**3GPP TSG-SA3 Meeting #109AdHoc-e *draft\_S3-230111-r1***

**Electronic meeting, 16 - 20 January 2023**

**Source: ZTE**

**Title: Conclusion for KI#1**

**Document for: Approval**

**Agenda Item: 5.6**

# 1 Decision/action requested

***Approve this pCR to provide conclusion text for KI#1***

# 2 References

 [1] TR33.737 v0.3.0

# 3 Rationale

 There are three scenarios in KI#1[1].

For case 2, the conclusion had been reached in last meeting.

For Case 1, the AF is located in the HPLMN, and the AF also stores the encryption/decryption key used between the AF and the UE. The AF needs to transmit the key to the VPLMN NF for storage. In this case, AAnF and other home-domain NFs are not suitable for transmitting the key, because they do not know what is the real key.

For Case 3, if the AF is located in the Date Network, because the operator's network cannot force third-party AF to transmit the key to the operator's network, the AAnF can transmit KAF to the VPLMN NF for storage.

For different solutions of case 1 and case 3, because the AKMA belongs to a home service, it is not recommended to forcibly deploy the AKMA in VPLMN, which increases deployment costs of an operator. In addition, the AMF (SEAF) already has the function of storing user keys. If the supervision function needs to be supported in VPLMN, the AMF (SEAF) can be upgraded and reconstructed. If the supervision function is not supported in VPLMN, the home network does not need to transmit the related keys, and the AMF (SEAF) can ignore the key pushing request. This contribution is proposed to provide conclusion text to KI#1.

# 4 Detailed proposal

*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Start of 1st Change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\**

## 7.1 Conclusion to Key Issue#1

Regarding AKMA roaming architecture, AKMA architecture defined in TS 33.535[2] can be reused.

For case 1 (UE is in VPLMN and accessing an internal HPLMN AF), since the AF knows the encryption key used between the UE and the AF, The AF needs to transmit the key to the VPLMN NF(e.g. AMF) for storage.

For case 2 (UE in VPLMN accessing an internal AF of the VPLMN), since the AF knows the encryption key used between the UE and the AF, the LI requirements can be fulfilled by the AF, thus no normative work is needed.

For case 3 (UE is in VPLMN and accessing an external AF in the Data Network (Internet)), since the operator's network cannot force third-party AF to transmit the key to the operator's network, the AAnF can transmit KAF to the VPLMN NF(e.g. AMF) for storage.

Editor’s Note:  Further conclusion on LI, e.g. providing other security parameters, avoiding under-collection of traffic, etc, is FFS.*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*End of 1st Change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\**