|  |  |
| --- | --- |
| 3GPP TR 23.700-48 V0.2.0 (2022-04) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  5G System Enhancements for Edge Computing; Phase 2  (Release 18) | |
|  | |
|  | 3GPP-logo_web |
|  | |
| 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 Void 9

3.3 Abbreviations 9

4 Architectural assumptions and principles 10

4.1 Architectural Assumptions 10

4.2 Architectural Requirements 10

5 Key issues 10

5.1 KI#1: Accessing EHE in a VPLMN when roaming 10

5.1.1 Description 10

5.1.2 Scenarios 11

5.1.3 Assumptions 11

5.2 KI#2: Fast and efficient network exposure improvements 11

5.2.1 Description 11

5.2.2 Use cases and scenarios 12

5.2.3 Assumptions 12

5.3 KI#3: Policies for finer granular sets of UEs 12

5.3.1 Description 12

5.3.2 Scenarios 13

5.3.3 Assumptions 13

5.4 KI#4: Influencing UPF and EAS (re)location for collections of UEs 13

5.4.1 Description 13

5.4.2 Scenarios 14

5.4.3 Assumptions 14

5.5 KI#5: GSMA OPG impacts and improvements for EHE operated by separate party 14

5.5.1 Description 14

5.5.2 Scenarios 15

5.5.3 Assumptions 15

5.6 KI#6: Avoiding UE to switch away from EC PDU Session 15

5.6.1 Description 15

5.6.2 Scenarios 16

5.6.3 Assumptions 16

5.7 KI#7: Obtain and maintain mapping table between IP address/IP range with DNAI 16

5.7.1 Description 16

5.7.2 Scenarios 17

5.7.3 Assumptions 17

6 Solutions 17

6.0 Solution-Key issue matrix 17

6.1 Solution 01 (KI#1): EAS discovery in Home Routed roaming scenario 18

6.1.1 Description 18

6.1.2 Procedures 19

6.1.2.1 Procedure for EAS discovery when HPLMN has the knowledge of EAS deployment information in VPLMN 19

6.1.2.2 Procedure for EAS discovery when HPLMN does not have the knowledge of EAS deployment information in VPLMN 20

6.2 Solution 02 (KI#1): Session Breakout in Visited PLMN 21

6.2.1 Description 21

6.2.2 Procedure 22

6.3 Solution 03 (KI#1): EAS (re)discovery procedure in roaming scenario 23

6.3.1 Description 23

6.3.2 Procedures 24

6.3.2.1 EAS discovery procedure in roaming scenario 24

6.3.2.2 EAS rediscovery procedure in roaming scenario 27

6.3.3 Impacts on existing entities and interfaces 28

6.4 Solution 04 (KI#1): Support EAS discovery in VPLMN via HR PDU Session 28

6.4.1 Description 28

6.4.2 Procedure 29

6.4.3 Impacts on services, entities and interfaces 31

6.5 Solution 05 (KI#1): Accessing V-EHE via HR PDU session 31

6.5.1 Description 31

6.5.2 Procedures 32

6.5.3 Impacts on services, entities and interfaces 33

6.6 Solution 06 (KI#1): URSP solution to support roamers access to EHE in a VPLMN 33

6.6.1 Description 33

6.6.2 Procedures 34

6.6.3 Impacts on Existing Nodes and Functionality 34

6.7 Solution 07 (KI#1): Using URSP Rules to Establish an LBO PDU Session 35

6.7.1 Description 35

6.7.1.1 General 35

6.7.1.2 Procedure 35

6.7.2 Impacts on services, entities and interfaces 35

6.8 Solution 08 (KI#1): V-ECS Discovery during Steering of Roaming 36

6.8.1 Description 36

6.8.1.1 General 36

6.8.1.2 Procedure 36

6.8.2 Impacts on services, entities and interfaces 38

6.9 Solution 09 (KI#1): PDU Session configuration from EASDF 38

6.9.1 Description 38

6.9.2 Procedures 39

6.9.2.1 Procedures for PDU Session configuration from EASDF 39

6.9.3 Impacts on services, entities and interfaces 40

6.10 Solution 10 (KI#1): LBO PDU Session establishment using PLMN criteria in RSD 40

6.10.1 Description 40

6.10.2 Procedure 41

6.10.3 Impacts on services, entities and interfaces 41

6.11 Solution 11 (KI#2): Exposure of Network Congestion 41

6.11.0 General 41

6.11.1 Procedure 41

6.11.2 Impacts on services, entities and interfaces 43

6.12 Solution 12 (KI#2): Efficient exposure of RAN information 43

6.12.1 Key Issue mapping 43

6.12.2 Description 43

6.12.3 Procedures 45

6.12.3.1 Procedure for subscribing information 45

6.12.3.2 Procedure for information report 46

6.12.4 Impacts on services, entities and interfaces 47

6.13 Solution 13 (KI#2): Fast and efficient network exposure improvements 47

6.13.1 Introduction 47

6.13.2 Functional Description 48

6.13.3 Procedures 48

6.13.4 Impacts on services, entities and interfaces 50

6.14 Solution 14 (KI#4): Group Management 50

6.14.1 Introduction 50

6.14.2 Functional Description 50

6.14.3 Procedures 52

6.14.4 Impacts on services, entities and interfaces 54

6.15 Solution 15 (KI#4): Selection of common DNAI 54

6.15.1 Introduction 54

6.15.2 Functional Description 55

6.15.3 Procedures 55

6.15.3.1 General 55

6.15.3.2 Selection of the common DNAI 57

6.15.3.3 EAS selection and re-selection using ECS option, preconfigured 58

6.15.3.4 EAS selection and re-selection using ECS option, dynamic invoke of gSMF 59

6.15.3.5 EAS selection and re-selection via application layer 60

6.15.4 Impacts on services, entities and interfaces 61

6.16 Solution 16 (KI#4): Selecting the same EAS/DNAI for collection of UEs 62

6.16.1 Description 62

6.16.2 Procedures 62

6.16.3 Impacts on services, entities and interfaces 63

6.17 Solution 17 (KI#4): Application layer EAS selection for collections of UEs 64

6.17.1 Introduction 64

6.17.2 Functional Description 64

6.17.3 Procedures 64

6.17.3.1 EAS selection for multiple UE based application layer 64

6.17.4 Impacts on services, entities and interfaces 65

6.18 Solution 18 (KI#4): Discovery of the same EAS for collections of UEs 66

6.18.1 Description 66

6.18.2 Procedures 67

6.18.2.1 EASDF-related procedure 67

6.18.2.2 Direct DNS response to UE 68

6.18.2.3 EAS Discovery Procedure with Local DNS Server/Resolver 69

6.18.3 Impacts on services, entities and interfaces 69

6.19 Solution 19 (KI#4): Influencing UPF and EAS (re)location for collections of UEs 70

6.19.1 Introduction 70

6.19.2 Functional Description 70

6.19.3 Procedure 70

6.20 Solution 20 (KI#5): Global EASDF 71

6.20.1 Description 71

6.20.2 Procedures 72

6.20.2.1 Procedure for Global EASDF 72

6.20.3 Impacts on services, entities and interfaces 72

6.21 Solution 21 (KI#5): EAS Deployment information differentiated by PLMN ID 73

6.21.1 Introduction 73

6.21.2 Functional Description 73

6.21.3 Procedures 73

6.21.4 Impacts on services, entities and interfaces 73

6.22 Solution 22 (KI#5): EAS discovery for federated OPs 74

6.22.1 Introduction 74

6.22.2 Functional description 74

6.22.2.0 Option 0: SMF configuration 74

6.22.2.1 Option 1: Shared EASDF 74

6.22.2.2 Option 2: Per-PLMN EASDFs 75

6.22.3 Procedures 77

6.22.3.0 Option 0: SMF configuration 77

6.22.3.1 Option 1: Shared EASDF 78

6.22.3.2 Option 2: Per-PLMN EASDFs 79

6.22.4 Impact on existing entities and interfaces 80

6.22.4.0 Option 0: SMF configuration 80

6.22.4.1 Option 2: Shared EASDF 80

6.22.4.2 Option 3: Per-PLMN EASDFs 80

6.23 Solution 23 (KI#5): Improvements for EHE operated by separate party 80

6.23.1 Introduction 80

6.23.2 Functional Description 81

6.23.3 Solution Details 81

7 Evaluation 82

8 Conclusions 82

Annex A: Change history 82

# 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

Editor's note: The content of this clause is based on SP-211638, and can be improved based on contributions.

The present document describes key issues and solutions for the phase 2 of the system enhancements for Edge Computing in 5GS.

Edge Computing is supported in 5GS since Rel-15. During Rel-17 FS\_enh\_EC study described in TR 23.748 [4] , further enhancements for supporting Edge Computing have been studied, including discovery and re-discovery of EAS, edge relocation etc. 4 key issues from FS\_enh\_EC study have been concluded and progressed in TS 23.548 [3] . Some other issues were raised during the Rel-17 study but not studied due to the time limitation in Rel-17.

This technical report will document the study of potential system enhancements for enhanced edge computing support, including:

- improvements to roaming, to support access to EHE in a VPLMN (WT#1);

- defining use cases that may benefit from exposure of additional data via the Local UPF/NEF including describing (on a high level) the characteristics of the data and data delivery to fulfil the use cases; investigating the solutions and their feasibility and suitability for improved network exposure of UE traffic related information to common Edge Application Server via Local UPF/NEF, such as network congestion status (WT#3);

NOTE: XR/media and AI/ML services specific QoS information exposure are to be studied in corresponding study items with considering the same exposure framework as defined by this study.

NOTE: This objective will look at the use cases and the data to be exposed but not at the actual UPF exposure mechanism or UPF-originated data, if/when already covered by FS\_UPEAS.

- investigating the potential need and solutions for supporting offload policies to match more granular sets of UE(s) without exposing operator-internal configurations to 3rd party AFs (WT#5);

- investigating the potential need and solutions to influence of PSA-UPF and EAS (re)location for collection of UEs, e.g. in scenarios when UE(s) should use the same EAS and are not members of a pre-defined group (WT#6);

- investigating potential impacts related to the GSMA Operator Platform Group work, and potential improvements related with 5GC and EHE being operated by different organizations (WT#7);

- investigating the potential need and solutions to avoid the UE to switch the EC traffic away from the EC PDU Session and 5GS altogether, due to conflicting connectivity preferences in the device (e.g. via means outside of 3GPP connectivity, e.g. non-integrated Wifi) (WT#8);

- investigating the potential solutions for the AF to be able to obtain/determine the DNAI that is associated to a certain selected EAS, for subsequent use with already defined services provided to the AF (WT#9).

# 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)".

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

[4] 3GPP TR 23.748: "Study on enhancement of support for Edge Computing in 5G Core network (5GC)".

[5] GSMA OPG.02: "Operator Platform Telco Edge Requirements", https://www.gsma.com/futurenetworks/wp-content/uploads/2021/07/GSMA-OPG-Telco-Edge-Requirements-2021.pdf.

[6] SP-210583: "Reply LS to GSMA Operator Platform Group on edge computing definition and integration", SA#92e.

[7] IETF RFC 5681: "TCP Congestion Control".

[8] 3GPP TS 26.247: "Transparent end-to-end Packet-switched Streaming Service (PSS); Progressive Download and Dynamic Adaptive Streaming over HTTP (3GP-DASH)".

[9] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".

[10] 3GPP TR 23.700-85: "Study on enhancement of 5G User Equipment (UE) policy".

[11] 3GPP TS 24.526: "User Equipment (UE) policies for 5G System (5GS); Stage 3".

[12] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode".

[13] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS)".

[14] 3GPP TS 38.415: "NG-RAN; PDU session user plane protocol".

[15] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)".

# 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], TS 23.501 [2], TS 23.548 [3] 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].

## 3.2 Void

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1], TS 23.501 [2], TS 23.548 [3] 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].

# 4 Architectural assumptions and principles

## 4.1 Architectural Assumptions

Existing solutions defined in Rel-15, Rel-16 and Rel-17 will be considered as baseline in this study.

The architecture for support of Edge Computing in 5GC shall be based on the following architecture assumptions:

- the architecture for Edge computing specified in Release 17 is used as basis for further potential enhancement;

- the Edge Hosting Environment (EHE) can be under the control of the serving network operator or a 3rd party;

- interconnectivity between EHEs of different operators cannot be assumed to be available for all deployments.

## 4.2 Architectural Requirements

Editor's note: This clause will document agreed architecture requirements.

- The solutions should minimize the impact on the application layer.

# 5 Key issues

## 5.1 KI#1: Accessing EHE in a VPLMN when roaming

### 5.1.1 Description

Editor's note: This key issue corresponds to Work Task #1 in SP-211638. This clause can be further improved based on contributions.

The purpose of this key issue is to define 5GS improvements to support the UE access to an EHE in a VPLMN.

Two scenarios (i.e. UE accessing EHE in VPLMN via an LBO PDU Session and UE accessing EHE in VPLMN via a PDU Session established as HR) are described in clause 5.1.2.

For the scenario using LBO PDU Session, potential solutions should address the following:

- how to establish the LBO PDU Session towards the correct S-NSSAI/DNN pair in order to access an EHE in the VPLMN;

- how to support Rel-17 edge computing related procedures, such as EAS (re-)discovery, as specified in TS 23.548 [3], clause 6.

For the scenario using a PDU Session with a PSA in the HPLMN, potential solutions should address the following:

- how to authorize the PDU session to support local traffic routing to access an EHE in the VPLMN;

- whether and how to support charging for the local traffic of a PDU session that supports local traffic routing to access an EHE in the VPLMN;

- how to support Rel-17 edge computing related procedures, such as EAS (re-)discovery, as specified in TS 23.548 [3], clause 6;

- how to ensure proper policy control and QoS enforcement;

- potential impact on Policy and QoS control;

- how to configure the VPLMN ECS address to UE in roaming scenarios;

- how to support the edge relocation in roaming scenarios.

NOTE 1: Interaction with SA5 is expected regarding charging aspects where needed.

NOTE 2: Latency needs to be considered and addressed for all scenarios.

NOTE 3: In Rel-17, the ECS address is provided by UDM, which requires further consideration in scenarios with ECS in a VPLMN. This may need some coordination with SA WG6.

### 5.1.2 Scenarios

Editor's note: This clause will document the scenarios (and potential associated use cases) applicable to KI#1, if any. This clause will be removed if left empty.

For a roaming UE, accessing to EHE in VPLMN might be needed to fulfil use cases requiring edge computing. Two main scenarios should be considered:

1) UE accessing V-EHE via a Local Breakout (LBO) PDU Session:

The scenario supports all connectivity models and assumes that an LBO PDU Session is used to access an EHE in VPLMN for EC applications.

With a LBO PDU Session, the UE can access an EHE in VPLMN.

NOTE 1: Two different PDU Sessions are required to access an EHE in VPLMN and Home DN in HPLMN. With this scenario, it requires two sets of configurations (i.e. DNN and S-NSSAI pair).

2) UE accessing V-EHE via a Home Routed (HR) PDU Session (i.e. with PSA in HPLMN):

This scenario assumes the session breakout for the HR PDU Session is used to access EHE in VPLMN for EC application.

With a single PDU Session, UE can access an EHE in VPLMN and also the DN in HPLMN.

NOTE 2: With a single PDU Session and (DNN+S-NSSAI), it can support both EC and non-EC applications in either roaming or non-roaming case.

To support such PDU Session, it needs to be studied how the UE can access the V-EHE via a HR PDU Session. Two sub-scenarios may be considered:

2.1) HPLMN has the knowledge of EAS deployment information in VPLMN for specific services. The HPLMN triggers EAS discovery and local traffic routing in VPLMN.

2.2) HPLMN does not have the knowledge of EAS deployment information in VPLMN. The VPLMN triggers EAS discovery and local traffic routing in VPLMN.

### 5.1.3 Assumptions

Editor's note: This clause will document assumptions applicable to KI#1, if any. This clause will be removed if left empty.

## 5.2 KI#2: Fast and efficient network exposure improvements

### 5.2.1 Description

Editor's note: This key issue corresponds to Work Task #3 in SP-211638. This clause can be further improved based on contributions.

This key issue addresses improvements to fast and efficient network exposure of UE traffic related information to Edge Application Server via Local UPF/NEF to support additional information, such as network congestion status.

This key issue defines use cases that may benefit from exposure of additional data via the Local UPF/NEF including describing (on a high level) the characteristics of the data and data delivery to fulfil the use cases.

Based on the use cases, this key issue investigates solutions and their feasibility and suitability for improved network exposure of UE traffic related information to common Edge Application Server via Local UPF/NEF, such as network congestion status. In this case, the following issues should be studied:

- which information and at which level (e.g., per QoS Flow, per cell) needs to be provided to AF via local UPF/NEF?

- how the above information is obtained?

NOTE 1: XR/media and AI/ML services specific QoS information exposure are to be studied in corresponding study items with considering the same exposure framework as defined by this study.

NOTE 2: This key issue will look at the use cases and the data to be exposed but not at the actual UPF exposure mechanism or UPF-originated data, if/when already covered by the FS\_ UPEAS. UPF exposure mechanism to be discussed in FS\_UPEAS is possibly reused.

NOTE 3: The aim is to, whenever possible, re-use information already defined in existing 3GPP specifications.

### 5.2.2 Use cases and scenarios

Observation of the link characteristics is widely used to adjust the transmission behaviour in different scenarios. For example:

- For some transport layer protocols, e.g. TCP, QUIC, congestion control algorithms can be used to control packets transmission via 5GS based on e.g. observing packet loss and take it as indication of network congestion. For example, TCP congestion control algorithm defined in RFC 5681 [7] uses different ways to adjust congestion window, perform slow start, congestion avoidance, fast retransmit, and fast recovery, which leads to classic "sawtooth" congestion window.

- Media based services can benefit by low and consistent latency. This can be achieved by rate adaptation by the endpoints.

For Edge computing scenarios, most applications are sensitive to the change of network latency and throughput. When network congestion happens, if the application can be notified in a fast and efficient way (e.g. within a RTT of user packet transmission), these services can react to the change of network congestion status more agilely.

Editor's note: The use case(s) using network conditions needs further description including examples of typical applications.

NOTE: The solution in the following section 6 will use the use case(s) in this section as guidance to judge the feasibility and suitability.

### 5.2.3 Assumptions

Editor's note: This clause will document assumptions applicable to KI#2, if any. This clause will be removed if left empty.

## 5.3 KI#3: Policies for finer granular sets of UEs

### 5.3.1 Description

This key issue investigates the potential need and solutions for supporting offload policies for more granular sets of UE(s).

This key issue will study the following aspects:

- how to identify set of UEs at a finer granularity that are associated with a dedicated offload policy, and how to express the set of UE in the offload policy;

- impacts to 5GS needed to support providing traffic offload policy for such a set of UEs.

### 5.3.2 Scenarios

Considering limited or expensive EC resources, the application service provider or the operator may consider to provide EC services for certain users only under certain conditions, e.g., within a specific geographical area, or at specific time, etc. The AFs can provide the request to support some offload policies only for certain set of UE(s) following a set of specific criteria.

There are cases that traffic offload policy aims at a finer sets of UE(s), for instance, UEs satisfying a combination of criteria:

Case a: UEs within a specific geographical area and have been associated with specific service provided by operator or application service provider;

Case b: UEs that have been associated with a combination of services provided by operator or application service provider;

Case c: UEs within a specific geographical area and have been associated with a combination of services provided by operator or application service provider;

Case d: at specific time, UEs that have been associated with specific service or a combination of services provided by operator or application service provider;

Case e: UEs belongs to both group-A and group-B, or UEs belongs to group-A and associated with specific service. It is possible that these users belong to pre-defined groups or do not belong to any pre-defined groups.

### 5.3.3 Assumptions

Editor's note: This clause will document assumptions applicable to KI#3, if any. This clause will be removed if left empty.

Operator-internal configurations shall not be exposed to 3rd party AFs.

The application can be deployed in both central location(s) and edge cloud(s).

The application service provider is expected to be able to interact with the operator regarding setting the offload policies.

Solutions for this KI will identify their support for the following:

- AF under operator control;

- AF under 3rd party control.

## 5.4 KI#4: Influencing UPF and EAS (re)location for collections of UEs

### 5.4.1 Description

Editor's note: This key issue corresponds to Work Task #6 in SP-211638. This clause can be further improved based on contributions.

Investigate the potential need and solutions to influence of PSA-UPF and EAS (re)location for collection of UEs, e.g. in scenarios when UE(s) should use the same EAS and are not members of a pre-defined group.

In particular, the key issue will study the following aspects:

- whether and how to define a collection of UEs forming a dynamic ad-hoc group that should use the same EAS and/or same local part of DN and/or same DNAI and how the collection is identified;

- whether and how to influence UPF and EAS (re)location for a collection of UEs that should use the same EAS and/or same local part of DN and/or same DNAI;

- how to decide on a common local part of DN for the collection of UEs;

- for a given collection of UEs defined in the above, whether and how to determine if any UE in this collection have no access to EAS or local part of DN, and whether and how to define any specific treatments for such UE if any;

- how to handle coordination of the UPF(s) and EAS (re)location for collections of UEs;

- whether and how existing mechanisms suffice;

- whether and what improvements are required for EAS discovery and re-discovery for UEs belonging to a collection of UEs.

### 5.4.2 Scenarios

Editor's note: This clause will document the scenarios (and potential associated use cases) applicable to KI#4, if any. This clause will be removed if left empty.

There are use cases that UEs belonging to a non-predefined dynamic group should be treated the same way, and members of the dynamic group is likely to change dynamically, e.g. UE could join/leave the group randomly. For example:

- Multi-user low latency Gaming: In such use cases, the Application client running on the UE are served by a particular application server which is the corresponding game hosting server i.e. Edge Application Server (EAS). This EAS provides gaming services and maintains individual UEs gaming profile, user level registration details, etc. These members could change dynamically over period of time. Also, due to maintenance purposes or due to overload situation EAS would require to be relocated to another one, thus moving all registered users to the new EAS.

- Platooning: In case of platooning use case, all the member UEs involved have similar attributes and requirements, for example, all UEs in a particular platoon have similar mobility characteristics i.e. moving in the same direction and with similar speed, located in proximity to each other, and so on.

