**SA WG2 Meeting #S2-162 S2-240xxxx**

**15th -19th April 2024, Changsha, China (rev of S2-2404462)**

**Title: TR 23.700-63, Solution #1 update**

**Source: Vodafone, Nokia, Samsung**

**Document for: Approval**

**Agenda Item:**

*Abstract: This pCR proposes an update of solution 1 for KI#3*

# 1 Background

Solution#1 in TR 23.700-63 describes the information that is expected to be included by an AF at the time of requesting insertion/detection of specific headers/tags at the user plane.

The actual header(s)/tag(s) were unclearly described in the solution and could be interpreted as being part of the metadata proposed and/or referenced by the identifier, what may lead to complexity at the time of stage 3 implementation.This pCR proposes the actual header(s)/tag(s) as part of the list of parameters included by the AF, in a conditional way, to consider use cases in which the AF and app provider dynamically agree e.g. detection of a particular header/tag to be followed by a notification.

Additionally, the example related to PCF extracting protocol information from the metadata is removed, to avoid adding complexity to the solution.

The revised pCR incorporates the proposals from S2-2404122 and S2-2404940, as well as some paragraphs and notes from S2-2404499 to complement the direct reporting option and an alternative to some parameters in Header handling rule.

It also formats the subclauses for notifying, since two proposed ways of reporting are captured. The highlighted text is the formatting proposal

# 2 Proposal

It is proposed to agree the text below for inclusion into TR 23.700-63.

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

## 6.1 Solution #1: Provisioning of information for header handling

### 6.1.1 Description

Network operators can reach agreements with Application Service Providers to handle traffic specific to their applications in a particular way and/or under specific conditions, in terms of SLAs between both business parties.

Automation capabilities of 5G for network slicing, charging, interactions with AFs, use of analytics, etc permit MNOs to engage in agreements with Application service providers in a dynamic way compared to previous technologies and to provide relevant configurations for devices and network nodes using rules and policies to support such agreements.

One way of implementing agreements with an ASP is by exchanging in-band information included in the relevant protocols. Client, server or proxies in the traffic path can insert specific information or use specific protocols that imply a particular behaviour for the receiving entity. An example of insertion of information in Release 18 is the use of ECN for L4S to permit rate adaptation for a particular flow.

Release 18 specifications have also included functionality for Service Function Chaining capabilities so that an Application Function can request a particular steering of user plan traffic towards specific service functions in the N6-LAN. Additionally, in earlier releases, the enrichment of packet headers was possible in the uplink direction by including specifically the IMEI as part of the header. This capability has evolved in 5G to be more generic and make use of containers in FAR rules, however, it is still not available for request from the AF/operator platform and no functionality exists for notification upon detection of headers.

Recently, different standards organizations are engaged in developing protocols and market is developing mechanisms that permit the network to recognise the content so specific handling can be provided, while keeping the content encrypted.

The solution leverages existing functionality to address mechanisms that facilitate SLAs, in an environment where the variety of mechanisms and protocols keep on growing, using in-band information specific to the particular agreement:

- Header/tag(s) handling request in N6 or in N3 and reporting.

The existing functionality for AF traffic influencing, together with use of PFDs as needed, is used as baseline for the solution proposed. For the discovery of UPF(s) enhanced to handle header/tags insertion/detection, the following UPF capability is added in UPF profile stored in NRF:

- Header handling.

Different use cases may require procedures at different levels. The HTTP traffic is being reduced while encrypted protocols grow, so any potential insertion or detection would need to be at different layers, mainly transport and IP. To make the mechanism generic for different cases, it is proposed to use a rule referred to by an AF.

**\* \* \* \* Next Change \* \* \* \***

### 6.1.2 Procedures

#### 6.1.2.1 Insertion, detection and reporting request

The proposed rule provided by the AF can include:

- Identifier of the rule.

- (optional) One or more Header/tag name(s) and value(s)

The header/tag contains information to be detected, replaced or removed. It is conditionally included by the AF upon agreement with the application provider.

The Header/Tag name describes the content of the header/tag value.

Header/Tag value contains the actual value to be detected/added/removed. In case of replace, two header tag values need to be provided. The header tag value is not specified according to any specific protocol layer or protocol. The 5G CP handles the values as metadata and provides them to UPF. The specific protocol where this header is inserted/detected/replaced is part of SLA and left for UPF implementation. UPF is configured, based on SLA, to use these values to compose the *Header names*/*values* according to the specific protocol.

