**3GPP TSG-SA3 Meeting #102-e *S3-210162-r1***

**e-meeting, 18 - 29 January 2021** Revision of S3-20xxxx

**Source: ZTE Corporation**

**Title: New solution for key issue 4.1 in TR 33.846**

**Document for: Approval**

**Agenda Item: 5.5**

# 1 Decision/action requested

***This contribution proposes a new solution for key issue 4.1 .***

# 2 References

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

[1] 3GPP TR 33.846 “Study on authentication enhancements in 5G System”.

# 3 Rationale

This contribution proposes a new solution for key issue 4.1.

# 4 Detailed proposal

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

### 6.4.Y Solution #4.Y: Using time-based or partly time-based SQN generation

#### 6.4.Y.1 Introduction

This solution addresses is related to the key issue #4.1 Protection of SQN during AKA re-synchronisations and shows that the problem would not exist, if one of the following SQN generation schemes are used.

#### 6.4.Y.2 Solution details

As specified in Annex C.3 TS 33.102 [3], if the generation of sequence number is time-based or partly time-based, the value of SQN does not allow to trace the user over longer periods. Therefore, there may be no need to conceal SQN by an anonymity key as specified in section 6.3, TS 33.102 [3]. If the time-based or partly time-based SQN generation is used, the AK is not used and the SQN does not need protected.

Therefore, this solution propose to use time-based or partly time-based SQN generation to resolve this key issue.

#### 6.4.Y.3 Evaluation

This solution use time-based schemes to resolve the key issue#4.1 without impact on USIM and UDM. It does not work for non-time based schemes.

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