**3GPP TSG-SA3 Meeting #115AdHoc-e *S3-241276-r1***

Electronic meeting, online, 15 - 19 April 2024

**Source: Nokia, Nokia Shanghai Bell**

**Title: Architecture Assumptions**

**Document for: Approval**

**Agenda Item: 5.5**

# 1 Decision/action requested

***It is proposed that the architecture is added to the TR.***

# 2 References

[x1] TR 33.700-41, Study on enabling a cryptographic algorithm transition to 256-bits, Release 19

[x2] S3-235091, SID on enabling a cryptographic algorithm transition.

# 3 Rationale

The architecture must be described, to be able to derive the deployment options and the corresponding and relevant assumptions in the study TR[x1].

# 4 Detailed proposal

\*\*\* START of 1st CHANGE \*\*\*

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

CF Cryptographic Function

CK Ciphering Key

IK Integrity Key

ME Mobile Equipment

NAS Non-Access Stratum

NGC next Generation Core Network

RAN Radio Access Network

RRC Radio Resource Control

SMC Security Mode Command

UE User Equipment

XNAP Xn Application Protocol

USIM Universal Subscriber Identity Module

XnAP Xn Application Protocol

\*\*\* END of 1st CHANGE \*\*\*

\*\*\* START of 2nd CHANGE \*\*\*

### 4.x Architecture

The 5G System consists of a next-generation core network (NGC), the gNB and the UE. The UE consists of the mobile equipment (ME) and the USIM. The 5G system can interwork with another 5G system and/or can interwork with LTE system. Although the objectives of the SID on enabling a cryptographic algorithm transition to 256-bits ([x2]) do not foresee the analysis of the interwork between 5G system and LTE system, it is nevertheless not excluded that an LTE system is connected to a 5G system and thus implicitly generating signalling messages to a 5G system. These signalling messages could be on RAN level nodes and/or Core Network level nodes.

The architectural aspects are illustrated by the following Figure 4.x-1

A diagram of a computer network

Description automatically generated

Figure 4.x-1 Architecture overview.

The following is applicable:

(1) The NAS messages are exchanged end-to-end between the AMF and the UE. These messages are integrity and cipher protected by NAS security. The security activation will be after successful execution of NAS security mode command (NAS SMC) procedure.

(2) The AS messages are exchanged between the gNB/ng-eNB and the UE. These RRC messages are protected by AS security. The security activation will be performed after successful execution of AS security mode command (AS SMC) procedure. Since NAS messages will be piggybacked and/or send standalone over RRC, implicit these NAS messages will be integrity and cipher protected by AS security. The algorithm selection for AS security and NAS security is independent.

(3) The transport signalling (like X2, Xn, S1, Ng) will be protected by NDS/IPsec. The algorithm selection for the transport security layers is independent from the AS and NAS security, therefore NDS/IPsec is out of scope of this enabling of cryptographic 256-bit support.

(4) The management plane (M-plane) will be protected by the security requirements for the Management Network Function and is out of scope for this enabling of cryptographic 256-bit support.

(5) The interwork between two 5G system gNB’s is over the Xn interface. The corresponding signalling will be performed by the Xn application protocol (XnAP). The algorithm selection for the protection is out of scope, because relates to transport security, nevertheless, the information exchange for features like handover, dual connectivity, etc. should be taken into consideration.

(6) The interwork between the LTE system and the 5G system is over the X2 interface. The corresponding signalling will be performed through the X2 application protocol (X2AP). Although the messages are protected by transport security (see (3)), the procedures for selecting the key-length of the AS security must be adapted. It cannot be excluded that an LTE system is connected to a 5G system and thus implicitly is generating signalling messages to a 5G system.

(7). (8) On Core Network level, the nodes need to interwork either 5G system internal or between 5G system and LTE system. Although the interwork with LTE system is out of scope, it cannot be excluded that LTE system is signalling towards the 5G system.

(9) The USIM includes the key K for the derivation of the CK and IK on UE side.

(10) The UDM/ARPF includes the key K for the derivation of the CK and IK on Network side.

\*\*\* END of 2nd CHANGE \*\*\*