|  |  |
| --- | --- |
| 3GPP TR 23.700-63 V0.3.0 (2024-04) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on UPF enhancement for Exposure and SBA Phase 2  (Release 19) | |
|  | |
|  |  |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions of terms and abbreviations 7

3.1 Terms 7

3.2 Abbreviations 8

4 Architectural Assumptions and Requirements 8

4.1 Architectural Assumptions 8

4.2 Architectural Requirements 8

5 Key Issues 8

5.1 Key Issue #1: Selection of UPF providing a selected user plane functionality 8

5.1.1 Description 8

5.2 Key Issue #2: Enhancements on UPF information exposure 9

5.2.1 Description 9

5.3 Key Issue #3: Study enhancements for UPF handling of headers 9

5.3.1 Description 9

6 Solutions 10

6.0 Mapping of Solutions to Key Issues 10

6.1 Solution #1: Provisioning of information for header handling 10

6.1.1 Description 10

6.1.2 Procedures 11

6.1.2.1 Insertion/detection request 11

6.1.2.2 Header/tag reporting/notification 14

6.1.2.2.1 Header/tag reporting/notification leveraging Nnef\_TrafficInfluence\_Notify 15

6.1.2.2.2 Header/tag reporting/notification leveraging UPF Exposure Service 15

6.1.3 Impacts on services, entities and interfaces 17

6.2 Solution #2: UPF provision and selection based on new UPF functionality 17

6.2.1 Key Issue mapping 17

6.2.2 Description 17

6.2.3 Procedures 18

6.2.4 Impacts on services, entities and interfaces 18

6.3 Solution #3: Selection on UPF with extended user plane capabilities 19

6.3.1 Description 19

6.3.1.1 Solution Description 19

6.3.2 Procedures 19

6.3.3 Impacts on existing nodes and functionality 22

6.4 Solution #4: Selection of UPF providing specific user plane functionalities 22

6.4.1 Key Issue mapping 22

6.4.2 Description 22

6.4.3 Procedures 24

6.4.4 Impacts on services, entities and interfaces 25

6.5 Solution #5: Direct subscription of UPF event exposure service for TSC management 25

6.5.1 Description 25

6.5.2 Procedures 25

6.5.2.1 Direct subscription of UPF Event Exposure service for TSC management 25

6.5.3 Impacts on services, entities and interfaces 26

6.6 Solution #6: UPF selection based on the status of the supported functionalities 26

6.6.1 Key Issue mapping 26

6.6.2 Description 27

6.6.3 Procedures 27

6.6.4 Impacts on services, entities and interfaces 28

6.7 Solution #7: Translating SUPI/GPSI to NATed IP address 28

6.7.1 Description 28

6. 7.1.1 Background and problem description 28

6.7.1.2 High level description 29

6.7.2 Procedures 29

6.7.2.1 Procedure 29

6.7.2.2 Service definition 30

6.7.2.2.1 Nupf\_GetPublicIPaddressAndPort 30

6.7.3 Impacts on services, entities and interfaces 30

6.8 Solution #8: UPF event exposure during UPF relocation 30

6.8.1 Key Issue mapping 30

6.8.2 Description 31

6.8.2 Procedures 31

6.8.3 Impacts to Services, Entities and Interfaces 32

6.9 Solution #9: DNAI Mapping information exposure 32

6.9.1 Description 32

6.9.2 Procedures 33

6.9.3 Impacts on services, entities and interfaces 33

6.10 Solution #10: Subscription to UPF Event Exposure Services in the event of UP Path change 34

6.10.1 Key Issue mapping 34

6.10.2 Description 34

6.10.3 Procedures 35

6.10.4 Impacts on services, entities and interfaces 36

6.11 Solution #11: Direct subscription of UPF event from NEF/trusted AF or NWDAF 36

6.11.1. Description 36

6.11.2 Procedures 37

6.11.2.1 Direct subscription of UPF Event Exposure service from NEF/trusted AF 37

6.11.2.2 Direct subscription of UPF Event Exposure service from NWDAF 38

6.11.3 Impacts on services, entities and interfaces 38

6.12 Solution #12: Direct subscription to UPF Event Exposure service via N6 39

6.12.1 Key Issue mapping 39

6.12.2 Description 39

6.12.2.1 General 39

6.12.2.2 Solution Description 39

6.12.3 Procedures 40

6.12.4 Impacts on services, entities and interfaces 44

6.13 Solution #13: UPF Discovery and Direct Subscription to UPF for AF 44

6.13.1 Description 44

6.13.2 Procedures 45

6.13.2.1 General call flow 45

6.13.2.2 UPF discovery by utilizing Header information and Subscription via CP 46

6.13.2.3 UPF Discovery and subscription by utilizing Header information 46

6.13.3 Impacts on services, entities and interfaces 48

7 Overall Evaluation 48

8 Conclusions 48

8.1 Interim Conclusions for Key Issue #1: Selection of UPF providing a selected user plane functionality 49

Annex <X> (informative): Change history 50

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The Technical Report continues the study on key issue description, solution and conclusion on UPF enhancement for Exposure and SBA Phase 2.

The scopes include the following aspects:

- Study potential enhancements on UPF selection to discover UPF with specific user plane functionalities, e.g. NAT, Packet inspection, etc;

- Study potential enhancements on UPF event exposure service to optimize the procedures related to UPF data collection, e.g. direct/indirect subscription of the UPF via control plane from application;

- Study potential enhancements to support the AF instruction via 5GC to UPF for packet inspection (e.g. UPF detection of certain IP header, HTTP header, etc.) for UL/DL traffic, as well as report collection of the indicated packet inspection from UPF.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System (5GS); Stage 2".

[3] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[4] 3GPP TS 23.503: "Policies and Charging control framework for the 5G System; Stage 2".

[5] 3GPP TS 29.510: "5G System; Network function repository services; Stage 3".

[6] 3GPP TS 29.244: "Interface between the Control Plane and the User Plane nodes".

[7] 3GPP TS 23.548: "5G System Enhancements for Edge Computing; Stage 2"

# 3 Definitions of terms and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

<ABBREVIATION> <Expansion>

# 4 Architectural Assumptions and Requirements

## 4.1 Architectural Assumptions

- The architecture and framework as specified in TS 23.501 [2], TS 23.502 [3], and TS 23.503 [4] are regarded as the baseline for this study.

- User plane architecture changes are outside of scope and user plane architecture as defined in TS 23.501 [2] will be taken as a basis.

- The functional split in 5GS between UPF and other functional entities remains unchanged.

- Selection of the UPF for the PDU Session remains an SMF functionality, not replicated in any other NF.

- Functionalities of other NFs, for example, the NEF functionality to authorize requests from the Application Functions are not replicated in UPF.

## 4.2 Architectural Requirements

The following architectural requirements are applicable to this study:

- Solutions shall build on the 5G System architectural principles as defined in TS 23.501 [2], including flexibility and modularity for newly introduced functionalities.

- UPF event exposure service registration/deregistration and discovery as defined in Release-18 will be taken as basis.

- Indirect subscription of UPF event exposure via SMF can use either PFCP message or SBI interface based on the event type.

- The performance of UPF user plane traffic handling shall not be degraded due to mechanisms defined in this study.

- No impact is introduced on N3, N9 interfaces for this study.

- The N4, N6 interfaces are based on the existing interface design and remain backward compatible.

- Any new mechanisms compared to the Rel. 18 UPEAS need to be justified.

- The co-existence for the UPF supporting new functionality included in this study and UPF supporting previous release should be considered.

# 5 Key Issues

## 5.1 Key Issue #1: Selection of UPF providing a selected user plane functionality

### 5.1.1 Description

Currently a UPF advertises the features it supports in the NF profile of UPF registered in NRF as specified in e.g. 3GPP TS 29.510 [5] clause 6.1.6.2.13 and/or over PFCP as defined in 3GPP TS 29.244 [6]. An SMF leverages the exposed UPF information for proper UPF discovery and selection. A UPF implementation may support more optional functionalities like NAT, Packet Inspection, etc which are not fully specified by 3GPP. The following should be studied:

- Whether there is a need and how to extend the existing UPF advertising capabilities.

- Whether and how the input parameter(s) for UPF selection by SMF should be enhanced to support selection of UPF supporting specific user plane functionalities, e.g. NAT, Packet Inspection, etc.

## 5.2 Key Issue #2: Enhancements on UPF information exposure

### 5.2.1 Description

UPF Event Exposure service is supported in 5GS since Rel-17 and enhanced in Rel-18. Rel-18 UPEAS has defined mechanisms for both direct and indirect subscription to the UPF Event Exposure Service. In Release 19, further study is proposed on whether and how to enhance UPF information exposure, including the direct or indirect subscription to the UPF event exposure service.

The key issue is to identify use cases for enhancements on UPF event exposure service and for each use case determine whether and how the consumer can directly or indirectly contact the UPF for its subscription.

The following aspects should be studied in relation to UPF exposure service(s):

- Identify the specific use case and scenarios that require optimizing the procedures related to UPF data collection with enhancements on UPF direct or indirect subscription;

- Whether and how the consumer NF can directly or indirectly contact the UPF for its subscription;

- How to authorize the consumer NF for directly subscribing to UPF event exposure service(s), and how to update/release the subscription;

- How to support the UPF relocation when some NFs have subscribed the direct or indirect subscription of UPF information.

- Which Event ID(s) can be subscribed/requested directly or indirectly to the UPF exposure service;

- Whether there are use cases that require other enhancements on UPF exposure services

NOTE: Any enhancements with existing mechanisms need to be justified by analysing the benefits vs. drawbacks compared to existing mechanisms.

## 5.3 Key Issue #3: Study enhancements for UPF handling of headers

### 5.3.1 Description

This KI maps to the WT#3 of the SID.

The KI will study the enhancements needed to permit additional handling of packet headers by UPF. The following aspects will be studied:

- Analyse the use cases and problems to be solved and the feasibility of headers handling (i.e. insert, detect) in UPF for the different protocol layers (e.g. application, transport, IP layer…), including for the case of encrypted and unencrypted protocols.

- Whether and how to enhance the interface between a trusted AF or untrusted AF (i.e. via NEF) and 5GC to permit configuration of the UPF to insert or detect specific headers in different protocol layers in uplink and downlink directions, with consideration to:

- User Privacy and anonymity.

- Applicability of the configuration, e.g. S-NSSAI/DNN, FQDN, PDU Session, traffic flows, per subscriber , DNAI, etc

- Frequency of the insertion/detection, e.g. only once, all packets in the applied configuration, upon changes of traffic destination, etc.

- Whether and how the Policy and Charging Control framework and 5GC interfaces (e.g. N4) need to be enhanced

- Whether and how to enhance the interface between trusted AF or untrusted AF (i.e. via NEF) and 5GC for the UPF to expose information related to the detection of packet headers in uplink and downlink.

