**3GPP TSG-SA3 Meeting #123 *draft\_S3-252692-r1***

**Goteborg, Sweden, 25 – 29 August 2025 merger of S3-252692, S3-252618**

**Source: ChinaTelecom, ZTE, Nokia**

**Title:** **New KI for NR\_Femto\_Sec\_Ph2**

**Document for: Approval**

**Agenda Item: 6.1.3**

# 1 Decision/action requested

***Approve the pCR to FS\_NR\_Femto\_sec\_ph2***

# 2 References

[1] 3GPP TS 33.xxx

# 3 Rationale

As described in S3-252419, it is required to study the security requirements and potential solutions to enhance the security of NR Femto devices, to detect misconfigured or compromised NR Femto devices, and to eliminate the security impacts from misconfigured or compromised NR Femto devices.

This contribution proposes new KI for NR\_Femto\_Sec\_Ph2.

# 4 Detailed proposal

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

## 5.X Key Issue #X: Detection of misconfigured/compromised 5G NR Femto devices

### 5.X.1 Key issue details

NR Femto devices are deployed outside operator domain and considered to be in un-trusted environments. Un-detected misconfigured or compromised NR Femto devices can lead to disruptions in services to UEs. A misconfigured or compromised NR Femto device with valid credentials and subscription to serve the victim UE can pose various threats including authentication replay attacks, broadcasting CAG IDs that it is not authorized to serve, denial of service attacks, etc.. Besides, misconfigured or compromised NR Femto devices may report false security baseline information to the SeGW and pose potential security threats to the NR Femto MS and the core network.

Potential security enhancements to NR Femto security architecture to detect such misconfigured or compromised NR Femto devices are needed to ensure that UEs, the NR Femto MS and the core network do not become victims of such devices.

### X.2 Security threats

A misconfigured or compromised NR Femto device with valid credentials and subscription to serve the victim UE can pose various threats including authentication replay attacks, broadcasting CAG IDs that it is not authorized to serve, denial of service attacks, etc.to the connected UEs.

A misconfigured or compromised NR Femto device with valid credentials and subscription to connect to the SeGW can pose various threats including abnormal traffics, abnormal signalling messages, denial of service attacks to the NR Femto MS and the core network.

### 5.X.3 Potential security requirements

The 5G system shall be able to detect misconfigured or compromised femto devices and eliminate associated risks, e.g. preventing the abnormal traffics/signalling threats..

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