|  |
| --- |
| 3GPP TR 23.700-63 V0.2.0 (2024-02) |
| 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 address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://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 members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® 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 leveraging Nnef\_TrafficInfluence\_Notify 12

6.1.3 Impacts on services, entities and interfaces 13

6.2 Solution #2: UPF provision and selection based on new UPF functionality 13

6.2.1 Key Issue mapping 13

6.2.2 Description 14

6.2.3 Procedures 14

6.2.4 Impacts on services, entities and interfaces 14

6.3 Solution #3: Selection on UPF with extended user plane capabilities 15

6.3.1 Description 15

6.3.1.1 Solution Description 15

6.3.2 Procedures 15

6.3.3 Impacts on existing nodes and functionality 18

6.4 Solution #4: Selection of UPF providing specific user plane functionalities 18

6.4.1 Key Issue mapping 18

6.4.2 Description 18

6.4.3 Procedures 20

6.4.4 Impacts on services, entities and interfaces 21

6.5 Solution #5: Direct subscription of UPF event exposure service for TSC management 21

6.5.1 Description 21

6.5.2 Procedures 21

6.5.2.1 Direct subscription of UPF Event Exposure service for TSC management 21

6.5.3 Impacts on services, entities and interfaces 22

6.6 Solution #6: UPF selection based on the status of the supported functionalities 22

6.6.1 Key Issue mapping 22

6.6.2 Description 23

6.6.3 Procedures 23

6.6.4 Impacts on services, entities and interfaces 24

6.7 Solution #7: Translating SUPI/GPSI to NATed IP address 24

6.7.1 Description 24

6. 7.1.1 Background and problem description 24

6.7.1.2 High level description 25

6.7.2 Procedures 25

6.7.2.1 Procedure 25

6.7.2.2 Service definition 26

6.7.2.2.1 Nupf\_GetPublicIPaddressAndPort 26

6.7.3 Impacts on services, entities and interfaces 26

7 Overall Evaluation 26

8 Conclusions 27

Annex <X> (informative): Change history 28

# 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".

# 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 |  |
|  |  |  |  |

## 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.

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:

- Identifier

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

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

- Reporting conditions: Threshold based, periodical with the relevant threshold values and periodicity;

- Reporting content e.g. header/tag “x” detected, header/tag “a” is replaced by header/tag “b”, header/tag “c” is added, etc.

- Information relevant to parties in SLA

The information relevant to the parties in the SLA is handled as metadata and is assumed as pre-agreed information between the parties to include header/tags related 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 actual rule(s) is(are) provided in the relevat Nnef\_TrafficInfluence operation (create/update/delete) by the AF, together with the direction for handling, i.e. uplink, downlink. As opposed to influencing on routing or SFC, in this case 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). In step#2, NEF confirms the AF is authorised to use this rule based on local configuration, and then will store/update the received data in the UDR for data set pointing to application data.

At notification from UDR, PCF verifies the content of the metadata as the pre-agreed information between the parties and transforms it in the relevant information to be inserted/detected (e.g. header/tag, protocol layer, etc), including in addition the rule contents together with the direction of handling, in the PCC rule. If the AF requests reporting on header/tag detection, the PCF includes in the PCC rule(s) the information required for reporting the event.

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.

In step#6, SMF installs PDR/FAR and URR (if reporting required) rules using N4 procedures into the UPF.

Editor’s Note: Whether header handling exposure is part of Nnef\_TrafficInfluence or another service (e.g. a new service) is FFS

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

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.

In case the detection action is not associated with any insertion/removal/modification/replacement, 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)**

Upon detection of the header/tag requested by the AF, the N4 Session Report with “Start of Traffic (usage report)” is assumed to be used by UPF. This usage report shall include the information related to the header/tag that has been detected.

If the detection action is associated with an insertion/removal, modification or replacement, the N4 Session report with “Start of Traffic (usage report)” is proposed to be used as well by the UPF. The usage report shall include instead information about the header/tag detected and the action performed on it.

Editor’s Note: Whether to use Start of Traffic (usage report) or a new parameter is FFS

The following sequence from TS 23.502 clauses 4.3.6.3 to apply for this solution upon notification from the UPF:



**Figure 6.1.2.2-2 Notification from UPF(TS** **23.502 [3] clause** **4.3.6.3)**

Editor’s Note: What parameters are to be used in Nsmf\_EventExposure for header/tag handling is FFS

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

NOTE: Reporting detection of a header for Any UE or for some popular applications can cause UPF to issue lots of reports and consequently high signaling load. Requesting reporting of a header/tag detection in UEs traffic needs to be considered with care.

### 6.1.3 Impacts on services, entities and interfaces

- NEF

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

- UDR

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

- PCF

- PCC rule to add a header tag identifier and metadata

- SMF

- 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

- UPF

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

## 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 6.6.3-1 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.

# 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..

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 |