**3GPP TSG SA WG3 (Security) Meeting #94 ad-hoc *S3-190974***

**Kista (Sweden), 11 March – 15 March 2019** *revision of S3-190685*

**Source: Huawei, HiSilicon**

**Title: Solution #1 update**

**Document for: Approval**

**Agenda Item: 5.13**

# 1 Decision/action requested

***This contribution proposes a pCR for the update to solution #1 of TR 33.825.***

# 2 References

[1] 3GPP TR 23.725 Study on enhancement of Ultra-Reliable Low-Latency Communcation (URLLC) v0.4.0

# 3 Rationale

The solution #1 is proposing to address the user plane security polich handling for URLLC service. Since the whole solution details are about the standalone network architecture, for the agreed DC architecture which is applicable for the URLLC service as defined in TR 23.725[1], the solution details are not clear.

The contribution proposes the update of solution #1.

# 4 Detailed proposal

It is proposed to approve the following changes for inclusion in TR 33.825.

\*\*\* BEGIN CHANGES \*\*\*

## 6.1 Solution #1: Security solution for handling UP security policy for multiple PDU sessions for redundant data transmission

### 6.1.1 Introduction

This solution addresses key issue #3: UP security policy handling for multiple PDU sessions established for redundant data transmission.

According to TS 23.501 [xx] and TS 23.502 [xx], the SMF should determine and provide the UP security policy for a PDU session to the gNB connected to 5GC during the PDU session establishment procedure.

The UP security policy should indicate whether UP confidentiality and/or UP integrity protection shall be activated or not for all DRBs belonging to that PDU session. The UP security policy should be used by gNB to activate UP confidentiality and/or UP integrity for all DRBs belonging to the PDU session.

According to TS 23.501 [xx], the User Plane Security Policy provides the same level of information than User Plane Security Enforcement information. Once the User Plane Security Enforcement information is determined at the establishment of the PDU Session, it is provided to the UE and applies for the life time of the PDU Session. 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.

### 6.1.2 Solution details

The User Plane Secuirty Policy for multiple PDU Sessions used for redundant data transmission should have the same setting for encryption and for integrity protection. The gNB should not be allowed to override the UP Secuirty Policy received from the 5G Core Network. The setting defined in clause 5.10.3 TS 23.501[xx] should apply with the following modifications:

* Encryption:

- only "Required" or "Not Needed" is allowed;

- "Preferred" is not allowed:

* Integrity protection:

- only "Required" or "Not Needed" is allowed;

- "Preferred" is not allowed:

In addition, if redundant data transmission is taking place over E-UTRA (connected to 5GC), then the setting of "Required" for Integrity protection is not allowed.

When Dual Connectivity as described in Figured 5.3.1-1 of the KI #3 is used, both of the two redundant PDU sessions are initially established via the MgNB. The SMF shall provide two UP security policies for each of the two redundant PDU sessions to the MgNB during the PDU sessions establishment procedure, if SMF recognizes one of the UP security policies is not the same as the other one, the SMF shall modify the UP security policies to make sure them to be same.

However, MgNB shall ensure that the two redundant PDU sessions have the same UP integrity and encryption activation after the MgNB receives UP security policy and proceeds according to TS 33.501 [xx] clause 6.6.1.

### 6.1.3 Evaluation

The proposed solution needs to modify the existing UP security policy definition as specified in TS 23.501 [xx] which is provided to the NG-RAN by SMF for a PDU session. The modification is specific for URLLC services.For DC architecture used for URLLC service, the solution is applicable if the UP security policies which are used by Master node and Secondary node for redundant PDU session transmissions are the same.

Based on above analysis of the proposed solution, the solution is able to meet the potential security requirements of KI #3.

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