ETSI TS 123 548 V18.6.0 (2024-07)

5G;
5G System Enhancements for Edge Computing;
Stage 2
(3GPP TS 23.548 version 18.6.0 Release 18)

Reference
RTS/TSGS-0223548vi60

Keywords
5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification 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.

1 Scope

The present document defines the Stage 2 specifications for enhancements of 5G System to support Edge Computing.

2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

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

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

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

[4] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System; Stage 2".

[5] 3GPP TS 23.558: "Architecture for enabling Edge Applications (EA)".

[6] IETF RFC 7871: "Client Subnet in DNS Queries".

[7] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[8] 3GPP TS 24.526: "User Equipment (UE) policies for 5G System (5GS); Stage 3".

[9] 3GPP TS 29.500: "Technical Realization of Service Based Architecture; Stage 3".

[10] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[11] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[12] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

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] 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] and TS 23.501 [2].

Central DNS resolver/server: A DNS resolver/server centrally deployed by the 5GC operator or 3rd party and is responsible for resolving the UE DNS Queries into suitable Edge Application Server (EAS) IP address(es).

Edge Application Server: An Application Server resident in the Edge Hosting Environment.

Edge Hosting Environment: An environment providing support required for Edge Application Server's execution.

Local part of DN: The set of network entities of a DN that are deployed locally. The local access to the DN provides access to the local part of DN.

Local DNS resolver/server: A DNS resolver/server that may be locally deployed by 5GC operator or 3rd parties within the Local DN, and is responsible for resolving UE DNS Queries into suitable EAS IP address(es) within the local DN. The L-DNS resolvers/servers may or may not have connectivity with C-DNS depending on the deployment.

3.2 Abbreviations

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

C-DNS	Central DNS
C-NEF	Central NEF
C-PSA UPF	Central PSA UPF
EAS	Edge Application Server
EASDF	Edge Application Server Discovery Function
ECS	Edge Configuration Server
EDC	Edge DNS Client
EEC	Edge Enabler Client
EES	Edge Enabler Server
EHE	Edge Hosting Environment
L-DN	Local part of DN
L-DNS	Local DNS
L-NEF	Local NEF
L-PSA UPF	Local PSA UPF
HR-SBO	Home Routed Session BreakOut

4 Reference Architecture and Connectivity Models

4.1 General

Edge Computing enables operator and 3rd party services to be hosted close to the UE's access point of attachment, so as to achieve an efficient service delivery through the reduced end-to-end latency and load on the transport network.

5GS supports Edge Hosting Environment (EHE) deployed in the DN beyond the PSA UPF. An EHE may be under the control of either the operator or 3rd parties.

The Edge Computing features defined in this specification are applicable to PLMN(s) and to SNPN(s).

The Local part of the DN in which EHE is deployed may have user plane connectivity with both a centrally deployed PSA and locally deployed PSA of same DNN. Edge Computing enablers as described in clause 5.13 of TS 23.501 [2], e.g. local routing and traffic steering, session and service continuity, AF influenced traffic routing, are leveraged in this specification.

Edge Computing in the serving network (e.g. for Local Break Out roaming scenario in case of PLMN access) is supported, but for AF guidance to PCF determination of URSP rules, the Serving network (e.g. VPLMN or serving SNPN) has no control on URSP, so cannot influence UE in selecting a specific Edge Computing related DNN and S-NSSAI.

4.2 Reference Architecture for Supporting Edge Computing

The reference architectures for supporting Edge Computing are based on the reference architectures specified in clause 4.2 of TS 23.501 [2]. The following reference architectures for non-roaming, LBO roaming and HR with Session Breakout (HR-SBO) roaming scenarios further depict the relationship between the 5GS and a DN where Edge Application Servers (EASs) are deployed in an EHE.

Figure 4.2-1 depicts 5GS architecture for non-roaming scenario supporting Edge Computing with UL CL/BP.

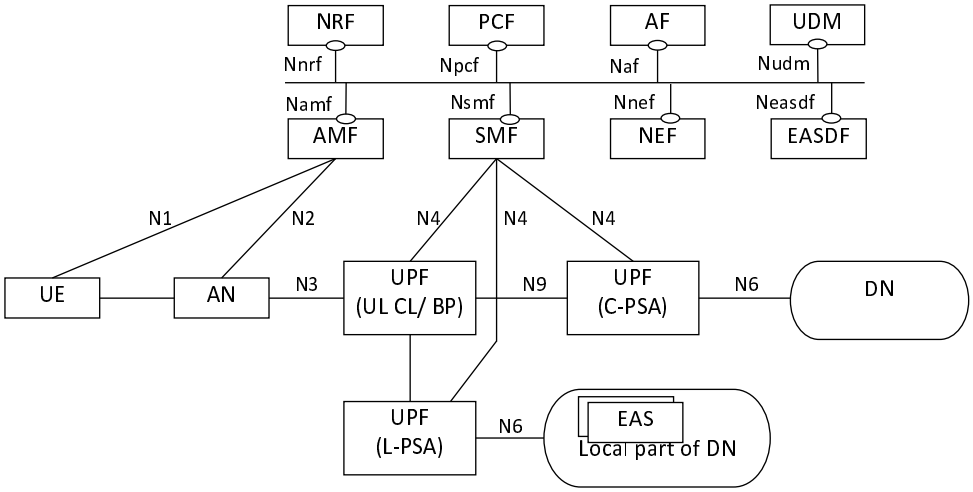

Figure 4.2-1: 5GS providing access to EAS with UL CL/BP for non-roaming scenario

Figure 4.2-2 depicts 5GS architecture for non-roaming scenario supporting Edge Computing without UL CL/BP.

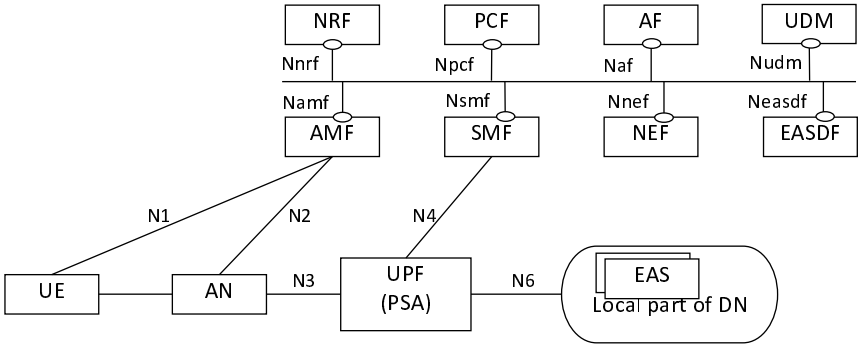

Figure 4.2-2: 5GS providing access to EAS without UL CL/BP for non-roaming scenario

Figure 4.2-3 depicts 5GS architecture for LBO roaming scenario supporting Edge Computing with UL CL/BP.

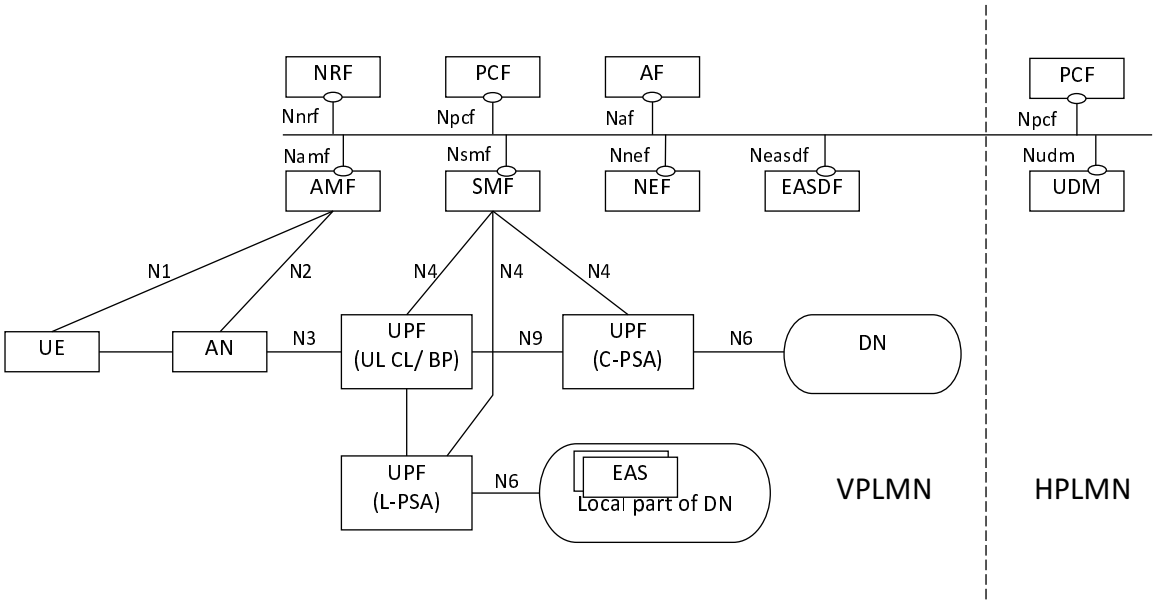

Figure 4.2-3: 5GS providing access to EAS with UL CL/BP for LBO roaming scenario

Figure 4.2-4 depicts 5GS architecture for LBO roaming scenario supporting Edge Computing without UL CL/BP.

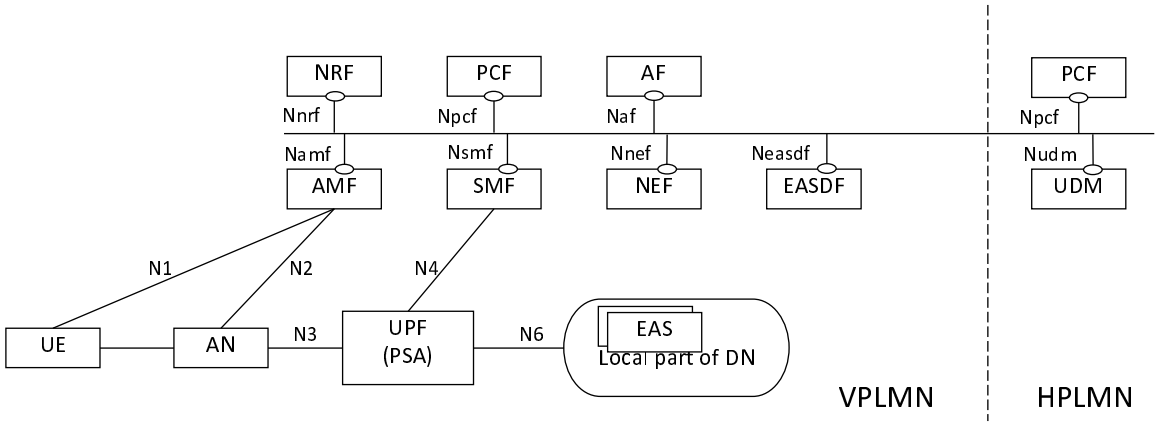

Figure 4.2-4: 5GS providing access to EAS without UL CL/BP for LBO roaming scenario

Figure 4.2-5 depicts 5GS architecture for HR-SBO roaming scenario supporting Edge Computing with UL CL/BP.

