**3GPP TSG-SA3 Meeting #11*6*** ***S3-242246-r1***

**Jeju, South Korea, 20th - 24th May 2024**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.503** | **CR** | **0187** | **rev** | **1** | **Current version:** | **18.2.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Clause 6.3.6 in TS 33.503 - correction |
|  |  |
| ***Source to WG:*** | Philips International B.V. |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5G\_ProSe\_Ph2 |  | ***Date:*** | 2023-05-20 |
|  |  |  |  |  |
| ***Category:*** | **C** |  | ***Release:*** | Rel-18 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | Clause 6.3.6 requires a 5G ProSe Remote UE to disclose its PEI if requested by a 5G ProSe UE-to-network relay in Step 4b without further checks. This leads to a privacy issue, namely traceability/linkability.Clause 6.3.6, steps 2 and 4b require a 5G ProSe UE-to-network relay to store a PEI without further checks. This makes the 5G ProSe UE-to-network relay prone to storage saturation attack. There are some typos in Clause 6.3.6. |
|  |  |
| ***Summary of change:*** | Introduction of checks to avoid traceability, linkability, and storage saturation attacks.  |
|  |  |
| ***Consequences if not approved:*** | A 5G ProSe Remote UE is prone to traceability/linkability attacks, and a 5G ProSe UE-to-network relay is prone to storage saturation attacks. |
|  |  |
| ***Clauses affected:*** | 6.3.6 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

**\*\*\* START OF CHANGES \*\*\***

##### 6.3.6.3.1.1 PC5 security establishment for Emergency Service over UE-to-Network relay

Figure 6.3.6.3.1.1-1 shows the PC5 security establishment procedure for the 5G ProSe UE-to-Network Relay communication when an Emergency Relay Service Code is used. This procedure is based on the procedure in clause 6.3.3.2.2 and clause 6.3.3.3.2.



Figure 6.3.6.3.1.1-1: PC5 link security establishment for Emergency Service over UE-to-Network relay

If relaying emergency service with PC5 link security is not required for a 5G ProSe Remote UE has no USIM based on the regulation, there is no discovery security materials (and UP-PRUK in case of UP based security procedure) provisioned for an Emergency RSC.

0. The 5G ProSe UE retrieves discovery material with the procedures as specified in clause 6.1.3.2. For UP based security procedure, the 5G ProSe Remote UE retrieves UP-PRUK as specified in step 1 of clause 6.3.3.2.2.

If the 5G ProSe Remote UE has no USIM, this step is skipped. The discovery security materials, if exist, and the Emergency RSC are locally configured in the 5G ProSe UE.

1. The discovery procedure for the Emergency RSC is performed between a 5G ProSe Remote UE, and the 5G ProSe UE-to-Network Relay, using the discovery parameters and discovery security material that are obtained in step 0.

If no discovery security material is provisioned or locally configured, the announcement and discovery of Emergency RSC may be performed without security protection if the regulation allow.

2. If the 5G ProSe Remote UE has a USIM, the 5G ProSe Remote UE sends a Direct Communication Request (DCR) to trigger PC5 security establishment for Emergency RSC using UP based security procedure as specified in step 4 of clause 6.3.3.2.2 or CP based security procedure as specified in step 3 to step 13 of clause 6.3.3.3.2.

If the 5G ProSe Remote UE has no USIM, then the 5G ProSe Remote UE sends a Direct Communication Request that contains PEI and Emergency RSC to the 5G ProSe UE-to-Network Relay. The Direct Communication Request message including PEI and Emergency RSC may be sent without protection if no discovery security material is provisioned or locally configured in the 5G ProSe Remote UE.

If UP/CP-PRUK ID or SUCI is received from the 5G ProSe Remote UE, the 5G ProSe UE-to-Network Relay performs UP based security procedure as specified in step 4 of clause 6.3.3.2.2 or CP based security procedure as specified in step 3 to step 13 of clause 6.3.3.3.2.

If only PEI and Emergency RSC are received from the 5G ProSe Remote UE, the 5G ProSe UE-to-Network Relay skips step 4 of clause 6.3.3.2.2 for UP based security procedure or step 3 to step 13 of clause 6.3.3.3.2 for CP based security procedure if the regulation and the operator policy allow. The 5G ProSe UE-to-network relay shall store the PEI.

3a. If UP based security procedure as specified in step 4 of clause 6.3.3.2.2 or CP based security procedure as specified in step 3 to step 13 of clause 6.3.3.3.2 in step 2 was successfully performed, then the 5G ProSe UE-to-Network Relay shall proceed with the Direct Security Mode procedure as specified in steps 5a-5d in clause 6.3.3.2.2 for UP based security procedure or step 14 to step 16 of clause 6.3.3.3.2 for CP based security procedure.

