**3GPP TSG-SA3 Meeting #111 *S3-23xxxx***

**Berlin, Germany, 22 - 26 May 2023**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.513** | **CR** | **XXXX** | **rev** | **-** | **Current version:** | **17.1.0** |  |
|  | | | | | | | | |
| *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:*** | SCAS release reference corrections | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5G\_Ph2 | | | | |  | ***Date:*** | | | 2023-05-22 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-18 |
|  | *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:*** | | SA3 has been adding the release numbers explicitly to any of the references pertaining to the network function targeted by the SCAS work, for example reference 2 in TS 33.511. This is because the SCAS work has always been one "release late" since it is challenging to develop the SCAS requirements and tests in parallel to targeted new features within the same release timeline. The references have not been regularly updated and some SCAS specifications include more than one reference to the same specification, for example references 2 and 7 in TS 33.512. This practice is neither future proof nor it is documented anywhere. Furthermore, for SCAS evaluation of network products, this dependency on previous releases in SCAS documents turned out to be not very useful anyway. This issue has been discussed several times in previous SA3 meetings and the proposed resolution is documented in [S3-231050](https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_110_Athens/docs/S3-231050.zip). | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Removal of the release number from the relevant references and minor reformulations to avoid verbatim content copies from other specifications | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Unnecessary dependencies on previous releases and risk for confusion on scope of SCAS specifications | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 4.2.2.1, 4.2.2.2, 4.2.2.3, 4.2.2.4, 4.2.2.5, 4.2.2.6, 4.2.2.7, 4.2.2.8 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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\*\*\*\*

# 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 33.501: "Security architecture and procedures for 5G system".

[3] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

[4] 3GPP TS 23.501: "System Architecture for 5G system".

[5] 3GPP TS 29.281: "General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U) ".

[6] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[7] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[8] void

\*\*\*\* Next Changes\*\*\*\*

#### 4.2.2.1Confidentiality protection of user data transported over N3 interface.

*Requirement Name:* Confidentiality protection of user data transported over N3 interface.

*Requirement Reference: TS 33.501 [2], Clause 9.3*

*Requirement Description:* The transported user data between gNB and UPF is expected to be confidentiality protected as specified in TS 33.501 [2], clause 9.3.

*Threat Reference*: TR 33.926 [7], Clause L.2.2, "No protection or weak protection for user plane data ".

**TEST CASE:**

**Test Name:** TC\_UP\_DATA\_CONF\_UPF

**Purpose:**

Verify that the transported user data between gNB and UPF are confidentiality protected over N3 interface.

**Procedure and execution steps:**

**Pre-Condition:**

- UPF network product is connected in simulated/real network environment.

- The tunnel mode IPsec ESP and IKE certificate authentication is implemented.

- Tester shall have knowledge of the security parameters of tunnel for decrypting the ESP packets.

- Tester shall have access to the N3 interface between gNB and UPF.

- Tester shall have knowledge of the confidentiality algorithm and confidentiality protection keys used for encrypting the encapsulated payload.

**Execution Steps:**

The requirement mentioned in this clause is tested in accordance with the procedure mentioned in clause 4.2.3.2.4 of TS 33.117 [3].

**Expected Results:**

The user data transported between gNB and UPF is confidentiality protected.

**Expected format of evidence:**

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

\*\*\*\* Next Changes\*\*\*\*

#### 4.2.2.2 Integrity protection of user data transported over N3 interface

*Requirement Name:* Integrity protection of user data transported over N3 interface.

*Requirement Reference: TS 33.501 [2], Clause 9.3*

*Requirement Description:* The transported user data between gNB and UPF is expected to be integrity protected as specified in TS 33.501 [2], clause 9.3.

*Threat Reference*: TR 33.926 [7], Clause L.2.2, "No protection or weak protection for user plane data"

**TEST CASE:**

**Test Name:** TC\_UP\_DATA\_INT\_UPF

**Purpose:**

Verify that the transported user data between gNB and UPF are integrity protected over N3 interface.

