1. Discussion of conclusions and potential solutions of ProSe Ph2
2. Q1: Can PKMF also provision security materials for protecting direct discovery set?

[CATT] presents.

[Nokia] asks questions.

[IDCC] asks questions for clarification

[Huawei] asks question about direct discovery with PKMF. It is not clear. PKMF is not involved in Q1.

[CATT] clarifies, if it is for network operator, then it is ok. But if it is for ...., then we need to consider this. The question just shows this.

[IDCC] comment PKMF question is not needed now.

Chair asks whether it is the same view for Huawei.

[Huawei] clarifies it is similar comment, so very confused.

Chair summarizes it seems option 2 is more preferred and asks whether CATT can accept it in order to move forward. “Conclusion: Option2, let us not worry PKMF provisioning now “

[CATT] clarifies such conclusion can be accepted though CATT has some concerns on that.

1. Q2: How are the two sets of security materials used to protect UE-to-UE relay discovery messages?

[CATT] presents.

Chair asks question.

[CATT] clarifies.

[IDCC] comments there may be a missing option.

Chair asks IDCC to clarify whether comments refers to option 2, rather than to introducing new option.

[IDCC] clarifies that option 2 is not good enough so it needs to be revised.

[Huawei] prefers option 1.

[QC] agrees with IDCC’s comment, option 2 should be changed.

Chair asks whether QC prefers option 2.

[QC] clarifies it tends to prefer option 2 but it needs to be revised.

[Oppo] prefers option 1 as it is agreed in previous meeting.

[Philips] shares same view with IDCC.

Chair comments that option 2 and option 3 will bring drawback about implementation, increase complexity.

[CATT] clarifies option 3 is always used in industry.

[Docomo] asks question about benefit to reduce key set, but unnecessary options are not good.

[QC] comments.

[Huawei] replies.

Chair shares same view with Huawei, that option 1 can cover all cases against option 2+3.

[IDCC] comments.

[CATT] clarifies option 1 is simplest and does not need to consider negotiation.

Chair tries to conclude that option 1 can provides flexibility by provisioning and there is no need to consider option 2 and option 3. “Conclusion: Option1 provides flexibility by provisioning, no need for Option2 and 3 “

[CATT] comments it means dynamic control missed.

Chair doesn’t agree with this comment.

[Philips] comments.

Chair points if it is not in TR it means there is no agreement.

Chair urges to move forward based on option 1, as it can provide flexibility with provisioning even though it doesn’t support dynamic negotiation

1. Q3:For the scenario of UE-to-UE Relay Communication with integrated Discovery. Modifed question, Question 3: Does SA3 need to define security mechanism to support integrated discovery?

[CATT] presents.

Chair asks whether it is already in TR now.

[CATT] clarifies the case is already in SA2’s TS.

Chair asks what is difference between normal discover and integrated discovery.

[CATT] clarifies.

[Xiaomi] comments on question 3. it needs to be revised, it should be security discovery.

[IDCC] comments.

Chair asks why mandatory mechanism is needed.

[CATT] clarifies, related solution are provided by Philips, asks Philips to clarify.

[Philips] clarifies.

[CATT] gives clarification about solution, it may be benefit for V2X.

[Xiaomi] challenges it is ProSe discussion but not V2X.

[CATT] clarifies it is U2U relay.

[Xiaomi] doesn’t agree with the clarification from CATT.

[Xiaomi] comments.

[CATT] clarifies V2X is used as example to show it can be used in U2U relay.

[QC] comments.

Chair considers majority prefers option 1.

[Xiaomi] doesn’t agree with the comment, comments that is SA2 decision, it should not be considered as security conclusion and the message is signalling rather then user message.

[CATT] prefers option 1, even it can live with option 3.

[Xiaomi] considers option 3 is ok.

[Philips] prefers option 3.

[Huawei] clarifies.

Chair asks whether option 1 means the signalling is not protected?

[Huawei] clarifies it does not mean not protected, protection can be left for application layer.

[Ericsson] comments, shares similar view with Huawei.

[CATT] supports Huawei’s comment.

[Xiaomi] comments the message is generated by network layer, asks how to protected by application layer.

[QC] comments the message should be considered to have integrity protection only when it is related with people’s sensitive data.

Chair suggests to give more explanation for each case and then discuss in next meeting.

[IDCC] comments there is related contribution 2.S3-23aabb Discussion on ProSe UE-to-UE Relay discovery security with Model A

Chair asks to presents.

[IDCC] presents.

Chair asks whether it is for information sharing or need to discuss.

[IDCC] clarifies it needs to discuss.

[QC] doesn’t follow observation 2 and 3. the issue is not in sa3 scope. Maybe it should be in scope of SA2.

[IDCC] replies.

Chair proposes to discuss it in the next meeting.

1. Topic 2

[CATT] provides brief introduction.

[Xiaomi] comments.

[CATT] proposes if U2U relay is out of coverage, application layer security mechanism can be applied instead of network layer security feature.

[Xiaomi] comments and doesn’t agree with proposal.

1. Topic 3 “7.4 Key issue #4: Privacy in the UE-to-UE Relay Scenario “

[CATT] presents.

[CATT] clarifies the title is wrong, should be revised, but content is correct.

[IDCC] comments.

[Oppo] comments if there is no progress it should be deleted. Only ran dependency part should be addressed.

[IDCC] clarifies.

Chair think it need to be discussed in next meeting.

1. Topic 4 RAN2 LS R2-2304559 LS to SA3 on security for L2 UE-to-UE relay.docx

End to End Bearer ID, in the hop by hop scenario is not understood by the group. How does the peer end points learn the e2e bearer id?

Action item: get more detail from RAN2 colleagues internally, LS exchange will take time.