### 5.4.3 Assumptions

Editor's note: This clause will document assumptions applicable to KI#4, if any. This clause will be removed if left empty.

## 5.5 KI#5: GSMA OPG impacts and improvements for EHE operated by separate party

### 5.5.1 Description

As indicated in the LS out SP-210583 to GSMA Operator Platform Group (OPG) [6], the ongoing GSMA OPG work may have impacts on 5G architecture.

GSMA OPG introduced the concept of Federation of Operator Platforms introduced in GSMA OPG.02 [5], to allow Application Providers to reach a wider geographical area and user base. The following aspects shall be studied:

- investigate potential impacts related to the GSMA Operator Platform Group work, and potential improvements related with 5GC network and EHE being operated by different organizations;

- investigate potential impacts related to the GSMA Operator Platform Group work on EAS discovery;

- how the 5GS facilitates edge relocation between an EAS deployed by a source EHE provider to another EHE deployed by a target EHE provider, even in scenarios when EHEs are operated by different service providers.

### 5.5.2 Scenarios

Clause 3.3.5 of the GSMA OPG.02 [5] requirement document introduces the Edge Node Sharing scenario in which EAS A (hosted by Operator A) is to be accessed by Operator B’s network (see Figure 2 of clause 3.3.5 of GSMA OPG.02 [5] in Figure 5.5.2-1 below). The same modelling and solutions of a 3rd party provider hosting the EHE are considered.

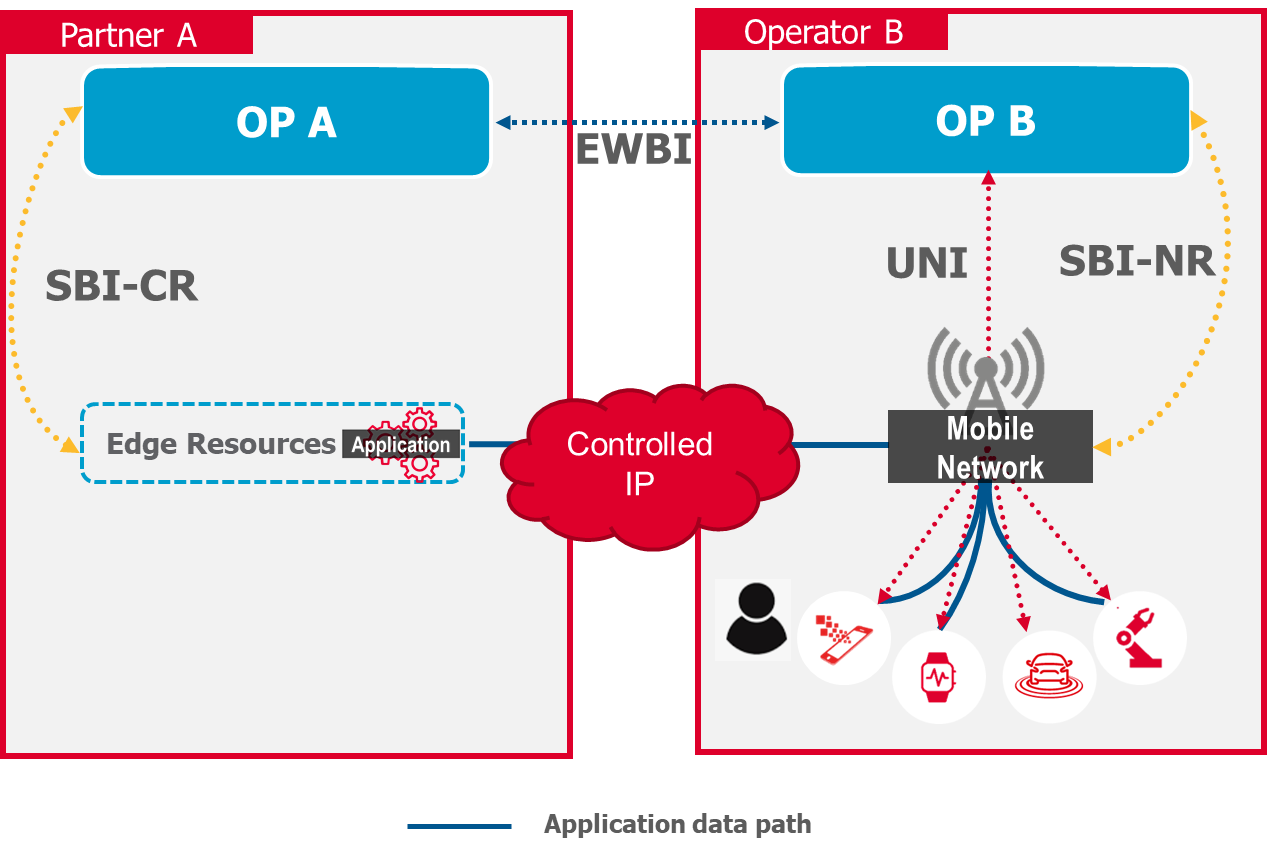


Figure 5.5.2-1: Edge Node Sharing scenario as per GSMA OPG.2 [5].

In Figure 5.5.2-1, the following terms defined in the GSMA OPG.02 [5] requirement document are used:

E/WBI East/Westbound Interface

OP Operator Platform

SBI-CR Southbound Interface – Cloud Resources

SBI-NR Southbound Interface – Network Resources

UNI User to Network Interface

### 5.5.3 Assumptions

Editor's note: This clause will document assumptions applicable to KI#5, if any. This clause will be removed if left empty.

## 5.6 KI#6: Avoiding UE to switch away from EC PDU Session

### 5.6.1 Description

Editor's note: This key issue corresponds to Work Task #8 in SP-211638. This clause can be further improved based on contributions.

This key issue investigates the potential need and solutions to avoid the UE to switch the EC traffic away from the EC PDU Session and 5GS altogether, due to conflicting connectivity preferences in the device (e.g. via means outside of 3GPP connectivity, e.g. non-integrated Wi-Fi).

In particular, this key issue will address:

- how to determine what traffic is using the 5G System to access edge computing resources, and specifically in what granularity the traffic can be identified (e.g. Flow and/or PDU Session);

- what actions might be taken when some application traffic is currently using the 5G System to access edge computing resources and connectivity outside of 5GS becomes available.

Editor's note: If and how to address user preferences is FFS.

### 5.6.2 Scenarios

Editor's note: This clause will document the scenarios (and potential associated use cases) applicable to KI#6, if any. This clause will be removed if left empty.

5GS may provide a number of enablers for Edge Computing, those for 3GPP Rel-17 being specified in TS 23.548 [3]. For example:

- EAS (Re-)discovery for Distributed Anchor and Multiple PDU Sessions Connectivity Model;

- EAS (Re-)discovery over Session Breakout Connectivity Model;

- Edge Relocation Involving AF Change.

In some scenarios, these Edge Computing enablers cannot be used if the UE switches to an access for all UP traffic that is not integrated with 5GS or does not provide the expected characteristics. Problematic cases include:

- non-integrated access, where re-connecting to the 5GS is not possible, e.g., because lack of UE support or an N3IWF could not be discovered or connected to and these Edge Computing enablers can only be reached via the 5GS;

- re-connecting to the 5GS is possible but results in long UP paths because of e.g., a centralized N3IWF;

- session breakout scenarios where an UL CL and L-PSA is used to obtain EC connectivity and switching to an access that is not integrated with 5GS would therefore break the EC connectivity.

A UE may use a PDU Session to access Edge Computing Services. When non-integrated connectivity becomes available for the UE, the UE's connectivity preferences may dictate that the UE use the non-integrated connectivity for traffic that is currently accessing Edge Computing Services via the 5G System.

### 5.6.3 Assumptions

Editor's note: This clause will document assumptions applicable to KI#6, if any. This clause will be removed if left empty.

This key issue should consider all of the connectivity models that are described in clause 4.3 of TS 23.548 [3] (i.e. Distributed Anchor Point, Session Breakout, and Multiple PDU Session).

## 5.7 KI#7: Obtain and maintain mapping table between IP address/IP range with DNAI

### 5.7.1 Description

For edge computing scenarios, it is important for AF to obtain target DNAI in order to determine the target new EAS for edge relocation. Up to Rel-17, it has been assumed that the AF has been provisioned with the proper DNAI information if it is required to use it during its interactions with the 5GC. This key issue will investigate the potential solutions for the AF to be able to obtain/determine the DNAI that is associated to a certain selected EAS, for subsequent use with already defined services provided to the AF.

The following aspects shall be studied:

- what information the AF should provide to 5GC (e.g., IP address or range thereof (i.e.IPv4 subnetwork and IPv6 prefixes) , FQDN) and how it should provide it to help determine proper DNAI if the AF does not have knowledge of the DNAI information;

- whether and how the 5GC can provide a DNAI to AF to help the subsequent AF influence/request.

### 5.7.2 Scenarios

What we have met in the real network is that the AF does not understand the DNAI information. All the DNAIs are created by operators and transmitted to AF based on offline configuration. The DNAI information has been supported since Rel-15 by TS 23.501 [2] AF influence procedure.

However, there still existing the scenario that the AF has not been provided beforehand with DNAI information and needs to know the DNAI(s) associated with the EAS(s) in the EHE under its responsibility.

### 5.7.3 Assumptions

The existing service operations used by the AF and making use of DNAI shall not be impacted by this new functionality.

# 6 Solutions

## 6.0 Solution-Key issue matrix

The solutions in clause 6 can apply to one or more key issues described in clause 5 of this report. Table 6.0-1 describes the relationship between solutions and key issues.

Editor's note: The table below will be updated with actual content when generating the TR with approved contributions. Page number is automatically updated to ease reference (ctrl-left click to reach the solution).

Table 6.0-1: Solution-Key issue matrix

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Solution | | Key issues | | | | | | |
| Title | (page) | KI#1 | KI#2 | KI#3 | KI#4 | KI#5 | KI#6 | KI#7 |
| 01: EAS discovery in Home Routed roaming scenario | 18 | X |  |  |  |  |  |  |
| 02: Session Breakout in Visited PLMN | 21 | X |  |  |  |  |  |  |
| 03: EAS (re)discovery procedure in roaming scenario | 23 | X |  |  |  |  |  |  |
| 04: Support EAS discovery in VPLMN via HR PDU Session | 28 | X |  |  |  |  |  |  |
| 05: Accessing V-EHE via HR PDU session | 31 | X |  |  |  |  |  |  |
| 06: URSP solution to support roamers access to EHE in a VPLMN | 33 | X |  |  |  |  |  |  |
| 07: Using URSP Rules to Establish an LBO PDU Session | 35 | X |  |  |  |  |  |  |
| 08: V-ECS Discovery during Steering of Roaming | 36 | X |  |  |  |  |  |  |
| 09: PDU Session configuration from EASDF | 38 | X |  |  |  |  |  |  |
| 10: LBO PDU Session establishment using PLMN criteria in RSD | 40 | X |  |  |  |  |  |  |
| 11: Exposure of Network Congestion | 41 |  | X |  |  |  |  |  |
| 12: Efficient exposure of RAN information | 43 |  | X |  |  |  |  |  |
| 13: Fast and efficient network exposure improvements | 47 |  | X |  |  |  |  |  |
| 14: Group Management | 50 |  |  |  | X |  |  |  |
| 15: Selection of common DNAI | 54 |  |  |  | X |  |  |  |
| 16: Selecting the same EAS/DNAI for collection of UEs | 62 |  |  |  | X |  |  |  |
| 17: Application layer EAS selection for collections of UEs | 64 |  |  |  | X |  |  |  |
| 18: Discovery of the same EAS for collections of UEs | 66 |  |  |  | X |  |  |  |
| 19: Influencing UPF and EAS (re)location for collections of UEs | 70 |  |  |  | X |  |  |  |
| 20: Global EASDF | 71 |  |  |  |  | X |  |  |
| 21: EAS Deployment information differentiated by PLMN ID | 73 |  |  |  |  | X |  |  |
| 22: EAS discovery for federated OPs | 74 |  |  |  |  | X |  |  |
| 23: Improvements for EHE operated by separate party | 80 |  |  |  |  | X |  |  |

## 6.1 Solution 01 (KI#1): EAS discovery in Home Routed roaming scenario

### 6.1.1 Description

This solution is for Key Issue #1, which addresses 5GS improvements to support the UE access to an EHE in a VPLMN using a PDU Session with a PSA in the HPLMN including aspects related to:

- how to authorize the PDU session to support local traffic routing to access an EHE in the VPLMN;

- how to support Rel-17 edge computing related procedures, such as EAS (re-)discovery, as specified in TS 23.548 [3], clause 6;

The current standards only depict 5GS architecture for non-roaming and LBO roaming scenario supporting with UL-CL/BP. For Home Routed roaming scenario, the data flow of the UE needs to pass through the UPF of the VPLMN to the UPF of the HPLMN, the routing is controlled by SMF of the HPLMN, therefore the local traffic routing in the VPLMN cannot be achieved.

This solution proposes several ways to support UE access to VPLMN EHE in HR roaming scenarios according to different scenarios.

When HPLMN has the knowledge of EAS deployment information in VPLMN for specific services, H-SMF brings it to V-SMF during Home Routed PDU session establishment or modification, and V-SMF configure the V-EASDF according to the received EAS deployment information. H-SMF also sends the VPLMN ECS address and local traffic routing indication to V-SMF, and V-SMF performs EAS discovery and local traffic routing with V-EASDF.

If V-AF related information changes during this process, The V-AF can notify the H-AF of the information, and the H-AF configures it to the H-SMF according to the AF requests to influence traffic routing procedure defined in TS 23.502 [9], clause 4.3.6.2. H-SMF will send the new policy information about the HR PDU session to V-SMF, and V-SMF will redo the EAS discovery and local traffic routing in VPLMN according to the updated configuration, e.g. select the UL-CL and local DNS server according to the DNAI or update the configuration of V-EASDF.

NOTE: How the V-AF notifies the information to the H-AF is out of scope.

When HPLMN does not have the knowledge of EAS deployment information in VPLMN, after the H-SMF authorizes the V-SMF to perform local traffic routing, V-SMF retrieves the EAS deployment information of the VPLMN from the V-NEF and performs EAS discovery according to the EAS discovery procedure described in TS 23.548 [3].

In addition, the V-AF can also configure the V-SMF according to the AF influence on traffic routing procedure. In this case, during the HR PDU session establishment, the V-SMF needs to select a PCF in the VPLMN to establish the SM Policy Association. V-PCF may send the VPLMN ECS address obtained from V-AF to V-SMF.

Editor's note: It is FFS whether and how charging at VPLMN (reporting by V-UPF to V-SMF to V-CHF) can apply.

### 6.1.2 Procedures

#### 6.1.2.1 Procedure for EAS discovery when HPLMN has the knowledge of EAS deployment information in VPLMN

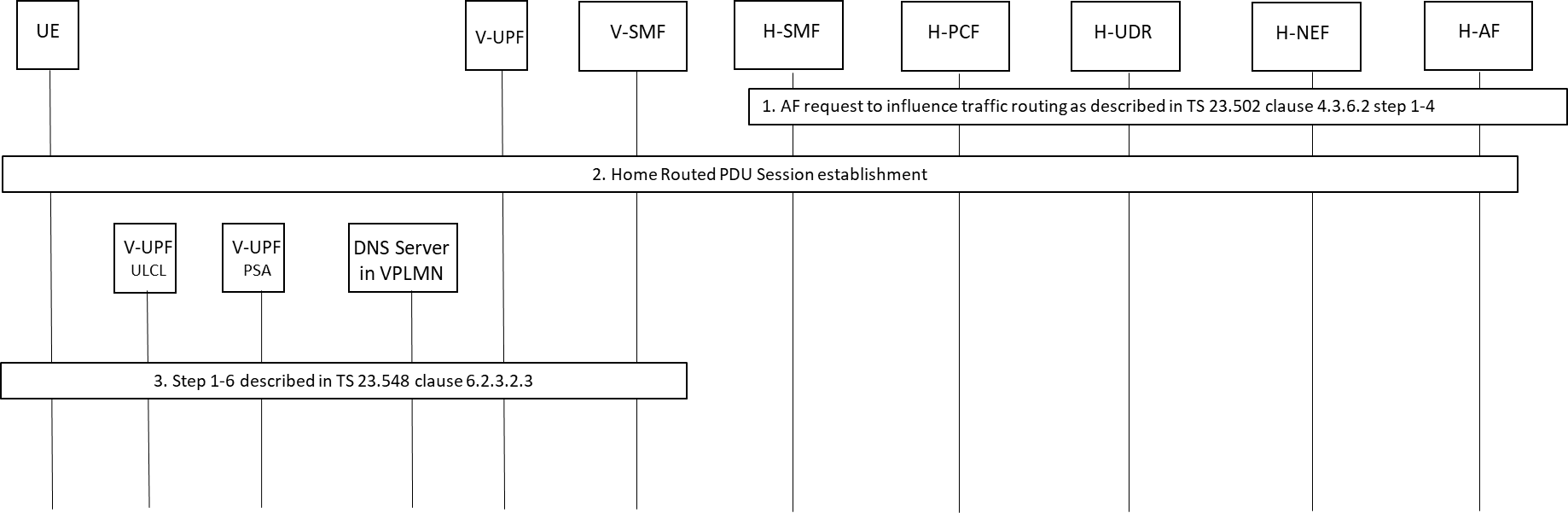


Figure 6.1.2.1-1: HPLMN triggered EAS discovery in HR roaming scenario

1. H-AF creates a new request with carrying V-AF application requirement and invokes a Nnef\_TrafficInfluence\_Create service operation and influence the traffic as described in TS 23.502 [9] clause 4.3.6.2 step 1-4.

NOTE 1: How V-AF sends application related information to H-AF is in SA6 scope. As an alternative the V-AF may depending on operator agreement act as a non trusted AF of the HPLMN (using NEF).

Editor's note: Whether the EAS deployment information is contained in AF request is FFS.

2. 5GS establishes a Home Routed PDU Session. During PDU Session establishment, H-SMF retrieve the new PCC rules impacted by the H-AF request for VPLMN from H-PCF using Rel-17 Npcf mechanisms, and sends Nsmf\_PDUSession\_Create response to V-SMF, which also includes an indication to authorize V-SMF to perform local traffic routing in VPLMN, VPLMN ECS address and new PCC rules. The indication and VPLMN ECS address are obtained by H-SMF from H-UDM.

Editor's note: It is FFS what the new PCC rules indicated in step 2 refer to and whether they replace N4 content that is sent from SMF to I-SMF over N16a (in case of traffic offload supported by an I-SMF) (I-SMF and V-SMF were so far modelled as supporting very similar behaviors).

NOTE 2: The new PCC rules are sent from H-SMF to V-SMF over N16.

3. Step 1-6 in TS 23.548 [3] clause 6.2.3.2.3 are performed. In step 1 of clause 6.2.3.2.3, UL-CL will be inserted by V-SMF.

NOTE 3: The local DNS server IP address will be configured to UE by V-SMF as described in TS 23.548 [3] clause 6.2.3.2.3 Option C based on the information provided in the AF request in step 1.

#### 6.1.2.2 Procedure for EAS discovery when HPLMN does not have the knowledge of EAS deployment information in VPLMN

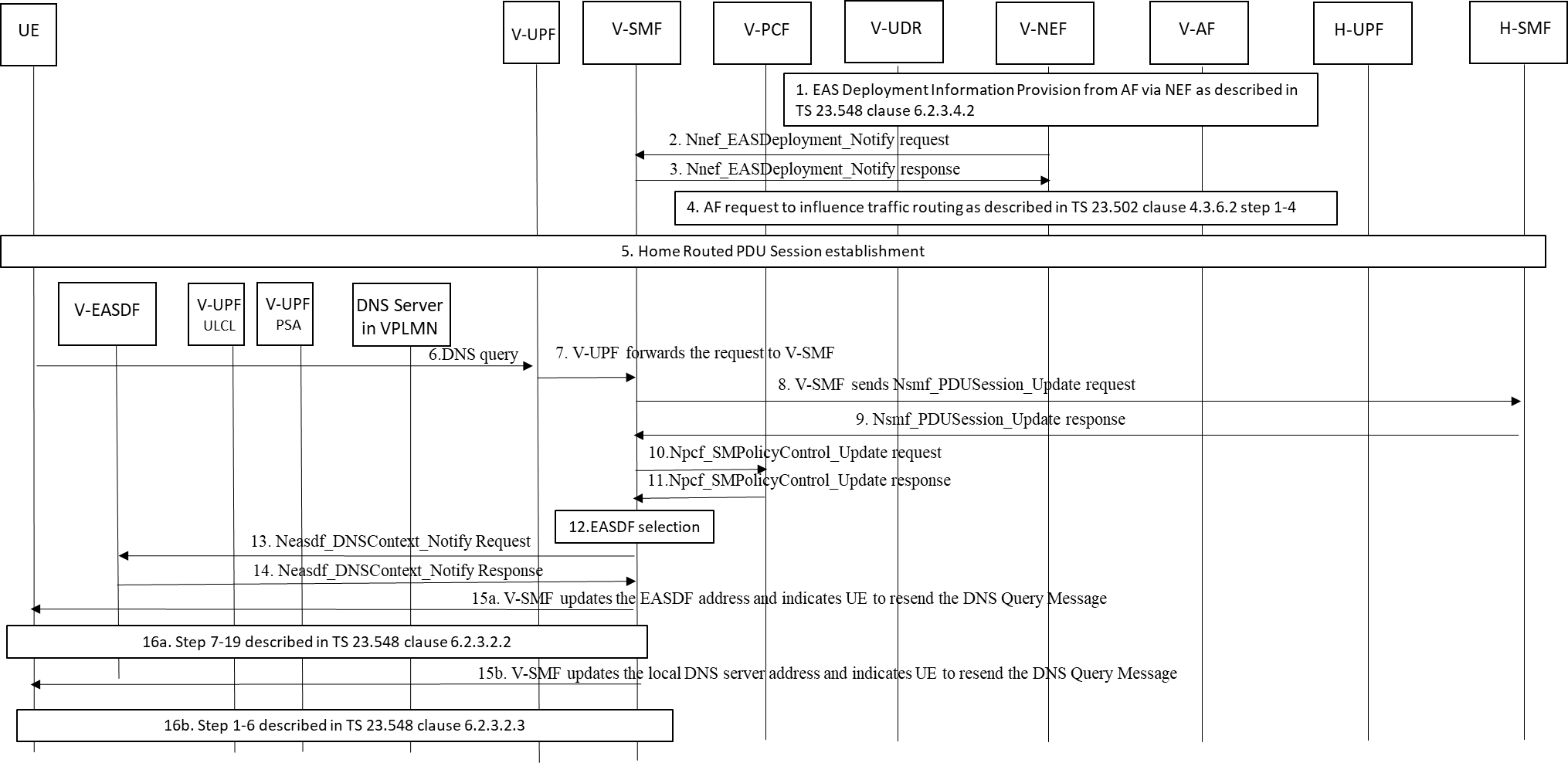


Figure 6.1.2.2-1: VPLMN triggered EAS discovery in HR roaming scenario

1. EAS deployment Information provisioned from AF via NEF as described in TS 23.548 [3] clause 6.2.3.4.2.

2-3. It is assumed that V-SMF has subscribed to EAS Deployment Information Change Notification from the V-NEF. The V-NEF invokes Nnef\_EASDeployment\_Notify to the SMF to provide the EAS Deployment Information.

