**3GPP TSG-SA3 Meeting #103-e *draft\_S3-211544-r1***

**e-meeting, 17 - 28 May 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.513** | **CR** | **Draft CR** | **rev** |  | **Current version:** | **16.2.0** |  |
|  | | | | | | | | |
| *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 changeaffects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | New test case on traffic filtering | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | S3 | | | | | | | | | |
| ***Source to TSG:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5G\_IPUPS | | | | |  | ***Date:*** | | | 2021-05-10 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | B |  | | | | | ***Release:*** | | | Rel-17 |
|  | *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:*** | | It has been specified in TS 33.501 clause 5.9.3.4 that “The IPUPS shall only forward GTP-U packets that contain an F-TEID that belongs to an active PDU session and discard all others. The IPUPS shall discard malformed GTP-U messages.” | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add a new test case on how IPUPS handles traffic that is not within an active PDU session.  Add a new test case on how IPUPS handles malformed GTP-U messages. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incomplete test cases | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 4.2.2.A (new), 4.2.2.B (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 Change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 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 (Release 15): "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".

[X] 3GPP TS 33.501 (Release 16): "Security architecture and procedures for 5G system".

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change 2\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 4.2.2.A IPUPS

*Requirement Name:*IPUPSpacketing handling

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

*Requirement Description:*

"The IPUPS shall 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[5], clause 5.9.3.4.

*Threat Reference:* TR 33.926 [7], Clause L.2.W, "invalid user plane data forwarding"

**TEST CASE:**

NOTE Z1: 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 environmentis set up with a V-SMF,an H-SMF, an H-UPF and a gNBwhich may be simulated.

**Execution Steps:**

1. The V-SMF requests the UPF with IPUPS functionality under test to establish a 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 toestablish 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-SMFprovides theUPF 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 theH-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 a 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 the GTP packetscaptured (e.g. pcap trace).

#### 4.2.2.B ProtectionagainstmalformedGTP-Umessages

*Requirement Name:* Protectionagainstmalformed GTP-Umessages

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

*Requirement Description:*

"The IPUPS shall discard malformed GTP-U messages."

as specified in TS 33.501[X], clause 5.9.3.4.

*Threat Reference:* TR 33.926 [7], Clause L.2.X

**TEST CASE:**

NOTE Z2: 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 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 Change 2 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*