|  |  |
| --- | --- |
| 3GPP TR 23.700-62 V1.1.0 (2022-10) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on UPF enhancement for Exposure and SBA  (Release 18) | |
|  | |
|  |  |
|  | |
| 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.  © 2022, 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 6

1 Scope 8

2 References 8

3 Definitions of terms, symbols and abbreviations 9

3.1 Terms 9

3.2 Symbols 9

3.3 Abbreviations 9

4 Architectural Assumptions and Requirements 9

4.1 Architectural Assumptions 9

4.2 Architectural Requirements 9

5 Key Issues 10

5.1 Key Issue #1: Study UPF event exposure service registration and discovery 10

5.1.1 Description 10

5.2 Key Issue #2: Support UPF expose information to other NFs 10

5.2.1 General description 10

6 Solutions 11

6.0 Mapping of Solutions to Key Issues 11

6.1 Solution #1: UPF event exposure service framework enhancements to support registration, deregistration and discovery via NRF 11

6.1.1 Description 11

6.1.2 Procedures 12

6.1.3 Impacts on services, entities and interfaces 20

6.2 Solution #2: <UPF event exposure service for TSC management> 21

6.2.1 Key Issue mapping 21

6.2.2 Description 21

6.2.3 Procedures 21

6.2.4 Impacts on services, entities and interfaces 25

6.3 Solution #3: using the proper subscription mechanism depending on the event targeted by the UPF event consumer 26

6.3.1 Key Issue mapping 26

6.3.2 Description 26

6.3.3 Procedures 28

6.3.4 selection of the proper UPF within the UPF(s) that serve a PDU Session 28

6.3.5 Impacts on services, entities and interfaces 28

6.4 Solution #4: upgrading N4 to pass necessary event filtering information to the UPF 29

6.4.1 Key Issue mapping 29

6.4.2 Description 29

6.4.3 Procedures 29

6.4.4 Impacts on services, entities and interfaces 30

6.5 Solution #5: registering UPF(s) serving a PDU session at UDM 30

6.5.1 Key Issue mapping 30

6.5.2 Description 30

6.5.3 Procedures 31

6.5.4 Impacts on services, entities and interfaces 32

6.6 Solution #6: Determining the UPF(s) that serve a UE address 32

6.6.1 Key Issue mapping 32

6.6.2 Description 32

6.6.3 Procedures 33

6.6.4 Impacts on services, entities and interfaces 33

6.7 Solution #7: Support to existing (Rel‑16-Rel‑17) data analytics with PDU Session Data Usage Events 34

6.7.1 Key Issue mapping 34

6.7.2 Description 34

6.7.3 Procedures 35

6.7.4 Impacts on services, entities and interfaces 38

6.8 Solution #8: Support to existing (Rel‑16-Rel‑17) data analytics with QoS Flow level measurements 39

6.8.1 Key Issue mapping 39

6.8.2 Description 39

6.8.3 Procedures 40

6.8.4 Impacts on services, entities and interfaces 42

6.9 Solution #9 to Key Issue 2: NWDAF collects information from UPF by event exposure 43

6.9.1 Mapping table between Analytics ID and the related information collection in UPF 43

6.9.2 Service based UPF event exposure 44

6.9.3 Procedure 46

6.9.4 Impacts on services, entities and interfaces 49

6.10 Solution #10: UPF event exposure service to NWDAF 50

6.10.1 Key Issue mapping 50

6.10.2 Description 50

6.10.3 Procedures 50

6.10.4 Impacts on services, entities and interfaces 52

6.11 Solution #11: UPF event exposure service to NWDAF subscribed directly from UPF 52

6.11.1 Key Issue mapping 52

6.11.2 Description 52

6.11.3 Procedures 52

6.11.4 Impacts on services, entities and interfaces 53

6.12 Solution #12: UPF registration to the NRF and NWDAF collecting data from UPF 54

6.12.1 Key Issue mapping 54

6.12.2 Description 54

6.12.3 Procedures 54

6.12.4 Impacts on services, entities and interfaces 55

6.13 Solution #13: Subscription to UPF Event Exposure Services in the event of UP Path change 56

6.13.1 Key Issue mapping 56

6.13.2 Description 56

6.13.3 Procedures 56

6.13.4 Impacts on services, entities and interfaces 57

6.14 Solution #14: Reduce the UPF performance impacts due to data reporting to NF consumer 57

6.14.1 Key Issue mapping 57

6.14.2 Description 57

6.14.3 Procedures 58

6.14.4 Impacts on services, entities and interfaces 58

6.15 Solution #15: Subscription of UPF Event Exposure Service 58

6.15.1 Key Issue mapping 58

6.15.2 Description 59

6.15.3 Procedures 59

6.15.4 Impacts on services, entities and interfaces 60

6.16 Solution #16: Direct/indirect subscription of the UPF event exposure service 60

6.16.1 Key Issue mapping 60

6.16.2 Description 60

6.16.3 Procedures 61

6.16.4 Impacts on services, entities and interfaces 63

6.17 Solution #17: Update/Release subscription of the UPF event exposure service 63

6.17.1 Key Issue mapping 63

6.17.2 Description 63

6.17.3 Procedures 63

6.17.4 Impacts on services, entities and interfaces 65

6.18 Solution #18: QoS parameters exposure by UPF 66

6.18.1 Key Issue mapping 66

6.18.2 Description 66

6.18.3 Procedures 66

6.18.4 Impacts on services, entities and interfaces 67

6.19 Solution #19: QoS Monitoring results exposure by UPF 67

6.19.1 Key Issue mapping 67

6.19.2 Description 67

6.19.3 Procedures 67

6.19.4 Impacts on services, entities and interfaces 69

6.20 Solution #20: UE IP address mapping information exposure by UPF 69

6.20.1 Key Issue mapping 69

6.20.2 Description 69

6.20.3 Procedures 70

6.20.4 Impacts on services, entities and interfaces 71

6.21 Solution #21: UPF Event Exposure with consideration on UPF performance 71

6.21.1 Key Issue mapping 71

6.21.2 Description 71

6.21.3 Procedures 72

6.21.4 Impacts on services, entities and interfaces 72

6.22 Solution #22: Support UPF event exposure service subscription update in case of UPF/SMF change 72

6.22.1 Key Issue mapping 72

6.22.2 Description 72

6.22.3 Procedures 73

6.22.4 Impacts on services, entities and interfaces 75

7 Overall Evaluation 75

7.1 Overall Evaluation of solutions for Key Issue #1 75

7.2 Evaluation for KI#2 76

8 Conclusions 79

8.1 Conclusions for Key Issue #1 79

8.2 Conclusions for KI#2 79

# 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 studies on key issue description, solution and conclusion on the support of better integration of UPF into the 5GC SBA. The objectives include:

- Study UPF event exposure service(s) registration/deregistration, and discovery via the NRF.

- Study UPF event exposure service(s) that would support, e.g.:

- Consumption of UPF exposure services by the PCF, NWDAF, CHF, NEF, Trusted AF and other NFs (if needed).

- (To support the UPF exposure service, if needed) Use of SMF services, PCF services, NWDAF services, CHF services, NEF services, Trusted AF services by the UPF.

NOTE 1: This will not define solutions where UPF exposes information that it is not originator of, i.e. not re-expose information owned and exposed by other NFs.

- Relevant Event IDs.

- Evaluate usage of UPF event exposure service(s) as defined in WT#2 also considering the architectural impacts.

NOTE 2: SMF is responsible for controlling UPF packet processing.

NOTE 3: The performance of UP traffic handling shall not be degraded due to mechanisms defined in this study.

NOTE 4: The study shall address generic UPF data exposure mechanisms via SBA based mechanisms, and the coordination with other SIDs for this aspect may be needed in study phase.

This study shall maintain the Rel‑17 backward compatibility on the N3, N6, N9, N4 interfaces.

# 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: "Policy and charging control framework for the 5G System (5GS); Stage 2".

[5] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[6] 3GPP TS 29.510: "Network Function Repository Services; Stage 3".

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

[8] 3GPP TS 29.244: "Interface between the Control Plane and the User Plane nodes".

[9] 3GPP TS 29.514: "5G System; Policy Authorization Service; Stage 3".

[10] 3GPP TR 23.700-48: "5G System Enhancements for Edge Computing".

[11] 3GPP TS 24.519: " Time-Sensitive Networking (TSN) Application Function (AF) to Device-Side TSN Translator (DS-TT) and Network-Side TSN Translator (NW-TT) protocol aspects, Stage 3".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 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 TR 21.905 [1].

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

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 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 the present study:

- The SMF is responsible for controlling UPF packet processing.

- The UPF can only expose 5GC information which is originated in the UPF.

## 4.2 Architectural Requirements

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

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

- The Rel‑18 N6, N4 interface shall be based on the existing interface design and backward compatible. No impact is introduced on N3, N9 interfaces from this study.

NOTE: This study is limited to event exposure, and thus interfaces can only be impacted due to this study.

- The usage of direct UPF event exposure for exposure of some data when these data are already available via usage of SMF + N4 needs to be justified.

- Some aspects as following should be considered when the solution evaluation is proposed:

- The co-existence for the UPF supporting UPEAS feature and UPF supporting Rel‑17 (i.e. not supporting the feature) should be considered.

# 5 Key Issues

## 5.1 Key Issue #1: Study UPF event exposure service registration and discovery

### 5.1.1 Description

This KI maps to the WT1 of the SID.

The KI will study the registration and discovery of UPF event exposure service(s). The following aspects should be studied:

- How to support UPF event exposure service(s) registration/deregistration on NRF, and what parameters to be registered in the NF profile of UPF.

- How to support UPF service discovery via the NRF, and what parameters that can be used for discovery.

- How to support UPF selection for a UPF event exposure service request targeting a specific UE or a specific PDU session.

This key issue is not meant to define for which UPF event / exposed information a direct consumer subscription to the UPF would take place (if any).

NOTE: The information to be registered to the NRF is related to the UPF event exposure service requirement.

## 5.2 Key Issue #2: Support UPF expose information to other NFs

### 5.2.1 General description

To enable flexible communication between UPF and other 5GC NFs, the UPF can expose network information to NFs through UPF event exposure service.

In Release 17, TS 23.548 [7] has supported that UPF can expose QoS monitoring results to local NEF. In Release 18, we need further study whether UPF can also expose other useful information to other NFs to optimize the network performance.

The key issue is to identify use cases for UPF event exposure (including the related Event Id) and for each use case determine whether the consumer directly contacts the UPF for its subscription or whether the consumer goes via an intermediate function like the SMF.

The following aspects should be studied to support UPF event exposure service(s):

- How and what specific information the UPF can expose to NWDAF so NWDAF can provide existing (Rel‑16, Rel‑17) data analytics as specified in TS 23.288 [5]. Support of New Rel‑18 data analytics per the Rel‑18 FS\_eNA\_Ph3 may also be considered in alignment with that study

- How and what specific information the UPF can expose to NEF/Local NEF/trusted AF, e.g. the information which can be exposed in Rel‑18 SA WG2 studies such as FS\_EDGE\_Ph2 and FS\_XRM, or information which has been justified for exposure.

NOTE: The Relevant Event IDs of the UPF event exposure services above can be introduced.

- Whether PCF, CHF, and other NFs need to invoke UPF event exposure service. If yes, how and what specific information the UPF can expose to these NFs.

- Whether the consumer NF directly subscribes the UPF or not. If yes, how to authorize the consumer NF for subscribing to UPF event exposure services via Nupf, and how to update/release the subscription.

# 6 Solutions

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |  |
| --- | --- | --- |
| Solutions |  |  |
|  | <Key Issue #1> | <Key Issue #2> |
| #1: UPF event exposure service framework enhancements to support registration, deregistration and discovery via NRF | X |  |
| #2: UPF event exposure service for TSC management |  | X |
| #3: using the proper subscription mechanism depending on the event targeted by the UPF event consumer |  | X |
| #4: upgrading N4 to pass necessary event filtering information to the UPF |  | X |
| #5: registering UPF(s) serving a PDU session at UDM |  | X |
| #6: Determining the UPF(s) that serve a UE address |  | X |
| #7: Support to existing (Rel‑16-Rel‑17) data analytics with PDU Session Data Usage Events |  | X |
| #8: Support to existing (Rel‑16-Rel‑17) data analytics with QoS Flow level measurements |  | X |
| #9: NWDAF collects information from UPF by event exposure |  | X |
| #10: UPF event exposure service to NWDAF |  | X |
| #11: UPF event exposure service to NWDAF subscribed directly from UPF |  | X |
| #12: UPF registration and NWDAF collecting data from UPF | X | X |
| #13: Subscription to UPF Event Exposure Services in the event of UP Path change |  | X |
| #14: Reduce the UPF performance impacts due to data reporting to NF consumer |  | X |
| #15: Subscription of UPF Event Exposure Service |  | X |
| #16: Direct/indirect subscription of the UPF event exposure service |  | X |
| #17: Update/Release subscription of the UPF event exposure service |  | X |
| #18: QoS parameters exposure by UPF |  | X |
| #19: QoS Monitoring results exposure by UPF |  | X |
| #20: UE IP address mapping information exposure by UPF |  | X |
| #21: UPF Event Exposure with consideration on UPF performance |  | X |
| #22: Support UPF event exposure service subscription update in case of UPF/SMF change |  | X |

## 6.1 Solution #1: UPF event exposure service framework enhancements to support registration, deregistration and discovery via NRF

### 6.1.1 Description

The solution introduces the service based UPF event exposure framework to support registration, deregistration and discovery via NRF. The following Figure 6.1.2-1 depicts the service-based interface Nupf introduced in the 5G system architecture.

The solution for registering UPF in NRF is based on the option in the existing solution described in clause 6.3.3.2 of TS 23.501 [2] and clause 4.17 of TS 23.502 [3], whereby the UPF registers directly with the NRF and hence does not use N4 for registering to NRF.

NOTE 1: As described in TS 23.501 [2], the NRF can alternatively be configured by OAM with information on the available UPF(s) or the UPF instance(s) may register its/their NF profile(s) in the NRF.



Figure 6.1.1-1: 5G system architecture with service based UPF

NOTE 2: Figure 6.1.1-1 shows an example of UPF with Nupf service. In the context of this solution the UPF is in the role of consumer of NRF services, i.e. this solution is about how UPF can register its NF profile in NRF with related Nupf service information and does not describe services provided by the UPF itself.

The solution also addresses UPF selection for a UPF event exposure service request targeting specific UEs and specific PDU sessions.

### 6.1.2 Procedures

#### 6.1.2.1 UPF Event Exposure service Registration

The following Figure 6.1.2.1-1 depicts the UPF Event Exposure service Registration procedure.



Figure 6.1.2.1-1: UPF Event Exposure service Registration procedure

1. The UPF sends the Nnrf\_NFManagement\_NFRegister Request message to NRF to inform the NRF of its NF profile when the NF service consumer becomes operative for the first time. The existing UPF NF profile parameters include e.g. S-NSSAI(s) and the associated NSI ID(s), DNN(s), IP range, information about the location of the UPF (operator specific information, e.g. geographical location, data centre), UPF Service Area (TAI List), DNAI, as described in TS 29.510 [6]. In addition, to support UPF Event Exposure Service, also Event Exposure Service Name, Supported Event ID(s) are provided with the UPF NF profile.

2. The NRF stores the UPF profile and marks the UPF Event Exposure service as available.

3. The NRF acknowledge UPF Registration is accepted via Nnrf\_NFManagement\_NFRegister response.

#### 6.1.2.2 UPF Event Exposure service Update

The following Figure 6.1.2.2-1 depicts the UPF Event Exposure service Update procedure.



Figure 6.1.2.2-1: UPF Event Exposure service Update procedure

1. UPF sends Nnrf\_NFManagement\_NFUpdate Request message (the updated NF profile of NF service consumer) to NRF to inform the NRF of its updated UPF profile.

2. The NRF updates the NF profile of UPF instance.

3. The NRF acknowledge UPF Update is accepted via Nnrf\_NFManagement\_NFUpdate response.

#### 6.1.2.3 UPF Event Exposure service Deregistration

The following Figure 6.1.2.3-1 depicts the UPF Event Exposure service Deregistration procedure.



Figure 6.1.2.3-1: UPF Event Exposure service Deregistration procedure

1. UPF sends Nnrf\_NFManagement\_NFDeregister Request message to NRF to inform the NRF of its unavailability.

2. The NRF marks the UPF unavailable. NRF may remove the NF profile of UPF according to NF management policy.

3. The NRF acknowledge NF Deregistration is accepted via Nnrf\_NFManagement\_NFDeregister response.

#### 6.1.2.4 UPF Event Exposure service Discovery

The following Figure 6.1.2.4-1 depicts the UPF Event Exposure service Discovery procedure.



Figure 6.1.2.4-1: UPF Event Exposure service Discovery procedure

1. Service consumer NF that requires UPF services invokes Nnrf\_NFDiscovery\_Request message to NRF with the intent to discover UPF. The input may include e.g. UPF service name, Event ID(s), TAI, NF type (i.e. UPF), S-NSSAI, DNN, DNAI, as described in TS 29.510 [6].

2. The NRF authorizes the Nnrf\_NFDiscovery\_Request and based on the UPF profile the NRF determines if the service consumer of the UPF is allowed to discover the UPF.

3. If allowed, the NRF determines a set of UPFs matching the input parameters included in the Nnrf\_NFDiscovery\_Request to the service consumer of the UPF via Nnrf\_NFDiscovery\_Request\_Response. The output includes one or more UPF instances, and for each UPF instance it includes UPF NF profile.

#### 6.1.2.5 UPF Selection for a UPF Event Exposure Service Request

##### 6.1.2.5.1 Procedure of UPF selection by the NF targeting PDU session or UE with information of IP address

There are different alternatives to find UPF when the consumer NF targets a specific PDU session or UE with information of IP address.

This solution is applied to discover PSA UPF where only the IP address provided to the UE can be used, i.e. the UE IP address stored in BSF.

Figure 6.1.2.5.1-1 shows one first alternative:



Figure 6.1.2.5.1-1: Procedure of UPF selection by the NF targeting PDU session or UE with information of IP address

1. If the consumer NF is an AF/NEF, it can use the UE IP address to discover the PCF from the BSF. Then the PCF can send response with the SMF for the PDU session to the AF/NEF.

2. The AF/NEF interacts with the SMF that responded by the PCF in step 1 to obtain the appropriate UPF information for PDU Session over the Nsmf\_EventExposure\_Subscribe service operation providing UE IP address and if available IP domain.

NOTE 1: The solution assumes there is no NAT between the EAS/AF and the UPF.

NOTE 2: The SMF Event Exposure service may be extended with new event (e.g. UPF ID).

3. The SMF responds Nsmf\_EventExposure\_Notify with the list of UPFs for the User PDU Session.

Figure 6.1.2.5.1-2 below shows second alternative:



Figure 6.1.2.5.1-2: Procedure of UPF selection by the NF targeting PDU session or UE through UPF registration information in NRF

0. The UPF sends its supported IP range (and IP domain if needed) in the NF profile provided to the NRF during the NF registration. The NF profile also contains the address of the UPF Event Exposure service.

1. If the consumer NF is an AF/NEF, the AF/NEF issues an Nnrf\_NFDiscovery\_Request service operation to find the appropriate UPF providing NF type (i.e. UPF) and UE IP address and if needed IP domain.

2. The NRF responds Nnrf\_NFDiscovery\_Request with the NF profiles of all UPFs that currently meet the AF/NEF discovery request.

In a third alternative:



Figure 6.1.2.5.1-3: Procedure of UPF selection by the NF targeting PDU session or UE with information of IP address using BSF

1. If the consumer NF is an AF/NEF, the AF/NEF uses UE IP address (and if needed IP domain) to obtain the SUPI from the BSF.

2. Procedure of UPF selection by the NF targeting PDU sessions of a certain UE with information of SUPI in 6.1.2.5.2-1 is applied.

##### 6.1.2.5.2 Procedure of UPF selection by the NF targeting PDU session or UE with information of SUPI, S-NSSAI and DNN

This solution is applied to discover central PSA UPF, local PSA UPF and distributed PSA UPF.



Figure 6.1.2.5.2-1: Procedure of UPF selection by the NF targeting PDU sessions of a certain UE with information of SUPI, S-NSSAI and DNN

1. The consumer NF (e.g. an NWDAF), issues an Nnrf\_NFDiscovery\_Request service operation to find the UDM providing the NF type, UE ID (SUPI).

2. The NRF responds Nnrf\_NFDiscovery\_Request with the NF profile of the UDM that currently meet the consumer NF discovery request.

3. The consumer NF issues an Nudm\_UECM\_Get request to find the SMF from UDM providing NF type, UE ID (SUPI), S-NSSAI, DNN.

4. The UDM finds the serving SMF for the UE providing SUPI, S-NSSAI, and DNN, as described in TS 23.502 [3].

5. The UDM responds the SMF ID over Nudm\_UECM\_Get service response to the consumer NF.

6-7 The consumer NF contacts NRF to get the SMF exposure service contact information for SMF ID unless it has it already.

