**3GPP TSG-SA3 Meeting #104 *S3-212464-r2***

**E-meeting, 16 - 27 Aug 2021**

**Source: MITRE**

**Title: New solution: Keying procedures for Group Member and Relay discovery: public safety case**

**Document for: Approval**

**Agenda Item: 5.9**

1 Decision/action requested

***This pCR proposes to solve Key Issues #1, #2, and #4***

2 References

[1] 3GPP TR 33.847 "Study on Security Aspects of Enhancement for Proximity Based Services in 5GS".

[2] 3GPP TS 33.303 "Proximity-based Services (ProSe); Security aspects".

[3] 3GPP TS 23.304 "Proximity based Services (ProSe) in the 5G System (5GS) ".

[4] 3GPP TR 23.752: "Study on system enhancement for Proximity based Services (ProSe) in the 5G System (5GS)".

3 Rationale

This solution aims to address keying for public safety discovery.

From TR 23.752 [4]:

In order to satisfy the normative stage-1 general requirements in TS 22.278 [2] and TS 22.261 [3] and TS 22.115 [4], the system shall:

- enable the direct discovery of the ProSe-enabled UE by other ProSe-enabled UEs within the same PLMNs or different PLMNs, including in coverage and out of coverage.

This one solution addresses both public safety discovery types (group member and relay) and works for in coverage and out of coverage.

This solution is in synergy with an update to the TS 23.304 [3] description of the policy/parameter provisioning for public safety by the PCF (“Step 0” in this solution).

4 Detailed proposal

SA3 is kindly requested to agree to the below pCR to TR 33.847.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* First Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 6.XX Solution #XX: Keying procedures for Group Member and Relay discovery: public safety case

6.XX.1 Introduction

This solution describes how the UE obtains the necessary security parameters to support group member and relay discovery, in coverage and out of coverage, for public safety scenarios. This solution addresses key issues #1, #2, and #4.

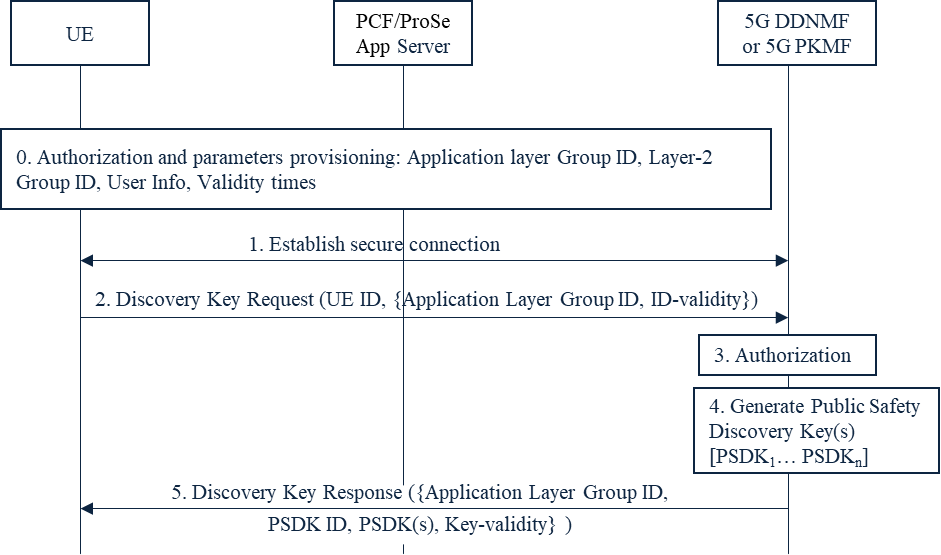
6.XX.2 Solution details

6.XX.2.1 Group member discovery case

Group member discovery is a type of restricted discovery and is expected to be supported in coverage and out of coverage. Group member discovery uses provisioned keys to support integrity, confidentiality and non-trackability of the discovery messages. A discovery root key from which other keys can be derived is used to secure over the air discovery and communications. This root key can be provisioned by the 5G DDNMF and/or by the 5G PKMF – this clarification is left for normative stage.

The solution follows that of TS 33.303 [2], where for both public safety discovery scenarios – group member discovery and relay discovery – the same solution is provided: a Public Safety Discovery Key (PSDK) is provisioned as the root key that is used for the protection of the Public Safety Discovery messages, and is associated with one or more Application Layer Group IDs or respectively Relay Service Codes (RSCs). Both of these identifiers are defined in TS 23.303 [5].

The procedures are shown below for Group Member Discovery.



**Figure 6.XX.2.1-1: Discovery key provisioning for group member discovery, public safety case**

Step 0: The UE connects to the network and obtains authorization from the PCF to perform Group Member discovery. The UE also gets the address of the 5GDDNMF of its HPLMN and/or of the 5G PKMF. Besides the security policy, the following additional parameters are sent to the UE: a set of one or more (ProSe) Layer-2 Group ID, User Info, Application Layer Group ID and their validity time(s).

NOTE 1: This step is briefly described in TS 23.304 [3].

Step 1: The UE establishes a secure connection with the 5GDDNMF or the 5G PKMF of its HPLMN. The UE ID is authenticated and authorized by the 5GDDNMF or the 5G PKMF.

