**3GPP TSG-****SA3 Meeting #104-e *S3-212809r1***

**e-meeting, 16 – 27 August2021**

**Source: Philips International B.V**

**Title: Update and evaluation of 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

Solution 32 has two remaining editor’s notes. In addition, some evaluation comments were made stating some of the restrictions of the current version of the solution. In this pCR we propose to address the editor’s notes and address the issues/restrictions that were stated in the current evaluation, and in addition provide further evaluation.

The first Editor’s Note states:

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

In the current version of TS 23.304 of the technical specification for 5G ProSe it is clear that the Relay Service Codes are allocated by the PCF and do not involve the DDNMF. Hence, the text is futher clarified to reflect this.

The second Editor’s Note states:

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

To address this Editor’s note we provided further details on how to use the Kausf to derive a key and how the AMF selects the AUSF and works together with the AUSF to decrypt the relay service code.

By adding the details on how the Remote UE’s AUSF and PCF can be used by the UE-to-Network relay’s AMF also addresses the evaluation comment that was given that the solution does not work if different AUSF and PCF are used. Thus, the statements related to this restriction were removed from the description.

The evaluation comments also mention that the solution is not aligned with SA2’s architecture because the solution assumes that the association between relay service codes and PDU session parameters is not provisioned to the UE-to-Network relay during initial authorization and configuration, whereas in SA2 architecture it does assume that this association is provisioned. In this pCR we propose to address this comment by introducing an alternative solution (ALTERNATIVE 1) which is aligned with SA2’s architecture whereby the association is provisioned during initial authorization and configuration. However, we kept the original solution as ALTERNATIVE 2 due to its higher privacy guarantees and have added stronger statements that if SA3 wants to propose this ALTERNATIVE 2 as solution for KI#16 that further alignment with SA2 is needed. In our perspective, it is the role of SA3 to ensure that the system architecture is secure, and thus, we think that it is worth discussing whether we should actively engage with SA2 to ensure a more secure system.

Furthermore, the solution has been clarified on how the layer-2 identifiers are used between subsequent messages to provide additional privacy protection. Also, further evalution details have been provided.

# 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 CHANGES \*\*\*\***

## 6.32 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, whereby in the solution description below we identify two different solution alternatives with different levels of protection and different levels of alignment:

*ALTERNATIVE 1*: As in solution #35, each UE-to-Network relay gets provisioned by the PCF with PDU session parameters associated with the supported Relay Service Codes during the initial authorization and provisioning step.

*ALTERNATIVE 2*: As solution #35, but with the difference that UE to Network relay does not get provisioned by the PCF with PDU session parameters associated with the supported Relay Service Codes during the 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. This alternative therefore would require alignment with SA2.

In both alternatives, 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. It is further assumed that the allocation of new values (i.e. aliases) for the Relay Service Codes is done by the PCF (or may be done in cooperation with the DDNMF).

NOTE 2: The details on how the PCF of the Remote UE and the UE-to-Network relay cooperate in the assignment and provisioning of the relay service codes, e.g. in a roaming scenario, are left for SA2 to decide. Also, the details on whether the DDNMF needs to be involved in the allocation of new values (i.e. aliases) for the Relay Service Codes or if this is sole responsibility of the PCF are left for SA2 to decide and are not further elaborated in this solution. Alignment with SA2 on these aspects can be done during SA3 normative phase.

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 0:** Remote UE gets authorized by the PCF 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 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 *ALTERNATIVE 1* of this solution, **t**he UE-to-Network relay does get provisioned with a set of PDU session parameters (S-NSSAI, DNN, etc.) for each Relay Service Code. In *ALTERNATIVE 2* of 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. In both alternatives of this solution, the UE-to-Network relay should further be provisioned with a set of spare Relay Service Code values.

NOTE 3: For step 0 the Remote UE and the UE-to-Network relay are assumed to be in coverage. For subsequent steps 1 through 10, 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 UE-to-Network relay 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.