# 6 Solutions

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |  |  |
| --- | --- | --- | --- |
|  | Key Issues | | |
| Solutions | Key Issue #1 | Key Issue #2 | Key Issue #3 |
| Solution #1: Provisioning of information for header handling |  |  | x |
| Solution #2: UPF provision and selection based on new UPF functionality #2 | x |  |  |
| Solution #3: Selection on UPF with extended user plane capabilities | x |  |  |
| Solution #4: Selection of UPF providing specific user plane functionalities | x |  |  |
| Solution #5: Direct subscription of UPF event exposure service for TSC management |  | x |  |
| Solution #6: UPF selection based on the status of the supported functionalities | x |  |  |
| Solution #7: Translating SUPI/GPSI to NATed IP address |  | x |  |
| Solution #8: UPF event exposure during UPF relocation |  | x |  |
| Solution #9: DNAI Mapping information exposure |  | x |  |
| Solution #10: Subscription to UPF Event Exposure Services in the event of UP Path change |  | x |  |
| Solution #11: Direct subscription of UPF event from NEF/trusted AF or NWDAF |  | x |  |
| Solution #12: Direct subscription to UPF Event Exposure service via N6 |  | x |  |
| Solution #13: UPF Discovery and Direct Subscription to UPF for AF |  | x |  |

## 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.

Recenly, 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:

- Specific traffic detection and 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 a rule referred to by an AF.

### 6.1.2 Procedures

#### 6.1.2.1 Insertion/detection request

The proposed rule shall include:

Table 1 – Input parameters from AF

|  |  |  |
| --- | --- | --- |
| Input parameters from AF | | |
| Header/Tag information  (NOTE 3) | Identifier | Example: tagID (1) pointing to preconfigured Tag Type= RAT and Tag Value to be included by 5GC nodes |
| Tag Type + Tag Value | Example: Tag Type=FQDN, Tag Value=domain.com |
| Header/Tag Actions | Action | Values: Insert, Detect, Remove, Replace |
| Condition | Values: Always, at initiation, during certain period |
| Direction | Values: UL, DL |
| Header/Tag Handling Instructions | Reference | Example: RuleID (1) poiting to preconfigured information in UPF for protocol info, encryption handling, etc |
| Additional Data | Non-standard info used by AF to complement the preconfigured ruleID |
| Reporting Instructions  (NOTE 1) | Type of report | Values: Direct, Indirect, No report  (NOTE 1) |
| Condition for reporting | Values: Threshold based, Periodical with periodicity, etc |
| Reporting correlation identifier | Correlation ID (NOTE 2) |
| Reporting-to address | UPF event consumer URI (NOTE 2) |

Editor’s NOTE: Further refinement of the parameters may be needed.

NOTE 1: The condition for reporting and reporting correlation apply when type of report is direct or indirect. Whether to include an explicit “no report” is left for stage 3.

NOTE 2: Nnef\_TrafficInfluence includes already a Notification Target Address that could be used as the UPF event consumer URI. A correlationID would need to be added. In Nnef\_TrafficInfluence these parameters are to report on user plane events. It remains to be seen if these existing parameters can be used also for the header handling reporting.

For the Reporting Instructions, there are two options for the AF to indicate whether direct reporting is required (i.e. using UPF exposure service):

- Option 1: Report Correlation ID and UPF event consumer notification URI values. The AF provides these attributes to indicate its preference to receive Session Reports directly from the UPF Exposure Service (see option 1 in Section 6.1.2.2.23) instead of default N4 based reporting described in Section 6.1.2.2.1.

- 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 are sent directly with UPF Exposure Service.

Editor’s Note: Only one of the above options, with its associated procedures in the following chapters, will be taken for conclusion.

The header/tag handling instructions are assumed as pre-agreed information between the parties to include header/tags handling related information (e.g. protocol layer, type of encryption, etc), which is pre-configured in the UPF. This parameter contains a reference to the pre-configured info as well as, optionally, additional data that the AF provides to complement the pre-configured information. This additional data is not standardised, but only interpreted by UPF based on SLA and implementation.

NOTE 3: Headers/Tags types and values can be conditionally included by the AF (according to the use case). When those are not included, the Identifier requested points to a preconfigured Header/Tag type whose value is to be determined by the PCF, SMF or UPF depending on the data from network and/or policy information.

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

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

The information in table 1 is provided in the relevat Nnef\_TrafficInfluence operation (create/update/delete) by the AF. 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 TS 23.502 clause 4.3.6.2 to apply for this solution:



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

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 request is authorised 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 verifies the content of the header/tag identifier (or the header/tag type and value) and the header/tag handling instructions as the pre-agreed information between the parties and transforms it in the relevant information to be inserted/detected (i.e. deriving header/tag type and value from the header/tag identifier, etc). It will be included in the PCC rule together with the handling instructions reference, the additional data contents (if provided), and the direction for handling. If the AF requests reporting on header/tag detection /replacing/removal, the PCF includes in the PCC rule(s) the information required for reporting the event including indicating whether duplicate reporting is needed.

NOTE 4: Duplicate reporting does not assume to provide two simultaneous notifications to the AF. Duplicate reporting refers to UPF reporting directly to the AF, if AF has requested so, and reporting to SMF via N4, in case SMF needs to perform some additional actions.

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.

In step#6, in case the AF request results in the selection/addition/removal/replacing of a UPF in the data path, the SMF discovers the UPF(s) from NRF with the UPF capability of specific header/tag detection and handling, then the following options exist:

**OPTION 1**

- 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. Further some additional action maybe included for SMF to perform in case of detection of particular header/tag.

**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

#### 6.1.2.2 Header/tag reporting/notification

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/tag 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 is to be expected for the reporting/notification of detected header/tags, according to the settings the AF makes 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)**

When UPF detects the header/tag requested by the AF, the UPF notifies with N4 Session Report to the SMF. The N4 session report shall include the information related to the header/tag that has been detected.

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 handing 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 the detection action 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. The 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 TS 23.502 clause 4.3.6.3, 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/Tag detected). SMF may notify PCF using the existing Npcf services for event reporting.

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.

NOTE 1: 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.

##### 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 2: 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 sent 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.

### 6.1.3 Impacts on services, entities and interfaces

- NEF

- Nnef\_TrafficInfluence service, include the new Header handling and reporting information for a new event as described in 6.1.2.1 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 header handling information in the PCC based on request received a local information and policies

- NRF:

- Storing new UPF capability in UPF profile.

- Discovery of UPF(s) with the new UPF capability of header/tag detection and handling

- SMF

- Discovery of UPF(s) with the new UPF capability of header/tag 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

- Impacts related to reporting over N4 (depending on the solution option selected)

- 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.

## 6.2 Solution #2: UPF provision and selection based on new UPF functionality

### 6.2.1 Key Issue mapping

This solution is for KI #1 Selection of UPF providing a selected user plane functionality.

### 6.2.2 Description

UPF has supported to register in NRF. This registration phase uses the Nnrf\_NFManagement\_NFRegister operation. But some the UPF capabilities are not included in the UPF Provisioning Information in the NRF.

For example, there are identified 3 scenarioes that justify use case that necessitate a need to extend the existing UPF capabilities in case UPF has integrated additional functionalities as below:

- Scenario 1: Identifying UPF supporting features as NAT.

Background: Multi solution environment where some of UPF support NAT, it is difficult to select UPF as per requirement.

- Scenario 2: DDoS protection or Firewall support in UPF.

Background: To identify which UPF enabled with security features.

- Scenario 3: Layer 7 DPI inspection

Background: One of the key product capabilities that is often integrated in the UPF is Deep Packet Inspection (DPI) based services. DPI is the examination of layer 7 (L7), which contains Uniform Resource Identifier (URI) information. In some cases, layer 3 (L3) and layer 4 (L4) analyzers that identify a trigger condition are insufficient for billing purposes, so layer 7 examination is used.

It would be beneficial that the UPF can register its capabilities in the NRF and NRF provides them to SMF, without relying on the N4 interface.

By adding the specific user plane functionalities of each UPF instance into the UPF Provisioning Information when registering in NRF, a consumer NF or an SMF can issue a request to the NRF including the UPF capabilities for proper UPF discovery and selection.

This contribution proposes to register/update the new UPF functionalities in NRF to support UPF selection/discovery with the specific user plane functionalities.

### 6.2.3 Procedures

Procedures in TS 23.502 clause 4.17.1 and clause  4.17.2 are reused to support registering specific UPF functionalities in NRF. The following UPF functionalities are added in UPF profile stored in NRF:

- NAT functionality, and the type of the NAT functionality e.g. static NAT, pooled NAT, NAPT, easy IP, and NAT server.

- Packet Inspection functionality, i.e., Layer 7 DPI.

- DDoS protection or Firewall

- DNS snooping

Procedures in TS 23.502 clause  4.17.6 is reused to support SMF provisioning of UPF via the NRF by providing the new UPF functionalities above in the request.

Procedures in clause 4.15.4.5.3 is reused to support UPF discovery via the NRF by providing the new UPF functionalities above in the request.

### 6.2.4 Impacts on services, entities and interfaces

NRF:

- Storing new UPF functionalities in UPF profile.

- Support of new query parameters accords with the new UPF functionalities, e.g. NAT, packet inspection.

SMF

- Discovery of several UPFs that accords with the new UPF functionalities, e.g. NAT, packet inspection.

UPF:

- Enhanced to register new UPF functionalities in the NRF

## 6.3 Solution #3: Selection on UPF with extended user plane capabilities

### 6.3.1 Description

#### 6.3.1.1 Solution Description

This solution proposes to improve current UPF selection by extending the baseline UPF capabilities announced in N4 and UPF NF profile in NRF by defining an open and generic value (e.g. octet string) which can be used for non-standard or partially supported features:

- The content of this new information element shall be configured by operator at UPF, and it represents the characteristics of this NF, which could be beyond current 3GPP standardized capabilities.

- The content syntax could be just a string or a sequence of bits values. This is for stage 3 to define what is the best syntax.

- SMF can use this information to choose right UPF according to the capabilities of UPF and the needs of the PDU session.

- This new information element is to be considered in the selection/re-selection of UPF (see clause 6.3.3.3 in TS 23.501 [1]).

The proposed solution can be used for addressing many scenarios. As an example, the new information element can be defined to correspond to:

- Different hardware configurations (e.g CPU or NIC (Network Interface Controller) that brings better capacity or latency characteristics).

- Partial support of a standardized feature.

- Non-standard features implemented in UPF, such as e.g. NAT, firewalling or advanced non standardized reporting or forwarding features that cannot be mapped to current information elements as capabilities.

And combinations of the above, simplifying management of complex deployments where several UPFs (potentially from different vendors and/or for special purpose e.g. tuned for the Edge) coexist.

