**3GPP TSG-SA3 Meeting #116 *draft\_S3-242567-r1***

Jeju, South Korea, 20th - 24th May 2024 merge of S3-241828, S3-242165, S3-242205

**Source: Nokia, Nokia Shanghai Bell, Huawei, HiSilicon, Ericsson, Samsung, China Unicom.**

**Title: Secure retrieval of 5G system UE Ids and privacy related information in the EDGE**

**Document for: Approval**

**Agenda Item: 5.14**

# 1 Decision/action requested

***In this box give a very clear / short /concise statement of what is wanted.***

# 2 References

[1] 3GPP TR 33.749 “Study on security aspects of enhancement of support for edge computing in the 5G Core (5GC) phase 3”

# 3 Rationale

The rationale for this Key Issue to part of TR 33.749[1] is detailed in the discussion paper S3-241827.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 1st change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 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*.

[x1] 3GPP TS 23.558: "Architecture for enabling Edge Applications".

[x2] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the 1st change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 2nd change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

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

### 5.3.X.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), Edge Enabler Server (EES) and/or Edge Enabler Client (EEC).

Clause 8.6.5 of 3GPP TS 23.558 [x1] defines *UE identifier API* which is used by an EAS or EEC to obtain the identifier of the UE if the EAS or EEC does not have it (e.g. it has not already cached). This identifier, called UE ID (could be the GPSI or the EEL-generated Edge UE ID, defined in clause 7.2.6 of 3GPP TS 23.558 [x1]), is used by the EAS to invoke capability APIs specific to UEs over EDGE-3 and/or EDGE-7 depending on the UE ID type.

The EES uses user information (e.g. IP address) received in the *UE Identifier API* invocation and obtains the UE identifier by interacting with NEF as specified in clause 4.15.10 of 3GPP TS 23.502 [x2]. The EES may utilize the Nnef\_UEId\_Get service (clause 4.15.10 of 3GPP TS 23.502 [x2]) providing the user information provided by the EEC. Without proper security mechanisms in place, *Nnef\_UEId API* services can be abused, so that UE Id may be disclosed to un-authorized entities, enabling them for example to track UEs.

Since user information may be used to determine the 5G system UE Id and consequently privacy related information (e.g., identity, location, etc.), it is needed to ensure that this user information being used in the APIs (*UE Identifier API* and *Nnef\_UEId* ) is trusted, and that the AFs (EAS, EES, ECS) and EEC are authorized to use this user information as parameter(s) in their API invocations.

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’s behalf.

The related security and privacy aspects in the use of the *UE Identifier API* and *Nnef\_UEId API* concern the information provided by the EEC, as well as the behaviour of EDGE Application Functions (AFs), namely EAS and EES. The security threats and corresponding requirements have been split to cover both aspects.

### 5.3.X.2 Security threats

#### 5.3.X.2.1 Threats posed by a malicious EEC

If the User information provided by the EEC is not verified and the EEC is not authorized to use them, a malicious or compromised EEC or a malicious API consumer can try to execute spoofing attacks to learn identifiers of other UEs.

#### 5.3.X.2.2 Threats posed by malicious EAS/EES outside of the operator domain

If the User information provided by the EEC do not ensure the privacy of the UE, EAS/EES can abuse the *UE Identifier API* and/or *Nnef\_UEId* APIs to break UE privacy (e.g., UE identity, location, etc.).

Editor’s note: Whether the abuse of the UE Identifier API and/or Nnef\_UEId APIs can be used to know the network topology is ffs.

### 5.3.X.3 Potential security requirements

#### 5.3.X.3.1 Verification of the user information provided by the EEC

5G system should support a mechanism to verify the user information provided by EEC.

#### 5.3.X.3.2 Protection of the UE privacy

5G system should verify that the EDGE application functions are authorized to retrieve the 5G system UE Id and that the procedures of calling *UE identifier API* and *Nnef\_UEId API* do not compromise the privacy related information.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the 2nd change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*