**3GPP TSG-SA3 Meeting #124 draft\_S3-253431-r1**

**Wuhan, China, 13 – 17 October 2025**

**Source: ChinaTelecom**

**Title: New solution on security protection for N4 interface for local access services**

**Document for: Approval**

**Agenda item: 6.1.3**

**Spec: TR 33.746**

**Version: v0.0.0**

**Work Item: FS\_NR\_Femto\_Sec\_Ph2**

**Comments**

Add a new solution on security protection for N4 interface for local access services.

\* \* \* First Change \* \* \* \*

## 6.Y Solution #Y: Enhance SeGW to support security protection for N4 interface

### 6.Y.1 Introduction

This solution addresses key issue #2. Considering the locally deployed UPF is located outside the operator’s security domain and interact with core network through N4 interface, which leads to the exposure threats to the core network, this solution propose to enhance the Security Gateway as defined in TS 33.545 [3] to prevent core network against the attacks through N4 interface. Locally deployed UPF shall securely communicate with SMF via SeGW in front of 5GC over N4 interface. All N4 related input/output traffic over the trust boundary should be delegated and protected by Security Gateway.

### Y.2 Solution details

### 6.Y.2.1 Security architecture

The security aspect enhancements to system architecture of clause 4.1 in TS 33.545 [3] for security protection for N4 interface are further depicted in Figure 6.Y.2.1-1.

UE

NR Femto

SeGW

Insecure link

Operator’s security domain(s)

NR Femto GW

NR Femto MS

NR Femto MS

SMF / AUSF / UPF / UDM

UPF

Figure 6.Y.2.1-1: Enhancement for security architecture of NR Femto

Security protections provided by the Security Gateway for the traffic through N4 interface between locally deployed UPF and SMF deployed in core network over the trust boundary can be categorized in the following way:

- Topology information hiding of the core network;

- Signalling message filtration;

- Security protection between the locally deployed UPF and the Security Gateway;

- Access control etc.

NOTE: It is assume that NR Femto GW is integrated with SeGW in this solution. Whether the above N4 security protection function is provide by NR Femto GW or SeGW is left to implementation.

### 6.Y.2.2 Topology hiding

The core network topology shall not be directly exposed to the locally deployed UPF through N4 interface.

The SeGW shall hide the 5GC topology so that the core network entity address information (such as IP addresses of SMF etc.) are not inadvertently exposed to the locally deployed UPF.

### 6.Y.2.3 Signalling message filtration

The Security Gateway shall supports to discard malformed signalling messages sent from the locally deployed UPF through N4 interface over the trust boundary according to 3GPP specifications.

The Security Gateway shall supports to block messages with wrong NF types sent from the locally deployed UPF through N4 interface over the trust boundary according to 3GPP specifications.

The Security Gateway supports the rate-limiting functionalities to defend itself and core network NFs against excessive or overload signalling messages of N4 interface.

### 6.Y.2.4 Security protection

Security requirements and functions as defined in clause 4.2.1.7 of TS 33.545 [3] can provide the mutual authentication and transport protection between the locally deployed UPF and the Security Gateway.

### 6.Y.2.5 Access control

The Security Gateway shall supports the access control mechanism for the locally deployed UPF accessing the SMF deployed in core network, e.g. configure the access control list.

### 6.Y.3 Evaluation

Editor’s Note: Evaluation of this solution is FFS.

\* \* \* End of Changes \* \* \* \*