4. If V-AF related information changes, V-AF creates a new request and invokes a Nnef\_TrafficInfluence\_Create service operation and influence the traffic as described in TS 23.502 [9] clause 4.3.6.2 step 1-4.

5. UE establishes Home Routed PDU Session. During the HR PDU Session establishment, V-SMF needs to establish a SM Policy Association with a PCF in VPLMN.

Editor's note: It is FFS how PCC instructions sent by V-PCF to V-SMF interact with PCC interactions sent by H-PCF to H-SMF and translated into QoS rules sent by H-SMF to V-SMF.

6. UE sends DNS Query message to V-UPF.

7. V-UPF forwards the request to V-SMF.

Editor's note: It is FFS whether steps 6 to 10 take place for any DNS request.

8. V-SMF decides to do the local traffic routing in VPLMN and sends the request of local traffic routing in VPLMN to H-SMF via Nsmf\_PDUSession\_Update request, and also sends the capability of supporting EASDF indication to H-SMF.

Editor's note: It is FFS what is the trigger for V-SMF to decide to do the local traffic routing in VPLMN and whether this trigger is some PCC interaction with V-PCF, meaning that step 10 takes place before step 8.

9. H-SMF sends the indication to authorize V-SMF to perform local traffic routing in VPLMN via or Nsmf\_PDUSession\_Update response. The indication is obtained by H-SMF from H-UDM.

10-11. V-SMF sends Npcf\_SMPolicyControl\_Update request to V-PCF to retrieve the new policy impacted by the AF request.

12. After authorized by H-SMF to perform local traffic routing in VPLMN, V-SMF selects V-EASDF.

13. The V-SMF invokes Neasdf\_DNSContext\_Create Request to the selected V-EASDF.

14. The EASDF invokes the service operation Neasdf\_DNSContext\_Create Response.

15a. If V-SMF has received the EAS deployment information in steps 2-3, V-SMF updates the EASDF address to UE and indicates UE to resend the DNS Query message to EASDF.

Editor's note: It is FFS how the V-SMF can indicate UE to resend the DNS Query message (this does not correspond to a standard DNS procedure and the V-SMF might not be able to inject User plane traffic into the TLS connection between the UE and its DNS server).

16a. Steps 7-19 in TS 23.548 [3] clause 6.2.3.2.2 are performed.

15b. If V-SMF did not receive the EAS deployment information in steps 2-3, and V-SMF received the application related information (e.g. DNAI, local DNS server address), V-SMF updates the local DNS server address to UE and indicates UE to resend the DNS Query message to local DNS server.

Editor's note: Whether the V-SMF can handle the DNS Query (take the role of UE) is FFS.

16b. Steps 1-6 in TS 23.548 [3] clause 6.2.3.2.3 are performed.

## 6.2 Solution 02 (KI#1): Session Breakout in Visited PLMN

### 6.2.1 Description

This solution corresponds to KI#1 and addresses the following aspects for the scenario using a PDU Session with a PSA in the HPLMN:

- how to authorize the PDU session to support local traffic routing to access an EHE in the VPLMN;

- how to support Rel-17 edge computing related procedures, such as EAS (re-)discovery, as specified in TS 23.548 [3], clause 6.

When roaming, the UE establishes a Home Routed Session that is capable of supporting session breakout in V-PLMN based on the subscription. In this scenario, the Home PLMN and Visited PLMN have an agreement on the support of the session breakout for the home routed session.

1) During the establishment of Home Routed PDU Session, Home PLMN allows the roaming UE to access the local part of DN identified by DNN based on its HPLMN subscription.

2) V-SMF in V-PLMN executes the session breakout procedure for the UE to access the local part of DN where the EAS in EHE is located in VPLMN. This can be triggered by the EAS discovery procedure using V-EASDF.

3) Through a Home Routed Session, the UE can access EAS deployed in EHE in VPLMN while the UE can also access the Home DN in the Home PLMN.

Editor's note: It is FFS whether and how charging at VPLMN can be done and how the V-SMF determines QoS and charging including usage monitoring to apply to the traffic being offloaded and whether the QoS for the locally offloaded traffic is still under control of HPLMN.



Figure 6.2.1-1: Architecture for Home Routing Session Breakout in Visited PLMN

### 6.2.2 Procedure



Figure 6.X-2-1: PDU Session Establishment Procedure for HR Session Breakout in VPLMN

Steps 1-4 During the registration procedure, the UDM sends the Home Routed Visited SBO (HR-VSBO) allowed indication to the AMF.

Steps 5-7 During the PDU Session establishment procedure, if the AMF receives the HR-VSBO allowed indication and AMF selects V-SMF supporting UL-CL with V-EASDF interaction, the AMF sends the HR VSBO allowed indication to the V-SMF.

Step 8 If the V-SMF decides to create HR VSBO session, V-SMF sends the VSBO request and V-EASDF/DNS address of VPLMN to the H-SMF.

Steps 9-10 The H-SMF checks whether the HR-VSBO is allowed based on its local configuration or subscription.

Steps 11-13 H-SMF checks whether the HR VSBO is allowed for the UE. If allowed, the H-SMF sends the VSBO grant indication with DNS server address set to the V-EASDF in PCO and Home DNS Server address to the V-SMF.

NOTE 1: If the H-SMF grants the HR-VSBO request, the V-SMF is allowed to offload for accessing the EHE in VPLMN without further control from HPLMN.

Editor's note: It is FFS whether further granularity on how HPLMN allows VPLMN traffic offload is to be supported.

Step 12 The V-SMF may perform the Local UPF insertion (or UL-CL insertion) procedure.

Editor's note: It is FFS how local UPF insertion can be performed in the middle of PDU Session Establishment.

Editor's note: It is FFS how the V-SMF determines where to insert traffic offload and for which traffic of the HPLMN.

Step 13 After the V-SMF performs Local UPF insertion for the local part of DN, the V-SMF performs the DNSContext creation procedure to send the DNS Message Handling Rules and Home DNS Server Address to the V-EASDF.

NOTE 2: With configured DNS Message Handling Rules configured to V-EASDF, all the DNS Queries using this PDU Session go to the V-EASDF, and DNS resolution for the local routed traffic is handled based on the Rel-17 mechanism for EAS discovery using EASDF. DNS Queries that do not match the rule configured by V-SMF go to the Home DNS Server.

Editor's note: It is FFS how the V-SMF determines the EDI needed to send the DNS Message Handling Rules to the V-EASDF.

NOTE 3: Step 12 can be performed when the Local UPF insertion procedure after the PDU Session Establishment.

Steps 14-15 The AMF forwards the PDU Session Establishment Accept/Reject to the UE.

After the above steps, the EAS (re)-discovery over Session Breakout Connectivity Model as specified in clause 6.2.3 of TS 23.548 [3] can be performed among the UE, V-SMF and V-EASDF based on the UE DNS Query so the UE can access EHE in VPLMN. With the same PDU Session, the UE can still access DN in HPLMN at the same time.

## 6.3 Solution 03 (KI#1): EAS (re)discovery procedure in roaming scenario

### 6.3.1 Description

KI#1 proposes the scenario: Accessing EHE in a VPLMN when roaming. This solution addresses one of these specific scenarios, i.e., UE accessing V-EHE for a PDU session with a PSA in HPLMN and assumes that HPLMN does not have the knowledge of EAS deployment information in VPLMN.

This solution proposes EAS (re)discovery procedure in V-EHE by transmitting a newly defined EC enabling indicator between V-SMF and H-SMF and using the V-EASDF. The UL-CL functionality is used to combine the features of HR and LBO roaming and steer local traffic to the local V-PSA. To minimize the impact of UE, UE is not aware of EASDF changing. The architecture is depicted in figure 6.3.1-1:

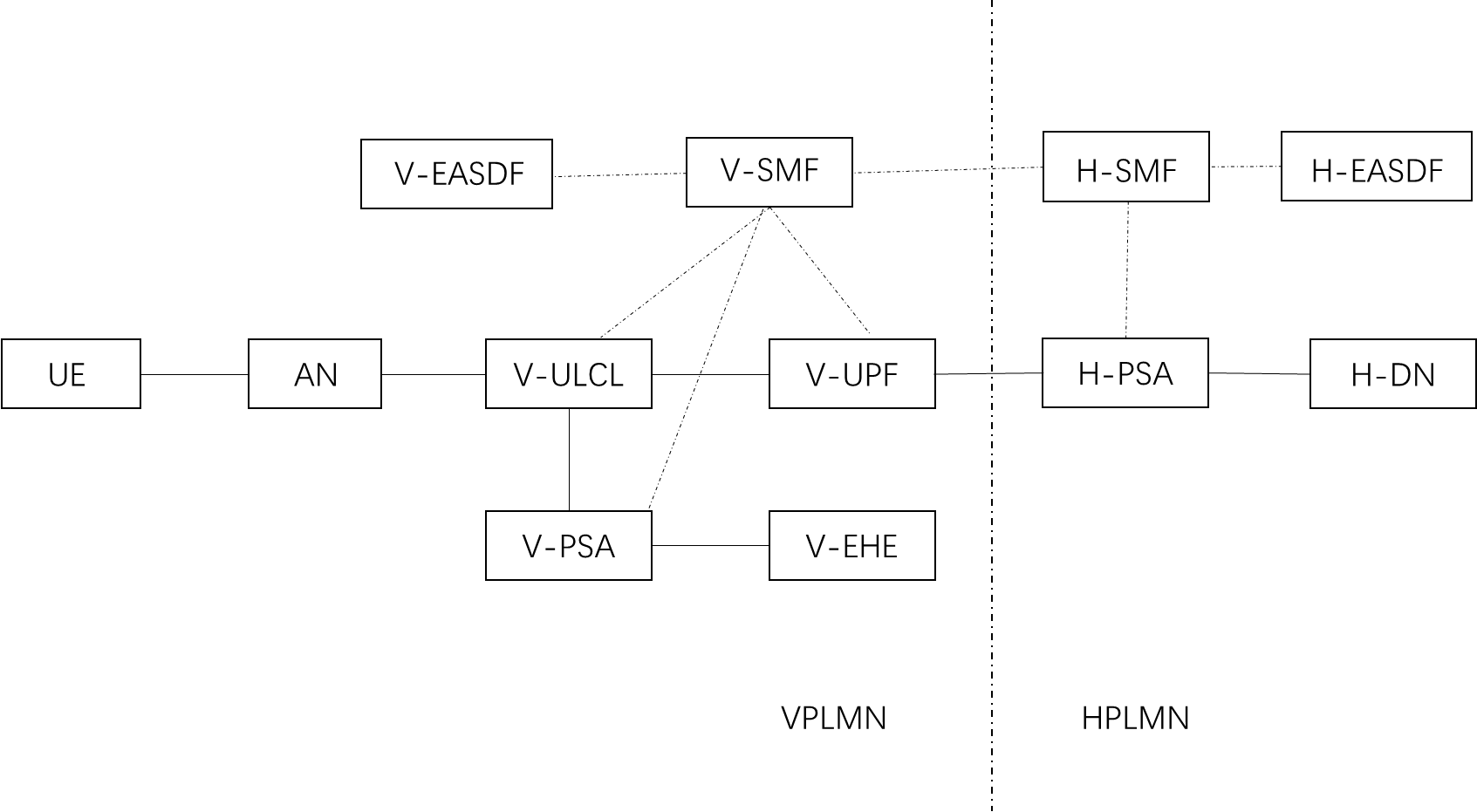


Figure 6.3.1-1: Accessing V-EHE for a PDU session with a H-PSA architecture

NOTE 1: Only some of the 5GS NFs that are the focus of this solution are shown in the above reference architecture figure. This architecture is based on 5GS architecture as specified in TS 23.501 [2].

NOTE 2: This EC enabling indicator means that VPLMN can apply the traffic offload related to EC service (e.g. UL-CL insertion for EC traffic) without any further HPLMN control.

Editor's note: It is FFS whether and how to support charging for the local traffic of a PDU session that supports local traffic routing to access an EHE in the VPLMN.

Editor's note: How the solution work in case of DNS security is FFS.

### 6.3.2 Procedures

#### 6.3.2.1 EAS discovery procedure in roaming scenario

When a UE that has established an HR PDU session expects to use edge computing service, the UE may send a DNS query to the serving network, the corresponding EAS discovery procedure is shown in figure 6.3.2.1-1:



Figure 6.3.2.1-1: EAS discovery procedure accessing V-EHE in roaming scenario

1. UE requests PDU session establishment for HR roaming as described in clause 4.3.2.2.2 of TS 23.502 [9]. During the PDU Session Establishment procedure, the H-SMF selects H-EASDF as described in clause 6.3 of TS 23.501 [2]. The H-SMF may consider the UE subscription information to select an H-EASDF as the DNS server of the PDU Session. H-SMF sends H-EASDF IP address included in PCO to UE via V-SMF.

H-SMF may indicate to the UE either that for the PDU Session the use of the EDC functionality is allowed or that for the PDU Session the use of the EDC functionality is required.

H-SMF provides DNS message handling rules to H-EASDF by invoking Neasdf\_DNSContext\_Create Request. H-EASDF responds with Neasdf\_DNSContext\_Create Response as described in clause 6.2.3.2.2 of TS 23.548 [3].

2. According to the SLA between application service provider and operator, when the Edge Computing enablers provided by 5GC are expected as described in clause 5.13 of TS 23.501 [2], UE sends DNS query using EDC functionality towards H-EASDF.

3. V-UPF delivers the DNS query to H-PSA via N9 tunnel and H-PSA delivers the DNS query to H-EASDF.

4. H-EASDF sends the DNS message to H-SMF by invoking Neasdf\_DNSContext\_Notify Request (information from the DNS Query e.g. target FQDN of the DNS Query) if the DNS message handling rule is met as described in clause 6.2.3.2.2 of TS 23.548 [3].

5. H-SMF responds with Neasdf\_DNSContext\_Notify response.

6. Based on UE location information, target FQDN of the DNS Query and HPLMN EAS deployment information provided by HPLMN AF (or local configuration), H-SMF determines that HPLMN cannot provide the EC service requested by the UE.

7. H-SMF sends the IP address of H-EASDF and the DNS Query to V-SMF; in addition, H-SMF sends an EC enabling indicator to V-SMF to indicate that this DNS query needs to be resolved to EHE deployed in VPLMN and UE is unaware of potential EASDF changing.

NOTE: Sending EC enabling indicator from H-SMF to V-SMF implies that the HPLMN authorizes VPLMN to manage the EC service according to the roaming agreement between these two operators.

8. V-SMF receives the EC enabling indicator and selects the V-EASDF as the DNS server of the PDU Session as described in clause 6.3 of TS 23.501 [2].

9. V-SMF drives related DNS message handling rule based on the DNS query, EAS deployment information provided by V-PLMN AF and/or local configuration. V-SMF sends this DNS message handling rule and the DNS query to V-EASDF via Neasdf\_DNSContext\_Update request.

Editor's note: It is FFS whether and how the V-SMF configures the DNS message handling rule considering H-EASDF as the DNS server for the DNS resolution for traffic routed to the HPLMN.

10. V-EASDF responds with Neasdf\_DNSContext\_Update response.

11. V-EASDF handles the DNS query according to the DNS message handling rule and sends the DNS query to the DNS server in VPLMN, the DNS server returns the DNS response including EAS IP address to V-EASDF.

12. V-EASDF sends the DNS response to the V-SMF by invoking Neasdf\_DNSContext\_Notify request including EAS information if the EAS IP address or the FQDN in the DNS response matches the DNS message detection template provided by the V-SMF as described in clause 6.2.3.2.2 of TS 23.548 [3], and V-EASDF buffers this DNS response.

13. V-SMF responds with Neasdf\_DNSContext\_Notify Response.

14. Based on EAS information received from the V-EASDF in Neasdf\_DNSContext\_Notify and other UPF selection criteria, V-SMF may determine the DNAI and determine the associated N6 traffic routing information for the DNAI. V-SMF may perform V-UL CL and V-PSA selection and insertion as described in TS 23.502 [9].

V-SMF configures the V-UL-CL with CN tunnel info provided by V-UPF and AN tunnel info provided by serving AN. The traffic routing rules are provided to V-UL-CL based on EAS information and H-EASDF IP address, e.g., V-UL-CL routes the traffic to V-PSA if the IP packet has a destination address of H-EASDF or EAS and routes other traffic to V-UPF.

V-SMF configures V-PSA with EASDF IP replacement information (i.e., H-EASDF IP address and port number, V-EASDF IP address and port number). In uplink direction, V-PSA replaces the destination address of the DNS query from H-EASDF to V-EASDF; in downlink direction, V-PSA replaces the source address of the DNS response from V-EASDF to H-EASDF so that the UE is not aware of EASDF changing.

Editor's note: It is FFS how the V-SMF knows the N6 traffic routing information.

15. V-SMF invokes Neasdf\_DNSContext\_Update Request (DNS message handling rule). The DNS message handling rule with the Control Action "Send the buffered DNS response(s) message to UE" indicates the V-EASDF to send the DNS response buffered in step 12 to UE.

16. V-EASDF responds with Neasdf\_DNSContext\_Update response.

17. V-SMF returns a positive response related with EC enabling indicator to H-SMF.

18. If it is indicated to send the buffered DNS response to UE in step 15, the V-EASDF sends the DNS response to the V-PSA.

19. V-PSA replaces the source address from V-EASDF to H-EASDF in the DNS response based on the V-SMF instructions and sends this DNS response to the UE via V-UL-CL.

#### 6.3.2.2 EAS rediscovery procedure in roaming scenario

The support for EAS rediscovery indication procedure enables the UE to refresh stale EAS information stored locally so that the UE can trigger EAS discovery procedure to discover new EAS information as described in clause 6.2.3.3 of TS 23.548 [3]. The corresponding EAS rediscovery procedure is shown in figure 6.3.2.2-1:



Figure 6.3.2.2-1: EAS rediscovery procedure accessing V-EHE in roaming scenario

0. The procedure in clause 6.3.2.1 executes with following difference to apply to EAS rediscovery:

In step 1, the UE may indicate its support for refreshing stale EAS information stored locally corresponding to the impact field per the EAS rediscovery indication from network during the HR PDU Session Establishment procedure.

In step 7, if the UE indicates such support, the H-SMF may send this indication to V-SMF by Nsmf\_PDUsession\_Update service.

NOTE: If the UE indicates such support, V-SMF may store this indication in the PDU session context.

1a. Due to the UE mobility the V-SMF triggers V-PSA insertion, change or removal for the PDU Session. The insertion, change or removal of V-PSA triggers EAS rediscovery.

1b. The V-AF triggers EAS relocation e.g. due to EAS load balance or maintenance, etc. and informs the V-SMF the related information indicating the EAS relocation.

Editor's note: It is FFS how V-AF and V-SMF know each other address and whether this assumes involvement of a V-PCF.

2. V- SMF sends PDU Session Modification Command (EAS rediscovery indication, [impact field]) to UE as described in step 2 of clause 6.2.3.3 of TS 23.548 [3], with the following differences:

V-SMF sends the impact field with the EAS rediscovery indication if the UE support indication received from H-SMF;

If V-SMF may choose new DNS settings for the PDU Session, it does not provide them to UE. V-SMF may configure V-PSA with corresponding EASDF IP replacement information as described in clause 6.3.2.1.

UE refreshes DNS record according to EAS rediscovery indication received from V-SMF.

3. UE may trigger EAS discovery procedure to get new EAS information. This DNS query is sent to corresponding DNS server using IP address replacement in VPLMN.

### 6.3.3 Impacts on existing entities and interfaces

Editor's note: this clause is FFS.

H-SMF:

- determines that HPLMN cannot provide the EC service based on UE location information, target FQDN of the DNS Query and HPLMN EAS deployment information provided by HPLMN AF (or local configuration).

- sends H-EASDF IP address, the DNS Query and an EC enabling indicator to V-SMF via Nsmf\_PDUSession\_Update service operation.

- sends the indication which indicates that UE supports to refresh stale EAS information stored locally corresponding to the impact field per the EAS rediscovery indication from network to V-SMF.

V-SMF:

- identifies the EC enabling indicator and manages the EC service for UE in VPLMN.

- sends the DNS query to V-EASDF via Neasdf\_DNSContext\_Update request.

- selects and inserts the V-UL CL and V-PSA based on local policy and does not need to interact with H-SMF.

- stores the indication which indicates that UE supports to refresh stale EAS information stored locally corresponding to the impact field per the EAS rediscovery indication from network in the PDU session context.

H-EASDF:

- sends the DNS query to H-SMF.

## 6.4 Solution 04 (KI#1): Support EAS discovery in VPLMN via HR PDU Session

### 6.4.1 Description

This solution corresponds to KI#1. The scenarios 2.1 and 2.2 are described in clause 5.1.2.