 If UP based security procedure as specified in step 4 of clause 6.3.3.2.2 or CP based security procedure as specified in step 3 to step 13 of clause 6.3.3.3.2 in step 2 failed or was skipped, the 5G ProSe UE-to-Network Relay shall send Direct Security Mode Command message to the 5G ProSe Remote UE indicating NULL ciphering algorithm and NULL integrity protection algorithm as chosen algorithms if the regulation and the operator policy allow.

When there has been no successful run of authentication of the 5G ProSe Remote UE, the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay independently generate the KNRPor KNR\_ProSe in an implementation defined way. All key derivations proceed as if they were based on a KNRPor KNR\_ProSe generated from a successful authentication run.

If the 5G ProSe Remote UE receives the Direct Security Mode Command message indicating NULL integrity algorithm and NULL encryption algorithm as chosen algorithms, then the 5G ProSe Remote UE shall accept NULL ciphering and NULL integrity algorithms indicated in Direct Security Mode Command message if, and only if, the 5G ProSe Remote UE has sent an Emergency RSC in step 2. The 5G ProSe Remote UE shall set the UP integrity protection as not activated for this connection.

3b. If the 5G ProSe Remote UE receives the Direct Security Mode Command message indicating non-NULL integrity and non-NULL encryption algorithm then the 5G ProSe Remote UE proceeds step 5a-5d in clause 6.3.3.2.2 for UP based security procedure or step 14- step 16 of clause 6.3.3.3.2 for CP based security procedure.

If the 5G ProSe Remote UE receives the Direct Security Mode Command message indicating NULL integrity and NULL encryption algorithm in step 3a and has accepted the message, then the 5G ProSe Remote UE shall send a Direct Security Mode Complete message and shall include the UP integrity protection policy as NOT NEEDED in the Direct Security Mode Complete message.

If the 5G ProSe UE-to-network relay receives the Direct Security Mode Complete message with no protection, the 5G ProSe UE-to-Network Relay shall only accept the message if 5G ProSe UE-to-Network Relay sent Direct Security Mode Command message including NULL integrity and NULL encryption algorithm in step 3a and if the 5G ProSe Remote UE has sent an Emergency RSC in step 2.

4a. If UP based security procedure as specified in step 4 of clause 6.3.3.2.2 or CP based security procedure as specified in step 3 to step 13 of clause 6.3.3.3.2 in step 2 failed or was skipped and PEI is not received from the 5G ProSe Remote UE in the Direct Communication Request, the 5G ProSe UE-to-Network Relay sends a Remote Identity Request message to the 5G ProSe Remote UE to retrieve the PEI based on the regulation and the operator policy.

4b. When the 5G ProSe Remote UE receives a Remote Identity Request message from the 5G ProSe UE-to-network relay, then the 5G ProSe Remote UE sends a Remote Identity Response message including its PEI to the 5G ProSe UE-to-network relay if, and only if, the 5G ProSe Remote UE has sent an Emergency RSC in step 2. The 5G ProSe UE-to-network relay shall store the PEI.

5. If the 5G ProSe UE-to-network relay receives the Direct Security Mode Complete message in step 3b, and after successful verification, the 5G ProSe UE-to-Network Relay responds with a protected Direct Communication Accept message to the 5G ProSe Remote UE to complete the PC5 connection establishment procedure.

If the 5G ProSe UE-to-network relay receives the Direct Security Mode Complete message with no protection, and the 5G ProSe UE-to-Network Relay has accepted the message based on the conditions described in step 3b, the 5G ProSe UE-to-Network Relay shall send Direct Communication Accept message with no protection to the 5G ProSe Remote UE.

The 5G ProSe UE-to-Network Relay includes the configuration of UP integrity and confidentiality protection based on the agreed UP security policy in the Direct Communication Accept message as specified in TS 33.536 [6].

6. The 5G ProSe Remote UE and 5G ProSe UE-to-Network Relay continues the rest of procedure for the emergency service over relay as specified in TS 23.304 [2]. The 5G ProSe UE-to-Network Relay sends a Remote UE Report to the SMF for the Emergency RSC. The 5G ProSe UE-to-Network Relay includes Remote User ID i.e. (UP-/CP-) PRUK ID if UP or CP based security procedure is successfully performed. Otherwise, the 5G ProSe UE-to-Network Relay includes the PEI of the 5G ProSe Remote UE in the Remote UE Report.

If UP confidentiality protection is not activated for this connection, the UP confidentiality protection algorithm is the same as the selected signalling confidentiality algorithm as specified in TS 33.536 [6].

If UP integrity protection is not activated for this connection, the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay do not put MAC-I into PDCP packet.

UP protection for the layer 2 relaying emergency service shall be handled as specified in clause 10 of TS 33.501[3].

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