**3GPP TSG-SA3 Meeting #101-e *S3-202937***

**e-meeting, 09-20 November 2020** Revision of S3-XXXX

**Source: Intel**

**Title: Key Issue for UE and Paging Server Communication**

**Document for: Approval**

**Agenda Item: 5.19**

1 Decision/action requested

***It is proposed to approve the Key issue for UE and Paging Server Communication in MUSIM TR 33XXX.***

2 References

[1] 3GPP TR 23.761: " Study on system enablers for devices having multiple Universal Subscriber Identity Modules (USIM)"

3 Rationale

pCR Proposes a new key issue related to the security of UE and Paging Server Communication.

4 Detailed proposal

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

5.X Key issue #X: UE and Paging Server Communication

5.X.1 Key issue details

As per 23.761[YY], A Multi-USIM device is needed to monitor each connected system's paging channel for MT services destined to that device. UE's paging notification and reception need to be done with minimal interruption to ongoing services in the current system and without performing undesirable operations (e.g., Wasting resource, reaching misleading assumption of reachability). MUSIM devices which are unable to simultaneously monitor paging on all 3GPP RATs and systems in which it is in Idle state or RRC\_Inactive state (for 5GS) needs to choose the paging channel(s) to monitor, which can lead to unsuccessful paging on the other paging channel(s). There are two solutions, to prevent unnecessary interruption of the current service to receive paging (Solution #7, Solution #12, Solution #27), proposed in the 23.761[YY]. While connected to a MUSIM system, all these solutions deliver paging notifications of 3GPP RATs and systems in which UE is in Idle or inactive state through a currently active network. Solutions to this key issue should study security and privacy aspects related to communication between UE and paging server..

5.X.2 Threats

If the communication between UE and paging server is not integrity protected, an attacker could modify the paging notification data or even inject fake paging notification on behalf of the network over the air interface.

If the communication between UE and the paging server is not encrypted, an attacker could eavesdrop on the air interface's paging notification data, causing linkability attacks.

Editor’s Note: Security threats related to privacy aspects of UEs behaviour are FFS

5.X.3 Potential security requirements

The 3GPP System shall support integrity protection and replay protection of paging notification.

The 3GPP System shall support the confidentiality protection of paging notification.

Editor’s Note: Security requirements related to privacy aspects of UEs behaviour are FFS

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