**Procedure and execution steps:**

**Pre-Condition:**

- UPF network product is connected in simulated/real network environment.

- The tunnel mode IPsec ESP and IKE certificate authentication is implemented.

- Tester shall have knowledge of the security parameters of tunnel for decrypting the Encapsulated Security Payload (ESP) packets.

- Tester shall have knowledge of the authentication algorithm (Hash Message Authentication Code) and the protection keys.

**Execution Steps:**

The requirement mentioned in this clause is tested in accordance to the procedure mentioned in clause 4.2.3.2.4 of TS 33.117 [3].

**Expected Results:**

The user data transported between gNB and UPF is integrity protected.

**Expected format of evidence:**

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

\*\*\*\* Next Changes\*\*\*\*

#### 4.2.2.3 Replay protection of user data transported over N3 interface

*Requirement Name:* Replay protection of user data transported over N3 interface

*Requirement Reference: TS 33.501 [2], Clause 9.3*

*Requirement Description:* The transported user data between gNB and UPF is expected to be replay protected as specified in TS 33.501, clause 9.3.

*Threat Reference*: TR 33.926 [7], Clause L.2.2, "No protection or weak protection for user plane data"

**TEST CASE:**

**Test Name:** TC\_UP\_DATA\_REPLAY\_UPF

**Purpose:**

Verify that the transported user data between gNB and UPF are replay protected.

**Procedure and execution steps:**

**The following procedure is executed if UPF supports IPsec.**

**Pre-Condition:**

- UPF network product is connected in simulated/real network environment.

- The tunnel mode IPsec ESP and IKE certificate authentication is implemented.

- Tester shall have knowledge of the security parameters of tunnel for decrypting the ESP packets.

- Tester shall have access to the original user data transported via N3 reference point between gNB and UPF.

**Execution Steps:**

The requirement mentioned in this clause is tested in accordance with the procedure mentioned in clause 4.2.3.2.4 of TS 33.117 [3].

**Expected Results:**

The user data transported between UE and UPF is replay protected.

**Expected format of evidence:**

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

\*\*\*\* Next Changes\*\*\*\*

#### 4.2.2.4 Protection of user data transported over N9 interface Within a PLMN

*Requirement Name:* Protection of user data transported over N9 within a PLMN.

*Requirement Reference: TS 33.501 [2], Clause 9.9*

*Requirement Description:* As specified in clause 9.9 in TS 33.501 [2], interfaces internal to the 5G Core can be used to transport signalling data as well as privacy sensitive material, such as user and subscription data, or other parameters, such as security keys. Therefore, confidentiality and integrity protection is required.

For the protection of the non-SBA internal interfaces, such as N4 and N9, NDS/IP is expected to be used as specified in TS 33.501 [2], clause 9.9.

*Threat Reference*: TR 33.926 [7], Clause L.2.2, "No protection or weak protection for user plane data "

**TEST CASE:**

**Test Name:** TC\_UP\_DATA\_CONF\_UPF\_N9

**Purpose:**

Verify that the protection mechanism implemented for user data transport over N9 interface in a PLMN conforms to the selected security profile.

**Procedure and execution steps:**

**Pre-Condition:**

- UPF network products are connected in simulated/real network environment.

- The tunnel mode IPsec ESP and IKE certificate authentication is implemented.

- Tester shall have knowledge of the security parameters of tunnel for decrypting the ESP packets.

- Tester shall have access to the N9 interface between two UPFs within a PLMN.

- Tester shall have knowledge of the confidentiality algorithm and confidentiality protection keys used for encrypting the encapsulated payload.

**Execution Steps:**

The requirement mentioned in this clause is tested in accordance with the procedure mentioned in clause 4.2.3.2.4 of TS 33.117 [3].

**Expected Results:**

The user data transported on N9 within a PLMN is protected.

