**3GPP TSG-SA3 Meeting #124 draft\_S3-253704-r1**

**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, Privacy, 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, and privacy 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, Privacy, 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 privacy risks that need to be addressed at the exposure interface (e.g., via NEF or other relevant exposure mechanism).

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.

 - Protect confidentiality, integrity, and freshness (replay protection) of the exposed data during transport.

 - Ensure that exposure of UE-related data complies with user consent and applicable privacy requirements.

### 5.X.2 Security threats

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

Inadequate authorization or coarse-grained access control could overexpose UE-related data to authenticated OTT servers (e.g., beyond relevant vendor or purpose).

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

Exposure of privacy-sensitive or personally identifiable 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 exposure of UE-related data to the OTT server.

The 5GS should enable granular level access control to be able to restrict and control the flow of UE related data towards OTT server.

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

The 5GS shall provide means to mitigate privacy risks associated with the exposure of UE-related data.

Editor’s note: whether and what UE data collection parameters can be privacy sensitive is FFS, based on RAN2 progress on collected data parameters definitions.