For this solution it is assumed that for security protection of the discovery messages a solution that meets the requirements for restricted discovery in KI#1 is used. This implies that only UE-to-Network relays that have the respective key to decrypt the discovery message from the Remote UE can decrypt the Relay Service Code. For further privacy protection in line with KI#11, the Remote UE must frequently change its layer-2 identifier used for model B solicitation messages, preferably using a different layer-2 identifier for each subsequent solicitation message. The Remote UE should also randomly pause between sending two subsequent messages and frequently change the keys to protect the messages, and if possible also interchange with soliciting other Relay Service Codes.

**Step 2:** Remote UE sends a Direct Communication Request to the selected relay to establish a secure PC5 unicast link for relaying. The Remote UE shall select a different layer-2 ID for the Direct Communication Request from the layer-2 ID that was used in previous model B solicitation messages. In this solution, the Direct Communication Request message includes at least:

* the SUCI or 5G-GUTI of the Remote UE (i.e. ID\_Remote),
* an encrypted value representing the Relay Service Code (RSC) concatenated 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,
* 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:

* in case of *ALTERNATIVE 1:* the decrypted Relay Service Code in order to retrieve the PDU session parameters
* in case of *ALTERNATIVE 2*: the PDU session parameters from the network.

The keys K\_enc and K\_int are used to ensure the confidentiality and for integrity of the message. These keys can be derived from the latest KAUSF of the Remote UE by using the key derivation function in TS 33.220 and a unique distinguishing FC identifier. These keys could also be derived from the long term security material for relay connection as received in step 0a (e.g. PRUK). To ensure replay protectation, other inputs to the key derivation function can include nonces N\_Relay and N\_Remote. Another input can be a counter so that the receiving party, i.e., the AUSF, can check that a malicious node is not replaying messages from the remote UE.

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.

The Message Authentication Code may be calculated as follows:

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

where “|” indicates concatenation.

**Step 3a:** Upon receiving the Direct Communication request, the UE-to-Network relay verifies the presence of its nonce N\_Relay, and verifies its freshness.

**Step 3b:** If the nonce is valid, fresh and not repeated in a short timeframe, 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 value of the Relay Service Code concatenated 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 selects the AUSF/UDM/PKMF based on ID\_Remote (i.e. SUCI/5G-GUTI of the Remote UE) and then together with the AUSF/UDM/PKMF derive K\_enc and K\_int based on ID\_Remote and the received nonces, and then decrypt and verify the integrity of the message fields. To this end the AMF may need to send the information received in the NAS Relay Authorization Request/Key Request to the respective AUSF, which after verifying the integrity and decrypting the value, returns the decrypted RSC and ID\_Relay to the AMF. Subsequently, the AMF can verify if the ID\_Relay matches the identity of the UE-to-Network Relay from which the message was received. Otherwise, the AMF breaks off the procedure if these do not match.

**Step 4b:** The AMF together with the selected 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 additional steps:

1. AMF selects the PCF based on ID\_Remote and request 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 (in this case initiated by the network, e.g. through UE configuration update procedure) 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 as in Step 2).

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.

The following step only gets executed in case of *ALTERNATIVE 2*:

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).

**Step 6:** In case of *ALTERNATIVE 1:*TheAMF adds the decrypted Relay Service Code and the encrypted and integrity protected new Relay Service Code alias received from the PCF for the Remote UE (as received in step 5a) to the NAS Relay Authorization Response/Key Response message to be sent back to the UE-to-Network Relay

In case of *ALTERNATIVE 2*: TheAMF adds the PDU session parameters for the requested Relay Service Code (as received in step 5b) and the encrypted and integrity protected new Relay Service Code alias received from the PCF for the Remote UE (as received in step 5a) 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

This solution mitigates the privacy issues in key issue #16 in the following ways:

In case of discovery: the privacy issues in key issue #16 are mitigated by mandating a frequent change in layer-2 identifiers used during discovery, e.g. for each subsequent Model B solicitation request, the Remote UE cannot easily be traced using a requested Relay Service Code, in particular if it is not the only Relay Service Code it solicitates for and randomly pauses between sending subsequent solicitation messages to avoid any pattern detection. Furthermore, since the layer-2 identifiers are also changed before sending a subsequent Direct Connection Request, whereby the requested Relay Service Code is encrypted (using a different key than used during discovery), the discovery process cannot be linked to the connection setup process.

