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

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

**Source: KDDI Corporation**

**Title: DRAFT New Key Issue on different cryptographic key lengths across AMF change and AMF reallocation**

**Document for: Approval**

**Agenda Item: TBD**

# 1 Decision/action requested

***Approve the pCR to TR 33.700***

# 2 References

None

# 3 Rationale

This contribution proposes a new key issue for different cryptographic key lengths across AMF change and AMF reallocation.

# 4 Detailed proposal

For SA3 to accept this proposal.

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

## 5.X Key Issue #X: Different cryptographic key lengths across AMF change and AMF reallocation

### 5.X.1 Key issue details

As the 5G system transitions to 256-bit cryptographic algorithms, the situation may arise that a network deployment only partially supports 256-bits. That is, certain network elements are already upgraded to support 256-bit cryptographic algorithms, while others do not support them, yet.

In these scenarios, there is a risk of different key sizes being used for NAS security to protect a single session as the UE moves through the network and AMF changes or AMF reallocations occurs, depending on the AMF the UE is connected to. **To illustrate the problem, assume that the UE is capable of 256-bit cryptographic algorithms:**

1. The UE is attached to an AMF that supports 256-bit cryptographic algorithms. Therefore, a 256-bit cryptographic algorithm is selected.
2. Next, the UE hands over to an AMF that does not support 256-bit cryptographic algorithms. Therefore, the algorithm agreed between the UE and the AMF is a 128 bit-algorithm.
3. Next, the UE is again handed over, this time to an AMF that does support 256-bit cryptographic algorithms. As such, a 256-bit cryptographic algorithm is selected.

As the above example illustrates, AMF changes (e.g., due to a N2 handover or AMF reallocation) can pose a challenge in such a mixed deployment scenario: What is the expected handover behaviour of UE and network? Is it possible to realize a uniform 256-bit cryptographic protection even if not all AMFs are upgraded and configured to support 256 bits or, alternatively, is it possible to have a mechanism that allows for more uniform algorithm strength to avoid unnecessary switching between algorithm strength either way?

### 5.X.2 Threats

**Unless source AMF and target AMF both support** the same algorithms, a change in algorithm strength may occur at every AMF change / AMF reallocation. Such discrepancies are undesirable from a security point of view.

### 5.X.3 Potential security requirements

The 5G System should be able to ensure uniform cryptographic key lengths for NAS security across AMF change and AMF reallocation to avoid unnecessary switching between algorithm strength.

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