**3GPP TSG-SA3 Meeting #124 draft\_S3-253432-r1**

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

**Source: ChinaTelecom**

**Title: New sol on security detection of misconfigured femto devices**

**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 sol on security detection of misconfigured Femto node.

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

## 6.Y Solution #Y: Security detection of misconfigured 5G NR Femto node

### 6.Y.1 Introduction

This solution address the KI #1: Detection of misconfigured/compromised 5G NR Femto node.

It is propose to enhance the 5G NR Femto node to support to report itself configuration information for security detection and monitoring to the security management function which is a part of the 5G NR Femto MS.

It is propose to enhance the 5G NR Femto MS to support the security management function which can receive the configuration information from the 5G NR Femto node and perform the security detection and monitoring based on operator’s policy.

### Y.2 Solution details

The security procedure for security detection of 5G NR Femto node are further depicted in Figure 6.Y.2.1-1.



Figure 6.Y.2.1-1: Security procedure for security detection of 5G NR Femto node

0a. The 5G NR Femto node and Security gateway has established a secure connection of management plane with the Security Management function respectively.

NOTE x: The Security Management function is apart of the 5G NR Femto node MS.

0b. The 5G NR Femto node has established IPSec tunnels with the Security gateway.

1. The Security Management function configures the 5G NR Femto node for security data collection for detection of the misconfigured 5G NR Femto node according to the operator’s policy.
2. The 5G NR Femto node collect and report itself configuration information for security detection and monitoring to the Security Management function. The transmission of configuration information are protected by the security connection of management plane.

NOTE y: The collected typical configuration information can be running processes, secure password configurations, open ports and services, user permissions, and so on.

1. The Security Management function perform the security detection and monitoring based on the configuration information collected from the 5G NR Femto node.

NOTE z: Detail methods of security detection are not specified in this document. Operators can assess the security risks of current Femto node by checking their configuration status, and then implement corresponding security hardening to prevent the potential attacks on Femto node.

### 6.Y.3 Evaluation

Editor’s Note: Evaluation is FFS.

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