* In case of ALTERNATIVE 1, during discovery a UE-to-Network relay can associate a solicited Relay Service Code with the pre-provisioned PDU session parameters, and hence has access to some privacy specific information of the Remote UE if the UE-to-Network relay supports the respective Relay Service Code. This implies that for the UE-to-Network relays in vicinity of the Remote UE that support the respective Relay Service Code and can decrypt the respective discovery solicitation message the security requirements of key issue#16 can temporarily not be met. However, given the frequent change in layer-2 identifiers and the change to the Relay Service Code to a new alias after subsequent connection setup, this may be an acceptable risk.
* In case of ALTERNATIVE 2, during discovery a UE-to-Network relay cannot associate a solicited Relay Service Code with pre-provisioned PDU session parameters. Hence, the security requirements of key issue #16 are met during discovery. Furthermore, the selected UE-to-Network relay that is given the PDU session parameters during the subsequent connection setup process cannot trace the Remote UE with the solicited Relay Service Code since the Relay Service Code is changed to a new alias (using a message that cannot be decrypted by that selected UE-to-Network relay) and the Remote UE will use the new alias in subsequent discovery messages.

In case of connection setup: the privacy issues in key issue #16 are mitigated by enabling only the UE-to-Network relay that is selected by the Remote UE and for which the Remote UE has issued a Direct Connection Request to link the requested Relay Service Code to a set of PDU session parameters.

* In case of ALTERNATIVE 1, this is achieved by only exposing the requested Relay Service Code to the selected UE-to-Network relay after it has been decrypted/integrity verified by the home network and the request to set up a relayed connection via the selected UE-to-Network for the respective Remote UE and requested Relay Service Code has been authorized/approved by the home and serving networks.
* In case of ALTERNATIVE 2, this is achieved by only providing the PDU session parameters to the selected UE-to-Network relay after it has been decrypted/integrity verified by the home network and the request to set up a relayed connection via the selected UE-to-Network for the respective Remote UE and requested Relay Service Code has been authorized/approved by the home and serving networks.

The Relay Service Code and the identifiers of both the Remote UE and the selected UE-to-Network relay are encrypted/integrity protected in such manner that only the home network of the remote UE can decrypt/verify these values, so neither eavesdroppers nor any of the other UE-to-Network relays nor other Remote UEs can make the link between the respective Relay Service Code and its associated PDU session parameters. This is so even if in ALTERNATIVE 1 each UE-to-Network Relay and each Remote UE is provisioned with associations between Relay Service Codes and PDU session parameters beforehand. Replaying this encrypted value (i.e. ENCRYPT(K\_enc, RSC | ID\_Relay)) by another UE-to-Network relay will fail because the core network will verify that the ID\_Relay in the encrypted value corresponds to the identifier of the UE-to-Network Relay that sent this encrypted value to the core network along with the NAS Authorization request.

However, this privacy risk is only temporary for the duration of the communication session, since the Remote UE will use a different Relay Service Code in subsequent discovery and connection setup messages and this different Relay Service Code was provided to the Remote UE using a message that cannot be decrypted by a UE-to-Network Relay, only by the Remote UE.

In both ALTERNATIVE 1 and ALTERNATIVE 2, this solution requires the AMF to support new procedures to retrieve from the PCF a new RSC that is encrypted. In case of ALTERNATIVE 2, the AMF also needs to support new procedures to retrieve from the PCF the PDU session parameters associated with the requested RSC. This second alternative is not aligned with the procedures in TS 23.304 [16] where the PDU Session parameters to be used for the relayed traffic for each associated Relay Service Code (RSC) are provisioned to both a Remote UE and UE-to-network relay before PC5 link setup when Layer-3 UE-to-Network relay is used. Hence, if ALTERNATIVE 2 is adopted given its stronger privacy guarantees, then alignment with SA2 will be required.

Editor’s Note: Further evaluation is FFS.

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