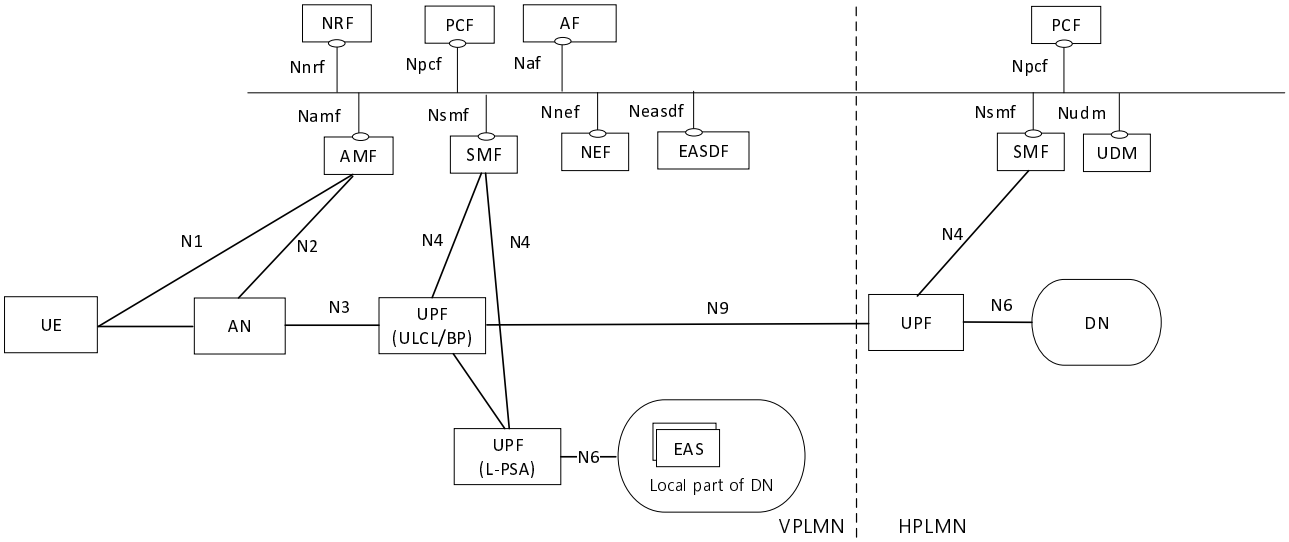

Figure 4.2-5: 5GS providing access to EAS with UL CL/BP for HR-SBO roaming scenario

NOTE 1: Only some of the 5GS NFs are shown in the above reference architecture figures. In the above figures, the split between the UPF acting as UL CL/BP and the UPF acting as local PSA is illustrative.

NOTE 2: Only the control plane of EASDF is depicted in the figure, the user plane between the EASDF and the UPF (i.e. over which the DNS messages are exchanged) is part of N6. Additionally, the EADSF may have direct connectivity with the local parts of one or more Data Networks.

NOTE 3: For the HR-SBO roaming scenario, there can be other UPF(s) located in VPLMN between the UPF acting UL CL/BP and the UPF acting as remote PSA in HPLMN.

4.3 Connectivity Models

5GC supports the following connectivity models to enable Edge Computing:

- Distributed Anchor Point: For a PDU Session, the PSA UPF is in a local site, i.e. close to the UE location. The PSA UPF may be changed e.g. due to UE mobility and using SSC mode 2 or 3.

- Session Breakout: A PDU Session has a PSA UPF in a central site (C-PSA UPF) and one or more PSA UPF in the local site (L-PSA UPF). The C-PSA UPF provides the IP Anchor Point when UL Classifier is used. The

Edge Computing application traffic is selectively diverted to the L-PSA UPF using UL Classifier or multi-homing Branching Point mechanisms. The L-PSA UPF may be changed due to e.g. UE mobility.

- Multiple PDU Sessions: Edge Computing applications use PDU Session(s) with a PSA UPF(s) in local site(s). The rest of applications use PDU Session(s) with PSA UPF(s) in the central site(s). Any PSA UPF may be changed due to e.g. UE mobility and using SSC mode 3 with multiple PDU Sessions.

URSP rules, for steering the mapping between UE applications and PDU Sessions, can be used for any connectivity model and they are required for the Multiple PDU Sessions model.

These three connectivity models are illustrated in Figure 4.3-1:

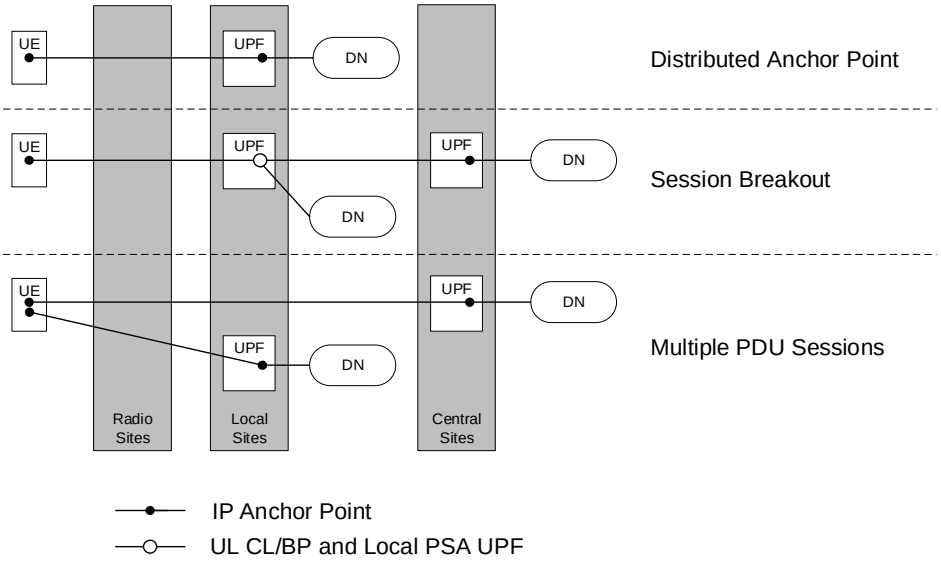

Figure 4.3-1: 5GC Connectivity Models for Edge Computing

5 Functional Description for Supporting Edge Computing

5.1 EASDF

5.1.1 Functional Description

The Edge Application Server Discovery Function (EASDF) includes one or more of the following functionalities:

- Registering to NRF for EASDF discovery and selection.
- Providing DNS security information to SMF.
- Handling the DNS messages according to the instruction from the SMF, including:
  - Receiving DNS message handling rules and/or BaselineDNSPattern from the SMF.
  - Exchanging DNS messages from the UE.
  - Forwarding DNS messages to C-DNS or L-DNS for DNS Query.
  - Adding EDNS Client Subnet (ECS) option into DNS Query for an FQDN.
  - Reporting to the SMF the information related to the received DNS messages.
  - Buffering/Discarding DNS messages from the UE or DNS Server.

- Providing a DNS response with a specific IP address to a DNS query.
- Constructing and sending DNS Query messages with specific FQDN and ECS option.

- Terminates the DNS security, if used.

The EASDF has direct user plane connectivity (i.e. without any NAT) with the PSA UPF over N6 for the transmission of DNS signalling exchanged with the UE. The deployment of a NAT between EASDF and PSA UPF is not supported.

Multiple EASDF instances may be deployed within a PLMN.

The interactions between 5GC NF(s) and the EASDF take place within a PLMN.

5.1.2 EASDF Discovery and Selection

The EASDF discovery and selection is defined in clause 6.3 in TS 23.501 [2].

5.2 Edge DNS Client (EDC) Functionality

5.2.1 Functional Description

The Edge DNS Client (EDC) functionality is a 3GPP functionality in the UE that ensures that DNS requests from applications are sent to the DNS Server's (e.g. EASDF/DNS resolver) IP address received from the SMF in the ePCO. The EDC functionality in the UE is a UE capability that ensures the usage of the EAS discovery and re-discovery functionalities defined in clause 6.2.

NOTE 1: A UE without EDC functionality can use the EAS (re-)discovery functionalities provided by EASDF, but the usage of the EASDF cannot be ensured since it may use a different DNS server from the DNS server provided by the operator.

Figure 5.2-1 depicts the Edge DNS Client (EDC) functionality in the UE.

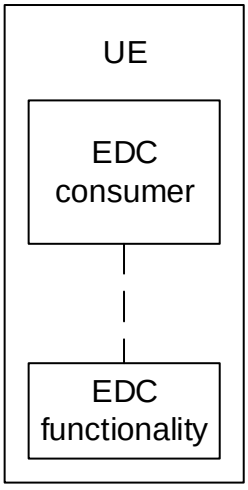

Figure 5.2-1: EDC functionality in the UE

NOTE 2: Whether EDC functionality is provided to the consumer directly or via/by the UE's operating system is implementation specific. The APIs between EDC consumer and EDC functionality are out of scope of 3GPP.

A UE that hosts the EDC functionality indicates its capability in the PCO during the PDU Session Establishment and the PDU Session Modification procedures. The EDC functionality includes the following functionalities:

- Configures the DNS Client with the DNS Server's configuration (IP address and, conditionally, DNS security information of the EASDF/DNS resolver; see TS 24.501 [11] and TS 33.501 [12]) received from the SMF in the ePCO according to TS 23.501 [2] clause 5.6.10.1.

- DNS Client:
  - Provides the capability to the consumer in the UE to resolve FQDN using DNS Queries towards the DNS Server (e.g., EASDF/DNS resolver) indicated by the SMF.
  - Sends DNS Queries towards the DNS Server indicated by the SMF via the related PDU session.
  - Forwards EAS IP addresses and other relevant information included in the DNS responses received from the DNS Server to the consumer in the UE.
- Provision of DNS settings (Optional):
  - Provides to the consumer in the UE the configuration of the DNS Server (IP address and, conditionally, DNS security information of the EASDF/DNS resolver; see TS 24.501 [11] and TS 33.501 [12]) received from the SMF. The consumer in the UE can explicitly request the DNS Server's configuration and/or can subscribe/unsubscribe to receive updates of the DNS Server's configuration.

When the UE performs an FQDN resolution request for an application, the UE shall use the EDC functionality to perform the DNS resolution in one of the following cases:

- the application mapped onto the PDU Session explicitly requests the use of the EDC functionality and the SMF indicated, at PDU Session Establishment or at PDU Session Modification, that the use of the EDC functionality is allowed for that PDU session; or
- the SMF indicated, at PDU Session Establishment or at PDU Session Modification, that the use of the EDC functionality is required for the PDU Session for the specific DNN. In this case, the UE shall use the EDC functionality for all the applications mapped onto that PDU Session.

NOTE 3: Whether the specific DNN(s) is applied is based on the agreement between the MNO and the application provider.

NOTE 4: User preferences at OS level related to the use of DNS server do not apply when the EDC functionality is used.

NOTE 5: It is subject to local regulatory requirements whether the MNO can force the UE to use EDC functionality.

6 Procedures for Supporting Edge Computing

6.1 General

Edge Computing enables operator and 3rd party services to be hosted in EAS close to the UE's point of attachment. The traffic to EAS can be routed based on the UE position and EAS availability "near to" that position.

The subsequent clauses describe the procedures for supporting Edge Computing in 5G System considering different connectivity models, including:

- EAS discovery and re-discovery.
- Edge relocation.
- Network exposure to Edge Application Server.
- Support of 3GPP application layer architecture defined in TS 23.558 [5].
- Support of AF guidance to PCF determination of proper URSP rules.

