**3GPP TSG-SA3 Meeting #124 draft\_S3-253704-r8**

**Wuhan, China, 13 – 17 October 2025** merger of S3-253290, S3-253392, S3-253299

**Source: Interdigital, CATT, Huawei (?), OPPO (?)**

**Title: New Key Issue on Security, and Authorization for Exposure of UE Data towards OTT Servers**

**Document for: Approval**

**Agenda item: 5.2.6**

**Spec: 3GPP TR 33.785**

**Version: 0.0.0**

**Work Item: FS\_AIML\_CN\_Ph2\_SEC**

**Comments**

This contribution proposes a new key issue on exposure security, authorization, for UE data towards OTT servers, and focuses strictly on the exposure interface between the core network and OTT.

\* \* \* First Change (all text new) \* \* \* \*

## 5.X Key Issue #X: Security, and Authorization for Exposure of UE Data towards OTT Servers

### 5.X.1 Key issue details

As studied in TR 23.700-04 [2], training data for AI/ML-based NR air interface operation with UE-side model training may be transferred via the 5G Core (5GC) and then exposed to external OTT servers. The exposure of such UE-related data outside the 3GPP domain introduces security and that need to be addressed at the exposure interface (e.g., via NEF

The exposure interface requires mechanisms to:

 - Authenticate OTT servers before any data exposure.

 - Authorize and apply service-specific access control to restrict exposed data to what is necessary for the OTT server.

 - Provide confidentiality, integrity, and replay protection of the exposed data during transport.

 - Ensure that exposure of UE-related data complies with user consent

### 5.X.2 Security threats

Unauthenticated or impersonating OTT servers could obtain sensitive UE-related data.

Without authorization, OTT servers can abuse UE-related data exposure services. .

Leakage, tampering, or replay of UE-related data in transit across the exposure interface could compromise integrity, confidentiality.

Exposure of UE information without proper consent may violate regulations and create liabilities for the MNO.

### 5.X.3 Potential security requirements

The 5GS shall support mutual authentication between the 5GC exposure function(s) (e.g., NEF) and OTT servers handling UE-related data.

The 5GS shall support authorization mechanisms for services related to exposure of UE-related data to the OTT server.

The 5GS shall support confidentiality, integrity, and replay protection for UE-related data during transfer to the OTT via NEF.