**3GPP TSG-SA3 Meeting #102e- Bis *S3-210983-r1***

**e-meeting, 1 - 5 March 2021** Revision of S3-2xxxxx

**Source: Intel**

**Title: Updates to solution 1**

**Document for: Approval**

**Agenda Item: 2.19**

# 1 Decision/action requested

***It is requested to approve the key issue for 33.873***

# 2 References

[1] LS S2-2006011: " LS on System support for Multi-USIM devices."

[2] S2-2100080: “Notes of SA2#143E\_CC#0 - pre-meeting moderated email discussion results v3”

[3] 3GPP TS 33.501: "Security architecture and procedures for 5G System."

[4] 3GPP TR 23.761: " Study on system enablers for devices having multiple Universal Subscriber Identity Modules (USIM)"

# 3 Rationale

This pCR proposes resolution of Editor’s notes on solution #1 as follows and provide evaluation:

Editor’s Note: The need for three different authentications and the threats mitigated by each is FFS:

Editor’s Note: The security implications of securing Uu interface with only network auth (i.e., no authentication of the UE) is FFS

Editor’s Note: It needs to be clarified in step 3a, 3b whether ciphering or integrity protection is done on only busy indication or full nas message*.*

1) Added figure to match the steps.

2) Added description from SA2 TR to match verbiage.

3) It is also clarified that NAS message is ciphered and integrity protected.

# 4 Detailed proposal

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start Of Changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

## 6.1 Solution #1: Security Solution for Busy Indication using NAS signaling

### 6.1.1 Introduction

This solution addresses key issue #1: Security Aspects of Busy Indication.

The key issue proposes to support a mechanism to prevent DoS attack caused by busy indication. Solution reduces the severity of the DoS attacks and identify the DoS attacks by handling the response to paging for MT service. Solution described proposes a solution allowing the UE to send a busy indication to the network in a NAS message as a response to a page.

### 6.1.2 Solution details

The procedure below assumes that UE-1 can periodically pause the RRC-connection allowing UE-2 to perform page monitoring.



**Figure 6.1.2-1 BUSY Indication using NAS Signaling**

0. A device with USIM, i.e., UE1, is in connected mode and UE2 is in IDLE mode.

1. The AMF-2 serving the UE-2 sends a paging request message to RAN-2. RAN-2 pages UE-2

2. Upon receiving the paging message UE-2, if UE supporting NAS BUSY indication decides to send a NAS BUSY indication, responds with a BUSY indication vis NAS message after RACH procedure. RAN-2 forwards the NAS message to the AMF-2.

a. The Busy Indication NAS message shall be ciphered. The cipher mechanism as defined in clause 6.4.4 of TS 33.501 [3] can be reused to protect the in the NAS message.

b. The Busy Indication NAS message shall be integrity protected. The integrity protection mechanism as defined in clause 6.4 3 of TS 33.501 [3] can be reused to integrity protect the in the NAS message.

Editor’s Note: It is FFS how GUTI re-allocation is done when GUTI gets revealed in the busy indication message.

Editor’s Note: It is FFS to verify with RAN whether UE can do a 3-way NAS exchange in network B, when it is in active state in network A.

### 6.1.3 System impact

UE:

- Uses existing NAS integrity and ciphering mechanism as per 33.501[3].

AMF:

- Uses existing NAS integrity and ciphering mechanism as per 33.501[3].

Note: Details of NAS message to send busy indication will be defined by SA2 or CT1 group.

### 6.1.4 Evaluation

Above solution relies on already defined mechanisms in TS 33.501[3] to send ciphered and integrity protected BUSY indication and fulfills security requirements of Key issue 1.

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End Of Changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***