6.2 EAS Discovery and Re-discovery

6.2.1 General

In Edge Computing deployment, an application service may be served by multiple Edge Application Servers typically deployed in different sites. These multiple Edge Application Servers that host service may use a single IP address (anycast address) or different IP addresses. To start such a service, the UE needs to know the IP address(es) of the Application Server(s) serving the service. The UE may do a discovery to get the IP address(es) of a suitable Edge Application Server (e.g. the closest one), so that the traffic can be locally routed to the Edge Application Server and service latency, traffic routing path and user service experience can be optimized.

EAS discovery is the procedure by which a UE discovers the IP address(es) of a suitable Edge Application Server(s) using Domain Name System (DNS). EAS Re-discovery is the EAS Discovery procedure that takes place when the previously discovered Edge Application Server cannot be used or may have become non-optimal (e.g. at edge relocation).

The DNS server to be used for EAS (re-)discovery may be deployed in different locations in the network as Central DNS (C-DNS) server or as Local DNS (L-DNS) resolver/server.

NOTE 1: The C-DNS servers and/or L-DNS resolvers/servers can use an anycast address.

NOTE 2: The C-DNS servers or L-DNS resolvers/servers can contact any other DNS servers for recursive queries, which is out of scope of this specification.

NOTE 3: This specification describes the discovery procedure based on 5GS NFs as to ensure the UE is served by the application service closest to the UE's point of attachment. However, this does not exclude other upper layer solution that can be adopted by operator or service provider, like the EAS Discovery procedure defined in TS 23.558 [5], or other alternatives shown in Annex A and Annex B. How those other solutions work, or whether they are able to guarantee the closest application service for the UE, is out of the scope of this specification.

In order to provide a translation of the FQDN of an EAS into the address of an EAS as topologically close as possible to the UE, the Domain Name System may use following information:

- The source IP address of the incoming DNS Query; and/or,
- an EDNS Client Subnet (ECS) option (as defined in RFC 7871 [6]).

NOTE 4: UE IP address can be subject to privacy restrictions, which means that it is not to be sent to Authoritative DNS / DNS Resolvers outside the network operator within EDNS Client Subnet option or as Source IP address of the DNS Query. UE source IP address can be protected by using NAT mechanism.

EAS (re-)discovery procedures described in this specification should use the top level domains (TLDs) in the public namespace by default.

If a private namespace is used, an Edge Computing Service Provider (ECSP) can provision DNS information in the EAS Deployment information via AF request with its Application Identifier, or DNN and NSSAI. Since private namespaces do not have a common root server or naming, the DNS information for each ECSP should be stored individually to prevent any overwriting of resolution entries.

NOTE 5: The DNS information provided by ECSP in the EAS Deployment Information can be used to select the DNS settings for a PDU Session mainly if the PDU Session is specific for the ECSP services.

If the UE applications want to discover/access EAS by using the mechanisms defined in this TS, the UE shall support receiving DNS settings in PCO during PDU Session Establishment and PDU Session Modification, and the DNS Queries generated by the UE for these applications shall be sent to the DNS server/resolver (e.g. EASDF) indicated by the SMF. To ensure this, the application in the UE either requests the EDC functionality to send a DNS Query or, alternatively, uses the EDC functionality to get the configuration of the DNS Server (IP address and, conditionally, DNS security information of the EASDF/DNS Server/ Resolver; see TS 24.501 [11] and TS 33.501 [12]) indicated by the SMF (see clauses 5.2.1 and 6.2.4) then resolves the FQDN by its own DNS mechanism.

For EASDF, the DNS security information may be provided by EASDF to SMF. The DNS security information of the EASDF/Local DNS Server/Resolver may also be locally configured in the SMF.

NOTE 6: The DNS security information of Local DNS Server/Resolver can be locally configured in the SMF if they belong to same security domain.

NOTE 7: It is the decision of the application in the UE whether to use the EDC functionality or not to resolve the FQDN. If it does not use the EDC functionality, the usage of the EAS (re-)discovery procedures defined in clause 6.2 cannot be ensured.

The case of EAS (Re-)discovery over Distributed Anchor connectivity model is described in clause 6.2.2. For Multiple PDU Sessions connectivity model, the description in clause 6.2.2 also applies to the PDU Session(s) with Local PSA. The case of EAS (Re-)discovery over Session Breakout connectivity model is described in clause 6.2.3.

6.2.2 EAS (Re-)discovery over Distributed Anchor Connectivity Model

6.2.2.1 General

6.2.2.2 EAS Discovery Procedure

For the Distributed Anchor connectivity model, in PDU Session Establishment procedure, the SMF selects a DNS Server for the PDU Session. The DNS Server is configured to UE via PCO, and may also be configured via DHCP and/or IPv6 RA. The SMF determines the DNS server address for the PDU Session based on local configuration and EAS Deployment Information provided by AF when applicable.

In order to provide a translation of the FQDN of an EAS into the address of an EAS as close as possible to the UE (where closeness relates to IP forwarding distance), the DNS system uses mechanisms described in clause 6.2.1.

For Distributed Anchor Point connectivity model, in order to provide addressing information to the DNS system that is related to the UE topological location, when a DNS Query is sent via the Local PSA UPF,

- either the DNS Query is resolved by a DNS resolver, which then adds a DNS EDNS Client Subnet option that may be built based on a locally pre-configured value or based on the source IP address of the DNS Query; then send the DNS Query to the Authoritative DNS server, which may take into account the DNS EDNS Client Subnet option as defined in RFC 7871 [6], or

- the DNS Query is resolved by a DNS server that is close to the PSA UPF: the Authoritative DNS server may take into account the source IP address of the DNS Query.

6.2.2.3 EAS Re-discovery Procedure at Edge Relocation

In order to change the PDU Session Anchor serving a PDU Session of SSC mode 2/3 for a UE, SMF triggers session continuity, service continuity and UP path management procedures as indicated in clause 4.3.5.1, 4.3.5.2 and 4.3.5.3 of TS 23.502 [3]. During these procedures, for SSC mode 2/3, it is recommended that the UE applies the following behaviour:

The UE DNS cache should be bound to the IP connection. When the UE detects the PDU Session release or new IP prefix is allocated within the PDU Session, the UE removes the old DNS cache related to old/removed IP address/prefix, for example, the old Edge Application Server address information.

NOTE 1: UE DNS cache refers to cache at any level (OS and Application). Whether the DNS cache of Application is included or influenced depends on application's behaviour and UE implementation.

With this behaviour, when the establishment of a new PDU Session triggers EAS rediscovery for an FQDN, the UE can reselect a new EAS for that FQDN.

For SSC mode 2, the procedure in clause 4.3.5.1 of TS 23.502 [3] applies with following differences:

- In step 3, when the new PDU Session has been established, UE can reselect a new EAS for the FQDN with an EAS Discovery procedure if the recommended UE behaviour has been followed.

For SSC mode 3 with multiple PDU Sessions, the procedure in clause 4.3.5.2 of TS 23.502 [3] applies with following difference:

- In step 5, the UE can reselect a new EAS for the FQDN with an EAS Discovery procedure if the recommended UE behaviour has been followed.

For SSC mode 3 with IPv6 Multi-homed PDU Session that all new traffic going via new IPv6 prefix, the procedure in clause 4.3.5.3 of TS 23.502 [3] applies with following difference:

- After steps 10-11 where SMF notifies the UE of the availability of the new IP prefix, the UE starts using it for all new traffic, including DNS Queries. The UE can reselect a new EAS for the FQDN with an EAS Discovery procedure if the recommended UE behaviour has been followed.

Then UE can reselect a new EAS for the FQDN with an EAS discovery procedure as defined in clause 6.2.2.2.

NOTE 2: For SSC mode 3 with Multi-homed PDU Sessions, an EAS re-discovery indication may as well be sent as described in clause 6.2.3.3.

The SMF may also trigger EAS rediscovery as defined in clause 6.2.3.3 when new connection to EAS needs to be established in case the UE indicate support for this. This trigger may also be used by the SMF based on the AF trigged EAS relocation as described in clause 6.3.7.

6.2.2.4 Procedure for EAS Discovery with Dynamic PSA Distribution

5GC supports an EAS discovery procedure that allows that at PDU Session Establishment the SMF selects a Central PSA, regardless if a Local PSA is available to the SMF and then, it allows to dynamically re-anchor the PDU Session and transition to a Distributed Anchor Point connectivity model when needed. This is applicable to PDU Sessions of both SSC mode 2 and SSC mode 3.

This procedure relies on EASDF capability to influence the DNS Query of a FQDN so that the EAS Discovery considers a candidate UE topological location of a PSA further out in the network than current PSA. The PDU Session re-anchoring to the edge is performed as part of the EAS Discovery procedure.

This procedure requires that the DNS settings provided to the UE for the PDU Session are respected.

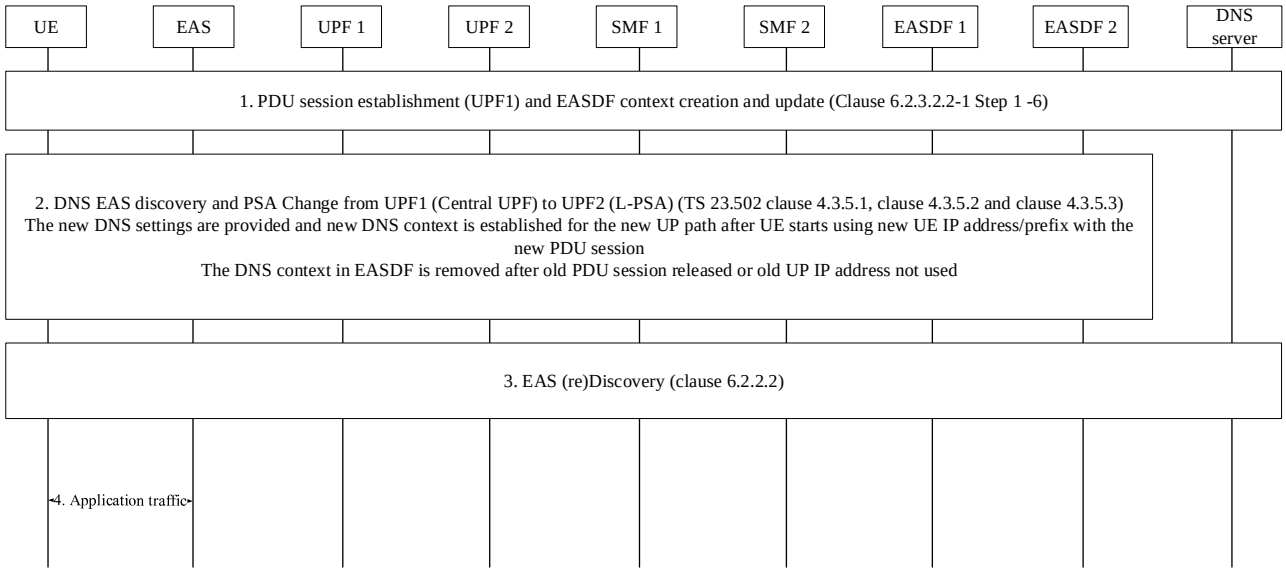

Figure 6.2.2.4-1 Application server discovery with Dynamic PSA distribution using EASDF

The EAS Discovery procedure with Dynamic PSA distribution for both SSC mode 2 and SSC mode 3 PDU Sessions using EASDF is described in Figure 6.2.2.4.-1.

