**3GPP TSG-****SA3 Meeting #103-e *S3-212114***

**e-meeting, 17 – 28 May 2021**

**Source: Philips International B.V**

**Title: Update to solution #32**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***We request SA3 to consider incorporating the suggested updates to solution #32 of TR 33.847.***

# 2 Rationale

The following two Editor’s notes in steps 3 and 4a are interrelated:

Editor’s Note: It is FFS how the U2N relay can check if the nonce is valid if it cannot verify the message integrity.

Editor’s Note: it is FFS which core network entity keeps track of the used nonces.

Both editor’s notes relate to the prevention of replay attacks, i.e. the U2N relay or the Core Network need to check if the Direct Communication Request received from the Remote UE uses a recently issued and non-duplicated nonce from the U2N relay, otherwise the message may be a replayed message. The current text is confusing since the nonce is checked in both step 3 and step 4a, once by the U2N relay, and once by the Core Network. During the discussion it was implied that also the U2N relay would then also need to be able to verify the message integrity, resulting in the Editor’s note in step 3. And of course if the core network would need to check duplication of the nonces, it would need to keep track of those nonces in the core network, hence leading to the Editor’s Note in step 4a. But actually the core network does not need to check the nonces again if they are already verified by the U2N relay. In fact, the two verification steps (i.e. verification of the nonce being replayed and message integrity check) can be done separately and distributed amongst the two entities, i.e. the U2N relay can check if its nonce is used properly and not re-used, and the Core Network can check if the message integrity is correct. If one of these verification checks fails, then the direct connection setup request will fail.

This implies that the Editor’s Note in step 3 can be removed, i.e. the U2N relay can check the nonce without verifying its integrity, since the integrity will be checked by the core network anyway, and also the Editor’s note in step 4 can be removed, i.e. if the U2N relay checks for correct use of its nonce and if is replayed or not, then the core network does not need to do that again. This is clarified in the proposed changes.

Furthermore, it is clarified that the new values to be used for the Relay Service Codes can be seen as a kind of aliases, that can be used instead of the original value of the Relay Service Code, but that are e.g. still associated with the same PDU session parameters and authorization policies.

Furthermore, in step 8 some spurious left-over about layer-2 identifiers from a previous version of the solution was removed.

# 3 Detailed proposal

We ask SA3 to kindly consider including the following change to TR 33.847 to address the above mentioned editor’s notes in solution #32 and to provide some clarifications.

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

## Solution #32: Mitigating privacy issues of relay service codes and PDU parameters for L3 UE-to-NW relays.

### 6.32.1 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 the values of the relay service codes for Remote UEs and UE-to-Network Relays to mitigate privacy issues. These values can be seen as a kind of aliases, that can be used instead of the original value of the Relay Service Code, but that are e.g. still associated with the same PDU session parameters and authorization policies.

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 to be the same for both the Remote UE and the UE-to-Network relay. It is further assumed that the allocation of new values (i.e. aliases) for the 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 values (i.e. aliases) for the 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).

### 6.32.2 Solution Details

The procedure for updating relay service codes to mitigate privacy issues is depicted in Figure 6.32.2-1.



Figure 6.32.2-1: 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 long term security material for ProSe discovery (e.g. root discovery key such as PSDK as defined in TS 33.303) and for relay connections (e.g. root relay connection key, such as PRUK as defined in TS 33.303), possibly with security material to allow direct communication over PC5 (e.g. the long term credentials in TS 33.536 that form the root of the security of the PC5 unicast link to derive 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 Code values.

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 can 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 (i.e. ID\_Relay) and a fresh nonce N\_Relay 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 SUCI or 5G-GUTI of the Remote UE (i.e. ID\_Remote), and an encrypted Relay Service Code (RSC) together with the SUCI or 5G-GUTI of the selected UE-to-Network relay (i.e. ID\_Relay), the nonce N\_Relay received from the UE-to-Network relay, a fresh nonce N\_Remote generated by the Remote UE, and a Message Authentication Code for integrity protection of each of these parameters. The Relay Service Code and the identity of the selected UE-to-Network relay are encrypted (together) to prevent an eavesdropper to link these identities to the Remote UE, and to ensure that only the UE-to-Network relay that is selected by the Remote UE will receive the PDU session parameters from the network.