NOTE: Headers/Tags values can be conditionally included by the AF (according to the use case). When value is not included, the "Reference to Information relevant to parties in SLA" points to a preconfigured Header/Tag value

- (optional) Conditions for header/tag handling e.g. always, at initiation, during certain period.

The conditions are agnostic of the specific protocol for header handling.

- (optional) Actions: Add , Remove, Replace, Detect one or more header/tag(s).

Editor’s Note: Whether the header handling (e.g. detection) requested by the AF can trigger any actions performed by SMF is FFS.

- Reference to Information relevant to parties in SLA

The "Reference to Information relevant to parties in SLA" includes a reference to a configuration in UPF which is based on the SLA. It is forwarded transparently to the UPF. It is used by UPF to map to pre-configured information related to header/tag handling (e.g. protocol layer, type of encryption, etc). This preconfigured information may also refer to Actions and Conditions, e.g. in case these parameters are not provided by the AF.

- (optional) 5GS parameter name list

This list is included if PCF/SMF need to provide information to UPF that UPF is not going to receive otherwise, and/or if NEF should authorize using 5GS information upon request by that AF.

- Information related to reporting of header handling actions:

- Reporting conditions: Threshold based, periodical with the relevant threshold values and periodicity. or indication that direct reporting to AF is not required

- Information related to direct reporting to AF:

o Option 1: Report Correlation ID and UPF event consumer notification URI values. The AF provides receive Session Reports directly from the UPF Exposure Service (see Section 6.1.2.3).

o Option 2. the AF provides Notification Target Address (+ Notification Correlation ID) attributes to request to receive Session Reports, and direct indication to request that they sent directly with UPF Exposure Service.

These two options are further described in the solution description below

The information in the above-described rule will be provided to the UPF.

The content of the report from UPF depeneds on the on the Action for the header handling. The report from UPF includes:

- Action taken (i.e. the UPF reports the action taken, e.g. detected, removed, replaced, insert)

- Detected header (in case action is remove, replace or detect). The UPF reports the removed header if action is Remove, and the replaced header if action is Replace and the detected header if action is Detect.

- Final header (in case action is add or replace). The UPF reports the final header, i.e. the added header if action is Add, or the sent header if Replace.

Leveraging on the NF service Nnef\_TrafficInfluence, and following the description in clauses 5.6.7 and 5.6.16 of TS 23.501, an AF may request the SMF, via NEF and PCF, handling some header/tag to the protocol at the user plane for:

- a particular S-NSSAI/DNN; and

- a particular application; and/or

- UL/DL or both directions

- a particular UE/group of UEs or any UE.

The actual rule(s) is(are) provided in the relevant Nnef\_TrafficInfluence operation (create/update/delete) by the AF, together with the parameters above. The AF request may not always need to be linked to an ongoing PDU session. The request can be applied to the ongoing or future PDU session.

The following sequence is extracted from clause 4.3.6.2 of TS 23.502 [3] to apply for this solution:



Figure 6.1.2-1: Nnef\_TrafficInfluence operation (clause 4.3.6.2 of TS 23 502 [3])

In step 1, the AF inserts the rule contents, including the information that is relevant for the parties (as metadata). The request may target “any UE”.

In step 2, NEF confirms the AF is authorised to use this rule based on local configuration, and then will store/update the received data in the UDR for data set pointing to application data.

At notification from UDR, PCF receives and authorizes the rule and the PCF includes it in the PCC rule(s) with the information required for reporting the event, including indicating whether PCF also wishes to receive the notification..

In step#5, the PCF determines if existing PDU Sessions are potentially impacted by the AF request. For each of these PDU Sessions, the PCF updates the SMF with corresponding new policy information about the PDU Session.

For future PDU Sessions, PCF delivers policy information during SM policy establishment.

NOTE 1: Values need be provided by PCF or SMF for parameters that SMF or UPF, respectively, need and may not have otherwise. (the 5GS parameter name list in the header handling rule is used for this)

In step#6, n installs relevant N4 rules. Two potential options are described in this solution:

Option1:

The SMF installs PDR/FAR and URR including new Report Correlation ID (if reporting required) rules using N4 procedures into the UPF and if Report Correlation ID exists, then the SMF subscribes (on behalf of the AF) to the UPF Exposure Service’s Traffic Influence Reporting event (see Section 6.1.2.2.2) using this ID and UPF event consumer notification URI that was provided together with the ID.

