**3GPP TSG-****SA3 Meeting #101-e *S3-210543***

**e-meeting, January 18 - 29 2021**

**Source: Philips International B.V**

**Title: Solution** **to mitigate privacy issues of relay service codes and PDU parameters for L3 UE-to-NW relays**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***We request SA3 to consider including this solution for KI#11 and KI#16 of TR 33.847.***

# 2 Rationale

In section 8 (conclusion) of the SA2 TR 23.752 Study on system enhancement for Proximity based Services (ProSe), it states:

[For KI#3 Support for UE-to-Network relay:]

*For L3 Relay discovery procedure, it is proposed to adopt the standalone discovery procedure (i.e. Model A and Model B), and, the additional information advertised by Relay UE as described in Sol#28 as the basis for normative work*

[For KI#8 Support of PC5 Service Authorization and Policy/Parameter Provisioning]

*Solution #35 is selected for normative work for UE-to-Network Relay aspect and can be further updated based on the conclusion for KI#3.*

In Solution #28 Relay Service Codes are used during discovery of UE-to-Network Relays. Given that Remote UEs should be able to operate out-of-coverage, the Relay Service Codes are expected to be quite static and have a fairly long lifetime (i.e. probably more in terms of hours rather than in seconds). As described in Key Issue #11 of TR 33.847 this introduces privacy risks.

In addition, as described in Solution #28 and in further detail in solution #35 (and similarly also in 16), in case of Layer-3 relaying each Relay Service Code is associated to a set of PDU session parameters (S-NSSAI, DNN, etc.) to be used for the relayed traffic. The Remote UEs and UE-to-Network Relays receive this association during the Service Authorization and Provisioning procedure (i.e. solution #35). As described in Key Issue #16 of TR 33.847 exposing PDU session parameters such as S-NSSAI and DNN, or the representation of these parameters (i.e. through Relay Service Codes) in discovery messages and/or connection setup messages introduces additional privacy risks.

This solution mitigates the privacy risks related to the use of Relay Service Codes by making sure that adversaries (which may include other Remote UEs and UE-to-Network Relays) cannot correlate the use of a Relay Service Code to a particular Remote UE or UE-to-Network Relay for a prolonged period of time, and cannot easily correlate the Relay Service Codes to a set of PDU session parameters.

# 3 Detailed proposal

We ask SA3 to kindly consider including the following solution in TR 33.847 to address key issues #11 and #16.

**\*\*\*\* START OF CHANGE 1 \*\*\*\***

## 6.X Solution #X: Mitigating privacy issues of relay service codes and PDU parameters for L3 UE-to-NW relays.

### 6.X.1 Introduction

This solution addresses key issues #11 (UE identity protection during ProSe discovery) and #16 (Privacy protection of PDU session-related parameters for relaying) for Layer-3 UE-to-Network Relay connections, in particular it addresses the privacy issues related the use of relay service codes and their associated PDU session parameters during discovery and connection setup.

This solution builds on top of solutions for key issues #4 and #9 (such as solution #1, #6, #10, #15, …) by adding a mechanism for updating relay service codes for Remote UEs and UE-to-Network Relays to mitigate privacy issues.

NOTE 1: how exactly this mechanism is to be integrated with solutions for key issues #4 and #9 depends on which solution is selected as baseline for normative work, and details can be defined during normative phase.

It further builds on solution #35 of TR 23.752, with the difference that UE to Network relay does not get provisioned by the PCF with PDU session parameters associated to each Relay Service Code during initial authorization and provisioning step. Instead the PDU session parameters are provided by the network only to the single UE-to-Network relay that is selected by the Remote UE and only after the network has verified the Remote UE and the selected Relay UE are authorized to set up a relay connection for the given Relay Service Code, and not to other UE-to-Network relays in vicinity for additional privacy protection.

In this solution, in line with solution #35 of TR 23.752, it is assumed that the Relay Service Codes are provisioned to the Remote UE and UE-to-Network Relay by the PCF. The PCF is assumed tobe the same for both the Remote UE and the UE-to-Network relay. It is further assumed that the allocation of (new) Relay Service Codes may be done by the PCF itself or may be done in cooperation with the DDNMF.

NOTE 2: The details on whether the PCF or the DDNMF allocate (new) Relay Service Codes and how the PCF and the DDNMF may cooperate are left for SA2 to decide, and are not further elaborated in this solution.

Editor’s Note: This solution may need to be updated when SA2 has concluded which entity allocates the Relay Service Codes.

It is also assumed that the AMF and the AUSF for the Remote UE and the UE-to-Network relay are the same. For simplicity the steps related to AUSF, UDM and PKMF are not described separately (the details depend on the respective solutions for key issue #4 and #9).

### 6.X.2 Solution Details

The procedure for updating relay service codes to mitigate privacy issues is depicted in Figure 6.X.2-1.



Figure 6.1.X-1: Procedural call flow for updating relay service codes to mitigate privacy issues

**Step 0a/b:** Remote UE gets authorized by the PCF [See NOTE 2]) for relay discovery and connection setup, and is provisioned with a set of Relay Service Codes each associated with a set of PDU session parameters (S-NSSAI, DNN, etc.). Furthermore, the Remote UE gets provisioned with security material for discovery (e.g. discovery key) and for relay connections (e.g. Krelay, PRUK, REAR key), possibly with security material to allow direct communication over PC5 (e.g. KNRP).

