**3GPP TSG-SA3 Meeting #106-e *S3-220290***

**e-meeting, 14 - 25 February 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *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:*** | Resolving EN on authorization in MSGin5G | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Samsung | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 2022-01-25 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***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:*** | | This contribution proposes to resolve the following Editor’s Note:  Editor's Note: Further clarification on usage of GPSI or SUPI for authorization in MSGin5G services is FFS.  Below are the observations and proposal as discussed in S3-220299:  **Observation 1:** From the given definitions in TS 23.554 (in clause 6.1.2), it is understood that UE service ID is used to authenticate and authorize the associated UE to the MSGin5G Service at the application layer.  **Observation 2:** From clause 8.1.1 and clause 8.1.2 of TS 23.554, it is understood that UE service ID is assigned by MSGin5G server via VAL UE configuration data.  **Observation 3:** From clause 6.4, it is understood that MSGin5G UE ID is equivalent to device identifier. As per the Table 8.2.1-1 and Table 8.2.1-2 in TS 23.554, UE identifier (i.e. MSGin5G UE ID) could be MSISDN, external identifier.  **Observation 4:** MSGin5G UE sends UE service ID mandatory in the registration request, MSGin5G UE ID is part of MSGin5G Client Profile which is optional.  **Observation 5:** As per the normative text for MSGin5G client authentication and authorization, TLS with AKMA is proposed for client authentication. The AKMA procedure defines authorization of UE, however it is not service specific.  **Proposal:** The 5G system shall support service specific authorization for authorizing an MSGin5G client. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | It is proposed to have a token based authorization mechanism to authorize the UE by the MSGin5G server for MSGin5G services. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Without specifying service specific authorization, any UE will be able to obtain services, which they are not authorized for. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | X.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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\*\*\*\*\****

X.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.

A secure connection shall be established between MSGin5G Client and MSGin5G Server before client authorization. If SEAL is supported then the Identity Management for the MSGin5G client shall follow the procedure defined in TS 33.434[xx], to obtain an access token from the SEAL Identity Management server scoped for accessing services from MSGin5G Server. The access token shall include the UE service ID and MSGin5G UE ID which is presented to the MSGin5G server for authorization. . The MSGin5G server shall present the access token to the MSGin5G server when requesting the MSGin5G services. The MSGin5G server shall validate the signature of the access token prior to granting the requested services. The method used to provision the MSGin5G server with the SEAL Identity Management Server signature validation credentials is out of scope of this document.

NOTE: If SEAL architecture and Identity Management Server are not supported then UE service ID is not authorized.

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