**3GPP TSG-SA3 Meeting #115AdHoc-e *S3-241308-r1***

Electronic meeting, online, 15 - 19 April 2024

**Source: Huawei, HiSilicon, Interdigital, Ericsson, Nokia, Nokia Shanghai Bell, Intel, Xiaomi, China Telecom**

**Title: Addressing the editor's note in the key issue on store and forward Satellite Operation**

**Document for: Approval**

**Agenda Item: 5.7**

# 1 Decision/action requested

***Approve the pCR to TR 33.700-29***

# 2 References

[1] TR 23.700-29

# 3 Rationale

There is an Editor’s Note on the feasibility of the denial of service (i.e. caused by false user-plane data or control-plane data). This contribution proposes to add the corresponding threat illustrating the potential denial of service caused by false user-plane data.

# 4 Detailed proposal

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

### 5.1.2 Security threats

Due to the nature of the S&F mode during the feeder link’s intermittent unavailability, the following threats can manifest themselves:

- When the UE and 3GPP network cannot mutually authenticate, such condition may cause availability issue.

- Without authentication, confidentiality, integrity, and anti-replay protection there will be no security protection of the communication between UE, 3GPP system on board satellite, and ground-based 3GPP systems.

For the uplink control plane data (e.g. NAS message) and user plane data (e.g. if integrity protection is not activated), the 3GPP systems on board the satellite are not able to verify its integrity. It is hard to detect whether the data is sent from a genuine UE or an attacker. All the uplink data needs to be stored during the feeder or ISL links’ period of unavailability. Hence, the storage capacity can be easily exhausted by spoofed data with the attack over the air. This issue is amplified by the inability to upgrade hardware (e.g., radios, memory) on board of satellite. As an example, in case of the incomplete AKA procedure, user-plane data or control-plane data from unauthorized UE, the storage resource of on board satellite 3GPP system may be exhausted, resulting in the denial of service (DoS) attack.

NOTE: The risk of resource depletion of the 3GPP system is dependent on the agreed architecture solution direction of S&F KI in TR 23.700-29 [2].

### 5.1.3 Potential security requirements

The 3GPP system shall support mutual authentication between the UE and the 3GPP network in the Store and Forward Satellite Operation.

The 3GPP system shall support means to provide confidentiality, integrity, and anti-replay protection for user-plane and control-plane messages between UE and the 3GPP network in the Store and Forward Satellite Operation.

The 3GPP system shall support means to mitigate the potential denial of service attack in the Store and Forward Satellite Operation.

Editor’s Note: whether there are more security requirements is FFS.

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