**3GPP TSG-SA3 Meeting #101-e *draft\_S3-210246-r2***

**e-meeting, 18 - 29 January 2021** Revision of S3-21xxxx

**Source: Huawei, HiSilicon**

**Title: Propose to resolve EN in KI#16**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***Approve this contribution to resolve EN in KI#16 in TR 33.847***

# 2 References

N/A

# 3 Rationale

The contribution proposes to address EN in KI#16:

Editor’s Note: It is FFS whether for Layer-2 relays existing mechanisms (as described above) can be assumed to be sufficient and do not need to be studied further.

In case of Layer-2 relays, the existing mechanism in clause 5.15.9 of TS 23.501 allows the network to indicate the remote not to expose the requested NSSAI information to the UE-to-network relay during initial registration. The subsequent messages between remote and core network are sent only after AS security is established and hence the PDU-session related sensitive information contained in that request is not exposed to the UE-to-Network relay. For the above reasons, the existing mechanisms are sufficient to address the problem in L2 UE-to-network relay. The detailed solution reusing existing mechanism is also illustrated in S3-210245.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* BEGINNING OF CHANGES\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 5.16 Key Issue #16: Privacy protection of PDU session-related parameters for relaying.

## 5.16.1 Key issue details

As part of Key Issue #3 in TR 23.752 [2], SA2 studies layer-2 and layer-3 relays. One of the aspects to be studied as denoted in Key Issue #3 is:

*“- How to support end-to-end requirements between Remote UE and the network via a UE-to-Network Relay, including QoS (such as data rate, reliability, latency) and the handling of PDU Session related attributes (e.g. S-NSSAI, DNN, PDU Session Type and SSC mode).”*

In case of Layer-2 relays, the Remote UE itself is responsible to perform initial registration and set up the PDU session with the Core Network, and the UE-to-Network relay is expected to transparently forward all RRC and NAS messages to/from the network. Although privacy-sensitive slice information from a Remote UE may be revealed to a UE-to-Network relay if requested NSSAI information is included during the initial registration, it is assumed that the inclusion of the requested NSSAI information can be controlled in a similar manner as specified in clause 5.15.9 “Operator-controlled inclusion of NSSAI in Access Stratum Connection Establishment” of TS 23.501 [15]. The subsequent PDU session request is sent only after AS security is established between the UE and the network and hence the privacy sensitive information contained in that request (e.g. requested NSSAI, requested DNN) is not exposed to the UE-to-Network relay.

For Layer-3 relays, the UE-to-Network relay is responsible for setting up a PDU session to the Core Network on behalf of the Remote UE, in order to send the relayed traffic to the Core Network. To facilitate this, the UE-to-Network relay needs to be provided with the PDU session parameters that the Remote UE needs to use for its applications to make sure it connects to the correct DNN, slice, etc. However, if information about PDU session attributes, such as information about a particular slice and/or DNN that a Remote UE wishes to use, is exposed, pre-configured or otherwise made available to UE-to-Network relays or other Remote UEs, this may impose a privacy risk for the Remote UE. In particular, since relay UEs and remote UEs are typically end-user devices, and hence these may not be trusted at the same level as base stations or core network functions.

Several solutions in TR 23.752 [2] (such as solutions #16, #19, #28, #35) that are dealing with preconfiguring PDU session parameter related information to Remote UEs and UE-to-Network relays, dealing with discovery, and dealing with connection setup have already identified an action for SA WG3 to study the privacy concerns that were raised, e.g.:

*“Editor's note: The privacy protection for S-NSSAI information and group information in discovery message and the security of pre-configuring, storing and exposing all this privacy sensitive information with the UE-to-Network relay is FFS and in coordination with SA WG3.”*

*“NOTE: The privacy aspects of preconfiguring slicing information in UE-to-Network relays need to be coordinated with SA WG3.”*

*“NOTE 1: The privacy aspects of transporting PDU session parameters using an unsecured PC5 Direct Communication Request message need to be coordinated with SA WG3.”*

This key issue is to study the privacy issues related to the pre-configuration of PDU session parameter related information to UE-to-Network relays and Remote UEs, and privacy issues related to exposing PDU session parameter related information during discovery and/or connection setup messages.

Editor’s Note: It is FFS whether for Layer-2 relays existing mechanisms (as described above) can be assumed to be sufficient for ProSe discovery and PC5 connection setup scenarios and do not need to be studied further.

NOTE: The existing mechanisms are sufficient to address the security requirement of this KI for communication between remote UE and core network via L2 UE-to-Network relay.

### 5.16.2 Security threats

Information related to slices and DNNs that a UE uses or wishes to use for its relay operation (i.e. for the purpose of relay selection and/or setting up a relayed connection to the network), is privacy sensitive as it may reveal that a UE belongs a special subscription group, e.g. police/law enforcement/customs, or is linked e.g. to a healthcare facility. This leads to the following threats:

- Exposure of this information in the clear (e.g. in discovery or connection setup messages) enable eavesdroppers to perform privacy attacks on Remote UEs or UE-to-Network relays.

### 5.16.3 Potential security requirements

The 5G System shall provide a means to mitigate tracing and tracking privacy attacks on Remote UEs based on potential exposure of slicing information, DNN information, and other PDU session related persistent information.

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