NOTE 2: As this connection is established on the user plane, the same mechanism as used to protect the PC3 interface can be re-used. Either solution #5 or solution #11 can be used for securing the connection.

Step 2: The UE sends a discovery key request to the 5GDDNMF or the 5G PKMF of its HPLMN. In the key request includes at least the following information: UE ID, set of one or more Application Layer Group IDs and their validity times.

Step 3: The 5GDDNMF or the 5G PKMF checks whether the UE is authorized for group member discovery.

Step 4: If the check in step 3 is successful, then the 5GDDNMF or the 5G PKMF generates one or more Public Safety Discovery Keys (PSDK1… PSDKn) corresponding to the Application Layer Group ID and its PLMN ID. More than one PSDK may be generated, but the overall validity time should match the validity times of the corresponding set of Application Layer Group IDs of Step 2. The Expiry Time of the PSDK needs to be set such that the keys for later periods have a longer expiration period. PSDKs that have not expired can be used for discovery in out of coverage cases.

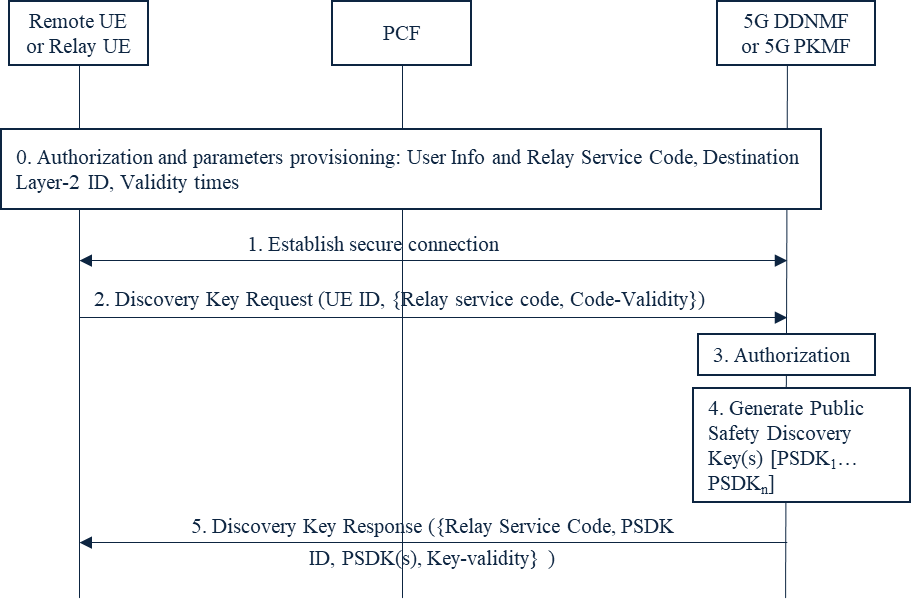
NOTE 3: When and how often the discovery keys need to be generated is left for normative work.NOTE 4: The security keys in the Code-Sending Security Parameters of discoverer UE and the security keys in the Code-Sending Security Parameters of discoveree UE must be generated from two different PSDKs to avoid impersonation attacks in certain discovery configurations.

Step 5: The 5GDDNMF or the 5G PKMF sends the key response to the UE. The key response message includes at least the following information: UE ID, PDSK identifier, PDSK, validity time.

6.XX.2.2 Relay discovery case

The procedures are similar to the ones for Group Member Discovery. For Relay discovery, the procedures for the relay discovery are identical, with the following exceptions:

* The UE is now the Remote UE or the UE-to-network Relay
* Instead of parameter Application Layer Group ID, the Relay Service Code is used.
* Instead of Layer-2 Group ID, the Destination Layer-2 ID is used



**Figure 6.XX.2.2-1: Discovery key provisioning for relay discovery, public safety case**

6.XX.3 Evaluation

The solution addresses key issues #1, and partially key issues #2, and #4 in the following way. Authorization for the UE to act as a group member, or UE-to-network relay, or Remote UE is provided by the PCF. The PCF provisions both policy as well as group member and relay discovery parameters, along with their validity times. In addition, this solution describes how the UE obtains discovery keying material to support Group Member Discovery, in coverage and out of coverage. Lastly, the solution describes how the Remote UE and the UE-to-network Relay retrieve the discovery keying material for the corresponding Relay Service Code(s). This solution is intended for Public Safety services.

The following observations are made:

The UE is provisioned by the PCF with the address of the 5G DDNMF and/or the 5G PKMF.

This solution has no impact on the RAN or the network nodes AMF, AUSF.

In this solution, the 5G DDNMF, or another NF – the 5G PKMF (located in the UE’s HPLMN or external to it), handles the management of discovery keys for discovering a group member UE or a UE-to-network Relay.

SA2 has defined the 5G DDNMF in TS 23.304 [16] in the architecture, with reference points and services provided.

SA2 has not defined the NF - 5G PKMF, which manages discovery keys, in the architecture for the Group member discovery and UE-to-network relay scenarios as proposed in this solution, but SA2 did not define the PKMF in LTE either.

In LTE, the PKMF is only used for Public Safety.  This solution proposes to reuse the logic of the 5G DDNMF (or the ProSe Function in LTE) or the 5G PKMF which is part of the PLMN.

SA2 should make note that the security material for relay discovery is not provisioned by the PCF, but by the 5G DDNMF or 5G PKMF.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*