8. The consumer NF obtains UPF information from the SMF provided by the UDM over the Nsmf\_EventExposure\_Subscribe service operation providing SUPI, S-NSSAI, and DNN.

If for a PDU session, the consumer NF needs to subscribe only to PSA UPFs on a given DNAI, it may provide DNAI in the request to SMF as input filter. If the consumer NF needs to subscribe only to the UPFs that will steer traffic of an App id or application flow, it may provide them in the request to SMF as input filter. SMF will return information of UPFs that may see that traffic according to its knowledge.

NOTE: Some rules may have been predefined in UPF, and SMF may only be aware of the rules that it has provisioned in UPF itself.

9. The SMF responds Nsmf\_EventExposure\_Notify with the requested UPF ID and the type of UPF.

If the User PDU Session UP path changes, SMF may send a notification to consumer NF according to the subscription. Consumer NF can then create, update or remove the subscription to UPF event exposure service according to the impact on the UPF selection.

##### 6.1.2.5.3 Procedure of UPF selection by the NF with information of S-NSSAI, DNN and/or DNAI



Figure 6.1.2.5.3-1: Procedure of UPF selection by the NF with information of S-NSSAI, DNN and/or DNAI

0. The UPF sends its S-NSSAI, DNN, DNAI, UPF Service Area, Supported Event ID(s) to the NRF during the UPF Event Exposure service registration procedure as described in clause 6.1.2.1.

1. The consumer NF (for example, NWDAF) issues an Nnrf\_NFDiscovery\_Request service operation to find the appropriate UPF providing NF type (i.e. UPF), S-NSSAI, DNN, DNAI and Event ID(s).

2. The NRF responds Nnrf\_NFDiscovery\_Request with the list of all UPFs that currently meet the request.

##### 6.1.2.5.4 Procedure of UPF selection by the NF targeting specific PDU sessions and UEs with information of Group Identifier

Two procedures are possible:



Figure 6.1.2.5.4-1: Procedure of UPF selection by the NF with information of Group Identifier

1. If the consumer NF is an NWDAF, the NWDAF issues an Nnrf\_NFDiscovery\_Request service operation to find the UDM providing the NF type and Group ID.

2. The NRF responds Nnrf\_NFDiscovery\_Request with the NF profile of the UDM that currently meets the NWDAF discovery request.

NOTE: It is assumed that all members of a Group ID belong to the same UDM.

3. NWDAF requests the list of SUPIs that correspond to the Group ID using Nudm\_SDM\_Get.

4. UDM returns the list of SUPIs.

5. For each SUPI, NWDAF triggers from step 3 of procedure in clause 6.1.2.5.2.

As an alternative, UPF(s) can be selected as described in clause 6.1.2.5.3. with procedure of UPF selection by the NF with information of S-NSSAI, DNN and/or DNAI. The Group ID is included as target in the subscription request to the UPFs that determine the specific target PDU Sessions, if any, in that UPF.

### 6.1.3 Impacts on services, entities and interfaces

SMF:

- Determine the UPF that serves the target UEs in the scope of any UE according to parameters of NWDAF IP address, DNN, S-NSSAI.

- Nsmf Event Exposure Subscription needs to be enhanced to support exposing the information of UPF(s) that matches a PDU session and notify any changes according to subscription.

NRF:

- Discovery of several UPFs that accords with the UE IP address or IP range/domain.

AF/NEF:

- Invoke the BSF using the UE address (i.e. IP address or MAC address), DNN, S-NSSAI as discovery criteria.

UDM:

- Newly introduce UDM event consumers (e.g. NWDAF).

PCF:

- Update Npcf\_SMPolicyControl service so that PCF receives and can store the SMF ID for the policy association.

- Update the Npcf\_EventExposure service for PCF to send the SMF ID for the PDU session to the AF/NEF.

## 6.2 Solution #2: <UPF event exposure service for TSC management>

### 6.2.1 Key Issue mapping

This solution addresses KI 2.

### 6.2.2 Description

The SMF and UPF may exchange TSC management information container, such as the user plane node Management Information Container (UMIC) and Port Management Information Container (PIMC) over an N4 session. However, Port management information is transferred transparently via 5GS between TSN AF or TSCTSF and DS-TT in UE or NW-TT in UPF, respectively, inside a PMIC. User plane node management information is transferred transparently via 5GS between TSN AF or TSCTSF and NW-TT in UPF inside a UMIC. As a result, in order for TSC management information to be directly provided to TSN AF or TSCTSF by NW-TT in UPF, the UPF event exposure service should be invoked. TSC management information can thus be exposed to TSN AF or TSCTSF via the UPF.

NOTE: Transferring TSC management information from TSNAF/TSCTSF to NW-TT/UPF is outside the scope of this solution.

Table 6.2.2-1: NF Services provided by UPF

| Service Name | Description | Example Consumer(s) |
| --- | --- | --- |
| Nupf\_EventExposure | This UPF service provide the support for event exposure. | TSN AF, TSCTSF |

Nupf\_EventExposure service enables an NF (e.g. TSA AF or TSCTSF) to subscribe and get notified about UPF events for TSC management information. The following service operations are defined for the Nupf\_EventExposure service:

- Nupf\_EventExposure\_Subscribe.

- Nupf\_EventExposure\_UnSubscribe.

- Nupf\_EventExposure\_Notify.

The TSC management information event can be notified to TSN AF or TSCTSF. This UPF event notification may contain PMIC(s) and/or UMIC along with the associated NW-TT port number as described in clauses 5.8.2.11.14 and 5.28.3 of TS 23.501 [2]. TSN AF or TSCTSF subscribes and receives event notifications if specific port management information for a NW-TT port changes or user plane node management information changes. In other words, the UPF notifies TSN AF or TSCTSF if port management information or user plane node management information has changed that TSN AF or TSCTSF has subscribed for.

### 6.2.3 Procedures

In this solution, procedures are proposed to (un)subscribe/notify the UPF event for TSC management information. The UPF is selected for a PDU Session serving TSC as described in clause 6.3.3.3 of TS 23.501 [2]. TSN AF or TSCTSF can identify the PDU session during the PDU session establishment procedure. Then, UPF/NW-TT triggers the N4 Session Level Reporting Procedure to forward the PMIC(s) and/or UMIC to SMF.

Two methods are proposed for subscribing UPF event exposure service as follows:

- TSN AF or TSCTSF subscribes the UPF event (Figure 6.2.3.1-1).

- Instead of TSN AF or TSCTSF, SMF subscribes the UPF event (Figure 6.2.3.2-1).

#### 6.2.3.1 TSN AF/TSCTSF based UPF event subscription

This clause describes the procedure for TSN AF or TSCTSF to (un)subscribe the UPF event and receive the event notification for TSC management information. TSN AF or TSCTSF can apply the procedure of UPF selection by the NF targeting PDU session specified in clause 6.1.2.5.1 in solution #1 to discover the UPF with the PDU session.



Figure 6.2.3.1-1: UPF event exposure based on TSN AF/TSCTSF subscription

0. Procedure of UPF selection by the NF targeting PDU session in Solution #1 is performed.

1. TSN AF or TSCTSF sends Nupf\_EventExposure\_(Un)scribe service operation for TSC management information event to the UPF.

2. The event notification is triggered if there are changes in UMIC/PMIC from the UPF/NW-TT or the PDU session is released.

3. UPF sends the event notification for TSC management information over Nupf\_EventExposure\_Notify service operation to TSN AF or TSCTSF.

#### 6.2.3.2 SMF based UPF event subscription

This clause describes how SMF can (un)subscribe the UPF event so that TSN AF or TSCTSF receives the event notification for TSC management information. The PDU Session Establishment as defined clause 4.3.2.2.1-1 of TS 23.502 [3] is used to establish a PDU Session serving for TSC. During this procedure, the SMF selects a UPF for the PDU Session that supports functions as defined in clause 5.28.1 of TS 23.501 [2]. As a result, the SMF may subscribe to the UPF event as a result of the PCF initiated SM Policy Association Modification as described in Figure 4.16.5.2-1 of TS 23.502 [3], rather TSN AF or TSCTSF.



Figure 6.2.3.2-1: UPF event exposure based on SMF subscription

1. TSN AF or TSCTSF subscribes for TSN/TSC events using the Npcf\_PolicyAuthorization\_Subscribe operation. Subscription indicates that UPF direct report of TSC management information is preferred.

2. If the PCF has received indication that UPF direct report is preferred or a Port Management Information Container for the PDU Session and related port number from the TSN AF or TSCTSF, the PCF issues a Npcf\_SMPolicyControl\_UpdateNotify request with possibly updated policy information about the PDU Session and/or target address for the notification when UPF direct report is preferred. Then, the SMF acknowledges the PCF request with a Npcf\_SMPolicyControl\_UpdateNotify response.

3. SMF sends Nupf\_EventExposure\_(Un)scribe service operation for TSC management information event to the UPF. As an alternative, the SMF may configure direct reporting information (refer to the clause 7.5.2.9 of TS 29.244 [8]) on the UPF using N4 Session Modification procedure.

NOTE: If the SMF does not configure direct reporting information during N4 Session Modification procedure (i.e. the UPF does not support direct reporting to TSN AF or TSCTSF), the UPF reports TSC management information to the SMF via the N4 interface.

4. The event notification is triggered if there are changes in UMIC/PMIC from the UPF/NW-TT or the PDU session is released.

5. UPF sends the event notification for TSC management information over Nupf\_EventExposure\_Notify service operation to TSN AF or TSCTSF.

#### 6.2.3.3 Bridge information reporting

During the SM Policy Association Establishment procedure, if the PCF detects the request relates to SM Policy Association enabling integration with TSN or TSC, the PCF may provide policy control request trigger for 5GS Bridge Information. TSN AF can (un)subscribe TSC management information events to the UPF using the methods given above in this scenario.



Figure 6.2.3.3-1: UPF event exposure during 5GS Bridge information reporting

The procedure of 5GS Bridge information reporting in Figure F.1-1 of TS 23.502 [3] is performed with the following differences and clarifications:

1. PDU Session Establishment as defined clause 4.3.2.2.1-1 of TS 23.502 [3] is used to establish a PDU Session serving for TSC.

2. The SMF sends the information received in step 1 to the TSN AF or TSCTSF via PCF to establish/modify the 5GS Bridge. The TSN AF or TSCTSF subscribes for TSN events over the newly created AF session using the Npcf\_PolicyAuthorization\_Subscribe operation (step 2d).

The TSN AF can use any PDU Session to subscribe with the NW-TT for bridge or port management information notifications. Similarly, the UPF can use any PDU Session to send bridge or port management information notifications.

3. The procedure of UPF event exposure in Figure 6.2.3.1-1 or steps from 2 to 5 of Figure 6.2.3.2-1 is performed to use UPF exposure service for TSC management information between the UPF and TSN AF.

The TSN AF or TSCTSF may additionally provide an indication of event notification which contains a Notification Target Address when subscribing for TSN/TSC events to the PCF. The QoS Monitoring information may include an indication of local event notification which contains a Notification Target Address in a similar manner. According to clause 5.8.2.11.11 of TS 23.501 [2], the UPF reports the QoS Monitoring information via Nupf\_EventExposure\_Notify service operation, as indicated by the indication of local event notification. Therefore, the TSN AF or TSCTSF requests the UPF to directly report TSC management information event via Nupf\_EventExposure\_Notify service operation by either adding the indication of event notification in TSC management information or subscribing to the event notification via Nupf\_EventExposure\_Subscribe.

#### 6.2.3.4 Analysis of directly reporting TSC management information

UPF/NW-TT reports TSC management information event using the N4 Session Level Reporting procedure as specified in clause 4.4.2.2 of TS 23.502 [3]. The UPF shall give the TSC management information, as defined in clause 6.2.2, to the SMF when it detects the TSC management information event that needs to be reported. The SMF then initiates the SM Policy Association Modification procedure as described in clause 4.16.5.1 of TS 23.502 [3]. If the SMF has reported TSC management information, such as PMIC with port number or UMIC, then the PCF transparently transports the received PMIC and the related port number or UMIC to the TSN AF or TSCTSF as described in clauses 6.1.3.23 and 6.1.3.23a of TS 23.503 [4].

The definition of 5GS Bridge information is included in Table 6.1.3.5-1 of TS 23.503 [4], which may contain user-plane Node ID, UE-DS-TT residence time and Ethernet port or IP address for the PDU Session and/or PMIC and/or UMIC. Two procedures are introduced to handle 5GS Bridge information: 5GS Bridge information reporting in Figure F.1-1 of TS 23.502 [3] and 5GS Bridge configuration in Figure F.2-1 of TS 23.502 [3]. TSC management information is delivered by TSN AF or TSCTSF to configure TSC management information in UPF/NW-TT in a 5GS Bridge configuration. The 5G Bridge information reporting is connected to the reporting of TSC management information from UPF/NW-TT to TSN AF or TSCTSF from the perspective of the UPF event exposure service.



Figure 6.2.3.4-1: 5GS Bridge information reporting [3]

Step 2a of Figure 6.2.3.4-1 involves the SMF initiating SM Policy Association modification, and step 2b shows the PCF delivering the Npcf PolicyAuthorization Notify message to the TSN AF or TSCTSF. The PCF transmits 5GS Bridge information to the TSN AF or TSCTSF when it has the 5GS Bridge information received from SMF and has a subscription for the 5GS Bridge information Notification from the TSN AF or TSCTSF. The parameters in PMIC or UMIC are not handled by SMF/PCF during 5GS Bridge information reporting. With reference to steps 1 and 2 of Figure 6.2.3.4-1, the UPF/NW-TT can therefore provide event exposure services to directly report TSC management information events.

### 6.2.4 Impacts on services, entities and interfaces

**UPF:**

- Needs to support UPF event exposure service operations for TSC management information.

- New event id for TSC management information is available to UPF.

**SMF:**

- (Optional) May support UPF event exposure service operations for TSC management information.

**PCF:**

- (Optional) May support UPF event exposure service operations for TSC management information by providing UPF direct reporting information to SMF.

**TSF AF / TSCTSF:**

- Needs to support UPF event exposure service operations for TSC management information.

## 6.3 Solution #3: using the proper subscription mechanism depending on the event targeted by the UPF event consumer

### 6.3.1 Key Issue mapping

This solution addresses KI 2.

### 6.3.2 Description

The solution strives to ensure usage of the proper subscription mechanism depending on the event targeted by the UPF event consumer, assuming that in any case discussed in this clause the notifications are sent by the UPF using Nupf\_EventExposure Service. The UPF event consumer is the NF that will receive Nupf\_EventExposure\_Notify service operation; it may sometimes differ from the NF that provides the subscription request to the UPF.

The analysis and technical mechanisms defined in solution 3, 4, 5 and 6 consider the R18 requirements that the UPF event consumer may be a NWDAF (per requirements expressed in TS 23.288 [5]), or an AF / a NEF requesting QoS related exposure (as being studied as part of R18: FS\_EDGE\_Ph2 or FS\_XRM). (future) Application of these solutions for other usage of UPF event exposure by NEF/ AF or for other UPF event consumers is not precluded.

To determine the proper method to be used by the UPF event consumer to subscribe to UPF event notification, it is needed to take into account the target of the monitoring (one UE, ... any UE) as well as the filtering to apply to the events being reported (as recalled in Annex A):

- A set of UPF(s) possibly for a Network Slice and / or DNN.

- A UE or a group of UEs or any UE in a Network Slice and / or DNN.

- An application, a set of IP flows.

- An Area of Interest (i.e. set of TAIs), as defined in TS 23.501 [2].

- A RAT Type or Frequency or both.

NOTE: The determination the proper method to be used by the UPF event consumer to subscribe to UPF event notification needs to take into account different aspects: on one hand direct subscription from the UPF event consumer to UPF can in some cases reduce the signalling load within the 5GC but on the other hand the SMF is aware of more information about a PDU Session than the UPF and such information may be required by event filtering; Requiring the SMF to keep UPF(s) up to date about information such as the TAI / Cell / RAT type / satellite backhaul serving a PDU Session would induce MUCH more signalling than the signalling gained by a direct subscription from final UPF event consumer. Making UPF aware of information such as the TAI / RAT type / satellite backhaul serving a PDU Session goes against the SDN principle that a simpler and efficient User plane entity should focus on packet switching, and should not be bothered by information only relevant for the Control Plane.

For all mechanisms described below (except the mechanism in item 1) UPF(s) need to register their event exposure service onto NRF using Nnrf\_NFManagement as described in solution 1.

Following mechanisms are considered with descending order of priority (if the UPF reporting does not meet conditions of item 1, then conditions of item 2 are evaluated, etc.)

1. If the UPF event retrieval requires some action from the 5G AN / 5G RAN, as for NEF/ AF requesting QoS related exposure defined in Rel-17 for QoS monitoring, the UPF event consumer subscribes via the SMF. This ensures that the SMF can request 5G (R)AN action (such as reporting QoS information to the UPF) at N2 PDU session resource creation / modification e.g. after PDU Session UP (re)-establishment or after mobility (e.g. HandOver or mobility between 3GPP and Non 3GPP access).

- Potential Outputs from the Rel-18 Edge Computing Study requiring getting information from NG RAN are potential examples where such mechanism is needed.

2. If the event retrieval is associated with a UE location dependant filter (e.g. an Area of interest corresponding to a set of Tracking Areas or a RAT Type / an Access Type and/or a SSID/BSSID), the UPF event consumer subscribes via the SMF; This ensures that the SMF being already aware of ULI (User Location Information such Tracking Areas/ SSID/BSSID) and of RAT Type / Access Type can control whether UPF needs to report.

NOTE: an alternative mechanism could have been envisaged: in order to ensure that the UPF can apply event subscription filters set by a direct NF consumer subscription to UPF events, the 5G AN would provide via GTP-u the UPF with following information associated with a GTP-u tunnel PDU Session: the associated ULI (TAI, cell id, etc.) RAT type, etc. Then the UPF would use this information to check whether some UPF event subscription filters match; if yes the UPF would start considering the corresponding traffic for the notifications related with the UPF event subscription. This kind of solution would impact the 5G AN which is forbidden by the FS\_UPEAS SID SP‑211652.

Examples where such mechanism is needed are:

- Requirements within clause 6.11.1 of TS 23.288 [5] on "WLAN performance analytics requests" and recalled in item 5 of Annex A of this TR.

- The following Requirements when Analytics Filter Information includes a location (e.g. ECGI, TA) / an AoI:

- Requirements within Table 6.8.2-2 of TS 23.288 [5]: "Data Collected from the UPF or from the AF related to User Data Congestion Analytics requests" and recalled in item 3 of Annex A of this TR.

- Requirements within Table 6.10.2-5 of TS 23.288 [5]: "UE data volume dispersion collected from serving UPF" and recalled in item 4 of Annex A of this TR.

- Requirements within clause 6.14.1 of TS 23.288 [5] "User plane performance analytics" and recalled in item 7 of Annex A of this TR.

3. When the target of UPF event subscription is a UPF itself (possibly for a set of DNN and / or slice) the final NF consumer uses Nnrf\_NFDiscovery to discover the UPF (TS 29.510 [6] already supports discovering UPF(s) based on the DNN and or S-NSSAI they serve or based on UPF locality). N4 nevertheless needs to be upgraded as described in solution 4 in order for the UPF to be able to apply UPF event subscription filters on parameters such as the DNN:

- this mechanism applies e.g. to Table 6.5.2-2 of TS 23.288 [5]: "Data collected by NWDAF for UPF load analytics" recalled in item 2 of Annex A of this TR;

- for this kind of event the functionality of the UPF for a PDU Session (PSA, UL CL, simple forwarder) needs does not need to be considered.

4. When the Target of Analytics Reporting = a UE identified by a SUPI or by its address (and for IP a DNN + a S-NSSAI) it is needed to identify which UPF(s) serve the relevant PDU Sessions of the UE.

This applies to following TS 23.288 [5] Requirements when the UE target is an Individual UE AND Analytics Filter Information does NOT include a location (e.g. ECGI, TA) / an AoI. For example:

- Requirements within Table 6.8.2-2 of TS 23.288 [5]: "Data Collected from the UPF or from the AF related to User Data Congestion Analytics requests" and recalled in item 3 of Annex A of this TR.

- Requirements within Table 6.10.2-5 of TS 23.288 [5]: "UE data volume dispersion collected from serving UPF" and recalled in item 4 of Annex A of this TR.

- Requirements within TS 23.288 [5] clause 6.14.1 "User plane performance analytics" and recalled in item 7 of Annex A of this TR.

- TS 23.288 [5] Table 6.5.2-2: Data collected by NWDAF for UPF load analytics recalled in item 2 of Annex A of this TR.