The procedure is as follows:

1. PDU Session Establishment, allocation of an EASDF and sending rules to the EASDF. Steps 1-6 in the procedure 6.2.3.2.2-1 for EAS Discovery Procedure with EASDF for Session Breakout connectivity model are applied. If Dynamic PSA distribution applies to the PDU Session based on SMF local configuration, the SMF may have selected a Central PSA at PDU Session Establishment, regardless of whether a Local PSA is available.

2. The UE sends a DNS Query message for an FQDN to the EASDF via Central PSA. Steps 7-12 in the procedure in figure 6.2.3.2.2-1 for EAS Discovery Procedure with EASDF for Session breakout Connectivity are applied. That is, the EASDF checks the DNS Query against the DNS Handling Rules in the DNS Context and reports to

SMF and/or forwards to DNS for resolution as instructed by these rules. For resolution, it applies Option A or option B in the procedure 6.2.3.2.2-1 or sends the DNS Query to a pre-configured DNS server/resolver if none of them applies.

When the DNS Response is received, EASDF checks it against the DNS context matching conditions for reporting. If applicable, it reports to SMF the selected EAS and handles the DNS Response as instructed by SMF DNS handling rules: when there is a change of PDU Session Anchor per SSC mode 2 or 3, the SMF indicates to EASDF to discard the DNS Response.

When no DNS Response is sent to the UE, the UE is expected to restart the DNS Query over the new PDU Session).

For further details see clause 6.2.3.2.2.

SMF determines that the central UPF (PSA) needs to be changed to an Edge UPF (L-PSA) and it triggers one of the procedures to change the PSA of the PDU Session to a distributed anchor. Which procedure is triggered depends on the SSC mode of the PDU Session and also on SMF configuration:

- Change of SSC mode 2 PDU Session Anchor with different PDU Sessions as in clause 4.3.5.1 of TS 23.502 [3]. The procedure applies with the following differences:

  In step 2, the DNS context for the session is removed from EASDF as part of the PDU Session Release procedure (in step 12 of the PDU Session release procedure in TS 23.502 [3] in 4.3.4.2).

  In step 3, SMF selects and provisions the DNS settings for the new PDU Session as required by the procedure for EAS Discovery on Distributed anchor as described in clause 6.2.2.2.

- Change of SSC mode 3 PDU Session Anchor with multiple PDU Sessions as in clause 4.3.5.2 of TS 23.502 [3]. The procedure applies with the following differences:

  In step 4 in clause 4.3.5.2 of TS 23.502 [3], SMF selects and provisions the DNS settings for the new PDU Session as required by the procedure for EAS Discovery on Distributed anchor as described in clause 6.2.2. Step 3 in 6.2.2.4 could happen any time after this step.

  In step 6 in clause 4.3.5.2 of TS 23.502 [3], the old DNS context for the old session and old UE IP address/prefix of UE are removed from EASDF as part of the PDU Session Release procedure (in step 12 of the PDU Session Release procedure in TS 23.502 [3] in 4.3.4.2).

- Change of SSC mode 3 PDU Session Anchor with IPv6 Multi-homed PDU Session as in clause 4.3.5.3 of TS 23.502 [3]. The procedure applies with the following differences:

  In steps 10-11 in clause 4.3.5.3 of TS 23.502 [3], SMF also manages the EASDF context and provides new DNS settings to the UE if needed:

  - If EASDF is not going to be used, SMF sends the UE the new DNS settings in a PDU Session Modification Command and removes the EASDF context.

  - If EASDF is going to be used, SMF may update existing EASDF context or it may remove it and create a new one, for example, to select a new EASDF. If a new EASDF is selected, SMF sends the UE the new DNS settings in a PDU Session Modification Command and may also send them in Router Advertisement.

    After steps 10-11 in clause 4.3.5.3 of TS 23.502 [3], UE starts using IP@2 for all new traffic, including DNS messages, and SMF can already perform from step 3 in figure 6.2.2.4-1.

  The PDU Session establishment in this step includes the actions described above in step 1 in figure 6.2.2.4-1 if DNS Queries should be able to trigger re-anchoring of the session to a more distributed PSA.

NOTE 1: When new DNS settings do not involve EASDF, new DNS Query will not trigger re-anchoring of the PDU Session to a L-PSA deployed even further out in the network.

To remove the Session context in EASDF, SMF invokes Neasdf_DNSContext_Delete Request/Response.

NOTE 2: Dynamic re-anchoring to an edge PSA implies that the UE IP address is changed from a UE IP address corresponding to the old (central) PSA to a UE IP address corresponding to the new (edge) PSA for all applications on the PDU Session.

NOTE 3: Further re-anchoring (to a central UPF) can be triggered if activity is monitored e.g. if EC application traffic ceases. In that case, EASDF is provided again in the DNS settings for the PDU Session. New EAS Discovery will go to EASDF and be handled as described in step 1.

3. A new discovery procedure is triggered for the application over the new PSA: the UE resends a DNS Query targeting the application. (Re)discovery follows the EAS (re)Discovery procedure for distributed anchor connectivity model as in clauses 6.2.2.2 and 6.2.2.3.

NOTE 4: Clause 6.2.2.3 describes the UE behaviour that makes it possible to reselect a new EAS over the new PSA. With change of SSC mode 3 PDU Session Anchor with IPv6 Multi-homed PDU Session, an EAS rediscovery indication can as well be sent as described in clause 6.2.3.3.

4. Application traffic starts via the PDU Session Edge PSA to the EAS selected in step 3.

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

6.2.3.1 General

This clause describes the EAS discovery and re-discovery procedures for PDU Session with Session Breakout connectivity model.

The following Session breakout models are defined:

- Dynamic Session Breakout: ULCL/BP/Local PSA (and their associated traffic filters and forwarding rules) are inserted based on DNS Response provided by the EASDF or based on the common EAS. The detail of the ULCL/BP/Local PSA insertion or relocation triggered by the DNS Response message received for the EAS (Re-)discovery is described in the procedure in clause 6.2.3.2.2.

- Pre-established Session Breakout: ULCL/BP/Local PSA (and their associated traffic filters and forwarding rules) are inserted without dependency on the DNS Response(s) for the EAS (Re-)discovery. They are typically inserted based on local configuration or per traffic routing information from AF request within AF influence on traffic routing procedure. For the ULCL/BP/Local PSA insertion or relocation triggered by traffic routing information from AF request, the traffic routing information from AF request is received by the SMF via the SM policy which is created during the procedure PDU Session establishment or is updated during the lifetime of the PDU Session (e.g. updating the SM policy with the traffic routing information based on the detected application identifier based on the received application traffic like DNS Query or service data for the application). The details are described in clauses 4.3.5 and 6.2.1.2 of TS 23.503 [4] and in clause 5.6.7.1 of TS 23.501 [2] and in clause 4.3.6.2 of TS 23.502 [3].

6.2.3.2 EAS Discovery Procedure

6.2.3.2.1 General

For PDU Session with Session Breakout connectivity model, based on UE subscription (e.g. DNN) and/or the operator's configuration, the DNS Query sent by UE may be handled by an EASDF (see clause 6.2.3.2.2), or by a local or central DNS resolver/server (see clause 6.2.3.2.3).

NOTE 1: For the scenario where the TE and MT are separated, information provided by the SMF in the NAS message during the PDU Session Establishment or Modification may not be provided to the TE. Annex C documents mitigations for this scenario.

NOTE 2: The DNS Query sent by UE may or may not carry EDNS Client Subnet option in the DNS message.

The common EAS for a set of UEs can be provided by AF or determined by 5GC, if not provided by AF, with EAS discovery procedure via EASDF (see clause 6.2.3.2.5).

The common DNAI for a set of UEs can be provided by AF or determined by 5GC, if not provided by AF, with EAS discovery procedure via EASDF (see clause 6.2.3.2.6) or Local DNS resolver/server (see clause 6.2.3.2.4).

For the different procedures, when 5GC determines the common EAS/DNAI, the NEF determines the common EAS/DNAI with input from SMFs (see clause 6.2.3.2.7).

6.2.3.2.2 EAS Discovery Procedure with EASDF

For the case that the UE DNS Query is to be handled by EASDF, the following applies.

- The AF may provide EAS Deployment Information to NEF which may store it in UDR, as defined in clause 6.2.3.4. SMF may retrieve EAS Deployment Information from NEF as described in clause 6.2.3.4 or has locally preconfigured information. EAS Deployment Information is used for creating DNS message handling rule on EASDF and it is not dedicated to specific UE session(s).

  EAS Deployment Information may apply to all PDU Sessions with a certain DNN, S-NSSAI and/or specific Internal Group Identifier(s).

- The SMF may provide BaselineDNSPattern to EASDF, the BaselineDNSPattern are derived from EAS Deployment Information provided by AF and are not dedicated to specific PDU Session; SMF configures EASDF with BaselineDNSPattern according to the procedures defined in clause 6.2.3.4.

  The Baseline DNS message detection template ID may be used by the EASDF to refer to Baseline DNS message detection template, and derive array of FQDN ranges and/or array of EAS IP address ranges. The Baseline DNS handling actions ID may be used by the EASDF to refer to Baseline DNS handling actions information, and derive actions related parameters.

  The Baseline DNS message detection template ID and the Baseline DNS handling actions ID are unique per SMF set when a SMF set controls an EASDF and shall be unique per SMF otherwise, within an EASDF Baseline

  BaselineDNSPattern may contain one or several items, where each item is either a Baseline DNS message detection template or a Baseline DNS handling actions information. Each BaselineDNSPattern item may be updated or deleted using Baseline DNS message detection template ID or Baseline DNS handling actions ID to identify the updated or deleted item

  - Baseline DNS message detection template
    - Baseline DNS message detection template ID
    - DNS message type = DNS Query or DNS Response:
      - If DNS message type = DNS Query:
        - Array of (FQDN ranges).
      - If DNS message type = DNS Response:
        - Array of FQDN ranges and/or array of EAS IP address ranges.
  - Baseline DNS handling actions information:
    - Baseline DNS handling actions ID:
      - ECS option.
      - Local DNS server IP address.

NOTE 1: The FQDN can be set to wildcard to indicate the default DNS Server (e.g. the C-DNS), for the case in which the DNS message should be forwarded to the default DNS Server.

NOTE 2: The BaselineDNSPattern can be configured for a specific application with the related FQDN set in the detection template.

NOTE 3: The definition of structure of Baseline DNS handling actions ID and Detection template ID is left to stage 3. As an example, Baseline DNS handling action ID and Detection template ID could contain a concatenation of the SMF ID or SMF set Id and of SMF implementation selected information such as the DNAI or a sequence number. The EASDF is not meant to understand the structure of Baseline DNS handling actions ID and Detection template ID.

- During the PDU Session establishment procedure, the SMF may obtain the EAS Deployment Information from the NEF if not already retrieved (by subscription of such information to the NEF as described in clause 6.2.3.4.3)

or the SMF is preconfigure with the EAS Deployment Information and the SMF selects an EASDF and provides its address to the UE as the DNS Server to be used for the PDU Session.

