performs steps 1-5 as described in TS 33.102, clause 6.3.5, and sends the Nudm\_UEAuthentication\_Get Response message to the AUSF.

3. The tester checks whether the Nudm\_UEAuthentication\_Get Response message sent from the UDM under test contains a new authentication vector.

**Expected Results:**

The UDM sends an Nudm\_UEAuthentication\_Get Response message with a new authentication vector to the AUSF.

NOTE: The expected results would be that the UDM/AUSF sends an Nausf\_UEAuthentication\_Authenticate Response message with EAP Request/AKA’-Challenge for EAP AKA’, or 5G SE AV for 5G AKA to the AMF, if the UDM and AUSF network products are collocated without an open N13 interface.

**Expected format of evidence:**

Evidence suitable for the interface, e.g., Screenshot, packet capture or application log containing the operational results.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of 4th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 5th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 4.2.2.2 Storing of authentication status of UE by UDM

*Requirement Name:* Storing of authentication status of UE by UDM.

*Requirement Reference:* TS 33.501 [2], clause 6.1.4.1a

*Requirement Description:* The UDM stores the authentication status of the UE (SUPI, authentication result, time stamp, and the serving network name) after authentication as specified in TS 33.501 [2], clause 6.1.4.1a.

*Threat References*: TR 33.926 [4], clause E.2.2.3, Failure to store of authentication status.

*Test Case:*

**Test Name:** TC\_AUTH\_STATUS\_STORE\_UDM

**Purpose:**

Verify that the UDM under test stores the authentication status of UE.

**Procedure and execution steps:**

**Pre-Condition:**

- UDM network product is connected with an AUSF in simulated/real network environment.

- The tester shall have access to the UDM under test.

**Execution Steps:**

1. The tester shall send an Nudm\_UEAuthentication\_Get Request message to the UDM with the UE credentials and a selected serving network name.

2. The tester shall receive a successful Nudm\_UEAuthentication\_Get Response from the UDM.

3. The tester shall simulate the successful authentication by sending the Nudm\_UEAuthentication\_ResultConfirmation Request message with a selected timestamp to the UDM.

4. The tester shall receive a successful Nudm\_UEAuthentication\_ResultConfirmation Response message from the UDM.

5. The tester shall compare the serving network name stored in the UDM against the serving network name retrieved from the Nudm\_UEAuthentication\_Get Request message and the serving network name retrieved from the Nudm\_UEAuthentication\_ResultConfirmation Request message.

6. The tester shall compare the SUPI stored in the UDM (retrieved from the Nudm\_UEAuthentication\_ResultConfirmation Response message) against the SUPI retrieved from the Nudm\_UEAuthentication\_Get Response message.

7. The tester shall compare the timestamp stored in the UDM against the time of authentication procedure retrieved from the Nudm\_UEAuthentication\_ResultConfirmation Request message.

**Expected Results:**

The storing of authentication status (SUPI, timestamp, and the serving network name) of UE at the UDM is verified.

**Expected format of evidence:**

Evidence suitable for the interface, e.g., evidence can be presented in the form of packet capture or screenshot/screen-capture.

NOTE: Void

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of CHANGES\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*