**3GPP TSG-SA3 Meeting #102-e *S3-210145***

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

**Source: Nokia, Nokia Shanghai Bell, Samsung, Huawei, HiSilicon**

**Title: MUSIM privacy issues relating to Paging Cause exposure**

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

Approve the pCR for key issue relating to Paging Cause

# 2 References

# 3 Rationale

In LS S2-2006011 on System support for Multi-USIM devices, SA2 asked “Q1: Please confirm whether exposing the Paging Cause in cleartext poses any privacy/security issues. “

# 4 Detailed proposal

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

5.1 Key issue #x: Privacy and security aspects of exposing ‘paging cause’

5.1.1 Key issue details

In TR 23.761 [2], a Multi-USIM device with concurrent registrations over 3GPP RAT associated with multiple USIMs procedures is discussed. A multi-USIM device can efficiently perform some activity (e.g., listen to paging) in a system while communicating in another system.

The network sends a paging request to notify the UE of a pending MT service. The Paging indication may additionally contain a ‘paging cause’ value indicative of the type of service/data pending for the UE in the network. In TR 23.761, only one ‘paging cause’ value has been agreed, but privacy and security aspects of exposing multiple values, corresponding to different mobile terminated services and data need to be analyzed.

The UE may be registered for any type of services in the network, this means that all the QoS types need to be considered. TS 23.501 in Table 5.7.4-1: Standardized 5QI to QoS characteristics mapping, indicating different services, as quoted below.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **5QI**  **Value** | **Resource Type** | **Default Priority Level** | **Packet Delay Budget**  **(NOTE 3)** | **Packet Error**  **Rate** | **Default Maximum Data Burst Volume**  **(NOTE 2)** | **Default**  **Averaging Window** | **Example Services** |
| 1 | GBR | 20 | 100 ms  (NOTE 11,  NOTE 13) | 10-2 | N/A | 2000 ms | Conversational Voice |
| 2 | (NOTE 1) | 40 | 150 ms  (NOTE 11,  NOTE 13) | 10-3 | N/A | 2000 ms | Conversational Video (Live Streaming) |
| 3  (NOTE 14) |  | 30 | 50 ms  (NOTE 11,  NOTE 13) | 10-3 | N/A | 2000 ms | Real Time Gaming, V2X messages  Electricity distribution – medium voltage, Process automation - monitoring |
| 4 |  | 50 | 300 ms  (NOTE 11,  NOTE 13) | 10-6 | N/A | 2000 ms | Non-Conversational Video (Buffered Streaming) |
| 65  (NOTE 9,  NOTE 12) |  | 7 | 75 ms  (NOTE 7, NOTE 8) | 10-2 | N/A | 2000 ms | Mission Critical user plane Push To Talk voice (e.g., MCPTT) |
| 66  (NOTE 12) |  | 20 | 100 ms  (NOTE 10,  NOTE 13) | 10-2 | N/A | 2000 ms | Non-Mission-Critical user plane Push To Talk voice |
| 67  (NOTE 12) |  | 15 | 100 ms  (NOTE 10,  NOTE 13) | 10-3 | N/A | 2000 ms | Mission Critical Video user plane |
| 75  (NOTE 14) |  |  |  |  |  |  |  |
| 71 |  | 56 | 150 ms (NOTE 11, NOTE 13, NOTE 15) | 10-6 | N/A | 2000 ms | "Live" Uplink Streaming (e.g. TS 26.238 [76]) |
| 72 |  | 56 | 300 ms (NOTE 11, NOTE 13, NOTE 15) | 10-4 | N/A | 2000 ms | "Live" Uplink Streaming (e.g. TS 26.238 [76]) |
| 73 |  | 56 | 300 ms (NOTE 11, NOTE 13, NOTE 15) | 10-8 | N/A | 2000 ms | "Live" Uplink Streaming (e.g. TS 26.238 [76]) |
| 74 |  | 56 | 500 ms (NOTE 11, NOTE 15) | 10-8 | N/A | 2000 ms | "Live" Uplink Streaming (e.g. TS 26.238 [76]) |
| 76 |  | 56 | 500 ms (NOTE 11, NOTE 13, NOTE 15) | 10-4 | N/A | 2000 ms | "Live" Uplink Streaming (e.g. TS 26.238 [76]) |
| 5 | Non-GBR | 10 | 100 ms  NOTE 10,  NOTE 13) | 10-6 | N/A | N/A | IMS Signalling |
| 6 | (NOTE 1) | 60 | 300 ms  (NOTE 10,  NOTE 13) | 10-6 | N/A | N/A | Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.) |
| 7 |  | 70 | 100 ms  (NOTE 10,  NOTE 13) | 10-3 | N/A | N/A | Voice, Video (Live Streaming) Interactive Gaming |
| 8 |  | 80 | 300 ms  (NOTE 13) | 10-6 | N/A | N/A | Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive |
| 9 |  | 90 |  |  |  |  | video, etc.) |
| 69  (NOTE 9, NOTE 12) |  | 5 | 60 ms  (NOTE 7, NOTE 8) | 10-6 | N/A | N/A | Mission Critical delay sensitive signalling (e.g., MC-PTT signalling) |
| 70  (NOTE 12) |  | 55 | 200 ms  (NOTE 7,  NOTE 10) | 10-6 | N/A | N/A | Mission Critical Data (e.g. example services are the same as 5QI 6/8/9) |
| 79 |  | 65 | 50 ms  (NOTE 10,  NOTE 13) | 10-2 | N/A | N/A | V2X messages |
| 80 |  | 68 | 10 ms  (NOTE 5,  NOTE 10) | 10-6 | N/A | N/A | Low Latency eMBB applications Augmented Reality |
| 82 | Delay Critical GBR | 19 | 10 ms (NOTE 4) | 10-4 | 255 bytes | 2000 ms | Discrete Automation (see TS 22.261 [2]) |
| 83 |  | 22 | 10 ms (NOTE 4) | 10-4 | 1354 bytes  (NOTE 3) | 2000 ms | Discrete Automation (see TS 22.261 [2]);  V2X messages (UE - RSU Platooning, Advanced Driving: Cooperative Lane Change with low LoA. See TS 22.186 [111]) |
| 84 |  | 24 | 30 ms  (NOTE 6) | 10-5 | 1354 bytes  (NOTE 3) | 2000 ms | Intelligent transport systems (see TS 22.261 [2]) |
| 85 |  | 21 | 5 ms  (NOTE 5) | 10-5 | 255 bytes | 2000 ms | Electricity Distribution- high voltage (see TS 22.261 [2]).  V2X messages (Remote Driving. See TS 22.186 [111], NOTE 16) |
| 86 |  | 18 | 5 ms  (NOTE 5) | 10-4 | 1354 bytes | 2000 ms | V2X messages (Advanced Driving: Collision Avoidance, Platooning with high LoA. See TS 22.186 [111]) |