When the consumer of UPF event exposure can, within the UPF(s) that serve a target PDU Session, determine the proper UPF where to subscribe for event exposure (see clause 6.3.4):

- The mechanism described in solution 6 is used when the target UE is identified by its SUPI.

- The mechanism described in solution 5 is used when the target UE is identified by its (IP or MAC) address.

Otherwise the consumer of UPF event exposure requests the SMF controlling the target PDU session to subscribe to the proper UPF(s) on its behalf.

5. When the Target of Analytics Reporting = Internal-Group Identifier (for a DNN + a S-NSSAI) it is needed to identify which UPF(s) serve the relevant PDU Sessions of the group.

The final NF consumer uses Nnrf\_NFDiscovery to discover the UPF(s) serving a DNN + S-NSSAI. N4 nevertheless needs to be upgraded as described in solution 4 in order for the UPF to be able to apply UPF event subscription filters on Internal-Group Identifier.

This applies for example to the same TS 23.288 [5] Requirements as defined in item 4 above when Analytics Filter Information does NOT include a location (e.g. ECGI, TA) / an AoI and the UE target is an Internal-Group Identifier.

Editor's note: Subscribing onto all the UPF(s) that can serve a DNN + S-NSSAI for groups that involve very few users (hence a limited number of UPF(s)) is not efficient. It is FFS whether a more optimised solution is possible.

### 6.3.3 Procedures

The procedure of solution 1, solution 4, solution 5 and solution 6 may apply according to the analysis of clause 6.3.2.

### 6.3.4 selection of the proper UPF within the UPF(s) that serve a PDU Session

Some UPF (event) reporting target the UPF itself so any UPF that meets some criteria (e.g. UPF supporting a slice, in a locality) should be considered.

Some UPF reporting relate to a target (application) flow so relate to the UPF(s) that supports this (application) traffic flow. For a PDU Session, only one UPF that handle such a traffic flow should be involved for the reporting, for example in following case:

- (Annex A, item 1) The Observed Service Experience analytics may provide Service Experience for an Edge Application over a UP path: Service experience in an Application or a set of Applications over a specific UP path (UPF, DNAI and EC server). UPF needs to report observed bit rate, delay, number of packet transmission / retransmission.

If no care is taken, then there is the risk of double counting: if UPF reporting is triggered at both the UL CL UPF and the PSA UPF that serve the target application flow within a PDU Session we incur following risks:

- Counting twice where the UPF event consumer (NWDAF) would receive twice the information on the number of packet transmission and may assume twice the traffic.

- Doubling the signalling where the report about the observed bit rate, delay etc…would be sent by multiple (at least 2) UPF(s) for the same traffic.

(This assumes deployments where the UL CL UPF and the PSA UPF are different UPF(s)).

Furthermore, if the traffic handling of the target (application) flow is moved from old UPF(s) to new UPF(s) (UL CL and PSA relocation due e.g. to UE mobility) then if direct subscription to UPF reporting is done by the consumer (NWDAF) of UPF reporting, then this consumer becomes responsible of requesting the event reporting to the new UPF(s) in case of change of serving UPF.

NOTE: Usage of solution 1, 5 or solution 6 depends on the type of analytics / exposure that the final UPF event consumer requires. Whether a PDU Session uses multiple UPF(s) (I-UPF, UL CL, different PSA) depends on SMF policies related with DNN+s-NSSAI as well as on UE mobility. Both aspects (the type of analytics / exposure versus usage of multiple UPF(s) for a PDU Session) are not related with each other, thus the issue of contacting the right UPF may take place when each of solution 1, solution 5 and solution 6 applies.

### 6.3.5 Impacts on services, entities and interfaces

Impacts depend on which of solution 1, solution 4, solution 5 and solution 6 applies.

## 6.4 Solution #4: upgrading N4 to pass necessary event filtering information to the UPF

### 6.4.1 Key Issue mapping

This solution addresses KI 2.

### 6.4.2 Description

The UPF event consumer may, as defined in solution 3, be a NWDAF, an AF or a NEF.

The solution runs as follows:

- in order to ensure that the UPF can apply event subscription filters set in a subscription to UPF events, the SMF provides UPF with following information associated with an N4 Session: the associated DNN, S-NSSAI (already existing information), list of Internal-Group Identifiers (the UE subscription and hence the PDU /N4 Session may be associated with more than one Internal-Group Identifier).

- the UPF uses this information to check whether some UPF event subscription filters match; if yes the UPF starts considering the N4 session for the notifications related with this UPF event subscription.

### 6.4.3 Procedures



Figure 6.4.3-1: N4 Session Establishment procedure

0. The UPF may receive a subscription to event reporting with a filter criteria that may contain a DNN, a S-NSSAI, a User group identifier (this is the case where the UPF receives a subscription before the N4 session establishment).

When UPF receives step 0 it needs to check whether there are already on-going N4 sessions that match the subscription filters. For these N4 sessions step 0 may immediately trigger step 5.

1. SMF receives the trigger to establish a new PDU Session or change the UPF for an established PDU Session as in step 1 of TS 23.502 [3] Figure 4.4.1.2-1.

2. The SMF sends an N4 session establishment request message to the UPF. The SMF provides UPF with following information associated with an N4 Session: the associated DNN, S-NSSAI, list of Internal-Group Identifiers; This step may also correspond to a N4 Session modification.

3. The UPF responds with an N4 session establishment (or modification) response Session as in step 3 of TS 23.502 [3] Figure 4.4.1.2-1.

If the UPF (by configuration or other means) utilizes an NWDAF, UPF may provide the received information to its NWDAF.

4. The UPF may receive a subscription to UPF event reporting with a filter criteria that may contain a DNN, a S-NSSAI, a User group identifier (this is the case where the UPF receives a subscription after the N4 session establishment).

5. Based on the received information in step 2, the UPF determines whether the N4 session matches the filter criteria of the subscription to UPF event reporting and if this is the case starts taking into account the PDU Session for such reporting.

### 6.4.4 Impacts on services, entities and interfaces

The solution impacts N4 (delivery of extra information such as DNN or Internal-Group Identifier) thus the SMF and the UPF.

## 6.5 Solution #5: registering UPF(s) serving a PDU session at UDM

### 6.5.1 Key Issue mapping

This solution addresses KI 2. It addresses the case where the UPF event consumer desires to subscribe to UPF(s) event exposure and targets PDU Sessions involving a UE identified by its UE ID.

### 6.5.2 Description

The UPF event consumer may, as defined in solution 3, be a NWDAF, an AF or a NEF.

The solution runs as follows:

- The SMF updates the UDM/UDR with the list of UPF(s) serving a PDU Session via Nudm\_UECM service (Nudm\_UECM\_Registration and Nudm\_UECM\_Update when the UPF information changes). The information provided to the UDM may contain:

- The SUPI, DNN, S-NSSAI (already provided as part of Nudm\_UECM\_Registration).

- The set of address(es) used by the user equipment on the PDU Session; this needs to be refreshed when new UE MAC addresses are notified to the SMF or when the SMF allocates new prefixes in a multi-homed PDU session.

- The UPF instance Id of each UPF involved in the PDU Session. This information needs to allow the UPF event consumer to contact the NRF to discover the parameters needed to subscribe onto the UPF event exposure.

- the Type of UPF (UL CL, PSA, traffic forwarder, IPUPS) and the DNAI this UPF serves (for the PSA UPF).

NOTE: The functionality of the UPF for the PDU Session (PSA, UL CL, simple forwarder, etc..) needs to be considered. Failure to do so may induce that the NWDAF considers multiple time the same traffic (e.g. at UL CL and at PSA) or does not request (delay, packet loss) statistics at the right place (which should be the PSA); see also clause 6.3.4.

Editor's note: Whether the UPF information can be stored in the UDM is FFS.

- The UPF event consumer invokes Nudm\_UECM\_Get to get the list of UPF serving a PDU session identified by the SUPI/GPSI, a DNN, a S-NSSAI and possibly an UE address (IP address or MAC address).

- The UDM provides the UPF instance Id of each UPF that matches the Nudm\_UECM\_Get.

- The UPF event consumer uses this information to get information on the UPF exposure service from NRF.

- The UPF event consumer subscribes to the UPF event exposure.

- The UPF notifies the UPF event consumer.

### 6.5.3 Procedures



Figure 6.5.3-1: Registering UPF(s) serving a PDU session at UDM

0. UPF(s) need to register their event exposure service onto NRF using Nnrf\_NFManagement as described in solution 1.

1. A PDU Session is established or modified and the modification requires a change of UPF to serve the PDU Session (e.g. due to UE mobility or to new PCC rule or to EASDF induced UL CL insertion).

The SMF selects new UPF(s) and establishes N4 session with these UPF(s). This may imply usage of solution 4.

2. The SMF registers the PDU Session on UDM or updates the PDU Session registration on UDM. Nudm\_UECM\_Registration and Nudm\_UECM\_Update when the UPF information changes. The information provided to UDM is described in clause 6.5.2.

3. the UPF event consumer invokes Nudm\_UECM\_Get to get the list of UPF serving a PDU session identified by the SUPI/GPSI, a DNN, a S-NSSAI and possibly an UE address (IP address or MAC address).

4. the UDM provides the UPF instance Id of each UPF that matches the Nudm\_UECM\_Get.

5. the UPF event consumer uses this information to get information on the UPF exposure service via Nnrf\_NFDiscovery\_Request.

6. the NRF provides the requested information.

7. the UPF event consumer issues Nupf\_EventExposure\_Subscribe.

8. when the conditions set in Nupf\_EventExposure\_Subscribe match, UPF issues Nupf\_EventExposure\_Notify.

### 6.5.4 Impacts on services, entities and interfaces

The solution impacts SMF, UDM and the UPF event consumers (NWDAF, NEF, AF).

## 6.6 Solution #6: Determining the UPF(s) that serve a UE address

### 6.6.1 Key Issue mapping

This solution addresses KI 2. It addresses the case where the UPF event consumer desires to subscribe to UPF(s) event exposure and targets PDU Sessions involving a UE identified by its UE address.

### 6.6.2 Description

The UPF event consumer may, as defined in solution 3, be a NWDAF, an AF or a NEF.

The solution runs as follows:

- Per Rel-17 specifications, the SM PCF issues Nbsf\_Management\_Register to Register the tuple (UE address(es), SUPI, GPSI, DNN, S-NSSAI, PCF address(es), PCF instance id, PCF Set ID) for a PDU Session. The SM PCF issues Nbsf\_Management\_Update to update the information.

- The UPF event consumer invokes the BSF (Nbsf\_Management\_Discovery ) using the UE address (i.e. IP address or MAC address), DNN, S-NSSAI as discovery criteria to get the SUPI of the UE.

- Then the UPF event consumer can invoke solution 5.

### 6.6.3 Procedures



Figure 6.6.3-1: Determining the UPF(s) that serve a UE address

1. A PDU Session is established or modified as described in Rel-17, clauses 4.3.2 and 4.3.3 of TS 23.502 [3].

2. SM Policy Association Establishment / Modification using Npcf\_SMPolicyControl\_Create / Npcf\_SMPolicyControl\_Update as described in Rel-17, clause 4.16.4 / clause 4.16.5 of TS 23.502 [3].

3. At SM Policy Association Establishment, the SM PCF issues Nbsf\_Management\_Register to Register the tuple (UE address(es), SUPI, GPSI, DNN, S-NSSAI, PCF address(es), PCF instance id, PCF Set ID) for a PDU Session. At SM Policy Association modification, the SM PCF issues Nbsf\_Management\_Update to update the information (new set of UE address associated with a PDU session). All these interactions are per Rel-17 specifications.

4. The UPF event consumer invokes the BSF (Nbsf\_Management\_Discovery Request) using the UE address (i.e. IP address or MAC address), DNN, S-NSSAI as discovery criteria.

5. The BSF answers (Nbsf\_Management\_Discovery Response) with the SUPI of the UE.

6. Then the UPF event consumer can invoke solution 5.

### 6.6.4 Impacts on services, entities and interfaces

- The UPF event consumer needs to invoke the BSF using the UE address (i.e. IP address or MAC address), DNN, S-NSSAI as discovery criteria.

- Nbsf\_Management\_Discovery Response needs to provide as output the SUPI of the UE.

- Impacts of solution 5.

## 6.7 Solution #7: Support to existing (Rel‑16-Rel‑17) data analytics with PDU Session Data Usage Events

### 6.7.1 Key Issue mapping

This Solution addresses KI#2.

### 6.7.2 Description

This solution extends the Rel-17 UPF Event Exposure service with two new events for the collection of information of user data usage of the User PDU Session:

- One event provides measurements, and it will be referred to as UserDataUsageMeasures along the solution and can include following information:

- Volume Measurement: measures of data volume exchanged (UL, DL and/or overall) and/or number of packets exchanged (UL, DL and/or overall) with or without application granularity. This measurement can also include number of packets transmitted for applications where that is possible to differentiate.

- Throughput Measurement: measures of data throughput (UL and DL) measures aggregated for the PDU Session or per application.

- The other event provides statistical measurements, and it will be referred to as UserDataUsageTrends along the solution and can include following information:

- Throughput Statistic Measurement (average and/or peak throughput) over the measurement period for the PDU Session or per application.

Both events provide measurement context (for example, the measurement period) and information of the PDU Session. When the information refers only to certain traffic, an identifier e.g. Application Id may also be included.

This solution defines a UPF Event Exposure Subscription operation that consumers can use to subscribe to UPF Event Exposure service for the two new events, UserDataUsageMeasures and UserDataUsageTrends. Subscription can be for a UE, "Any\_UE", or a specific PDU Session. The Event Subscription includes filters for the data collection, and measurement, event reporting and notification control information like which data that is requested and with which granularity (for the PDU Session or for an Application within the PDU Session).

In this solution, the subscription to UPF does not have any impact on UPF packet matching procedure and it does not degrade the performance of UPF user plane traffic handling. When for exposure the UPF traffic differentiation in the User PDU Session is according to the packet detection rules that have been installed for each PFCP session by SMF, when measurements are requested for an/per application, UPF considers for the measurements of a User PDU Session and App Id only the traffic that is matching a PDR which has that App Id.

The event notifications are sent to the consumer according to the notification control information received in the subscription to the event.

This solution satisfies following Rel-16-Rel-17 NWDAF Analytics UPD Data Collection needs as follows:

- NF Load: UserDataUsageMeasures event with Volume Measurement (see NOTE 1) accumulated for the PDU Session.

- User data Congestion: UserDataUsageTrends event with Throughput Statistic Measurement with per application or IP Packet Filter Set measures over a measurement period.

- UE Communications: UserDataUsageMeasures event with Volume Measurement and Throughput Measurement with per Application or IP Packet Filter Set measures or with PDU Session aggregated measures for a UE\_communication (see NOTE 2).

- WLAN Performance analytics: UserDataUsageMeasures event with Volume Measurement and Throughput Measurement measured for a PDU Session.

- Dispersion: UserDataUsageMeasures event with Volume measurement and per application or IP Packet Filter Set measures (they are exclusive) or with PDU Session aggregated measures.

NOTE 1: The solution defines the Volume Measurements with similar definition as in the Traffic Usage Report.

NOTE 2: UE Communication definition may imply measuring periods are defined, for example, in relation to application activity/inactivity.

UPF reporting related with Delay measurements, and in general measurements related to QoS Flows is not addressed by this solution.

### 6.7.3 Procedures

#### 6.7.3.1 Subscription to UPF for Data Collection for "Any UE"

Figure 6.7.3.1-1 below shows the procedure for UPF Event Exposure subscription and notification for the UserDataUsageMeasures and UserDataUsageTrends events that can be used in scenarios targeting data collection from UPF for "Any UE".

Example UCs are NWDAF data collection for NF Load NWDAF analytic (clause 6.5 of TS 23.288 [5]), or for User Data Congestion Analytic (clause 6.8 of TS 23.288 [5]).



Figure 6.7.3.1-1, Data Collection from UPF for Any\_UE

A description of the procedure in Figure 6.7.3.1-1follows:

1. In a first step, UPF registers its profile in NRF.

2. NWDAF receives a request from a consumer.

If type of Analytic is for example "NF Load" and NFs type=UPF, it may be for UPFs only within an Area of Interest (AoI) and specific S-NSSAI, or it may be for a given UPF Id. If for example Type of Analytic is "User Data Congestion", if "Any UE", it always includes AoI, and if the request includes a SUPI, the user location determines the AoI but UPF data collection is still for "Any UE" within AOI. In this case, the consumer may also request N top consuming Applications.

3. NWDAF identifies the Data required for this analytic and starts data collection as in TS 23.288 [5]. In this case, data from UPF is required.

4. NWDAF selects the relevant UPFs with assistance from NRF. It can take into account information received in the request (for example, S-NSSAI and/or AoI).

NOTE 1: When a PDU Session user plane consists of more than one UPF, only some of them may have service area overlapping the AoI and be selected. Their role may be ULCL/BP and/or PSA. Depending on the deployment, NWDAF may be configured to use procedure in Figure 6.7.3.1-2 instead for a given Analytic.

5. NWDAF sends Nupf\_EventExposure Subscribe for Event= UserDataUsageMeasures / UserDataUsageTrends to relevant UPF(s) for "Any UE" and it may include filters like S-NSSAI or AoI (list of TAs). NWDAF provides Event Reporting Info including the DataSubset requested.

6. UPF Selects the PDU Sessions that match the filters and for that, it may perform sampling according to input received or local configuration. It starts to produce measurements for those sessions as requested.

NOTE 2: When application traffic differentiation for exposure is conditioned by the PFCP session packet detection rules, the application differentiation that may be needed by exposure is considered in the definition of the rules to apply to the PDU Sessions, so that SMF installs packet detection rules in the PFCP sessions in UCL/BP and/or PSA (see NOTE 1) accordingly.

The selection of PDU Sessions may change during the lifetime of the subscription e.g. at termination or establishment of PDU Sessions that meet the criteria, or UEs entering/leaving the AoI according to user location information (ULI) received over N4.

NOTE 3: NWDAF subscription to AMF/SMF events for the AoI widens the mobility events where UPF gets ULI updates, improving accuracy of UPF PDU Session selection for the AoI.

If Subscription has included AoI, and the PDU Session selection in UPF does not support this filter condition, UPF rejects the request from NWDAF.

NOTE 4: Upon reject, NWDAF identifies that it needs to create the mapping of PDU sessions per TA. NWDAF can subscribe to UE mobility event notifications of AMF to retrieve the list of SUPIs in the AoI (not needed if this information is already known). It can then apply instead the procedure in clause 6.7.3.2 on the retrieved list of SUPIs or subscribe to UPF without AoI filter condition using the retrieved list of SUPIs to filter the UPF events (step 8).

7. UPF sends Nupf\_EventExposure Notify for Event= UserDataUsageMeasures / UserDataUsageTrends for the selected PDU Sessions. The notifications include SUPI, DNN and S-NSSAI as available and conveys measurements and context according to the subscription.

8. NWDAF derives the Requested Analytic.

NOTE 5: NWDAF may at this stage use AMF/SMF information to filter the UPF events for the AoI.

9. NWDAF provides the Analytic requested.

#### 6.7.3.2 Subscription to UPF for Data Collection for certain PDU Sessions

Figure 6.7.3.1-2 below shows the procedure for UPF Event Exposure subscription and notification for the UserDataUsageMeasures and UserDataUsageTrends events that can be used in scenarios targeting data collection from UPF for certain UEs or PDU Sessions.

If Analytic is targeting "Any UE", this procedure can still be preferred or even needed for a preselection of the PDU Sessions (for example, when UPF lacks information to evaluate some filters), or as a way to perform the PDU Session sampling in SMF only when SMF also contributes to the analytic.

Example for UCs are NWDAF data collection for WLAN Performance analytics (clause 6.11 of TS 23.288 [5]), Dispersion analytics (clause 6.10 of TS 23.288 [5]), and for UE Communication analytics (clause 6.7 of TS 23.288 [5]).



Figure 6.7.3.1-2: Data Collection from UPF for certain PDU Sessions

A description of the procedure in Figure 6.7.3.1-2 follows:

Prerequisite: When application traffic differentiation for exposure is conditioned by the PFCP session packet detection rules, SMF has installed packet detection rules in the PFCP sessions with rules for the applications for which differentiated measurements may be needed.

1. NWDAF receives a request from a consumer.

As an example, type of Analytic may be "UE Dispersion" requesting a Data Volume Dispersion Analytic (DVDA) for "Any UE", a UE or a UE\_Group including filters like S-NSSAI, AoI and/or App Ids for applications of interest. Another example would be a request with type of Analytic "WLAN performance" for "Any UE", a UE or a UE\_Group in an AoI and for certain SSID/BSSID. In another example, Analytic type could be "UE Communication" targeting a UE or UE Group and specific Applications.

2. NWDAF identifies the Data required for this analytic and starts data collection as in TS 23.288 [5]. This analytic requires Data Collection from UPF and for that, the UPF PDU Session identifiers and UPF service contact information needs to be collected from SMF. SMF may contribute to this analytic with other data.