The new information element proposed is referred to as *AdditionalSupportInfo* in following clauses.

### 6.3.2 Procedures

The solution enhances the following procedures:

- It extends the PFCP Association Setup (see clause 4.4.3.1 with “N4 Association Setup Procedure” and clause 4.4.3.2 “N4 Association Update Procedure” in TS 23.502 [3]) adding new capabilities for supported functionalities. This is for stage 3 to define, for example extending current IE Supported-Features IE in PFCP with one more bit and adding a new *AdditionalSupportInfo* IE with a new octet string that contains the information configured locally in UPF (as described in 6.3.1).

- It extends UPF registration in NRF (clause 4.17.1 “NF service Registration” and clause  4.17.2 “NF service update” in TS 23.502 [3]) by adding in NF profile for UPF new capabilities. This is for stage 3 to define, for example extending SupportedPfcpFeatures in UpfInfo element in Nnrf\_NFManagement NFRegister Request message with one more bit and adding a new *AdditionalSupportInfo* IE that contains the information configured locally in UPF (as described in clause 6.3.1).

- It enhances UPF discovery assisted by NRF (see discovery procedures, e.g. clause 4.17.4 “NF/NF service discovery by NF service consumer in the same PLMN” in TS  23.502 [3]). The Consumer may include in Nnrf\_NFDiscovery Request message the desired value of new *AdditionalSupportInfo* parameter in the NFProfile.

- It enhances UPF selection by the SMF. As part fo PDU Session Management, SMF must select the UPF for the PDU Session. As indicated in clause 6.3.3.3 “Selection of an UPF for a particular PDU Session” in TS 23.501 [1], the capability of the UPF including the new *AdditionalSupportInfo* IE and the functionality required for the particular PDU session shall be considered so an appropriate UPF can be selected by matching the functionality and features required.

See below in figure  6.3.2-1 how this solution enhances UPF Selection during PDU Session Establishment (based on clause 4.4.3 in TS  23.502 [3]).

When this procedure is triggered, UPF has already provided its capabilities to SMF over N4 or SMF gets them from NRF as described above. As shown in figure 6.3.2-1, it is in the step 8 of this procedure where SMF performs UPF selection. For such selection, the UPF new capabilities (including *AdditionalSupportInfo* IE) are considered by SMF in addition to the baseline ones so an appropriate UPF can be selected by matching the functionality and features required

Editor's Note: it is FFS if there is any existing IE in PFCP/NF profile that can be used

How the SMF determines information about the user plane network topology, also including this new *AdditionalSupportInfo*, is based on operator configuration (as indicated in NOTE1 in clause 6.3.3.3 Selection of an UPF for a particular PDU Session in TS 23.501.

AMF

P

C

F

UDM

(R)AN

UE

7

b.

SM

Policy

Association

Establishment

or

SMF initiated

SM

Policy

Association

Modification

10

a

.

N

4

Se

ssion

Establishment

/Modification

Request

1.

PDU Session

Establishment

Request

UPF

SMF

10

b

.

N

4

Session Establishment

/Modification

Response

9

. SMF initiated SM Policy Association Modification

1

1

.

Namf\_Communication\_N1N2MessageTransfer

1

3

.

AN

-

specific resource setup

(PDU Session Establishment Accept)

1

2

. N

2

PDU Session

Requ

est

(NAS msg)

1

4

. N

2

PDU Session

Re

sponse

1

5

. Nsmf

\_

PDUSession\_

UpdateSM

Context

Request

1

6

a

.

N

4

Session

Modification

Request

1

6

b

.

N

4

Session

Modification

Response

1

9

. IPv6 Address Configuration

First Uplink Data

First Downlink Data

8

. UPF selection

:

**(new) SMF consider UPF AddditionSupport Info**

2. SMF selection

1

7

. Ns

mf\_

PDUSession\_

UpdateSM

Context

Response

7

a. PCF selection

DN

6

.

PDU Session authentication/authorization

3

.

Ns

mf\_

PDUSession\_

CreateSMContext

Request

4. Subscription retrieval

/ Subscription

for updates

2

1

.

Unsubscription

5

. Ns

mf\_PDUSession\_CreateSMContext Response

1

8

.

Nsmf\_

PDUSession

\_

SMContext

Status

Notify

16c. Registration

20. SMF initiated SM Policy Association Modification

**Figure 6.3.2-1 Example of UE-requested PDU Session Establishment for non-roaming and roaming with local breakout (TS** **23.502[3] clause** **4.3.2.2)**

### 6.3.3 Impacts on existing nodes and functionality

UPF, SMF, NRF are impacted.

Impacts results from adding the *AdditionalSupport Info* information in UPF configuration and in the procedures for:

- PFCP Association Setup.

- UPF registration in NRF.

- UPF discovery assisted by NRF.

- UPF selection by the SMF.

As described in clause 6.3.1.

## 6.4 Solution #4: Selection of UPF providing specific user plane functionalities

### 6.4.1 Key Issue mapping

This solution addresses Key Issue #1.

### 6.4.2 Description

The functionality of the UPF is defined in 3GPP TS 23.501 clause 6.2.3. Currently a UPF advertises the features it supports in the NF profile of the UPF registered in NRF as specified in e.g. 3GPP TS 29.510 clause  6.1.6.2.13, and/or over PFCP as defined in 3GPP TS 29.244. An SMF leverages the exposed UPF information for proper UPF discovery and selection. A UPF implementation may support optional functionalities like NAT, Packet Inspection, etc. which might be useful for a PDU session. For the most optimal UPF selection for a PDU session a solution needs to address the following aspects:

1. How does the SMF determine the UPF functionalities that should be considered for the selection of the most appropriate UPF for a given PDU session?

2. How the UPF discovery is enhanced to enable an SMF to discover a UPF offering functionalities like NAT, Packet Inspection, etc. which are considered useful for the relevant PDU session?

The current solution proposes that the SMF determines the UPF functionalities for a PDU session based on:

**1. Configuration**: The SMF may be configured with the UPF functionalities to use for PDU sessions established for a given DNN/S-NSSAI. The UPF functionalities may be required and/or desired for the PDU Session.

**2. Subscription information from the UDM/UDR**: The SMF may receive subscription information from the UDM, during (or after) the establishment of the PDU session, indicating functionalities that are required and/or desired for the PDU session. For example, subscription information for children might require parental control for the internet DNN/S-NSSAI.

**3. Policy information received from the PCF:** The SMF may receive policy information from the PCF, during (or after) the establishment of the PDU session, indicating functionalities that are required and/or desired for the PDU session. The PCF may be configured with relevant policies e.g. per DNN/S-NSSAI, or per subscriber, group(s) of subscribers, etc. For example, for subscribers of a specific enterprise some functionalities might be required and/or preferred.

**4. Input from the incoming request.** The incoming request is not modified in this solution, existing input can be leveraged.

When the SMF determines a UPF functionality as required for the PDU Session it only selects a UPF supporting the UPF functionality. If such a UPF does not exist, the PDU Session Establishment request is rejected. When the SMF determines a UPF functionality as desired for the PDU Session the SMF prefers selecting a UPF supporting the desired functionality, however if such a UPF is not available the PDU Session is served by a UPF supporting at least all required functionalities. For a combination of required and desired functionalities for a PDU Session the SMF selects a UPF for the PDU Session supporting all the required functionalities and most of the desired functionalities possible. For the cases were the optimal UPF for a PDU Session is loaded or located away from the current UE location etc. it is up to the SMF implementation/configuration to make the best possible UPF selection considering all relevant functionalities and the rest KPIs. The following flowchart describes the logic followed by the SMF:



**Figure 6.4.2-1: UPF selection logic at the SMF**

Examples of UPF functionalities that may be required or desired for a PDU session are the following:

- support of Deep Packet Inspection (DPI) with specific DPI levels, e.g. specific transport levels such as QUIC, MP-QUIC, MP-TCP, MASQUE and/or application such as HTTP, RTP, SIP, WebRTC, etc.;

- support of parental control, with optionally specific controls to be enforced to the traffic;

- support of MASQUE proxy functionality.

The UPF advertises its functionalities in its NF profile via proper extensions. Discovery query parameters used by the SMF are enhanced accordingly to support the discovery of the UPF functionalities. The SMF leverages the Nnrf\_NFDiscovery service to retrieve UPF profiles. Desired functionalities are queried as optional to the NRF so that the NRF returns UPFs either supporting these functionalities, if such UPFs exist, or UPFs which do not support the desired functionalities. Utilizing the returned UPF profiles from the NRF, SMF selects the best possible UPF to serve a PDU Session.

UPF functionality advertisement can also take place over N4 via the existing PFCP messages and proper extensions of the UP Function Features.

### 6.4.3 Procedures

Figure 6.4.3-1 depicts the procedure summarizing the solution. Only changes to existing TS 23.502 procedures to include new parameters are mentioned.



**Figure** **6.4.3-1: Procedure for selecting the optimal UPF for a PDU Session supporting required and desired functionalities**

1. A PDU Session Establishment (Modification) request is received at the SMF. No modifications are foreseen by this solution to this message.

2. SMF retrieves session related subscription information from the UDM which might include required and/or desired functionalities for the PDU Session.

3. Policy association (modification) is triggered by the SMF.

4. PCC rules might include required and/or desired functionalities for the PDU Session.

5. SMF discovers UPFs with the help of NRF by issuing an Nnrf\_NFDiscovery request. Required and desired UPF functionalities are included in the query.

6. NRF returns the profiles of the UPFs supporting at least the required UPF functionalities.

7. SMF selects the best UPF supporting all the required functionalities, if it exists, and the maximum set of desired functionalities.

8. N4 Session Establishment/Modification request properly extended, if needed, to configure the UPF as necessary for using the required and/or optional functionalities.

### 6.4.4 Impacts on services, entities and interfaces

- UDM/UDR – Session subscription information might include required and/or desired functionalities for the PDU Session of the subscription.

- PCF – includes in the PCC rule required and/or desired functionalities for the PDU Session.

- NRF – supports the UPF profile with the extended functionalities. The NRF also supports enhanced discovery with new query parameters for the UPF functionalities.

- SMF – supports extended UPF discovery and selection based on required and/or desired UPF functionalities for the PDU Session. The SMF also supports any N4 extensions for the proper UPF configuration for using the required and/or desired UPF functionalities.

- UPF – supports extended UPF functionalities, their advertisement in UPF profile and/or N4 interface and their configuration if needed from the SMF via PFCP messages.

## 6.5 Solution #5: Direct subscription of UPF event exposure service for TSC management

### 6.5.1 Description

This solution is applicable for a case the UPF employs the NW-TT functionality. According to the latest TS 23.501 specification, the assumptions are as follows.

- 5GS TSN bridge has a single NW-TT entity within UPF.

- Bridge ID is to distinguish between bridge instances within 5GS

- To support TSN, the user plane node ID is Bridge ID.

