**3GPP TSG-SA3 Meeting #124 draft\_S3-253707-r1**

**Wuhan, China, 13 – 17 October 2025** revision of S3-253291

**Source: Interdigital**

**Title: New Solution: Security for Operator-Controlled UE Data Collection and Exposure**

**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 solution based on architectural baseline of TR 23.700-04 Solution #19. The solution covers authentication, authorization, transport security, privacy protection, user consent enforcement, replay/freshness protection, and secure exposure via NEF or equivalent.

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

## 6.X Solution #X: Security for Operator-Controlled UE Data Collection and Exposure

### 6.X.1 Introduction

This solution addresses Key Issue #1 and Key Issue #X.

This solution builds on TR 23.700-04 Solution #19 (standardized transfer of standardized data over UP for UE-side data collection) and introduces security enhancements in the 5GS for: (i) secure UE connection setup and data transfer with a Data Collection Function (DCF), and (ii) secure, authorized, and privacy-preserving exposure of UE-related data towards OTT servers via the 5GC exposure function (e.g., NEF).

### 6.X.2 Solution details

**Architecture scope and roles**

- DCF in the MNO domain manages Data Collection Profiles (DCPs) and orchestrates UE data collection and transfer, consistent with Solution #19.

- The exposure interface uses the NEF (or equivalent 5GC exposure function) to expose authorized subsets of collected data with any applicable post-processing prior to forward to OTT servers.

### **Security functions**

### 1) Mutual authentication and session protection (UE↔DCF)

 - The UE establishes an application-layer secure association with the DCF using shared key derived from network credentials. Transport security (e.g., TLS/QUIC) is bound to the shared key. Options for shared key derivation are:

- Option #1: AKMA-based keys (TS 33.535 [x]). DCF acts as an AF, and obtains KAF from the AAnF over SBI.

- Option #2: KSEAF or KAMF derived shared key. DCF obtains the shared key from AMF/SEAF over SBI.

Editor’s note: shared key derivation and service operations for exchange of shared key between AMF/SEAF and DCF (option #2) are FFS.

### 2) UE authorization and policy enforcement

### - The DCF authorizes a UE to participate per DCP using subscription, consent, and operator policy.

### 3) Data minimization and privacy protection

###  - Before exposure outside the MNO domain, the DCF applies per parameter pseudonymization, masking, or filtering per DCP visibility configuration.

###  - Identifiers not authorized for external exposure can be replaced by DCF with pseudonymous identifiers.

###  - DCF checks whether UE location information can be exposed externally based on existing LCS privacy profile, as per TS 23.273 [y].

Editor’s note: whether and what data can be subject to data minimization is FFS based on RAN2 progress on data collection parameters definition.

### 4) Consent enforcement inside the Core Network

###  - The DCF acts as the consent enforcement point for data collection from the UE, i.e., checks consent from UDM/UDR for permissions, as per TS 33.501 [z], Annex V.

### 5) Exposure toward OTT servers (NEF-facing)

###  - NEF enforces mutual authentication with OTT server.

###  - Exposure is constrained to authorized datasets and based on consent.

Editor’s note: whether and how user consent exposure applies will be decided by SA3 based on SA6 progress.

NOTE: Above points 1, 2 and 4 address Key Issue #1, while points 3 and 5 address Key Issue #X.

### 6.X.3 Evaluation

Editor’s note: evaluation is FFS.