The SMF configures the EASDF with DNS message handling rules to handle DNS messages related to the UE(s). The DNS message handling rule has a unique identifier and includes information used for DNS message detection and associated action(s). The DNS handling rules is defined as following:

- Precedence of the DNS message handling rule;
- DNS Handling Rule Identity;
- A Baseline DNS message detection template ID and/or a DNS message detection template (optional and includes at least one of the following, if existing):
  - DNS message type = DNS Query or DNS Response:
    - If DNS message type = DNS Query:
      - Source IP address (i.e. UE IP address).
      - Array of (FQDN ranges) (optional).
    - If DNS message type = DNS Response:
      - Array of FQDN ranges and/or array of EAS IP address ranges (optional).
- DNS message Identifier (if received from EASDF);

NOTE 4: For DNS message type = Query, the UE IP address provided at DNS context creation (Neasdf_DNSContext_Create Request) is considered if not provided explicitly as part of the DNS message detection template.

NOTE 5: DNS message Identifier is used by EASDF for matching between the message reported in the Neasdf_DNSContext_Notify and the corresponding DNS message handling rule included in Neasdf_DNSContext_Update.

- Action(s) (includes at least one action); the possible actions include:
  - Reporting Action: Report DNS message content to SMF (i.e. target FQDN and if available: IP address information provided back by the DNS server). This reporting action may include reporting-once indication. If this indication is included, the EASDF reports the DNS message content to the SMF once if the DNS message detection template matches the first incoming DNS Query or DNS Response message.

NOTE 6: With reporting-once indication, the DNS message detection template should contain the EAS IP address ranges corresponding to the same DNAI. Resetting the Reporting-once indication can be used by the SMF to allow reporting associated with a DNS handling rule when the SMF has removed the UL CL/BP e.g. when the UE has moved out of the area associated with the current DNAI and thus insertion of a new UPF offloading capability can be considered.

  - Forwarding Action: Send the DNS message(s) to a DNS server/resolver(s) as follows:

    A. Including the information to build optional EDNS Client Subnet option to be included in the DNS message, or to be used for replacing the EDNS Client Subnet option received in the DNS Query message from the UE. (The information for the EASDF to build the EDNS Client Subnet option is either included in the DNS handling rule, or Baseline DNS handling actions ID acts as a reference to the Baseline DNS handling actions Information. This corresponds to the option A defined below.

    B. the information for the DNS message target address is either included as DNS Server Address indicated in the DNS handling rule, or the Baseline DNS handling actions ID included in the DNS handling rules refers to DNS message target address information; if no DNS Server Address is provided by the SMF in the rule, then the EASDF is to forward the DNS message to a locally preconfigured default DNS server/resolver. This corresponds to the option B defined below.

    C. Respond directly to the DNS request. In this case the EASDF is configured by the SMF not to forward the DNS Query to the DNS server, instead it creates a response based on EAS IP address provided by the SMF.

NOTE 7: The forwarding action can include either A, B or C.

- Control Action: Performs at least one of control actions on the DNS message(s) as follows:
  - Build DNS response from DNS query with indicated IP address (e. g. common EAS). The EASDF is expected to handle the response it has built the same way as a response it has received from a remote DNS server.
  - Buffer the DNS message(s).
  - Send the buffered DNS Response(s) message to UE.
  - Discard cached DNS Response message(s).
  - Construct and send DNS Query message(s).

When the EASDF forwards a DNS message (to the UE or towards a DNS server), it uses its own address as the source address of the DNS message. When the EASDF forwards the DNS message to the UE the EASDF based on configuration either replace the received EDNS Client Subnet option with the one provided by the UE (i.e. if provided by the UE) or remove any received EDNS Client Subnet.

The SMF may use following information to create DNS message handling rules associated with a PDU Session:

- Local configuration associated with the (DNN, S-NSSAI, Internal Group Identifier) of the PDU Session; and/or
- EAS Deployment Information provided by the AF or preconfigured in the SMF; and/or
- Information derived from the UE location such as candidate L-PSA(s); and/or
- PDU Session information, like PDU Session L-PSA(s) and ULCL/BP; and/or
- Internal Group Identifier received in the Session Management Subscription data from the UDM; and/or
- IP address or DNAI (e.g. common EAS, common DNAI) cached locally or retrieve from UDR via PCF.

NOTE 8: For example, the SMF can derive the IP address for ECS based on the N6 IP address(es) associated with serving L-PSA(s) locally configured or in the NRF.

NOTE 9: Providing in DNS EDNS Client Subnet option an IP address associated with the L-PSA UPF protects the privacy of the (IP address of the) UE.

- If the FQDN in a DNS Query matches the FQDN(s) provided by the SMF in a DNS message detection template, based on instructions by SMF, one of the following options is executed by the EASDF based on a corresponding DNS message handling rule:
  - Option A: The EASDF includes or replaces an EDNS Client Subnet (ECS) option into the DNS Query message as defined in RFC 7871[6] and sends the DNS Query message to the DNS server for resolving the FQDN. The DNS server may resolve the EAS IP address considering the EDNS Client Subnet option and sends the DNS Response to the EASDF;
  - Option B: The EASDF sends the DNS Query message to a Local DNS server which is responsible for resolving the FQDN within the corresponding L-DN. The EASDF receives the DNS Response message from the Local DNS server.

NOTE 10: Option B does not support the scenario where the PSA UPF for transferring DNS Query between EASDF and DNS server, or the EASDF has no direct connectivity with the Local DNS servers.

  The SMF instructions for a matching FQDN may as well indicate EASDF to contact SMF. SMF then provides the EASDF with a DNS message handling rule;

- If the DNS Query from the UE does not match a DNS message handling rules set by the SMF, then the EASDF may simply forward the DNS Query towards a preconfigured DNS server/resolver for DNS resolution;
- When the EASDF receives a DNS Response message, the EASDF notifies the EAS information (i.e. EAS IP address(es), the EAS FQDN and if available the corresponding IP address within the ECS DNS option) to the SMF if the DNS message reporting condition provided by the SMF is met (i.e. the EAS IP address or FQDN is

within the IP/FQDN range). The SMF may then select the target DNAI based on the EAS information and trigger UL CL/BP and L-PSA insertion as specified in clause 6.3.3 in TS 23.501 [2] based on the Notification.

NOTE 11: To avoid SMF overloading caused by massive reporting, the overload control mechanisms defined in clause 6.4 of TS 29.500 [9] can be used.

The information to build the EDNS Client Subnet option or the Local DNS server address provided by the SMF to the EASDF are part of the DNS message handling rules to handle DNS Queries from the UE. This information is related to DNAI(s) for that FQDN(s) for the UE location, or in the case a common DNAI is used for the set of UEs, the information is determined based on the common DNAI of the set of UEs. The SMF may provide DNS message handling rules to handle DNS Queries from the UE to the EASDF when the SMF establishes the association with the EASDF for the UE and may update the rules at any time when the association exists. For the selection of the candidate DNAI for a FQDN for the UE, the SMF may consider the UE location, network topology, EAS Deployment Information and related policy information for the PDU Session provided as defined in clause 6.4 of TS 23.503 [4] or be preconfigured into the SMF. After the UE mobility, if the provided Information for EDNS Client Subnet option or the Local DNS server address needs to be updated, the SMF may send an update of DNS message handling rules to the EASDF.

NOTE 12: If multiple candidate DNAIs are available after considering the UE location, network topology and EAS deployment, the SMF selects one DNAI from the multiple ones based on operator's policy. For examples, the SMF can select the DNAI randomly, or based on selection weight factor if provided by AF, or select the DNAI closest to the UE location.

NOTE 13: To protect the SMF (e.g. to block DOS from the EASDF), the EASDF IP address for DNS Query Request is only accessible from the UE IP address via UPF.

Once the UL CL/BP and L-PSA have been inserted, the SMF may decide that the DNS messages for the FQDN are to be handled by Local DNS resolver/server from now on. This option is further described in clause 6.2.3.2.3.

To avoid EASDF sending redundant DNS message reports triggering UL CL/BP insertion corresponding to the same DNAI, the SMF may send reporting-once control information (i.e. DNS message handling rule with DNS message detection template containing EAS IP address ranges with reporting-once indication set) to EASDF to instruct the EASDF to report only once for the DNS messages matching with the DNS message detection template of the reporting-once control information for the DNS message detection template. In addition, the SMF may instruct the EASDF not to report DNS Responses to SMF corresponding to some FQDN ranges and/or EAS IP address ranges e.g. once the UL CL/BP and L-PSA have been inserted for the corresponding EAS IP address ranges for Pre-established session breakout while there is configuration for the related EASDF reporting DNS Responses. After the removal or change of the L-PSA, the SMF may instruct the EASDF to restart the reports of the DNS messages.

If the SMF, based on local configuration, decides that the interaction between EASDF and DNS Server in the DN shall go via an UPF, the SMF sends corresponding N4 rules to this UPF to instruct this UPF to forward DNS message between EASDF and the external DNS server. In this case, DNS messages between EASDF and DNS Server described in this clause are transferred via this UPF transparently.

NOTE 14: Based network configuration, one UPF is used to transmit DNS signalling between EASDF and DNS servers. The N4 session between the SMF and this UPF is not related to a specific PDU Session but provides rules targeting Downlink traffic from DNS servers to the EASDF and associated with the traffic of multiple UE(s); the traffic forwarding between EASDF and this UPF is realized by IP in IP tunnelling .The EASDF provides the SMF with the source address it uses to contact DNS servers and with the destination address where it expects to receive the tunnelled traffic.

