**3GPP TSG-SA3 Meeting #102bis-e *draft\_S3-210897-r3***

**e-meeting, 1 - 5 March 2021** Revision of S3-21xxxx

**Source: Huawei, HiSilicon**

**Title: New solution for ProSe one-to-one rekeying**

**Document for: Approval**

**Agenda Item: 2.9**

# 1 Decision/action requested

***Approve this contribution to add new solution to TR 33.847***

# 2 References

N/A

# 3 Rationale

This contribution proposes to add the security establishment during one-to-one PC5 connunication rekeying.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* BEGINNING OF CHANGES\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 6.X Solution #X: Security establishment of one-to-one PC5 communication rekeying

### 6.X.1 Solution overview

This solution addresses the following security requirement in Key Issue #12: Security of one-to-one communication over PC5:

‘The system shall support means for a secure refresh of the UE security context.’

The initiating UE starts a Direct Rekeying Request to the receiving UE to trigger the refresh of security context between UEs, similar to the rekeying procedures as specified in clause 6.5.5.3 of TS 33.303 [6]. After receiving the Direct Rekeying Request, new root key shared only between two UEs is generated securely by running Direct authentication and key establishment. New security context is derived after the Direct Security Mode Command message based on the new root key.

### 6.X.2 Solution details

Initiating UE

Receiving UE

2. Direct rekeying Request ( Initiating UE's security capabilities )

3. Direct Auth and Key Establishment

4. Direct Security Mode Command( Chosen\_algs, Initiating UE's security capabilities )

5. Direct Security Mode Complete ( )

1. existing One-to-One Communication

6. Direct Rekeying Accept ( )

0. ProSe Parameter pre-configuration and previsioning

Figure 6.x.2-1 Procedures for one-to-one communication rekeying over PC5

0. ProSe security-related parameter (for one-to-one secure communication over PC5) pre-configuration and provisioning.

1. The initiating UE and receiving UE already have established ProSe one-to-one communication.

2. The initiating UE starts a Direct Rekeying Request message containing the initiating UE’s security capabilities. The initiating UE’s security capabilities are the confidentiality and integrity protection algorithms that the initiating UE accepts for this connection. The message may also include a Re-auth Flag, if UE\_1 wants to rekey the root key between the initiating UE and the receiving UE

3. The receiving UE may initiate the Direct authentication and key establishment procedures with the initiating UE. This is mandatory if the Re-auth Flag appears in the Direct Rekeying Request message. The new root key shared only between two UEs is generated securely after Direct authentication and key establishment procedures.

4. The receiving UE uses the Chosen\_algs to indicate the selected confidentiality and integrity protection algorithms of this link and includes the Chosen\_algs in the Direct Security Mode Command message. The initiating UE’s security capabilities are sent back to the initiating UE. New security context is derived by using the new root key generated in step 3. The receiving UE integrity protects the Direct Security Mode Command message with the new security context before sending it to the initiating UE.

Editor’s Note: How the UEs derive new session keys based on this rekeying procedure is FFS.

Editor’s Note: The parameters that is included in Direct Rekey Request and Direct Security Mode Command is FFS.

NOTE: The security activation status of both signalling and user plane remain the same for the lifetime of this PC5 link. The signalling and user plane use the same security algorithm if they have the same security activation status.

5. The initiating UE derives the new security context using the new root key generated in step 3. After the Direct Security Mode Command message passes integrity check, the initiating UE is then ready to both send and receive both signalling and user plane traffic protected with the new security context. The initiating UE sends the Direct Security Mode Complete message protected with new security context to the receiving UE.

6. The receiving UE replies the Direct Rekeying Accept message to accept the Direct Rekeying Request.

### 6.X.3 Evaluation

The Solution #x addresses the security requirement of secure refresh of UE security context in key issue #12. The secure refresh of UE security context is based on the root key that is securely established only between two UEs using the Direct authentication and key establishment procedure.

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