**3GPP TSG SA WG3 (Security) Meeting #94 ad-hoc *S3-190976***

**Kista (Sweden), 11 March – 15 March 2019** *revision of S3-190683*

**Source: Huawei, HiSilicon**

**Title: Evaluation for solution #3**

**Document for: Approval**

**Agenda Item: 5.13**

# 1 Decision/action requested

***This contribution proposes a pCR for add the evaluation for solution #3 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 contribution is proposing to add evaluation part for solution #3 to delete the following Editor’s note: The evaluation of the solution is FFS.

# 4 Detailed proposal

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

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

## 6.3 Solution #3: Security policy handling for redundant data transmission

### 6.3.1 Introduction

This solution addresses Key Issue#3 and Key Issue#4 by identifying how to handle the security policy for redundant transmission. In this solution, it is assumed that the redundant transmissions are established by two independent paths which require two RAN nodes and two UPFs to a single UE. This solution is based on the following architecture (see TR23.724 v0.4.0 clause 6.1):



Figure 6.3.1-1 redundant transmission architecture

This architecture is based on Dual Connectivity architecture, except that there are two UPFs.

According to the figure above, if there are two PDU sessions that take two different user plane paths which are used to transfer the redundant data, the security policy for the redundant PDU sessions shall be ensured to be the same.

### 6.3.2 Solution details

## 6.3 Solution #3: Security policy handling for redundant data transmission

### 6.3.1 Introduction

This solution addresses Key Issue#3 and Key Issue#4 by identifying how to handle the security policy for redundant transmission. In this solution, it is assumed that the redundant transmissions are established by two independent paths which require two RAN nodes and two UPFs to a single UE. This solution is based on the following architecture (see TR23.724 v0.4.0 clause 6.1):



Figure 6.3.1-1 redundant transmission architecture

This architecture is based on Dual Connectivity architecture, except that there are two UPFs.

According to the figure above, if there are two PDU sessions that take two different user plane paths which are used to transfer the redundant data, the security policy for the redundant PDU sessions shall be ensured to be the same.

### 6.3.2 Solution details

If the high-reliablity is fulfilled by redundant transmission based on NR-DC architecture, the following user plane security policy mechanism shall apply:

In case where one of the redundant PDU Session data transmissions is terminated at the MgNB and the other one is terminated at the SgNB, these two redundant data transmissions shall have the same UP integrity protection and ciphering policy. In addition, the MgNB shall inform the SgNB with its UP integrity protection and encryption activation decision of the PDU Session which is terminated at MgNB but is redundant with the other PDU Session terminated at the SgNB.

MgNB shall make the decision on UP encryption protection and integrity protection according to the UP security policy for these two redundant transmissions. The MgNB shall inform the SgNB the encryption protection and integrity protection indications of the transmission terminated at itself via SgNB Addition/Modification Request message during when the corresponding redundant transmission is moved to SgNB. At the reception of the indications, the SgNB shall attempt to comply with the request from MgNB to ensure these two UP ciphering protection indications are the same.

If the UP security policy indicates UP integrity protection “not needed”, the MgNB and SgNB shall always deactivate UP integrity protection. If the UP security policy indicates UP encryption protection “not needed”, the MgNB shall have the encryption protection either “on” or “off”, and inform the decision to SgNB.

Editor’s Note: The above paragraph needs more clarification.

Particularly, in case of the MgNB cannot activate UP confidentiality and/or integrity when the received UP security policy is "Required", the MgNB shall reject establishment of UP resources for the PDU Session and indicate the decision to the SgNB in order to make sure these two redundant transmissions have the same UP encryption protection and integrity protection.

In all cases, the SgNB shall inform the UP integrity protection and encryption indications to the MgNB in the SgNB Addition/Modification Request Acknowledgement message. The MgNB shall forward the UP integrity protection and encryption indications to the UE in RRC Connection Reconfiguration message.

### 6.3.3 Evaluation

The solution is applicable for the redundant data transmission of URLLC services based on Dual Connectivity architecture. The solution fulfils the potential security requirements of KI #3.

Editor’s note: The further evaluation of the solution is ffs.

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