**3GPP TSG-WG SA2 Meeting #152E *S2-2205580***

**E-meeting, August 17 - 26, 2022 (*revision of S2-220xxxx*)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **23.501** | **CR** | **DUMMY** | **rev** | **-** | **Current version:** | **17.5.0** |  |
|  | | | | | | | | |
| *For* ***HE******LP*** *on using this form: comprehensive instructions can be found at  http://www.3gpp.org/Change-Requests.* | | | | | | | | |
|  | | | | | | | | |

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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Per-QoS Flow User Plane security control | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Intel | | | | | | | | | |
| ***Source to TSG:*** | SA2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI18 | | | | |  | ***Date:*** | | | 2022-08-10 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *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. | | | | | | | | *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:*** | | In many cases the user plane traffic is encrypted in end-to-end manner between the application client in the UE and the application server in the data network. In such cases the use of the UP integrity protection and UP confidentiality protection does not bring much value, while it requires the UE and the gNB to unnecessarily waste processing resources for ciphering and deciphering, as well as for calculation of the message authentication codes on per packet basis. With the ever-increasing data rates of service data flows it is expected that the avoidance of unnecessary processing for user plane security will be beneficial for both the UEs and the gNBs.  Conversely, in some cases the AF may want to make sure that 5GS will activate user plane security on the radio interface. This would be useful for the cases where the User Plane Security Enforcement information (currently determined based on subscription and the DNN/S-NSSAI) is defaulted to “Preferred” or “Not Needed”. In this case the AF request would guarantee the activation of UP security for the related radio bearer, while the remaining traffic on the PDU Session remains without UP security on the radio. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clause 5.10.3: introduces control of User Plane security on per-QoS Flow basis. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Unnecessary waste of processing resources in UE and gNB. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.10.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \* \* \* \*

### 5.10.3 PDU Session User Plane Security

The User Plane Security Enforcement information provides the NG-RAN with User Plane security policies for a PDU session. It indicates:

- whether UP integrity protection is:

- Required: for all the traffic on the PDU Session UP integrity protection shall apply.

- Preferred: for all the traffic on the PDU Session UP integrity protection should apply.

- Not Needed: UP integrity protection shall not apply on the PDU Session.

- whether UP confidentiality protection is:

- Required: for all the traffic on the PDU Session UP confidentiality protection shall apply.

- Preferred: for all the traffic on the PDU Session UP confidentiality protection should apply.

- Not Needed: UP confidentiality shall not apply on the PDU Session.

When either the UP integrity protection or the UP confidentiality protection for the PDU Session is indicated as “Required” or “Preferred”, the SMF may include a User Plane Security Indication set to “Not Needed” for specific QoS Flow(s) of that PDU Session. When the User Plane Security Indication set to “Not Needed” is available for a QoS Flow, the NG-RAN may turn off the UP integrity protection and UP confidentiality protection for the radio bearer corresponding to that QoS Flow.

When either the UP integrity protection or the UP confidentiality protection for the PDU Session is indicated as “Preferred” or “Not Needed”, the SMF may include a User Plane Security Indication set to “Required” for specific QoS Flow(s) of that PDU Session. When the User Plane Security Indication set to “Required” is available for a QoS Flow, the NG-RAN shall turn on the UP integrity protection and UP confidentiality protection for the radio bearer corresponding to that QoS Flow.

User Plane Security Enforcement information applies only over 3GPP access. Once determined at the establishment of the PDU Session the User Plane Security Enforcement information applies for the life time of the PDU Session.

NOTE 1: Applicability of UP integrity protection of UP Security Enforcement is defined in TS 33.501 [29] and TS 38.300 [27].

The SMF determines at PDU session establishment a User Plane Security Enforcement information for the user plane of a PDU session based on:

- subscribed User Plane Security Policy which is part of SM subscription information received from UDM; and

- User Plane Security Policy locally configured per (DNN, S-NSSAI) in the SMF that is used when the UDM does not provide User Plane Security Policy information.

