SA WG2 Meeting #S2-170 S2-2507500

25 - 29 August, 2025, Goteborg, Sweden

**Source: Samsung, SK Telecom**

**Title: KI#2 Interim Agreements**

**Document for: Approval**

**Agenda Item: 20.3.1**

**Work Item / Release: FS\_AIML\_CN\_Ph2 /Rel-20**

*Abstract of the contribution: This contribution proposes the interim agreements for AIML\_CN KI#2.*

# Discussion

In TR 23.700-04 V0.2.0 (2025-05), there are ten solutions documented for KI#2. This contribution provides comprehensive analysis on all documented solutions on KI#2 and proposes the potential interim agreements for SI conclusions and normative work.

**Solution#22** proposes to configure the UPF to report information to NWDAF as the input data of analytics. The UPF reporting data includes the detected packets complying with certain pattern, (Abnormal) amounts of traffic received from external source and Rate of dropped packets. The analytics consumers, e.g. PCF, SMF, OAM, or AF, may use the analytics output to optimise PCC rules or QoS, to configure UPFs to block abnormal traffic, to correct abnormal traffic, etc.

**Solution#23** proposes to collect various NWDAF input data from multiple data sources, including the locally observed abnormal UP pattern related information from UPF, the Traffic pattern Information from AF, etc. Based on the traffic characteristics collected from different sources, the NWDAF derives the Analytics on UP Traffic Pattern to provide the risk level and traffic pattern information of the targeting UPF(s). The consumers, e.g. SMF or PCF, could use the output analytics for UPF management or policy determination or update.

**Solution#24** proposes collocate UPF and NWDAF containing AnLF to reduce the CP load for ML inference, and the UPF can directly use the output analytics generated by the AnLF for further actions. In this solution, the NWDAF containing MTLF provides the trained ML model for User Plane Traffic Exception analytics to the NWDAF containing AnLF that is collocating with the corresponding UPF. MTLF collects data from UPF for ML model training, including UPF local data, N3 measurements, N6 measurements. The data collection is expected during off-peak hours.

**Solution#25** proposes to collect QoS monitoring data from UPF as NWDAF analytics input data to derive the output analytics on user plane traffic pattern. The output analytics will help PCF with QoS and PCC rules optimisation for the target application.

**Solution#26** proposes to enhance the UPF to perform local data processing and reports the locally pre-processed data to the NWDAF based on the received instructions; and therefore, to reduce the UPF reporting load. The local data pre-processing instructions may depends on the Analytics ID and corresponding performance metrics. In detail, to trade-off the UPF pre-processing load and reporting load, the NWDAF instruction may include the certain volume of data to be reported by UPF, data sampling related information, reporting of statistical data based on feature extraction.

**Solution#27** proposes to collect various NWDAF input data from multiple data sources, including N3, N6 and N9 related data from UPF or OAM, Traffic characteristics and (Abnormal) data packet related information from UPF or AF, etc. Based on the input data, the NWDAF could derive the analytics on UP management analytics for the targeting UPF(s), including the UP performance, cause of performance degradation, and associated traffic characteristics. The consumers, e.g. PCF or SMF, will use the output analytics to optimise policy configuration and optimise UP management rules.

**Solution#28** proposes to enhance UPF to derive analytics by performing ML inference; and therefore, the UPF can directly consume the outputs to block the UP traffic towards malicious and/or forbidden sites. The UPF can retrieve the corresponding trained ML Model from NWDAF (MTLF). The training data include AF data (e.g. a Content filtering DB) and UPF data (e.g. UP traffic parameters).

**Solution#29** proposes collect various traffic indicators from the UPF, SMF and OAM based on flow-level metrics packet rate, protocol information, etc. Based on the input data, the NWDAF generates per-UPF analytics results for multiple UEs and application flows, including flow stability indicators, protocol-level info, abnormal packet indicators, etc. The consumers, e.g. PCF or SMF, will use the output analytics to optimise policy configuration and optimise UP management rules.

**Solution#30** proposes to consider UPF as the consumer of analytics on traffic pattern and anomaly information; and therefore, by consuming the output analytics, the UPF is able to perform user plane traffic handling optimization and trigger SM Policy Association Modification towards SMF by sending N4 report.

**Solution#31** proposes to consider UPF and SMF as the consumer of analytics. The consumer UPF could detect malicious IP packets, allocate more resource before the bursts, adjust interface thresholds, based on the Analytics output. The consumer SMF could select/reselect suitable UPF for new PDU sessions, adjust N4 rules based on the Analytics. In this solution, various NWDAF input data is collected from multiple data sources (e.g. UPF, OAM, SMF) on UP operation information, UPF status, N4 session info, etc. The output includes UPF performance information, traffic characteristics, reason for the anomaly, etc.