- To support integration with IETF DetNet, the user plane node ID can be Router ID. The user plane node ID may be pre-configured in the UPF based on deployment.

- TSN AF or TSCTSF has and stores the Bridge ID or Router ID and its address before subscription of UPF event exposure service for TSC management.

Based on the assumption, TSN AF or TSCTSF can directly subscribe UPF event exposure service to exchange TSC management information (i.e. UMIC and/or PMIC).

### 6.5.2 Procedures

#### 6.5.2.1 Direct subscription of UPF Event Exposure service for TSC management



Figure 6.5.2.1: Direct subscription of UPF Event Exposure service for TSC management

1. TSN AF or TSCTSF gets user plane node ID as Bridge ID or Router ID through PDU session establishment procedure.

2. TSN AF or TSCTSF gets UMIC for the address of user plane node ID through PDU session modification procedure via PCF and SMF.

3. TSN AF or TSCTSF stores user plane node ID and its address.

4. The consumer NF directly subscribes the UPF event exposure service for TSC management or time synchronization and deterministic networking between TSN AF or TSCTSF and NW-TT via Nupf\_EventExposure\_Subscribe service operation.

5. When the subscribed event is occurred, the UPF sends the collected UPF data (i.e., TSC management information) via Nupf\_EventExposure\_Notify service operation to the consumer NF.

Editor’s Note: The impact of this procedure to the existing procedures of TSN Bridge information exchange and management is FFS.

### 6.5.3 Impacts on services, entities and interfaces

TSN AF or TSCTSF:

- Supports direct subscription of UPF event exposure services for TSC management (i.e., Event ID).

UPF:

- Supports direct subscription of event exposure services for TSC management (i.e., Event ID).

## 6.6 Solution #6: UPF selection based on the status of the supported functionalities

### 6.6.1 Key Issue mapping

The solution applies to Key Issue #1: Selection of UPF providing a selected user plane functionality.

### 6.6.2 Description

As described in the Key Issue #1, UPF advertises the features it supports in the NF profile of UPF registered in NRF. A UPF implementation may support more optional functionalities like NAT, Packet Inspection, etc. An SMF leverages the exposed UPF information for UPF selection.

In the context of TS 23.501[2], the exposed features are introduced as following parameter(s) and information that may be considered in the UPF selection by the SMF.

- Capability of the UPF and the functionality required for the particular UE session: An appropriate UPF can be selected by matching the functionality and features required for an UE.

Note:

- The capability or functionality to be provided may be further described as a part of UPF Provisioning Information in the NRF.

In UPF implementations, individual functionality can be enabled/ disabled after the provisioning. In such a case, the individual functionality may be seen as to be provided from the NF profile perspective because it has been provisioned. But it may not be available.

The objective of the UPF selection in the SMF is to discover available UPF instance(s). NFDiscovery can be used to clarify if individual functionalities are supported or non-supported.

This solution further clarifies if the individual functionalities are available or unavailable out of the discovered UPF(s) so that SMF can accurately select available UPF(s)

Assumptions:

- As described in TS 23.501 [2], OAM configures NF Profile for the UPF.

### 6.6.3 Procedures

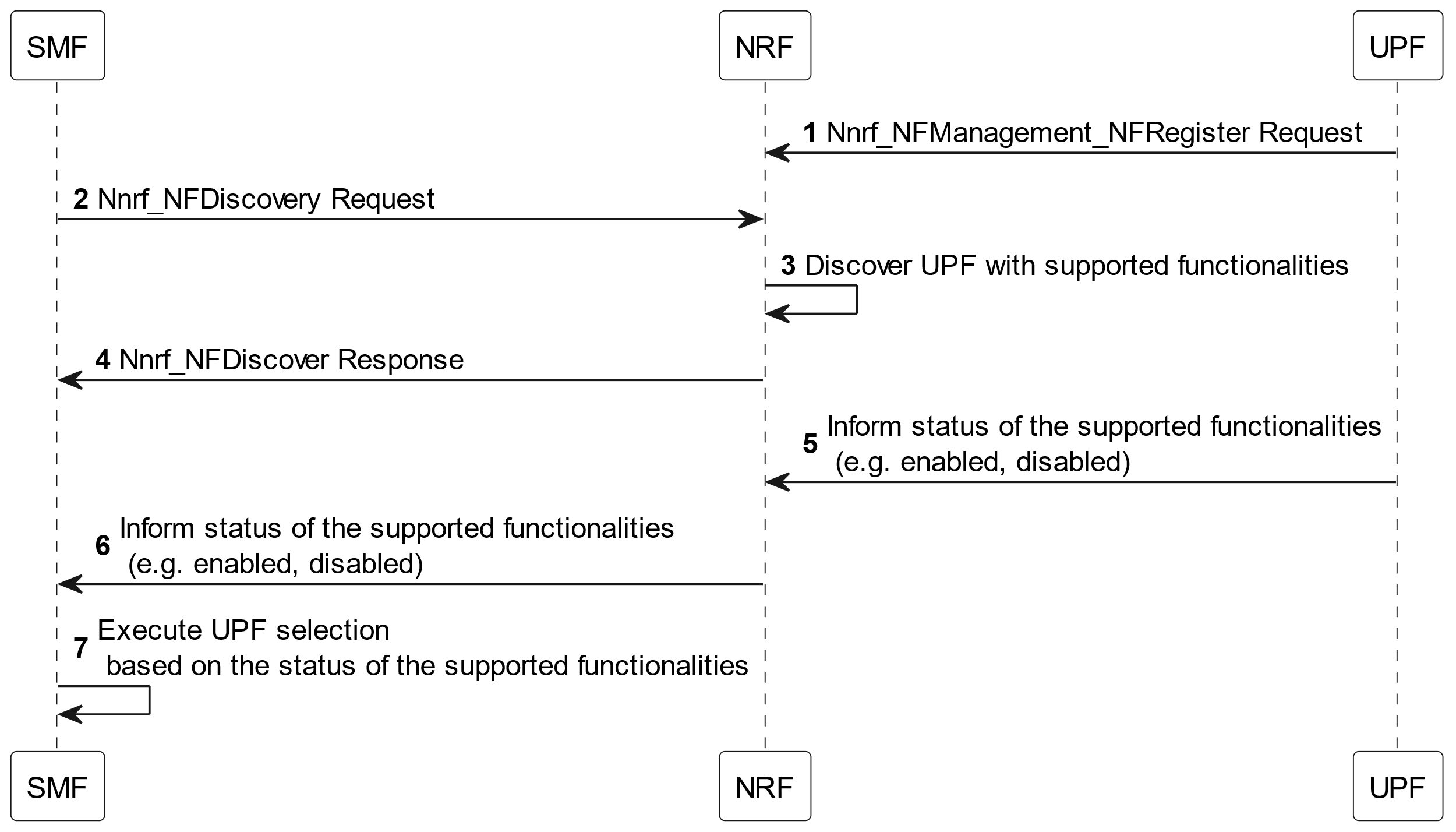


Figure 6.6.3- Procedure to notify status of functionalities in UPF

1. UPF invokes Nnrf\_NFManagement\_NFRegister service to request NRF to register the configured NF Profile for the UPF.

2. In PDU session establishment, for example, SMF invokes Nnrf\_NFDiscovery service to request NRF to discover UPF(s) that supports event exposure service to notify status of running functionalities (e.g. active, inactive of NAT, Packet Inspection, etc.).

3. NRF responds SMF to give NF Profile for the UPF that matches the request.

4. SMF has:- a list of UPF(s) that supports targeted functionalities

5. UPF informs status of the individual functionalities in the discovered UPF(s)

6. NRF informs status of the individual functionalities in the discovered UPF(s)

Editor’s note: Which operation is used and impacts are for further study.

- Leveraging Nnrf\_NFManagement service operations

- N4 Node Level Procedures

Editor’s note: Impacts to the existing PDU session needs to be studied.

7. SMF executes UPF selection based on the status of the supported functionalities in the UPF. For example, UPF in which the status of NAT is active is selected if UPF with NAT is requested.

Editor’s Note: How UPF know which SMF is to be notified and how to notify it as no SMF endpoint information.

Editor’s Note: It is FFS for SMF what is the difference of the one functionalities in the UPF is disable comparing to the one functionalities is not included in the UPF NF profile.

### 6.6.4 Impacts on services, entities and interfaces

SMF:

- UPF selection based on the status of the supported functionalities

UPF:

- Notification about status of supported functionalities

NRF:

- Notification about status of supported running functionalities

## 6.7 Solution #7: Translating SUPI/GPSI to NATed IP address

### 6.7.1 Description

#### 6. 7.1.1 Background and problem description

While in R18 UPEAS item, the NAT related issues are introduced and solved. If NAT deployed in network, there exists the mapping table between internal private UE IP address (used in 5GC internally) and public UE IP address used in application server.

If NAT is supported in network, there exists the problem that in eNA UE data collection procedure listed below:

- As indicated in step 3a and 3b in section 6.2.8.2.3 of TS 23.288[x], the NWDAF subscribes to the AF in trusted/untrusted domain for UE data collection. In the request from NWDAF, the SUPI or to GPSI is included to identify the target UE for data collection. And also indicated in the section 6.2.8.2.4.1 of TS  23.288[x], the UE IP address is used to identify the user plane connection established between the UE application and the AF for data collection. The AF is required to correlate the UE IP address to the SUPI or to GPSI. Or, as indicated in section 6.2.8.2.4.4, the NWDAF should correlate the UE IP address to the SUPI or to GPSI.

- And as described in section 6.2.8.2.4.2, 6.2.8.2.4.3 and 6.2.8.2.4.4, the AF or NWDAF uses the SUPI/GPSI to obtain the serving SMF id(s) from UDM, and request the SMF to obtain the allocated IPv4 address or IPv6 prefix for the UE. After these procedures, the AF or NWDAF gets the UE IP address.

However, the allocated IPv4 address here that AF or NWDAF gets from SMF is a private IP address, not the public UE IP address. The SMF or DHCP can only allocate the private UE IP address. And in the internal 5GC, between the interaction of each 5GC elements, only the private UE IP address is used.

Even if the AF receives the private UE IP address, the AF cannot identify the target UE for data collection, because the AF can only identify the public UE IP address, if the NAT function is deployed in UPF.

So, as the description above, after introducing the NAT functionality, there is a lack of a process to provide public UE IP address to AF to identify the target UE for data collection.

#### 6.7.1.2 High level description

NWDAF can subscribe to the AF in order for the AF to collect data from UE which can be used by NWDAF for analytics to the UE. In the subscription, the NWDAF can provide the SUPI/GPSI to the AF, and the AF then needs to be able to correlate the IP flow between itself and the UE with the received SUPI/GPSI. The NWDAF can also by itself provide the IP address to the AF, i.e. NWDAF translates SUPI to UE IP address.