As described in clause 5.1.2, a roaming UE may access V-EHE via an established HR PDU Session. To support such scenario, session breakout to access EHE in VPLMN is used. The following aspects are included:

- The H-PCF provides authorization policy which indicates local traffic routing in VPLMN is authorized for the UE accessing the VPLMN.

- UL-CL/BP and local PSA insertion.

The V-SMF performs selection and insertion of UL-CL/BP and local PSA based on UE location when receiving the authorization policy from H-SMF without considering EAS deployment information in VPLMN. In this case, UL-CL/BP is selected based on UE location.

For scenario 2.1, the V-SMF may select and insert UL CL/BP and local PSA based on UE location and target DNAI after PDU Session is established. The V-SMF selects target DNAI based on DNAIs received from H-SMF. The DNAIs are determined by H-SMF based on EAS IP report from H-EASDF. In this case, UL-CL/BP is selected based on UE location and selected EAS IP address.

- EAS discovery using H-EASDF.

For scenario 2.1, the H-SMF obtains ECS option/local DNS server from V-SMF during DNS based EAS discovery procedure and send it to H-EASDF. The H-EASDF handles DNS queries including FQDNs deployed in VPLMN based on the ECS option/local DNS server as defined in TS 23.548 [3]. In this case, different FQDNs may use different ECS option/local DNS Server.

For scenario 2.2, the H-SMF obtains ECS option/local DNS server from V-SMF during PDU Session Establishment and send it to H-EASDF. The H-EASDF handles all DNS queries of the UE based on this ECS option/local DNS server. In this case, all DNS queries requested by the UE will share same ECS option/local DNS server.

Editor's note: How to perform charging for local routed traffic in VPLMN is FFS.

Editor's note: How to support UE mobility in scenario 2.2 is FFS.

Editor's note: It is FFS how to determine whether to change of EAS at UE mobility.

### 6.4.2 Procedure

Figure 6.4.2-1 shows the procedure of EAS discovery in VPLMN via HR PDU Session.



Figure 6.4.2-1: EAS discovery in VPLMN via HR PDU Session

1. UE sends PDU Session establishment request to V-SMF.

2. The V-SMF sends Nsmf\_PDUSession\_Create Request to H-SMF.

For scenario 2.2 where HPLMN does not have the knowledge of EAS deployment in VPLMN, the V-SMF may, based on UE location, send information to build ECS option/local DNS server for the VPLMN from V-SMF to H-SMF.

3. The H-SMF receives authorization policy which indicates whether local traffic routing in the VPLMN is authorized from H-PCF.

4. H-SMF invokes Neasdf\_DNSContext\_Create Request including DNS handling rule to H-EASDF.

For scenario 2.2, the H-SMF may send the information to build ECS option/local DNS server as described in step 2 to the H-EASDF.

5. The H-SMF sends Nsmf\_PDUSession\_Create Response including authorization policy to the V-SMF.

Editor's note: It is FFS what is the content of authorization policy.

The H-SMF sends H-EASDF address to the V-SMF.

6. [Conditional] The V-SMF performs UL-CL/BP and local PSA selection and insertion if the authorization policy indicates local traffic routing in the VPLMN is authorized. In this case the V-SMF selects DNAI for the UL-CL/BP insertion based on UE location.

7. The V-SMF sends PDU Session Establishment accept message including the H-EASDF address to UE.

8. UE sends DNS query which includes FQDN deployed in the VPLMN to the H-EASDF.

For scenario 2.1, H-SMF may obtain ECS option/local DNS server from V-SMF by performing steps 9-12:

9. The H-EASDF reports the FQDN to H-SMF by invoking Neasdf\_DNSContext\_Notify Request.

H-SMF determines candidate DNAIs of VPLMN corresponding the FQDN based on the EAS deployment information in the VPLMN. H-SMF may consider UE location to select the candidate DNAIs of VPLMN in this step. (steps 10-12)

10; The H-SMF initiates Nsmf\_PDUSession\_Update Request service including candidate DNAIs of VPLMN to the V-SMF.

11. V-SMF determines the target DNAI based on UE location and provides information to build ECS option or local DNS server to H-SMF based on the target DNAI.

12. H-SMF invokes Neasdf\_DNSContext\_Update Request to H-EASDF including updated DNS handling rule, e.g. information to build ECS option or local DNS server.

13. The H-EASDF adds ECS option into the DNS query and sends it to C-DNS server, or sends the DNS query to the local DNS server if the DNS query matches the DNS handling rule as described in clause 6.2.3 of TS 23.548 [3].

H-EASDF receives the DNS Response including EAS IP address which is determined by the DNS system.

For scenario 2.1, H-SMF may trigger V-SMF selecting and inserting UL-CL/BP and local PSA by performing steps 14-16:

14. The H-EASDF invokes Neasdf\_DNSContext\_Notify Request including EAS IP to the H-SMF based on DNS handling rule.

15. The H-SMF triggers the V-SMF to perform UL-CL/BP and local PSA selection and insertion.

H-SMF determines target DNAI of VPLMN corresponding the EAS IP based on the EAS deployment information in the VPLMN.

The H-SMF initiates Nsmf\_PDUSession\_Update Request service including target DNAI of VPLMN to the V-SMF.

The V-SMF selects and inserts UL-CL/BP and local PSA based on the target DNAI.

The V-SMF sends Nsmf\_PDUSession\_Update Response to H-SMF.

16. The H-SMF invokes Neasdf\_DNSContext\_Update Request to trigger the H-EASDF sending DNS response to UE.

17. The H-EASDF sends the DNS response including the EAS IP to UE.

Editor's note: It is FFS whether procedures defined for I-SMF may be used for this call flow e.g. in step 15.

### 6.4.3 Impacts on services, entities and interfaces

Editor's note: The content of clause on Impacts on services, entities and interfaces is FFS.

H-PCF:

- retrieve and send authorization policy to H-SMF which indicates local traffic routing in VPLMN is authorized.

H-SMF:

- send H-EASDF address to V-SMF;

- send authorization to V-SMF;

- receive information to build ECS option/local DNS server from V-SMF;

- for scenario 2.1:

- send candidate DNAIs to V-SMF.

- for scenario 2.2:

- configured with information to build ECS option/local DNS server.

V-SMF:

- receive H-EASDF address from H-SMF;

- receive authorization policy from H-SMF;

- for scenario 2.1:

- receive candidate DNAIs from H-SMF;

- determine information to build ECS option/local DNS server based on candidate DNAIs and UE location;

- send information to build ECS option/local DNS server to H-SMF;

- receive target DNAI from H-SMF and perform ULCL/BP insertion.

- for scenario 2.2:

- send ECS Option/local DNS server of the VPLMN to H-SMF;

- determine DNAI and perform UL-CL/BP insertion based on the UE location and authorization policy.

## 6.5 Solution 05 (KI#1): Accessing V-EHE via HR PDU session

### 6.5.1 Description

The following solution corresponds to the key issue #1 on Accessing EHE in a VPLMN when roaming as specified in clause 5.1.

The UE establishes a Home Routed PDU session using session breakout to access the EHE in VPLMN. The V-SMF determines the HR PDU session for V-EHE should be activated based on the EAS information and roaming offload policy received from H-PCF via H-SMF, and configures the traffic routing rule and Usage Report Rule to assist traffic offload to V-EAS and usage information report from UL-CL V-UPF or BP V-UPF to H-SMF via V-SMF for offline and online charging.



Figure 6.5.1-1: UP traffic and CP signalling for scenario of accessing V-EHE via a HR PDU session

### 6.5.2 Procedures



Figure 6.5.2-1: Accessing V-EHE via a HR PDU session

1. The UE initiates a Home Routed PDU session establishment procedure with V-SMF.

2. The V-SMF sends Nsmf\_PDUSession\_Create Request to H-SMF.

3. The H-PCF may provide the authorized roaming offload policy to V-SMF via H-SMF. The roaming offload policy includes the specific Application Identifier(s) or FQDN set or IP range, and indicates if the Application Identifier or FQDN or EAS IP is satisfied, the HR PDU session for V-EHE is activated (e.g. inserts a V-UPF accessing EAS).

4. The V-SMF selects a V-EASDF as specified in clause 6.2.3 of TS 23.548 [3]. According to the roaming offload policy, the V-SMF configures DNS message handling rules to EASDF.

Editor's note: It is FFS how to handle the DNS resolution for traffic routed to the HPLMN.

5. The UE sends a DNS Query message to the V-EASDF, and the V-EASDF performs EAS discovery as specified in clause 6.2.3 of TS 23.548 [3]. The discovered EAS information is reported to V-SMF.

6. Based on the received EAS information (e.g. EAS IP address) and the roaming offload policy, the V-SMF decides to insert or relocate UL-CL/BP V-UPF and PSA V-UPF for traffic offload to the V-EAS.

7. The V-SMF configures traffic routing rule and Usage Report Rule on the UL-CL V-UPF or the BP V-UPF. The traffic routing rule includes EAS IP (for UL-CL) or IP prefix @local PSA (for BP) to route traffic towards the V-EAS. The Usage Report Rule is to request the report of the relevant usage information via monitoring traffic from UE to V-EAS, which is used for offline and online charging.

8. UL and DL traffic routed between UE and V-EAS via UL-CL V-UPF or BP V-UPF. The UL-CL V-UPF or V-UPF collects and reports the usage information to V-SMF.

9. The V-SMF sends usage information received from V-UPF to the H-SMF, and the H-SMF generates charging information. Alternatively, the V-SMF may generate the charging information, and sends both usage information and charging information to H-SMF.

### 6.5.3 Impacts on services, entities and interfaces

V-SMF:

1. receives the roaming offload policy included in PCC rule from H-PCF via H-SMF.

2. generates traffic routing rule and Usage Report Rule according to EAS information and roaming offload policy.

3. sends usage information (and charging information, if it is generated by V-SMF) to H-SMF.

4. configures DNS message handling rules to EASDF according to the roaming offload policy.

V-PCF:

1. creates PCC rule that includes roaming offload policy.

## 6.6 Solution 06 (KI#1): URSP solution to support roamers access to EHE in a VPLMN

### 6.6.1 Description

UE not served by their home network should where possible (when allowed by their home network) benefit from traffic offload and Edge Computing capabilities deployed by their serving network.

A solution is to leverage TS 23.548 [3] clause 6.6 "Support of AF Guidance to PCF Determination of Proper URSP Rules" and clause 4.15.6.10 of TS 23.502 [9] "Application guidance for URSP rules determination mechanisms" as defined for Rel-17. This is to guide UE for traffic to be offloaded in the VPLMN to use a specific DNN and slice deployed in LBO mode while the rest of he traffic can use HR PDU session(s).

An AF belonging to the VLMN reaching the NEF of the HPLMN (a roaming partner) indicates the (VPLMN) DNN and slices related with traffic offload / EC that it supports (per TS 23.548 [3], clause 6.6 "Support of AF Guidance to PCF Determination of Proper URSP Rules" and clause 4.15.6.10 of TS 23.502 [9] "application guidance for URSP rules determination mechanisms"); this indication can be leveraged by the PCF of the HPLMN to (if authorized by HPLMN policies) provide dedicated URSP rules applicable to relevant users of the HPLMN when they are roaming in that VPLMN. These URSP may have a validity condition corresponding to the VPLMN location but should refer to S-NSSAI(s) defined by the HPLMN. The interaction from AF in VPLMN to the NEF in HPLMN may use the SEPP to interact between the VPLMN and the HPLMN.

Editor's note: Potential impacts to use SEPP for this kind on interaction are FFS.

This interaction between the VPLMN AF and the HPLMN NEF is not related to a specific UE, but is meant to cover all UEs matching the VPLMN related location criteria.

The VPLMN AF provides HPLMN S-NSSAI(s) (that are determined from the VPLMN S-NSSAI(s)).

NOTE 1: As the VPLMN has the translation between HPLMN S-NSSAI(s) and the VPLMN S-NSSAI(s), translation needed in the VPLMN to serve the HPLMN users.

The H-PCF may, based on local policies, determine whether to always send the URSP rules immediately to the UE or to send these rules only when the UE is served by the corresponding serving PLMN, e.g. waiting to be triggered from a V-PCF of that PLMN in step 3 of TS 23.502 [9], clause 4.6.11.

The PCF of the HPLMN when it sends such URSP update to a UE, needs, as for Rel-17, to ensure that the DNN, S-NSSAI provided in the URSP rules sent to the UE is allowed in LBO mode in the user subscription (in UDM/UDR) even when the UE is roaming in that VPLMN.

NOTE 2: This solution can also apply for UEPO (see TR 23.700-85 [10]).

The VPLMN may provide Geographical or VPLMN location (e.g. VPLMN TAI or cells) related validity conditions for the URSP to apply. When the VPLMN AF provides the HPLMN with VPLMN validity conditions, the VPLMN location information (e.g. VPLMN TAI or cells) contains a VPLMN ID that may be used by the H-PCF to understand that this information is specific for a VPLMN.

Depending on H-PCF policies (on when to deliver URSP(s) valid in remote PLMN(s)) and on the situation (e.g. UE arriving rapidly in a new PLMN when for example the user arrives by plane in a remote country), it may take some time before URSP rules takes effect in UE: it may happen that the UE gets URSP(s) applicable to the VPLMN while HR PDU Sessions have already been established. As defined in TS 23.503 [13], "For every newly detected application the UE evaluates the URSP rules in the order of Rule Precedence and determines if the application is matching the Traffic descriptor of any URSP rule." Thus, it may happen that some traffic has started using HR PDU sessions, but as soon as new application interactions start, corresponding traffic will gradually be moved to LBO PDU sessions in the serving PLMN while already started IP flows may go on using the H-UPF.

Editor's note: It is FFS whether the solution addresses following case. Suppose there is some traffic from Application 1 that uses an HR PDU Session. Next, the UE moves to the VPLMN. We now want the traffic from Application 1 to move to an LBO PDU Session.

NOTE 3: Before concluding this solution for normative work, alignment check with FS\_eUEPO shall be done in order to avoid any conflict with the conclusion of KI#1 in TR 23.700-85 [10]. Final decision on generic URSP enhancement for supporting LBO roaming case should be made within FS\_eUEPO study.

### 6.6.2 Procedures

The solution reuses existing procedures.

### 6.6.3 Impacts on Existing Nodes and Functionality

- The VPLMN and the HPLMN as part of the roaming agreement need to ensure that a VPLMN AF can contact the NEF of the HPLMN to use the API defined in clause 4.15.6.10 of TS 23.502 [9], "Application guidance for URSP rules determination mechanisms".

- Potential UDM impact to ensure that the DNN, S-NSSAI provided in the URSP rules sent to the UE is allowed in LBO mode in the user subscription (in UDM/UDR) even when the UE is roaming in that VPLMN.

## 6.7 Solution 07 (KI#1): Using URSP Rules to Establish an LBO PDU Session

### 6.7.1 Description

#### 6.7.1.1 General

This solution addresses that part of Key Issue #1 that considers how to establish the LBO PDU Session towards the correct S-NSSAI/DNN pair in order to access an EHE in the VPLMN.

The principles of this solution are:

- In Rel-17, a URSP rule can already be configured with Location Criteria that indicates to the UE that the route (i.e. PDU Session) should only be established, or used, when the UE served by certain cell(s), RAN node(s), or TAIs. This feature can be used to cause the UE to select a DNN/S-NSSAI combination that is appropriate for the PLMN where the UE is registered (e.g. an LBO Session). Location criteria is defined in TS 24.526 [11] and may be a list of cell(s), RAN node(s), or TAI(s). This solution proposes that Location Criteria can also include a PLMN ID.

NOTE: Whether a PLMN ID can be encoded as part of Location Criteria or encoded as a new validation criteria information element is left to stage 3.

- When a route includes Location Criteria, a "Revaluation Required" indication can be added to the RSD. A "Revaluation Required" indication in the RSD indicates to the UE that the UE should re-evaluate URSP rules for traffic that uses the PDU Session and if the Location Criteria becomes invalid and release the PDU Session no traffic is using the PDU Session after re-evaluation. In other words, the PDU Session may be released when the UE leaves the PLMN, cell(s), RAN node(s), or TAI(s) where the location criteria is valid and all traffic is moved to a different PDU Session (e.g. an LBO PDU Session).

- Triggering re-evaluation will cause the UE to select a new route. The new route may include location criteria for the UE's new location and a PDU Session will be established with a DNN/S-NSSAI combination that is better suited for the UE's new location (e.g. for the PLMN where the UE is now registered).

#### 6.7.1.2 Procedure

The UE receives URSP rules. Some URSP rules may have a Traffic Descriptors that are associated with edge services. The RSDs of these URSP rules may include Location Criteria. By including Location Criteria, the URSP rule can be configured such that the UE will select a DNN/S-NSSAI combination for PDU Session Establishment based on the UE's cell, RAN Node, TAI or PLMN ID. Thus, the UE will use a DNN/S-NSSAI combination based on the PLMN that the UE is registered with.

Existing Rel-17 behaviour is that when the UE leaves the cell, RAN Node, or tracking area, the UE will continue to use the PDU Session until URSP Rules are re-evaluated. However, the UE is not required to re-evaluate URSP rules for the traffic.

This solution proposes that the RSD(s) also include a "Revaluation Required" indication. When a change of cell, RAN node, TAI, or PLMN occurs, the existing PDU Session will be released if no longer needed and the UE will re-evaluate URSP rules. URSP re-evaluation will cause the UE to choose a new RSD for the traffic. The location criteria in the new RSD will cause the UE to select a DNN/S-NSSAI that is associated with the PLMN where the UE is currently registered.

NOTE: Before concluding this solution for normative work, alignment check with FS\_eUEPO shall be done in order to avoid any conflict with the conclusion of KI#1 in TR 23.700-85 [10]. Final decision on generic URSP enhancement for supporting LBO roaming case should be made within FS\_eUEPO study.

### 6.7.2 Impacts on services, entities and interfaces

PCF:

- can include the "Revaluation Required" indication in RSDs or URSPs.

- can include a PLMN ID in location criteria.

UE:

- can receive the "Revaluation Required" indication in RSDs or URSPs.

- can use the "Revaluation Required" indication to decide when to trigger PDU Session release and URSP Re-evaluation.

- can receive a PLMN ID in location criteria.

## 6.8 Solution 08 (KI#1): V-ECS Discovery during Steering of Roaming

### 6.8.1 Description

#### 6.8.1.1 General

This solution addresses that part of Key Issue #1 that considers how to how to configure the VPLMN ECS address to UE in roaming scenarios.

The principle of this solution is that the Steering of Roaming framework that is specified in TS 23.122[12] can be extended to provide information to the UE so that the EEC can communicate with an ECS in VPLMN (i.e. a V-ECS). This solution explains how the SoR transparent container can be used to provide information to the UE that can be used to establish an LBO PDU Session that is used to reach a V-ECS.

NOTE: CT1 has stage-2 and stage-3 responsibility for the Steering of Roaming feature. If this solution is selected for normative work, coordination with CT1 would be required.

#### 6.8.1.2 Procedure

As one option, the SoR transparent container can be used to provide an FQDN or an IP Address of a V-ECS to the UE. When the UE accesses the provided FQDN or IP Address, URSP rules may steer the UE to use a DNN/S-NSSAI combination that can be used to reach the ECS (e.g. an LBO Session).

As a second option, the SoR transparent container can be used to provide a DNN/S-NSSAI combination to the EEC. In this case, the DNN/S-NSSAI combination may be used to send a PDU Session Establishment Request in the VPLMN that will result in an LBO PDU Session. The SMF in the VPLMN may then send ECS Address Configuration Information to the UE as described in TS 23.548 [3]. The EEC may then use the ECS FQDN or IP Address from the ECS Address Configuration Information.

Figure 6.8.1.2-1 procedure illustrates a procedure for this solution.



Figure 6.8.1.2-1: V-ECS Discovery during Steering of Roaming

1. The UE receives the SoR Transparent Container. The SoR Transparent Container may include a new information element called ECS Discovery Information. The ECS Discovery Information may include ECS Contact Information (O), ECS Provider ID (O), DNN (O), and S-NSSAI (O). The network may have been pre-provisioned with the ECS Discovery information (e.g. via OAM) and what ECS Discovery information is sent to the UE may be based on roaming agreement (e.g. the roaming agreement may allow the HPLMN to point the UE to an ECS in the EHE of the VPLMN).

2. As described in TS 23.122 [10], the reception of the SoR Transparent Container triggers the UE to perform PLMN Selection.

3. The UE registers with a PLMN that was provided in the SoR Transparent Container.

4. The UE establishes an LBO PDU Session that will be used to communicate with the V-ECS and/or to obtain ECS Contact Information from the VPLMN.

Option A: The ECS Discovery Information from step 1 may have included only ECS Contact Information (i.e. an FQDN of an ECS in the VPLMN). In this case, URSP rules may steer the UE to use a DNN/S-NSSAI combination that can be used to reach the ECS (e.g. an LBO Session).

Option B: The ECS Discovery Information from step 1 may have included only a DNN / S-NSSAI combination. In this case, the combination may be used to send a PDU Session Establishment Request that will result in an LBO session. The SMF in the VPLMN may then send ECS Address Configuration Information to the UE as described in TS 23.548 [3].

5. The EEC sends a Service Provisioning Request to an ECS in the visited network. The ECS address was obtained in step 1 or step 4.

6. The EEC receives a Service Provisioning Response.

### 6.8.2 Impacts on services, entities and interfaces

SoR-AF:

- can provide ECS Discovery Information.

UE:

- can receive the ECS Discovery Information in the SoR Transparent Container.

## 6.9 Solution 09 (KI#1): PDU Session configuration from EASDF

### 6.9.1 Description

This solution addresses KI#1: Accessing EHE in a VPLMN when roaming.

In this solution, the UE uses a predefined FQDN to the EASDF that is shared between operators. For example, GSMA could host the root entry for this Global EASDF. This solution is based on that the Global EASDF supports either configuration for a local EASDF or configuration for the UE to set up a new PDU Session.