Option 2:

The SMF installs in UPF PDRs with associated FARs including the Header handling Rule. The Header handling Rule provides UPF with instructions for what to report, reporting conditions and when Direct Reporting applies, contact information:

- When Direct reporting applies, the Notification Target Address (+ Notification Correlation ID) is included in FAR. When notification triggers are met, UPF sends Nupf\_EventExposure notification for a new Event. This new event is subscribed by SMF on behalf of AF using FAR.

- When N4 reporting is required, SMF associates a URR to the PDR, the report trigger being that FAR header handling notification conditions are met. The N4 report could be sent in addition to or instead of the Nupf Event Exposure notify.

This option is also further described in Section 6.1.2.2.2

**\* \* \* \* Next Change \* \* \* \***

#### 6.1.2.2 Header/tag reporting/notification

##### 6.1.2.2.1 General

When a detection action is requested by the AF, SMF and UPF are instructed to report information included by the client or server side under the SLA. The instruction for detecting a header may or may not be associated with an insertion/removal/modification/replacement.

The AF may decide whether the Nnef\_TrafficInfluence\_Notify service or Nupf\_EventExposure service (i.e. direct reporting) is to be expected for the reporting/notification of detected headers or in relation to actions, according to the settings the AF provides in the request as described in clause 6.1.2.1

When the notification/reporting is requested via Nnef\_TrafficInfluence\_Notify, the procedure in TS 23.502 clause 4.4.2.2 is applicable to this solution upon detection in the UPF of a PDR associated to a URR.



**Figure 6.1.2.2-1 N4 Session Report (TS** **23.502 [3] clause** **4.4.2.2)**

Alternatively, the AF can indicate its preference to use direct reporting based on UPF Exposure Service by

- Option 1, including both Report Correlation ID and UPF event consumer notification URI values in Traffic Influence header handling rule described in Section 6.1.2.1. In this case, the procedure is described in clause 6.1.2.2.2.

- Option 2, including Notification Target Address (+ Notification Correlation ID) attributes to request to receive Session Reports, and direct indication to request that they sent directly with UPF Exposure Service

If UPF detects a header tag requested by the AF or when notification (which may include the detection action) that is associated with an insertion/removal, modification or replacement,

- Option 1, if Report Correlation ID value was not defined, then the UPF again uses N4 Session report to notify the SMF with “Start of Traffic (usage report)” is proposed to be used as well by the UPF. The usage N4 session report shall include instead information about the header/tag detected and the action performed on it.

- Option 2, if URR reporting trigger is set to be that, during execution of the header handling Rule in the FAR (on same PDR), the conditions for notification are met. UPF uses N4 Session report to notify to the SMF. The N4 session report includes information of the action, detected header and sent header. This is further described in clause 6.1.2.2.2

##### 6.1.2.2.1 Header/tag reporting/notification leveraging Nnef\_TrafficInfluence\_Notify

The following simplified sequence, derived from clause 4.3.6.3 of TS 23.502 [3], is to apply for this solution upon notification from the UPF:



Figure 6.1.2.2.1-1: Notification of header detection to AF using Nnef\_TrafficInfluence service

Based on the configuration by AF, upon receiving N4 Session Report from SMF, SMF may use Nsmf\_EventExposure\_Notify operation to expose relevant information to the NEF/AF (e.g. Header detected). SMF may notify PCF if a reporting trigger is met.

After the step 2b, the actions the AF may execute are not depicted; those will depend on the agreement with the MNO.

After the Step 3a, the actions the PCF may execute are not depicted and may depend on the SLA between AF and MNO or operator policies.

NOTE: Reporting detection of a header for Any UE or for some popular applications can cause UPF to issue lots of reports and consequently high signaling load. Requesting reporting of a header/tag detection in UEs traffic needs to be considered with care. If high signaling load is concerned, then alternative solution using direct reporting from UPF to AF should be used, instead of N4 based reporting.

**\* \* \* \* Next Change \* \* \* \***

##### 6.1.2.2.2 Header/tag reporting/notification leveraging UPF Exposure Service

There are two possible options:

Option 1:

The AF can include Report Correlation ID and UPF event consumer notification URI values in the Traffic Influence rule in the request of new Nnef\_TrafficInfluence service and after that the same ID can be used in subscribing new Traffic Influence Reporting event of UPF Exposure Service to receive direct Session Reports from the UPF.