One solution to this correlation is for the AF/NEF to query UPF for this mapping e.g. via SMF. Since a UE can have many PDU sessions for a DNN and S-NSSAI each with its own NAT address, and the UE can also have many ongoing IP flows on a PDU session where only one of these is towards the AF, there must be a way to distinguish the flow between the UE and the AF from all other flows. This solution proposes that the AF provides a list of its IP addresses that the AF uses for its communication with the UEs, or if AF uses NEF, the NEF is configured with the list of IP address the AF uses for its communication with UEs, or the UPF provides the full NAT mapping table for a UE address.

### 6.7.2 Procedures

#### 6.7.2.1 Procedure

SMF

NF/AF

UPF

1. Nsmf\_GetPublicIPaddressAndPort req.

2. Nupf\_GetPublicIPaddressAndPort req.

3. Nupf\_GetPublicIPaddressAndPort resp.

2. Nsmf\_GetPublicIPaddressAndPort req.

Figure 6.7.2-1: Getting NATed IP address and port

0. PDU session(s) has been established. If GPSI is known, NF(e.g. NEF or NWDAF)/AF has translated GPSI to SUPI. NF has discovered SMF(s) handling ~~a~~ the PDU session(s) for the combination of SUPI and DNN and S-NSSAI. The NF needs to know the endpoint addresses of the remote end (that is, all possible destination IP addresses of the UE IP flows e.g. the AF endpoints) if it is the NF and not AF that is to execute the procedure.

1. NF/AF sends 1. Nsmf\_GetPublicIPaddressAndPort request (SUPI, DNN, S-NSSAI, optionally: list of public IP addresses for the remote endpoint, e.g. the AF endpoints) to SMF. The NF (e.g. NEF or NWDAF) consumes Nudm\_UECM\_Get to obtain the address of SMFs that serving this UE.

NOTE 1: If the UE has several PDU sessions for the DNN and S-NSSAI, and these are served by different SMFs, the NF/AF sends a request to each of those SMFs.

2. SMF translate the SUPI, DNN and S-NSSAI to UE private IP address(es), and sends Nupf\_GetPublicIPaddressAndPort request (UE private IP address and, DNN, S-NSSAI, and if received, list of public IP addresses for the remote end) to UPF.

NOTE 2: If the UE has more than one PDU session for the DNN and S-NSSAI, then if the SMF uses IP address in the request to UPF, the SMF sends several requests to UPF.

3. UPF finds all related NAT mappings for the received UE private IP address (or SUPI) and if a list of public addresses was received in step 2., UPF selects the NAT mapping of the UE flows with destination IP address within the received list of public IP addresses for the remote end, and UPF responds with Nupf\_GetPublicIPaddressAndPort response (UE's NATed Public IP address, TCP/UDP Port). If UPF did not receive a list of public IP addresses for the remote end, UPF responds with all NAT mappings related to UE IP address in Nupf\_GetPublicIPaddressAndPort response.

4. SMF forwards the received info in step 3 to NF/AF.

If AF requested the public IP address via NEF, and if NEF receives the full mapping NAT mapping table (i.e., UPF did not receive a list of public IP addresses for the remote end), NEF only provides the public IP address and port that is relevant for the AF.

NOTE 3: providing full mapping table to an untrusted AF might have some privacy issues.

Editor's note: The main use case is data collection, it is FFS if the IP connection used between AF and UE in TS 26.531 is short lived or if it is long lived.

#### 6.7.2.2 Service definition

##### 6.7.2.2.1 Nupf\_GetPublicIPaddressAndPort

**Service operation name:** Nupf\_GetPublicIPaddressAndPort\_Get

**Description:** NF service consumer gets the NATed UE public IP address and Port, for the IP flow between the UE and a remote end, e.g. an AF.

**Inputs, Required:** private UE address (UE IP address assigned by 5GC for the PDU session).

**Inputs, Optional:** DNN, S-NSSAI, IP domain, list of public IP addresses of the remote end.

**Outputs, Required:** if list of public IP addresses was in Inputs: a public IP address and source TCP/UDP port (or non, if no NAT mapping was found). If no list of public IP addresses was in Inputs: the full NAT mapping table for the UE IP address.

**Outputs, Optional:** None

### 6.7.3 Impacts on services, entities and interfaces

NWDAF: New service operation, need to know the end point addresses of the remote end, e.g. via configuration.

NEF: New service operation, need to know the end point addresses of the remote end, e.g. via configuration, or via signalling from AF.

AF: New service operation, can provide the end point addresses of the remote end to NEF. A trusted AF provides these endpoint addresses.

SMF: new service.

UPF: new service, providing NAT mapping.

## 6.8 Solution #8: UPF event exposure during UPF relocation

### 6.8.1 Key Issue mapping

This solution is for KI #2: Enhancements on UPF information exposure.

### 6.8.2 Description

Rel-18 UPEAS has defined mechanisms that consumer (e.g., NWDAF) can subscribe to UPF for the events (e.g., QoS Monitoring) via SMF, and the UPF can directly send the event notification to the consumer.

NOTE 1: This solution focuses on the indirect subscription of UPF via SMF.

After the consumer subscribes to the UPF events, the UPF relocation may occur. For example, the condition for triggering UPF relocation may be one of the following:

- UE mobility: The SMF determines that the UE moves out of the serving area of the source UPF.

- Load balancing: The SMF determines that the serving UPF of the UE is overloaded and selects a new UPF to serve the UE.

- Service experience change: The SMF determines, e.g., based on NWDAF service experience analytics, that the current UP path cannot meet a service experience requirement, then determines to select a new UPF.

NOTE 2: This solution focuses on the UPF relocation, SMF relocation is not involved.

When the SMF determines that the UPF needs to be relocated, the SMF can select a target UPF, then unsubscribe from the source UPF and subscribe to the target UPF for the event exposure. When an unsubscribe is received, the source UPF may already collect some data, and the SMF can determine how to handle the collected data based on the indication in the subscription from the consumer, e.g., discard the collected data, send the collected data to the consumer immediately, send the collected data based on the Event Reporting Information. The SMF can indicate the source UPF how to handle the collected data when unsubscribing the source UPF, for example, discard the collected data, send the collected data to the consumer immediately, send the collected data to the consumer based on the Event Reporting Information.

### 6.8.2 Procedures

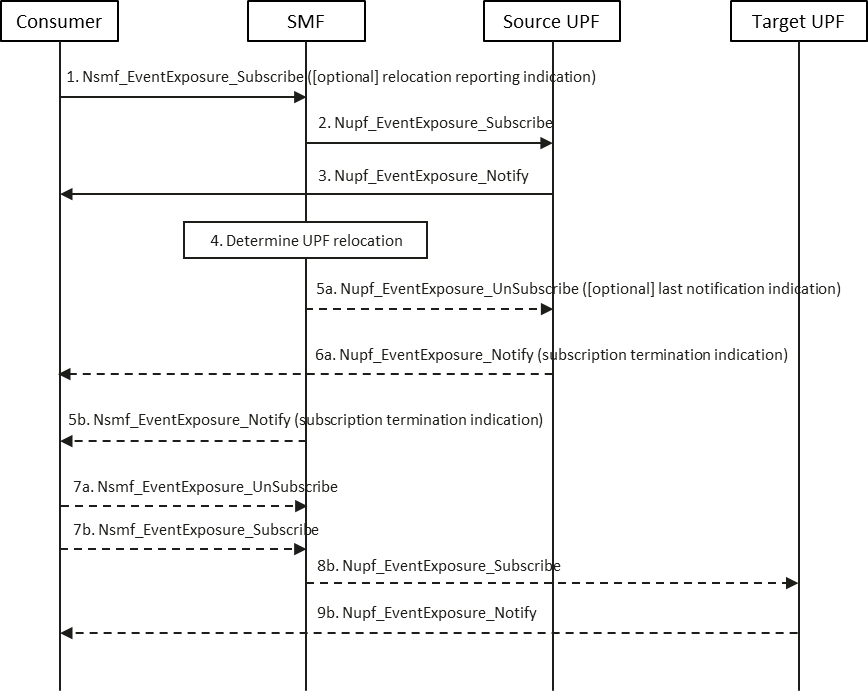


Figure 6.8.2-1: Procedure for UPF relocation

1-3. Consumer (e.g. NWDAF) subscribes to the UPF via the SMF, and the UPF sends notification for the subscribed event directly to the consumer. The consumer may include a relocation reporting indication, which indicates how to handle the data collected by the source UPF when UPF relocation occurs.

4. The SMF determines that the UPF needs to be relocated.

5a-6a. The SMF unsubscribes to the source UPF. The SMF may include a last notification indication in the unsubscribe message, which indicates how the source UPF handles the collected data. When the last notification indication indicates that the source UPF sends the collected data to the consumer, the source UPF sends the last notification to the consumer, which includes the collected data and the subscription termination indication. The subscription termination indication indicates that the subscription of the consumer has been terminated. The last notification to the consumer may also include a cause code (e.g. UPF relocation) corresponding to the subscription termination indication.

5b. As an alternative to step 5a-6a, the SMF may directly send the notification to the consumer, which includes the subscription termination indication, and may also include a cause code (e.g. UPF relocation) corresponding to the subscription termination indication.

7a. The consumer may unsubscribe to the UPF event exposure if the consumer determines that there is no need to subscribe to the target UPF.

7b-9b. As an alternative to step 7a, the consumer may update the event subscription, then the SMF may select a new UPF as target UPF, and send the updated event subscription to the target UPF. The target UPF will send notification for the subscribed event directly to the consumer.

### 6.8.3 Impacts to Services, Entities and Interfaces

Consumer NF:

- Indicate how to handle the data collected by source UPF when the UPF relocation occurs.

- Unsubscribe or update the subscription for the UPF event exposure based on the last notification from source UPF.

SMF:

- Indicate the source UPF how to handle the collected data when unsubscribing the source UPF.

Source UPF:

- Send the collected data and subscription termination indication to the consumer based on the last notification indication from SMF.

## 6.9 Solution #9: DNAI Mapping information exposure

### 6.9.1 Description

In clause 6.8 of TS 23.548[7], the AF may request DNAI mapping information from 5GC via NEF. The DNAI mapping information includes the EAS address information (i.e. IP address(es), EAS IP range(s) or FQDN(s)) and the associated DNAI. The DNAI mapping information is statically configured in the NEF/UDR by the OAM. This is not very efficient, since this needs the operators to be aware of any deployment changes in the Local DN.

This solution proposes that the DNAI mapping information is configured in the L-UPF, which is deployed in the Local DN and can be easily configured with the DNAI mapping information, e.g. IP address(es), EAS IP range(s) or FQDN(s). The NEF requests the DNAI mapping information from the L-UPF and stores them in the UDR. Then the AF can request the DNAI mapping information from the NEF/UDR, as described in clause 6.8 of TS 23.548[7].