For a specific VPLMN, if the HPLMN requires the UE to use a new (LBO) PDU Session to access the V-PLMN's EHE, then the HPLMN will configure the Global EASDF with configuration for the UE to use to set up a new PDU Session. When the UE initiates the new PDU Session, then the UE will receive all needed configuration from the V-SMF for EAS discovery in the V-PLMN's network. If the HPLMN instead uses HR PDU Session, then it will configure the Global EASDF with the IP address of the EASDF in the V-PLMNs network. The UE will then use that one to discover EAS(s) in the V-PLMN. This allows the V-PLMN to utilize local traffic routing to the V-PLMNs EHE according to the agreement between them.

Editor's note: It is FFS whether there is, and if yes, how to solve conflicts between the different global ESDADF configuration requests from different PLMN(s).

Editor's note: It is FFS whether this configuration relates to the UE IP address AND thus that the GSMA EASDF will be involved for every roamer. Otherwise, it is FFS how the GSMA EASDF determine which VPLMN the UE is using to reach the GSMA EASDF.

The Global EASDF acts as a DNS server to provide the UE with either the IP address of the EASDF that the UE should use in the V-PLMN or the S-NSSAI/DNN combination that the UE will use to set up a PDU Session.

This solution does not utilize URSP rules for the UE to retrieve and set up new PDU Session.

Editor's note: Alignment to the Rel-18 study FS\_eUEPO is FFS.

### 6.9.2 Procedures

#### 6.9.2.1 Procedures for PDU Session configuration from EASDF



Figure 6.9.2-1: Procedure for PDU Session configuration from EASDF

0. Pre-requisites: The UE has a Home Routed PDU Session and the HPLMN has configured the Global EASDF with appropriate configuration for supported Visitors EHE(s).

1. The UE performs a DNS query to the Global EASDF. Since this is a public FQDN to the Global EASDF, the UE may use any locally configured DNS Server that in turn will use next DNS server in the DNS hierarchy until it goes to the Global EASDF.

Editor's note: The root FQDN for the Global EASDF and the structure of VPLMN/HPLMN's identity in the query including the structure of how V-PLMN's configuration is stored in the DNS is FFS.

2. The Global EASDF responds with either the configuration the UE needs to set up a PDU Session in the V-PLMN or the IP address of the local EASDF.

If the V-PLMN uses existing PDU Session (HR PDU Session with local traffic routing) then the Global EASDF is configured with the V-PLMN's EASDF. If the operators require a new LBO PDU Session, then the Global EASDF is only configured with the configuration the UE needs to set up the new PDU Session.

Editor's note: The format and which DNS service record to use is FFS.

Editor's note: How and what triggers the V-PLMN's EASDF selection and related DNS handling rule configuration is FFS if the HR PDU session with local traffic routing is used.

NOTE: When the HR PDU session with local traffic routing is used, the V-EASDF sent to the UE via DNS response applies to the DNS query being handled. The subsequent DNS queries are sent to the Global EASDF for further handling, which may repeat step 2.

3. If PDU Session configuration was received, then the UE initiates a PDU Session Establishment procedure with the configuration received in previous step. The SMF may indicate to the UE the EASDF that the UE shall use for this PDU Session according to TS 23.548 [3] clause 6.2.3.2.2 step 1 & 2.

4. The UE performs EAS Discovery, same as TS 23.548 [3] clause 6.2.3.2.2 step 7. In case the UE received an EASDF address during step 2 above, then the UE uses that address instead of the one provided by the PDU Session establishment.

5. EASDF sends the DNS Response(s) to the UE, same as TS 23.548 [3] clause 6.2.3.2.2 step 19.

6. The UE application starts to utilize the provided EAS.

### 6.9.3 Impacts on services, entities and interfaces

Editor's note: This clause is FFS.

## 6.10 Solution 10 (KI#1): LBO PDU Session establishment using PLMN criteria in RSD

### 6.10.1 Description

This solution corresponds to KI#1, and addresses the scenario which UE accessing EHE in VPLMN using LBO PDU Session.

For better illustration, it is assumed that Service 1 is deployed in both HPLMN and EHE in VPLMN, and Service 2 is deployed only in HPLMN (or deployed in EHE in VPLMN, but the UE is not allowed to access to EHE in VPLMN for Service 2).

When UE accesses to VPLMN, UE may access to EHE in VPLMN via a LBO PDU Session, and access to HPLMN via a HR PDU Session. That means URSP rules with different RSDs shall be used for Service 1 accessing to EHE in VPLMN and Service 2 accessing to HPLMN.

When UE access to HPLMN, it is unnecessary to access to Service 1 and Service 2 via different PDU Sessions. That means URSP rules with same RSD shall be used for Service 1 and Service 2.

Adding Route Selection Validation Criteria related to PLMN(s) is a way to meet both requirements on S-NSSAI/DNN pair mentioned above. Table 6.10.1-1 illustrates the enhanced RSD, and Table 6.10.1-2 gives an example of the enhanced RSD for Service 1.

Table 6.10.1-1: Route Selection Descriptor with PLMN criteria

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Information name | Description | Category | PCF permitted to modify in URSP | Scope |
| Route Selection Descriptor Precedence | Determines the order in which the Route Selection Descriptors are to be applied. | Mandatory (NOTE 1) | Yes | UE context |
| **Route selection components** | *This part defines the route selection components* | Mandatory (NOTE 2) |  |  |
| Network Slice Selection | Either a single value or a list of values of S-NSSAI(s). | Optional  (NOTE 3) | Yes | UE context |
| DNN Selection | Either a single value or a list of values of DNN(s). | Optional | Yes | UE context |
| … | … | … | … | … |
| **Route Selection Validation Criteria**  (NOTE 6) | *This part defines the Route Validation Criteria components* | Optional |  |  |
| Time Window | The time window when the matching traffic is allowed. The RSD is not considered to be valid if the current time is not in the time window. | Optional | Yes | UE context |
| Location Criteria | The UE location where the matching traffic is allowed. The RSD rule is not considered to be valid if the UE location does not match the location criteria. | Optional | Yes | UE context |
| **PLMN Criteria (new)** | **The PLMN(s) the matching traffic is allowed. The RSD is not considered to be valid if the serving PLMN is not in the PLMN criteria.** | **Optional** | **Yes** | **UE context** |

Table 6.10.1-2: An example of RSDs with PLMN criteria

|  |  |  |  |
| --- | --- | --- | --- |
| URSP rule | Information name | | Content |
| Traffic Descriptor | | Service 1 |
| RSD 1 | Network Slice Selection | S-NSSAI 1 |
| DNN Selection | DNN 1 |
| **PLMN Criteria** | **HPLMN** |
| RSD 2 | Network Slice Selection | S-NSSAI 1 |
| DNN Selection | DNN 2 |
| **PLMN Criteria** | **VPLMN 1, VPLMN 2, …** |

NOTE: Before concluding this solution for normative work, alignment check with FS\_eUEPO shall be done in order to avoid any conflict with the conclusion of KI#1 in TR 23.700-85 [10]. Final decision on generic URSP enhancement for supporting LBO roaming case should be made within FS\_eUEPO study.

### 6.10.2 Procedure

The provision of the enhanced URSP with PLMN criteria re-uses the procedure in current specification TS 23.502 [9], or UE may be pre-configured the URSP. When UE triggers PDU Session selection or PDU Session establishment based on URSP, the UE takes the serving PLMN into consideration.

### 6.10.3 Impacts on services, entities and interfaces

PCF:

- PCF controls the UE to use different DNN+S-NSSAI in different PLMN by including PLMN Criteria in URSP RSDs.

UE:

- UE shall consider the serving PLMN when it determines whether to re-use or establish PDU Session, if PLMN Criteria is included in the selected Route Selection Descriptor.

## 6.11 Solution 11 (KI#2): Exposure of Network Congestion

### 6.11.0 General

This solution corresponds to KI#2 on Fast and efficient network exposure improvements.

Based on the use cases and scenarios in clause 5.2.2, the following network congestion information needs to be exposed to AF via local UPF/NEF:

- QoS Notification Control. For GBR QoS Flow, RAN exposes "GFBR can no longer be guaranteed" (or "GFBR can be guaranteed"), as well as the reference to the matching Alternative QoS Profile to AF via local UPF/NEF.

- Network Congestion indication. For non-GBR QoS Flow, RAN exposes network congestion indication that indicates network congestion occurs to AF via local UPF/NEF.

- Network Congestion Level. This indicates the degree of RAN congestion. RAN exposes network congestion level to AF via local UPF/NEF.

NOTE 1: How to determine the network congestion level of a RAN node is up to RAN implementation.

NOTE 2: This solution targets to services with user plane packet transmission.

### 6.11.1 Procedure

Figure 6.11.1-1 shows the call flow for exposing network congestion information to AF via local UPF/NEF.



Figure 6.11.1-1: Network Congestion Information Exposure to AF via local UPF/NEF

The procedure is based on the Network exposure to Edge Application Server procedure in clause 6.4.2.1 of TS 23.548 [3].

0. The UE establishes a PDU Session as defined in clause 4.3.2.2.1 of TS 23.502 [9]. A local PSA UPF is selected for this PDU Session.

1. AF initiates setting up an AF session with required QoS procedure as defined in clause 6.4.2.1 of TS 23.548 [3].

The AF may subscribe to direct notification of network congestion for the service data flow to PCF.

2. The PCF makes policy information based on the AF request and initiates PDU Session Modification procedure as described in clause 4.3.3.2 of TS 23.502 [3], steps 1b, 3b, 4-8b. The PCF sends policy information to SMF.

If the SMF receives the indication of direct notification of network congestion, the SMF invokes Namf\_Communication\_N1N2MessageTransfer service of AMF, and AMF sends N2 PDU Session Request to RAN to indicate the RAN to expose network congestion information via local UPF. Based on local configuration, the SMF can further determine whether to enable direct notification of network congestion for this QoS Flow to NG-RAN.

NOTE 1: With this enhancement, the PCF can be configured to only enable the Notification control over User Plane for the QoS Flow subject to edge computing.

The SMF sends network congestion detection indication to UPF to enable network congestion notification detection. A report updating threshold may be informed to the UPF.

Editor's note: How the report updating threshold is determined is FFS.

The N2 SM information also includes measure frequency, report threshold.

If there is no corresponding UL service data flow template for the service data flow, e.g., the service data flow has different QoS requirements for uplink and downlink, the SMF also indicates a different QoS Flow with corresponding UL service data flow template to the RAN for the reporting. The RAN exposures network congestion information via UL packets corresponding to the indicated QoS Flow.

3. Based on local configuration and step 2, the RAN determines network congestion information when network congestion occurs. The network congestion information can be any information listed in clause 6.11.0.

4. In case the reporting condition is met, the RAN sends the network congestion information to the local PSA via the GTP-U header of corresponding UL packet.

If the RAN is requested to report the network congestion information via a different QoS flow, the RAN sends the network congestion information via UL packets corresponding to the QoS Flow indicated by the SMF.

If no UL packet can be used when report is needed, RAN generate a dummy UL packet for the report.

As described in clause 6.11.0, the network congestion information includes QoS Notification Control information (for GBR QoS Flow) and network congestion level/indication (for non-GBR QoS Flow).

NOTE 2: It is up to RAN implementation to decide whether a changed network congestion information needs to be updated to the local PSA based on e.g. local configured update condition.

NOTE 3: RAN can repeat the network congestion information to the local PSA multiple times to avoid loss of the report.

5. The local PSA exposes/updates the network congestion information to AF as described in step 4 of Figure 6.4.2.1-1 of TS 23.548 [3].

If a report updating threshold is informed by the SMF in step 2, local PSA updates the latest network congestion information to the AF when the difference between latest and previous reported network congestion information exceeds the report updating threshold.

NOTE 4: The AF logic after receiving the network congestion information is not in the scope of this study.

### 6.11.2 Impacts on services, entities and interfaces

AF:

- subscribe direct notification of network congestion information from 5GC.

SMF:

- indicate RAN to expose network congestion information via local UPF.

- indicate a UL QoS Flow for RAN to be used to expose network congestion information when there is no UL QoS Flow of the service data flow.

RAN:

- support expose network congestion information via local UPF.

## 6.12 Solution 12 (KI#2): Efficient exposure of RAN information

### 6.12.1 Key Issue mapping

The solution applies to KI#2: Fast and efficient network exposure improvements.

### 6.12.2 Description

In general, the application server support monitoring the data rate of the link between the client and server. The application server uses the monitored result to adjust service data throughput and the handling within the server. There are many factors impacting on the data rate of the link, e.g. the congestion of the transport network. The 5GS link is partial segment of the link between the client and server. Reporting network resource congestion of the 5GS can help the application server to estimate the bottle neck is in 5GS or other part between the server and the client, when the link data rate decreases outstandingly.

Hence, it is proposed to expose the network congestion of the 5GS to the application server.

In general, the bottleneck of the network congestion is the RAN congestion since the time-frequency resource is limited. However, the RAN does not support service-based interface and it is not efficient to expose RAN's congestion from RAN to AF via AMF-SMF-PCF-NEF.

In order to support efficient exposure of RAN's congestion, it is proposed to considered to expose RAN's congestion via user plane, as shown in figure 6.12.2-1.



Figure 6.12.2-1: exposure RAN's congestion

The solution is based on the existing Network Exposure functionality with the following enhancement:

- The AF subscribes the network congestion with a UE address.

- The PCF generates a PCC rule for RAN to report RAN's congestion.

- The SMF generates a QoS flow's QoS profile for RAN report.

- The RAN reports RAN Congestion Start, RAN Congestion End, RAN's congestion level from the UL data in the QoS flow for RAN report.

- The UPF detects the RAN Congestion Start, RAN Congestion End, RAN's congestion level from the UL data in the QoS flow for RAN report.

### 6.12.3 Procedures

#### 6.12.3.1 Procedure for subscribing information



Figure 6.12.3.1-1: Subscribing Normal Data Transmission Interruption event and Date Rate

1. The AF subscribes the Network Congestion (e.g. RAN congestion) by sending Nnef\_EventExposure\_Subscribe request (UE address, event ID(s)).

2. The NEF authorizes the AF request.

3. The NEF interacts with the PCF by triggering a Npcf\_PolicyAuthorization\_Subscribe request to the Network Congestion (e.g. RAN congestion).

4. Upon reception of the subscribe request of Network Congestion for a UE address, the PCF generates a QoS rule for RAN to report RAN’s congestion. The PCC rule includes an indication that the PCC rule is used for RAN report information.

The PCF also generates a QoS monitoring policy for network congestion measurement.

5. The PCF responds to the NEF a Npcf\_Policy Authorization\_Create response.

6. The NEF sends a Nnef\_AFsessionWithQoS\_Create response message to the AF.

7. The PCF initiates SM Policy Association Modification Request (PCC rule) to the SMF.

The SMF maps a QoS flow for the PCC rule from the PCF. The QoS flow's QoS profile includes the indication that the QoS flow is used for RAN report information.

The SMF generates the QoS Monitoring configuration for UPF: RAN congestion detection indication.

The SMF generates the QoS Monitoring configuration for RAN: RAN congestion measurement indication, measure frequency, report threshold.

8. The SMF replies SM Policy Association Modification Response to the PCF.

9. The SMF initiates N4 Session Modification Request (QoS Monitoring configuration, QoS rule) to the UPF.

Upon reception of QoS Monitoring configuration, the UPF enables the RAN's congestion detection and report.

10. The UPF(s) respond to the SMF.

11. For SMF requested modification, the SMF invokes Namf\_Communication\_N1N2MessageTransfer ([N2 SM information] (PDU Session ID, QFI(s), QoS Profile(s), QoS Monitoring configuration), N1 SM container)).

12. The AMF may send N2 ([N2 SM information received from SMF], NAS message (PDU Session ID, N1 SM container (PDU Session Modification Command))) Message to the (R)AN.

Upon reception of QoS flow’s QoS profile and the indication that the QoS flow is used for RAN report information, the RAN skip to map DRB for the QoS flow and make the QoS flow terminated between the RAN and the UPF.

Upon reception of QoS Monitoring configuration, the RAN enables the RAN congestion measurement and report.

14. The (R)AN may acknowledge N2 PDU Session Request by sending a N2 PDU Session Ack Message to the AMF.

15-16. The AMF forwards the N2 SM information and the User location Information received from the AN to the SMF via Nsmf\_PDUSession\_UpdateSMContext service operation. The SMF replies with a Nsmf\_PDUSession\_UpdateSMContext Response.

17-18. The SMF may update N4 session of the UPF(s) that are involved by the PDU Session Modification by sending N4 Session Modification Request message to the UPF.

#### 6.12.3.2 Procedure for information report



Figure 6.12.3.2-1: Normal Data Transmission Interruption event and measured Date Rate

1&2. When the RAN congestion starts or congestion level reaches the report threshold, the NG-RAN indicates the RAN Congestion Start and RAN congestion level in the GTP-U header of the UL data.

3. Upon detection of the RAN Congestion Start and RAN congestion level from the UL data, the UPF triggers the Nupf\_EventExposure\_Notify message to report the RAN Congestion Start and RAN congestion level.

4. The NEF sends a Nnef\_Nnef\_EventExposure\_Notify (RAN Congestion Start and RAN congestion level) message to the AF.

5&6. When the RAN congestion ends, the NG-RAN indicates the RAN Congestion End in the GTP-U header of the UL data.

7. Upon detection of the RAN Congestion End from the UL data, the UPF triggers the Nupf\_EventExposure\_Notify message to report the RAN Congestion End.

8. The NEF sends a Nnef\_Nnef\_EventExposure\_Notify (RAN Congestion End) to the AF.

### 6.12.4 Impacts on services, entities and interfaces

AF:

- subscribe network congestion information from 5GC.

PCF:

- generate a PCC rule for RAN to report RAN's congestion. The PCC rule includes an indication that the QoS rule is used for RAN report information.

- generate a QoS monitoring policy for RAN congestion information measurement.

SMF:

- indicate RAN to expose RAN congestion information via UPF.

- setup a QoS flow between the RAN and UPF for RAN to report RAN congestion information.

RAN:

- setup a QoS flow between the RAN and UPF for RAN to report RAN congestion information.

- detect and report RAN congestion information to UPF.

UPF:

- detect and expose RAN congestion information to AF/NEF.

## 6.13 Solution 13 (KI#2): Fast and efficient network exposure improvements

### 6.13.1 Introduction

This solution addresses the KI#2: Fast and efficient network exposure improvements. This solution reuses mechanism defined to establish QoS Monitoring as specified in TS 23.501 [2] clause 5.33.3, TS 23.502 [9] clause 4.3.3 and support of network exposure with low latency to local AF as specified in TS 23.548 [3] clause 6.4.2.

Editor's note: In FS\_UPEAS further enhancements will be defined for support of network exposure.

The solution is based on following principles:

- The local AF subscribes the low latency exposure of cell ID, etc. from the PCF via a local NEF.

- NG-RAN provides information such as cell ID(s) as requested by the SMF.

- UPF exposes received information as defined in TS 23.502 [9] clause 5.2.26 and further enhanced in FS\_UPEAS to local NEF/AF.

- The local AF may use received information about the cell(s) currently serving a UE to retrieve current and predicted UE and cell radio conditions from RAN. Such information may be used by local AF and applications, for instance, to trigger video codec rate adaption and prevent user experience degradation.

Editor's note: Which additional information is exposed is FFS.

### 6.13.2 Functional Description

This solution addresses KI#2 and the following principles are used:

1. The local AF subscribes using Nnef\_AFSessionWithQoS / Npcf\_PolicyAuthorization\_Subscribe service the low latency exposure of cell ID(s), etc. from the PCF via a local NEF as defined in TS 23.548 [3] clause 6.4.2.1. The local AF may also subscribe direct event notification from the UPF to the local AF as defined in TS 23.548 [3] clause 6.4.2.1.

2. PCF sends this subscription to SMF as defined in TS 23.548 [3] clause 6.4.2.1, together with requested information.

3. The SMF configures NG-RAN via AMF, and the UPF over N4 for the UPF, with the requested to notify AF.

4. NG-RAN node sends the requested information e.g. cell ID(s) in NG-RAN UL (Uplink) over GTP-u to UPF. Requested nformation may be sent, e.g., using UL PDU Session Information as defined in TS 38.415 [14] for QoS Monitoring information.

Editor's note: How fast and frequent would the information need to be provided to the AF is FFS.

NOTE: AF may use e.g. Cell ID to obtain additional information e.g. using APIs defined by ETSI MEC, etc. but these are outside the scope of this solution.

5. This SMF provided configuration is transferred to the new/target NG-RAN node when the UE has been handed over to a the new/target NG-RAN node.

6. If the serving cell Id(s) has changed (and upon receiving the SMF request), the NG-RAN provides the latest/new serving cell Id(s).

7. The UPF exposes received information to local NEF/AF as defined in TS 23.502 [9] clause 5.2.26 and further enhanced in FS\_UPEAS.

### 6.13.3 Procedures

This procedure is based on TS 23.548 [3] clause 6.4.2.1 for Network Exposure to Edge Application Server and further enhanced in FS\_UPEAS as follows:

UE

RAN

AMF

L-PSA UPF

SMF

PCF

Local NEF/  
NEF

AF

new AF

0. PDU Session establishment

1a. AF Session (cell ID(s), other info indication)

1b. Npcf\_PolicyAuthorization\_Subscribe

3. UL GTP-u packet(s) including requested information

4a. Nupf\_EventExposure\_Notify

4b. Nnef\_EventExposure\_Notify

2a. PCC rules in Npcf\_SMPolicyControl\_Create / Npcf\_SMPolicyControl\_UpdateNotify

2b. N4 Session Modification

2c. PDU Session Resource Setup / Modify

Figure 6.13.3-1: Reporting information by the NG RAN to local AF.

0. The UE establishes a PDU Session as defined in clause 4.3.2.2.1 of TS 23.502 [9]. A L-PSA UPF is assigned for this PDU Session.

1. The AF initiates setting up an AF session with required QoS procedure as defined in clause 4.15.6.6 of TS 23.502 [9].

In the request, the AF may subscribe to direct notification of requested information such as Cell ID(s), for the service data flow to PCF possibly via Local NEF or NEF.

The AF may also first initiate an AF Session with PCF and later subscribe to direct notification of requested information to PCF by invoking Npcf\_PolicyAuthorization\_Subscribe service operation.

The local AF or NEF may discover a local NEF as specified in TS 23.548 [3] clause 6.4.2.1 step 1.