Similarly, UE-to-Network Relay gets authorized by the PCF [See NOTE 2] for relay discovery and connection setup, and is provisioned with its supported Relay Service Codes, and security material for discovery (e.g. discovery key). In this solution, **t**he UE-to-Network relay does not get provisioned with a set of PDU session parameters (S-NSSAI, DNN, etc.) for each Relay Service Code, and the UE-to-Network relay should be provisioned with a set of spare Relay Service Codes.

NOTE 3: For step 0a and 0b the Remote UE and the UE-to-Network relay are assumed to be in coverage. For subsequent steps 1 through 9, the Remote UE is assumed to be out of coverage, and the UE-to-Network relay is assumed to be in coverage.

**Step 1:** Remote UE discovers the UE-to-Network Relay through model A or B open or restricted discovery procedure by using one (or more) of the Relay Service Codes provisioned to the Remote UE. In this solution, the UE-to-Network relay should provide its SUCI or 5G-GUTI to the Remote UE during discovery.

**Step 2:** Remote UE sends a Direct communication request to the selected relay to establish a secure PC5 unicast link for relaying. In this solution, the message includes at least the Relay Service Code, the SUCI or 5G-GUTI of the Remote UE and the SUCI or 5G-GUTI of the selected UE-to-Network relay, whereby each of these identities are encrypted to prevent an eavesdropper to link these identities to the Remote UE. The key used for encryption is a key derived from the latest KAUSF of the Remote UE, possibly in conjunction with the security material for relay connection as received in step 0a (e.g. Krelay, PRUK, REAR key).

Editor’s Note: Need to add more details on the derivation of the encryption key used for protection of the relay service code and the other proposed arguments in the Direct Communication Request message, and how to protect the Direct Communication Request against replay protection.

**Step 3:** UE-to-Network relay issues a NAS Relay Authorization Request/Key Request to the AMF. In this solution, the UE-to-Network relay includes the encrypted Relay Service Code and SUCI/5G-GUTI of the Remote UE and the selected UE-to-Network relay in the NAS Relay Authorization Request/Key Request.

**Step 4:** The AMF together with the AUSF/UDM/PKMF authenticate the Remote UE and verify if the Remote UE and the selected Relay UE are authorized to set up a relay connection for the given relay service code and generate the respective key material for the remote UE and selected UE-to-Network relay. Details of this procedure can be found in the respective solution for key issue #4 and #9.

**Step 5:** In this solution, after it has been verified that the relay connection is authorized for the respective relay service code in step 4, the AMF performs the following two additional steps:

1. AMF retrieves from the PCF the PDU session parameters associated with the requested Relay Service Code (to be returned to the UE-to-Network relay).
2. AMF requests the PCF to provide a different Relay Service Code [See NOTE 2] (e.g. one of the spare Relay Service Codes or a new Relay Service Code) for the Remote UE to replace the Relay Service Code that was used during connection setup, and may also prepare a fresh 5G-GUTI for the Remote UE and a new layer-2 ID to use for subsequent discovery messages over PC5. The PCF should encrypt this payload for the Remote UE in a manner that it cannot be decrypted by the UE-to-Network relay (e.g. using a key derived from the latest KAUSF of the Remote UE).

**Step 6:** AMF adds the PDU session parameters for the requested Relay Service Code (as received in step 5a) and the received encrypted payload from the PCF for the Remote UE (as received in step 5b) to the NAS Relay Authorization Response/Key Response message to be sent back to the UE-to-Network Relay.

**Step 7a/b:** UE-to-Network relay uses the information received in step 6 to complete the secure link setup between the Remote UE andthe UE-to-Network relay. In this solution, the UE-to-Network relay adds the encrypted payload for the Remote UE received from the PCF (which includes the new Relay Service Code) to the Direct Security Mode Command as additional parameter.

**Step 8:** In this solution, the Remote UE updates its list of relay service codes based on theencrypted PCF payload it received in the Direct Security Mode command. The Remote UE will use the different relay service code and the received different layer-2 identifier in subsequent discovery and/or Direct Connection setup requests.

**Step 9:** During or after secure connection setup over PC5 is completed, the UE-to-Network relay configures/initiates the PDU session used for relaying with the PDU session parameters (received in step 6) related to the Relay Service Code..

**Step 10:** The UE-to-Network relay can now now start relaying data from the Remote UE to the network via the selected UE-to-Network relay.

NOTE 4:At some point in time, the UE-to-Network relays and other Remote UEs may need to be updated as well (e.g. after all spare relay service codes have been used). This can be done independently using the authorization and provisioning procedure as described in steps 0a and 0b.

NOTE 5: during the time the Remote UE is connected to the UE-to-Network relay, the Remote UE and UE-to-Network relay should run the Link Identifier Update procedure as defined in TS 33.536 to change the L2 identifiers of the UEs involved in the PC5 unicast link

### 6.X.3 Evaluation

TBD.

**\*\*\*\* END OF CHANGE 1 \*\*\*\***