**3GPP TSG-SA3 Meeting #115AdHoc-e *draft\_S3-241367-r1***

Electronic meeting, online, 15 - 19 April 2024

**Source: Nokia, Nokia Shanghai Bell**

**Title: KI Secure retrieval of 5G system UE Ids and privacy related information**

**Document for: Approval**

**Agenda Item: 5.14**

# 1 Decision/action requested

***It is requested to approve the Key Issue***

# 2 References

[i] 3GPP TR 33.749: "Study on security aspects of enhancement of support for edge computing in the 5G Core (5GC) phase 3"

[ii] 3GPP TS 23.501: "System architecture for the 5G System (5GS); Stage 2"

[iii] 3GPP TR 23.700-49: "Study on Enhancement of support for Edge Computing in 5G Core network - Phase 3"

# 3 Rationale

This pCR introduces a new Key Issue for the study TR 33.749 [x].

# 4 Detailed proposal

**\*\*\*\*** START OF CHANGE **\*\*\*\***

## X.Y Key Issue #Y: Secure retrieval of 5G system UE Ids and privacy related information.

### X.Y.1 Key issue details

This Key issue addresses the security and privacy aspects related to the retrieval of 5G system UE Ids and privacy related information (e.g., UE location) by an Edge Application Server (EAS) and/or Edge Enabler Client (EEC).

Existing Release 18 specifications would allow an EAS (in general an Application Function, AF) to retrieve a 5G UE Id from a network identifier (e.g., IP address, MAC address) to be used in subsequent API calls. More specifically, in TS 23.501 [ii] clause 5.20 describes how NEF may determine the Permanent Identifier of the UE, and how NEF may provide an AF (Application Function) specific UE identifier to the AF by Nnef UEId service.

Without proper security mechanisms in place, Nnef\_UEId service can be abused, so that UE Id may be disclosed to un-authorized entities, enabling them for example to track UEs.

Using the network identifiers such as IP addresses in the requests of 5G identities may also lead to security and privacy issues (e.g., spoofing, location tracking, etc.).

Finally, following the security principle of sharing information on a need-to-know principle, it should be analysed whether and how (i.e. under which circumstances) EAS needs to know the 5G UE Id when requesting a service on the UE behalf.

### X.Y.2 Security threats

Among others, the following threats can be exploited by a potential attacker:

- If user information provided by the EEC is not verified and the EEC is not authorized to use this information, a malicious or compromised EEC or a malicious API consumer can try to execute IP address spoofing attacks. In this case, the EAS obtains an incorrect UE identifier, when the EAS use this incorrect UE identifier to invoke capability APIs specific to UE over EDGE-7, unauthorized information (e.g. UE location) belonging to another UE is exposed to the EAS.

- If the user information provided by EEC does not ensure privacy of the UE, the EAS might be able to deduce information related to the UE that compromise the privacy (e.g., position, UE identity, etc.).

- Replay type of attacks: An attacker that gets to know the 5G UE Id, does not need to involve the UE anymore to request the specific service. This allows an authenticate EAS to request any service it is allowed to, based on current access control solutions, any time it wants.

### X.Y.3 Potential security requirements

The procedure and corresponding services intended to retrieve the 5G system UE Id and privacy related information should be secured to prevent security and privacy breaches caused by compromised or malicious application servers.

The user information provided by the EEC should be verified, to ensure security and privacy during the 5G system UE Id retrieval procedure, and the EEC should be authorized by 5G system to use this information.

**\*\*\*\*** END OF CHANGE **\*\*\*\***