2. The PCF makes the policy decision and initiates the PDU Session modification procedure as defined in clause 4.3.3.2 of TS 23.502 [9], steps 1b, 3b, 4-8b.

If the direct notification is subscribed, 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.

If the SMF receives (2a) the indication of direct event notification form the PCF and the SMF determines that the L-PSA UPF supports such reporting, the SMF sends (2b) requested information indication and associate the indication with the target local NEF or local AF address to the L-PSA UPF via N4 rules.

The SMF sends (2c) via N2 to NG-RAN within a PDU Session resource Create/Modify (defined in TS 38.413 [15]) a request to send to the UPF requested information that contains e.g. the cell(s) currently serving a PDU Session, etc.

3. The L-PSA UPF obtains requested information sent in GTP-u by NG-RAN.

If the SMF had beforehand requested that the NG-RAN sends an indication and the PDU Session resources have been released in the NG-RAN, the NG-RAN needs to send to the UPF an indication that the cell(s) currently serving the PDU Session and /or the UE identity as handled by the NG-RAN are no more valid.

If there is no UL traffic the NG-RAN may send a GTP-u packet with no user plane traffic (dummy UL packet).

The NG-RAN may send updated serving cell Id(s) and/or UE identity as handled by the NG-RAN in multiple UL packet sent over 5GS N3 interface (in order to not lose the information if some UL traffic was discarded between the NG-RAN and the UPF responsible of the reporting to the EC AF).

4. The L-PSA UPF sends the notification related requested information over Nupf\_EventExposure\_Notify service operation as specified in TS 23.548 [3] clause 6.4.2.1 step 4 (a, b).

5-8. may follow as specified in TS 23.548 [3] clause 6.4.2.1.

### 6.13.4 Impacts on services, entities and interfaces

Editor's note: This clause lists impacts to services, entities, and interfaces.

Proposed information exposure impacts the same entities and interfaces as QoS monitoring defined in Rel-16.

NG-RAN:

- should support exposing of requested information such as Cell ID(s) in GTP-u packets.

UPF:

- should support exposing of requested information such as Cell ID(s) in GTP-u packets.

- should support exposing requested information which includes cell ID(s) in Nupf\_Event\_Exposure\_Notify.

NEF, PCF, SMF:

- should support indication of RAN assistance information in Nnef\_AFSessionWithQoS / Npcf\_PolicyAuthorization\_Subscribe.

SMF and UPF:

- N4 should support indication of requested information.

## 6.14 Solution 14 (KI#4): Group Management

### 6.14.1 Introduction

This solution addresses the Key Issue #4, and in particular how to define a collection of UEs forming a dynamic ad-hoc group. This dynamic ad-hoc group may be then used to identify the users that should use the same EAS and/or same local part of DN and/or same DNAI.

This solution makes the following assumptions:

- AF determines the identities of the UEs that should be part of the collection and creates an ad-hoc group for this collection to the 5GC. The AF includes an External Group ID in the group creation request. The AF can add or remove users in the group in dynamic manner. 5GC stores the group members with associated Internal and External Group IDs.

- The AF uses the Traffic Influence and EAS Deployment services to submit edge service related data for the given ad-hoc group as identified by the External Group ID. No impact to Rel-17 is foreseen.

- The 5GC is responsible to determine and select a common local part of the DN for the group members. This step is not in the scope of this solution proposal.

Editor's note: For the dynamic group management, coordination between FS\_EDGE\_Ph2 and FS\_GMEC is needed.

### 6.14.2 Functional Description

The solution is based on the following principles:

- In this solution, the AF is responsible to create and maintain the ad-hoc group data in 5GC. NEF provides a generic Group Management service for the AF to create, modify and delete ad-hoc groups in 5GC. Generic here means that the group data does not contain any service specific data, but instead any service data can be associated with the corresponding group identifier. This solution proposal describes how the traffic influence service data and EAS Deployment Information data can be associated with the group data, but the same principle could be used with any other service data.

- Upon receiving a request to include a user into a group (i.e. when the group is created or a new user is added to the group), the UDM ensures that the group data and individual subscription data are aligned; i.e. the UDM updates the individual user subscription data for the group member to contain the Internal Group ID of the group. In similar manner, when the AF requests a user to be removed from a group, the UDM removes the corresponding Internal Group ID from the individual user subscription data. A user may belong to more than one group.

- Nnef\_TrafficInfluence service as specified in Rel-17 is used to store the DNN/S-NSSAI and the Internal Group ID. The service data may contain an "Indication of traffic correlation" parameter as defined in clause 5.6.7 in TS 23.501 [2] to indicate that a common local part of DN should be selected. The service data is applicable for all members of the given group using the given DNN/S-NSSAI.

- Nnef\_EASDeployment service as specified in clause 6.2.3.4 in TS 23.548 [3] is used to store the EAS Deployment Information in the NEF and UDR. The SMF retrieves the EAS Deployment Information from the NEF and configures the DNS handling rules to EASDF correspondingly. EAS Deployment Information can contain an Internal Group ID as described in Table 6.2.3.4-1 in TS 23.548 [3]. The service data is applicable for all members of the given group using the given DNN/S-NSSAI.

- A single DNN/S-NSSAI may be used by multiple ad-hoc groups. In this case the groups may be controlled by the same or different AFs, each submitting a different traffic influence service data containing the same DNN/S-NSSAI.

The figure 6.14.2-1 illustrates the overall structure of the Group management data, Traffic Influence data, and EAS Deployment Information data.



Figure 6.14.2-1: Overall structure of the Group management data and Traffic Influence data

The NEF provides three distinct services: 1) generic Group Management service, 2) Traffic Influence service, and 3) EAS Deployment service.

For the Group Management service, either a new service must be specified, or the existing Nnef\_ParameterProvision service is used as specified in clause 5.29.2 in TS 23.501 [2]. In the latter case, the Nnef\_ParameterProvision service shall be generalized so that it can be used also for groups that are not specific for 5G VN group communication service. This means that the group data should not be required to contain any service specific data, as the group data can be referenced from any service.

As specified in clause 5.29.2 in TS 23.501 [2], the UDM ensures that the group data and user subscription data are aligned, i.e. the user who is listed as a member in the group data should have the same group identity in the user subscription data.

For the Traffic Influence and EAS deployment services, the existing procedures are used to store the traffic influence data and EAS Deployment Information data into UDR. The traffic influence data and EAS Deployment Information data can contain a DNN/S-NSSAI and Internal Group ID that the service data is applicable for.

The figure 6.14.2-2 illustrates how the UDMs can align the group data and individual subscription data in a case where the group data and individual user subscription data are served by different UDMs.



Figure 6.14.2-2: Different UDMs serving the user(s) and group

AF invokes a group creation request to the NEF (not shown in the figure). The NEF discovers the UDM-1 based on the External Group ID. The UDM-1 receives the group creation request from the NEF. UDM-1 stores the group data into UDR (not shown in the figure). UDM-1 uses the SUPI to discover the UDM for the member (UDM-2). UDM-1 uses a new service operation Nudm\_SDM\_Set to update the user subscription data for the member's SUPI and adds the Internal Group ID of the group to the user subscription data. If the user subscription data is updated via OAM, the UDM-2 notifies the UDM-1 for the data change.

Editor's note: It is FFS whether the multiple UDMs case needs to be supported.

### 6.14.3 Procedures

Figure 6.14.3-1 describes an overview of the procedure to create an ad-hoc group that is used to determine the collection of users that should have a common local part of DN.



Figure 6.14.3-1: Creation of a group and using it for selecting the local part of DN

1. Group Management:

The AF invokes a group creation request to the NEF. The group creation request contains an External Group ID and list of GPSIs that are members in the group. NEF uses an UDM service to create the group. The group data contains the members (GPSIs) and External Group ID. The UDM may further store the group data into UDR. UDM/UDR assigns an Internal Group ID for the group and stores it to the group data.

Upon receiving a request to include a user into a group, the UDM updates the individual user subscription data for the group members to contain the Internal Group ID of the group.

Editor's note: It is FFS how it is ensured that the Internal Group ID for different groups stored in different UDMs and/or UDRs are unique.

2. Edge service management (no impact):

AF uses the Nnef\_TrafficInfluence service as specified in clause 4.3.6.2 in TS 23.502 [9] to influence SMF routeing decisions for User Plane traffic of PDU Sessions. AF uses the Nnef\_EASDeployment service as specified in clause 6.2.3.4 in TS 23.548 [3]. The AF may include an External Group ID to the service requests. If the AF requires that the same local part of DN is used for the group members when they access the given DNN/S-NSSAI, the AF includes the "Indication of traffic correlation" parameter to the Nnef\_TrafficInfluence service request.

The NEF uses the Nudm\_SDM\_Get (Group Identifier Translation, External Group ID) service to resolve the External Group ID to Internal Group ID, as specified in Rel-17. The NEF stores the TrafficInfluence service information and EAS Deployment Information in the UDR. The service data contains the DNN/S-NSSAI and Internal Group ID as specified in Rel-17. The PCF(s) that have subscribed for the Traffic Influence data for the matching DNN/S-NSSAI and Internal Group ID receive a notification from the UDR.

3. PDU Session establishment (not in the scope of this solution):

Upon PDU Session establishment, the SMF retrieves the user subscription data from the UDM. The user subscription data may contain one or more Internal Group IDs. The SMF passes the DNN/S-NSSAI and Internal Group ID(s) to the PCF as specified in clause 4.16.4 in TS 23.502 [9]. If the PCF does not have the traffic influence service data for the given DNN/S-NSSAI and Internal Group ID, the PCF retrieves it from the UDR.

The SMF retrieves the EAS Deployment Information for the given DNN/S-NSSAI and Internal Group ID(s) from the NEF as described in clause 6.2.3.4 in TS 23.548 [3].

4. Selecting the common local part of DN (not in the scope of this solution):

If the traffic influence service data contains the "Indication of traffic correlation" parameter, 5GC determines and selects a common local part of the DN for all PDU Sessions that use the given DNN/S-NSSAI where the user is a member in the given group.

### 6.14.4 Impacts on services, entities and interfaces

Assuming that the existing Nnef\_ParameterProvision service is used as specified in clause 5.29.2 in TS 23.501 [2] to provide a generic Group Management service, the impacts are limited to the generalization of the Nnef\_ParameterProvision service as described below.

NEF:

- Nnef\_ParameterProvision service is enhanced to remove a requirement to provide any service specific data in group creation. At least DNN and S-NSSAI are currently mandatory parameters in the Nnef\_ParameterProvision\_Create service operation when a 5G VN group is created.

UDM:

- Nudm\_ParameterProvision service is enhanced to remove a requirement to provide any service specific data in group creation. At least DNN and S-NSSAI are currently mandatory parameters in the Nudm\_ParameterProvision\_Create service operation when a 5G VN group is created.

- A new service operation Nudm\_SDM\_Set for an NF service consumer (UDM) to update user subscription data located under another UDM.

UDR:

- Nudr\_DataManagement service is used to manage the group data in the UDR. The service is enhanced to remove a requirement to provide any service specific data when the group data is stored in UDR. At least DNN and S-NSSAI are currently mandatory parameters in the Group Data Subset in subscription dataset for a 5G VN group. The UDR stores the Internal/External Group IDs and the member list (list of SUPIs).

## 6.15 Solution 15 (KI#4): Selection of common DNAI

### 6.15.1 Introduction

This solution aims to address the KI#4 created for WT#6 related to the influence on UPF and EAS (re)location for a collection of UEs in scenarios when the UEs should use the same EAS and are not members of a pre-defined group.

As addressed under the key issue description, the UPF selection and relocation, and deciding on a common local part of DN are the focus of this solution. In practice, an optimal common local part of DN would be needed to make the service experience best for all UEs in the group.

How to define a collection of UEs forming a dynamic ad-hoc group is not in the scope of this solution proposal.

### 6.15.2 Functional Description

The solution is based on the following principles:

- Group SMF (gSMF) entity is introduced to determine the location of the common local part of DN (L-DN) and used for common DNAI selection.

- Individual SMFs one by one add more sessions to the collection of PDU Sessions that is managed by the gSMF, and gSMF selects the common DNAI for this collection of PDU sessions. gSMF can re-consider the common DNAI whenever a new PDU session "joins" to an existing collection of PDU Sessions.

- The interface between SMF and gSMF can be based on subscribe/notify model, so even if the gSMF fails to select the common DNAI in some error case, the individual SMFs can proceed as with regular UPF/DNAI selection as a fallback.

- gSMF can make the decision on the common DNAI based on the information it receives from individual SMFs. Then, each SMF selects the location of the UPF based on the common DNAI and relocates the UPF on PDU Session basis.

- For selecting the common DNAI, gSMF may further use Analytics services from NWDAF for determining service experience between the gNB and candidate UPFs.

- Nnef\_TrafficInfluence service as specified in TS 23.501 [2] is used to store the DNN/S-NSSAI, Internal Group ID, and a list of DNAIs. The traffic influence data may contain an "Indication of traffic correlation" parameter as defined in clause 5.6.7 in TS 23.501 [2] to indicate that a common DNAI should be selected. PCF retrieves the traffic influence data from UDR and constructs the PCC Rules accordingly. No impact to Nnef\_TrafficInfluence service is foreseen.

- Nnef\_EASDeployment service as specified in clause 6.2.3.4 in TS 23.548 [3] is used to store the EAS Deployment Information in the NEF and UDR. The SMF retrieves the EAS Deployment Information from the NEF and configures the DNS handling rules to EASDF correspondingly. EAS Deployment Information can contain an Internal Group ID as described in Table 6.2.3.4-1 in TS 23.548 [3]. No impact to Nnef\_EASDeployment service is foreseen.

- The solution proposes to enhance the PCC Rules by adding a new identifier "influence-id", which is associated with the list of DNAIs in the PCC Rules. UDR assigns the "influence-id" for each entry in the traffic influence data in the UDR when the entry is created as specified in Rel-17. In this solution, the PCF retrieves the "influence-id" from the UDR as part of the traffic influence data and includes it to the PCC Rules. This is necessary when the same DNN/S-NSSAI is used by multiple ad-hoc groups (Internal Group IDs), where each group has different traffic influence service data (e.g. list of DNAIs) containing the same DNN/S-NSSAI. In this case the PCC Rules will contain multiple lists of DNAIs and the "influence-id" is used to determine the lists of DNAIs in different PDU Sessions that are related to each other.

### 6.15.3 Procedures

#### 6.15.3.1 General

The overall procedure is described in figure 6.15.3.1-1.



Figure 6.15.3.1-1: Overall procedure

1. Prerequisite: AF has created an ad-hoc group in 5GC. AF submits the traffic influence data and EAS Deployment Information data for the group to 5GC. This step is out of scope of this solution.

2. Upon PDU Session establishment, the SMF retrieves the user subscription data from the UDM. The user subscription data may contain one or more Internal Group IDs. The SMF passes the DNN/S-NSSAI and Internal Group ID(s) to the PCF as specified in clause 4.16.4 in TS 23.502 [9]. If the PCF does not have the traffic influence service data for the given DNN/S-NSSAI and Internal Group ID(s), the PCF retrieves the data from the UDR. The PCF creates or updates the PCC Rules to the SMF.

The PCC Rules contain a list of DNAIs associated with the "Indication of traffic correlation" and with "influence-id". The PCF retrieves the "influence-id" from the UDR, thus the value of "influence-id" remains the same across all PDU Sessions that use the same traffic influence data.

Editor's note: The input for the SMF retrieving the PCC rules with with the "Indication of traffic correlation" and with "influence-id" is FFS.

[Optional] If the DNS queries are to be used to influence to the EAS address selection as described in clauses 6.15.3.2 and 6.15.3.3, the SMF retrieves the EAS Deployment Information as described in TS 23.548 [3].

3. SMF(s) invoke the gSMF for selection of the common DNAI. This is described in clause 6.15.3.2.

Depending on the variation of the procedure, the SMF(s) may invoke the gSMF either based on the user subscription and service data as received in steps 1 and 2, or alternatively the SMF(s) invoke gSMF in dynamic manner based on DNS Query from the UE.

Rest of the clauses describe the following procedures:

- Clause 6.15.3.2 "Selection of the common DNAI" describes the core procedure in the solution how gSMF selects the common DNAI. This procedure is part of all solution variants.

- Clause 6.15.3.3 "EAS selection and re-selection using ECS option, preconfigured" describes a solution variant where SMF(s) invoke the gSMF based on the preconfigured user subscription and service data before any DNS Query from the UE. ECS option in DNS request is used to indicate the common DNAI to the DNS server.

- Clause 6.15.3.4 "EAS selection and re-selection using ECS option, dynamic invoke of gSMF" describes a solution variant where SMF(s) invoke the gSMF based on a DNS Query from the UE. ECS option in DNS request is used to indicate the common DNAI to the DNS server.

- Clause 6.15.3.5 "EAS selection and re-selection via application layer" describes a solution variant where SMF(s) invoke the gSMF based on the user subscription and service data. Early/late UP path change notifications are used to indicate the common DNAI to the application layer.

#### 6.15.3.2 Selection of the common DNAI

Figure 6.15.3.2-1 describes a procedure for selection of common DNAI for the collection of UEs that should use a common local part of DN and common EAS.



Figure 6.15.3.2-1: Selection of the common DNAI

1. SMF receives the user subscription data and PCC Rules as described in step 2 in clause 6.15.3.1. Based on the "Indication of traffic correlation" and "influence-id" associated with a list of DNAIs in the PCC Rules, SMF knows that it needs to discover a gSMF for a selection of a common DNAI. SMF discovers the gSMF from NRF. SMF discovers one gSMF for each "influence-id" associated with a list of DNAIs in the PCC Rules.

BSF can be used to ensure that the same gSMF is selected for all PDU Sessions with the same "influence-id"; SMF uses the "influence-id" to retrieve the gSMF identity from the BSF. If the registration in BSF for the given "instance-id" does not exist, the SMF discovers the gSMF from NRF, using e.g. the Internal Group ID as a discovery factor. gSMF registers the "influence-id" to BSF after gSMF has been selected for the first PDU Session for an "influence-id".

Editor's note: How SMF discovers gSMF from NRF is FFS.

2. The SMF invokes the gSMF and indicates the "influence-id", SUPI, DNN/S-NSSAI, and a list of DNAIs for the given "influence-id" as received in the PCC Rules to the gSMF. The SMF invokes the gSMF for each "influence-id" associated with a list of DNAIs in the PCC Rules.

3. For the selection of the common DNAI for a collection of PDU Sessions associated with the same "influence-id", the gSMF may consider the UE locations, network topology, or the current Analytics from NWDAF for service experience between the gNB and candidate UPFs. gSMF can subscribe for UE location info (UE mobility events) for the SUPI from the AMF.

If the gSMF uses Analytics services from NWDAF, the gSMF invokes the NWDAF on PDU Session and "influence-id" basis.

4. gSMF determines the common DNAI per each "influence-id" and notifies the SMF(s) of the corresponding "influence-id" for the result. Based on the notification from the NWDAF, or any internal trigger, gSMF can reselect a new common DNAI, and notify the SMF(s) for the change of the common DNAI accordingly.

5. The SMF(s) select and relocate the UPF based on the notifications from gSMF. The SMF configures the UPF to route the UL traffic towards the EAS in the L-DN. The details depend on how the EAS is discovered and is described in clause 6.15.3.2.

6. Whenever a new UE that belongs to the same Internal Group ID initiates a PDU Session with the given DNN/S-NSSAI, the steps 2-5 are performed for the new PDU Session.

If the gSMF determines a new common DNAI for the group, the SMF(s) of the existing PDU Sessions are notified by the gSMF for a new common DNAI. This may be done e.g. due to a new PDU Session joining to the group, or one of the existing PDU Sessions are released, or one or more of the UEs in the group are moving and the gSMF finds a more optimal DNAI.

#### 6.15.3.3 EAS selection and re-selection using ECS option, preconfigured

Figure 6.15.3.3-1 describes a procedure for EAS selection and re-selection for a group of UEs when DNS queries from the UE influence to the EAS selection. EDNS Client Subnet option in the DNS Query is used to indicate the common DNAI to the DNS server. The SMF subscription for the common DNAI from gSMF is done based on the pre-configured edge service data that is applicable for the PDU Session, i.e. traffic influence data and EAS Deployment Information as described in TS 23.548 [3].

The flow is applicable for all connectivity models described in TS 23.548 [3]. UPF in the figure correspond to PSA UPF in the local site (L-PSA UPF). In case of Session Breakout connectivity model, the UL-CL or BP is used although not shown in the figure. In case of Distributed Anchor connectivity model, instead of EASDF a DNS resolver that is preconfigured with the ECS Option may be used.



Figure 6.15.3.3-1: EAS (re-)selection using ECS option, preconfigured

Pre-requisite: SMF receives the user subscription data and PCC Rules as described in step 2 in clause 6.15.3.1. SMF has invoked the gSMF as described in clause 6.15.3.2. gSMF notifies the SMF for the common DNAI.

1. The SMF uses the common DNAI to select the UPF. The SMF configures the EASDF for the DNS message handling rules using the EAS Deployment Information as described in TS 23.548 [3]. The SMF may notify the AF for UP path change events via early and/or late notifications as described in clause 4.3.6.3 in TS 23.502 [9], based on subscriptions in the PCC Rules. The notifications indicate the common DNAI as a target DNAI.

2. When the UE initiates a DNS Query, the EASDF matches it against the rules it has received from the SMF. Based on the DNS message handling rules from SMF, the EASDF inserts an EDNS Client Subnet option to the DNS Query. The EDNS Client Subnet option refers to a location that is topologically close to the common DNAI. The DNS server may resolve the EAS IP address considering the EDNS Client Subnet option and sends the DNS Response via the EASDF and UPF1 to the UE.

3. Application client and EAS transmit data via the user plane via UPF.

4. If the gSMF determines a new common DNAI as described in step 6 in clause 6.15.3.2, the gSMF notifies all SMF(s) that have subscribed for the given "instance-id". The SMF(s) reselect the UPF accordingly. SMF(s) notify the AF as in step 2.