Clause 6.2.2 of TS 23.288 [5] specifies some options for how to select SMF:

- If Target is a UE or a UE Group, NWDAF can select the SMF(s) with UDM assistance as specified in clause 6.2.2 of TS 23.288 [5].

- If Target is "Any UE", NWDAF selects SMF with assistance of NRF taking into account filter conditions if any received in the request. If AoI is also provided, NWDAF can first determine the users within AoI with AMF assistance and proceed as when Target is a UE.

3. NWDAF sends Nsmf\_EventExposure Subscribe to SMF including the target and any conditions that need be considered for filtering or sampling the PDU Sessions. The SMF response/notification includes UPF identifiers of the User PDU Sessions matching the request and the information of the UPFs to be contacted. If needed, information of whether UPF is acting as PSA and DNAI could also be provided. This information may have been retrieved already during SMF data collection for the analytic in step 2.

NOTE 1: SMF event notifications of already specified exposure events can be enhanced for this purpose, for example UPF Info, PDU session establishment or Information on PDU Session for WLAN (see clause 5.2.8.3 of TS 23.502 [3]).

4. NWDAF takes SMF information as input for the data collection from UPF. It sends Nupf\_EventExposure Subscribe for Event= UserDataUsageMeasures / UserDataUsageTrends to the UPF handling the PDU Session. The subscription targets a PDU Session. The request includes Event Reporting Info, including the DataSubset requested.

If Subscription has included AoI and UPF supports this condition, UPF takes into account whether UE is entering/leaving the AoI according to user location information (ULI) received over N4. If UPF does not support this filter condition UPF rejects the request from NWDAF.

NOTE 2: Upon reject, NWDAF identifies that it needs to create the mapping of PDU session and TA itself. When there are many UE(s) in an AoI and many mobility in and out of the AoI, it may be convenient for the NWDAF to filter the events rather than performing many subscription/unsubscription to UPF to avoid high signalling load.

NOTE 3: The signalling impacts of Providing user location information (ULI) received over N4 and on NWDAF receiving UPF notifications for UE(s) that are not in the AoI needs to be assessed.

5. UPF starts the measurement for the PDU Session as requested.

6. UPF sends Nupf\_EventExposure Notify for Event= UserDataUsageMeasures / UserDataUsageTrends for the PDU Session. The notification includes SUPI, DNN and S-NSSAI as available and conveys measurement information according to the subscription.

7. NWDAF derives the Requested Analytic.

8. NWDAF provides the Analytic requested.

### 6.7.4 Impacts on services, entities and interfaces

This solution impacts the System as follows:

- Nupf Event Exposure Service is enhanced with two new events and a subscription operation for those events:

- The target of the subscription to these events may be "any UE", a SUPI, or a given User PDU Session (identified by UE IP address and DNN or N4 Session ID). DNN and S-NSSAI and AoI can be included as filter conditions.

- The subscription request also includes Event Reporting Information (including required DataSubset (Volume Measurement and/or Throughput Measurements or Throughput Statistic Measurement), Control Information for the measurements (like granularity) and Reporting and Notification Control Information for the event.

- Nupf Event Exposure service Notification provides information for a user PDU Session identified by UE IP address and DNN (and/or N4 Session ID) and includes SUPI and S-NSSAI when available.

- Nsmf Event Exposure service subscription notification includes UPF PDU Session identifier and UPF Event Exposure service contact information. If needed, information of whether UPF is acting as PSA and DNAI could also be provided.

NOTE: Decision is left for stage 3 for whether enhancing notifications of already specified events or defining a new SMF event.

For new UserDataUsageMeasures event, it includes:

- Volume Measurement: measures of data volume exchanged (UL, DL and/or overall) and/or number of packets exchanged (UL, DL and/or overall) with or without application granularity. This measurement can also include number of packets transmitted and retransmitted for applications where that is possible to differentiate.

- Throughput Measurement: measures of data throughput (UL and DL) aggregated for the PDU Session or per application.

For new UserDataUsageTrend event, it includes:

- Throughput Statistic Measurement (average and/or peak throughput) over the measurement period for the PDU Session or per application.

And for both events, it includes measurement context (for example, time stamps for the packets and the measures) and when the information refers to an application, the corresponding Application Id or Packet Filter Set.

- UPF is enhanced to produce measurements according to UserDataUsageMeasures event and UserDataUsageTrends event and to send notifications as instructed in the subscription.

- SMF is enhanced to provide ULI (TA) to UPF over N4. UPF is enhanced to map PDU sessions to an AoI with TA granularity based on N4 ULI and to determine which PDU Sessions are for users with an AoI.

- NWDAF is enhanced to collect Data Usage measurements from UPF with UPF Event Exposure Service Subscription using UserDataUsageMeasures / UserDataUsageTrends event. It receives Nupf Event Exposure notifications for UserDataUsageMeasures / UserDataUsageTrends event with information as requested, and correlates information from different sources to produce Analytics.

## 6.8 Solution #8: Support to existing (Rel‑16-Rel‑17) data analytics with QoS Flow level measurements

### 6.8.1 Key Issue mapping

This is a solution for KI#2.

### 6.8.2 Description

This solution extends Rel-17 UPF Exposure Service QoS Monitoring event, with additional measurements of QoS Flow level performance information for a User PDU Session and QoS Flow. Besides, the QoS Monitoring measurement, this event can provide:

- QoS Flow Bandwidth measurements: It provides bitrate measurements (UL, DL and/or overall) for a PDU Session and QoS Flow.

NOTE 1: This event can be extended with other QoS Flow performance measurements in the future when available and required.

With this extension, the NWDAF requirements on UPF event exposure service(s) to collect performance data of PDU Session QoS Flows are satisfied as follows:

- Observed Service Experience: using the QoS monitoring event and from that, QoS Monitoring Measurement and/or QoS Flow Bandwidth measurements for the PDU Session and QFI as requested. See NOTE 2.

NOTE 2: UPF awareness of Packet transmission and retransmission depends on the specific application transport protocol. Number of Packet transmission and retransmission can't be measured for a QoS Flow in UPF due to this limited visibility. The observed number of packets transmitted/retransmitted or a retransmission rate measurement can be considered in UPF event exposure for User PDU Session service data usage for applications with transport protocols that allow so. This has been considered in Solution 7.

In this solution, the subscription to QoS monitoring event goes via SMF which simplifies the procedure and guarantees aligned selection decisions for data collection from UPF and SMF.

SMF determines the PDU Sessions and UPFs impacted by this request and determines the QFI of QoS Flows to be monitored (for example the QFI for the PDU Session and Application).

When packet delay for QoS Flows measurement is requested, SMF can decide whether this subscription influences QoS Monitoring activation and how. SMF may activate QoS Monitoring. SMF may only update activation towards UPF with direct reporting information. SMF sends Session Reporting Rules to UPF with Control Information for the measurements and with Direct Reporting information accordingly.

UPF notifies the QoS Monitoring event directly to NWDAF as instructed. It provides Measurements as requested (QoS Monitoring Measurement and/or QoS Flow Bandwidth measurements) including for which QFI they have been performed.

### 6.8.3 Procedures

This procedure provides NWDAF with QoS Flow level Measurements for a User PDU Session.



Figure 6.8.3-1: Procedure for Data Collection of QoS Flow Performance measurements from UPF. Example Use case for Observed Service Experience Analytic (clause 6.4 of TS 23.288 [5])

The procedure is as follows:

1. NWDAF receives an Analytics Info Request that requires UPF Data collection, in this example, for Service Experience (OSE) for an Application Id. For example, that could be for a UP Path (DNAI) for a specific UE and for certain DNN and S-NSSAI.

2. NWDAF determines the data collection needed, in this case, QoS Flow Performance Data and other data network information from NF providers and from AF, as specific in clause 6.4 of TS 23.288 [5]. NWDAF selects the entities that provide input data, including the SMF for the Subscription to UPF QoS Flow performance Data.

NOTE 1: How NWDAF selects SMF is specified in clause 6.2.2 of TS 23.288 [5]. including how any filter for Area of Interest (AOI) is considered for SMF selection (and by SMF for PDU Session Selection). If NWDAF subscription to SMF is for a UE or UE Group, NWDAF may subscribe indirectly via UDM. If it is for "Any UE", it subscribes directly to SMF.

NOTE 2: An operator should use "any UE" with caution, since per flow monitoring of a large amount of flows could have impact on UPF performance.

3. NWDAF sends a Nsmf\_Event Exposure Subscribe Operation to SMF for QoS Monitoring Event. The request includes the event filters (target (for example SUPI) and other like DNN, S-NSSAI, DNAI and AppId) and event Reporting Information (required DataSubset (QoS Monitoring Measurement and/or QoS Flow Bandwidth Measurements), Control Information for the measurements and Reporting and Notification Control Information).

4. SMF Selects the target PDU Session. SMF also determines the UPF that has to perform the measurements (DNAI if provided is considered at this stage) and the QFI of QoS Flows to be monitored (e.g. QFI allocated to the Application in the PDU Session).

5-6. SMF can decide whether this subscription influences QoS Monitoring activation and how. SMF may activate QoS Monitoring. SMF may only update previous activation providing UPF with direct reporting information. SMF sends a Session Modification update towards UPF with Session Reporting Rules including Control Information for QoS Monitoring Measurements and/or QoS Flow Bandwidth Measurements and Direct Reporting information.

7. UPF performs the QoS Flow measurements as required with AN assistance when needed.

8. QoS Flow Level measurements trigger a Nupf Event Exposure Notification towards NWDAF according to the Control Information received. The Notification is for a PDU Session and QoS Flow and includes among other QoS Monitoring Measurement and/or QoS Flow Bandwidth Measurements with corresponding QFI.

9. NWDAF derives the requested Analytics for the data that it has collected.

10. NWDAF sends a Response to the Analytics Info Request with the Estimated Experience for the User and Application on the UP Path.

### 6.8.4 Impacts on services, entities and interfaces

This solution impacts the System as follows:

- Nsmf Event Exposure Subscription needs to be enhanced:

- It is enhanced to support subscription to QoS Monitoring event, so NWDAF as consumer can collect data of QoS Flow performance. The target of the subscription to this event may correspond to a UE ID (SUPI), an Internal Group Identifier, or may include a "Any UE" indication. Event Filters are used to specify the conditions for notifying the events. Example parameters for this event are DNN, S-NSSAI, DNAI, Application Identifier.

- The subscription includes also additional Event Reporting. Information, including the required DataSubset (QoS Monitoring Measurement and/or QoS Flow Bandwidth Measurements), Control Information for the measurements and Reporting and Notification Control Information).

- PFCP Session Establishment/Modification is enhanced as follows:

- Session Reporting Rules (SRR) are enhanced to support new type of session data to report for Direct Reporting. Rules are enhanced to provide new Control for QoS Monitoring per QoS Flow for the QoS Flow Bandwidth Measurements. Direct Reporting is always provided.

- Control for QoS Flow Bandwidth Measurements includes QFI, requested measurements (UL, DL and/or overall bitrate), Reporting Frequency (for example, by event or periodic) and complementary information as needed, like thresholds to trigger reporting, or measurement period (periodic reporting).

- SMF is enhanced as follows:

- To support the described Subscription to QoS Monitoring event, select the relevant PDU Session, and determine the Session Reporting Rules, including the described enhancements. SMF sends these Rules to UPF in PFCP Session Establishment/Modification message to activate monitoring and reporting towards NWDAF.

- UPF is enhanced as follows:

- To support the new information in Session Reporting Rule, perform the requested measurements and trigger notifications according to these rules. It sends the notification as instructed by Direct Reporting Information. It supports the enhancements in Nupf Event Exposure Notification for QoS Monitoring event including for QoS Flow Bandwidth Measurements (see below).

- Nupf Event Exposure Notification for QoS Monitoring event is enhanced as follows:

- It is extended to convey QoS Flow Bandwidth measurements (UL, DL and/or overall bitrate) including the QFI for which the measurement has been performed.

NOTE: Additional measurements may be provided in the future (as an example, with QoS Flow retransmission rate measurements) and services/interfaces should allow such extensions.

- NWDAF is enhanced as follows:

- To collect QoS Flow level performance measurements from UPF subscribing to SMF Event Exposure Service Subscription for QoS Monitoring event. It receives Nupf Event Exposure notifications for QoS Monitoring event with the Measurements for QFIs, and correlates information from different sources to produce Analytics.

## 6.9 Solution #9 to Key Issue 2: NWDAF collects information from UPF by event exposure

### 6.9.1 Mapping table between Analytics ID and the related information collection in UPF

According to TS 23.288 [5], some of the Analytics ID in NWDAF needs the information from UPF.

The details of the information are listed in Table 6.9.1.

Table 6.9.1: Analytics ID and the related information collection from UPF

|  |  |  |  |
| --- | --- | --- | --- |
| Information | Source | Analytics ID | Description |
| QoS flow Bit Rate | UPF | Service Experience | The observed bit rate for UL direction; and  The observed bit rate for DL direction. |
| QoS flow Packet Delay | UPF |  | The observed Packet delay for UL direction; and  The observed Packet delay for the DL direction. |
| Packet transmission | UPF |  | The observed number of packet transmission. |
| Packet retransmission | UPF |  | The observed number of packet retransmission. |
| Traffic usage report | UPF | NF load | Report of user plane traffic in the UPF for the accumulated usage of network resources (see TS 29.244 [8]) |
| UE communication (1..max) | UPF, AF | UE communication | Communication description per application |
| >Communication start |  |  | The time stamp that this communication starts |
| >Communication stop |  |  | The time stamp that this communication stops |
| >UL data rate |  |  | UL data rate of this communication |
| >DL data rate |  |  | DL data rate of this communication |
| >Traffic volume |  |  | Traffic volume of this communication |
| PDU Session ID (1..max) | SMF |  | Identification of PDU Session. |
| > N4 Session ID | SMF,UPF |  | Identification of N4 Session. |
| > Inactivity detection time | SMF,UPF |  | Value of session inactivity timer. |
| Application ID | UPF or AF | User Data Congestion | Application identifier as defined in TS 23.501 [2] clause 5.8.2 (see NOTE 1). |
| IP Packet Filter Set | UPF or AF |  | IP Packet Filter set as defined in TS 23.501 [2] clause 5.8.2 (see NOTE 1). |
| Measurement period | UPF or AF |  | Measurement period. |
| Throughput UL/DL | UPF or AF |  | Average Throughput UL/DL over the measurement period. |
| Throughput UL/DL (peak) | UPF or AF |  | Peak Throughput UL/DL over the measurement period. |
| Timestamp | UPF or AF |  | Time when measurements are taken. |
| Achieved sampling ratio | UPF |  | Sampling ratio achieved by UPF (see NOTE 2). |
| UE IP address | UPF | UE Dispersion | UE IP address. |
| Timestamp | UPF |  | A timestamp of the collected information. |
| Application ID | UPF |  | Identify the application at the UPF. |
| IP 5-tuple | UPF |  | IP 5-tuple. |
| Location of Application | UPF |  | List of Internet applications represented by DNAI(s). |
| Data Volume UL/DL | UPF |  | Sum of UE data volume exchanged per application during the period. |
| Application duration | UPF |  | Duration for the application (e.g. Voice talk time). |
| UE communications (1..max) | UPF | WLAN Performance | List of communication time slots |
| > Communication start |  |  | The time stamp that PDU session(s) for WLAN starts. |
| > Communication stop |  |  | The time stamp that PDU session(s) for WLAN ends. |
| > UL data rate |  |  | UL data rate of PDU session(s) for WLAN. |
| > DL data rate |  |  | DL data rate of PDU session(s) for WLAN. |
| > Traffic volume |  |  | Traffic volume of PDU session(s) for WLAN. |

### 6.9.2 Service based UPF event exposure

**Service description:** This service provides events related to PDU Sessions towards consumer NF. The service operations exposed by this service allow other NFs to subscribe and get notified of events happening on UPFs. The following are the key functionalities of this NF service.

NOTE 1: In Rel‑18, the only consumers of UPF event exposure is SMF and NWDAF when collecting data for network data analytics from NWDAF.

- Allow consumer NFs to directly subscribe and unsubscribe for an Event ID on UPF;

- Allow the NWDAF to collect data indirectly for network data analytics;

- Notifying events on the UPF to the subscribed NFs; and

- Allow consumer NFs to acknowledge or respond to an event notification.

The following events can be subscribed by a NF consumer (Event ID is defined in clause 4.15.1):

- QoS flow Bit Rate.

- QoS flow Packet Delay.

- Packet transmission.

- Packet retransmission.

- Traffic usage report.

- Communication start and stop (3GPP access or WLAN access).

- UL/DL data rate (3GPP access or WLAN access).

- Traffic volume (3GPP access or WLAN access).

- Throughput UL/DL.

- Throughput UL/DL (peak).

- Timestamp.

- Achieved sampling ratio.

According to the Analytic ID from consumer, the NWDAF can decide which kind of information should be collect from UPF in the form of event ID. And then, the NWDAF triggers subscription request towards SMF which controls of the dedicated UPF that data generation, and the SMF determines the UPF and sends data collection request to UPF. According to the event ID, the UPF collects the data and exposes the related information to NWDAF directly.

### 6.9.3 Procedure

#### 6.9.3.1 UPF data collection for single UE



Figure 6.9.3.1-1: Data collection for single UE from service based UPF

0. The UPF registers to SMF with the supported event exposure which represented by event ID(s) via N4 Association Setup procedure.

1. The analytics consumer sends a request to the NWDAF for analytics on a specific UE, using either the Nnwdaf\_AnalyticsInfo or Nnwdaf\_AnalyticsSubscription service. The NF can request statistics or predictions or both. The type of analytics is set to either of the Analytics ID defined in TS 23.288 [5]. The NF provides the UE id in the Target of Analytics Reporting. Analytics Filter Information optionally contains DNN, S-NSSAI, Area of Interest, etc.

2. The NWDAF determines the event ID of UPF event exposure according to Analytics ID. Each event ID represents the data needed to be collected from UPF. For example, if consumer requests for the service experience analytic, the NWDAF can decide event ID is Service Experience, and the data needed to be collected from UPF are: QoS flow Bit Rate, QoS flow Packet Delay, Packet transmission, Packet retransmission.

3. The NWDAF sends Nudm\_UECM\_Get\_Request(SUPI, type of requested information set to SMF Registration Info and the S-NSSAI and DNN) to UDM to get the SMF ID that serving the target UE.

4. The UDM provides the SMF id and the corresponding PDU Session id, S-NSSAI, DNN using Nudm\_UECM\_Get\_Response to the NWDAF.

5. The NWDAF sends Nsmf\_EventExposure\_Subscribe to the SMF, including the Event ID of UPF event exposure determined by NWDAF in step 2 and additional Direct Reporting indicating that the UPF should send the event notifications directly to NWDAF. The NWDAF requests SMF to represent NWDAF to perform data collection from UPF.

6. The SMF responses to NWDAF for subscription.

7. The SMF determines the UPF that serves the UE, according to PDU session id, UE id, and possibly S-NSSAI and DNN.

8. The SMF performs Nupf\_EventExposure\_Subscribe request to the UPF that determined in step 7 for data collection from UPF. In the request, the following parameters are included: PDU session id, Event ID that represents the kind of data needs to be collect, NWDAF IP address, DNN, S-NSSAI, UE id. Each of the data is represented by Event ID, for example, Event ID = QoS flow Packet Delay. The UPF receives several Event ID, and collects the corresponding data. All of the Event ID and corresponding data constructs the analytics in NWDAF.

If the UPF doesn't support some of the event ID(s) according to the step 0 or Direct Reporting is not enabled from the NWDAF in the step 5, the related data will be collected via N4 procedure between SMF and UPF. Then, the SMF may notify NWDAF of the event report using Nsmf\_EventExposure\_Notify.

9. The UPF responses with subscription request.

10. The UPF sends the notification related with Event ID data collection information over Nupf\_EventExposure\_Notify service operation. The notification is sent to Notification Target Address that may correspond to the NWDAF.

11. The NWDAF derives requested analytics, in the form of statistics or predictions or both.

12. NWDAF to NF: Nnwdaf\_AnalyticsInfo\_Request response or Nnwdaf\_AnalyticsSubscription\_Notify.

The NWDAF provides requested analytics to the NF consumer, using either Nnwdaf\_AnalyticsInfo\_Request response or Nnwdaf\_AnalyticsSubscription\_Notify, depending on the service used in step 1.

#### 6.9.3.2 UPF data collection for any UE

Different from the data collection for single UE, for the any UE situation, the UPF which the UEs are served for is not the single one. But for a specific Analytics ID, the destination IP address, DNN, DNAI, S-NSSAI etc. can be used to determine the potential UPFs that serves the UE that meets the requirements, for example, the UEs that in the same slice or access the same DNN or IP address.



