**3GPP TSG-SA3 Meeting #102-e *S3-210147***

**e-meeting, 18th – 29th January 2021** Revision of S3-2xxxxx

**Source: Nokia, Nokia Shanghai Bell, Lenovo, Motorola Mobility**

**Title: Secure Busy Indication by MUSIM UE**

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

Approve the solution proposal for MUSIM Busy Indication to address key Issue#1

# 2 References

# 3 Rationale

As described in key issue #1 in 3GPP MUSIM TR 33.wxy S3-203411(approved in SP-201131), security threat and requirement has been agreed as below:

“Threat: If the Busy indication is modified or replayed by attackers, the network may be spoofed to believe the UE appears busy and not respond to paging, causing Dos attack on UE.

Security requirements: 3GPP system shall support a mechanism to identify and prevent DoS attack caused by busy indication.”

In LS S2-2006037 on System support for Multi-USIM devices, SA2 also asked “Q5: Please provide feedback if it is feasible (and secure) that the Busy Indication is sent as RRC message instead (no NAS message to the CN) i.e. as a RRC response to paging without requiring an RRC connection [RAN2, RAN3, SA3] “

# 4 Detailed proposal

### \*\*\*\*\*\*\*\*\* START OF CHANGES (all text new) \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 6.Y.1 Solution #Y: Secure NAS Busy Indication by MUSIM UE

#### 6.Y.1.1 Introduction

This solution addresses the key issue #1 Security Aspects of Busy Indication. Since the UE is busy communicating in one network, the UE is expected to send the BUSY indication without becoming active in the network which is paging the UE. A full NAS message cannot be sent in the network paging the UE, instead a short BUSY indication is sent in the RRC message Msg3 to the gNB, which forwards indication to the AMF. Hence the solution requires that,

1. The indication from UE to the AMF need to contain the UE identity

2. Busy indication, need to be unique from the UE, so that spurious messages can be filtererd out.

This means that the short BUSY indication need to be something similar to an integrity MAC of a regular NAS message. Since the UE is in idle state in the network, the UE and AMF shares a NAS context. This context could be used to generate an integrity MAC or token. Since the AMF is aware of the UL NAS COUNT, similar to the regular NAS message, computing an integrity MAC using the NAS COUNT will ensure that the AMF is able recognise the correct MAC.

Since regular NAS message cannot be used to generate the integrity MAC, an assigned Paging token is used to compute the integrity MAC, which is used as the Busy indication. The Paging Token is a unique token assigned to the UE, by the AMF in a secured NAS message for example in the NAS SMC or may be even later.

When the UE is Paged in another network, if the UE is busy and wants to send a BUSY indication, UE computes an integrity MAC using the NAS parameters stabled in that network and the assigned Paging Token as input. For the AMF, the BUSY indication is valid, only if the UE is being paged. The busy indication is also unique to the UE because of the unique Paging Token assigned and the UL NAS COUNT.

#### 6.Y.2.1 Solution details

##### 6.Y.2.1.1 Paging token assignment



Figure 6.Y.2.1.1-1 Paging token assignment at AMF & UE

A multi-USIM UE with two USIMs is considered;

* USIM A registered to RAN A / AMF A and
* USIM B registered to RAN B / AMF B.

Figure 6.Y.2.1.1-1 above depicts the paging assignment by the AMF to the UE.

Step 1. Registration and primary authentication is performed for both USIMs (A & B) with respective home environment.

Step 2. AMF A is aware of the MUSIM capable UE, with capbalilties information received from UE and subscription information received from UDM. AMF A generates a unique token PAGING\_TOKEN\_A and stores it in UE security context for future MAC verification. PAGING\_TOKEN\_A, for example could be a 128 bit or 64 bit long random generated value. AMF A also sends the same “PAGING\_TOKEN\_A” as one of the parameters in encrypted and integrity protected NAS Message to USIM A. Received token is stored in UE for later use.

Step 3. AMF B is aware of the MUSIM capable UE, with capbalilties information received from UE and subscription information received from UDM. AMF B generates a unique token PAGING\_TOKEN\_B and stores in UE security context for future MAC verification. AMF B also sends the same “PAGING\_TOKEN\_B” in NAS message to UE. Received token is stored in UE for later use. “PAGING\_TOKEN” is considered as shared secret between AMF and UE. One of the examples of NAS message in which paging token can be shared is Security mode command.

Editor note: NAS message for assigning the paging token to the UE is FFS.

##### 6.Y.2.1.2 Paging and busy indication handling

 

Figure 6.Y.2.1.2-1 Paging and Busy indication handling

Step 1. USIM A moves to connected mode with RAN A / AMF A. USIM B is in idle mode with RAN B / AMF B.

Step 2. From AMF B (via RAN B), when paging is received for USIM B, UE computes a shortMAC-I using previously stored PAGING\_TOKEN\_B, as shown in figure 6.Y.2.1-3 below.

Step 3. UE forms a NAS payload for the busy indication message along with the UE identifier 5G-S-TMSI(48 bits) and the computed shortMAC-I (16 bits) and sends it to the base station RAN B. Since the UE is in idle in network B, RRC can only send maximum of 64 bits payload / content over the air in first uplink transmission. When busy indication is received in RAN B from USIM B, RAN B forwards the NAS payload to the AMF B using the NGAP protocol. RAN B transparently forwards the NAS payload (5G-S-TMSI and shortMAC-I) to AMF B.

If the UE is being paged and AMF B is expecting aresponse form it, AMF B retrieves the PAGING\_TOKEN\_B from the UE security context and computes shortXMAC-I, as shown in figure 6.Y.2.1-3. Received shortMAC-I is compared with expected shortXMAC-I. If verification is successful, then it is considered as valid Busy indication message received against paging message sent before. AMF stops further paging the UE. It is to be noted that the AMF B receives the Busy indication message only for a short window of time during and after the paging operation. Outside of this window, the AMF B doesn’t process any Busy indication messages for the particular UE indicated by the S-TMSI, to filter out unwanted messages from possible attackers.

Figure 6.Y.2.1.2-1 shows the handling of paging and corresponding response (busy indication) procedures

Editor’s Note: Size of the NAS payload in the first RRC message is FFS to be verified with RAN2.

##### 6.Y.2.1.3 ShortMAC-I / ShortXMAC generation



**Figure 6.Y.2.1-3** shortMAC-I and shortXMAC-I generation at UE and AMF

The input parameters to the integrity algorithm are a 128-bit integrity key named KEY, a 32-bit COUNT, a 5-bit bearer identity called BEARER, the 1-bit direction of the transmission i.e. DIRECTION, and the PAGING\_TOKEN (received in Security mode command from AMF) or the 5G-GUTI instead of the PAGING\_TOKEN (in case it was not provisioned by the AMF). The DIRECTION bit is 0 for uplink and 1 for downlink.

Based on these input parameters the UE computes a 32-bit message authentication code (MAC-I/NAS-MAC) using the integrity algorithm NIA. From the computed 32 bit MAC value, use only the 16 LSB of MAC-I / NAS-MAC as shortMAC-I. At receiver end, the AMF computes the expected message authentication code (XMAC-I / XNAS-MAC) with input parameters like KEY, COUNT, DIRECTION, BEARER, PAGING\_TOKEN (retrived from UE security context). 32 bit XMAC-I / XNAS-MAC is computed and from this output, only 16 LSB is retrieved, which we call it as shortXMAC-I.

Figure 6.Y.2.1-3 explans the shortMAC-I and shortXMAC-I generation procedure at UE & AMF.

#### 6.Y.3.1 Evaluation

TBD

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