**Way forward of KI#1 Conclusion in R18 ProSe TR 33.740**

**Backgrounds:**

**A.**

The key Issue #1 In TR 33.740 focuses on the Security for UE-to-UE Relay discovery. The security requirements of this Key Issue include confidentiality protection, integrity protection, replay protection and privacy protection of discovery messages for UE-to-UE Relay discovery.

* *The 5G System shall provide a means for confidentiality protection, integrity protection and replay protection of discovery messages for UE-to-UE Relay discovery.*
* *The 5G System shall provide a means to protect the privacy sensitive information of source UE and target UE during UE-to-UE Relay discovery procedure.*
* *The 5G System shall provide a means to securely provision the security materials for UE-to-UE Relay discovery.*

**B.**

SA2 (TS 23.304 and TR 23.700-33) has specified the following points about UE-to-UE Relay discovery:

* *The 5G ProSe UE-to-UE Relay Discovery message contains two sets of identifiers, a Direct Discovery set and a UE-to-UE Relay Discovery set.*
	+ *The Direct Discovery set of identifiers are part of the contents of the 5G ProSe Direct Discovery message.*
	+ *The UE-to-UE Relay Discovery set of identifiers contain information to support the discovery of the 5G ProSe UE-to-UE Relay and extensions of the Direct Discovery.*
* *For UE-to-UE Relay Model A discovery, the Type of Discovery Message, User Info ID of the UE-to-UE Relay, RSC, list of User Info ID of Target UE are contained in the Announcement message.*

**C.**

There are two candidate solutions to address the security requirements of KI#1:

Approach #1: Using one set of security material to protect both the U2U Discovery Set and the Direct Discovery Set in the UE-to-UE relay discovery messages.

Approach #2: Using two sets of security materials to protect both the U2U Discovery Set and the Direct Discovery Set in the UE-to-UE relay discovery messages, respectively.

**D.**

Arguments were raised during previous discussions that two key sets of security materials (i.e. Approach #1) are not capable to maintain the freshness and prevent the replay attacks of the protected direct discovery sets (i.e. list of User Info ID of Target UE) in model A discovery.

**E.**

SA2 (TS 23.304) has specified the 5G ProSe UE-to-UE Relay Communication with integrated Discovery, in which UEs use Direct Communication Request to perform the discovery and initiate the link establish, instead of processing either Model A or Model B discovery prior to the link establishment.

**Questions for show of hands**

**Question 1: In addition to PKMF being used to provide U2U discovery security materials, can PKMF be used to provide direct discovery security materials in U2U discovery scenario?**

Option 1: Yes

Option 2: No

Conclusion:

**Question 2: Use one or two sets of security materials to protect UE-to-UE relay discovery messages?**

Option 1: One set

Option 2: Two sets

Conclusion:

**Question 3: For the scenario of 5G ProSe UE-to-UE Relay Communication with integrated Discovery, in addition to the procedure defined by SA2, SA3 needs to define additional discovery security mechanism for this procedure?**

Option 1: Yes

Option 2: No

Conclusion: