**3GPP TSG-SA WG3 Meeting #101-e draft\_S3-203058-r1**

**e-meeting, 9 – 20 November 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v11.4* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **0977** | **rev** | **-** | **Current version:** | **16.3.0** |  |
|  | | | | | | | | |
| *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:*** | Clarification on security policy configuration for TSC services | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, Hisilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | Vertical\_LAN\_SEC | | | | |  | ***Date:*** | | | 2020-10-22 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *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:*** | | UP security enforcement informtion formulation is not align with UP security policy used in the clause 6.6.1 of TS 33.501. Therefore, alignment is required.  Another issue is how to configure the “required” policy is not clear for implementation. Considering that security policy received from UDM will be taken as the priority, it is proposed to configure the policy in the UDM as one option in the note. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Align the formulation of the security policy with the content in clause 6.6.1.  Clarification on one way to configure the “required” security policy | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Unclear specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | L.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\* \* \* First Change \* \* \* \*

Annex L (normative):  
Security for TSC service

## L.1 General

The 5G TSC service is described in 3GPP TS 23.501 [2]. It allows the 5G System to be integrated transparently as a bridge in an IEEE TSN network [75], where the 5GS system acts as one or more TSN Bridges of a TSN network.

## L.2 Access security for a 5GS TSC-enabled UE

A 5GS TSC-enabled UE accesses the 5G network as described in this document except where differences are provided in the following clauses.

## L.3 Protection of user plane data in TSC including gPTP control messages

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 policy for UP confidentiality and UP integrity protection 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.

NOTE: The "required" of the security policy can be configured in the UDM. The SMF receives the UP security policy from the UDM, and forwards the received security policy to the gNB during the PDU session establishment procedure.

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