**Expected format of evidence:**

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

\*\*\*\* Next Changes\*\*\*\*

#### 4.2.2.5 Signalling Data Protection

*Requirement Name:* Protection of signalling data transported over N4 interface.

*Requirement Reference: TS 33.501 [2], Clause 9.9*

*Requirement Description:* As specified in clause 9.9 in TS 33.501 [2], interfaces internal to the 5G Core can be used to transport signalling data as well as privacy sensitive material, such as user and subscription data, or other parameters, such as security keys. Therefore, confidentiality and integrity protection is required.

For the protection of the non-SBA internal interfaces, such as N4 and N9, NDS/IP is expected to be used as specified in TS 33.501 [2], clause 9.9..

*Threat Reference*: TR 33.926 [7], Clause L.2.3, "No protection or weak protection for signalling data over N4 interface"

**TEST CASE:**

**Test Name:** TC\_CP\_DATA\_CONF \_UPF\_N4

**Purpose:**

Verify that the protection mechanism implemented for signalling data transmitted over N4 conforms to selected security profile.

**Procedure and execution steps:**

**Pre-Condition:**

- UPF and SMF network products are connected in simulated/real network environment.

- The tunnel mode IPsec ESP and IKE certificate authentication is implemented.

- Tester shall have knowledge of the security parameters of tunnel for decrypting the ESP packets.

- Tester shall have access to the N4 interface between SMF and UPF.

- Tester shall have knowledge of the confidentiality algorithm and confidentiality protection keys used for encrypting the encapsulated payload.

**Execution Steps:**

The requirement mentioned in this clause is tested in accordance with the procedure mentioned in clause 4.2.3.2.4 of TS 33.117 [3].

**Expected Results:**

The signalling data transported over N4 interface is protected.

**Expected format of evidence:**

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

\*\*\*\* Next Changes\*\*\*\*

#### 4.2.2.6 TEID uniqueness

*Requirement Name:* TEID uniqueness.

*Requirement Reference:*

*TS 23.501 [4], Clause 5.8.2.3.1; TS 29.281 [5], Clause 5.1; TS 23.060 [6], Clause 14.6*

*Requirement Description:*

Allocation and release of CN Tunnel Info is performed when a new PDU Session is established or released. This functionality is supported either by SMF or UPF, based on operator’s configuration on the SMF as specified in TS 23.501[4], clause 5.8.2.3.1.

Tunnel Endpoint Identifier (TEID): This field unambiguously identifies a tunnel endpoint in the receiving GTP U protocol entity. The receiving end side of a GTP tunnel locally assigns the TEID value the transmitting side has to use as specified in TS 29.281[5], clause 5.1.

The TEID is a unique identifier within one IP address of a logical node as specified in TS 23.060 [6], clause 14.6.

*Threat Reference:* TR 33.926 [7], Clause L.2.4, "Failure to assign unique TEID for a session"

**TEST CASE:**

**Test Name:** TC\_TEID\_ID\_UNIQUENESS\_UPF

**Purpose:**

Verify that the TEID generated by UPF under test for each new GTP tunnel is unique.

**Pre-Conditions:**

Test environment is set up with SMF, which may be real or simulated, and UPF under test. The tester is able to trace traffic between the UPF under test and the SMF (real or simulated). SMF configures UPF under test to generate the TEIDs.

**Execution Steps:**

1) The tester intercepts the traffic between the UPF under test and the SMF.

2) The tester triggers the maximum number of concurrent N4 session establishment requests.

3) The tester captures the N4 session establishment responses sent from UPF to SMF and verifies that the F-TEID created for each generated response is unique.

**Expected Results:**

The F-TEID set in each different N4 session establishment response is unique.

**Expected format of evidence:**

Files containing the triggered GTP messages (e.g. pcap trace).

\*\*\*\* Next Changes\*\*\*\*

#### 4.2.2.7 IPUPS

*Requirement Name:* IPUPS packeting handling

*Requirement Reference: TS 33.501[2], clause 5.9.3.4*

*Requirement Description:*

The IPUPS is expected to only forward GTP-U packets that contain an F-TEID that belongs to an active PDU session and discard all others as specified in TS 33.501 [2], clause 5.9.3.4.

