**3GPP TSG-SA3 Meeting #101-e draft\_S3-202920-r1**

**e-meeting, 9 – 20 November 2020**

**Source: ZTE**

**Title: New solution for key issue#1 in TR 33.850**

**Document for: Approval**

**Agenda Item: 5.11**

# 1 Decision/action requested

***This contribution proposes a new solution for key issue#1 .***

# 2 References

*(Reference - in list form - should be made to previous related SA3/3GPP/etc. documents.)*

[1] 3GPP TR 33.850 “ Study on security aspects of enhancements for 5G Multicast-Broadcast Services (MBS)”.

# 3 Rationale

This contribution proposes a new solution for key issue#1.

# 4 Detailed proposal

***\*\*\*\* START OF CHANGES \*\*\*\****

## 6.X Solution #X: Authentication and authorization for multicast communication service based on AKMA

### 6.X.1 Solution overview

This solution, which is based on AKMA, addresses the key issue #1 Security of authentication and authorization for multicast communication service.

### X.2 Solution details



Figure 6.x.2-1 Authentication between the MBSF/MSF-C and UE based AKMA

1. UE shall generate the AKMA Anchor Key (KAKMA) and the A-KID from the KAUSF before initiating communication with an AKMA Application Function, i.e MBSF/MSF-C, as specified in TS 33.535[x].
2. UE derive a key KMBS for authentication with the MBSF/MSF-C .
3. When UE try to join the multicast service, UE computes MAC-I and then UE sends a MBS service request to MBSF/MSF-C. The service request include A-KID and MAC-I.

Editor’s Note: How to derive the MAC-I is FFS.

3-6. Upon receiving the request, the MBSF/MSF-U discovers the AAnF, then AAnF generates KMBS and sends the KMBS to MBSF/MSF-C.

Editor’s Note: It is FFS how to discover the correct AAnF.

Editor’s Note: How MBSF/MSF-C obtains authorization information is FFS.

Editor’s Note: It is ffs whether primary authentication is sufficient to authenticate the UE towards the MBSF.

7. The MBSF/MSF-C verifies the MAC-I using the KMBS, when the verification is succeed, and if the UE is authorized to perform the operation,Then the MBSF/MSF-C sends a service response to the UE.

### 6.X.3 Solution evaluation

TBD

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

***\*\*\*\* START OF CHANGES \*\*\*\****

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 23.757: " Study on architectural enhancements for 5G multicast-broadcast services ".

[3] 3GPP TS 33.246: " Security of Multimedia Broadcast/Multicast Service (MBMS) ".

[4] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description".

[x] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

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