3GPP TSG-SA WG3 Meeting #100-bis-e S3-203318

e-meeting, October 12 - 16 2020

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

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

**Document for: Approval**

**Agenda Item: 5.9 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)

[2] 3GPP TS 23.501: “System Architecture for the 5G System”

# 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-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 UEAlthough privacy sensitive slice information from a Remote UE may be revealed to a UE-to-Network relay if requested NSSAI information is included during initial registration, it is assumed that the inclusion of the requested NSSAI information can be controlled in a similar manner as specified in Section 5.15.9 “Operator-controlled inclusion of NSSAI in Access Stratum Connection Establishment” of TS 23.501 [2], given that the UE-to-Network relay is expected to transparently forward all RRC and NAS messages to/from the network.

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. 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.

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 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.”

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 in Change 1 and add the reference in Change 2 to TR 33.847.

\*\*\* BEGIN OF CHANGES 1\*\*\*

## 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 [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 Section 5.15.9 “Operator-controlled inclusion of NSSAI in Access Stratum Connection Establishment” of TS 23.501 [ZZ]. 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. For Layer-2 relays existing mechanisms (as described above) are assumed to be sufficient and do not need to be studied.

### 5.x.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.- Providing UE-to-Network relay devices or Remote UE devices (e.g. during connection setup or during pre-configuration) with persistent and/or 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 or persistent information.

### 5.x.3 Potential security requirements

The 5G System shall provide a means to mitigate tracing and tracking privacy attacks on Remote UEs by analysing and collating slicing information, DNN information, and other PDU session related persistent information by an attacker.

\*\*\* END OF CHANGES 1 \*\*\*

\*\*\* BEGIN OF CHANGES 2\*\*\*

# 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*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 23.752: "Study on system enhancement for Proximity based Services (ProSe) in the 5G System (5GS)".

[3] 3GPP TS 22.278: "Service requirements for the Evolved Packet System (EPS)".

[4] 3GPP TS 22.261: "Service requirements for the 5G system; Stage 1".

[5] 3GPP TS 23.303: "Proximity-based services (ProSe); Stage 2".

[6] 3GPP TS 33.303: "Proximity-based Services (ProSe); Security aspects".

[7] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[8] 3GPP TS 33.536: "Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services".

[9] 3GPP TS 23.287: "Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services".

[10] 3GPP TS 23.502: "Procedures for the 5G System (5GS); Stage 2".

[11] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[ZZ] 3GPP TS 23.501: “System Architecture for the 5G System”

\*\*\* END OF CHANGES 2 \*\*\*