**3GPP TSG SA WG3 (Security) Meeting #94 ad-hoc *S3-190971***

**Kista (Sweden), 11 March – 15 March 2019** *merge of S3-190682***,** *S3-190631*

**Source: Huawei, HiSilicon, NEC**

**Title: Adding some clarification and removing the ENs for solution #5**

**Document for: Approval**

**Agenda Item: 5.13**

# 1 Decision/action requested

***This contribution proposes a pCR for adding more clarification to solution #5 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 some clarification for solution 5 and delete the Editor’s note in Solution details part. It makes how to derive the key for URLLC clearer.

The contribution proposes the modification of solution #5.

# 4 Detailed proposal

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

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

## 6.5 Solution #5: Security for redundant data transmission

### 6.5.1 Introduction

The solution addresses the Key issues # 1 and #2 in the present document. This solution also addresses Key issue #1: Supporting high reliability by redundant transmission in user plane in TR 23.725 [xx] and also complies with the related SA2 conclusions specified in TR 23.725 [xx] clause 8.1. Adopting different security protection for the redundant user planes at the UE for two different gNBs will increase the computation complexity, drain battery life and impacts the low latency and reliability requirements of the URLLC services. However, the potential danger of applying separate security protection outweights the convenience of using the same security contexts. For example, if the same security key is used for the two redundant user planes, then having one of the two UP paths compromised implies that both the two redundant user planes' security is compromised. To prevent this situation, it is proposed to use a scheme in which cryptographic separation is achieved while using the same key for both of the two redundant user planes, similar to the security procedures for dual connectivity specified in TS 33.501 [xx]. This also results in minimal impact to the URLLC requirement specific changes.

### 6.5.2 Solution details

The solution proposes that both PDU sessions transferring via two user plane paths are using the same key based on the SgNB addition procedure of Dual Connectivity. In this case, the MgNB applies the security key (KUR key) derived from the KgNB and provides to the SgNB in the SgNB Addition request message over the Xn-C interface between MgNB and SgNB as specified in TS 33.501 [xx]. The security key is also used by MgNB to protect one of the redundant transmissions. The SgNB then derives its own security context using other input parameters such as the PDU session information specific to the redundant user plane path, URLLC identification information and any other required information along with KUR to the KDF to derive the security context for the redundant user plane protection. Other input parameters such as the PDU session information to the redundant user plane data protection will ensure cryptographic separation between the redundant user plane data. After that, the MgNB and the SgNB shall generate their own RRC and UP keys from KUR as well as UE side as described in Annex A.8 of TS 33.501 [xx] except that the input key is KUR. This mechanism can prevent attackers from identifying the related redundant data stream.

During RRC connection establishment between UE and MgNB the KUR is derived at MgNB, where KgNB, information on URLLC connection and PDU session such as their identifiers can be input to the KDF (Key Derivation Function) to derive the key. Random value and data counter value at MgNB, which are sent from MgNB to UE, can also be input to the KDF. Security is established between UE and MgNB, where integrity and confidentiality protection for uplink data (from UE to MgNB) is configured with security keys KURint and KURenc, respectively for URLLC communication. MgNB sends SgNB addition request for URLLC which includes security key, KUR, information indicating that this request is for URLLC, and security capabilities for integrity protection and ciphering used for the data from UE. The security capabilities are the same as the ones used in MgNB.When two redundant data is transmitting, it is necessary to make separation between multiple redundant PDU Session handled between UE and gNB. The KUR key is introduced in this proposal for securing the redundant data transmission. KUR key gets refreshed for different PDCP counts when there is a redundant data transmission.

NOTE 1: KUR key should be the specific key for the URLLC services based on Dual Connectivity architecture. Particularly, if there are only two redundant data transmission PDU sessions of multiple PDU sessions, the specific key KUR key should be used to identify the URLLC services.

Editor’s Note: Further security analysis on using the same key at MN and SN is needed.



Figure 6.5.2-1 security context derivation procedure

### 6.5.3 Evaluation

The solution fulfill the cryptographic separation requirement of KI #1. Moreover, the solution fulfil the confidential protection and integrity protection for radio bears of redundant transmission requirement of KI #2.

Editor’s note: More justification for not using KSN for URLLC service is required.

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