**3GPP TSG-SA3 Meeting #108e *draft\_S3-222133-r1***

**e-meeting, 22 - 26 August 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | 1471 | **rev** | **1** | **Current version:** | 17.6.0 |  |
|  | | | | | | | | |
| *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:*** | Correction of Transport security protection for MSGin5G interfaces | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | China Mobile | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GMSG | | | | |  | ***Date:*** | | | 2022-08-04 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***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:*** | | The MSGin5G-3 interface is assumed as SBI in TS 33.501 and it is specified that security protection mechanism of SBI shall be reused. However, according to the clarification from SA6, the Application Server could be located inside or outside of the operator domain. When the Application Server is outside the operator domain, the security protection of MSGin5G-3 shall reuse the protection of the NEF-AF mechanism defined in clause 12.3. Such requirement is missing in the current specification.  Besides, SA6 specified the MSGin5G-7 interface (the interface between the MSGin5G Server and the Broadcast Message Gateway), which was a newly defined interface that SA3 did not include it at the time of study. Therefore, the specification is lacking the security protection mechanism for this interface/ | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | 1) Clarify the security protection of MSGin5G-3 should based on clause 12.3 of TS 33.501 if the Application Server is outside the operator domain.  2) Clarify the security protection of MSGin5G-7 should be based on TLS. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incomplete specifcation. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Annex Y.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  |  | Other core specifications | | | |  | | |
| ***affected:*** | |  |  | Test specifications | | | |  | | |
| ***(show related CRs)*** | |  |  | O&M Specifications | | | |  | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\*\*\* START CHANGEs \*\*\*

Annex Y (normative):   
Security aspects of the Message Service for MIoT over the 5G System (MSGin5G)

# Y.1 General

This Annex specifies the security aspects of Message Service for MIoT over the 5G System (MSGin5G). The general features of MSGin5G are described in 23.554 [106], 22.262 [107].

# Y.2 Authentication and authorization between MSGin5G client and MSGin5G Server

The Authentication and authorization between MSGin5G Client and MSGin5G Server shall be based on AKMA, which is specified in TS 33.535 [91]. Before initiating communication with MSGin5G Server, the UE needs to have performed primary authentication and registered with the 5GC, resulting in the successful generation of KAKMA and A-KID at both MSGin5G Client and the 5GC as specified in clause 6.1, TS 33.535 [91].

Once the UE is registered in 5GC, the MSGin5G Client in the UE and the MSGin5G Server may use TLS for authentication as specified in Annex B of TS 33.535 [91] with the MSGin5G Server taking the role of AKMA AF.

Methods other than TLS with AKMA may be used for authentication between the MSGin5G Client and MSGin5G Server, depending on the Ua\* protocols.

When MSGin5G service is used with SEAL, the application architecture described in TS 23.554 [106] is followed. In this case, authorization of the MSGin5G UE by the MSGin5G server is performed by validating the association between the UE service ID and UE ID (SUPI/GPSI). The UE service ID is acquired via the MSGin5G registration request, as specified in TS 23.554 [106]. The Configuration Management server or MSGin5G Configuration Function maintains association of the assigned UE service ID with the UE ID. The MSGin5G server retrieves the association from the Configuration Management server or MSGin5G Configuration Function using the UE ID received from the AAnF and verifies whether the UE service ID received in the registration request message is associated with the UE ID in the retrieved association information.

# Y.3 Transport security protection for MSGin5G interfaces

The MSGin5G-1 interface may be protected by TLS based on KAF established by AKMA as specified in TS 33.535 [91]. The MSGin5G Client and the MSGin5G Server establish the TLS session following the procedures defined in Annex B of TS 33.535 [91].

The MSGin5G-1 interface may be protected using mechanisms other than TLS with AKMA, depending on the Ua\* protocols.

For the data protection over MSGin5G-3 interface between MSGin5G Server and Application Server, if the Application Server is inside the operator domain, the transport security protection on SBI interface shall be reused as specified in clause 13. If the Application Server is outside the operator domain, the Application Server shall connect to the MSGin5G Server via NEF, clause 12.3 in the present document is applicable with the Appplication Server taking the role of the AF.

For MSGin5G-2, MSGin5G-4 and MSGin5G-7 interfaces, TLS shall be used for transport protection unless network security is provided by other means.

\*\*\* END CHANGEs \*\*\*