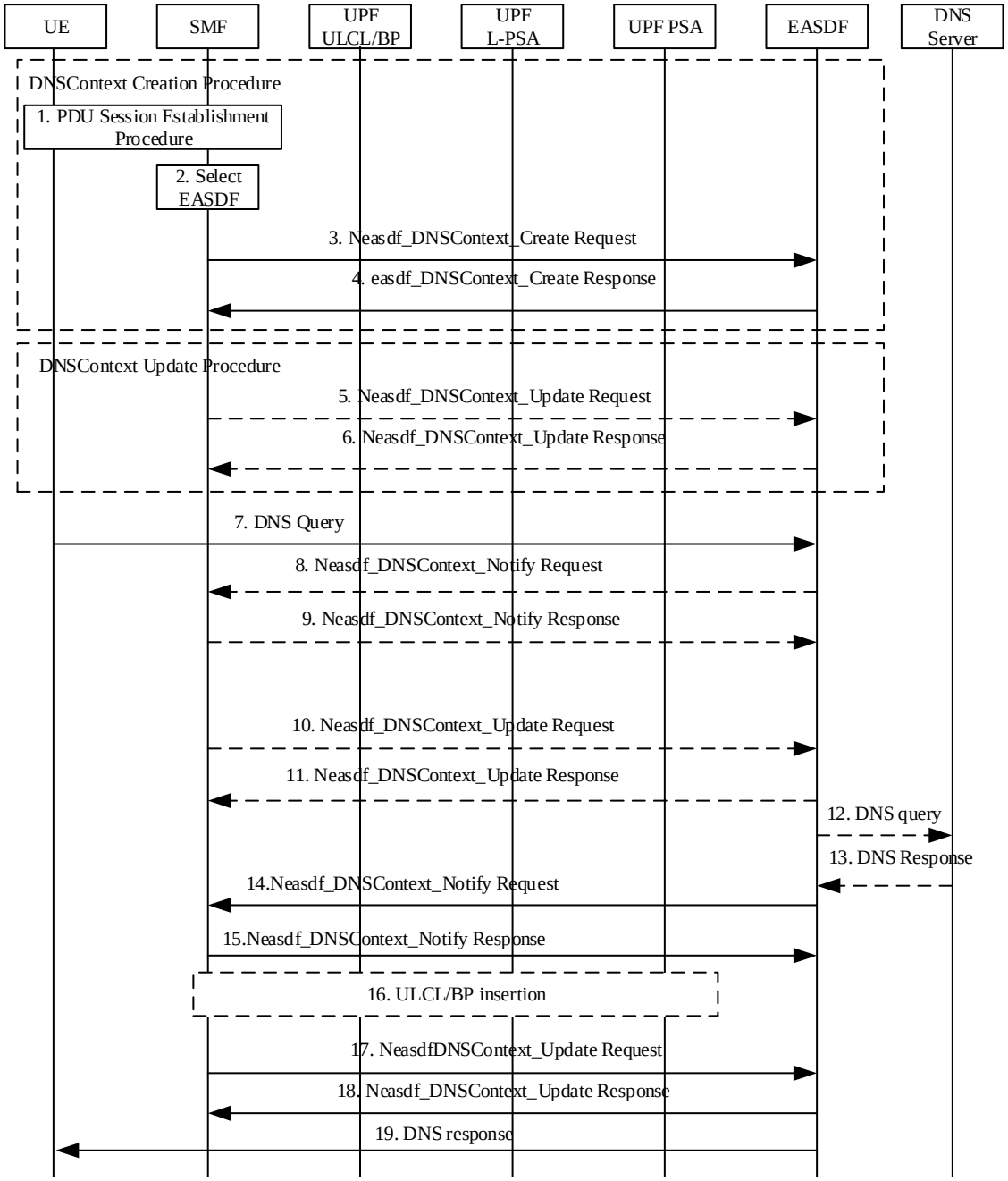

Figure 6.2.3.2.2-1: EAS discovery procedure with EASDF

1. UE sends PDU Session Establishment Request to the SMF as shown in step 1 of clause 4.3.2.2.1 of TS 23.502 [3]. The SMF retrieves the UE subscription information from the UDM (which may optionally include an indication on UE authorization for EAS discovery via EASDF) and checks if the UE is authorized to discover the EAS via EASDF. If not authorized, this procedure is terminated, and the subsequent steps are skipped.

2. During the PDU Session Establishment procedure, the SMF selects EASDF as described clause 6.3 of TS 23.501 [2]. The SMF may consider the UE subscription information to select an EASDF as the DNS server of the PDU Session.

   The 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.

   If the SMF, based on local configuration, decides that the interaction between EASDF and DNS Server in the DN shall go via the PSA UPF, the SMF configures PSA UPF within N4 rules to forward the DNS message between EASDF and DN.

3. The SMF invokes Neasdf_DNSContext_Create Request (UE IP address, DNN, notification endpoint, (DNS message handling rules)) to the selected EASDF.

   This step is performed before step 11 of PDU Session Establishment procedure in clause 4.3.2.2.1 of TS 23.502 [3].

   The EASDF creates a DNS context for the PDU Session and stores the UE IP address, the notification endpoint and potentially provided DNS message handling rule(s) into the context.

   The EASDF is provisioned with the DNS message handling rule(s), before the DNS Query message is received at the EASDF or as a consequence of the DNS Query reporting.

4. The EASDF invokes the service operation Neasdf_DNSContext_Create Response and if it exists, provides EASDF DNS security information.

   After this step, the SMF includes the IP address of the EASDF as DNS server/resolver for the UE in the PDU Session Establishment Accept message as defined in step 11 of clause 4.3.2.2.1 of TS 23.502 [3]. The UE configures the EASDF as DNS server for that PDU Session.

   If the UE requested to obtain UE IP address via DHCP and the SMF supports DHCP based IP address configuration, the SMF responds to the UE via DHCP response with the allocated UE IP address and/or the DNS server address containing the IP address of the EASDF.

5. The SMF may invoke Neasdf_DNSContext_Update Request (EASDF Context ID, (DNS message handling rules)) to EASDF. The update may be triggered by UE mobility, e.g. when UE moves to a new location, or by a reporting by EASDF of a DNS Query with certain FQDN, or, the update may be triggered by insertion/removal of Local PSA, e.g. to update rules to handle DNS messages from the UE or by new PCC rule information.

6. The EASDF responds with Neasdf_DNSContext_Update Response.

7. If required (see clause 5.2.1), the Application in the UE uses the EDC functionality as described in clause 6.2.4 to send the DNS Query to the EASDF. The UE sends a DNS Query message to the EASDF.

8. If the DNS Query message matches a DNS message detection template of DNS message handling rule for reporting, the EASDF sends the DNS message report to SMF by invoking Neasdf_DNSContext_Notify Request (information from the DNS Query e.g. target FQDN of the DNS Query). The EASDF may add a DNS message identifier in the Neasdf_DNSContext_Notify. The DNS message identifier uniquely identifies the DNS message reported and is used to associate the corresponding DNS message handling rule included in Neasdf_DNSContext_Update Request with the identified DNS message. The DNS message identifier is generated by EASDF.

9. The SMF responds with Neasdf_DNSContext_Notify Response.

10. If DNS message handling rule for the FQDN received in the report need to be updated, e.g. provide updates to information to build/replace the EDNS Client Subnet option information, the SMF invokes Neasdf_DNSContext_Update Request (DNS message handling rules) to EASDF. If the EASDF provided a DNS message identifier, the SMF adds this DNS message identifier to the corresponding DNS message handling rule included in Neasdf_DNSContext_Update. If the EASDF did not provide a DNS message identifier, the SMF may use the DNS message type (Request) and the target FQDN to uniquely identify the DNS message.

    For Option A, the DNS handling rule includes corresponding IP address to be used to build/replace the EDNS Client Subnet option. For Option B, the DNS handling rule includes corresponding Local DNS Server IP address. The EASDF may as well be instructed by the DNS handling rule to simply forward the DNS Query to a pre-configured DNS server/resolver.

11. If the SMF provided a DNS message handling rule with DNS message identifier, the EASDF only applies the DNS message handling rule to the corresponding DNS message. The EASDF responds with Neasdf_DNSContext_Update Response.

12. The EASDF handles the DNS Query message received from the UE as the following:

    - For Option A, the EASDF adds/replaces the EDNS Client Subnet option into the DNS Query message as specified in RFC 7871[6] and sends it to C-DNS server;

- For Option B, the EASDF removes EDNS Client Subnet option if received in the DNS query and sends the DNS Query message to the Local DNS server.

If no DNS message detection template within the DNS message handling rule provided by the SMF matches the requested FQDN in the DNS Query, the EASDF may simply send a DNS Query to a pre-configured DNS server/resolver.

13. EASDF receives the DNS Response including EAS IP addresses which is determined by the DNS system and determines that the DNS Response can be sent to the UE.

14. The EASDF sends DNS message reporting to the SMF by invoking Neasdf_DNSContext_Notify request including EAS information if the EAS IP address or the FQDN in the DNS Response message matches the DNS message detection template provided by the SMF. The DNS message reporting may contain multiple EAS IP address if the EASDF has received multiple EAS IP address(es) from the DNS server it has contacted. The DNS message reporting may contain the FQDN and the EDNS Client Subnet option received in the DNS Response message. The EASDF may also add DNS message identifier to the reporting. The DNS message identifier uniquely identifies the DNS response reported, and the EASDF can associate the corresponding DNS message handling rule included in Neasdf_DNSContext_Update Request with the identified DNS response. The DNS message identifier is generated by EASDF.

    Per the received DNS message handling rule, the EASDF does not send the DNS Response message to the UE but waits for SMF instructions (in step 17), i.e. buffering the DNS Response message.

    If the DNS Response(s) is required to be buffered and reported to the SMF, when the reporting-once control information is set, EASDF only reports to SMF once by invoking Neasdf_DNSContext_Notify request for DNS Responses matching with the DNS message detection template.

15. The SMF invokes Neasdf_DNSContext_Notify Response service operation.

16. The SMF may perform UL CL/BP and Local PSA selection and insert UL CL/BP and Local PSA.

    Based on EAS information received from the EASDF in Neasdf_DNSContext_Notify, other UPF selection criteria, as specified in clause 6.3.3 in TS 23.501 [2], and possibly Service Experience or DN performance analytics for an Edge Application as described in TS 23.288 [10], the SMF may determine the DNAI. The SMF may also determine the associated N6 traffic routing information for the DNAI according to N6 traffic routing information for the DNAI included in EAS Deployment Information and configure Local PSA UPF with forwarding actions derived from the N6 traffic routing information. The SMF may perform UL CL/BP and Local PSA selection and insertion as described in TS 23.502 [3]. In case of UL CL, the traffic detection rules and traffic routing rules are determined by the SMF based on IP address range(s) per DNAI included in the EAS Deployment Information or according to PCC rule received from PCF or according to preconfigured information.

17. The SMF invokes Neasdf_DNSContext_Update Request (DNS message handling rules). If the EASDF provided a DNS message identifier, the SMF adds this to the corresponding DNS message handling rule included in Neasdf_DNSContext_Update Request. If the EASDF did not provide a DNS message identifier, the SMF may use the DNS message type (Response) and the FQDN to uniquely identify the DNS response message.

    The DNS message handling rule with the Control Action "Send the buffered DNS response(s) message to UE" indicates the EASDF to send DNS Response(s) buffered in step 14 to UE. Other DNS message handling rule may indicate the EASDF not to send further DNS Response message(s) corresponding to FQDN ranges and/or EAS IP address ranges.

18. If the SMF provided a DNS message handling rule with DNS message identifier, the EASDF only applies the DNS message handling rule to the corresponding DNS response. The EASDF responds with Neasdf_DNSContext_Update Response.

19. If indicated to send the buffered DNS response(s) to UE in step 17, the EASDF sends the DNS Response(s) to the UE and handles the EDNS Client Subnet option as described above.

During PDU Session Release procedure, the SMF removes the DNS context by invoking Neasdf_DNSContext_Delete service.

6.2.3.2.3 EAS Discovery Procedure with Local DNS Server/Resolver

For the case that the DNS message is to be handled by Local DNS resolver/server, the DNS Query is routed to the Local DNS resolver/server corresponding to the DNAI where the L-PSA connects. The SMF selects the Local DNS server address based on the DNAI corresponding to the inserted local PSA, local configuration and based on EAS Deployment Information in AF request as specified in clause 6.2.3.4.2. Based on the operator's configuration, one of the following options may apply when UL CL/BP and Local PSA have been inserted (during or after PDU Session Establishment):

- Option C: The SMF configures the local DNS server to the UE as new DNS server. The 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. In addition, the SMF also configures traffic routing rule on the UL CL (including e.g. Local DNS server address) or the BP (e.g. the new IP prefix @ Local PSA) to route traffic destined to the L-DN including the DNS Query messages to the L-PSA. The L-DNS server resolves the DNS Query either locally or recursively by communicating with other DNS servers.

- Option D: If the SMF has been configured that DNS Queries for an FQDN (range) query can be locally routed on the UL CL, then the subsequent DNS Queries for the FQDN (range) will be locally routed to a Local DNS server.

NOTE 1: Option D assumes that ULCL steering is based on L4 information (i.e. DNS port number) and that ULCL has visibility of the DNS traffic (i.e. FQDN in the DNS Query message). The UPF may be instructed by the SMF to apply different forwarding of non-ciphered UL DNS traffic based on the target domain of the DNS Query. Option D requests modification of destination IP address of DNS messages. Whether this is allowed or not is subject to local regulations. Option D does not apply to DoH or DoT messages.