*Threat Reference:* TR 33.926 [7], Clause L.2.5, "invalid user plane data forwarding"

**TEST CASE:**

NOTE 1: This test case is only applicable to UPF supporting IPUPS.

**Test Name:** TC\_IPUPS\_PACKET\_HANDLING

**Purpose:**

Verify that the packets not belonging to an active PDU session is discarded.

**Pre-Conditions:**

Test environment is set up with a V-SMF, an H-SMF, an H-UPF and a gNB which may be simulated.

**Execution Steps:**

1) The V-SMF requests the UPF with IPUPS functionality under test to establish an N4 session for a PDU session in home-routing roaming. The UPF with IPUPS functionality under test responds to the SMF with the F-TEID for the N9 tunnel towards the H-UPF, and the F-TEID for the N3 tunnel towards the gNB.

2) The V-SMF requests the H-SMF to establish a PDU session providing the received F-TEID for the N9 tunnel.

3) The H-SMF requests the H-UPF to establish an N4 session providing the received F-TEID for the N9 tunnel. H-UPF in the response provides its F-TEID for the N9 tunnel. The H-SMF provides the received F-TEID from the H-UPF to the V-SMF.

4) The V-SMF requests the gNB to allocate resource for the PDU session providing the F-TEID for the N3 tunnel received at step 1. The gNB replies with its F-TEID for the N3 tunnel to the V-SMF.

5) The V-SMF provides the UPF with IPUPS functionality under test with the received F-TEID assigned by the gNB for the N3 tunnel and the received F-TEID assigned by the H-UPF for the N9 tunnel.

6) The H-UPF is triggered to send GTP-U packets using the F-TEID assigned by the V-UPF for the N9 tunnel.

7) The H-UPF is triggered to send GTP-U packets using an F-TEID different than the one assigned by V-UPF for N9 tunnel.

**Expected Results:**

When the H-UPF is triggered to send GTP-U packets using the F-TEID assigned by the V-UPF for the N9 tunnel (step 6 in the execution steps), GTP-U packets are witnessed over the N3 tunnel.

When the H-UPF is triggered to send GTP-U packets using an F-TEID different than the one assigned by the V-UPF (step 7 in the execution steps), no GTP-U packets are witnessed over the N3 tunnel.

**Expected format of evidence:**

Files recording the GTP packets captured (e.g. pcap trace).

\*\*\*\* Next Changes\*\*\*\*

#### 4.2.2.8 Protection against malformed GTP-U messages

*Requirement Name:* Protection against malformed GTP-U messages

*Requirement Reference: TS 33.501[2], clause 5.9.3.4*

*Requirement Description:* The IPUPS is expected to discard malformed GTP-U messages as specified in TS 33.501[2], clause 5.9.3.4.

*Threat Reference:* TR 33.926 [7], Clause L.2.6, "Threats of malformed GTP-U messages"

**TEST CASE:**

NOTE 1: This test case is only applicable to UPF supporting IPUPS.

**Test Name:** TC\_IPUPS\_MALFORED\_MESSAGES

**Purpose:**

Verify that malformed messages are discarded by UPF.

**Pre-Conditions:**

The pre-conditions in clause 4.4.4 of TS 33.117 [3] apply, except that fuzzing tools supporting GTP-U protocol is available.

**Execution Steps:**

The execution steps follow those in clause 4.4.4 of TS 33.117 [3], except that the protocol the fuzzing tool is executed against is GTP-U and the interface is N9.

**Expected Results:**

The expected results in clause 4.4.4 of TS 33.117 [3] apply except that the protocol and the interface contained in the testing documentation are GTP-U and N9 respectively.

**Expected format of evidence:**

The expected format of evidence in clause 4.4.4 of TS 33.117 [3] apply.

\*\*\*\* End of Changes\*\*\*\*