# Proposal

It is proposed to adopt the following changes into TR 23.700-04.

**\*\*\* Start of the change \*\*\***

# 7 Interim agreements

## 7.1 Agreed Principles

### 7.1.X Agreed Principles for KI#2

Editor's note: This clause will include the principles that are agreed as work progresses for the specific KI#Y. This may be populated directly or e.g. also when a topic in clause 7.2.Y gets resolved and a principle is agreed.

Use case #1 and #2 in clause 5.1 will be supported in the normative work to support efficient user plane management and performance optimization.

The following principles may be considered for the normative work:

- No impact on RAN and UE operation.

- New analytics ID(s) to support user plane traffic pattern and behaviour analysis will be defined and supported by NWDAF.

- The service consumer the analytics service may be SMF, PCF, and OAM.

- To provide analytics to the consumers for UP performance and corresponding policy optimisation, based on consumer’s request, the NWDAF may provide the following **output analytics**, e.g.:

- (abnormal) traffic pattern information of traffic flow, e.g.

- IP packet filter(s) and/or IP Protocol (TCP, UDP, etc.),

- (max./ min/ average of) data rate, drop/error rate, data burst, data volume, etc.

- the associated application info, affected UPF(s) and/or UE(s).

 .

- if abnormal traffic pattern information is provided by NWDAF, evaluation or status of UP performance, the reason for UP anomaly, , e.g., DDoS, misbehaved (IoT) devices, malicious and/or forbidden sites, etc.

- To derive the output analytics, the following **input data** may be collected from NFs to support the NWDAF-based analytics:

data related to UPF performance- (abnormal) data traffic pattern information related information collected different from different data sources (e.g. UPF, SMF, AF, etc.).

- Information identifying the associated application, UPF and/or UE of the collected traffic pattern information.

* Consumer action: For example, by taking the output Analytics into account,
	+ The SMF may (re-)select UPF to distribute load, (re-)configure UPF for preventing anomalies, e.g. based on abnormal traffic pattern information.
	+ The PCF may update policy or QoS.
* To reduce the reporting load of input data sources (e.g. UPF),
	+ The analytics consumer may include the Analytics Filter Information for input data filtering. e.g. application info, IP Packet Filter Set or IP protocol type. Based on configuration and/or threshold provided by NWDAF, UPF may pre-process data locally and only report (abnormal) traffic pattern information that meets NWDAF requirements.

## 7.2 Topics for further consideration

### 7.2.X Topics for further consideration for KI#2

Editor's note: This clause will include the topics for further consideration as work progresses for the specific KI#Z. Eventually this clause should only contain topics for further consideration that did not result in agreements (i.e. in agreed principle(s) in a clause 7.1.Z) and can either be then marked as not pursued or postponed to a future release.

The following topics are for further consideration for KI#2:

* Whether the UPF can be the consumer of the user plane traffic pattern and behaviour analysis or not.
* Whether new UPF or SMF events are needed or not for NWDAF data collection.
* Whether the UPF will have AI capability or not, e.g. by collocating with AnLF.
* How to reduce the reporting load of input data sources? For example by configuring appropriate Analytics Filter Information, combining notification to NWDAF at UPF for multiple events, etc.
* Details of **NWDAF input data** are FFS. Examples of potential NWDAF input data may include:
	+ data related to UPF performance, e.g. N3/N6/N9 performance data, user plane latency, UPF load and capacity.
	+ data related to the service flow, e.g. application info, transport protocol information, IP Packet Filter Set or PDR, (abnormal) data information, traffic characteristics (including data burst size, traffic volume, packet delay, data loss/drop rate).
	+ Whether and what data packet level information will be considered as NWDAF input data is FFS.
* Details of NWDAF output data are FFS. Examples of potential **NWDAF output analytics** may include:
	+ traffic pattern information.
	+ the reason for UP anomaly , e.g., DDoS, misbehaved (IoT) devices, malicious and/or forbidden sites, etc.
* Examples of potential reasons for UP anomaly may inlcude:
	+ DDoS, misbehaved (IoT) devices, malicious and/or forbidden sites, unexpected traffic pattern (e.g. high data volume, high/ low rate, abnormal traffic bursts), unnecessary UE wake-up, too many malformed/ duplicate/ retransmitted/ fragmented packets, etc.

**\*\*\* End of the change \*\*\***