**3GPP TSG-SA3 Meeting #102 -e *S3-210209-r2***

**e-meeting, 18th - 29th January 2021** merge of S3-210214

**Source: Intel, Apple**

**Title:** **Security Solution for Busy Indication using NAS signaling**

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

***It is proposed to approve the Solution for busy indication in MUSIM TR 33XXX.***

# 2 References

*(Reference - in list form - should be made to previous related SA5/3GPP/etc. documents.)*

*(For changes against a draft TS/TR, a pseudo CR - a.k.a. pCR - will be provided using this Tdoc template. In this case, the number, name and version of the draft TS/TR used as base must be provided and the version must be the latest available version of the draft TS/TR.)*

<Examples of references, please delete when you have inserted your actual references:

[1] 3GPP TS 32.500 SON Concepts and Requirements

[2] 3GPP TS 99.999 This example has a very long name, because then we can see how thi References paragraph will handle paragraphs spanning more than one line.

[3] 3GPP TS 99.999 Title of the document

[4] S5-991234, CR 32.999 v10.1.1, Inverting architecture of SON

[5] [S5-100001](http://www.3gpp.com/ftp/TSG_SA/WG5_TM/TSGS5_69/Docs/S5-100001.zip), Agenda, 3GPP SA5#69 Comment>

# 3 Rationale

pCR Proposes a new NAS Based solution related to the security of Busy indication.

# 4 Detailed proposal

**\*\*\*\*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 23.761: " Study on system enablers for devices having multiple Universal Subscriber Identity Modules (USIM)"

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

**\*\*\*\*NEXT CHANGES \*\*\***

## 6.Y Solution #Y: Security Solution for Busy Indication using NAS signaling

### 6.Y.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.Y.2 Solution details

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

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

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

3. Upon receiving the paging message UE-2, if it decides to send a busy indication, responds with a NAS message with new cause value "Busy" after RACH procedure. RAN-2 forwards the NAS message to the AMF-2. 1.

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

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

Editor’s Note: The procedure shall align with SA2, such as how does the UE-2 decide to send a busy indication, and whether the “Busy” is called a cause value.

Editor’s Note: The figure reflecting the steps needs to be added

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.

### 6.Y.3 System impact

UE:

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

AMF:

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

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

6.Y.4 Evaluation

Editor's Note: Each Solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

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