- The maximum supported data rate per UE for integrity protection for the DRBs, provided by the UE in the Integrity protection maximum data rate IE during PDU Session Establishment. The UE supporting NR as primary RAT, i.e. NG-RAN access via Standalone NR, shall set the Integrity protection maximum data rate IE for Uplink and Downlink to full rate at PDU Session Establishment as defined in TS 24.501 [47]. A UE not supporting NR as primary RAT and supporting E-UTRA connected to 5GC, shall set the Integrity protection maximum data rate IE for Uplink and Downlink to NULL at PDU Session Establishment as defined in TS 24.501 [47].

The User Plane Security Indication is provided from AF to PCF (via NEF) in association with a Flow description. The PCF provides the User Plane Security Indication to SMF inside the PCC rule. SMF forwards the User Plane Security Indication to NG-RAN inside the N2 SM information.

The User Plane Security Enforcement information provides the MME with User Plane integrity protection policies for the PDU session (PDN Connection). The information indicates whether UP integrity protection is:

- Required: for all the traffic on the PDU Session (PDN Connection) UP integrity protection shall apply.

- Preferred: for all the traffic on the PDU Session (PDN Connection) UP integrity protection should apply.

- Not Needed: UP integrity protection shall not apply on the PDU Session (PDN Connection).

In turn, the MME provides per EPS bearer User Plane Security Enforcement information to the E-UTRAN. All the bearers within a PDN Connection share the same User Plane integrity protection policies.

The UE capability to support user plane integrity protection with EPS is indicated to AMF in the S1 UE network capability information. If the UE supports user plane integrity protection with EPS, and the AMF supports the associated functionality, the AMF indicates this to SMF at PDU Session Establishment using NG-RAN. If the UE and AMF support user plane integrity protection with EPS, for PDU Sessions with UP integrity protection of UP Security Enforcement Information set to Required, the SMF may perform the EPS bearer ID allocation procedure as described in TS 23.502 [3] clause 4.11.1.4. If the UE does not support user plane integrity protection with EPS or the AMF does not support the associated functionality, the SMF shall not trigger the EPS bearer ID allocation procedure in clause 4.11.1.4 of TS 23.502 [3].

Unless the UE, the serving eNB and the MME support user plane integrity protection with EPS, the SMF+PGW-C shall reject a PDN Connection Establishment using EPS if the UP Security Enforcement Information has UP integrity protection set to Required.

The SMF+PGW-C shall (e.g. based on the received RAT Type) reject a PDN Connection Establishment using GERAN/UTRAN if the UP Security Enforcement Information has UP integrity protection set to Required.

NOTE 2: This assumes that the optional user plane integrity protection for GPRS specified in Release 13 has not been deployed.

The SMF may, based on local configuration, reject the PDU Session Establishment request depending on the value of the maximum supported data rate per UE for integrity protection.

NOTE 3: Reasons to reject a PDU Session Establishment request can e.g. be that the UP Integrity Protection is determined to be "Required" while the maximum supported data rate per UE for integrity protection is less than the expected required data rate for the DN.

NOTE 4: The operator can take care to reduce the risk of such rejections when configuring the subscribed User Plane Security Policy for a DNN. For example, the operator may apply integrity protection "Required" only in scenarios where it can be assumed that the UE maximum supported data rate per UE for integrity protection is likely to be adequate for the DN.

The User Plane Security Policy provide the same level of information than User Plane Security Enforcement information.

User Plane Security Policy from UDM takes precedence over locally configured User Plane Security Policy.