Figure 6.9.3.2-1: Data collection for single UE from service based UPF

For example in Figure 6.9.3.2-1, the NF consumers request the service experience towards the application server 1 for any UE. In the whole PLMN, the NWDAF should select out the UEs which has connection to AS-1 and determines the related UPF to collect data. But unlike in the single UE scenarios, the related SMF can be discovered in UDM by subscription data, for the any UE situation, the SMF which is responsible for the session management for the UEs to access DNN or application server IP address should be discovered by other means.



Figure 6.9.3.2-2: Data collection for any UE from service based UPF

0. The UPF registers to SMF with the supported event exposure which represented by event ID(s) via N4 Association Setup procedure. This procedures may be repeated between different UPF and SMF.

1. The analytics consumer sends a request to the NWDAF for analytics on any UE, using either the Nnwdaf\_AnalyticsInfo or Nnwdaf\_AnalyticsSubscription service. The NF can request statistics or predictions or both. The type of analytics is set to either of the Analytics ID defined in TS 23.288 [5]. The NF provides the any UE in the Target of Analytics Reporting. Analytics Filter Information optionally contains DNN, S-NSSAI, Area of Interest, Application IP address, APP ID, DNAI and etc.

2. The NWDAF determines the event ID of UPF event exposure according to Analytics ID. Each event ID represents the data needed to be collected from UPF. For example, if consumer requests for the service experience analytic, the NWDAF can decide event ID is Service Experience, and the data needed to be collected from UPF are: QoS flow Bit Rate, QoS flow Packet Delay, Packet transmission, Packet retransmission.

2a. If the information provided by NF consumer only includes application server address and it can’t be directly used for SMF discovery in NRF, the NWDAF should recover the DNAI first from NEF/UDR. If the DNAI does not exist in the Nnwdaf\_AnalyticsInfo request or Nnwdaf\_AnalyticsSubscription request in step 1 and only the Application Server Address(es) exists in request, the NWDAF decides that Application Server Address(es) can’t be directly used in SMF discovery in NRF and obtain the target DNAI from 5GC by the mapping table between Application IP range/address and DNAI based on the conclusion of TR 23.700-48 [10]. So, the NWDAF sends request to NEF to obtain DNAI by providing EAS IP/IP range and/or FQDN. NEF responds to the NWDAF directly if DNAI is stored in NEF locally or the NEF recovers the DNAI from UDR. After obtaining the DNAI from NEF, the NWDAF triggers the SMF discovery in NRF using the DNAI in any UE situation. The details services between NWDAF and NEF, and the details between NEF and UDR should be coordinated with R18 EGDE item.

3. Due to the analytic is for any UE, the related SMF should be discovered first. In the scope of any UE, the potential UEs that related to the analytics ID has the same features below:

- Connect to the same application server IP address.

- Connect to the same S-NSSAI.

- Connect to the same DN.

The NWDAF discovers a set of SMF instances by Nnrf\_NFDiscovery request towards NRF according to the common features of UEs that the analytics ID refers to, including DNN, S-NSSAI, Area of Interest, Application IP address, APP ID, DNAI. This request is responsible for discovery all of the SMFs that controls the UE which coordinates with the conditions in analytics requests to NWDAF.

If the area of interest is existing in the Nnwdaf\_AnalyticsInfo request or Nnwdaf\_AnalyticsSubscription request in step 1, this information can be transformed to the Service Area of SMF for SMF discovery to NRF.

NOTE: The mechanism of mapping table between application IP address/range and target DNAI needs to be coordinated with R18 eEDGE phase 2 item.

4. The NRF responses with several SMF ID, SMF IP address that controls the UE which coordinates with the conditions in analytics requests to NWDAF.

5. The NWDAF sends several Nsmf\_EventExposure\_Subscribe requests to the several of SMFs discovered by NRF, including the Event ID of UPF event exposure set to in step 2 and additional Direct Reporting indicating that the UPF should send the event notifications directly to NWDAF, and other parameters used to determine UPF including DNN, S-NSSAI, Area of Interest, Application IP address, APP ID, DNAI. The NWDAF requests these SMFs to represent NWDAF to perform data collection from UPF.

6. All these SMFs should determine the UPF which serves the UEs accord with the condition of DNN, S-NSSAI, Area of Interest, Application IP address, APP ID, DNAI.

7. The several SMFs performs Nupf\_EventExposure\_Subscribe request to each UPFs individually that determined in step 6 for data collection from UPF. In the request, the following parameters are included: PDU session id, Event ID that represents the kind of data needs to be collect, NWDAF IP address, DNN, S-NSSAI, Area of Interest, Application IP address, APP ID, DNAI.

If the UPF doesn't support some of the event ID(s) according to the step 0 or Direct Reporting is not enabled from the NWDAF in the step 5, the related data will be collected via N4 procedure between SMF and UPF. Then, the SMF may notify NWDAF of the event report using Nsmf\_EventExposure\_Notify.

Editor's note: For the any UE scenarios, how to reduce the multiple notification message of data collections from UPF is FFS.

8. The UPF responses with subscription request.

9. The each of UPF sends the notification related with Event ID data collection information over Nupf\_EventExposure\_Notify service operation. The notification is sent to Notification Target Address that may correspond to the NWDAF.

10. The NWDAF derives requested analytics, in the form of statistics or predictions or both.

11. NWDAF to NF: Nnwdaf\_AnalyticsInfo\_Request response or Nnwdaf\_AnalyticsSubscription\_Notify.

The NWDAF provides requested analytics to the NF consumer, using either Nnwdaf\_AnalyticsInfo\_Request response or Nnwdaf\_AnalyticsSubscription\_Notify, depending on the service used in step 1.

### 6.9.4 Impacts on services, entities and interfaces

UPF:

- Newly introduced UPF Services and UPF Service Operations to support SMF or NWDAF to collect data.

- Newly defined Event ID to the available data in UPF.

- Expose UPF related data collection information to NWDAF directly.

SMF:

- Represent NWDAF to request UPF to collect dedicated data.

- Consumer of UPF services for data collection.

- Determine the UPF that serves the target UEs in the scope of any UE according to parameters of NWDAF IP address, DNN, S-NSSAI, Area of Interest, Application IP address, APP ID, DNAI.

NRF:

- Discovery of several SMFs that accords with the parameters that related to the UEs.

NWDAF:

- Sends the AS IP/IP range and/or FQDN to NEF to retrieve the corresponding DNAI.

- Responsible to transfer the area of interests from NF consumer to SMF service area for SMF discovery in NRF.

NEF:

- NEF responds to the NWDAF directly if DNAI is stored in NEF locally or the NEF recovers the DNAI from UDR.

## 6.10 Solution #10: UPF event exposure service to NWDAF

### 6.10.1 Key Issue mapping

This solution addresses KI 2.

### 6.10.2 Description

Annex A of this TR has analysed the NWDAF requirements of UPF event exposure, which contains seven aspects of information. In this solution, the NWDAF subscribes to the UPF data via the SMF, and the UPF directly sends the collected UPF data to NWDAF.

### 6.10.3 Procedures



Figure 6.10.3-1: UPF Information Exposure to NWDAF

For case 1, where the NWDAF requests UPF information Exposure for a certain UE or a group of UEs, step1 and 2 are as follows:

1. The NWDAF invokes Nudm\_UECM\_Get service operation to retrieve the appropriate SMF by providing UE ID and NF type.

2. The UDM provides a Nudm\_UECM\_Get response to the NWDAF with the corresponding SMF.

For case 2, where the NWDAF requests UPF information Exposure for a certain AOI, steps 1 and 2 are as below:

1. The NWDAF discovers the SMF instances by invoking Nnrf\_NFDiscovery request with UPF Event Exposure Service towards NRF, including Area of Interest, to get the SMF which has the capability to subscribe to UPF on behalf of NWDAF for UPF information reporting.

NOTE: For UPF, "UPF Event Exposure Service" indicates that the UPF supports information reporting. For SMF, "UPF Event Exposure Service" indicates that the SMF supports to subscribe to UPF on behalf of NWDAF for UPF information reporting.

2. The NRF responses with SMF ID and SMF IP address to NWDAF.

3. The NWDAF sends the request to the SMF to subscribe UPF data, including the following information:

- Notification Target Address (NWDAF address).

- Indication of UPF Event Exposure Service.

- Event Filter Information: S-NSSAI, Application Id, Area of Interest.

- Target of Event Reporting: a UE or a group of UEs or any UE.

- Subscription Information:

- UL/DL Throughput, UL/DL packets or number of connections.

- N3 delay, N6 delay, E2E delay, UL/DL packet loss, or UL/DL packet retransmission.

- UL/DL Data Volume.

4a. For case 2, the SMF discovers the UPF instance by invoking Nnrf\_NFDiscovery request with UPF Event Exposure Service towards NRF, including Area of Interest, to get the UPF which supports user plane data reporting. And the NRF responses with UPF IP address to the SMF.

4b. For case 2, the SMF subscribes to AMF by invoking Namf\_EventExposure\_Subscribe with Event "Number of UEs present in a geographical area" to get the UE list 1 in the AOI.

4c. SMF locally determines the UE list 2 for user plane data reporting which is included in the Target of Event Reporting sending to UPF.

If the Target of Event Reporting from NWDAF is a UE or a group of UEs, the SMF determines UE list 2 for user plane data reporting which locate(s) in the AOI by matching the UE or group of UEs from Target of Event Reporting with the UE list 1 from AMF in step 4b.

If the Target of Event Reporting from NWDAF is any UE, the UE list 2 is the UE list 1 from AMF in step 4b.

4. The SMF sends the request to the UPF over N4 Session Establishment Request/Response message including the NWDAF address, Event Filter Information, Target of Event Reporting, and Target Subscription Information. For case 1, Target of Event Reporting is the certain UE or the group of UEs same as step 1, For case 2, Target of Event Reporting is the UE list 2 from step 4c.

5. The UPF responds with the locally collected UPF data by invoking Nupf\_EventExposure\_Notify service operation to the NWDAF.

6a. For case 2, the SMF keeps monitoring to update UE list 1 by invoking Namf\_EventExposure\_Subscribe with Event "UE moving in or out of Area of Interest".

6b. The SMF determines the updated UE list 2 for user plane date reporting same as step 4c with the result from AMF from step 6a.

6c. The SMF sends the request to the UPF over N4 Session Modification Request/Response message including the Target of Event Reporting which is the updated UE list from step 6b. And the UPF responds to SMF same as step 5.

### 6.10.4 Impacts on services, entities and interfaces

UPF:

- Support newly defined UPF Service to collect UPF data.

- Expose UPF related data collection information to NWDAF.

- Support new indication "UPF Event Exposure Service" and registration to NRF.

SMF:

- Represent NWDAF to request UPF to collect UPF data.

- Consume UPF service for data collection.

- Support new indication "UPF Event Exposure Service" and registration to NRF.

NRF:

- Support new indication "UPF Event Exposure Service" registration from SMF and UPF.

## 6.11 Solution #11: UPF event exposure service to NWDAF subscribed directly from UPF

### 6.11.1 Key Issue mapping

This is a solution for KI#2.

### 6.11.2 Description

Annex A of this TR has analysed the NWDAF requirements of UPF event exposure service, which contains the following seven aspects of information:

1. QoS flow level Network Data from 5GC NF related to the QoS profile assigned for a particular service (identified by an Application Id or IP filter information), including QoS flow Bit Rate, QoS flow Packet Delay, Packet transmission, and Packet retransmission.

2. Data collected by NWDAF for UPF load analytics (i.e. Traffic usage report), and service data from 5GC related to UE communication (e.g. UE communications, N4 Session ID, and Inactivity detection time).

3. Data Collected from the UPF or from the AF related to User Data Congestion Analytics, e.g. Application ID, IP Packet Filter Set, Measurement period, Throughput UL/DL, Throughput UL/DL (peak), Timestamp, and Achieved sampling ratio.

4. UE data volume dispersion collected from serving UPF, e.g. UE UP address, Timestamp, Data Volume UL/DL, Application ID, IP 5-tuple, Location of Application, and Application duration.

5. User plane performance analytics for a specific Edge Computing application for a UE, group of UEs, or any UE over a specific serving anchor UPF/DNAI/Edge Application Server Instance.

6. Data collected by NWDAF for WLAN performance analytics, e.g. UE communications.

### 6.11.3 Procedures

For the analytics targeting PDU session related information of a specific UE, e.g. QoS flow level Network Data, UE data volume dispersion, User plane performance analytics for a specific Edge Computing application, the NWDAF can find the UPF by using SUPI, S-NSSAI, and DNN via UDM and SMF, as described in Solution 1.

For the analytics targeting "any UE" (possibly for specific DNN and or slices), e.g. Data collected by NWDAF for UPF load analytics, User Data Congestion Analytics, Data Volume dispersion analytics, WLAN performance analytics, the NWDAF can find the UPF by using S-NSSAI, DNN, or DNAI from NRF that has the UPF registration information, as described in Solution 1.



Figure 6.11.3-1: UPF Information Exposure to NWDAF

1. The NWDAF find the UPF(s) according to the specific use case.

For the analytics targeting PDU session related information of a specific UE, e.g. QoS flow level Network Data, UE data volume dispersion, User plane performance analytics for a specific Edge Computing application, the NWDAF can find the UPF by using SUPI, S-NSSAI, and DNN via UDM and SMF, as described in Solution 1.

For the analytics targeting "any UE" (possibly for specific DNN and or slices), e.g. Data collected by NWDAF for UPF load analytics, User Data Congestion Analytics, WLAN performance analytics, the NWDAF can find the UPF(s) by using AoI, S-NSSAI, DNN, or DNAI from NRF that has the UPF registration information, as described in Solution 1.

2. The NWDAF sends the request for requesting the collected data over Nupf\_EventExposure\_Subscribe service operation to the UPF(s). For the "Any UE" scenarios, the request is sent to the relevant UPF(s) including filters like S-NSSAI, DNN, or AoI.

NOTE: For the any UE scenarios, different UEs may be served by different UPFs. For the subscription to the same UPF, the UPF will concatenate the collected data of its serving UE into one notification reply message. Therefore, only one notification message of data collections will be sent for "any UE" filtered by specific DNN and/or slices which served by the same UPF.

If the subscription has included AoI, the UPF need to determine which UEs are in the AoI and whether the UEs are entering/leaving the AoI according to user location information (ULI) received from SMF over N4.

3. The UPF selects the PDU Sessions that match the filters and responds the requested collected data for the selected PDU Sessions over Nupf\_EventExposure\_Notify service operation to the NWDAF.

### 6.11.4 Impacts on services, entities and interfaces

UPF:

- Newly introduced UPF Service Operations to support NWDAF to subscribe the UPF event exposure service directly.

- Expose UPF related data collection information to NWDAF directly.

SMF:

- ULI (User location Information) is provided by SMF to UPF over N4.

## 6.12 Solution #12: UPF registration to the NRF and NWDAF collecting data from UPF

### 6.12.1 Key Issue mapping

This Solution addresses KI#1 and KI#2.

### 6.12.2 Description

Regarding to UPF event exposure service, the UPF may support different mechanism of data collection and data reporting per UPF data type, which can be identified with UPF Event IDs. Some of these Event IDs are suitable for direct subscriptions from the NF consumer to the UPF, but some of them are more suitable for indirect subscriptions to the UPF via SMF. For example:

- Some UPF event IDs such as UPF measurement or detection data per UE controlled by N4 session, it is more appropriate for them to be subscribed by the consumer to the UPF via SMF.

- On the other hand, some UPF event IDs such as UPF load, Traffic usage report UPF measurement or detection data for any UE or some aggregated data for any UE, they are more appropriate to be subscribed by the consumer to the UPF directly without disturbing the SMF.

In this solution, UPF registration to NRF procedure can be enhanced:

- The UPF registers to the NRF with information including Supported Event ID(s), direct subscription indication and/or indirect subscription indication.

- The direct subscription indication indicates the UPF supports NF consumer subscribe data directly from it, and the indirect subscription indication indicates the UPF supports NF consumer subscribe data from it via the SMF.

- For direct or indirect subscription, the NF profile can also include the corresponding event ID (s).

When the NF consumer (e.g. NWDAF) discovers the UPF from the NRF, the NRF determines appropriate UPF(s) matching the input parameters from the NF consumer (e.g. NWDAF), and feedbacks the NF consumer

- the UPF instance ID + Direct Subscription indication within corresponding UPF NF profile;

- or Indirect Subscription indication within corresponding UPF NF profile.

Then, the NWDAF subscribes to the UPF directly or indirectly based on the NF discovery outputs from NRF, which are specified in the procedure in clause 6.12.3.2.

### 6.12.3 Procedures

#### 6.12.3.1 Procedure for UPF Registration to NRF

Regarding UPF Registration to NRF, the procedure is same with clause 6.1.2.1: UPF Event Exposure service Registration, except the following change in step 1:

The UPF NF profile parameters in addition include direct subscription indication and/or indirect subscription indication:

- The direct subscription indication indicates the UPF supports NF consumer subscribe data directly from it, and the indirect subscription indication indicates the UPF supports NF consumer subscribe data from it via the SMF.

- For direct or indirect subscription, the NF profile can also include the corresponding event ID (s), and for the indirect subscription.

#### 6.12.3.2 Procedure for NWDAF collecting data from UPF



Figure 6.12.3.2-1: NWDAF collects data from UPF procedure

1. NWDAF that requires UPF data invokes Nnrf\_NFDiscovery\_Request message to NRF to find appropriate UPF(s), including target NF service Name (i.e. UPF Event Exposure Service), AOI, target NF type (i.e. UPF), Event ID, S-NSSAI, DNN, DNAI.

2. The NRF determines one or more appropriate UPF(s) matching the input parameters included in the Nnrf\_NFDiscovery\_Request. The NRF sends the NF discovery outputs to the NWDAF.

The output includes one or more UPF instances, and for each UPF instance it includes UPF NF profile:

- If a UPF supports NF consumer subscribes the event ID directly from it, the feedback UPF NF profile includes Direct Subscription indication in it.

- If a UPF supports NF consumer subscribes the event ID from it via SMF, the feedback UPF NF profile includes Indirect Subscription indication.

The NWDAF subscribes to the UPF directly or indirectly based on the NF discovery outputs from NRF.

3. For the discovered UPF instance with Direct Subscription indication in the UPF NF profile, the NWDAF subscribes to the UPF for the event ID by invoking Nupf\_EventExposure Subscribe.

4. For the discovered UPF instance with Indirect Subscription indication in the UPF NF profile, the NWDAF discovers the SMF as described in solution 10 for a certain UE scenario or a certain AOI scenario, and then the NWDAF subscribes to the SMF by invoking Nsmf\_EventExposure\_Subscribe for the event ID of UPF. Then the SMF on behalf of the NWDAF performs data collection from UPF with N4 procedure.

The UPF responds the requested collected data over Nupf\_EventExposure\_Notify service operation to the NWDAF.

### 6.12.4 Impacts on services, entities and interfaces

UPF:

- Registers to the NRF with information including direct subscription indication and/or indirect subscription indication.

NRF:

- The NRF registers for the UPF with information including direct subscription indication and/or indirect subscription indication.

- The NRF discovers appropriate UPF(s) matching the input parameters from the NF consumer (e.g. NWDAF), and feedbacks the NF consumer the UPF instance ID with corresponding UPF NF profile, which includes Direct Subscription indication or Indirect Subscription indication.

UPF data consumer (e.g. NWDAF):

- Subscribes to the UPF directly or indirectly based on the NF discovery outputs from NRF.

## 6.13 Solution #13: Subscription to UPF Event Exposure Services in the event of UP Path change

### 6.13.1 Key Issue mapping

This solution addresses KI#2.

### 6.13.2 Description

This solution aims to provide a mechanism of subscribing to the Target UPF in the perspective of the Consumer NF when either a UPF is relocated or an I-UPF is inserted.

While subscribing to UPF's Event Exposure Service, consumer NF can indicate to the subscribed UPF (source UPF) the following:

1. An indication of notifying the information of new UPF (in case UPF is relocated, or a additional UPF is added for the PDU Session path), or,

2. An indication to subscribe to the new UPF on behalf of it.

The Source UPF may then subscribe to the relevant SMF for notification of UP path change. The SMF then informs the Target UPF instance ID and other relevant information to the Source UPF.

The rest of the solution is described in the next section.

Editor's note: Although the proposed solution utilizes SMF event Exposure service for getting the target UPF information; we can discuss solutions which leverages N4 for the required task.

### 6.13.3 Procedures



Figure 6.13.3.1: Overview of procedure

A description of the procedure in Figure 6.13.3.1 is as follows:

0. The consumer NF subscribes to Source UPF for event exposure services. In the request it provides indication for:

A. Indication for getting Target UPF info in case of UPF relocation.

B. Indication of subscribing to target UPF on behalf of the consumer NF in case UPF relocation happens.

1. UPF subscribes for event notification for UPF relocation for the relevant PDU Session.

2. SMF decides for UPF relocation for the relevant PDU Session.

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

4. Based on the subscription request in Step. 0, Source UPF notifies the NF with the information received from the SMF.

Editor's note: It is FFS whether the solution is in the scope as per the architectural assumption. The UPF can only expose 5GC information which is originated in the UPF.