The key (K\_enc) used for encryption can be derived from the latest KAUSF of the Remote UE or from the long term security material for relay connection as received in step 0a (e.g. PRUK, using nonces N\_Relay and N\_Remote as additional input to the key derivation function.

NOTE 4: the selection of which key to use, and further details on the key derivation are left for normative phase, as they depend on which solution(s) are chosen for key issues #4 and #9. See also NOTE 1.

Editor’s Note: Need to add more details on the derivation of the encryption key used for protection of the relay service code.

The Message Authentication Code may be calculated as follows:

 MAC (K\_int, ID\_Remote | N\_Relay | N\_Remote | ENCRYPT(K\_enc, RSC | ID\_Relay) )

**Step 3a:** Upon receiving the Direct Communication request, the UE-to-Network relay the relay verifies the presence of its nonce N\_Relay. The UE-to-Network relay also verifies the used nonce against replay attacks.

**Step 3b:** If the nonce is valid and not re-used, the UE-to-Network relay issues a NAS Relay Authorization Request/Key Request to the AMF. In this solution, the UE-to-Network relay includes ID\_Remote, the encrypted Relay Service Code together with SUCI/5G-GUTI of the selected UE-to-Network relay (i.e. ENCRYPT(RSC | ID\_Relay)), the nonces and the Message Authentication Code received in step 2 in the NAS Relay Authorization Request/Key Request.

**Step 4a:** The AMF together with the AUSF/UDM/PKMF derive K\_enc and K\_int based on ID\_Remote and the received nonces, and then verify the integrity of message fields and decrypt to obtain the RSC and ID\_Relay, and verify if the ID\_Relay matches the identity of the UE-to-Network Relay from which the message was received.

**Step 4b:** 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 (RSC) 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 value serving as an alias for the original Relay Service Code [See NOTE 2] for the Remote UE to be used instead of the Relay Service Code value that was used during discovery and connection setup. We distinguish two options here:
* Option 1: the alias value is chosen to be one of the values in the set of spare Relay Service Code values that are already provisioned to UE-to-Network relays in step 0b. In this case, all UE-to-Network relays that are already provisioned with this spare Relay Service Code value can be discovered and used by the Remote UE without any update procedures of the UE-to-Network relays involved, and without affecting the discovery and connection setup of other Remote UEs that are still using the original Relay Service Code.
* Option 2: the alias value is chosen to be a new value for the respective Relay Service Code. In this case, all involved UE-to-Network relays using the respective Relay Service Code need to be provided with the new alias for the respective Relay Service Code. The provisioning procedure as described in step 0b can be used for providing the alias to the UE-to-Network relays, which can add the provided alias to a list of aliases for the respective Relay Service Code.

The PCF should encrypt this Relay Service Code alias 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).

NOTE 5: The PCF can also prepare a fresh 5G-GUTI for the Remote UE to use for subsequent discovery and connection setup over PC5 in this step and include it as well in the response for further privacy protection.

**Step 6:** AMF adds the PDU session parameters for the requested Relay Service Code (as received in step 5a) and the encrypted Relay Service Code alias received 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 Relay Service Code alias received for the Remote UE ) to the Direct Security Mode Command as additional parameter.

**Step 8:** In this solution, the Remote UE updates its list of relay service codes and the aliases based on theencrypted Relay Service Code alias it received in the Direct Security Mode command. The Remote UE will use the received alias for the Relay Service Code 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 start relaying data from the Remote UE to the network via the selected UE-to-Network relay.

NOTE 6:At some point in time, the UE-to-Network relays and other Remote UEs may need to be updated as well (e.g. to renew the authorization policies for relay service codes or after all spare relay service code values have been used). This can be done independently using the authorization and provisioning procedure as described in steps 0a and 0b.

NOTE 7: 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

### 6.32.3 Evaluation

TBD.

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