**3GPP TSG-SA3 Meeting #123 S3-252892**

Goteborg, Sweden, 25 – 29 August 2025

|  |
| --- |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Security of IMS avatar communication – providing the authorization token to the receiving UE in the receiving UE centric rendering mode |
|  |  |
| ***Source to WG:*** | Philips International B.V. |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** | 2025-08-18 |
|  |  |  |  |  |
| ***Category:*** |  |  | ***Release:*** | Rel-19 |
|  | *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 canbe 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:*** | As concluded in TR 33.790, a new clause in TS 33.328 is needed, which provides a summary of the security of IMS avatar communication, a reference to the related clauses in TS 23.228, a list of security requirements among other changes.Although the token details have been specified, it is not clear in receiving UE centric rendering mode when is the token provided to the receiving UE. |
|  |  |
| ***Summary of change:*** | A new clause. which provides a summary of the security of IMS avatar communication, a reference to the related clauses in TS 23.228, a list of security requirements among other changes.In receiving UE centric rendering mode, the sending UE provides the receiving UE during the avatar animation negotiation phase (step 4 in AC11.3.2.2 of TS 23.228) with the URL associated with the chosen avatar ID and the authorization token enabling it (i.e., the receiving UE) to retrieve the Sending UE’s Avatar representation from BAR.  |
|  |  |
| ***Consequences if not approved:*** | Security of IMS avatar communication is not specified. |
|  |  |
| ***Clauses affected:*** | Annex X (new clause), Annex X.1 (new), Annex X.2 (new), Annex X.3 (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:*** |  |

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

# Annex X (Normative): Security for IMS avatar communication

## X.1 General

This clause specifies the security for IMS avatar communication.

TS 23.228 [3], Annex AC.11, has specified the procedures for IMS avatar communication.

## X.2 Security requirements

The security requirements for the security and privacy of IMS avatar communication are:

- The 3GPP system shall support means for integrity and confidentiality protection for Avatar ID List downloading, avatar representation downloading and Avatar ID transferring.

- The 3GPP system shall support means to ensure that stored Avatar representations and Avatar-IDs are accessed and used only by authenticated and authorized entities, e.g. MF, DC AS, UEs .

## X.3 Security Procedures

The security procedures are based on the TS 23.228 [3] AC.11 procedures with the following security handling.

To prevent the sending UE from providing an Avatar ID belonging to another UE, it shall be verified whether the avatar ID provided by the sending UE is in the sending UE’s Avatar ID list.

Editor's Note: Whether BAR and/or DC AS verifies the Avatar ID provided by the sending UE is in the the sending UE's Avatar ID list is FFS.

The authorization of avatar representation downloading shall be based on a token mechanism. The token shall include the Avatar ID chosen by the sending UE, the UE ID of the sending UE (i.e., IMPU), one of MF ID or DC AS ID, the BAR ID, and expiration time. In case of the receiving UE centric rendering mode, the token shall/should further include the receiving UE ID (i.e., IMPU) and shall be provided to the receiving UE, through the established application data channel together with the URL associated with the Avatar ID chosen by the sending UE. The BAR shall verify the token as follows:

- The BAR shall verify the signature of the token.

- The BAR shall verify whether the Avatar ID in the Avatar representation downloading request matches that in the token.

- The BAR shall verify whether the UE ID of the sending UE in the Avatar representation downloading request matches that in the token.

- In the receiving UE centric rendering mode, the BAR shall/should verify whether the receiving UE ID in the Avatar representation downloading request matches that in the token.

- The BAR shall check whether the MF ID or the DC AS ID in the token matches the entity sending the Avatar representation downloading request.

- The BAR shall check whether the BAR ID in the token matches its own ID.

- The BAR shall check, based on the token expiration time, whether the token is valid.

 - If the token verification is successful, the BAR shall send the sending UE's Avatar representation to the MF or DC AS.

The e2DCe or e2e media plane protection mechanism in clause 5 shall be reused for authentication, integrity and confidentiality protection between UE and MF, UE and DC AS for Avatar ID list downloading and avatar representation downloading, Avatar ID transfer via BDC/ADC. The security specification in Annex P.1 shall be reused for security of aspects of SBA in IMS media control interface, to protect SBA communication between MF/DCSF and DC AS/BAR. The security specification in TS 33.501 [11], clause 12 shall be reused for protection of the NEF – AF interface, to protect communication between DCSF and DC AS if the DC AS is deployed outside of operator’s domain.

In a receiving UE centric rendering mode, the receiving UE should delete the avatar representation of the sending UE after the avatar communication session is over.

NOTE X: This can mitigate the situation of the receiving UE from using the avatar representation of the sending UE in a sending UE centric procedure after a receiving UE centric avatar session where receiving UE receives the avatar representation of the sending UE for rendering.

Editor's Note: SA2 alignment is needed with respect to other types of authorization aspects, e.g. authorization upon signalling.

Editor's Note: Whether the receiving UE ID is a mandatory or an optional field in the token in the UE centric rendering mode and whether BAR verifies it is FFS.

\*\*\* END OF CHANGES \*\*\*