Table 1: Standardized 5QI to QoS characteristics mapping

All the services in the table above may not relevant in the context of Paging cause, but few of the services are relevant. Also a combination of the few services such as {conversational voice + IMS signaling} are quite relevant.

According to the solution#1 in the 3GPP TR 23.761 [1], the Paging Cause and the service preferences are configured by the user or a pre-configured logic specific to the Multi-USIM device (and out of 3GPP scope). An Editor's note are captured as follow:

“*Editor's note: Whether exposing the Paging Cause in clear poses as security issue will be determined by SA WG3.*”

If the Paging Cause exposed in clear, the paging cause may be tampered by an attacker, which may cause potential attacks.

5.1.2 Threats

If paging cause is transmitted in clear, by initiating different services, an attacker can locate a target user/UE in a tracking area observing the paging broadcasts. This could lead to violation of privacy in certain situations.

If one or more paging causes are signalled to the UE, this provides more opportunity for fraudulent attackers in tracking the user and identifying them by invoking more service types to the UE.

Observing the Paging cause in the paging message and an immediate response from the UE, when there are not many users around helps to track and isolate the person. GUTI reallocation definitely helps to mitigate continuous tracking of the UE. However it does not hide privacy of the UE, when number of UEs are very few at a spot or a cell. Identification of presence of the UE in a particular area is possible using the distinctive paging cause like MC, V2X.

Further, when the type of service/data pending for the UE in the network is revealed by the paging cause in clear, then it provides enough critical input data for analytics on the network , like frequency of paging for V2X/Smart grid service in the network.

Currently, the paging message is not protected. If the Paging Cause exposed in clear, the paging cause of a USIM (CM\_IDLE or RRC\_Inactive state) may be tampered by an attacker, this USIM may incorrectly respond to the paging request. As a result, another USIM that has on-going services is disconnected from the network, causing DoS attacks.

5.1.3 Potential security requirements



The system shall support confidentiality protection mechanism for the paging cause to mitigate the threat on privacy of the UE and the network, and to mitigate the DoS attacks, when paging cause is included in the paging request.

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