The SMF(s) trigger an EAS rediscovery procedure with the UE(s). In case of Distributed Anchor Point connectivity model as described in TS 23.548 [3], when the SMF relocates the UPF, the UE detects that the PDU Session is released or new IP prefix is allocated within the PDU Session, and the UE removes the old DNS cache related to old/removed IP address/prefix as described in clause 6.2.2. in TS 23.548 [3].

In case of Session Breakout connectivity model as described in TS 23.548 [3], the SMF sends PDU Session Modification Command (EAS rediscovery indication, [impact field]) to UE as described in in clause 6.2.3.3 in TS 23.548 [3]. The EAS rediscovery indication indicates to refresh the cached EAS information. The UE behaves as described in TS 23.548 [3].

The UE(s) resolve the new EAS address as in step 2. Application client and the new EAS transmit data via the user plane via new UPF.

If the PCC Rules indicate multiple "influence-ids" with Session Breakout connectivity model, the SMF(s) may assign a separate local PSA for each common DNAI, if necessary. In Distributed Anchor connectivity model, the SMF(s) can assign a local PSA that is most optimal for any of the common DNAIs.

#### 6.15.3.4 EAS selection and re-selection using ECS option, dynamic invoke of gSMF

Figure 6.15.3.4-1 describes a procedure for EAS selection and re-selection for a group of UEs when DNS queries from the UE influence the EAS selection. EDNS Client Subnet option in the DNS Query is used to indicate the common DNAI to the DNS server. The invoke of the gSMF is done in dynamic manner based on the DNS Queries from the UE, in addition to edge service data that is applicable for the PDU Session, i.e. traffic influence data and EAS Deployment Information as described in TS 23.548 [3].

The flow is applicable for all connectivity models described in TS 23.548 [3]. In case of Session Breakout connectivity model the UL-CL or BP is used although not shown in the figure.



Figure 6.15.3.4-1: EAS (re-)selection using ECS option, dynamic model

Pre-requisite: SMF receives the user subscription data and PCC Rules as described in step 2 in clause 6.15.3.1.

1. The SMF configures the EASDF for the DNS message handling rules using the EAS Deployment Information as described in TS 23.548 [3].

2. The SMF assigs a central UPF (C-UPF) for the PDU Session.

3. When the UE initiates a DNS Query, the EASDF matches it against the rules it has received from the SMF.

4. Based on the DNS message handling rules from SMF, the EASDF reports the FQDN to the SMF. The SMF uses the user subscription data and edge service data as described in clause 6.15.3.1 step 3 to determine that the FQDN is related to a group service where a gSMF needs to be invoked.

The SMF invokes the gSMF as described in clause 6.15.3.2. The SMF selects the UPF based on the common DNAI as described in clause 6.15.3.2.

In case of Session Breakout connectivity model, the SMF configures the EASDF to insert an EDNS Client Subnet option to the DNS Query, as described in step 2 in clause 6.15.3.3.

In case of Distributed Anchor connectivity model, the SMF triggers an EAS rediscovery procedure with the UE as described in step 4 in clause 6.15.3.3.

5. In case of Distributed Anchor connectivity model, the UE re-initiates a DNS Query as in step 4 in clause 6.15.3.3. The EASDF matches it against the rules it has received from the SMF.

Based on the DNS message handling rules from SMF, the EASDF inserts an EDNS Client Subnet option to the DNS Query. The DNS server returns the EAS address to the UE.

6. Application client and EAS transmit data via the user plane via L-UPF.

7. If the gSMF determines a new common DNAI as described in step 6 in clause 6.15.3.2, the gSMF notifies all SMF(s) that have subscribed for the given "instance-id". The SMF(s) reselect the UPF accordingly. UE(s) perform an EAS reselection as described in step 4 in clause 6.15.3.2.

Editor's note: The signaling storming in control plane needs to be avoided.

If the PCC Rules indicate multiple "influence-ids" with Session Breakout connectivity model, the SMF(s) may assign a separate local PSA for each common DNAI, if necessary. In Distributed Anchor connectivity model, the SMF(s) can assign a local PSA that is most optimal for any of the common DNAIs.

#### 6.15.3.5 EAS selection and re-selection via application layer

Figure 6.15.3.5-1 describes a procedure for EAS selection and re-selection for a group of UEs when application layer protocols are used to redirect the application client in the UE to an EAS serving the group. In this case, DNS queries from the UE do not influence to the EAS selection. The flow is applicable for all connectivity models described in TS 23.548 [3]; in case of Session Breakout model, the UPFs in the figure correspond to PSA UPF in the local site (L-PSA UPF).

In this procedure, the EASDF is not involved and the Nnef\_EASDeployment service is not used.



Figure 6.15.3.5-1: EAS (re-)selection via application layer

Pre-requisite: SMF receives the user subscription data and PCC Rules as described in step 2 in clause 6.15.3.1. SMF has invoked the gSMF as described in clause 6.15.3.2. gSMF notifies the SMF for the common DNAI.

1. The SMF uses the common DNAI to select the UPF. The SMF notifies the AF for UP path change events via early and/or late notifications as described in clause 4.3.6.3 in TS 23.502 [9]. The notifications indicate the common DNAI as a target DNAI.

2. The application layer informs the UE for the group FQDN that corresponds to the current common DNAI. The UE resolves the EAS address via DNS Query. Alternatively, the application layer can inform the EAS IP address(es) directly via application layer. This step is out of scope of 3GPP.

3. Application client and EAS transmit data via the user plane via UPF.

4. If the gSMF determines a new common DNAI, the gSMF notifies all SMF(s)that have subscribed for the given "instance-id". The SMF(s) reselect the UPF accordingly. SMF(s) notify the AF as in step 1. The UE(s) resolve the new EAS address as in step 2. Application client and new EAS transmit data via the user plane via new UPF.

If the PCC Rules indicate multiple "influence-ids" with Session Breakout connectivity model, the SMF(s) may assign a separate local PSA for each common DNAI, if necessary. In Distributed Anchor connectivity model, the SMF(s) can assign a local PSA that is most optimal for any of the common DNAIs.

### 6.15.4 Impacts on services, entities and interfaces

gSMF:

- a new function. Determines the common DNAI for a collection of UEs. Notifies the SMF(s) that have subscribed for the common DNAI.

SMF:

- discovers and invokes the gSMF. Selects the UPF based on the common DNAI as notified by the gSMF.

PCF:

- receives the "influence-id" from UDR and includes it into PCC Rules as part of traffic influence data.

UDR:

- UDR indicates the "influence-id" to the PCF in Nudm\_DataManagement service response for each entry in the traffic influence data in the UDR.

## 6.16 Solution 16 (KI#4): Selecting the same EAS/DNAI for collection of UEs

### 6.16.1 Description

This solution corresponds to KI#4:

- whether and how to define a collection of UEs forming a dynamic ad-hoc group that should use the same EAS and/or same local part of DN and/or same DNAI and how the collection is identified;

- whether and what improvements are required for EAS discovery and re-discovery for UEs belonging to a collection of UEs.

The solution assumes the member of UE collection is dynamic, UEs join/leave dynamically, and here are two scenarios:

- scenario#1: the application layer just indicates 5GC to select the same EAS or the same DNAI for collection of UEs accessing the application service and under certain criteria (e.g. UEs within a specific location area), and it is 5GC to decide UE list belongs to the UE collection.

- scenario#2: the application indicates 5GC to select same EAS or the same DNAI for the UE collection without providing UE list belongs to the UE collection explicitly.

Editor's note: It if FFS what is the difference between the scenarios and how the scenarios are reflected in the procedures below.

## 6.16.2 Procedures

The following is the procedure for selecting the same EAS for collection of UEs accessing the same application. The procedures defined in figure 4.3.6.2-1 in TS 23.502 [9] and figure 6.2.3.2.2-1 in TS 23.548 [3] are reused.

There could be only one SMF for serving the collection of UEs that connecting to the same EAS/DNAI for accessing the same application, or there could be multiple SMF for different UEs in the collection. For the latter case, UDR is used for coordination between SMFs to make sure selecting the same EAS/DNAI for UEs, i.e. SMF send the selected EAS IP/DNAI to UDR or SMF gets the updated EAS IP/DNAI from UDR.



Figure 6.16.2-1: Discovery procedure for selecting the same EAS/DNAI for collection of UEs

1. The AF request in Step 1 of figure 4.3.6.2-1 in TS 23.502 [9] is used to request selecting the same EAS or same DNAI for UEs accessing the application as identified in the AF Request. An eas\_correlation indication or dnai\_correlation indication is provided for indicating selecting the same EAS or the same DNAI (i.e. selecting EAS corresponding to the same DNAI) for collection of UEs accessing the same application (e.g. FQDN), Spatial Validity Condition could be provided for limiting the location of the UEs, and also "any UE" or an UE list will be provided for defining UE collection accessing the same EAS or the same DNAI (the UE list could be determined by AF based on application layer mechanism). The DNAI could be determined and provided by AF to PCF and then to SMF. When eas\_correation is used, the solution assumes that the DNS returns only one IP address for a DNS query. If the DNS is expected to return more than one IP address, then dnai\_correlation can be used.

In step 5 of figure 4.3.6.2-1 in TS 23.502 [9], PCF determines the UEs influenced by the AF Request, and based on AF request, PCF creates PCC rule with FQDN, and eas\_correlation indication or dnai\_correlation indication to SMF.

Editor's note: It is FFS how eas\_correlation and dnai\_correlation are expressed in the PCC Rules.

2. The same as step 1~9 in figure 6.2.3.2.2-1 in TS 23.548 [3].

3. If FQDN in Neasdf\_DNSContext\_Notify Request is for the application (e.g. FQDN) indicated in AF request , and if eas\_correlation indication is set, SMF determines the UE belongs to collection of UEs accessing the application and determines the UE needs to select the same EAS as UEs in the UE collection; or if dnai\_correlation indication is set, SMF determines the UE belongs to collection of UEs accessing the application and determines the UE needs to select EAS corresponding to the same DNAI as UEs in the UE collection.

Editor's note: How the SMF determines the UE belongs to the collection of UEs and what information and how the SMF retrieves for making the decision.

4. In case of multiple SMFs, SMF synchronizes with UDR and receives EAS IP or DNAI for the UE collection. UDR maintains EAS IP or DNAI for the UE collection.

5. Based on step 10~19 in figure 6.2.3.2.2-1 in TS 23.548 [3]:

For selecting the same EAS case: if the same EAS for the UE collection has not been determined yet, steps 10~15 are used for discovering an EAS, and between step 14 and step 16, SMF could send the selected EAS IP to UDR; When the same EAS for the UE collection has been determined, in step 17, SMF sends DNS message handling rule with IP address for the EAS instructing EASDF to return the IP address for the EAS to UE in step 19, step 10~15 are skipped;

Editor's note: It is FFS what information is stored in the UDR, what parameter(s) are used as a key by the SMF to retrieve the information, and when and how the information in UDR is removed.

For selecting EAS corresponding to the same DNAI case: if no DNAI for the UE collection has been determined, in step 10 SMF determines DNAI for the UE collection and selects information to build ECS option or Local DNS server based on the DNAI; When DNAI for the UE collection has been determined, in step 10 SMF determines information to build ECS option or local DNS server related to the DNAI, and sends DNS message handling rule with the information to build ECS option or local DNS server.

6. If UDR is used for coordination between SMFs for selecting the same EAS or the same DNAI for collection of UEs, SMF synchronizes EAS IP/DNAI with UDR.

### 6.16.3 Impacts on services, entities and interfaces

AF:

- to be updated with eas\_correlation indication/ dnai\_correlation indication for indicating selecting the same EAS/DNAI for collection of UEs accessing the application.

NEF:

- Nnef\_TrafficInfluence service is impacted to include "eas\_correlation indication" or "dnai\_correlation indication", list of FQDNs and list of UE identitities.

SMF:

- to be updated for storing and retrieving the EAS/DNAI from UDR and using the retrieved EAS/DNAI when selecting the same EAS/DNAI for collection of UEs.

UDR:

- to be updated for maintaining mapping between the collection of UEs and EAS IP/DNAI for the application. UDR is in charge of storing the DNAI/EAS as indicated by SMF.

EASDF:

- to be updated for create and send DNS response to UE.

PCF:

- Npcf\_SMPolicyControl\_UpdateNotify service is to be updated to transmit PCC rule with eas\_correlation indication/ dnai\_correlation indication, and FQDN(s).

## 6.17 Solution 17 (KI#4): Application layer EAS selection for collections of UEs

### 6.17.1 Introduction

This solution corresponds to KI #4. This solution assumes that the AF is responsible for generating the collection of the UEs and select the same EAS for the collection of the UEs. The SMF(s) selects the candidate DNAI(s) for the UE(s) and exposes them to the AF. The AF determines the common DNAI considering the candidate DNAI(s) from different SMFs, then the AF can select the proper EAS with the common DNAI for the collection of the UEs.

### 6.17.2 Functional Description

This solution is based on the following principles:

- The AF can determine the user list and sends the UE list and available DNAI list to 5GC to query the candidate DNAI(s) for the UEs.

- SMF decides the candidate DNAI(s) for the UE(s) in the UE list served by the SMF according to the location of the UE(s) and the DNAI topology.

NOTE: The UEs of the group may be served by multiple SMFs.

- The AF can determine the common DNAI based on candidate DNAIs from SMF(s) and then discover an EAS and notify the UEs about the selected EAS via the application layer.

### 6.17.3 Procedures

#### 6.17.3.1 EAS selection for multiple UE based application layer

This solution focuses on the EAS selection for multiple UE based application layer.



Figure 6.17.3.1-1: Application layer implementation for EAS selection

1. The AF groups the UEs and generates the UE list (UE addresses) of the collection of UEs according to its application logic. The AF sends Nbsf\_management\_Discovery request(s) to the BSF to retrieve the PCF(s) for each UE in the UE list.

2 For each UE, AF sends AF retrieve request to the PCF to query the candidate DNAI(s). The AF request may include the available DNAI list where EAS instances are deployed. The AF request may also include the UE list. The AF may send the AF request to PCF directly, or via the NEF.

3. PCF sends the DNAI retrieve request to SMF.

4. SMF selects the candidate DNAI(s). The SMF may consider the UE location and available DNAI list provided by AF to select the closest available DNAI(s) as candidate DNAI(s). The SMF may also provide the DNAI(s) in a prioritized order.

5. SMF notifies the AF (optionally via NEF) about the candidate DNAI(s) of the UE.

6. After receiving the candidate DNAI(s) of each UE in the list, the AF selects a proper EAS and a common DNAI according to the DNAI(s).

7. AF initiates AF influence on traffic routing procedure as defined in clause 4.3.6.4 of TS 23.502 [9] for each UE in the UE list to route the application traffic to the common DNAI.

8. The AF notifies the UEs about the selected EAS via application layer.

9. The users connect to the same EAS via the common DNAI and start the service.

### 6.17.4 Impacts on services, entities and interfaces

AF/NEF:

- Support of sending new AF retrieve request to query the candidate DNAI(s) of a list of UEs.

PCF:

- Support of handling the AF retrieve request and sending corresponding DNAI retrieve request to SMF.

SMF:

- Support of selecting the candidate DNAI(s) for the UE according to the location of the UE(s) and the DNAI topology. Support of notifying the AF about the candidate DNAI(s) of the UE.

## 6.18 Solution 18 (KI#4): Discovery of the same EAS for collections of UEs

### 6.18.1 Description

In order to realize the discovering the same EAS to collections of UEs, the following conditions should be satisfied:

- The same FQDN in DNS query or a group of FQDNs that can be resolved to a certain EAS IP address by DNS server. The same EAS can be mapped to one FQDNs or a group of FQDNs. Only the collections of the UEs request the same DNS query with these FQDNs, that the DNS server can provide the same EAS IP address.

- The collections of the UEs have the similar UE location. For example, in a stadium, some of the players can access the 5GC by the same gNB or a group of gNBs. According to the UE location information, the 5GC can identify that these UEs should be served by the same EAS.

When the pre-condition above are guaranteed, that for the 5GC side, the following procedures can be used to realize to discover the same EAS for these UEs:

- Use the same DNS server to resolve the FQDN. It needs the 5GC to deliver the same DNS server IP address to these UEs, for example, the EASDF or local DNS server.

- If the same local DNS server is selected, that whether the EAS will be resolved depends on the DNS server's mechanism that is out of scope.

- If the same EASDF is selected, that all these DNS query should be treated with the same way, that applied to the same DNS message handling rules. Whether and how the C-DNS or L-DNS to resolve the same EAS depends on the DNS server's mechanism that is out of scope.

- Directly responds to the DNS query to UE. This way only applies to the EASDF. That if the EASDF identifies that the UE's DNS query should be replied with the same EAS that other UEs use, the EASDF can directly respond with the DNS query without having the DNS related procedure to DNS server.

Table 6.18.1-1: Example of pre-conditions of configured the same EAS

|  |  |
| --- | --- |
| Pre-condition | Actions to configured the same EAS to the UEs which satisfies the pre-condition |
| UE location:   * Cell ID: from XXX1 to XXX9 * DNAI: from XXA to XXE * TAI   FQDN:  FQDN = ABC.com | Action 1: DNS message handling rules   * Local DNS server = 10.1.1.1 * ECS option = X.X.X.X   Action 2: EAS IP address   * 192.168.1.1 |

### 6.18.2 Procedures

#### 6.18.2.1 EASDF-related procedure



Figure 6.18.2.1-1: EASDF related procedure to discover the same EAS

0. The SMF determines the pre-conditions of the UEs that should be configured with the same EAS. The pre-conditions may be a local policy or derived based on PCC rule received from PCF (e.g. AF provision). The pre-conditions are defined below:

- The same FQDN in DNS query or range of FQDNs that can be resolved to a certain EAS IP address by DNS server. The same EAS can be mapped to one FQDNs or a group of FQDNs. Only the collections of the UEs request the same DNS query with these FQDNs, that the DNS server can provide the same EAS IP address.

- The collections of the UEs have the similar UE location, for example, the same UE location or the UE location in the optional scope. According to the UE location information, the 5GC can identify that these UEs should be served by the same EAS. The UE location includes: Cell ID, range of Cell ID, TAI lists, DNAI, range of DNAI, gNB ID, range of gNB ID, DNN, S-NSSAI.

Editor's note: It is FFS how the AF provides the pre-conditions to 5GC and how the SMF receives the pre-conditions.

0. The 5GC can deliver the same DNS server IP address to these UEs that satisfies the pre-conditions, for example, the EASDF.

1. The UE sends a DNS Query message to the EASDF.

2. The same procedure as step 8 defined in figure 6.2.3.2.2-1 of TS 23.548 [3]. The EASDF provides the FQDN in DNS query to SMF.

3. The same procedure as step 9 defined in figure 6.2.3.2.2-1 of TS 23.548 [3].

4. The SMF recovers the UE location from AMF by Namf\_EventExposure\_Subscribe (event ID = UE location). The UE location information is used by SMF to identify whether this UE should be configured with the same EAS.

5. The AMF responds to SMF.

6. The AMF notifies the SMF with the UE location information, including: TAI, Cell ID and etc.

7. SMF determines whether the UE is satisfied with the pre-conditions, according to UE location information and FQDN. The SMF can also recover the DNAI, PSA ID, DNN, S-NSSAI of the UE or the UE's PDU sessions. If the UE location information is in the scope of UE location that defined in pre-conditions, and the FQDN is also in the scope of pre-defined scope, the SMF determines:

- Use the same DNS server to resolve the FQDN. The DNS query should be treated with the same way, that applied to the same DNS message handling rules, e.g. the same DNS server address or information of EDNS Client Subnet option is indicated in the Forwarding Action.

- Directly responds to the DNS query to UE. This way only applies to the EASDF. That if the SMF identifies that the UE's DNS query should be replied with the same EAS that other UEs use, the SMF can set the DNS message handling rules to EASDF to directly respond with the DNS query without having the DNS related procedure to DNS server, e.g. add a new action for Forwarding Action: forward the DNS response with specific EAS IP address to UE.

Editor's note: How to solve multiple SMF instances is FFS.

8. The SMF updates the DNS message handling rule to guarantee the same EAS discovery for this UE. The SMF invokes Neasdf\_DNSContext\_Update Request (DNS message handling rules) to EASDF, and the DNS message handling rules are the same as pre-defined of other UEs.

For Option A, the DNS handling rule includes the same corresponding IP address to be used to build the EDNS Client Subnet option. For Option B, the DNS handling rule includes corresponding Local DNS Server IP address which is also the same as other UEs.

9-15. The same procedure from step 11 to step 19 as defined in figure 6.2.3.2.2-1 of TS 23.548 [3].

According to the enhancement from SMF, this UE can receive the same EAS IP address as other UEs which satisfies the pre-condition.

#### 6.18.2.2 Direct DNS response to UE



Figure 6.18.2.2-1: Direct DNS response to UE

0-6. The same procedure as indicated in Figure 6.18.2.1-1 from step 0 to step 6.

7. SMF determines whether the UE is satisfied with the pre-conditions, according to UE location information and FQDN. The SMF can also recover the DNAI, PSA ID, DNN, S-NSSAI of the UE or the UE's PDU sessions. If the UE location information in the scope of pre-defined UE location, and the FQDN is also in the scope of pre-defined scope, the SMF determines the discover the same EAS to this UE as other UEs in group. SMF decides to have a direct DNS response to the UE.

8-9. The same procedure as indicated in Figure 6.18.2.1-1 from step 8 to step 9. But SMF invokes Neasdf\_DNSContext\_Update Request (DNS message handling rules) to EASDF to directly response to the UE DNS query with the same EAS IP address that other UEs are served.

10. The EASDF sends the DNS Response(s) to the UE with the same EAS IP address that other UEs are served.

#### 6.18.2.3 EAS Discovery Procedure with Local DNS Server/Resolver



Figure 6.18.2.3-1: EAS Discovery Procedure with Local DNS Server/Resolver

1. The UE sends a PDU session establishment request to SMF.

2. SMF determines whether the UE is satisfied with the pre-conditions, according to UE location information and FQDN. The SMF can also recover the DNAI, PSA ID, DNN, S-NSSAI of the UE or the UE's PDU sessions. If the UE location information in the scope of pre-defined UE location, and the FQDN is also in the scope of pre-defined scope, the SMF determines the discover the same EAS to this UE as other UEs in group. The SMF determines the DNAI and selects corresponding PSA UPF serves the DNAI, and determines DNS server (s) to ensure a dynamic group uses the same EAS and/or same DNAI.

