**3GPP TSG-SA3 Meeting #100e *S3-201609***

**e-meeting, 17 - 28 August 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.536** | **CR** | **0002** | **rev** | **-** | **Current version:** | **16.0.0** |  |
|  | | | | | | | | |
| *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:*** | Corrections on security establishment | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Interdigital | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eV2XARC | | | | |  | ***Date:*** | | | 2020-08-5 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *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 can be 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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | * In section 5.3.3.1.4.3, step 4, with non-NUL integrity algorithm selected the UE\_1 check that the received LSBs of KNPR-sess ID is unique shall be done in the context of current DCR only. Otherwise a check for uniqueness locally, may lead UE1 to reject the DSMC message due to a LSBs of KNPR-sess ID collison with LSBs of KNPR-sess ID used by any existing link An attacker may be able to obtain knowledge of the LSBs of KNPR-sess ID andassociatedlink identifiers in use by other UEs already connected to the target UE. * The entire KNRP-sess ID shall be used to pinpoint locally the security context since the same MSBs of KNPR-sess ID from UE\_1may be used bymultiple peer UEs making the MSBs of KNPR-sess ID used alone not sufficient to uniquely identify the security context locally. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | * It is proposed to clarify the check of LSBs of KNPR-sess ID uniqueness received in DSMC relative to current DCR * Clarify that the KNPR-sess ID is used to uniquely identify the security context locally. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | * The LSBs of KNPR-sess ID in use may be leaked leading to linkability/trackability attacks if the check of LSBs of KNPR-sess ID uniqueness is not done in relative to current DCR * UE is unable to establish and use a unique security context per peer UE | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.3.3.1.4.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

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

5.3.3.1.4.3 Security establishment during connection set-up

The clause describes how security is established during connection set-up. The signalling flow is shown in figure 5.3.3.1.4.3-1.



Figure 5.3.3.1.4.3-1: Security establishment at connection set-up

1. UE\_1 has sent a Direct Communication Request to UE\_2. This message shall include UE\_1's security capabilities (the list of algorithms that UE\_1 will accept for this connection) and UE\_1's signalling security policy. The UE\_1 shall also include Nonce\_1 (for session key KNRP-sess generation), and the most significant 8-bits of the KNRP-sess ID in this message if UE\_1's signalling integrity protection policy is either "REQUIRED" or "PREFERRED". The most significant 8-bits of the KNRP-sess ID shall be chosen such that UE\_1 will be able to locally identify a security context that is created by this procedure using the KNRP-sess ID. The message may also include a KNRP ID if the UE\_1 has an existing KNRP for the UE that it is trying to communicate with. The absence of the KNRP ID parameter indicates that UE\_1 does not have a KNRP for UE\_2. The message also contains Key\_Est\_Info (see clause 5.3.3.1.3.2).

2. UE\_2 shall reject the Direct Communication Request if UE\_1's signalling security policy is "NOT NEEDED" while UE\_2's security policy is "REQUIRED". UE\_2 shall also reject the Direct Communication Request if UE\_1's signalling security policy is "REQUIRED" while UE\_2's security policy is "NOT NEEDED". UE\_2 may initiate a Direct Auth and Key Establish procedure with UE\_1. This is mandatory if the UE\_2 does not have the KNRP and KNRP ID pair indicated in step 1, and signalling is needed to establish the keys for the particular use case.

3. UE\_2 shall send the Direct Security Mode Command message to UE\_1. This message shall only contain the MSB of KNRP ID and optionally Key\_Est\_Info if a fresh KNRP is to be generated (see clause 5.3.3.1.3). UE\_2 shall include the Chosen\_algs parameter to indicate which security algorithms the UEs will use to protect the data in the message. The Chosen-algs may only indicate the use of the NULL integrity algorithm if UE\_2's signalling integrity security policy is either NOT NEEDED or PREFERRED. UE\_2 shall also return the UE\_1's security capabilities and UE\_1's signalling security policy to provide protection against bidding down attacks. In the case that the NULL integrity algorithm is chosen, the NULL confidentiality algorithm shall also be chosen and UE\_2 shall set the KNPR-sess ID of this security context to the all zero value.

The following procedures in step 3 shall only be executed if the UE\_2 decides to at least activate the integrity security protection for this connection: UE\_2 shall also include Nonce\_2 to allow a session key to be calculated, as well as the least significant 8-bits of KNRP-sess ID in the messages. These bits are chosen so that UE\_2 will be able to locally identify a security context that is created by this procedure. UE\_2 shall calculate KNRP-Sess from KNRP and both Nonce\_1 and Nonce\_2 (see clause A.3) and then derive the confidentiality (if applicable) and integrity keys based on the chosen algorithms (clause A.2). UE\_2 shall integrity protect the Direct Security Mode Command before sending it to UE\_1. UE\_2 is then ready to receive both signalling and user plane traffic protected with the new security context. UE\_2 shall form the KNRP-sess ID from the most significant bits it received in step1 and least significant bits it sent in step3.

4. On receiving the Direct Security Mode Command, the UE\_1 shall first check the Chosen\_algs and shall accept the NULL integrity algorithm only if its security policy for signalling integrity protection is either NOT NEEDED or PREFERRED. Then UE\_1 shall check the returned UE\_1's security capabilities and UE\_1's signalling security to avoid bidding down attacks if NULL integrity algorithm is selected for signalling integrity protection. If the above check passes, UE\_1 shall send unprotected Direct Security Mode Complete message to UE\_2. UE\_1 shall set the KNRP-sess ID of this security context to the all zero value.

Under the condition of non-NULL integrity algorithm indicated in the Chosen\_algs, UE\_1 shall first check that the received LSB of KNRP-sess ID is unique, by checking that it has not been sent by another UE responding to this Direct Communication Request i.e. such that resulting KNRP-sess ID is not already being used for another link. If the LSB of KNR-sess ID is not unique, then UE\_1 shall respond with a Direct Security Mode Reject message including a cause value to specify that the LSB of KNRP-sess ID is not unique. The peer UE-2 receiving a Direct Security Mode Reject message shall inspect the cause value and, if the cause is related to the session identifier uniqueness then, the UE-2 shall generate a new LSB of KNRP-sess ID and reply to UE-1 again (i.e., UE-2 shall send a Direct Security Mode Command message with the new LSB of KNRP-sess ID). UE\_2 shall associate the new LSB of KNRP-sess ID with the security context that is created in step 3. UE-2 shall erase the former LSB of KNRPP-sess ID from its memory. On receiving this new Direct Security Mode Command, UE\_1 shall process the message from the start of step 4.

If the LSB of KNPR-sess ID is unique, UE\_1 shall calculate KNRP-sess and the confidentiality and integrity keys in the same way as UE\_2. UE\_1 shall check that the returned UE\_1 security capabilities and UE\_1's signalling security policy are the same as those it sent in step 1. UE\_1 shall also check the integrity protection on the message. If both these checks pass, then UE\_1 creates a security context to be associated with the KNRP-sess ID. UE\_1 is ready to send and receive signalling and user plane traffic with the new security context. UE\_1 shall send integrity protected and confidentiality protected Direct Security Mode Complete message to UE\_2. UE\_1 shall form the KNRP-sess ID from the most significant bits it sent in step1 and least significant bits it received in step3. KNRP-sess ID is used to locally identify the security context that is created by this procedure.

5. If the Chosen\_algs in step 3 includes non-NULL integrity algorithm, UE\_2 checks the integrity protection on the received Direct Security Mode Complete. If this passes, UE\_2 is now ready to send user plane data and control signalling protected with the new security context. UE\_2 deletes any old security context it has for UE\_1.

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