**3GPP TSG-SA3 Meeting #108e-AdHoc *draft\_S3-222797-r1***

**e-meeting, 10 - 14 October 2022**

**Source: Ericsson**

**Title: Resolve** **EN for protection of DCR in Solution4**

**Document for: Approval**

**Agenda Item: 5.3**

# 1 Decision/action requested

***This document proposes to resolve ENs for protection of DCR in solution4.***

# 2 References

[1] 3GPP TR 23.700-33

[2] 3GPP TR 33.740

# 3 Rationale

This contribution proposes to resolve the following ENs in Solution #4: PC5 security establishment when L3 UE-to-UE relay is out of coverage.

* Editor’s Note: Its FFS whether the included parameters in Direct Communication Request message in step 2 can be protected by the discovery keys similar as to the Direct Communication Request message when establishing a secure PC5 link in between Remote UE and UE-to-network relay.

Clause 6.3.5 of TS 33.503 describes the mechanism to protect the privacy of information sent over Direct Communication Request message based on the security parameters used for discovery.

It is proposed that the same protection as described in TS 33.503 can be applied for UE-to-UE Relay case.

* Editor’s Note: Its FFS how token freshness is guaranteed as any peer UE can replay the token (since sent in the clear in DCR).

It is our view that token is short lived and can contain expiration time which is assigned by the network. Therefore, token freshness has been taken care.

The risk of token being sent clear in DCR thus intercepted and replayed by any other peer UE can be mitigated by, either reusing the similar DCR privacy protection of UE-to-Network relay case by encrypting the token or moving the token exchange procedure until Direct Security Mode Complete thus the token exchange is protected by the established security context.

In our view, both methods are feasible. Message-specific confidentiality has been supported in UE-to-Network relay case, and the keystreams are bound to UTC time counter. It is sufficient to mitigate replay attack by applying a similar keystream to protect the token in the DCR.

It is proposed that token in DCR is protected by keystream similarly as UE-to-Network relay case. Calculation of keystream for token protection for UE-to-UE relay can be decided in Normative work.

# 4 Detailed proposal

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

## 6.4 Solution #4: PC5 security establishment when L3 UE-to-UE relay is out of coverage

### 6.4.1 Introduction

This solution addresses Key issue #2: Security of UE-to-UE Relay and Key issue #3: Authorization in the UE-to-UE Relay Scenario. This solution addresses a L3 UE-to-UE relay.

For UE-to-UE relay use cases, the L3 UE-to-UE relay may be in or out of 3GPP coverage. This solution provides a mechanism for PC5 security setup procedure between a source UE or target UE and a L3 UE-to-UE relay when the L3 UE-to-UE relay is out of 3GPP coverage.

This solution assumes long term credentials are provisioned into the UE(s) and form the root of the security of the PC5 unicast link as specified in TS 33.536 [9].

This solution proposes to use authorization tokens as in OAuth 2.0 to indicate that a source UE or a target UE or a L3 UE-to-UE relay is authorized to use a specific UE-to-UE service or to serve a specific UE-to-UE service. When the source UE or the target UE or the L3 UE-to-UE relay registers in the 3GPP network and is authorized to use the UE-to-UE service, the network provides a token stating what kind of UE-to-UE service it can use or serve. The token has an expiration time and is signed with a private key. The network also provides the public key to the UEs to be used for verifying the token from other parties.

Editor’s Note: Which network function provides authorization token and how the UEs get the public key of token signing entity are FFS.

### 6.4.2 Solution details

Figure 6.4.2-1 illustrates the high-level procedure of the proposed solution.



Figure 6.4.2-1: High-level procedure of PC5 security between Source/Target UE and UE-to-UE relay

0. The 5G ProSe Source/Target UE and UE-to-UE relay are provisioned with the discovery security materials and request authorization tokens when they are in coverage.

Editor’s Note: Further provisioned parameters e.g., PC5 security policies of UE-to-UE relay, public keys are FFS.

1. The discovery procedure for UE-to-UE Relay is performed by the 5G ProSe Source UE using the discovery parameters and discovery security material, based on the Relay Service Code for UE-to-UE Relay.

2. If discovery result indicates the UE-to-UE Relay supports Direct Relay service authentication and authorization, the 5G ProSe Source UE sends a Direct Communication Request (DCR) that contains Relay Service Code (RSC) of the 5G ProSe UE-to-UE Relay service and Authorization token of 5G ProSe Source UE which is retrieved from step 0, and also the Key\_Est\_Info used for direct authentication and key establishment. Protection of Authorization token and RSC in DCR can be done in a similar way as described in TS33.503 [6].

NOTE: The details regarding the ciphering algorithm can be decided in Normative work.

Editor’s Note: The need for authorization token is FFS”.

3. Direct Auth and Key Establish procedure as specified in TS 33.536 [9] is performed.

4. The 5G ProSe UE-to-UE Relay uses the public key provided by the network to verify the token of the 5G ProSe Source UE that the 5G ProSe Source UE is authorized to get the UE-to-UE relay service.

5. The 5G ProSe UE-to-UE Relay derives KNRP and other security material as specified in TS 33.536 [9]. The 5G ProSe UE-to-UE Relay sends a Direct Security Mode Command message to the 5G ProSe Source UE including the Authorization token of 5G ProSe UE-to-UE Relay which is retrieved from step 0. The protection of the Authorization token is applied in the same way as step 2.

6. The 5G ProSe Source UE uses the public key provided by the network to verify the token of the 5G ProSe UE-to-UE Relay that the 5G ProSe UE-to-UE Relay is authorized to provide the UE-to-UE relay service. The 5G ProSe Source UE derives KNRP and other security material similar as the 5G ProSe UE-to-UE Relay in step5.

7. The 5G ProSe Source UE sends the Direct Security Mode Complete message to the 5G ProSe UE-to-UE.

8. The 5G ProSe Source UE and 5G ProSe UE-to-UE Relay continue with the rest of procedure for the UE-to-UE relay service over the secure PC5 link.

Editor’s Note: Further and remaining messages needs to be updated and clarified in step 8.

9. Step 1-8 are repeated for PC5 security establishment between the 5G ProSe Target UE and 5G ProSe UE-to-UE Relay.

Editor’s Note: It is FFS whether PC5 security set up procedure between target UE and Relay UE is performed after or in parallel to the PC5 security set up procedure between source UE and Relay UE.

10. The 5G ProSe Source UE and the 5G ProSe Target UE may establish an end-to-end Security via 5G ProSe UE-to-UE relay. The detail is not described in this solution.

Editor’s Note: The method for providing End to End IP security is FFS.

Editor’s Note: The need of End-to-end security in L3 relay is FFS,

Editor’s Note: The impact on the protocol stack to support end-to-end security for a L3 relay is FFS.

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