3GPP TSG-SA WG3 Meeting #100-bis-e S3-202632

e-meeting, October 12 - 16 2020 *revision of S3-*

**Source: Philips International B.V.**

**Title: New Key Issue on privacy of PDU session parameters.**

**Document for: Approval**

**Agenda Item: 2.9 Study on Security Aspects of Enhancement for Proximity Based Services in 5GS.**

# 1 Decision/action requested

***This contribution proposes a new KI for*** ***TR 33.847.***

# 2 References

[1] 3GPP TR 23.752 V0.5.0 Study on system enhancement for Proximity based Services (ProSe) in the 5G System (5GS) (Release 17)

# 3 Rationale

TR 23.752 [1] describes the following aspect to be studied as part of Key Issue #3: Support of UE-to-Network Relay:

*- 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).*

As identified earlier by SA3 (e.g. see KI#6 in TR 33.813), PDU session related attributes, such as slice information and DNN, are privacy sensitive as they may reveal that a UE belongs e.g. to police/law enforcement.

In case of 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. 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. If information about PDU session attributes, such as information about some slice and/or DNN that a Remote UE wishes to use, is exposed, pre-configured or otherwise made available to a UE-to-Network relay, this imposes a privacy risk for the Remote UE.

NOTE: in case of Layer-2 relays the Remote UE itself is responsible to set up the PDU session with the Core Network without requiring the UE-to-Network relay to set up a PDU session on behalf of the Remote UE, so this is much less of an issue.

In TR 23.752 several solutions are captured on how to handle PDU session parameters for Layer-3 UE-to-Network Relays, i.e.:

1. In solutions #16 and #35, it is proposed to provision both the Remote UE and the UE-to-Network Relay with the following discovery parameters:

“The associated PDU session parameters (S-NSSAI, DNN, SSC mode, etc.) to be used for relayed traffic for each UE-to-Network Relay Service Code or Service ID (Only for Layer 3 UE-to-Network Relay)”

1. In solution #19, it is proposed to include PDU session related information on e.g. network slices and DNN in discovery announce and discovery request/response messages.
2. In solution #28, it is proposed to use Relay Service Codes associated with network slicing information, e.g. S-NSSAI, for both discovery announce and discovery request/response messages. And furthermore, for setting up a connection between the Remote UE and a selected UE-to-Network relay, it proposes to include the PDU session requirements (e.g. S-NSSAI (together with PLMN ID), DNN, PDU Session Type, SSC mode) in the Direct Communication Request message during the PC5 connection establishment procedure

Several of these solutions have identified an action for SA3, 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.”

Therefore, we think it is important to introduce a corresponding key issue for TR 33.847.

# 4 Detailed proposal

It is proposed to add the following text to TR 33.847.

\*\*\* BEGIN OF CHANGES \*\*\*

## 5.x Key Issue #x: Privacy protection of PDU session related parameters for relaying.

## 5.x.1 Key issue details

As part of Key Issue #3 in TR 23.752, 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-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. 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. If information about PDU session attributes, such as information about some 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 imposes a privacy risk for the Remote UE. and remote UEs

Several solutions in TR 23.752 [1] (such as solutions #16, #19, #28, #35) that are dealing with preconfiguring PDU session parameters to Remote UEs and UE-to-Network relays, dealing with discovery, and dealing with connection setup have already identified an action for SA WG3, 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 pre-configuration of PDU session parameter information to UE-to-Network relays and Remote UEs, and privacy issues related to exposing PDU session parameters during discovery and/or connection setup messages.

Editor’s Note: for now, the privacy threats have only been identified for layer-3 relay architecture. It is FFS whether or not this key issue applies to layer-2 relay architecture. Hence, whether or not this key issue needs to be taken forward (i.e. for evaluation or normative work) in SA3 is contingent on SA2’s decision which of the respective relay architectures to which this key issue applies (i.e. layer-2, layer-3 or both) are chosen to move to normative phase.

### 5.x.2 Security threats

- Exposure of information related to slices and DNNs that a UE uses or wishes to use for its relay operation, is privacy sensitive as it may reveal that a UE e.g. belongs to police/law enforcement, or is linked to a healthcare facility.

- Pre-configuring a large set of UE-to-Network relay devices or Remote UE devices with relatively static information that can be associated to slicing and/or DNN information (such as relay service codes) may enable these devices to perform various privacy attacks including tracing and tracking of identities of Remote UEs by linking them to the relatively static information.

### 5.x.3 Potential security requirements

The 5G System shall provide a means to mitigate slicing, DNN and other PDU session related information to be used for tracing and tracking of Remote UEs.

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