In the UPF, for each triggered report event (Step1 in Figure 6.1.2.2-1) with the URR without Report Correlation ID specified, the default actions, i.e., reporting over N4, apply. But if the Report Correlation ID is found, then the UPF checks whether the Report Correlation ID value has Traffic Influence Reporting event subscriptions and if so, then the direct reporting is used towards the AF instead. If no subscription is found, then the reporting is ignored for time being.

New Traffic Influence Reporting event for UPF Exposure Service is defined in Table 1. If the AF has indicated its preference to receive Session Reports directly from the UPF, then the SMF discovers the UPF Exposure Service details from the NRF and subscribes to the UPF on behalf of the AF (like described in Figure 4.15.4.5.2-1 “Subscription to UPF event exposure service for certain UE(s) via SMF” in TS 23.502) by sending a UPF event exposure subscribe request (HTTP request like defined in TS 29.564) where the existing URR is referred by the given Reporting Correlation ID. If no URRs with the given ID is found, then the subscription fails, and respective HTTP error status is returned as described by Step2b in Figure 5.2.2.2.2-1 “Subscription creation“ in TS 29.564. If URR(s) with the given ID is(are) found, then the subscription is created and the related URR(s) will result Session reports to be sent as direct notifications to the consumer AF as shown in Figure 5.2.2.3.2-1 “UPF sends notification on subscribed events” in TS 29.564.

Table 1: Traffic Influence Reporting event.

|  |  |
| --- | --- |
| **Description** | This event provides Traffic Influence reporting directly for the subscriber instead of using N4 signaling. |
| **Subscription type** | Subscription to UPF/Nupf\_EventExposure Subscribe |
| **Subscription inputs to UPF** | Required:  - UPF event consumer notification URI.  - Reporting Correlation ID. |
| **Report type** | Continuous (event triggered) Report. |

Option 2:

The AF that wants to receive direct notifications indicates so in the Nnef\_TrafficInfluence request and AF includes then Notification Target Address (+ Notification Correlation ID. PCF includes this information with the Header handling Rule in the corresponding PCC Rule ent to SMF.

PCF can include a new Policy Control Request Trigger to request SMF to send the notifications that it receives from UPF to PCF.

NOTE: triggers are not sent per PCC Rule, therefore, when trigger is activated, the PCF is requesting to receive all notification reports that SMF receives from UPF. But the notification reports are sent to AF either by SMF or UPF, according to AF request

SMF translates the PCC Rule into the corresponding PDR(s) and includes the header handling Rule in the PDR:

- If Direct notification has been requested in the PCC Rule, the Notification Target Address (+ Notification Correlation ID) are also included with the header handling Rule in the FAR associated to the PDR(s).

- If SMF determines that the UPF notification report should be sent to SMF, SMF sends an associated URR. URR includes a new reporting trigger event that indicates UPF to send the report when a notification si triggered at execution of the header handling Rule in the FAR associated to that same PDR.

SMF may send a URR to UPF because AF has not indicated direct reporting (notifications are to be sent to AF from SMF). But, even if UPF reports directly to AF, SMF may send URR if SMF should also receive the notification reports for other purposes (e.g. to satisfy the PCF request).

UPF sends the header handling report notification in a new UPF event exposure event which can only be subscribed by SMF on behalf of the consumer.

**\* \* \* \* Next Change \* \* \* \***

6.1.3 Impacts on services, entities and interfaces

- NEF

- Nnef\_TrafficInfluence service, adding optional header tag rule Id, container/metadata, direction (uplink/downlink) and handling new event in the Event ID reported to AF

- UDR

- Nudr\_DataManagement service, adding new data subset in the Application data set.

- PCF

- PCC rule to add a header tag identifier and metadata, and specify UPF/SMF behaviour on detection of a header or another action.

NRF:

- Storing new UPF capability in UPF profile.

- Discovery of several UPFs that accords with the new UPF capability of specific traffic detection and handling.

- SMF

- Discovery of several UPFs that accords with the new UPF capability of specific traffic detection and handling.

- Nsmf\_EventExposure service, to include new event for notification to the AF

- To depict PDR/FAR/URR rules handling for header/tag handling.

- N4 updates

- Support new Report Correlation ID field in URR rule.

- Support Traffic Influence Reporting event subscriptions of the UPF Exposure Service on behalf of the AF.

- UPF

- N4 updates: Header handling capability, for insertion/modification/removal/replacement and/or detection

- UPF Exposure Service supports new Traffic Influence Reporting event.

- Support new Report Correlation ID field in URR and Traffic Influence Report handling.

**\* \* \* \* End of Changes \* \* \* \***