**3GPP TSG-SA3 Meeting #124 draft\_S3-253707-r3**

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

**Source: Interdigital**

**Title: New Solution: Security for UE Data Collection using a DCF**

**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 agreed key principles in TR 23.700-04 The solution covers authentication, authorization, transport security, replay protection,

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

## 6.X Solution #X: Security for Data Collection using a DCF

### 6.X.1 Introduction

This solution addresses Key Issue #1.

This solution builds on TR 23.700-04 (for the standardized transfer of standardized data over UP for UE-side data collection) and introduces security enhancements in the 5GS for secure UE connection setup and data transfer with a Data Collection Function (DCF),

### 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,

### **Security functions**

### 1) Authentication and session protection between UE and DCF

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

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

Editor’s Note: the role of DCF acting as AF is FFS needs alignment with SA2.

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

Editor’s note: How 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.

Editor’s Note: Whether and how DCP is applicable is FFS and depends on SA2.

### 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.

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

### 6.X.3 Evaluation

Editor’s note: evaluation is FFS.