The User Plane Security Enforcement information may include the maximum supported data rate for integrity protection provided by the UE, is communicated from SMF to the NG-RAN for enforcement as part of PDU session related information. If the UP Integrity Protection is determined to be "Required" or "Preferred", the SMF also provides the maximum supported data rate per UE for integrity protection as received in the Integrity protection maximum data rate IE. This takes place at establishment of a PDU Session or at activation of the user plane of a PDU Session. The NG-RAN rejects the establishment of UP resources for the PDU Session when it cannot fulfil User Plane Security Enforcement information with a value of Required. The NG-RAN may also take the maximum supported data rate per UE for integrity protection into account in its decision on whether to accept or reject the establishment of UP resources. In this case the SMF releases the PDU Session. The NG-RAN notifies the SMF when it cannot fulfil a User Plane Security Enforcement with a value of Preferred.

NOTE 5: For example, the NG-RAN cannot fulfil requirements in User Plane Security Enforcement information with UP integrity protection set to "Required" when it cannot negotiate UP integrity protection with the UE.

It is responsibility of the NG-RAN to enforce that the maximum UP integrity protection data rate delivered to the UE in downlink is not exceeding the maximum supported data rate for integrity protection.

It is expected that generally the UP integrity protection data rate applied by the UE in uplink will not exceed the indicated maximum supported data rate, but the UE is not required to perform strict rate enforcement.

User Plane Security Enforcement information and the maximum supported data rate per UE for integrity protection is communicated from source to target NG-RAN node at handover. If the target RAN node cannot support requirements in User Plane Security Enforcement information, the target RAN node rejects the request to setup resources for the PDU Session. In this case the PDU Session is not handed over to the target RAN node and the PDU Session is released.

If the UE or the new eNB or the MME does not indicate support of user plane integrity protection with EPS, PDU Sessions with UP integrity protection of the User Plane Security Enforcement information set to Required are not transferred to EPS as follows:

- In the case of mobility without N26, the SMF+PGW-C shall reject a PDN connectivity request in EPS with handover indication if the UP integrity protection of the User Plane Security Enforcement is set to Required.

NOTE 6: As described in clause 5.17.2.3.3, the UE does not know before trying to move a given PDU Session to EPC, whether that PDU session can be transferred to EPC.

- In the case of idle mode and connected mode mobility with N26 to EPS, or mobility without N26, the SMF+PGW-C ensures that the PDU session is released.

If the UE, target eNB and the target MME indicate support of User Plane Integrity Protection with EPS, PDU Sessions with UP integrity protection of the User Plane Security Enforcement information set to Required are transferred from 5GS to EPS according to existing procedures.

For the bearers of PDN Connections with UP integrity protection set to Required, at (both idle mode and connected mode) mobility (including intra-TA mobility) to an eNB that does not support User Plane Integrity Protection with EPS, the MME shall inform the SMF+PGW-C and the SMF+PGW-C ensures that the PDU session is released.

At connected mode mobility from EPS to GERAN/UTRAN or to a part of the EPS that does not support User Plane Integrity Protection, the source E-UTRAN shall ensure that EPS bearers with UP integrity protection of the User Plane Security Enforcement information set to Required are not handed over.

In the case of idle mode mobility from an MME that supports User Plane Integrity Protection, to an MME that does not support User Plane Integrity Protection, the (home) SMF+PGW-C shall trigger (e.g. based on the lack of MME UPIP capability information) the release of the bearers of PDN Connections with UP integrity protection set to Required.

At any (e.g. idle mode) mobility from EPS to GERAN/UTRAN, the (home) SMF+PGW-C shall trigger (e.g. based on the received RAT Type) the release of the bearers of PDN Connections with UP integrity protection set to Required.

PDU Sessions with UP confidentiality protection of the User Plane Security Enforcement information set to Required and UP integrity protection of the User Plane Security Enforcement information not set to Required, are allowed to be handed over to EPS regardless of how UP confidentiality protection applies in EPS.

In the case of dual connectivity, the Integrity Protection is set to "Preferred", the Master NG-RAN node may notify the SMF when it cannot fulfil a User Plane Security Enforcement with a value of Preferred. The SMF handling of the PDU session with respect to the Integrity Protection status is up to SMF implementation decision.

\* \* \* \* End of changes \* \* \* \*