NOTE: The DNAI mapping information may also be local configured in L-SMF if L-SMF is deployed in the Local DN. In this case the NEF request the DNAI mapping information from the L-SMF.

### 6.9.2 Procedures



Figure 6.9.2-1: DNAI Mapping Information Exposure

0. The NEF may discover L-UPF via NRF by invoking Nnrf\_NFDiscovery\_Request providing the DNAI. The NEF may also discover the L-UPF supporting the DNAI via local configuration.

1. The NEF sends the Nupf\_EventExposure\_Subscribe Request to the L-UPF to subscribe the DNAI mapping information.

2. The L-UPF sends the Nupf\_EventExposure\_Subscribe Response to the NEF, including the DNAI mapping information.

3. When DNAI mapping information is updated the L-UPF sends Nupf\_EventExposure\_Notify to NEF to provide the updated DNAI mapping information.

4. The NEF stores the DNAI mapping information in the UDR by invoking the Nudr\_DM\_Create/Update Request service operation.

5. The UDR response the NEF.

6. The AF request for the DNAI information from the NEF/UDR, as described in clause 6.8.2 of TS 23.548.

### 6.9.3 Impacts on services, entities and interfaces

UPF:

- Nupf\_EventExposure service is enhanced to provide the DNAI mapping information.

NEF:

- Subscribe and receive the DNAI mapping information from the L-UPF.

- Store the DNAI mapping information in the UDR

## 6.10 Solution #10: Subscription to UPF Event Exposure Services in the event of UP Path change

### 6.10.1 Key Issue mapping

This solution addresses KI#2.

### 6.10.2 Description

This solution aims to provide a mechanism to support UPF relocation when a consumer NF has directly subscribed to UPF for Event exposure. As per Rel-18, in case the UPF relocation happens, the consumer NF (which is in operator’s Trusted Domain) needs to perform the discovery of the relevant UPF again in order to subscribe to the new UPF for Event Exposure

The proposed solution is as follows:

- While subscribing to UPF’s Event Exposure Service, consumer NF can indicate to the subscribed UPF (source UPF) to receive a notification of the information of new UPF in case of UPF relocation happens for the session for which Consumer NF had subscribed to the UPF.

- The Source UPF may indicate to SMF to provide information of target UPF in case N4 session between UPF and SMF is released.

- The SMF then informs the Target UPF instance ID and other relevant information to the Source UPF and Source UPF can notify that information to Consumer NF.

- Consumer NF can then subscribe to the new UPF for the relevant Events. Thus saving the Consumer NF the further procedure to find the Serving UPF.

### 6.10.3 Procedures



Figure 6.10.3-1, Overview of procedure

It is assumed that the Consumer NF is inside the operator’s trusted domain, i.e. it is either NWDAF, TSCTSF, Trusted AF or NEF (in case an external AF subscribes to UPF event exposure via NEF). So authorization of consumer NF for using Nupf\_EventExposure service can be done based on existing mechanisms.

A description of the procedure in Figure 6.10.3.1 is as follows:

1. The consumer NF subscribes to Source UPF for event exposure services. The discovery of the corresponding UPF which needs to be subscribed to is assumed to be already done by the consumer NF before this step. In the request it provides indication for Target UPF info in case of UPF relocation. The Reporting Frequency would be set to one (i.e. at the time of UPF relocation).

2. UPF (using N4 interface) requests SMF to provide information of target UPF in case of UPF relocation.

3. SMF decides for UPF relocation for the relevant PDU Session(s).

4. SMF notifies the Source UPF regarding UPF ID of target UPF, and optionally other relevant information related to Event Exposure service endpoint.

NOTE 1: In case SMF does not provide information of Target UPF to the Source UPF in Step 4 (e.g. due to PDU Session release or SMF relocation), UPF may not proceed to Step 5, except in cases when Nupf\_EventExposure notify is needed to report parameters for subscribed Event ID (s) and is sent without information of Target UPF.

NOTE 2: In case Event subscription is for a specific UE, PFCP Session Release message may be used to carry the relevant target UPF information.

5. Based on the subscription request in Step. 1, and information received in Step 4, Source UPF notifies the NF optionally with the information of Target UPF received from the SMF. Source UPF is implicitly unsubscribed from event notification from UPF.

6. After receiving the information of the target UPF, if not already present, consumer NF may need to retrieve the NF profile for the target UPF, identified by the information received in Step 5, from NRF.Consumer NF may subscribe to Target UPF for event exposure service for the supported Event ID(s) for the relevant PDU Session.

7. A subscribed event is detected in this new UPF.

8. Target UPF notifies to consumer NF regarding the subscribed events.

The enhancement from the existing procedure is that the Consumer NF, once it is unsubscribed from Source UPF after Step 5 and receives the information of the target UPF, does not need to perform the discovery of serving UPF again.

### 6.10.4 Impacts on services, entities and interfaces

N4 interface is extended to exchange information related to Target UPF information in case of N4 Session release

Nupf\_EventExposure service is extended to include indication to notify information related to target UPF in case of UPF relocation. Nupf\_EventExposure Notify can include the information of the target UPF in case the UPF which is subscribed to is relocated.

## 6.11 Solution #11: Direct subscription of UPF event from NEF/trusted AF or NWDAF

### 6.11.1. Description

This solution addresses the case the NF service consumer of the UPF event exposure is NEF or trusted AF.

In this solution, the untrusted AF with SLA via NEF or trusted AF within the same 5GC domain directly can subscribe UPF exposure events in following cases:

- The solution is applicable if data collection from UPF if for one or more of these events:

- UserDataUsageMeasures,

- UserDataUsageTrends, (and/or applicable new events in the future subscribed using SBI to UPF).

- The solution extends the list of targets which allow direct subscription and filters. Those can be:

- Any UE or list of UEs (SUPIs, GPSIs or UE IP addresses).

The UE IP addresses are used for selecting the UPFs to subscribe to and by UPF for filtering the event reports. The consumer can identify the UPF for a UE IP address using NRF with existing functionality.

The SUPIs and GPSIs are used by UPF for filtering the event reports, not for selecting the serving UPFs to subscribe to. The NF consumer provides the full list of SUPIs/GPSIs to the UPFs subscribed to, and the UPFs targets those GPSIs/SUPIs it serves, i.e. the UPF can store subscriptions for SUPIs and GPSIs and activate the reporing when/if a corresponding PDU Session is established.

NOTE 1: In a deployment where UPF reporting filtered per SUPI and/or GPSI is expected, the SMF should provide UPF with the necessary information over N4. If the SMF is not configured to provide UPF with this information, then such UPF reporting filtering is not possible.

NOTE 2: In the case of subscription for a list of SUPIs/GPSIs, whether it is more optimal to subscribe via SMF or directly to UPF depends on the size of the SUPI/GPSI range and the number of UPFs.

* Application ID(s).

It is unclear why a subscription needs to be sent via SMF when application Id is included. UPF may report for the PDU Sessions where traffic of this application is identified.

* DNN(s) and S-NSSAI(s) (like is baseline)

Based on above the NEF or trusted AF may directly subscribe to the UPF event exposure service and optionally providing the requested UPF events data collection time period, to enhance UPF data collection subscription procedures.

NWDAF could also benefit of these enhancements.

### 6.11.2 Procedures

#### 6.11.2.1 Direct subscription of UPF Event Exposure service from NEF/trusted AF



Figure 6.11.2.1-1: Direct subscription of UPF event exposure from NEF or trusted AF

1. The untrusted AF with SLA between the ASP and the operator, invokes the Nnef\_EventExposure\_Subscribe service operation for the applicable events and applied targets to request UPF event exposure e.g. traffic volume, UL/DL data rate with any UE or list of UEs SUPIs, GPSIs or IP addresses, Application ID(s), DNN(s) and/or S-NSSAI(s) as the UPF detected monitoring events as defined in clause 4.15.3.1 of TS 23.502 [3] and may include requested reporting information.

2a/2b. The NEF / trusted AF invokes the Nnrf\_NFDiscovery service operation to discover the serving UPF(s) supporting the requested UPF event exposure service and filters. 3(a/b)/4. Upon receiving the discovered UPF(s) from the NRF, the NEF / trusted AF invokes the Nupf\_EventExposure Subscribe service operation with target list of UE SUPIs, GPSIs or IP addresses, Application Id(s), DNN(s) and/or S-NSSAI(s).

5a. If step 3a is used, the UPF notifies the detected UPF events to the subscribed NEF.

5b. Upon receiving the UPF event notification from the UPF, the NEF notifies the subscribed untrusted AF with the UPF events requested in the subscription.

6. If step 4 is used, the UPF notifies the detected UPF events to the subscribed trusted AF.

#### 6.11.2.2 Direct subscription of UPF Event Exposure service from NWDAF



Figure 6.11.2.2-1: Direction subscription of UPF event exposure from NWDAF

Pre-condition as step 0: NWDAF service consumer send Nnwdaf\_AnalyticsInfo\_Request or Nnwdaf\_AnalyticsSubscription\_Subscribe request to the NWDAF, including requested target(s) and optionally AoI.

1. The NWDAF determines whether needs to collect the corresponding data from UPF, e.g., if NWDAF already has the related data collection or other methods to collect data, then needn’t invoke the following data collection steps. If the UPF data needs to be collected, the NWDAF further determine whether the UPF data to be collected indirectly via SMF or directly from UPF. E.g., for QoS Monitoring event data collection for the ongoing specific PDU Session, the indirect UPF data collection via SMF is always needed. While if not required for the ongoing specific UE’s PDU Session and only the target(s) presented in the target period by the serving UPF(s) to be collected, then direct UPF data collection steps can be proceeded as Option 2 from step 3.

2. If the NWDAF determined indirect UPF data collection is needed as Option 1, then same procedure as step 3 – 5 in Figure 4.15.4.5.2-1 in TS 23.502 [3] to be followed.

3. If the NWDAF determined direct UPF data collection is needed as Option 2, the NWDAF invokes Nnrf\_NFDiscovery\_Request message including the target(s) information.

4. the NRF responds with the discovered UPF(s) information.

5. Upon receiving the discovered UPF(s) from the NRF, the NWDAF invokes the Nupf\_EventExposure Subscribe service operation with target list of UE SUPIs, GPSIs or IP addresses, Applicationd Id(s), DNN(s)and/or S-NSSAI(s).

6. The subscribed UPF event(s) is detected meeting the reporting requirement, the UPF notifies the detected UPF events to the subscribed NWDAF.

### 6.11.3 Impacts on services, entities and interfaces

NEF or trusted AF:

- Supports direct subscription of UPF event exposure service for the applicable events with extension of possible requested target(s) and filters.