5. Consumer NF may decide to unsubscribe or modify the Event Exposure Subscription.

6. If the Consumer NF chose option A in step 0, it may subscribe to Target UPF for event exposure service for the relevant PDU Session.

7. Target UPF notifies regarding the subscribed events.

8. If the consumer NF chose option B in step 0, the Source UPF subscribes to the relocated UPF on behalf of it. (Notification target is that of Consumer NF).

9. Target UPF notifies regarding the subscribed events.

Editor's note: For any UE scenarios, how to reduce the multiple notification message of target UPF(s) from UPF is FFS.

### 6.13.4 Impacts on services, entities and interfaces

Changes in Nsmf\_EventExposure service (or N4 signalling in the case we utilize N4).

Changes in Nupf\_Event\_Exposure service.

## 6.14 Solution #14: Reduce the UPF performance impacts due to data reporting to NF consumer

### 6.14.1 Key Issue mapping

This solution is for the "Key Issue#2: Support UPF expose information to other NFs" especially focus on how to reduce the UPF performance impacts due to data reporting to NWDAF.

The performance issue is also indicated in the Architectural Requirements i.e. clause 4.2:

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

### 6.14.2 Description

As defined in Annex A, multiple UPF information per Analytics ID are expected to be collected to help data analytics in NWDAF.However, it should be avoided the UPF's user plane traffic handling performance degradation due to UPF data reporting to NWDAF.

For example, the scope of the UPF data collection by NWDAF may be per AoI or per S-NSSAI (e.g. for the Service Experience as defined in clause 6.4 of TS 23.288 [5] and Abnormal Behaviour analytics as defined in clause 6.7.5 of TS 23.288 [5]), which means UE level UPF data in the UPFs, which is for all the UE associated the indicated the AoI or S-NSSAI, need be reported the to NWDAF. If the UE number is quite a big, the reporting impact to the UPF performance cannot be neglected.

There are following mechanisms can be considered on how to alleviate this event reporting impact to UPF performance:

1. Reuse the SMF based subscription/ notification mechanism: If different NWDAF subscribes the same UPF data to the UPF via the SMF, the SMF may combine the different subscriptions from different NWDAFs into one configuration/instruction to the UPF. The UPF will be instructed by SMF to report either directly to each NWDAF, or to the SMF via existing N4 interface. The SMF per different subscription information received before, it notify/distribute the UPF reports to different NWDAFs according to the subscriptions from the NWDAFs.

NOTE: If DCCF is deployed, it may be possible to consolidate subscriptions towards SMF.

2. Enhance the existing event subscription mechanism: UPF data for data analysis is not always time sensitive (especially for the training dataset collection). It is preferred not to immediately send those event notifications to the NWDAF when the event is detected but the UPF is at peak hour. Hence the event subscription can be enhanced as follows:

- Add a new IE, i.e. Reporting suggestion information, in the Event Reporting Information. The Reporting suggestion information includes Report urgency and Reporting window two information. Reporting urgency information represents whether this event report can be delay tolerant, i.e. the event report can be delayed. When the related event is detected, the Reporting window defines the last reporting valid time. For example if the event can be reported within two hours of the event detection, the reporting windows is two hours.

NOTE: Trade off between report sending and report storage needs to be evaluated at deployment.

3. Aggregating the event subscription/Notification: For the UE level UPF data reporting normally the granularity of event subscription and reporting is per UE level, i.e. each UE have a separated event subscription and event reporting. To reduce the number of event notification, when the UE level UPF event is subscribed, the subscription and notification can be per node level.

This mechanism can be combined with bullet 2. If the event which can be delay tolerant, the event subscription is per node level. When the event is detected, the UPF can aggregate the event notification. Within the event notification, the UE ID or other identifier is added to differentiate different UE related UPF event. Hence it can reduce the event notification sent to the NF consumer.

The above mechanism can be generalized to be applied for any NF consumer of UPF event exposure service.

### 6.14.3 Procedures

The enhancement on existing UPF event exposure subscription and notification service procedure is described as in clause 6.14.2.

### 6.14.4 Impacts on services, entities and interfaces

NF consumer of UPF event exposure service:

- Event Reporting Information:

- Add a new IE, i.e. Reporting suggestion information. It includes reporting urgency and reporting window information.

- Support UE level different UPF event subscription/notification can be aggregated as per Node level.

UPF:

- Per received Reporting suggestion information in the event subscription, the UPF can delay the event reporting.

- Support UE level different UPF event subscription/notification can be aggregated as per Node level.

## 6.15 Solution #15: Subscription of UPF Event Exposure Service

### 6.15.1 Key Issue mapping

This solution is for KI#2.

### 6.15.2 Description

The solution introduces for the AF to subscribe to UPF Event Exposure served by the UPF handling a specific IP Flow over the PDU session. In this solution, we provide how to discover the specific UPF with UE IP address.

### 6.15.3 Procedures

#### 6.15.3.1 UPF Event Exposure using NEF

##### 6.15.3.1.1 Procedure of UPF service operations information flow

The procedure is used by the AF/NEF to subscribe event notification to the UPF handling a specific PDU session. Cancelling is done by Nupf\_EventExposure\_Unsubscribe request identifying the subscription to cancel.



Figure 6.15.3.1.1: Procedure of UPF service operations information flow

1. In order to subscribe to Event Exposure service on a specific PDU session, the AF sends a request to the NEF with UE IP address.

2. The NEF sends the request to the BSF.

3. Based on UE IP address, the BSF can identify the specific UPF and sends the request to it.

4-6. Acknowledgements for each request.

##### 6.15.3.1.2 Procedure of UPF information in BSF

The procedure is used for storing UPF information in BSF.



Figure 6.15.3.1.1: Procedure of UPF information in BSF

0. The UE requests PDU session establishment.

1. During the PUD session establishment, the SMF sends Npcf\_SMPolicyControl\_Update Request message to the PCF with UE IP address and UPF ID information.

2. The PCF sends Nbsf\_Management\_Register Request message to the BSF with UE IP address and UPF ID information.

### 6.15.4 Impacts on services, entities and interfaces

Editor's note: This clause captures impacts on existing 3GPP nodes and functional elements.

## 6.16 Solution #16: Direct/indirect subscription of the UPF event exposure service

### 6.16.1 Key Issue mapping

This is a solution for KI#2.

### 6.16.2 Description

The UPF event exposure service needs to be permitted when a consumer NF wants to subscribe this service. This includes two scenarios:

- When the consumer NF subscribes the UPF event exposure service from UPF directly.

- When the consumer NF subscribes the UPF event exposure service via an SMF.

The solution introduces the subscription methods for both of the scenarios, including subscribing the UPF event service via user plane and via control plane. The consumer NFs may be AF/NEF, NWDAF. The UPF may support Nupf\_EventExposure\_Subscribe service operation. The SMF may support Nsmf\_UPFAccessAuthorization service operation.

### 6.16.3 Procedures

#### 6.16.3.1 UPF event exposure service subscription directly from the UPF



Figure 6.16.3.1-1: UPF event exposure service subscription directly from the UPF

0. The consumer NF finds the appropriate UPF(s) by using the UPF selection method as described in clause 6.1.2.5.

1. The consumer NF sends an Nupf\_EventExposure\_Subscribe request to the UPF for information exposure. The request includes the NF identity information of the consumer NF (e.g. NF name, NF type, IP address, FQDN), UPF event exposure mode (e.g. event-triggered, and periodically-triggered with a timer), exposure duration and the information expected to be exposed.

The consumer may request the UPF to expose UE-level information or NF-level information. If the request information is UE-level, the request may include UE IP address, UE ID (i.e. SUCI, GPSI), PDU session ID, and QFI. The information expected to be exposed may be UE related, e.g. UE location and PDU session rate. If the request information is NF-level, the information expected to be exposed may be UPF related, e.g. UPF load.

2. If consumer NF requests for provision information, i.e. UPF load and QoS parameters, skip step 2. If consumer NF requests for other information (e.g. measurement information), the UPF report the subscription request to the SMF (or to the PCF via the SMF) to decide whether, what information and how the UPF can expose to the consumer NF. The report includes the information received by UPF in step 1.

The SMF/PCF determines whether, what information and how the request is permitted based on the local strategy together with the received information (e.g. NF type of the consumer NF, the information expected to be exposed), and responds to the UPF (directly or via the SMF).

Alternatively, the UPF may decide whether, what information and how the UPF can expose to the consumer NF by itself, and reports an indication to the SMF/PCF.

3. (Optional) The UPF sends an Nupf\_EventExposure\_Subscribe response message to the consumer NF. The response includes an indication to whether the request in step 1 is successful or not.

If the subscription request is successful, the response may include the UPF event exposure mode (e.g. event-triggered, and periodically-triggered with a timer), exposure duration, whether the exposed information is NF-level or UE-level, and the information exposed to the consumer NF. If the subscription request is not successful, the response includes a Cause value indicating that the subscription failed.

4. The UPF exposes the information determined in step 2 directly to the consumer NF over Nupf\_EventExposure\_Notify service operation.

#### 6.16.3.2 UPF event exposure service subscription via an SMF



Figure 6.16.3.2-1: UPF event exposure service subscription via an SMF

0. The consumer NF finds the appropriate SMF as described in other solutions.

1. The consumer NF sends a subscription request to the SMF to subscribe to direct notification of UPF Event Exposure.

NOTE: The request may be over the Nsmf\_UPFAccessAuthorization\_Create/Subscribe service operation.

The request includes the NF identity information of the consumer NF (e.g. NF name, NF type, IP address, FQDN), UPF event exposure mode (e.g. event-triggered, and periodically-triggered with a timer), the exposure duration, and the information expected to be exposed.

The consumer NF may request the UPF to expose UE-level information or NF-level information. If the request information is UE-level, the request includes UE IP address, UE ID (i.e. SUCI, GPSI), PDU session ID, and QFI. The information expected to be exposed may be UE related, e.g. UE location and PDU session rate. If the request information is NF-level, the information expected to be exposed may be UPF related, e.g. UPF load.

2. The SMF determines whether, what information and how the UPF can expose to the consumer NF based on the local strategy together with the received information (e.g. NF type of the consumer NF, the information expected to be exposed). Optionally, the SMF may make the decision by considering the subscription information of this UE (if the request information is UE-level) from UDM.

3. If the subscription request is successful, the SMF sends a notification of direct event exposure to the UPF via the N4 interface. The notification may include the UPF event exposure mode (e.g. event-triggered, and periodically-triggered with a timer), the exposure duration, whether the exposed information is NF-level or UE-level, and the information exposed to the consumer NF.

The SMF may send a subscription response to the consumer NF including an indication that the request in step 1 is successful.

If the subscription request is not successful, the response includes a Cause value indicating that the subscription failed.

4. The UPF exposes the information determined in step 2 directly to the consumer NF over Nupf\_EventExposure\_Notify service operation.

### 6.16.4 Impacts on services, entities and interfaces

UPF:

- Newly introduced UPF Service Operations to support other NFs to subscribe the UPF event exposure service directly.

SMF:

- Newly introduced SMF Service and Service Operations to represent other NFs to subscribe the UPF event exposure service indirectly.

## 6.17 Solution #17: Update/Release subscription of the UPF event exposure service

### 6.17.1 Key Issue mapping

This is a solution for KI#2.

### 6.17.2 Description

The UPF event exposure service subscription may need to be updated or released based on the consumer NF's requirement. This includes two scenarios:

- Update/release UPF event exposure service subscription directly by UPF.

- Update/release UPF event exposure service subscription via an SMF.

The solution introduces the updating/releasing subscription methods for both of the scenarios. The UPF may support Nupf\_EventExposure\_Unsubscribe and Nupf\_EventExposure\_ModifySubscription service operation. The SMF may support Nsmf\_UPFAccessAuthorization service operation.

### 6.17.3 Procedures

#### 6.17.3.1 Update/release UPF event exposure service subscription directly by UPF

If the subscription of the UPF event exposure service by the consumer NF is sent directly to UPF, the updating/releasing procedure is as follow.



Figure 6.17.3.1-1: Update/release UPF event exposure service subscription directly by UPF

1. The consumer NF sends an Nupf\_EventExposure\_ModifySubscription (or Nupf\_EventExposure\_Unsubscribe) request to the UPF to update the subscription of (or unsubscribe) the UPF event exposure service. The request includes the consumer NF's Subscription Correlation ID.

2. Optionally, the UPF may report the update/release request to the SMF (or to the PCF via the SMF) to decide whether and what information to update/release. The request includes the information received by UPF in step 1.

The SMF/PCF determines whether and what information to update based on the local strategy together with the received information (e.g. NF type of the consumer NF, the information expected to be updated), and responds to the UPF (directly or via the SMF).

Alternatively, the UPF may decide whether and what information to update or whether to release the subscription by itself, and reports an indication to the SMF/PCF.

3. The UPF sends a response message to the consumer NF including an indication to whether the ModifySubscription/Unsubscribe request is successful or not. If the request is not successful, the response includes a Cause value indicating that the update/release failed.

4. The UPF sends the updating/releasing notification related with the updated information (if the notification is updating the exposed information) to the consumer NF over Nupf\_EventExposure\_Notify service operation.

#### 6.17.3.2 Update/release UPF event exposure service subscription via an SMF

If the subscription of the UPF event exposure service by the consumer NF is via an SMF, the subscription updating procedure is as follows.



Figure 6.17.3.2-1: Update UPF event exposure service subscription via an SMF

1. The consumer NF sends an updating subscription request to the SMF to update the information exposed from the UPF.

NOTE: The request may be over the Nsmf\_UPFAccessAuthorization\_Update service operation.

The request includes the consumer NF's Subscription Correlation ID, the UPF identity information (e.g. UPF IP address and FQDN), NF identity information of the consumer NF (e.g. NF name, NF type, IP address, FQDN), and the information expected to be updated.

2. The SMF determines whether to update the information exposure from the UPF to the consumer NF according to the local strategy together with the received information (e.g. NF type of the consumer NF, the information expected to be updated/released).

3. If the SMF permits the request in step 1, the SMF sends a notification for updating the information exposed to the consumer NF directly to the UPF via the N4 Session modification procedure. The notification includes the information to be updated. The SMF may send the response to the consumer NF including the decision result.

If the request in step 1 is not permitted, the SMF sends the response to the consumer NF including the Cause value of refusal cause.

4. The UPF sends the updating notification to the consumer NF about the exposed information to the consumer NF over the Nupf\_EventExposure\_Notify service operation. The notification includes the updated information to be exposed.

In this case, the subscription releasing procedure is the same with the steps in clause 6.17.3.1.

### 6.17.4 Impacts on services, entities and interfaces

UPF:

- Newly introduced UPF Service Operations to support other NFs to modify subscription of (or unsubscribe) the UPF event exposure service directly.

SMF:

- Newly introduced SMF Service and Service Operations to represent other NFs to update/release subscription of the UPF event exposure service indirectly.

## 6.18 Solution #18: QoS parameters exposure by UPF

### 6.18.1 Key Issue mapping

This is a solution for KI#2.

### 6.18.2 Description

In order to obtain QoS parameters with low latency, the AF may request to expose QoS parameters from UPF directly. The AF may want to know the QoS parameters for two reasons:

- If UPF receives a dynamic PCC rule from PCF, the AF may want to verify whether the UPF uses the QoS parameters as configured in the PCC rule.

- If UPF does not receive a dynamic PCC rule from PCF and use the default configuration, the AF may want to know the default configuration used by UPF.

The UPF may be instructed to report information about a QoS flow directly to the NEF, i.e. by passing the SMF and the PCF. This reporting may target a third-party AF that wants to know the QoS parameters (e.g. 5QI Value, Resource type, flow bit rates (GFBR, MFBR), packet rate, Usage report) used by UPF to guarantee the QoS flow. By exposing this information directly from UPF to NEF, the AF can know the QoS parameters with flexibility and low latency.

NOTE: Exposing the QoS parameters from UPF to AF directly is to find a way with lower latency and higher flexibility.

### 6.18.3 Procedures



Figure 6.18.3-1: QoS parameters exposure by UPF

1. The AF issues an Nnef\_EventExposure\_Subscribe (Application ID, GPSI, IP address) service operation to request QoS parameters from the L-NEF.

2. The L-NEF finds the appropriate UPF(s) by using the UPF selection method targeting the PDU sessions of a certain UE with information of IP address, as described in clause 6.1.2.5.1.

3. The L-NEF sends the Nupf\_EventExposure\_Subscribe request to the UPF to request QoS parameters.

NOTE: The QoS parameters requested to be exposed by UPF are configured in the UPF by 5GC which is QoS information used for packet processing. These QoS parameters are associated with PDU sessions and service flows which can be identified by AF, and are originated from the UPF without other operations by the UPF or any additional action from SMF, PCF, 5G AN.

4. The UPF responds the QoS parameters to L-NEF over the Nupf\_EventExposure\_Notify service operation.

5. The L-NEF responds the QoS parameters to the AF over the Nnef\_EventExposure\_Subscribe service operation.

### 6.18.4 Impacts on services, entities and interfaces

UPF:

- Newly introduced UPF Service Operations to support AF/Local NEF/NEF to subscribe the UPF event exposure service directly.

- Expose QoS parameter related information to AF/Local NEF/NEF directly.

## 6.19 Solution #19: QoS Monitoring results exposure by UPF

### 6.19.1 Key Issue mapping

This is a solution for KI#2.

### 6.19.2 Description

Some real time network information, e.g. user path latency, is useful for application layer. In R17, in order to expose network information timely to local AF, the L-PSA UPF may expose network information i.e. QoS monitoring results as defined in TS 23.501 [2], clause 5.33.3, to the local AF.

The UPF may be instructed to report information about a PDU Session directly to the local NEF/NEF/AF i.e. by passing the SMF and the PCF. The PSA UPF may support Nupf\_EventExposure\_Subscribe service operation.

### 6.19.3 Procedures

#### 6.19.3.1 QoS Monitoring results subscription directly from the UPF under the same PCF policy



Figure 6.19.3.1-1: QoS Monitoring results subscription directly from the UPF under the same PCF policy

0. The UE establishes a PDU Session and UPF notifies the QoS monitoring information to Local NEF/NEF/AF as described in step 0-5 in clause 6.4.2.1 of TS 23.548 [7]. The L-PSA UPF sends the direct subscription notification to the local AF or the local NEF together with the notification related with QoS monitoring information over Nupf\_EventExposure\_Notify service operation.

1. (when the reporting goes via local NEF) For the subsequent requests to subscribe direct notification of QoS monitoring from this AF for the same service data flow via Local NEF, the local NEF may directly invoke the Nupf\_EventExposure\_Subscribe service operation.

During the QoS monitoring initial request, AF allocated Transaction Reference ID to identify service data flow. Subsequent request is used for updating current subscription (e.g. update frequency of QoS monitoring report). AF invokes Nnef\_AFsessionWithQoS\_Update to update subscription for this service data flow with the same Transaction Reference ID. Local NEF can identify the request is for the same service data.

The L-UPF sends the notification related with QoS monitoring information over Nupf\_EventExposure\_Notify service operation to the local NEF, and local NEF reports to AF.

#### 6.19.3.2 QoS Monitoring results subscription directly from the UPF without PCF policy control

This solution is applied for the scenario that AF request to expose QoS monitoring results via a Local NEF.



Figure 6.19.3.2-1: QoS Monitoring results subscription directly from the UPF without PCF policy control

0. The AF finds the appropriate UPF(s) by using the UPF selection method as described in clause 6.1.2.5.

1. The AF requests to subscribe direct notification of QoS monitoring via Local NEF, the local NEF may directly invoke the Nupf\_EventExposure\_Subscribe service operation to the UPF for QoS monitoring results exposure. The request includes the AF identity information (e.g. IP address, FQDN).

2. The UPF reports the subscription request of direct event notification to the SMF.

SMF sends request to PCF to update rules of QoS monitoring. The PCF makes the policy decision and initiates the PDU Session modification procedure. The PCF includes the indication of direct event notification (including target local NEF or local AF address) for the service data flow within the PCC rule.

The SMF may activate the end to end UL/DL packet delay measurement between UE and PSA UPF for a QoS Flow to make the UPF obtain the QoS monitoring information, as described in clause 5.33.3 of TS 23.501 [2].

3. (Optional) The UPF sends an Nupf\_EventExposure\_Subscribe response message to the Local NEF, and the Local NEF replies to the AF. The response includes an indication to whether the request in step 1 is successful or not. If the subscription request is not successful, the response includes a Cause value indicating that the subscription failed.

4. The UPF sends the notification related with QoS monitoring information over Nupf\_EventExposure\_Notify service operation to the Local NEF, and the Local NEF reports to the AF by invoking Nnef\_EventExposure\_Notify service operation.

