**3GPP TSG-SA3 Meeting #123 S3-252990**

**Goteborg, Sweden, 25 - 29 August 2025**

**Source: Huawei, HiSilicon**

**Title: New Key Issue on authentication and authorization of UE connection setup with data collection NF with communication security**

**Document for: Approval**

**Agenda item: 6.1.7**

**Spec: 3GPP TS/TR <TS/TR number>**

**Version: <TS Version>**

**Work Item: Study on Security for Core Network Enhanced Support for Artificial Intelligence (AI) / Machine Learning (ML) Phase 2**

**Comments**

As per KI#1 in TR 23.700-04, which aims to investigate and develop architectural enhancements to support UE data collection to meet the requirements for AI/ML for NR air interface with UE-side model training. The work involves training ML models at the UE side, where the OTT server trains the ML model for the UEs. This process requires the transfer of training data from the UE to the 5G core and then to the OTT server

The motivation is to investigate means to authenticate and authorize the connection setup between UE and 5GC internal data collection NF before the actual transmission take place as highlighted in KI#1 of TR 23.700-04.

Additional objective is also to investigate means to achieve confidentiality and integrity protection for communication between UE and 5GC internal data collection NF as highlighted in KI#1 of TR 23.700-04.

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

## Y.X Key Issue#X: Security and Privacy of UE connection setup with Data Collection NF

### Y.X.1 Key issue details

The architecture requirement in clause 4.2 of TS 23.700-04 [xx] is that MNO has full controllability and visibility for standardized data. That means the training data between UE and the 5G core will be standardized and it is visible to 5G core and MNO will be data controller and privacy for UE data will to be considered.

The key issue aims to address the security issues, such as authentication and authorization for the UE during the connection setup with the data collection network function (Naming and role of data collection function is TBD and subject to progress of TR 23.700-04). This will ensure only legit and authorized UE are able to share its data towards the Data collection NF.

Another aspect is to address the security issues, ensuring integrity and confidentiality of the UE related data between UE towards the 5GC Data collection NF as studied in KI#1 of TR 23.700-04 to meet requirements for AI/ML for NR air interface operation with UE-side model training.

An additional aspect is to address the privacy issue for the 5GC Data collection NF to collect UE related data.

So, the focus is to identify the means to authenticate and authorize the connection setup between UE and NF before the data transmission take place and to study security and privacy of the communication between UE and data collection NF during data transmission.

### Y.X.2 Security threats

Lack of authentication and authorization may lead to unauthorized access to network services.

Lack of confidentiality, integrity protection in collecting UE related data can lead to disclosure and tampering of UE related information.

Tampering of UE related data in transit can also impact the quality of training data towards 5GC data collection NF and subsequently to external OTT servers.

Lack of user consent may lead compromise of UE privacy.

### Y.X.3 Potential security requirements

The 5GS should support mutual authentication and authorization between UE and data collection NF before data transmission takes place.

The 5GS should support confidentiality, integrity and replay protection for data in transit between UE and data collection NF.

The 5GS should support user consent mechanism for data collection by the network depending on the local regulations and operator policies.

NOTE: solution selection depends on progress by SA2.

\* \* \* End of Change \* \* \* \*