**3GPP TSG-SA3 Meeting #101e *S3-203514***

**e-meeting, 9 – 20 November 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.514** | **CR** | **DraftCR** | **rev** |  | **Current version:** | **16.1.0** |  |
|  | | | | | | | | |
| *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 | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Living CR to 33.514 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, Hisilicon, Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eSCAS\_5G | | | | |  | ***Date:*** | | | 2020.10.26 |
|  |  | | | |  | |  | | |  |
| ***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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | As defined in TS 33.501 clause L.3, the UP security enforcement information shall be set to "required" for data transferred from gNB to a 5GS TSC-enabled UE. This is also applicable to the gPTP messages sent in the user plane.  If the UP security enforcement information is not set to "required", the gPTP message transferred from gNB to a 5GS TSC-enabled UE, may be tampered or intercepted by the attacker. Hence, new test on this feature is required.  As defined in TS 33.501 clause K.3, to reduce incremental complexity added by security, all PDU sessions associated with a specific 5G LAN group should have the same UP security policy.  If the UP security policy within a specific 5G Lan group is not the same, the data may be leaked from the unprotected air interface. Especially, for the case that one security policy is “required’, while the other security policy is “not needed”. Hence, new test case on this configuration is required. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Adding a new test case on security enforcement for vertical LAN.  Adding a new test case on security enforcement configuration for TSC services. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | If the UDM does not follow the above requirement, the gPTP message transferred from gNB to a 5GS TSC-enabled UE, may be tampered or intercepted by the attacker.  If the UDM is configured with the same security policy for all the 5G LAN UEs, the 5G LAN service message transferred from gNB to the UE, may be tampered or intercepted by the attacker. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.2.X (new); 4.2.Y (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 the 1st change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 4.2.X User plane security procedures

#### 4.2.X.1 UP security enforcement configuration for TSC service

*Requirement Name*: UP security enforcement configuration

*Requirement Reference:* TS 33.501 [2], clause L.3, TS 23.501 [5], clause 5.10.3.

*Requirement Description*:

"After the 5GS TSC-enabled UE is authenticated and data connection is set up, any data received from a TSC bridge or another 5GS TSC-enabled UE shall be transported between DS-TT (in the UE) and NW-TT (in the UPF) in a protected way using the mechanisms for UP security as described in clause 6.6.

The UP security enforcement information shall be set to "required" for data transferred from gNB to a 5GS TSC-enabled UE. This is also applicable to the gPTP messages sent in the user plane."

as specified in TS 33.501 [2], clause L.3.

"The SMF determines at PDU session establishment a User Plane Security Enforcement information for the user plane of a PDU session based on:

- subscribed User Plane Security Policy which is part of SM subscription information received from UDM; and

- User Plane Security Policy locally configured per (DNN, S-NSSAI) in the SMF that is used when the UDM does not provide User Plane Security Policy information.

- The maximum supported data rate per UE for integrity protection for the DRBs, provided by the UE in the Integrity protection maximum data rate IE during PDU Session Establishment. The UE supporting NR as primary RAT, i.e. NG-RAN access via Standalone NR, shall set the Integrity protection maximum data rate IE for Uplink and Downlink to full rate at PDU Session Establishment as defined in TS 24.501 [47]."

as specified in TS 23.501 [5], clause 5.10.3.

*Threat References*: TR 33.926 [4], TBD.

NOTE: The test case below only applies to the UDMs which support the setting and providing of User Plane Security Policy for dedicated TSC service.

*Test Case*:

**Purpose:**

Verify that UP security enforcement information is set to "required" for dedicated TSC service.

**Pre-Conditions:**

Test environment with SMF. The SMF may be simulated.

A dedicated DNN/S-NSSAI combination is defined to identify the TSC service.

The security policy is configured in the UDM.

**Execution Steps**

1. During the PDU session establishment procedure, the SMF sends a Nudm\_SDM\_Get Request message to the UDM under test with a dedicated DNN/S-NSSAI combination.

2. The UDM under test sends the Nudm\_SDM\_Get Response back to the SMF with UP security enforcement information.

**Expected Results:**

The confidentiality and integrity protection requirements of the UP security enforcement information are set to “required”.

**Expected format of evidence:**

Save the logs and the communication flow in a .pcap file.

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Start of the 2nd change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 4.2.Y User plane security procedures

#### 4.2.y.1 UP security policy configuration for 5G LAN service

*Requirement Name*: UP security enforcement configuration

*Requirement Reference:* TS 33.501 [2], clause K.3, TS 23.501 [5], clause 5.10.3.

*Requirement Description*: "To reduce incremental complexity added by security, all PDU sessions associated with a specific 5G LAN group should have the same UP security policy. When generating the policy enforcement information, and to avoid the redundant double protection, the SMF may consider information by a DN-AAA about DN protection mechanisms already applied."

as specified in TS 33.501 [2], clause K.3.

"The SMF determines at PDU session establishment a User Plane Security Enforcement information for the user plane of a PDU session based on:

- subscribed User Plane Security Policy which is part of SM subscription information received from UDM; and

- User Plane Security Policy locally configured per (DNN, S-NSSAI) in the SMF that is used when the UDM does not provide User Plane Security Policy information.

- The maximum supported data rate per UE for integrity protection for the DRBs, provided by the UE in the Integrity protection maximum data rate IE during PDU Session Establishment. The UE supporting NR as primary RAT, i.e. NG-RAN access via Standalone NR, shall set the Integrity protection maximum data rate IE for Uplink and Downlink to full rate at PDU Session Establishment as defined in TS 24.501 [47]."

as specified in TS 23.501 [5], clause 5.10.3.

*Threat References*: TR 33.926 [4], TBD.

NOTE: The test case below only applies to the UDMs which support the setting and providing of User Plane Security Policy for 5G LAN service.

*Test Case*:

**Purpose:**

Verify that UP security policy is set to the same for all the 5G LAN UEs.

**Pre-Conditions:**

Test environment with SMF. The SMF may be simulated.

A dedicated DNN/S-NSSAI combination is defined to identify the 5G LAN service.

The security policy of the 5G LAN service is configured in the UDM.

**Execution Steps**

1. During the PDU session establishment procedure initiated by the UE1, the SMF1 sends a Nudm\_SDM\_Get Request message to the UDM under test with a dedicated DNN/S-NSSAI combination, and SUPI1.

2. The UDM under test sends the Nudm\_SDM\_Get Response back to the SMF1 with UP security policy1.

3. During the PDU session establishment procedure initiated by the UE2, the SMF2 sends a Nudm\_SDM\_Get Request message to the UDM under test with a dedicated DNN/S-NSSAI combination, and SUPI2.

4. The UDM under test sends the Nudm\_SDM\_Get Response back to the SMF2 with UP security policy2.

NOTE: SMF1 and SMF2 could be the same network function.

**Expected Results:**

The confidentiality and integrity protection requirements of the UP security policy1 and UP security policy2 are the same.

**Expected format of evidence:**

Save the logs and the communication flow in a .pcap file.

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