### 6.19.4 Impacts on services, entities and interfaces

UPF:

- Newly introduced UPF Service Operations to support AF/Local NEF/NEF to subscribe the UPF event exposure service directly.

- Expose QoS monitoring information to AF/Local NEF/NEF directly.

SMF:

- Activate the end to end packet delay measurement based on the UPF's indication.

## 6.20 Solution #20: UE IP address mapping information exposure by UPF

### 6.20.1 Key Issue mapping

This is a solution for KI#2.

### 6.20.2 Description

If UPF(s) employs a NAT functionality, the packets behind of the UPF (N6 interface) will use a public IP address (possibly shared by multiple UE(s) when Network Address and Port Translation applies) and the AF may not know the UE private IP address of the UE.

An AF, in the N6 interface, may detect abnormal events for those packets associated with a UE based on the public IP address and port number (public UE addressing information). The AF does not know the UE private IP address which is internally used in 5GC. Accordingly, the AF may fail to request proper action for the UE (e.g. policy change for the UE) brought the abnormal events, since the AF are not aware of the UE private IP address corresponding to the public UE addressing information.

In Rel-17, AF specific UE ID retrieval has specified that AF requests corresponding GPSI for an IP address of a UE. However, an IP address that has been NATed is not supported.

To get the mapped UE private IP address from UE public IP addressing information, the AF may request an UE IP address mapping information exposure to the UPF for a UE. This solution is applicable for the case the UPF supports the NAT, i.e. the NAT function deployed outside the UPF is not supported.

NOTE: The case where multiple UEs are allocated with the same private IP address can be addressed as follows:

- When this same private IP address is allocated to different UE(s) for different DNN and S-NSSAI(s) by associating the AF with a DNN and S-NSSAI.

- Otherwise and furthermore, the "ipDomain" attribute as defined in clause 4.2.2.2, Note 3, of TS 29.514 [9] may be leveraged.

Editor's note: Whether these information can be exposed outside to 3rd AS is FFS.

### 6.20.3 Procedures

#### 6.20.3.1 UPF registration in NRF with NATed IP pools



Figure 6.20.3.1-1: UPF registration in NRF for NATed IP pools

As illustrated in clause 6.1.2.2, an UPF, supporting the NAT functionality, may register in NRF providing UPF Provision information. The UPF Provision information may include Public IP address pool information (i.e. Public IP address range, additionally ports number range)) for NAT. The Public IP address pool information may be on per DNN and S-NSSAI basis.

#### 6.20.3.2 UE IP address mapping information exposure by UPF



Figure 6.20.3.2-1: UE IP address mapping information exposure by UPF

1. The AF issues Nnef\_EventExposure\_Subscribe (NATed addressing information, AF ID ) service operation to request UE IP address mapping information for a UE. The NATed addressing information comprise a Public IP address and a port number.

The AF request may be for one-time notification.

2. The NEF finds the appropriate UPF by using the UPF selection method targeting the NATed addressing information for a UE and the DNN=S-NSSAI associated with the AF ID. This may use NRF discovery (see clause 6.20.3.1). The NEF may also use the NATed addressing information to determine the "ipDomain" attribute as defined in clause 4.2.2.2, Note 3, of TS 29.514 [9].

3. The NEF sends the Nupf\_EventExposure\_Subscribe request (public UE addressing information, DNN,S-NSSAI associated with the AF ID) to the UPF to request UE IP address mapping information.

4. The UPF responds with the 5GC UE IP address mapping information to NEF over the Nupf\_EventExposure\_Notify service operation. The 5GC UE IP address mapping information comprises a private IP address of the UE.

5. The NEF responds to the AF over the Nnef\_EventExposure\_Notify service operation. The Nnef\_EventExposure\_Notify operation may provide 5GC UE IP addressing mapping information and may additionally include address assistance information which can help to uniquely identity the related IP address.

Editor's note: Whether the DNN/S-NSSAI, ipdomain information is the address assistance information and can be exposed outside to 3rd AS is FFS.

Editor's note: It is FFS how long the binding information can be kept at the AF.

### 6.20.4 Impacts on services, entities and interfaces

UPF:

- Support newly introduced UPF exposure Service Operations for the UE IP address mapping information.

- NAT support in UPF (how to perform NATing is out of 3GPP scope).

- Registration of NATed IP pools per IP Domain in UPF NFprofile.

NEF:

- Support newly introduced event exposure for the UE IP address mapping information by UPF.

NRF:

- Support UPF registration with UPF NAT information per IP Domain.

- Support UPF discovery with a NATed UE IP address as input.

## 6.21 Solution #21: UPF Event Exposure with consideration on UPF performance

### 6.21.1 Key Issue mapping

This solution addresses "Key Issue#2: Support UPF expose information to other NFs". Especially, it focuses on the following architecture requirements:

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

### 6.21.2 Description

The following mechanism decides whether the UPF event exposure is used or not at any time by taking a consideration on the UPF performance. The operator may want to keep UPF performance rather than to report the information to other NFs according to the threshold on UPF performance. By muting and resuming the UPF reporting based on the threshold of UPF performance configured from operator policy, it would be helpful to manage efficiently the UPF event exposure, and give the operator the flexibility of network deployments and managements.

To achieve it, a consumer NF (e.g. NEF, AF) may provide in its subscription request the consideration on UPF performance during EventExposure Service subscription for event notification, (e.g. as the reporting suggestion information of Solution#14 or as a new IE in the Event Reporting Information).

It is assumed that UPF is monitoring its performance by itself and such monitoring depends on the implementation.

For example, the request is to:

- indicate to the Event provider NF (i.e. UPF) that the notification of the available events shall be muted if the NF performance exceeds the threshold, providing a subscription to the automatic notification of reporting start/stop due to UPF overload, i.e. the event reporting can be started/stopped per UPF overload.

NOTE 1: The above notification control implies to the Event provider NF (i.e. UPF) to resume the notification to the Event consumer NF if NF performance does not exceed the threshold.

NOTE 2: The threshold of NF performance is pre-configured in UPF and may be updated via OAM.

NOTE 3: This solution is similar to delay reporting of Solution#14, but the event report of this solution is dynamically muted and resumed.

### 6.21.3 Procedures

The enhancement on existing UPF event exposure subscription and notification service procedure is described as in clause 6.21.2.

### 6.21.4 Impacts on services, entities and interfaces

NF consumer of UPF event exposure service:

- in the subscription request include the information for the event report notification with the consideration on NF performance.

UPF:

- Based on Reporting request information in the event subscription, the UPF can mute/resume the event reporting.

## 6.22 Solution #22: Support UPF event exposure service subscription update in case of UPF/SMF change

### 6.22.1 Key Issue mapping

This is a solution for KI#2.

### 6.22.2 Description

In the scenario that a consumer NF requests a single UE related information from the target UPF(s) via UPF event exposure service, a subscription update may be needed when the target PDU Session related UPF changes.

This solution aims to support the updating of target UPF for UPF event exposure service subscription in the perspective of consumer NF in case of UPF change during the life time of the PDU Session. Two mechanisms are proposed:

- The consumer NF subscribes SMF/UPF change notification from the SMF. An indication of notifying the consumer NF to subscribe information from new SMF/UPF is triggered once the SMF/UPF for serving the PDU Session changes and detected by the SMF.

- Add UE ID (SUPI, GPSI) and PDU Session ID list with the corresponding UPF ID in the BSF. Then the consumer NF can subscribe the UPF information from the BSF directly.

The details of these three solutions are described in the next clause.

### 6.22.3 Procedures

#### 6.22.3.1 The consumer NF subscribes SMF/UPF change notification from the SMF



Figure 6.22.3.1-1: Consumer NF subscribes UPF/SMF relocation notification from the SMF

0. The consumer NF subscribes to Source UPF for event exposure service.

1. The consumer NF issues an Nudm\_UECM\_Get request to find the Source SMF from UDM providing NF type, UE ID, S-NSSAI, DNN. The UDM finds the serving SMF for the UE as described in TS 23.502 [3], and responds the SMF ID over Nudm\_UECM\_Get service response to the consumer NF.

2. The consumer NF subscribes for event notification for UPF/SMF relocation for the relevant PDU Session from the Source SMF via Nsmf\_EventExposure\_Subscribe service operation.

3. The Source SMF decides for UPF relocation for the relevant PDU Session.

4. The Source SMF notifies the consumer NF regarding UPF ID of the Target UPF.

If the PDU Session is released, the SMF notifies the consumer NF that implicitly indices the release of the consumer subscription onto the SMF.

In Case 1: in case of SMF change, step 5-7 are executed.

In Case 2: in case of SMF change, step 8-10 are executed.

5. The consumer NF unsubscribe for event notification for UPF/SMF relocation for the relevant PDU Session from the Source SMF.

6. The consumer NF finds the Target SMF for the UE providing UE ID. There are two ways. The consumer NF may find the Target SMF by using the same way as described in step 1. Alternatively, the consumer NF may find the BSF by using the IP address, and then issues Nbsf\_Management\_Discovery to find the PCF(s) selected for the PDU Session identified by the tuple (UE IP address, SUPI, GPSI, DNN, S-NSSAI).

7. The consumer NF subscribes for event notification for UPF/SMF relocation for the relevant PDU Session from the Target SMF via Nsmf\_EventExposure\_Subscribe service operation.

8. The consumer NF unsubscribe the event exposure subscription from the Source UPF.

9. The consumer NF subscribe to Target UPF for event exposure service.

10. The target UPF notifies regarding the subscribed events.

#### 6.22.3.2 The consumer NF subscribes UPF change notification from the BSF by storing UPF ID and UE IP address in the BSF in PDU Session Establishment procedure



Figure 6.22.3.2-1: Store UPF ID and UE IP address in BSF

0. The UE establishes a PDU Session as defined in clause 4.3.2.2.1 of TS 23.502 [3].

1. During the PDU Session establishment procedure, the SMF sends Npcf\_SMPolicyControl\_Update Request message (with the list of UE IP address and UPF ID) to PCF.

2. The PCF sends Nbsf\_Management\_Register Request message to the BSF to store the list of UE IP address and UPF ID in the BSF.



Figure 6.22.3.2-2: Consumer NF subscribes UPF information notification from the BSF

1. The consumer NF (e.g. AF/NEF) invokes Nbsf\_Management\_Subscribe Request to obtain the UPF ID providing the UE IP address, S-NSSAI, DNN.

2. The BSF responds the UPF ID(s) to consumer NF via the Nbsf\_Management\_Notify Response message.

3. The consumer NF sends Nupf\_EventExposure\_Subscribe to relevant UPF(s) received in step 2 for event exposure service.

4. The UPF notifies regarding the subscribed events.

### 6.22.4 Impacts on services, entities and interfaces

SMF:

- Nsmf Event Exposure Subscription needs to be enhanced to support exposing the UPF ID that matches a PDU session.

BSF:

- Discovery of several UPFs that accords with the parameters that related to the UEs.

- Expose UPF ID to the consumer NF.

# 7 Overall Evaluation

## 7.1 Overall Evaluation of solutions for Key Issue #1

For KI#1:

- How to support UPF event exposure service(s) registration/deregistration on NRF, and what parameters to be registered in the NF profile of UPF.

- How to support UPF service discovery via the NRF, and what parameters that can be used for discovery.

Solution #1 (clauses 6.1.2.1-6.1.2.4) can be seen as the basis to solve these aspects of KI#1. It is also considered and enhanced by Solution #12, Solution #20 and Solution #1 (clause 6.1.2.5.3) further.

Solution #12 proposes direct subscription and indirect subscription for NWDAF collecting data from UPF. The impact of Solution #12 on KI #1 is that it proposes to include direct indication and/or indirect indication in UPF NF profile when UPF registers to NRF.

Solution #20 proposes that an UPF supporting NAT functionality may register Public IP address pool information per IP Domain in NRF. The Public IP address pool information may be on per DNN and S-NSSAI basis.

For KI#1:

- How to support UPF selection for a UPF event exposure service request targeting a specific UE or a specific PDU session.

Solution #1 (clauses 6.1.2.5.1 and 6.1.2.5.2) can also be considered to solve that aspect of KI#1:

- It can be used for UPF selection with information of UE IP address, as described in clause 6.1.2.5.1.

- It can be used for UPF selection with information of SUPI, S-NSSAI and DNN, as in clause 6.1.2.5.2.

- It can be used also for UPF selection with information of UE IP address, by first applying existing functionality for IP address translation into SUPI using BSF service.

- It can be used for UPF selection with information of Group Identifier by first applying existing functionality for Group Identifier translation into SUPI list using UDM service.

By specifying in normative phase the enhancements proposed in clause 6.1.2.1-6.1.2.5 from solution #1, clause 6.12.3.2 from solution #12, and clause 6.20.3.1 from solution #20, the following issues from KI#1 are covered:

- How to support UPF event exposure service(s) registration/deregistration on NRF, and what parameters to be registered in the NF profile of UPF.

- How to support UPF service discovery via the NRF, and what parameters that can be used for discovery.

The following issue from KI#1 is not covered:

- How to support UPF selection for a UPF event exposure service request targeting a specific UE or a specific PDU session.

**UPF discovery for data collection**

For UPF event exposure the UPF discovery is the necessary step to be considered. The UPF discovery can categorized as following option:

- Option 1: NRF based discovery (sol#1). The UPF registered its NF profile to the NRF. The NF consumer query the NRF, per the related query information, the NRF return the related UPF meet the query request.

- Option 2: SMF based discovery. There are further two option:

- Option 2.1: Only SMF is discovered (Sol#8/9/10). NF consumer get the serving SMF of the UE from the UDM per SUPI, which may require getting SUPI from IP address first (via BSF) or using IP address (via BSF) (Sol#1, 6.1.2.5.1-1). After that, the data collection from NF consumer is subscribed to the SMF only and SMF help to identity the related UPF.

- Option 2.2: the UPF is discovered via the assistance from SMF (Sol#1/2/7/11). NF consumer get the serving SMF for the UE from the UDM. Then it obtains the UPF information from the serving SMF. This option requires the SMF event exposure function enhancement to return a list of the UPF ID.

- Option 3: UDM/BSF based discovery (Sol#5/15). NF directly obtains the UPF information of the UE from the UDM (or BSF) if the serving SMF has registered the UPF information for the UE into the UDM (or BSF via the PCF). This option requires the SMF/UDM (or SMF/PCF/BSF) enhancement to register the UPF ID to the UDM (or BSF) and UDM (or BSF) send the required UPF ID to the NF consumer.

Option 2 and Option 3 target for the same case, i.e. the data collection is related to a specific UE or QoS flow.

For option 1, the NF profile of UPF can be used for discovery directly. This is suitable for the UPF direct subscription, e.g. UPF load analytics.

For option 2, option 2.2 need enhancement on the SMF. The SMF need not only expose the UPF ID but also the UPF role. In case of the UPF change, the SMF also need notify the UPF change to the NF consumer, i.e. the SMF need maintain an additional UPF information subscription context. Option 2.1 only the SMF is to be discovered. The data collection can be subscribed via the SMF. If there are UPF role change or UPF reallocation, it can be handled by the SMF directly and not need notify the NF consumer.

For option 3, it needs SMF register the related information to the UDM or BSF (via PCF). Also for each UPF role, e.g. PSA, I-UPF, the information need be registered to the UDM or BSF. Hence if the UPF role change or reallocation, the SMF also need update the related information at the UDM or BSF.

Option 2.1 is suitable for UPF event exposure service indirect subscription as it does not require the SMF enhancement. And also the UPF role exposure and change notification can be avoided.

## 7.2 Evaluation for KI#2

There are 21 candidate solutions proposed to address key issue#2, i.e. except solution#1, from solution#2 to #22. These 21 solutions can be group as follows:

- Group 1: How the UPF expose the data to the TSN AF/TSCTSF. The related solution is sol#2.

- Group 2: How the UPF expose the data to NWDAF. The related solution is sol#7, 8, 9,10,11,12.

- Group 3: How the UPF expose the data to NEF/AF. The related solution is sol#15, 18, 19, 20.

- Group 4: Generic issue related to UPF data collection. The related solution is sol#3,4,5,6,13,14,16,17, 21, 22.

**UPF Data collection to TSNAF/TSCTSF**

Solution#2 describes how TSN AF or TSCTSF collect the UPF/NW-TT PMIC/UMIC information via the UPF event exposure service. Currently this bridge information is encapsulated within containers and sent by UPF to SMF over N4. And only NW-TT in UPF, TSN AF and TSCTSF are requested to understand the information in those containers.

With this proposal, the additional ‘indication of UPF Direct Report’ is introduced for the UPF event exposure service in the case that the operation code is ‘subscribe-notify for parameter’ or ‘unsubscribe for parameter’. The NW-TT/UPF notification is unrelated to the other operation code defined in the container as described in TS 24.519 [11]. If enhanced with the addition of the indication of event notification, N7 and N4 can convey to UPF notification target information for direct report by UPF.

Solution#2 optimizes only part of the information reported by the NW-TT/UPF depending on the request from TSN AF or TSCTSF. Optimizing notifications is more important than optimizing subscriptions due to the frequent UPF notifications. UPEAS enables a reduction in the signalling path for UPF reporting in the case of (un)subscribe operation code from TSN AF or TSCTSF and UPEAS does not cover the exchange of TSC information between DS-TT in UE and TSN AF or TSCTSF.

**Proposal 1:** The UPF directly reports for transferring TSC management Information depending on the request from TSNAF/TSCTSF.

**UPF Data collection to NWDAF**

For Group 2 solution, the data collection can be categorized into two types:

- Direct subscription from UPF (sol#7, 11, 12), i.e. NWDAF directly subscribes the UPF data from the UPF.

- Indirect subscription via SMF (sol#8, 9, 10, 12), i.e. NWDAF firstly subscribes the UPF data from the SMF, then SMF transfer the subscription information to the UPF. There one different on which message should be used between the SMF and UPF, N4 procedure? Or Nupf\_EventExposure\_Subscribe service operation?

Solution 9 propose SMF use Nupf\_EventExposure\_Subscribe for event subscription. Solution 8/10/12 propose SMF use the N4 procedure for event subscription. Using the SBA based API for subscription allows to benefit from SBA advantages / features (defined now and in the future) and avoids un-necessary protocol translations. Using PFCP for some events allows reusing N4 IEs defined for the purpose.

For the data collection for single UE case, as it always need search the related SMF first. If we want to terminate the subscription at the UPF, a new UPF discovery mechanism is to be defined, e.g. enhance the SMF event exposure service. However if the subscription is terminated at the SMF, no enhancement is expected. Hence in this case the UPF data collection subscription is more suitable to be terminated at the SMF.

**Proposal 2:** For the data collection related to single UE case, the UPF data collection subscription is preferred to be terminated at the SMF.

**Proposal 3:** void.

**UPF Data collection to the NEF/AF**

For Group 3 solution, all solution is related to the data collection related to one flow within one PDU session. The solution can be summarized as below:

- Solution#15 describes how the direct subscription can be done via the BSF. It is unclear how the related flow information which need measurement is triggered?

- Solution#18 describes how the QoS parameter information at the UPF can be exposed to the AF to find a way with lower latency and higher flexibility. The QoS parameters requested to be exposed by UPF are provision information that are configured in the UPF by 5GC for packet processing and can be identified by AF. This information is provisioned by the UPF without other operations by the SMF or AN.

- Solution#19 describes how NEF do the subsequent subscription to the same QoS flow and how to use the direct UPF subscription to do the data collection from QoS Monitoring.

For the AF do the subscription to the same QoS flow, AF is allocated Transaction Reference ID during the QoS monitoring initial request to identify service data flow. Subsequent request is used for updating current subscription with the same Transaction Reference ID. Local NEF can identify the request is for the same service data and invoke Nupf\_EventExposure\_Subscribe service operation directly.

For the direct subscription to the UPF and UPF trigger the SMF action, it is unsuitable to trigger the UPF subscription directly. Normally this monitoring subscription is combined with the PCC rule and notified to the SMF. By doing that, the SMF can trigger the related action, e.g. PDU session modification. The input for the activate measurement also need consider the policy control from the PCF. So why not do the subscription via the SMF considering the UPF discovery may also need go via the SMF?

- Solution #20 describes how the UE IP address mapping information can be exposed by UPF so that the AF can know the UE private IP address which is internally used in 5GC. This is for the case that the UPF supports the NAT.

**Proposal 3:** For the data collection which need some action besides UPF, e.g. QoS flow characteristics measurement, the subscription should be terminated at the SMF.

**Generic issue related to UPF data collection**

For Group 4 solution, the solution is not bound to one specific type NF consumer. It can be considered in all UPF data collection case. The solution can be summarized as follows:

- Solution#3 give some generic guidance on whether the UPF data collection should be the direct subscription or indirect subscription. It can be considered when the NF consumer do the UPF event subscription and not need be concluded individually.