- Support to invoke Nnrf\_NFDiscovery service operation with requested target(s) to discover the serving UPF(s) for the requested UPF event.

NWDAF:

- Supports direct subscription of UPF event exposure service for the applicable events with extension of possible requested targets and filters.

- Support to invoke Nnrf\_NFDiscovery service operation with requested target(s) to discover the serving UPF(s) for the requested UPF event.

- Support input data collection for UPF exposure enhancement and the related analytics output enhancement,

UPF:

- Supports NEF and trusted AF as service consumer for direct subscription of the applied event exposure services.

- Supports Application Id filter.

- Supports subscriptions to SUPI(s) and GPSI(s) and activates reporting for the PDU session when they are established.

## 6.12 Solution #12: Direct subscription to UPF Event Exposure service via N6

### 6.12.1 Key Issue mapping

This solution is for KI #2.

### 6.12.2 Description

#### 6.12.2.1 General

In this solution direct subscription via N6 to the UPF Event Exposure service by an AF is described. The following related issues are addressed:

- How does the AF request the 5GC to directly subscribe to the UPF Event Exposure service via N6, and how is it authorized to directly subscribe to the UPF Event Exposure service via N6?

- How does the AF discover the properties of the UPF Event Exposure service to subscribe to, like the relevant endpoints, the version(s) of the exposed service, etc.?

- When a subscription request arrives at the UPF from the AF, how does the UPF know that the request is properly authorized by 5GC?

- How does the AF become aware of PSA UPF changes, to change its subscription to the new PSA UPF?

#### 6.12.2.2 Solution Description

If a UPF supports direct subscription via N6 to its Event Exposure service, it advertises this in its NF profile that it registers at the NRF. Dedicated Event Exposure service instances for direct subscription via N6 may be used as these service instances are accessed via N6 and hence exposed. Common Event Exposure service instances for subscription over both control plane and N6 are not excluded. Dedicated Event Exposure service instances for subscription via N6 are flagged accordingly in the UPF NF profile registered at the NRF, i.e. include in the relevant NFService IE an attribute (e.g. boolean) like “N6basedSubscription” with default value meaning "N6 based subscription” is not supported (e.g. boolean value false). Discovery query parameters are enhanced accordingly to support a new query parameter “n6-based-subscription” to discover UPF Event Exposure service instances that support (or do not support) N6 based subscription. This way the dedicated Event Exposure service instances for subscription via N6 may not even be discovered for subscription over the control plane, and vice-versa. If common Event Exposure service instances for subscription over both control plane and N6 are used, then these service instances in the UPF NF profile support registering different endpoints/parameters for N6 based subscription (vs. subscription via the control plane/5GC NFs). The endpoints exposed for subscription over the N6 are flagged accordingly.

The AF either leverages the Nnef\_AFsessionWithQoS procedure properly extended if subscription to the UPF Event Exposure service is for QoS Monitoring of a UE’s PDU Session or a new NEF service if subscription to the UPF Event Exposure service is for any new event for a specific UE’s PDU Session. The following description focuses on direct subscription to the UPF Event Exposure service for QoS Monitoring of a UE’s PDU Session. The AF requests the possibility and authorization to describe directly to the PSA UPF Event Exposure service. NEF/PCF proceeds with authorization of the AF request. NEF/PCF identifies the SMF serving the relevant PDU Session. SMF exposes a new Event: “PSA UPF change”. Among other things subscription to the new event notifies the UPF ID of the PSA UPF serving a PDU Session. NEF/PCF subscribes to the SMF “PSA UPF change” event and gets the UPF ID of the PSA UPF serving a PDU Session. NEF/PCF retrieves the UPF NF profile of the PSA UPF serving the PDU Session from the NRF and checks if it supports direct subscription via N6. If this is the case NEF/PCF returns to the AF the properties of the UPF Event Exposure service that can be used for subscription via N6 (N6 endpoints, version, http scheme, etc.). It also returns an access token to be used by the AF when subscribing directly to the UPF Event Exposure service via N6. The contents of the access token are specified in 3GPP TS 29.510 and include among other attributes the consumer, producer identities and the scope (the name of the services and the resource/operation-level scopes for which the access token is authorized for use). NEF also informs the UPF via the SMF for the access token issued and its consumer, together with subscription information related to the UPF event. Configured policies in the UPF might be activated based on the input from the NEF. The AF leverages the information provided by NEF/PCF and subscribes directly to the UPF Event Exposure service via the N6 interface providing a description of the data flows to be monitored in the direct subscription to the UPF. The UPF checks the authorization token and if it is OK accepts the AF request. Clause 6.7.3 of 3GPP TS 29.500 specifies how UPF validates a provided access token in a request.

NOTE: It is up to SA3 to decide if an authorization token is mandatory for the UPF to verify that the AF request via N6 is already authorized by 5GC or any other mechanism applies.

UPF still needs to identify the relevant QFIs for which monitoring is requested. For this purpose, SMF/PCF exposes a new operation which maps QoS parameters/References to the relevant QFI or NEF propagates QoS parameters/References to PCF, SMF and the SMF provides the QoS parameters/References together with the QFI of the QoS flows to the UPF. The AF also provides the notification endpoint(s) for receiving notifications from the PSA UPF.

The PSA UPF of a PDU Session may change for many reasons. To cope with PSA UPF changes SMF/NEF support a new Event: “PSA UPF change”. AF subscribes to the NEF event. The subscription may be explicit, or implicit e.g. when the AF requests the possibility to subscribe directly to the UPF Event Exposure service. NEF subscribes to the SMF event above. The subscription may be explicit, or implicit e.g. when the NEF requests to subscribe to the SMF via any new/existing event in which the UPF ID is provided. Upon PSA UPF change, notifications are sent including the properties of the UPF Event Exposure service via N6 of the new PSA UPF. Upon receiving a notification of a PSA UPF change the AF subscribes to the new PSA UPF via N6 and unsubscribes from the previous PSA UPF.

Editor’s note: It is up to SA3 to evaluate the risk of exposing control plane information (e.g. N6 routing information) of the UPF to untrusted AF.

### 6.12.3 Procedures



Figure 6.12.3-1: Setting up an AF session with required QoS procedure with request for direct subscription via N6 to the UPF Event Exposure service

The AF session with required QoS procedure described in TS 23.502 clause 4.15.6.6 is leveraged with the following extensions:

1. The AF includes in the Nnef\_AFsessionWithQoS\_Create/Update request message its request for direct subscription via N6 to the UPF Event Exposure service for QoS Monitoring.

2. Authorization includes authorization for direct subscription via N6 to the UPF Event Exposure service.

5. The response to the AF includes the properties of the UPF Event Exposure service via N6 (e.g. addressing information, http scheme, etc.) and also includes an authorization token to be used by the AF when directly subscribing to the UPF Event Exposure service via N6.

Between steps 1 and 5 of Fig. 6.12.3-1 the following functionalities are executed (in parallel to steps 3, 3a, 3b, 4, 4a, 4b):



Figure 6.12.3-2: Authorizing direct subscription via N6 to the UPF Event Exposure service and providing the properties of the relevant UPF Event Exposure service to the AF

1. NEF after receiving the AF request authorizes the AF request including authorizing (or not) the extra requirement to directly subscribe via N6 to the UPF Event Exposure service.

2. NEF determines the SMF serving the UE/PDU Session.

3. (3a.) NEF subscribes to Nsmf\_EventExposure Service which supports a new event: “PSA UPF change” with input the PDU Session ID of the PDU Session for which QoS monitoring is needed. (3b.) Upon successful subscription SMF returns to the NEF the UPF ID of the current PSA UPF and further notifies the NEF when a PSA UPF change occurs.

4. (4a. and 4b.) NEF retrieves the UPF NF profile of the PSA UPF with the UPF ID and determines if it supports direct subscription via N6 to its Event Exposure service.

5. If this is the case, (5a. and 5b.) NEF requests an authorization token from the NRF, on behalf of the AF, to be used for direct subscription to the UPF Event Exposure service via N6.

6. NEF returns response “5” to AF with the new required information.

As shown in Figure 6.12.3-2, the AF with the information provided by the NEF, directly subscribes to the UPF via N6 by sending a UPF Event Exposure subscribe request (HTTP request like defined in TS 29.564) to the N6 routable IP address of the UPF Event Exposure service. The AF provides a description of the data flows to be monitored in the direct subscription to the UPF and the authorization token provided by the NEF. The UPF checks the authorization token and accepts the request accordingly. The UPF responds to the AF with the status of the service after it has enabled the service or if service initiation failed.



Figure 6.12.3-2: Subscription creation (direct)

Once the subscribed service has been enabled in the UPF and acknowledged to the AF, the UPF starts sending notification reports about subscribed events, according to the service parameters and policies, directly to the AF via N6, as is shown in Figure 6.12.3-3.



Figure 6.12.3-3: UPF sends notification on subscribed events

A PSA UPF change triggers the following procedure:



Figure 6.12.3-4: PSA UPF change and subscription update.

1. SMF notifies the NEF of a PSA UPF change for a PDU Session and provides to the NEF the new PSA UPF (UPF-2) ID.

2. Steps 2, 2a, 2b, 3a, 3b are similar to steps 4, 4a, 4b, 5a, 5b in Fig. 6.12.3-2.

4. NEF sends PSA UPF change notification to the AF and the properties of the UPF Event Exposure service of the new PSA UPF (UPF-2), together with an authorization token.

5. AF unsubscribes from UPF-1.

6. AF subscribes to UPF-2.

### 6.12.4 Impacts on services, entities and interfaces

**AF:**

- Supports direct subscription via N6 to the UPF Event Exposure service for QoS Monitoring of a UE’s PDU Session,

- Supports proper security mechanism, e.g. providing an authorization token in the subscription request.

- Supports “PSA UPF change” via receiving relevant notification(s) and unsubscribing from the old PSA UPF and subscribing to the new PSA UPF.

**NEF (PCF):**

- Supports authorization of direct subscription via N6 to the UPF Event Exposure service for QoS Monitoring of a UE’s PDU Session and provisioning of proper information for the direct subscription to the AF. NEF supports a new exposure event “PSA UPF change” to notify the AF of PSA UPF changes.

**SMF:**

- Supports a new exposure event “PSA UPF change” to notify NEF of PSA UPF changes. SMF also supports linkage of QoS parameters/References to QFIs.

**UPF:**

- Supports direct subscription via N6 to its Event Exposure service.

**NRF:**

- Supports extensions for registering and discovering dedicated UPF Event Exposure service instances for direct subscription via N6.

**RAN/UE:**

- None.

## 6.13 Solution #13: UPF Discovery and Direct Subscription to UPF for AF

### 6.13.1 Description

When an AF needs to subscribe to UPF event exposure service, the current Rel-18 procedure as described in clause 4.15.3.2.3 of TS 23.502 [2] is as follows.