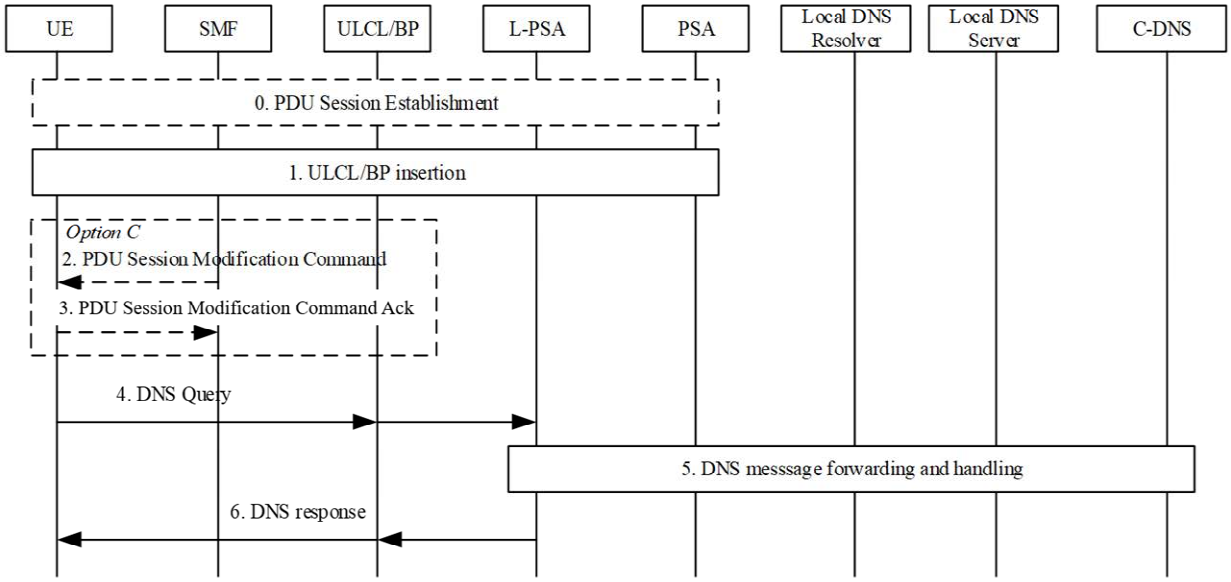

Figure 6.2.3.2.3-1: EAS discovery with Local DNS server/resolver

0. UE sends a PDU Session Establishment Request to the SMF as shown in step 1 of clause 4.3.2.2.1 of TS 23.502 [3]. The SMF retrieves the UE subscription information from the UDM (which may optionally include an indication on UE authorization for EAS discovery via EASDF) and checks if the UE is authorized to discover the EAS via EASDF. If not authorized, the actions related to EASDF in this procedure are skipped.

1. The SMF inserts UL CL/BP and Local PSA.

   UL CL/BP/Local PSA insertion can be triggered by DNS messages as described in clause 6.2.3.2.2. Or, the SMF may pre-establish the UL CL/BP and Local PSA before the UE sends out any DNS Query message (e.g. upon UE mobility). In this case, the SMF includes the IP address of Local DNS Server in PDU Session Establishment Accept message as in step 11 of clause 4.3.2.2.1 of TS 23.502 [3] or in a network initiated PDU Session Modification procedure. The UE configures the Local DNS Server as DNS server for that PDU Session.

NOTE 2: If the new DNS server address is provided to the UE, the UE can refresh all EAS(s) information (e.g. DNS cache) bound to the PDU Session, based on UE implementation.

The UL CL/BP and Local PSA are inserted or changed as described in TS 23.502 [3]. In the case of IPv6 multi-homing, the SMF may also send an IPv6 multi-homed routing rule along with the IPv6 prefix to the UE to influence the selection of the source Prefix for the subsequent DNS Queries as described in clause 5.8.2.2.2 of TS 23.501 [2].

When the UL CL/BP and Local PSA are inserted or simultaneously changed, the SMF configure the UL CL/BP for DNS Query handling:

- For Option C, the SMF configures traffic routing rule on the UL CL (including e.g. Local DNS server address) or the BP (e.g. the new IP prefix @ Local PSA) to forward UE packets destined to the L-DN to the Local PSA. The packets destined to L-DN includes DNS Query messages destined to Local DNS Server.

Steps 2 and 3 are performed for option C:

2. If the UL CL/BP and Local PSA are inserted after PDU Session Establishment, the SMF sends PDU Session Modification Command (Local DNS Server Address) to UE.

   If, based on operator's policy or UE's mobility, the Local DNS Server IP address in the local Data Network needs to be notified or updated to UE, the SMF sends PDU Session Modification Command (Local DNS Server Address) to UE.

3. The UE responds with PDU Session Modification Command Ack.

   The UE configures the Local DNS Server as the DNS server for the PDU Session. The UE sends the following DNS Queries to the indicated Local DNS Server.

   If EASDF was used as the DNS server for the PDU Session, the SMF may invoke Neasdf_DNSContext_Delete service to remove the DNS context in the EASDF.

NOTE 3: The UE does not need to know that the new DNS server is "local".

For the Split-UE in the option C case, the new address of Local DNS Server cannot be provided to the TE or the TE OS from the MT, Annex C documents mitigations for this scenario.

4. If required (see clause 5.2.1), the application in the UE uses the EDC functionality as described in clause 6.2.4 to send the DNS Query to the DNS Resolver/DNS Server indicated by the SMF in Step 0. UE sends a DNS Query message. In the case of IPv6 multi-homing the UE selects the source IP prefix based on the IPv6 multi-homed routing rule provided by SMF.

5. The DNS Query message is forwarded to the Local DNS Server and handled as described in following:

   - For Option C, the target address of the DNS Query is the IP address of the Local DNS Server. The DNS Query is forwarded to the Local DNS Server by UL CL/BP and Local PSA. The Local DNS Server resolves the FQDN of the DNS Query by itself or communicates with other DNS server to recursively resolve the EAS IP address.

   - For Option D: The Local PSA sends the DNS traffic to the Local DNS Server that resolves the FQDN target of the DNS Query by itself or that communicates with a C-DNS server to recursively resolve the EAS IP address.

NOTE 4: The Local PSA can send the DNS traffic to the Local DNS Server via tunnelling or via IP address replacement. If IP address replacement is used, the SMF sends the IP address of the Local DNS Server to the Local PSA and instructs the Local PSA to modify the packet's destination IP address (corresponding to EASDF) to that of the Local DNS Server.

6. The Local PSA receives DNS Response message from Local DNS server, it forwards it to the UL CL/BP and the UL CL/BP forwards the DNS Response message to UE.

NOTE 5: If IP address replacement has been enforced at step 5, the Local PSA replaces the source IP address to EASDF IP according to SMF instruction.

If SMF decides to remove the UL CL/BP and Local PSA as defined in clause 4.3.5.5 of TS 23.502 [3], e.g. due to UE mobility, the SMF sends a PDU Session Modification Command to configure the new address of the DNS server on UE (e.g. to set it to the address of EASDF).

6.2.3.2.4 Select common DNAI with Local DNS Server/Resolver for a set of UEs

The following procedure is for selecting common DNAI with Local DNS Server/Resolver for set of UEs.

NOTE: In this Release, when an operator deploys the Local DNS server option defined in clause 6.2.3.2.3, the operator needs to be ensured that a UE cannot be involved in more than one UE set for a DNN and S-NSSAI.

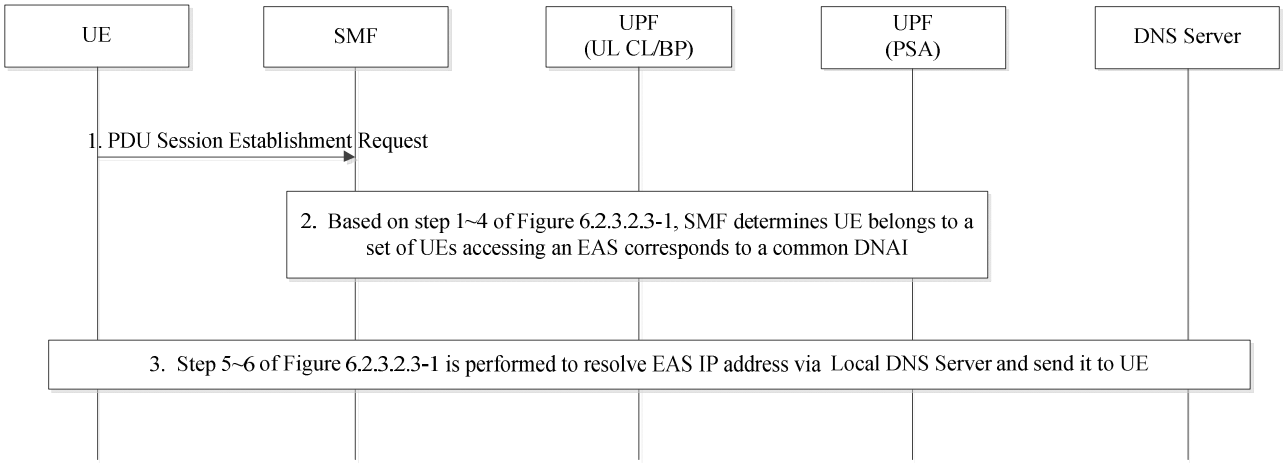

Figure 6.2.3.2.4-1: Discovery Procedure for selecting the common DNAI for a set of UEs with Local DNS Server/Resolver

1. The UE sends a PDU Session establishment request to SMF as specified in step 0 of Figure6.2.3.2.3-1.
2. The procedure in steps 1-4 of Figure 6.2.3.2.3-1 applies with following difference:

   In step 1, the SMF determines UE belongs to a set of UEs accessing an EAS corresponds to a common DNAI based on traffic correlation indication and Traffic correlation ID in the PCC rule.

   If the common DNAI is not available, the SMF notifies the NEF to determine the common DNAI as described in clause 6.2.3.2.7.

   Once the common DNAI is available, SMF inserts or changes a Local PSA serving the common DNAI and selects local PSA and local DNS server corresponding to the common DNAI.

   If the PDU session has been established and the PCC rule including updated common DNAI is provided to SMF, the SMF should reselect the local DNS server according to the common DNAI and configure the UE with new local DNS server in PCO using PDU session modification procedure.
3. The EAS information (e.g. EAS IP address) is resolved by Local DNS Server and sent the UE as described in steps 5-6 of Figure 6.2.3.2.3-1.

6.2.3.2.5 Common EAS discovery with EASDF for a set of UEs

The following is the procedure for common EAS discovery for a set of UEs accessing the same application. Different UEs can be served by different SMFs.

The common EAS IP address for the set of UEs may either be provided by AF or determined by 5GC. AF may provide the common EAS IP via AF Traffic influence procedure as defined in clause 4.3.6.2 of TS 23.502 [3], for this purpose, AF may determine the common EAS IP address based on candidate DNAI(s) reported by SMF as described in clause 4.3.6.3 of TS 23.502 [3]. Alternatively, if AF did not provide a common EAS IP address, the common EAS IP address may be determined by NEF as defined in clause 6.2.3.2.7 and is stored in UDR as part of AF traffic influence request information.

