**3GPP TSG-SA3 Meeting #116 *draft\_S3-242622-r2***

Jeju, Republic of Korea, 20th – 24th May 2024 *is the revision of S3-241984*

**Source: Huawei, HiSilicon,** **Deutsche Telekom, Xiaomi**

**Title: New key issue about UPF exposing new IP communication endpoint**

**Document for: Approval**

**Agenda Item: 5.15**

# 1 Decision/action requested

***Approve the pCR to TR 33.754[1].***

# 2 References

[1] 3GPP TR 33.754: "Study on security aspects for Multi-Access (DualSteer + ATSSS Ph-4) ".

[2] 3GPP TR 23700-54: "Study on Multi-Access (DualSteer and ATSSS\_Ph4) ".

# 3 Rationale

According to the objective of the SA3 R19 study FS\_MASSS\_Sec, we will study the security aspects of a simplified ATSSS architecture over non-3GPP access, in particular:

- whether to keep NAS security context on non-3GPP access.

- whether to keep IPsec on user plane and/or control plane of non-3GPP access.

- whether new security mechanisms are to be considered in UE procedures such as the registration and connectivity to the 5G system in the context of ATSSS between 3GPP access and non-3GPP access without 5G NAS.

For the PDU session establishment procedure over ATSSS-lite scenario, several solutions have been proposed in TR 23700-54[2]. Most of the solutions require that the UPF should expose its publid IP address to UE and establish direct IP connection with UE through NIN3A. This contribution proposes the key issue about the security risks caused by the new exposed IP communication endpoint.

# 4 Detailed proposal

Approve the following changes for inclusion in the TR 33.754.

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

### 5.X Key issue #X: UPF protection for exposing new IP communication endpoint

#### 5.X.1 Key issue details

Based on the current architecture assumption for ATSSS\_Lite in TR 23.700-54 [2], the use of N3IWF and TNGF is ruled out, and a direct IP connection is established between UE and UPF over the Internet. Most of the solution proposals (Solutions #2.2, #2.6, #2.7, and #2.8) require that public UPF address of the IP connection endpoint should be exposed, which increases the extent of exposure for 5G core networks. Further, the UPF must accept traffic from the internet destined to this UPF IP address.

Though UPF connecting to DN by N6 interface, the public UPF address is not directly exposed to the DN in any case, e.g. either in standard or in realy deployment. Because no use case or procedures have been specified to configure the UPF by DN directly, which means there is no dedicated configureation data to the UPF from a DN, then the UPF is just a kind of router from UE and DN point of view for exchanging the user plan data and the UPF never needs to accept any traffic from the DN destined to the UPF itself. Meanwhile, the N3IWF and TNGF is used as gateway for traditional non-3GPP access to prevent the UPF from connecting to the UE directly. Thus, exposing UPF IP address in the ATSSS\_Lite and requiring the UPF to accept traffic from the internet is a new threat to 5GS.

#### 5.X.2 Threats

Any malicious device no matter it is a malicious UE or anon-3GPP device may send messages to a specific UPF by using the public IP address of the UPF and leads to attacks like DDoS.

Since the packets sent to UPF can be from any point, and an attacker can construct packets with any source and destination addresses. Considering the source IP address of the UE assigned by 5GC may be in a certain rang, and by knowing the IP address of the UPF further decreases the difficulty to constust the fault messages. Thus, protection measures such as doing source and/or destination IP addresses check may not be enough to identify the attack, and the 5GC may face more challenge.

Since the UPF must accept traffic from the internet, an attacker may be able to reach internal network elements (e.g., a network function) by tunnelling packets through the UPF.

#### 5.X.3 Potential security requirements

TBD

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