- AF (who knows the UE’s GPSI) requests Nnef\_EventExposure service to NEF

- NEF sends the request Nudm\_EventExposure to UDM

- UDM finds the serving SMF corresponding to the request from NEF, and invokes Nsmf\_EventExposure to UPF

- SMF then finally sends Nupf\_EventExposure Subscribe message to relevant UPF

Furthermore, if the AF is unaware of UE’s GPSI, it needs to query using UE’s IP address, which further requires many additional steps. Also, each of the entities involved in the Event Exposure subscription call flow need to store the context of the relevant subscription, thus optimizations are needed in order to efficiently find the serving UPF for the corresponding target application flow for the AF.

AF can utilize the already established user plane between the UE and the application server (which is controlled by the same authority as the AF) to find the serving UPF for the corresponding session.

AF and operator need to have some service agreement in order for the UPF to detect particular header/protocol in the user plane packets of the UE’s application flow that contain information related to subscribing the serving UPF by AF. AF may provide its AF ID, along with notification address, Event IDs etc. in order to subscribe for particular UPF event exposure service. UPF may check its configured information to see if the AF request is valid and the AF is authorized or not in order to subscribe for UPF event exposure service.

Once the packet with relevant Header/tag is detected for a UE’s application flow, corresponding AF (which had service agreement with the operator) can be notified of the UPF’s address and optionally particular UE’s private address in order for the AF to directly subscribe for the UPF event exposure service via NEF.

This solution provides procedure to efficiently discovering the serving UPF for an Application flow and direct subscription by AF to UPF event exposure services without having to expose the UPF’s N6 routing information.

### 6.13.2 Procedures

#### 6.13.2.1 General call flow



Figure 6.13.2-1 General call flow

1. UPF/SMF/PCF are pre-configured by the AF to detect certain headers/protocol type in user plane.

NOTE: The policy/configuration may be stored for Any UE, and may require the use of some aspects of Solution#1. In addition to just detecting the header/tag UPF may also be configured to detect and process the content of the payload of the packet containing the relevant header/tag.

2. UE and the application server (same authority of the AF) have an established application flow between them.

3. The AF decides to subscribe UPF event exposure service for the particular UE.

4. AF (via the application server) sends user plane packet to UE with specific header/tag information

The headers (or the contents in payload) may indicate to UPF information related to AF ID, notification address etc.

5. Based on the UPF configuration (in Step 1), UPF detects the specific header/tag related to UPF discovery present in UE’s flow.

Editor's Note:: The exact format of header/ information in packet is to be determined by Stage-3.

Case A: If the configured action of the UPF (configuration done in Step 1) in case the header/tag is detected, is to notify the AF regarding serving UPF ID, Steps 6a, 7a, 8a are performed. UPF’s action may be to further drop the packet and notify the header/tag detected to SMF.

Case B: Else if configured action of the UPF (configuration done in Step 1) is to implicitly subscribe to AF event exposure, UPF proceeds with Step 6b. UPF’s action may be to further drop the packet, and notify the content of the packet, along with header/tag detected to SMF.

6a. UPF based on the header information in Step 5, notifies the AF of the UPF ID. This can be done using the principles of notification of header/tag handling events as specifies in Solution#1.

7a. AF to NEF: AF after knowing the serving UPF ID, subscribes via NEF for UPF event exposure. The request includes relevant Event IDs, Event Filters etc.

8a. If not already present in NEF, NEF receives the UPF profile from NRF for the UPF indicated by serving UPF ID, and directly subscribes for the UPF event exposure service for the relevant event, without the need for performing serving UPF discovery

6b. UPF and other NFs behaviour in Step 6b is described in detail in clause 6.13.2.3

#### 6.13.2.2 UPF discovery by utilizing Header information and Subscription via CP

This clause describes the details of case A as mentioned in clause 6.13.2.1. This case is an extension to the contents of the report that are notified to AF upon a header/tag detection.

Suppose in Step 1, UPF is configured to detect header X in UE’s data traffic. UPF action may be further defined to drop the packet/process the packet contents instead of forwarding it to UE

Now the application flow is assumed to be established between UE and Application server. Application server sends a user plane packet with the Header/Tag X. Once the UPF detects that packet, based on it’s configured action, the notification report sent to AF as done in Solution#1 is extended to include UPF ID (or some other reference ID) of the serving UPF.

This notification can be done via control plane as done in Solution#1

- UPF sends the N4 session report to SMF, SMF notifies the NEF about the header detection including information of the serving UPF, and NEF notifies the AF the serving UPF information for the AF session.

- Or UPF uses Nupf\_EventExposure Notify to inform serving UPF information (i.e. its own UPF ID etc.) to AF.

Editor's Note: the security implication of exposing 5GC internal information without proper authorization is to be evaluated by SA3

Second option is to perform this notification by inserting relevant header/tag information in user plane traffic and including information related to UPF in the contents, i.e. the configured action of UPF in Step 1 would be to detect Header/Tag X info and insert Header/Tag Y info.

Editor's Note: the security implication of exposing 5GC internal information without proper authorization is to be evaluated by SA3

Once the AF gets the information of the serving UPF for the AF session, it subscribes to UPF event exposure service, by including the received UPF ID in the Nnef request along with the relevant Event ID (s) that the AF wants to subscribe to. NEF can then directly subscribe to UPF (identified by the UPF ID) for event exposure. In case AF is internal, AF directly subscribes to UPF (without NEF).

NOTE: NEF/AF may first need to fetch NF profile of the UPF identified by UPF ID, to check whether the UPF supports relevant Event ID(s).

#### 6.13.2.3 UPF Discovery and subscription by utilizing Header information

This clause describes the details of case B as mentioned in clause 6.13.2.1.

For this case, instead of AF being notified about the serving UPF, AF is implicitly subscribed to UPF event exposure when the particular header/tag is detected in UE’s application traffic.

AF may include the relevant information (e.g. Event ID, notification target etc.) as the payload contents of the packet, or particular header/tag may implicitly map to particular info (e.g. Header X = 01 maps to Subscribe, Header X = 02 maps to Unsubscribe) based on SLA between AF and operator.

In case the AF request for Event subscription needs to be authorized, AF may further include Authenticate token in the packet contents and UPF may contact the NEF which can perform authorization of AF request.

NOTE: It is assumed that AF have obtained an authorization token beforehand from the NEF and included it in the contents of packet. In case AF is internal, this task may be done by NRF as done when a general consumer NF subscribes for event exposure services.

In case the authorization of relevant Event needs to be coordinated by other NFs (e.g. PCF), that NF may just be notified about the header/tag detection and subscribe to the UPF on behalf of the AF.

Example call flow is shown in Figure 6.13.2.3-1



Figure 6.13.2.3-1 UPF Discovery and subscription by utilizing Header information

As described in the above figure in addition to the SLA between AF and operator before for Header/tag handling, the AF also receives an “generic” authentication token from the NEF before hand for UPF event exposure subscription via User plane. AF can include this authentication token, along with the specific header/tag in the UE application flow in order to subscribe directly for UPF event exposure services. It is assumed that NRF can generate this “generic token”.

UPF and SMF actions are configured to handle the contents of the packet when a particular Header/Tag is detected.

Upon detection of the specific header/tag, UPF provides the contents of the packet to the SMF which include Authentication tok. SMF verifies whether authentication token. SMF does this by sending the token to NEF which verifies it and sends the verification result to NEF.

After the NEF has performed the verification it provides the result to SMF. SMF, based on the detected header/tag and/or information conveyed by the Authentication token, determines to subscribe UPF for the Event(s) for Nupf event subscription (in case UPF supports the relevant Event ID(s)).

NOTE: SMF may be configured (e.g. based on SLA) with a mapping between the Authentication token info and/or header/tags to relevant Event ID (s) that need to be subscribed for UPF event exposure.

Editor's Note: Details related to authentication token check and header/tag handling will be done by SA3 and Stage-3.

Editor's Note: the security implication of the generic token for all UPFs is to be evaluated by SA3

### 6.13.3 Impacts on services, entities and interfaces

For Case A

UPF impacts

- Detection of specific header/tag pertaining to AF request in UE’s user plane packets.

- Notifying the UPF ID/UPF information to the AF either via N6 or via control plane.

NEF impacts

- Directly subscribing to particular UPF for event exposure based on AF’s request for UPF event Exposure which include information of the serving UPF

For Case B

UPF impacts

- Detection of specific header pertaining to AF request in UE’s user plane packets.

- Providing authentication token received from the AF (inside the user plane packet with specific header/tags) to SMF.

NEF impacts

- Providing Authentication token to AFs for Direct Subscription of UPF event exposure services.

- Verifying the Authentication token for Direct subscription to AF, as received from SMF.

SMF impacts

- Requesting NEF to verify Authentication token received from UPF.

- Subscribing to UPF Event Exposure services based on Header/Tag detected and/or authentication token.

# 7 Overall Evaluation

Editor's Note: This clause will provide a general evaluation and comparison of the solutions per Key Issue #<X>

# 8 Conclusions

Editor's Note: This clause will capture conclusions for the study..

## 8.1 Interim Conclusions for Key Issue #1: Selection of UPF providing a selected user plane functionality

The following aspects are concluded as principles for normative work:

- Reusing procedures in clause 4.17.1 and clause 4.17.2 of TS 23.502 [3] to support registering the extended UPF functionalities in NRF.

- The following UPF functionalities are added in UPF profile stored in NRF:

- The functionality of NAT information exposure;

- Packet Inspection functionality (to differentiate between IP or MAC filter based packet detection, and the packet detection based on other means, e.g. layer 7 DPI);

- Defining operator configurable parameter in the N4 capabilities and UPF NF profile which can be used for non-standard or partially supported features and configured by operator to extend the baseline UPF capabilities. The format of the parameter is to be determined by stage 3.

- for example, the operator may configure values for this parameter to represent customized configuration (e.g, hardware accelerators (for example GPU, DPU etc.), Firewall, DDos Protection, etc.)

Editor’s NOTE: It is FFS whether the SMF selection logic of UPF can be based on subscription/and or policy information.

Annex <X> (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-01 | SA2#160AH-e |  |  |  |  | Implemented agreed CRs at SA2#160AHE – S2-2401109, S2-2401110, S2-2401199, S2-2401615, S2-24011616, S2-2401617 | 0.1.0 |
| 2024-02 | SA2#161 |  |  |  |  | Implemented agreed CRs at SA2#161 – S2-2403022, S2-2403437, S2-2403438, S2-2403439, S2-2403441, S2-2403442, S2-2403738, S2-2403739 | 0.2.0 |
| 2024-04 | SA2#162 |  |  |  |  | Implemented agreed CRs at SA2#162 – S2-2405159, S2-2405163, S2-2405400, S2-2405401, S2-2405687, S2-2405688, S2-2405689, S2-2405690 | 0.2.0 |