- Solution#4 describe that N4 interface need be enhanced to pass the related event filtering information to the UPF. It can be part of the data collection procedure.

- Solution#5/#6 describe how to find the related UPF via the SUPI or IP address. It is more related to KI#1.

- Solution#13 describe how the UPF event subscription can be updated if the UPF is changed. It may be more suitable to consider this procedure in the related context. For example if the UL-CL is released, no target UPF, how to consider this UPF subscription change case?

- Solution#14 describe how to avoid performance impact due to the UPF data collection. Similar consideration is also considered at the Solution#11 and Solution#21. There are at least two mechanisms can be considered, i.e. the NF consumer indicates the Reporting suggestion information in the Event subscription procedure and per Reporting suggestion information UPF can concatenate several notification message to the same notification endpoint in one notification message.

By doing so it can greatly reduce number of the event reporting message and avoid the impact at the peak time especially avoiding event exposure impact to the normal UPF data packet transfer handling. This also give some flexibility to the UPF on when to report the collected data to NF consumer.

- Solution#16 describe that when the UPF receives the event subscription it may notify to the SMF to verify whether the subscription is allowed or not. If the intention of this procedure is for service operation authorization, it can be done as part of the service operation discovery, which is defined by SA3 WG.

- Solution 17 describe two case, i.e. the update/release directly to UPF or update/release indirectly via the SMF. For the update/release directly, similar issue about the authorization process via SMF/PCF.

- Solution#21 describes whether the UPF event exposure is used or not at any time by taking a consideration on the UPF performance. By muting and resuming the UPF reporting based on the threshold of UPF performance configured from operator policy, it may be helpful to manage efficiently the UPF event exposure, and give the operator the flexibility of network deployments and managements. However due to the reporting is uncertain, it is unclear on its benefit of this type of reporting.

- Solution #22 describes how to support the updating of target UPF for UPF event exposure service subscription in case of UPF change during the life time of the PDU Session.

**Proposal 4:** To reduce the event exposure impact to the UPF, it is suggested to introduce the Reporting suggestion information in the Event subscription procedure and per Reporting suggestion information UPF can concatenate several notification message to the same notification endpoint in one notification message.

# 8 Conclusions

## 8.1 Conclusions for Key Issue #1

UPF(s) register their Event Exposure service(s), supported event ID(s) onto NRF. Procedures defined in the present TR, clauses 6.1.2.1 to 6.1.2.4 are endorsed as a baseline for normative specifications.

The conclusion for the not covered issue in KI#1 will be concluded as part of KI#2.

To collect the data from the related UPF, the related UPF(s) need be discovered. It is done as following:

- Option 1: NRF based discovery. The UPF registered its NF profile to the NRF. The NF consumer query the NRF, per the related query information, the NRF return the UPF meet the query request.

- Option 2: SMF based discovery. The NF consumer gets the serving SMF of the UE from the UDM per SUPI. If UE IP address is known the NF consumer may need to first get the SUPI (via BSF). After that, the data collection from NF consumer is subscribed to the SMF only and SMF help to identity the related UPF.

## 8.2 Conclusions for KI#2

The following interim conclusions are proposed for KI#2:

1. Subscription to UPF events via SMF is the rule except for the cases listed in bullet 2; Subscription via SMF means the final consumer of UPF event notifications sends the subscription request to the SMF and then the SMF is doing a third-party subscription onto UPF on behalf of this final consumer. Conversely the notifications are directly sent by the UPF to the final consumer of UPF notifications.

NOTE 1: Optimizing notifications is more important than optimizing subscriptions.

NOTE 2: Subscriptions related with AoI are handled by SMF that subscribe/unsubscribe to the relevant UPF(s) on behalf of the final consumer based on whether the UE is in the target AoI (for example, the SMF can first get the UE list within the AoI and keep being updated about the UE list by subscribing to AMF, and then subscribe/unsubscribe to the relevant UPF(s) on behalf of the final consumer). This allows the UPF not having to determine the AMF where to subscribe for UE presence in the AoI.

NOTE 3: For event subscriptions requiring interactions with 5G AN, a solution where the UPF event consumer would directly subscribe to UPF and then UPF would ask SMF to send N2 SM signalling to 5G AN would be more complex and not bring advantage.

2. Direct subscription to UPF (i.e. not requiring third party subscription to UPF via SMF) shall be possible for data collection where UPF is the source as defined in TS 23.288 [5], i.e. the following cases:

A. TS 23.288 [5] Table 6.5.2-2: Data collected by NWDAF for UPF load analytics recalled in item 2 of Annex A of the TR.

B. For analytics targeting "any UE" (possibly for specific DNN and or slices) and not related with an AoI or BSSID/SSID or with a specific data flow.

NOTE 4: This can relate to use cases such as Data collected by NWDAF for UPF load analytics, User Data Congestion Analytics, Data Volume dispersion analytics, WLAN performance analytics.

C. The case described in solution 20 (UE IP address mapping information exposure by UPF) where the 5GC NF (e.g., NEF, BSF) can directly discover the UPF that performs NAT (based on the NATed IP address) and then invoke directly the NAT related API at the UPF. This is an optional feature.

Normative work will be based on NEF contacting NRF and UPF before invoking BSF.

NOTE 5: Which 5GC NF can directly discover the UPF and invoke the NAT related API will be confirmed during normative phase.

3. In Rel18:

A. the only defined consumers of UPF event SUBSCRIBE are SMF, and NWDAF.

B. the only defined consumers of UPF event notifications are AF/NEF, TSNAF/TSCTSF and NWDAF.

4. UPF event exposure Service description: This service provides events related to PDU Sessions towards consumer NF. The service operations exposed by this service allow other NFs to subscribe and get notified of events happening on UPFs.

The following events may be subscribed by a NF consumer:

- Event: QoS monitoring. This event provides QoS Flow level performance information (information listed in Solution #8, clause 6.8.2).

- Event: UserDataUsageMeasures. This event provides information of user data usage of the User PDU Session (information listed in Solution #7, clause 6.7.2).

- Event: UserDataUsageTrends. This event provides statistical measurements (information listed in Solution #7, clause 6.7.2).

When the UPF provides notifications related to UserDataUsageMeasures or UserDataUsageTrends events the notifications may indicate the time stamps for the measures and also refer to the Application Id or Packet Filter Set indicated in the consumer subscription.

5. The subscription mechanisms for the defined UPF event exposure events are as follows:

- Event: QoS monitoring. Subscription is always indirect via SMF. UPF and SMF interact using PFCP.

- Event: UserDataUsageMeasures. SBI based subscription operation shall be used by SMF and other allowed direct consumers.

- Event: UserDataUsageTrends. SBI based subscription operation shall be used by SMF and other allowed direct consumers.

6. To determine which SMF to contact the final consumer of UPF events proceeds as follows:

- If the event targets any UE, the final consumer of UPF events looks up the NRF to discover all suitable SMF(s) (e.g. SMF(s) that serve the target combination of DNN and S-NSSAI).

- If the event targets a unique UE identified by its SUPI, the final consumer of UPF events sends Nudm\_UECM\_Get\_Request (SUPI, type of requested information set to SMF Registration Info and the S-NSSAI and DNN) to UDM to get the SMF ID serving the target UE.

- If the event target are UEs identified by a Group Identifier, the final consumer of UPF events sends Nudm\_SDM\_Get\_Request to UDM and requests the list of SUPIs that correspond to the Group ID. Final consumer then proceeds with these SUPIs as described above to get SMF ID serving each UE identified by one of received SUPIs.

If the consumer of NWDAF service doesn't provide the target DNN, S-NSSAI (these parameters are optional for NWDAF service defined in TS 23.288 [5]), and the event targets a unique UE identified by its SUPI, the NWDAF gets the list of all PDU Session for that SUPI via Nudm\_UECM\_Get\_Request and then determine which (DNN, S-NSSAI) it will consider.

If the consumer of NWDAF service doesn't provide the target DNN, S-NSSAI (these parameters are optional for NWDAF service defined in TS 23.288 [5]), but provides the application server IP address/FQDN, and the event targets a unique UE identified by its SUPI or any UE, the NWDAF obtain the target DNAI from 5GC by the mapping table between Application IP range/address and DNAI as described in clause 8.7 conclusion of TR 23.700-48 [10]. After obtaining DNAI from the NEF by providing AS IP/IP range and/or FQDN, the NWDAF uses the DNAI to trigger the SMFs discovery in NRF for single UE or any UE.

Editor's note: how to support following case is FFS: the case where the consumer of NWDAF service doesn't provide the target DNN, S-NSSAI, but provides the application server IP address/FQDN.

7. For the UPF data collection, the event subscription includes Reporting suggestion information as described in Sol#14, which is used to assist the UPF event notification. Per Reporting suggestion information UPF can concatenate several notification messages to the same notification endpoint in one notification message.

Annex A:  
Analysis on the NWDAF requirements of UPF event exposure service(s)

This Annex aims at listing and analysing the NWDAF requirements of UPF event exposure service(s).

NOTE 1: This clause recalls for information the main known usage of UPF information exposure in 5GC as defined in other 3GPP documents. If this clause and the quoted other 3GPP documents are not aligned, the quoted other 3GPP documents prevails.

NWDAF requirements as defined in TS 23.288 [5], for instance (the list is not exhaustive), contain:

1. Observed Service Experience: TS 23.288 [5] of Table 6.4.2-2 of: QoS flow level Network Data from 5GC NF related to the QoS profile assigned for a particular service (identified by an Application Id or IP filter information).

The Observed Service Experience analytics may provide Service Experience for an Edge Application over a UP path: Service experience for a UE or a group UEs or any UE in an Application or a set of Applications over a specific UP path (UPF, DNAI and EC server).

The Observed Service Experience analytics may also provide "Service experience for a UE or a group of UEs in an Application or a set of Applications over a RAT Type or over a Frequency or both" as defined in Table 6.4.1-1of TS 23.288 [5].

Table 6.4.2-2 (TS 23.288 [5]): QoS flow level Network Data from 5GC NF related to the QoS profile assigned for a particular service (identified by an Application Id or IP filter information)

|  |  |  |
| --- | --- | --- |
| QoS flow Bit Rate | UPF | The observed bit rate for UL direction; and  The observed bit rate for DL direction. |
| QoS flow Packet Delay | UPF | The observed Packet delay for UL direction; and  The observed Packet delay for the DL direction. |
| Packet transmission | UPF | The observed number of packet transmission. |

For NWDAF to provide Service Experience for an Application: Consumer NF sends an Analytics request/subscribe (Analytics ID = Service Experience, Target of Analytics Reporting = any UE or a UE identified by a SUPI or a group of UEs identified by a Group Id, Analytics Filter Information = (Application ID, S-NSSAI, DNN, Application Server Address(es), Area of Interest), Analytics Reporting Information=Analytics target period) to NWDAF.

2. Table 6.5.2-2 of TS 23.288 [5]: Data collected by NWDAF for UPF load analytics.

Table 6.5.2-2 (TS 23.288 [5]): Data collected by NWDAF for UPF load analytics

|  |  |  |
| --- | --- | --- |
| Information | Source | Description |
| Traffic usage report | UPF | Report of user plane traffic in the UPF |

UPF should report all traffic for all N4 (PDU) sessions that meet some criteria (S-NSSAI, Area of interest) -> SMF involvement may be considered when it is needed to determine which UPF(s) serve a UE in the area of interest.

- Table 6.7.3.2-1 of TS 23.288 [5]: Service Data from 5GC related to UE communication.

Table 6.7.3.2-1 (TS 23.288 [5]): Service Data from 5GC related to UE communication

|  |  |  |
| --- | --- | --- |
| UE communication (1..max) | UPF, AF | Communication description per application |
| >Communication start |  | The time stamp that this communication starts |
| >Communication stop |  | The time stamp that this communication stops |
| >UL data rate |  | UL data rate of this communication |
| >DL data rate |  | DL data rate of this communication |
| >Traffic volume |  | Traffic volume of this communication |
| > N4 Session ID | SMF, UPF | Identification of N4 Session. |
| > Inactivity detection time | SMF, UPF | Value of session inactivity timer. |

5GC Consumer NF sends a request to the NWDAF for analytics on UE(s), where the analytics type indicated by "Analytics ID" is set to "UE communication". The Target of Analytics Reporting is set to SUPI or an Internal Group Identifier and Analytics Filter may include Application ID and Area of Interest.

3. Table 6.8.2-2 of TS 23.288 [5]: Data Collected from the UPF or from the AF related to User Data Congestion Analytics.

Table 6.8.2-2 (TS 23.288 [5]): Data Collected from the UPF or from the AF related to User Data Congestion Analytics

|  |  |  |
| --- | --- | --- |
| Information | Source | Description |
| Application ID | UPF or AF | Application identifier as defined in TS 23.501 [2] clause 5.8.2 (see NOTE 1). |
| IP Packet Filter Set | UPF or AF | IP Packet Filter set as defined in TS 23.501 [2] clause 5.8.2 (see NOTE 1). |
| Measurement period | UPF or AF | Measurement period. |
| Throughput UL/DL | UPF or AF | Average Throughput UL/DL over the measurement period. |
| Throughput UL/DL (peak) | UPF or AF | Peak Throughput UL/DL over the measurement period. |
| Timestamp | UPF or AF | Time when measurements are taken. |
| Achieved sampling ratio | UPF | Sampling ratio achieved by UPF (see NOTE 2). |
| NOTE 1: Application Id and IP Packet Filter Set are mutually exclusive.  NOTE 2: UPF may apply data sampling to reduce the load on the UPF. This parameter is provided when no sampling ratio is configured at the UPF or the UPF could not fulfil the configured sampling ratio.  NOTE 3: Multiple outputs are provided by the UPF when multiple Service Data Flows are running at the UPF for the same UE and measurement period.  NOTE 4: How NWDAF collects information from UPF is not defined in this Release of the specification. | | |

The Consumer NF indicates a request for analytics for congestion in a specific location. The Analytics ID is set to "User Data Congestion" for transfer over user plane, control plane, or both, the Target of Analytics Reporting is set to "any UE" and Analytics Filter Information set to include a location (e.g. ECGI, TA) and an indication to provide the list of applications that contribute the most to the traffic.

4. Table 6.10.2-5 of TS 23.288 [5]: UE data volume dispersion collected from serving UPF.

Table 6.10.2-5 (TS 23.288 [5]): UE data volume dispersion collected from serving UPF

|  |  |  |
| --- | --- | --- |
| Information | Source | Description |
| UE IP address | UPF | UE IP address. |
| Timestamp | UPF | Time stamp of the collected information. |
| Data Volume UL/DL | UPF | Sum of UE data volume exchanged per UE across all applications. |
| NOTE: The Data volume can be reported either as total volume of the PDU session or periodically. It refers to the Data volume exchanged between the start and stop of the PDU session. When reported periodically, the period can be specified in the requested analytic target period or configured as a default value in the UPF. | | |

Table 6.10.2-6: UE data volume dispersion collected from serving UPF

|  |  |  |
| --- | --- | --- |
| Information | Source | Description |
| UE IP address | UPF | UE IP address. |
| Timestamp | UPF | A timestamp of the collected information. |
| Application ID | UPF | Identify the application at the UPF |
| IP 5-tuple | UPF | IP 5-tuple. |
| Location of Application | UPF | List of Internet applications represented by DNAI(s). |
| Data Volume UL/DL | UPF | Sum of UE data volume exchanged per application during the period. |
| Application duration | UPF | Duration for the application (e.g. Voice talk time). |
| NOTE 1: Application ID and IP 5-tuple are mutually exclusive.  NOTE 2: Multiple outputs are provided by the UPF when multiple applications are running at the UPF for the same UE and time period.  NOTE 3: The Data volume can be reported either as total volume of the PDU session or periodically. It refers to the Data volume exchanged between the start and stop of the PDU session. When reported periodically, the period can be specified in the requested analytic target period or configured as a default value in the UPF. | | |

In table 6.10.2-5, the data volume is collected per UE from the UPF. The collected UE information is applicable across all applications used by the UE between start and stop of the PDU session. The UPF reports volume per UE IP address across all applications.

In table 6.10.2-6, the UPF reports data volume per UE for specific application(s) in relation to the start and stop of the application as indicated by the application duration.

The Consumer NF sends a request to the NWDAF for dispersion analytics on a specific UE, any UE, or a group of UEs, using either the Nnwdaf\_AnalyticsInfo or Nnwdaf\_AnalyticsSubscription service. The Analytics ID is set to "UE Dispersion Analytics", the Dispersion Analytic (DA) type is set to "Data Volume Dispersion Analytics" (DVDA) or "Transactions Dispersion Analytics" (TDA) and Analytic Filter Information = (Area of Interest, slice, target period, optional UE class: Top-Heavy, Fixed, or Camper UEs). The NF or AF provides the UE ID or Internal Group ID in the Target of Analytics Reporting.

5. Clause 6.11.1 of TS 23.288 [5] on "WLAN performance analytics" requests:

Target of Analytics Reporting: a single UE (SUPI), a group of UEs (an Internal Group ID), or any UE.

Analytics Filter Information:

- Area of Interest (list of TA or Cells);

NOTE 2: Even though the Area of Interest may have been meant to indicate a UE location, it is questionable to use this information considering UE(s) that are IDLE over 3GPP access and thus whose 3GPP location cannot be determined. UPEAS is not meant to have UE impact.

- SSID(s);

- BSSID(s); and

The reporting should only apply for traffic exchanged on a target SSID and BSSID thus the UPF reporting should only be reported for target UE(s) exchanging traffic on a target SSID and BSSID or the UPF should be aware of the target SSID/BSSID.

|  |  |  |
| --- | --- | --- |
| UE communications (1..max) | UPF | List of communication time slots |
| > Communication start |  | The time stamp that PDU session(s) for WLAN starts. |
| > Communication stop |  | The time stamp that PDU session(s) for WLAN ends. |
| > UL data rate |  | UL data rate of PDU session(s) for WLAN. |
| > DL data rate |  | DL data rate of PDU session(s) for WLAN. |
| > Traffic volume |  | Traffic volume of PDU session(s) for WLAN. |

6. Clause 6.14.1 of TS 23.288 [5] "User plane performance analytics" requests:

- User plane performance analytics for a specific Edge Computing application for a UE, group of UEs, or any UE over a specific serving anchor UPF.

- User plane performance analytics for a specific Edge Computing application for a UE, group of UEs, or any UE over a specific DNAI.

- User plane performance analytics for a specific Edge Computing application for a UE, group of UEs, or any UE over a specific Edge Application Server Instance.

Analytics consumer sends an Analytics request/subscribe (Analytics ID = DN Performance Target of Analytics Reporting, Analytics Filter Information = (Application ID, S-NSSAI, DNN, Area of Interest, UPF anchor ID, DNAI, Application Server Address(es)), Analytics Reporting Information = Analytics target period) to NWDAF by invoking a Nnwdaf\_AnalyticsInfo\_Request or a Nnwdaf\_AnalyticsSubscription\_Subscribe service.

Some of these analytics target Any UE (possibly for specific DNN and or slices) and the NWDAF acting as a consumer of UPF exposure may target any UPF that serves the corresponding specific DNN and or slices.

Some of these analytics target a specific UE and it is thus needed for the NWDAF subscription to be forwarded to the UPF(s) that serve the target PDU sessions of this UE.

Annex B:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-02 | SA2#149E | S2-2200094 | - | - | - | Proposed skeleton agreed at S2#149E | 0.0.0 |
| 2022-02 | SA2#149E | - | - | - | - | Documents approved p-CR at S2#149E, including S2-2200095, S2-2201822, S2-2201823, S2-2201824, S2-2201825, S2-2201826 | 0.1.0 |
| 2022-04 | SA2#150E | - | - | - | - | Documents approved p-CR at S2#150E, including S2-2202758, S2-2203581, S2-2203582, S2-2203583, S2-2202652, S2-2203584, S2-2203585, S2-2203586, S2-2203587, S2-2203588 | 0.2.0 |
| 2022-05 | SA2#151E | - | - | - | - | Documents approved p-CR at S2#151E, including S2-2204311, S2-2204515, S2-2205320, S2-2204880, S2-2204881, S2-2204882, S2-2204883, S2-2204884, S2-2204885, S2-2204886, S2-2204887, S2-2204888, S2-2204520, S2-2204889, S2-2204890, S2-2204891, S2-2203748, S2-2204892, S2-2204893, S2-2204894 | 0.3.0 |
| 2022-08 | SA2#152E | - | - | - | - | Documents approved p-CR at S2#152E, including S2-2205868, S2-2205885, S2-2206149, S2-2206309, S2-2206324, S2-2206731, S2-2207188, S2-2207189, S2-2207190, S2-2207191, S2-2207192, S2-2207193, S2-2207194, S2-2207195, S2-2207196, S2-2207197 | 0.4.0 |
| 2022-09 | SA#97-e | SP-220827 | - | - | - | MCC editorial update for presentation to TSG SA for information | 1.0.0 |