**3GPP TSG-SA3 Meeting #101-e *draft\_S3-210245-r2***

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

**Source: Huawei, HiSilicon**

**Title: A solution to protect PDU session related parameters for L2 relay**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***Approve this contribution to provide new solution to KI#16 in TR 33.847***

# 2 References

N/A

# 3 Rationale

This solution addresses the Key Issue #16: Privacy protection of PDU session-related parameter for relaying. The UE-to-Network relay is responsible to transparently convey all the NAS and AS messages for the initial registration and PDU session establishment between the core network and the remote UE. This solution proposes to use the existing mechanism in order to protect the PDU session-related parameters.

# 4 Detailed proposal

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

## 6.x Solution #x: Protecting PDU session-related parameters for L2 relay with existing mechanism.

### 6.x.1 Solution overview

This solution addresses Key Issue #16: Privacy protection of PDU session-related parameter for relaying. In the L2 UE-to-network relay scenario, the PDU session-related parameters in the communications after initial registration between remote UE and core network transparently pass the relay with protected AS and NAS security. Hence only privacy sensitive PDU session-related parameters during initial registration are needed to be protected, specifically speaking, the NSSAI information in the initial registration messages.

This solution proposes to reuse the existing mechanism in order to protect the PDU session-related parameters that may expose to the UE-to-network relay during initial registration.

### 6.x.2 Solution details

Based on the threat mentioned in Key Issue #16, exposing slice and DNN information may violate privacy about a UE’s special subscription group belongings. The only privacy sensitive PDU session-related parameter that may expose to the L2 UE-to-network relay is the NSSAI information in the initial registration message as the subsequent parameters are covered by the protected AS and NAS information. This solution proposes to reuse the existing mechanism to protect PDU session-related parameters for L2 relay:

If the operator decides to protect the privacy of PDU session-related parameter(s) (i.e. slice information) for L2 relay, AMF shall provide the remote UE an ‘Access Stratum Connection Establishment NSSAI Inclusion Mode’ parameter in the Registration Accept message during the registration procedure. This parameter indicates the Remote UE to not include any NSSAI in the Access Stratum (AS), as specified in the mode (d) in 23.501 [15] clause 5.15.9. The remote UE shall by default not to provide NSSAI in the AS under UE-to-network relay scenario unless it has been provided with an indication to operate in other modes as specified in 23.501[15] clause 5.15.9.

The subsequent communications between remote UE and the core network are sent with AS and NAS security, thus the PDU session-related parameters (e.g. requested NSSAI, requested DNN) are prevented to be read by the UE-to-network relay.

### 6.x.3 Evaluation

The L2 UE-to-network relay doesn’t introduce any new security vulnerabilities related to Key Issue #16 during the communication between remote UE and core network via L2 UE-to-Network relay and the existing mechanism is capable to mitigate tracing and tracking privacy attacks on the remote UE caused by exposing PDU session-related parameters.

Editor’s Note: How to prevent PDU-session-related parameter exposure during discovery and PC5 connection, and corresponding evaluation are FFS.

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