**3GPP TSG-SA3 Meeting #101e *S3-203051-r1***

**e-meeting, 9 – 20 November 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.536** | **CR** | **0021** | **rev** | **1** | **Current version:** | **16.1.0** |  |
|  |
| *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:***  | Clarification on the security policy handling |
|  |  |
| ***Source to WG:*** | Huawei |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | eV2XARC |  | ***Date:*** | 2020-10-22 |
|  |  |  |  |  |
| ***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 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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | Currently, the receiving UE could determine whether to set the protection to on or off when both UP security policies are “Preferred”, i.e.“*User plane confidentiality protection set to off or on otherwise (i.e. when both the received user plane security policy and its own user plane security policy for the service had the confidentiality set to PREFERRED).*”The signalling security policy handling is similar.However, how does the receiving UE determine is not clear. It is suggest to clarify the policy which the receiving UE can use to make a decision, e.g. based on the UE’s computation and storage capability. |
|  |  |
| ***Summary of change:*** | Clarify that its owner security capacity can be used to determine the UP configuration. |
|  |  |
| ***Consequences if not approved:*** | Unclear specification. |
|  |  |
| ***Clauses affected:*** | 5.3.3.1.4.2.3 |
|  |  |
|  | **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:*** |  |

**\*\*\*\* START OF CHANGE 1 \*\*\*\***

5.3.3.1.4.2.3 Security policy handling

For a NR PC5 unicast link, the UE shall be provisioned with the following:

- The list of V2X services, e.g. PSIDs or ITS-AIDs of the V2X applications, with Geographical Area(s) and their security policy which indicates the following:

- Signalling integrity protection: REQUIRED/PREFERRED/NOT NEEDED

- Signalling confidentiality protection: REQUIRED/PREFERRED/NOT NEEDED

- User plane integrity protection: REQUIRED/PREFERRED/NOT NEEDED

- User plane confidentiality protection: REQUIRED/PREFERRED/NOT NEEDED

NOTE 1: No integrity protection on signalling traffic enables services that do not require security.

NOTE 2: Ensuring that only a connection with security is used for a V2X service is guaranteed if the signalling integrity security policy of at least one of the UEs for that V2X service is set to REQUIRED. It is recommended to set this security policy to REQUIRED in order to guarantee security protection.

NOTE 3: While some V2X applications are similar to Emergency Services and may require similar security policies handling, such V2X applications are outside of the scope of 3GPP.

REQUIRED means the UE shall only accept the connection if a non-NULL confidentiality or integrity algorithm is used for protection of the traffic.

NOT NEEDED means that the UE shall only establish a connection with no security.

PREFFERED means that the UE may try to establish security but may will accept the connection with no security. One use of PREFERRED is to enable a security policy to be changed without updating all UEs at once.

The handling of signalling security policy proceeds as follows:

- At initial connection, the initiating UE includes its signalling security policy in the Direct Communication Request message. The receiving UE(s) takes this into account when deciding whether to accept or reject the request and when deciding the agreed security policy to be sent back in the Direct Security Mode Command message. The initiating UE can reject the Direct Security Mode Command if the algorithm choice does not match its policy (see clause 5.3.3.1.4.3 for full details of the handling).

All the UP data of PC5 unicast link shall have the same security.

The handling of the user plane security policy proceeds with the following sequence:

a) At initial connection, the UE that sent the Direct Communications Request shall include the user plane security policy for the service in the Direct Security Mode Complete message.

b) If the signalling confidentiality protection is not activated, then UEs shall treat their user plane confidentiality policy for the V2X service for this connection as NOT NEEDED and the receiving UE shall set confidentiality for the user plane to off.

c) The receiving UE shall reject the Direct Communication Request when the following cases occur: 1) if the received user plane security policy had either confidentiality/integrity set to NOT NEEDED and its own corresponding policy is set to REQUIRED or, 2) if the received user plane security policy had either confidentiality/integrity set to REQUIRED and its own corresponding policy is set to NOT NEEDED.

d) Otherwise, the receiving UE may accept the Direct Communication Request and the response message shall include the configuration of user plane confidentiality protection based on the agreed user plane security policy, set as follows:

1) User plane confidentiality protection set to off if the received user plane security policy had either confidentiality set to NOT NEEDED and/or its own user plane security policy for the service is set to NOT NEEDED; or

2) User plane confidentiality protection set to on if the received user plane security policy had either confidentiality set to REQUIRED and/or its own user plane security policy for the service its own corresponding policy is set to REQUIRED; or

3) User plane confidentiality protection set to off or on otherwise (i.e. when both the received user plane security policy and its own user plane security policy for the service had the confidentiality set to PREFERRED).

User plane integrity protection set following the same rules as confidentiality protection but based on the received and its own user plane integrity protection policy for the service.

NOTE: When both UE’s signaling and the user plane security policies are PREFERRED, the receiving UE should set the confidentiality and/or integrity protection to on. There might be UE constraints limiting the enablement of confidentiality and/or integrity protection, e.g. UE hardware platform resource constrains/limitations.

Due to the purpose of adding a new V2X service to an existing PC5 unicast link, if the signalling and user plane security policies of the new V2X service are satisfied by the security in use for the PC5 unicast link, the initiating UE shall send the Link Modification Request to the receiving UE. The receiving UE shall reject the Link Modification Request if the security in use for the PC5 unicast link does not match the signalling and user plane security policies of the new V2X service.

The V2X layer of the UE shall pass the security configurations to its AS layer. The security configurations are mutually agreed by both sides' UEs, including the configuration of confidentiality and integrity protection.

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