3. Optionally, the SMF selects and inserts UL-CL/BP. The SMF configures the UL-CL/BP for DNS Query handling.

4. The SMF includes the IP address of Local DNS Server in PDU Session Establishment Accept message.

5. The EAS information (e.g. EAS IP address) is resolved by Local DNS Server and sent the UE.

### 6.18.3 Impacts on services, entities and interfaces

Editor's note: This clause lists impacts to services and interfaces.

SMF:

- determines the pre-conditions of whether the collections of the UE should be configured with the same EAS.

- determines whether the UE is satisfied with the pre-conditions, according to UE location information and FQDN. The SMF can also recover the DNAI, PSA ID, DNN, S-NSSAI of the UE or the UE's PDU sessions.

- decides to have a direct DNS response to the UE or configure the same DNS message handling rule to this UE DNS query, according to the configurations in the pre-conditions.

EASDF:

- directly responds to the UE DNS query with the EAS IP address that other UEs are served.

## 6.19 Solution 19 (KI#4): Influencing UPF and EAS (re)location for collections of UEs

### 6.19.1 Introduction

This solution aims to address the technical requirements related to key issue #4. In particular, it proposes for certain Edge Application use case e.g. all users playing a certain online game and registered to a particular EAS, or all UEs in a platoon, how these UEs collectively for an ad hoc and dynamic group, how to identify such group, how to handle coordination of the UPF(s) and EAS (re)location for the UEs belonging to the same group.

### 6.19.2 Functional Description

The following are the main principles of the solution:

- Application Function may create an ad hoc group of collection of UEs based on its own criteria, for example: all Users served by the same EAS that hosts an online gaming application.

- Application Function creates an ad hoc group of collection of UEs, and provides to 5GC, either directly of via NEF, the necessary group specific information, together with (external) group ID.

- NEF performs AF request authorization and provides necessary mappings, and configures UDM with ad hoc group information.

- Mapping based on: User ID (e.g. GPSI), UE ID (if provided), DNN, S-NSSAI;

- NEF maps external group ID into 5GC internal group and stores ad hoc group information in UDM indicating Group Type e.g. to differentiate between ad hoc dynamic Group vs Subscribed static group.

### 6.19.3 Procedure



Figure 6.19.3-1: AF Provisioning Ad hoc Group Information

1. Application Function configures an ad hoc dynamic group of a collection of UEs. These collection of UEs are based on common use case or application etc. e.g. all users registered on a particular gaming server (EAS) or UEs in a platoon. AF assigns an (external) Group ID to this collection of UEs. AF provisions this group information to 5GC either directly or via NEF and provides required details including: (external) group ID, Group Type (this is to differentiate with static groups based on user subscriptions), collection of UEs IDs forming the group or group property such as all users served by the same EAS.

Alternatively, AF may use new API e.g. Nnef\_GroupParameterProvision\_Create/update/delete to provision these information.

Editor's note: Use of group type is FFS.

2. NEF after authorizing the AF request, creates or updates these information in UDM using. It translates AF provides information into corresponding internal information such as external Group ID into an internal group ID. It then stores (or updates) these in UDM.

Editor's note: How to ensure uniqueness of internal group ID is FFS.

3-4. UDM uses Nudr\_DM\_Query/Update to UDR.

5-6. AF receives the Response message to its request in step 1.

7. Consumer Network Function e.g. SMF may subscribe and get notified on any changes to information related to the ad hoc group.

Editor's note: Details on how the group information is used is FFS.

## 6.20 Solution 20 (KI#5): Global EASDF

### 6.20.1 Description

This solution addresses KI#5: GSMA OPG impacts and improvements for EHE operated by separate party.

In this solution the UE uses a predefined EASDF that is global between operators. For example, GSMA could host this with the URL:

http://easdf.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org

Each operator that wants to support separate party's EHE into their network will then add these EHEs entry points into the DNS entry owned by themselves in the Global EASDF. There are two alternatives to do this, either they add the EAS entry point directly into the Global EASDF. The other alternative is to add the entry point to another EASDF into the Global EASDF. With the second alternative then the UE shall now use that received IP address as EASDF to discover the appropriate EAS according to existing procedures. Since the Global EASDF is based on standard DNS infrastructure that allows an operator to specify which order the UE shall select EAS/EASDF in the different separate party's operated EHEs. If we allow both alternatives, then it is up to the each operator to decide which method they want to use as long as we specify that the UE shall support both methods. The second alternative with discover another EASDF allows more static configuration in the Global EASDF.

### 6.20.2 Procedures

#### 6.20.2.1 Procedure for Global EASDF



Figure 6.20.2-1: Procedure for Global EASDF

0. Pre-requisites: HPLMN has configured the Global EASDF with appropriate entries for all separate party's EASDF and/or their EAS they want to enable in their network.

1. Existing PDU Session establishment procedure according to TS 23.548 [3] clause 6.2.3.2.2 step 1.

2. For Option A, the UE performs a DNS query to the Global EASDF. Since this is a public FQDN to the Global EASDF, the UE may use any locally configured DNS Server that in turn will use next DNS server in the DNS hierarchy until it goes to the Global EASDF.

Editor's note: The root FQDN for the global EASDF and the structure of VPLMN/HPLMN's identity in the query is FFS and needs to be specified.

NOTE 1: The unique identifier to use for querying another EASDF will be specified during the normative phase.

3. The Global EASDF responds with the IP address of the EASDF that the UE should use in next step.

4. The UE performs EAS Discovery, as specified in TS 23.548 [3] clause 6.2.3.2.2 step 7 except that it uses the IP address received in step 3 as DNS server for the DNS query instead of the one received during PDU Session establishment procedure.

5. EASDF sends the DNS Response to the UE, as specified in TS 23.548 [3] clause 6.2.3.2.2 step 19.

6. For Option B, The UE performs EAS Discovery, as specified in TS 23.548 [3] clause 6.2.3.2.2 step 7 and uses the IP address of the Global EASDF instead of the one received during PDU Session establishment procedure.

7. EASDF sends the DNS Response to the UE, as specified in TS 23.548 [3] clause 6.2.3.2.2 step 19.

8. The UE application starts to utilize the provided EAS.

### 6.20.3 Impacts on services, entities and interfaces

* Editor's note: This clause is FFS.

## 6.21 Solution 21 (KI#5): EAS Deployment information differentiated by PLMN ID

### 6.21.1 Introduction

This solution proposes an EAS discovery method for the scenario described in clause 2.1.5 of GSMA OPG.02 [5] that an OP deploys applications provided by Application Providers on another OP. This solution focuses on the scenario that the OPs are different PLMNs. In this case, the problem is to ensure the EAS deployed by HPLMN in VPLMN's EHE should only be discovered and accessed by the UE of the HPLMN roaming to the VPLMN and using LBO PDU Session. This solution introduces how to handle the DNS requests to ensure an EAS deployed by a PLMN can only be accessed by the UE of same PLMN.

This solution corresponds to KI#5.

### 6.21.2 Functional Description

This solution is based on the following principles:

- The EAS Deployment information provided by AF contains the EAS provider's ID (i.e. PLMN ID) to differentiate the EAS deployment information of different PLMNs. Different EAS providers (PLMNs) may use different DNS servers (e.g. C-DNS server or Local DNS server) to discover the EAS deployed by the PLMNs.

- During the PDU Session Establishment procedure, the SMF selects the proper PLMN's EAS Deployment Information based on UE's HPLMN ID and then generates corresponding DNS message handling rule to handle DNS messages related to the roaming UE.

### 6.21.3 Procedures

The EAS Deployment Information Provision procedure reuses the procedure defined in clause 6.2.3.4.2 of TS 23.548 [3]. The enhancement is that the EAS Deployment information provided by AF in step 1 includes PLMN ID to differentiate EAS deployment information of different PLMNs. EAS deployment information of different PLMNs may contain different DNS servers (e.g. C-DNS server or Local DNS server) or different ECS options.

The EAS Deployment Information Management in the SMF reuses the procedure defined in clause 6.2.3.4.3 of TS 23.548 [3].

The EAS discovery procedure with EASDF defined in clause 6.2.3.2.2 of TS 23.548 [3] is reused to discover the EAS(s) deployed by different providers. The enhancement is that the during the PDU Session Establishment procedure, the SMF selects the proper provider based on HPLMN ID. The SMF queries the UDR via NEF with the HPLMN ID to get the EAS Deployment information and configures the EASDF with DNS message handling rules to handle DNS messages related to the UE. Then the following steps in clause 6.2.3.2.2 of TS 23.548 [3] are reused for DNS queries and UL-CL/BP insertion.

### 6.21.4 Impacts on services, entities and interfaces

AF:

- support of sending EAS Deployment information with PLMN ID to differentiate the EAS deployment information of different providers.

SMF:

- support of selecting proper provider based on roaming UE's HPLMN ID and configures the EASDF according to the EAS Deployment information of the HPLMN.

## 6.22 Solution 22 (KI#5): EAS discovery for federated OPs

### 6.22.1 Introduction

This solution addresses Key Issue #5 and allows the discovery of an Edge Application Server (EAS) within a federation of Operator Platforms. It is assumed that the EAS is hosted by a different PLMN than the PLMN that is serving the UE.

### 6.22.2 Functional description

#### 6.22.2.0 Option 0: SMF configuration

This solution is based on the Rel-17 EAS based discovery procedures with the assumption that the SMFs of each PLMN supporting the OP federation needs to be configured with the DNAI values associated to the EAS' hosted by the other OPs of the federation. More in details:

- the SMF needs to know the EAS deployment information of the EAS running on other PLMN's edge infrastructure e.g., IP address range(s)/FQDN(s).

For example, if the EAS is running in MNO 2's PLMN#2, when the EAS discovery is triggered the EASDF in MNO 1's PLMN#1 will receive the DNS response from the DNS server knowing the EAS' address and will forward the EAS' address to the SMF in PLMN#1.

- At this point, after the SMF gets the IP address of EAS running in PLMN#2, in order to know that the EAS is instantiated in PLMN#2's edge infrastructure, it is required that SMF knows the mapping between the PLMN ID of the PLMN hosting the EAS and the corresponding IP address received as a result of DNS query so that the SMF can steer user plane path toward the PLMN#2's domain. This may require an update of the SMF each time an EAS is added or removed.

Editor's note: How SMF determines information of ECS option for the DNS query is FFS.

Editor's note: How to support the low latency requirement for edge computing when the traffic routing from MNO1's UPF to MNO2's DN is FFS.

#### 6.22.2.1 Option 1: Shared EASDF

This option is based on the concept of shared EAS Discovery Function (shared EASDF), which is a new network entity shared among multiple operators and used to support the discovery of EAS for federated edge services.



Figure 6.22.2.1-1: Architecture with deployed Shared EASDF

The Shared EASDF is a new network entity deployed in the core network and shared among the PLMNs of the MNOs that support a federation of Operator Platforms (OPs). The shared EASDF is hosted by a PLMN of the federation. The PLMN hosting the shared EASDF is the anchor PLMN. The communication between other PLMNs and the shared EASDF takes place via the serving EASDF (sEASDF) and the serving SMF (sSMF), that is via the EASDF and the SMF of the PLMN serving the UE.

Editor's note: Whether the shared EASDF is feasible for network operator is FFS. Checking with GSMA may be needed in the future.

Editor's note: How sSMF creates DNS context on shared EASDF is FFS.

The shared EASDF stores EAS deployment information such as EAS address hosted by other PLMNs within the federation. An operator in the federation needs to update its EAS information in the shared EASDF any time a change is applied (e.g., an EAS is added/modified/removed, or an MNO joins or leaves a federation).

Editor's note: How to support the low latency requirement for edge computing when the traffic routing from MNO1's UPF to MNO2's DN is FFS.

#### 6.22.2.2 Option 2: Per-PLMN EASDFs

This solution option is based on the communication between the EASDFs of the different PLMNs of the MNOs that support a federation of OPs. The EASDF of a PLMN manages information for EAS' that are hosted by the Edge Data Network of that PLMN, and the EASDF of a PLMN can interact with other PLMN’s EASDFs to support a federation of operator platforms.



Figure 6.22.2.2-1: Architecture with per-PLMN EASDF

In the figure above:

- serving EASDF (sEASDF) and the serving SMF (sSMF) are, respectively, the EASDF and the SMF of the PLMN of the federation that is currently serving the UE;

- partner EASDF (pEASDF) is the EASDF of the partner PLMN in the federation which hosts the Edge Application Server whose service is desired.

Editor's note: How to support the low latency requirement for edge computing when the traffic routing from MNO1's UPF to MNO2's DN is FFS.

Editor's note: How sSMF determine the proper pEASDF is FFS.

The EAS discovery is based on the existing EAS discovery procedures described in TS 23.548 [3], with the following changes:

- provisioning of EAS deployment information to 5GS

- For each of its EASs, the application service provider (via the AF) provides each PLMN of the federation with the EAS deployment information with PLMN ID, DNAI, and (list of) FQDNs necessary to discover the EAS within the federation. Such information is stored in the UDR following the EAS Deployment Information Provision from AF via NEF procedure (TS 23.548 [3], clause 6.2.3.4.2).

- The SMF retrieves the EAS deployment information from the UDR (TS 23.548 [3], clause 6.2.3.4.3), and provides the following pieces of information to the EASDF (TS 23.548 [3], clause 6.2.3.4.4):

a) FQDN filter: the list of filters regarding FQDN in the DNS query from the UE;

b) DNS server address filter: the list of filters regarding DNS server address in the DNS query from the UE;

c) PLMN ID associated with the FQDN filter or DNS server address;

d) Action: DNS query forwarding to the target pEASDF, reporting to the SMF.

- EAS discovery

- At EAS discovery (TS 23.548 [3], clause 6.2.3.2.2), the sEASDF determines the target pEASDF associated with the PLMN ID, if the received DNS query (from the UE) meets the following conditions:

- the FQDN in the DNS query matches with the configured FQDN filter associated with the DNAI/PLMN ID;

- the DNS server address in the query matches with the configured DNS address filter with the DNAI/PLMN ID.

- Based on the indication by the sSMF, the sEASDF forwards the query to target pEASDF.

- Target pEASDF replies with the specific DNAI/PLMN ID result.

- The result is reported to the sSMF.

### 6.22.3 Procedures

#### 6.22.3.0 Option 0: SMF configuration

This option re-uses the EAS discovery procedure defined in TS 23.548 [3], clause 6.2.3.2.2.

#### 6.22.3.1 Option 1: Shared EASDF



Figure 6.22.3.1-1: Modified EAS discovery (TS 23.548 [3] clause 6.2.3.2.2) for Option 1 and Option 2

The procedure is based on the EAS discovery procedure defined in TS 23.548 [3], clause 6.2.3.2.2, with the following changes:

- new step 9a: based on the DNS message report sent by the sEASDF in step 8/9, the SMF selects the shared EASDF.

- new step 9b/c: the sSMF creates the DNS context in the shared EASDF.

Editor's note: How sSMF creates DNS context on shared EASDF without having the UE's public IP address is FFS.

- step 10/11: the sSMF instructs the sEASDF to forward the DNS query to the shared EASDF; The sSMF provides to the serving EASDF the FQDN filter (e.g., FQDN ranges) to be reported. The FQDN filter indicates that the shared EASDF needs to be contacted to resolve the DNS query.

- new step 11a: the sEASDF forwards the DNS query to the shared EASDF.

- new step 13a: the shared EASDF resolves the DNS query and sends the DNS reply to the sEASDF.

NOTE: Alternatively to steps 11a/13a, the DNS query can be forwarded by the sEASDF to the shared EASDF via the SMF.

#### 6.22.3.2 Option 2: Per-PLMN EASDFs



Figure 6.22.3.2-1: Modified EAS discovery (TS 23.548 [3] clause 6.2.3.2.2) for Option 2

The procedure is based on the EAS discovery procedure defined in TS 23.548 [3], clause 6.2.3.2.2, with the following changes:

- new step 9a: based on the DNS message report sent by the sEASDF in step 8/9, the SMF selects the pEASDF.

- step 10/11: the sSMF instructs the sEASDF to forward the DNS query to the partner EASDF. The sSMF provides to the serving EASDF the FQDN filter (e.g., FQDN ranges) to be reported. The FQDN filter indicates that the partner EASDF needs to be contacted to resolve the DNS query.

- new step 11a: the sEASDF forwards the DNS query to the pEASDF.

- new step 13a: the pEASDF resolves the DNS query and sends the DNS reply to the sEASDF.

### 6.22.4 Impact on existing entities and interfaces

#### 6.22.4.0 Option 0: SMF configuration

SMF

- needs to know EAS deployment information (IP address range(s)/FQDN(s)) of each EAS running in the PLMNs of the operators supporting the OP federation;

- needs to be configured with mapping between EAS deployment information and PLMN ID. If EAS' are added or removed, the configuration information needs to be updated.

#### 6.22.4.1 Option 2: Shared EASDF

EASDF

- requires capability to communicate with shared-EASDF forward DNS query to and receive DNS response.

Shared-EASDF

- needs to be configured with IP range/FQDN of list of all EAS' running in PLMNs of operators participating in the OP federation.

SMF

- needs to be configured with shared-EASDF address.

#### 6.22.4.2 Option 3: Per-PLMN EASDFs

EASDF

- requires capability to communicate with EASDFs of another PLMN to forward DNS query to and receive DNS response.

SMF

- needs to be configured per-PLMN EASDF addresses.

## 6.23 Solution 23 (KI#5): Improvements for EHE operated by separate party

### 6.23.1 Introduction

This solution aims to address the technical requirements related to key issue #5. In particular, it provides solutions to, among others, how the 5GS facilitates edge relocation between an EAS deployed by a source EHE provider to another EHE deployed by a target EHE provider, even in scenarios when EHEs are operated by different service providers. This solution has following architecture assumptions:

- the architecture for Edge computing specified in Rel-17 is used as basis;

- the Edge Hosting Environment (EHE) can be under the control of the serving network operator or a 3rd party;

- the target and source AFs communicate with the SMF/NEF of a single PLMN;

- interconnectivity between EHEs of different operators is available, thus those deployments that does not support this would need further enhancements.

### 6.23.2 Functional Description

The following are the main principles of the solution:

- In case of multiple and/or different EHE providers, it is possible that there is no cooperation and agreements among different Edge domains, thus implying that source EHE is unaware of other/target EHE specific deployment details. In such cases, specific to Edge relocation scenarios, source AF is unaware of suitable target AF and/or target EAS. Thus, source AF is not always able to assist suitable AF and EAS relocation as per clause 4.3 of TS 23.548 [3].

- EHE providers likely have some kind of agreements with the 5GS, thus enabling 5GS to know respective EHE domain deployment details and corresponding AF, service area, TAI, application supported, etc.

### 6.23.3 Solution Details

- The selection of the target EHE, and corresponding AF/EAS is triggered due to multiple reasons, for example UE mobility, EAS overload, etc.

- SMF is able to know AF in the target EHE. This may be possible with either NRF or NEF maintaining AF list indicating for each AF one or more of these parameters: EHE domain it supports, service area, application supported, etc. This list could be based on e.g. pre-configuration and SLA with the EHE domain. Accordingly, SMF selects suitable target AF based on e.g. UE current location.

The figure 6.23.3-1 below provides call flow where AF and EAS relocations are performed during early and late notifications.



Figure 6.23.3-1: Procedure to support EAS and/or AF relocation between EHE from different provider

0. SMF decides to relocate AF and/or EAS based on different criteria such as UE new location, Anchor UPF relocation and so on.

1. As part of early notification, SMF provides target AF ID i.e. ID of the AF responsible for the new/target EC Domain corresponding to UE new location. SMF also provides source AF transaction ID. These are provided in the Nsmf\_eventExposure\_Notify and/or Nnef\_TrafficInfluence\_Notify.

2. Source AF on receipt of message in step 1 above, initiates AF context exchange and provides to target AF these information: source EAS ID, Service ID, etc.

3. Target AF responds by sending Relocation Reply with target EAS ID and Service ID.

4. EAS is relocated and if required application layer context are also exchanged.

NOTE: This may require some application layer exchange between source and target EAS/AFs. How these information are exchanged are outside the scope of SA2.

5. Source AF Acknowledges to SMF by sending Nnef\_EventExposure\_AppRelocationInfo and Nsmf\_EventExposure\_AppRelocation\_Info messages.

6. After confirmation from AF and considering information provided by AF, SMF may re-configure user plane path, etc. as required.

7. SMF sends Late notification to target AF in Nsmf\_eventExposure\_Notify and/or Nnef\_TrafficInfluence\_Notify.

8. Target AF sends acknowledgement to received late notification from SMF. New traffic descriptors are provided to replace the old ones which were provided earlier by the source AF.

9. Target AF sends Relocation Complete to the source AF so that the later deletes (relocated) EAS contexts.

# 7 Evaluation

Editor's note: This clause will capture the evaluations related to the solutions per KI.

# 8 Conclusions

Editor's note: This clause will capture the conclusions of the study.

Annex A:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-02 | SA2#149e | S2-2201771 |  |  |  | TR23.700-48 skeleton | 0.0.0 |
| 2022-02 | SA2#149e |  |  |  |  | Implementation of following documents approved in SA2#149e: S2-2200764, S2-2201772, S2-2201773, S2-2201774, S2-2201777, S2-2201778, S2-2201779, S2-2201775, S2-2201776 | 0.1.0 |
| 2022-04 | SA2#150e |  |  |  |  | Implementation of following documents approved in SA2#150e: S2-2203480, S2-2203481, S2-2203482, S2-2203483, S2-2203484, S2-2203603, S2-2203604, S2-2203485, S2-2203486, S2-2203605, S2-2203487, S2-2203488, S2-2203489, S2-2203490, S2-2202078, S2-2203491, S2-2203492, S2-2203493, S2-2202405, S2-2203494, S2-2203495, S2-2203496, S2-2203497, S2-2203498, S2-2203499, S2-2203500 | 0.2.0 |