**3GPP TSG-SA3 Meeting #111 *S3-233391***

**Berlin, Germany, 22 – 26 May 2023**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **DRAFT CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.513** | **CR** | **draftCR** | **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:*** | Changes for SCAS UPF for Rel18 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Keysight Technologies UK | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5G\_Ph2 | | | | |  | ***Date:*** | | | 2023-05-12 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***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:*** | | TS 33.501 – clause 9.3 specifies the UPF could support IPSec on its N3 interface or not. In case IPSec is not supported, a SEG may be used to terminate the IPSec tunnel.  Also, in TS 33.501 – clause 9.9, the specification defines that a SEG may be used to terminate the NDS/IP IPsec tunnels. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | NOTEs added to address this specific situations defined in TS 33.501  Requirements of test cases updated. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | SCAS test cases are inconsistent with the specifications | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 4.2.2.1, 4.2.2.2, 4.2.2.3, 4.2.2.4, 4.2.2.5, 4.4 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 draftCR's revision history:*** | | SA3#109: S3-224089  SA3#111: S3-232781, S3-232435 | | | | | | | | |

\*\*\*\*\* 1st CHANGE \*\*\*\*\*

#### 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 shall 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:**

NOTE 1: This test case is only applicable to UPF supporting IPSec in N3 interface without the use of a SEG

**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.

\*\*\*\*\* END OF 1st CHANGE \*\*\*\*\*

\*\*\*\*\* 2nd CHANGE \*\*\*\*\*

#### 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 shall 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:**

NOTE 1: This test case is only applicable to UPF supporting IPSec in N3 interface without the use of a SEG

**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.

\*\*\*\*\* END OF 2nd CHANGE \*\*\*\*\*

\*\*\*\*\* 3rd CHANGE \*\*\*\*\*

#### 

#### 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 shall 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:**

NOTE 1: This test case is only applicable to UPF supporting IPSec in N3 interface without the use of a SEG

**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.

\*\*\*\*\* END OF 3rd CHANGE \*\*\*\*\*

\*\*\*\*\* 4th CHANGE \*\*\*\*\*

#### 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 9.3*

*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 shall be used as specified in [3]."

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

**TEST CASE:**

NOTE 1: This test case is only applicable to UPF under test supporting IPSec in N9 interface without the use of a SEG

**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.

\*\*\*\*\* END OF 4th CHANGE \*\*\*\*\*

\*\*\*\*\* 5th CHANGE \*\*\*\*\*

#### 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 shall be used as specified in [3]."

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

**TEST CASE:**

NOTE 1: This test case is only applicable to UPF under test supporting IPSec in N4 interface without the use of a SEG

**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.

\*\*\*\*\* END OF 5th CHANGE \*\*\*\*\*

\*\*\*\*\* 6th CHANGE \*\*\*\*\*

4.4 UPF-specific adaptations of basic vulnerability testing requirements and related test cases

## 4.4.1 Introduction

There are no UPF specific addtions to clause 4.4.1 of TS 33.117 [3].

### 4.4.2 Port Scanning

There are no UPF specific addtions to clause 4.4.2 of TS 33.117 [3].

### 4.4.3 Vulnerability scanning

There are no UPF specific addtions to clause 4.4.3 of TS 33.117 [3].

### 4.4.4 Robustness and fuzz testing

The test cases under clause 4.4.4 of TS 33.117 [3] are applicable to UPF.

The interfaces defined for the UPF are in clause 4.2.3 of TS 23.501 [4].

According to clause 4.4.4 of TS 33.117 [3], the transport protocols available on the interfaces providing IP-based protocols need to be robustness tested. Following TCP/IP layer model and considering all the protocols over transport layer, for UPF, the following interfaces and protocols are in the scope of the testing:

* For N3: the UDP and GTP-U procotols.
* For N4: the UDP and PFCP protocols.
* For N9: the UDP and GTP-U protocols.
* The N6 is the connection with the Data Network (DN). The protocols used in this interface are not defined by the 3GPP and are not under the scope.

NOTE: There could be other interfaces and/or protocols requiring testing under clause 4.4.4 of TS 33.117 [3]

\*\*\*\*\* END OF 6th CHANGE \*\*\*\*\*