**3GPP TSG-SA3 Meeting #124 merges 3463, 3330 and 3627 in draft S3-253821-r1**

**Wuhan, CN, 13 - 17 Oct 2025**

**Source: Huawei, HiSilicon, Samsung, China Telecom**

**Title: New KI on Security Protection of Compromised WAB Nodes and Core Network Measures.**

**Document for: Approval**

**Agenda item: 5.2.14**

**Spec: TR 33.724**

**Work Item: FS\_5G\_WAB\_SEC**

**Comments**

This contribution proposes a new key issue on the integrity, authenticity, and confidentiality of messages delivered from WAB components during their interaction with the 5G core and RAN, as their deployment a mobile environment may expose the network to rogue signalling, topology manipulation, and persistent infiltration, requiring dedicated mitigation mechanisms.

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

# 2 References

[x1] 3GPP TR 33.745: “Study on security aspects of 5G Next Radio (NR) Femto”.

[x2] 3GPP TS 33.320: “Security of Home Node B (HNB) / Home evolved Node B (HeNB)”.

## \* \* \* Second Change \* \* \* \*Y.X Key Issue #X: Security Protection of Compromised WAB Nodes and Core Network Measures

### Y.X.1 Key issue details

Wireless Access Backhaul (WAB) nodes, consist of a WAB-gNB (gNB-like functionality) and a WAB-MT (UE-like functionality). These nodes operate in non-trusted environments and may serve as moving backhaul nodes for the 5GS, establishing NG, Xn, and OAM interfaces over PDU sessions through 3GPP backhauls. While 3GPP TR 33.745 [x1] studied NR Femto security and reused procedures from TS 33.320 [x2], security concerns specific to WAB nodes particularly compromised WAB nodes in untrusted environments remain unaddressed.

Additionally, core network components may not be equipped to detect anomalous behavior from compromised WAB-gNBs, due to the decentralized and mobile nature of such nodes. The compromised WAB nodes could lead to topology poisoning, signalling storms, or user-plane hijacking.

This key issue aims to address the security issues introduced by compromised WAB nodes, where failure to protect the integrity, authenticity, and confidentiality of messages delivered from WAB-gNB and WAB-MT components can expose the 5GS to topology spoofing, rogue signalling, and persistent infiltration.

### Y.X.2 Security threats

Potential security threat:

* Rogue WAB-gNB Injection: A compromised WAB node may inject unauthorized signalling or reroute traffic maliciously, particularly via spoofed message. Furthermore, a compromised WAB-gNB can attempt to broadcast unauthorized network identifiers or initiate rogue Xn association attempts with neighbouring gNBs causing service disruption.
* Topology Manipulation and Signalling Abuse: Moving WAB nodes may falsely report neighbour relationships via Xn or behave inconsistently across locations, leading to incorrect handover decisions, topology poisoning, or signalling loops.
* Persistent Threat via Dual Roles: Since WAB-MT behaves like a UE and WAB-gNB like a gNB, a compromised WAB can act in both roles to stage cross-layer attacks, bridging between RAN and CN trust domains.

### Y.X.3 Potential security requirements

The 3GPP system shall support security mechanisms to mitigate risks from compromised WAB nodes, preventing topology spoofing, rogue signalling, and mobility-related traceability threats.

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