**3GPP TSG-SA3 Meeting #115 *S3-240323***

**Athens, Greece, 26 February - 1 March 2024**

**Source: KDDI Corporation**

**Title: New Key Issue on different cryptographic key lengths in dual connectivity scenarios**

**Document for: Approval**

**Agenda Item: 5.5 New Study on enabling a cryptographic algorithm transition to 256-bits**

# 1 Decision/action requested

***Approve the pCR to TR 33.700-41***

# 2 References

[1] TS 33.501

# 3 Rationale

This contribution proposes a new key issue on different cryptographic key lengths in dual connectivity.

# 4 Detailed proposal

For SA3 to accept this proposal.

\*\*\* Start of 1st Change \*\*\*

## 5.X Key Issue #X: Different cryptographic key lengths in dual connectivity scenarios

### 5.X.1 Key issue details

The transition to 256-bit cryptographic algorithms may lead to network deployments that only partially support 256-bit cryptographic algorithms. In the context of dual connectivity, this means that there may be cases where not all RAN Nodes support cryptographic algorithms using 256-bit keys, e.g., because some of them have not been upgraded to a sufficiently recent Release, yet.

In these situations, there is a risk of inconsistent key sizes being used to protect different communication paths associated to a single subscriber session when using dual connectivity. Specifically, one can envisage a scenario in which the UE is connected to both a Master Node (MN) or Primary RAN and Secondary Node (SN) or Secondary RAN. Assuming a mixed deployment in which the MN already supports 256-bit cryptographic algorithms, but the SN only supports 128-bit cryptographic algorithms (or vice versa), can lead to the situation where the RRC and UP between the UE and the MN or SN is protected with algorithms using different length input keys, i.e. with algorithms of different strength. There will be no issue when MN and SN are carrying different data, while this can be an issue when the same data is sent on MN and SN.

A similar issue can be found when looking at integrity protection of the UP in Dual Connectivity for split PDUs. According to TS 33.501 [1] clause 6.10.4, ‘in the case of split PDU session where some of the DRB(s) is terminated at the MN and some DRB(s) is terminated at the SN, the MN shall ensure that all DRBs which belong to the same PDU session have the same UP integrity protection and ciphering activation’, which means that even though the SN can independently select the algorithm (clause 6.10.3.3), it has to at least provide the same level of security for DRBs that are offloaded to the SN.

Furthermore, TS 33.501 (clause 6.10.4) defines the desired behaviour for NGEN-DC, NE-DC, and NR-DC scenarios in case the UE does not indicate support of UP integrity protection with a ng-eNB and depending on if the UP integrity protection is required or not in the UE security policy like the below.

|  |  |  |  |
| --- | --- | --- | --- |
|  | UP Integrity Protection “required” | UP Integrity protection “preferred” | UP Integrity Protection “not needed” |
| NGEN-DC scenario | MN shall reject the PDU session.  **Result:** No DC. | MN shall always deactivate UP integrity protection. In this case, the SN shall always deactivate the UP integrity protection of any PDU session terminated at the SN.  **Result:** No UP integrity protection | MN and SN shall always deactivate UP integrity protection |
| NE-DC scenario | If the MN decides to activate the UP integrity protection for this PDU session, the MN shall not offload any DRB of the PDU session to the SN.  **Result:** No DC if UP integrity protection is turned on. | If the MN has activated any of this PDU session DRBs with UP integrity protection "on", the MN shall not offload any DRB of this PDU session to the SN. However, if the MN has activated all DRBs of this PDU session with integrity protection "off", the MN may offload DRBs of this PDU session to the SN. In this case, the SN shall not activate the UP integrity protection and shall always set the UP integrity protection indication to "off".  **Result:** No UP integrity protection *OR* no DC if UP integrity protection was "on". |
| NR-DC scenario | The MN makes the decision for PDU sessions that are terminated at the MN while the SN makes the decision for PDU sessions that are terminated at the SN.  Note that UP integrity is set on a per PDU basis and offloaded DRBs need to comply. | The MN makes the decision for PDU sessions that are terminated at the MN while the SN makes the decision for PDU sessions that are terminated at the SN.  Note that UP integrity is set on a per PDU basis and offloaded DRBs need to comply. |

Extracted summary from TS 33.501

\*The scenarios above are defined as the following:

* NGEN-DC: NG-RAN E-UTRA-NR Dual Connectivity (NGEN-DC) is the variant when the UE is connected to one ng-eNB that acts as a MN and on gNB that acts as a SN
* NE-DC: NR-E-UTRA Dual Connectivity (NE-DC) is the variant when the UE is connected to one gNB that acs as a MN and one ng-eNB that acts as a SN.
* NR-DC: NR-NR Dual Connectivity (NR-DC) is the variant when the UE is connected to one gNB that acts as a MN and oone gNB that acts as a SN.

In summary, for Dual Connectivity all DRBs belonging to the same PDU session will have the same ciphering and integrity protection. From the table above, one can see that for UP Integrity protection there are cases where this uniformity of security is achieved by either not offloading DRB that has UP Integrity protection turned on, or by simply not turning on UP Integrity protection altogether.In other words, it is shown the current system is already going through checks for the UP integrity protection on the SN.

With the transition to 256-bit, this poses the question: In such a scenario, does the same apply for selection of the strength of cryptographic algorithms? And what is the expected behavior if consistent use of 256-bit security cannot be ensured?

### 5.X.2 Threats

The use of cryptographic algorithms with inconsistent key lengths could lead to different levels of protection on AS layer. Unless the entire network is updated to support 256-bit cryptographic algorithms, there is a challenge in securing a configuration policy on preference for 128-bit or 256-bit.

### 5.X.3 Potential security requirements

In dual connectivity, the addition of a secondary node shall not degrade the security available with the main node.

In dual connectivity, the 5G system shall provide a mechanism for the operator to allow or disallow the mixed use of 128-bit and 256-bit cryptographic algorithms for offloaded DRBs belonging to the same PDU.

\*\*\* End of 1st Change \*\*\*