**3GPP TSG-SA3 Meeting #119AdHoc-e S3-250084-r2**

**Online, Electronic meeting, 13 -16 January 2025**

**Source: China Mobile**

**Title: Pseudo-CR on System architecture and security assumptions for Ambient IoT services**

**Document for: Approval**

**Agenda item: 5.9**

**Spec: 3GPP TR 33.713**

**Version: 0.5.0**

**Work Item: FS\_Ambient\_IoT\_Sec**

**Comments**

To address the Editor’s note in solution#36: *Whether this solution can be converted to a security architecture clause is FFS.* This contribution proposes the System architecture and security assumption for Ambient IoT services.

**Proposed Changes**

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

# 4 Security Architecture and Assumptions

Editor’s Note: This clause contains security architecture and assumptions to be considered for the study (e.g., per work task/KI).

The following system architecture and security assumptions are applicable to this study:

- If the existing authentication framework (e.g., 5G-AKA, EAP-AKA’, other EAP methods for SNPN) is not reused, a dedicated network for ambient IoT service shall be needed, and security isolation mechanism between the AIoT service domain and operator domain shall be needed (e.g. a security gateway may be deployed) to isolate the operator's legacy domain,..

NOTE: If multiple domains exist in the deployment of the architecture in figure x, the above policy applies.



Figure x System architecture and security assumption

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