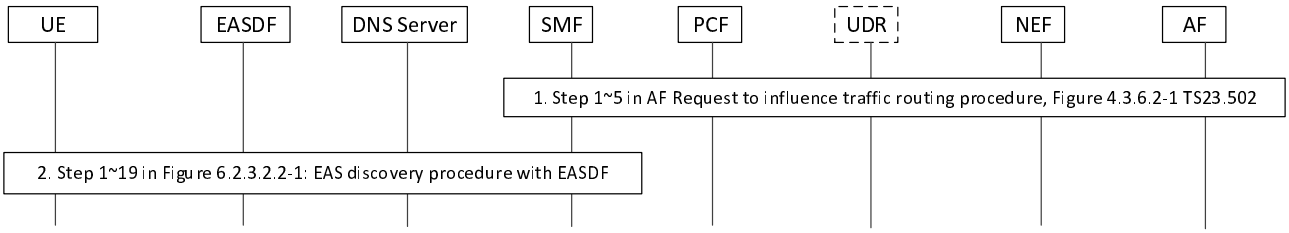

Figure 6.2.3.2.5-1: Common EAS discovery with EASDF for a set of UEs

1. The AF request in step 1 of figure 4.3.6.2-1 in TS 23.502 [3] is used to request selecting the common EAS for a set of UEs accessing the application as identified in the AF Request.

   AF may use External/Internal Group ID(s) or a list of UEs or any UE accessing the combination of DNN, S-NSSAI and DNAI as Target UE Identifier(s) and additionally Spatial Validity Condition to identify the set of UEs for correlated selection of common EAS.

   The following information may be included in AF request as defined in clause 5.6.7.1 of TS 23.501 [2]:

   - An EAS Correlation indication may be provided for indication of selecting the same EAS for the set of UEs accessing the same application.
   - A Traffic Correlation ID may be provided for identification of the set of UEs accessing the application identified by the Traffic Description in AF request.
   - A Common EAS IP address to be accessed by the set of UEs may be included in AF request, if it is determined by AF.
   - FQDN(s) may be included which is corresponding to the application traffic identified by Traffic Description in AF request.
   - Spatial Validity Condition could be provided for limiting the location of the UEs, and also "any UE" or a UE list or group ID can be provided for defining the set of UEs accessing the same EAS.

   In step 3a of figure 4.3.6.2-1 of TS 23.502 [3], NEF updates the AF influence data related to the traffic correlation ID in the UDR with a NEF information (i.e. Notification Endpoint of the NEF) to subscribe to be notified with information related to SMF's involvement for UE members of the set of UEs.

   In step 5 of figure 4.3.6.2-1 of TS 23.502 [3], PCF determines the UEs influenced by the AF Request and for each UE, based on AF request, PCF creates PCC rule with Traffic Correlation ID, EAS Correlation indication, Common EAS IP address, FQDN(s) and NEF information to SMF due to step 3a and sends the PCC rule to the SMF.

   If an existing PDU Session is impacted by the above PCC rule for common EAS discovery and if the UE has indicated that it supports to refresh EAS information stored locally, the SMF shall send PDU Session Modification Command (EAS rediscovery indication, [impact field]) to UE to refresh the cached EAS information as described in step 2 of clause 6.2.3.3.

2. Based on steps 1-19 in figure 6.2.3.2.2-1, with the following updates:

   In step 9:

   > If FQDN in Neasdf_DNSContext_Notify Request is corresponding to the application indicated in PCC rule, e.g. the FQDN is included in the FQDN(s) in the PCC rule and if EAS Correlation indication is set, SMF determines the UE belongs to the set of UEs identified by Traffic Correlation ID and accessing the application and determines the UE connects to the common EAS for the set of UEs. If FQDN(s) is included in PCC rule, the SMF can use the FQDN(s) in PCC rule and the FQDN in Neasdf_DNSContext_Notify Request to match the FQDN with the PCC rule, i.e. the matched PCC rule includes the FQDN(s) containing the FQDN in Neasdf_DNSContext_Notify Request.

   If the common EAS is not present in PCC rule or SMF decides to trigger the EAS discovery procedure to select a new EAS for the set of UEs (e.g. due to UE mobility):

   > Steps 10-15 are used for discovering of common EAS. After step 15, the procedure defined in clause 6.2.3.2.7 may be performed for common EAS IP coordination.

NOTE: Coordination procedure among SMFs always operates unless the SMF has been configured that it is the only SMF serving the set of UEs.

Else, if the common EAS is available (e.g. common EAS IP address is presented in PCC rule) and to be used for the set of UEs:

Steps 10-15 are skipped.

In step 16:

SMF may determine the DNAI based on the common EAS.

In step 17:

SMF sends DNS message handling rule including IP address for the common EAS and the Forwarding Action "Respond directly to the DNS request" for instructing EASDF to return the Common EAS IP address in a DNS response to UE directly.

In step 19:

If received IP address of the common EAS and instructed to respond directly in step 17, EASDF sends DNS response with the IP address of the common EAS to UE.

6.2.3.2.6 EAS discovery corresponding to Common DNAI with EASDF for a set of UEs

The common DNAI for the set of UEs can be provided either by AF or determined by 5GC. When the AF determines the common DNAI, the AF provides the common DNAI for the set of UEs via AF Traffic influence procedure as defined in clause 4.3.6.2 of TS 23.502 [3]. The AF may determine the common DNAI based on candidate DNAI(s) reported by SMF as described in clause 4.3.6.3 of TS 23.502 [3].

In the case that the AF did not provide a common DNAI, the 5GC determines the common DNAI. For this case, the common DNAI is determined by NEF and the NEF stores the common DNAI in UDR as part of AF traffic influence request information, as described in clause 6.2.3.2.7.

The following is the procedure for discovery EAS corresponding to a Common DNAI for set of UEs accessing the same application.

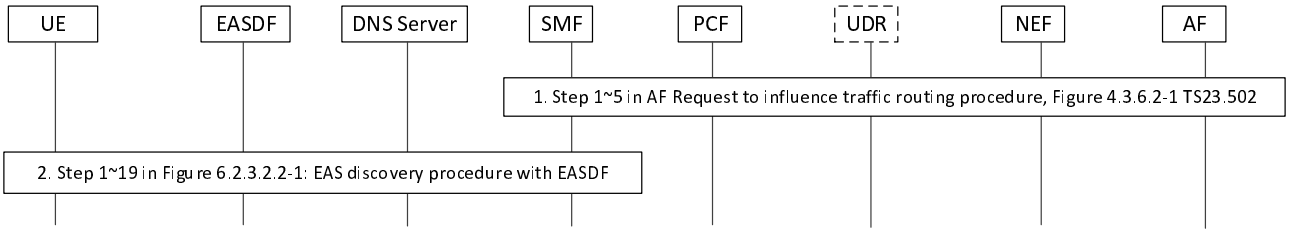

Figure 6.2.3.2.6-1: EAS discovery corresponding to Common DNAI for a set of UEs

1. The AF request in step 1 of figure 4.3.6.2-1 in TS 23.502 [3] is used to request selecting the common DNAI for a set of UEs accessing the application as identified in the AF Request.

   AF may use External/Internal Group ID(s) or a list of UEs or any UE as Target UE Identifier(s) and additionally Spatial Validity Condition to identify the set of UEs for correlated selection of common DNAI.

   The following information may be included in AF request as defined in clause 5.6.7.1 in TS 23.501 [2]:

   - An indication of traffic correlation may be provided for indication of selecting the same DNAI (i.e. selecting EAS corresponding to the same DNAI) for the set of UEs accessing the same application.
   - A Traffic Correlation ID may be provided for identification of the set of UEs accessing the application identified by the FQDN(s) in AF request.
   - A Common DNAI to be accessed by the set of UEs can be included in Potential locations of applications of the AF request, if it is determined by AF.

- FQDN(s) may be included which is corresponding to the application identified by Traffic Description in AF request.

- Spatial Validity Condition could be provided for limiting the location of the UEs, and also "any UE" or a UE list or group ID can be provided for defining set of UEs accessing the same DNAI.

In step 3a of figure 4.3.6.2-1 of TS 23.502 [3], NEF updates the AF influence data related to the traffic correlation ID in the UDR with a Notification Endpoint to subscribe to be notified with information related to SMF's involvement for UE members of the set of UEs.

In step 5 of figure 4.3.6.2-1 of TS 23.502 [3], PCF determines the UEs influenced by the AF Request, and for each UE, based on AF request, PCF creates PCC rule with Traffic Correlation ID and indication of traffic correlation, Common DNAI, FQDN(s) and Notification endpoint of NEF subscription received to step 3a and sends the PCC rule to the SMF.

If an existing PDU Session is impacted by the above PCC rule for EAS discovery corresponding to Common DNAI and if the UE has indicated that it supports to refresh EAS information stored locally, the SMF shall send PDU Session Modification Command (EAS rediscovery indication, [impact field]) to UE to refresh the cached EAS information as described in step 2 of clause 6.2.3.3.

2. Based on steps 1~19 in figure 6.2.3.2.2-1, with the following changes:

   In step 10:

   If FQDN in Neasdf_DNSContext_Notify Request is corresponding to the application indicated in PCC rule, e.g. the FQDN is included in the FQDN(s) in the PCC rule and if indication of traffic correlation is set, SMF determines the UE belongs to set of UEs identified by Traffic Correlation ID and accessing the application and determines the UE connects to EAS corresponding to the common DNAI for the set of UEs. If FQDN(s) is included in PCC rule, the SMF can use the FQDN(s) in PCC rule and the FQDN in Neasdf_DNSContext_Notify Request to match the FQDN with the PCC rule, i.e. the matched PCC rule includes the FQDN(s) containing the FQDN.

   If the common DNAI is not available in the PCC Rule received in step 1, the SMF invokes the NEF to determine the common DNAI as described in clause 6.2.3.2.7.

   Once the common DNAI is available, for Option A, SMF provisions EASDF with the information to build EDNS Client Subnet option that refers to a location that is topologically close to the common DNAI; for Option B, SMF provisions EASDF with Local DNS server related to the common DNAI.

6.2.3.2.7 Coordination among SMFs for Common EAS/DNAI determination

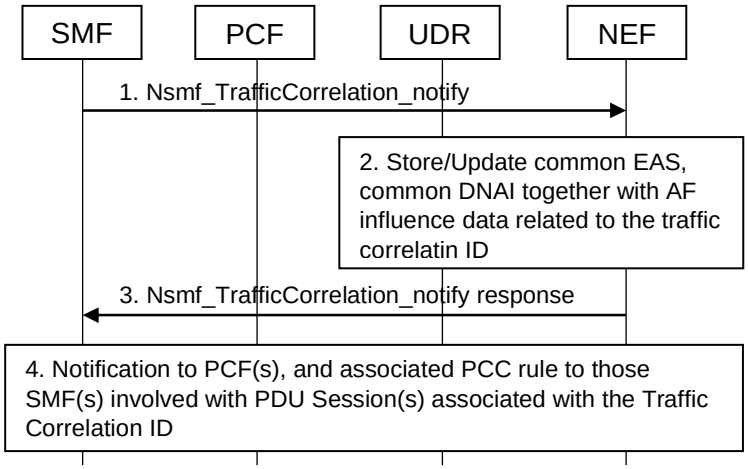

Figure 6.2.3.2.7-1: Handling of Common EAS, Common/DNAI for set of UEs

1. SMF sends Nsmf_TrafficCorrelation_Notify to the NEF with Notification Endpoint received in the PCC rule as described in clauses 6.2.3.2.5 and 6.2.3.2.6 and provides: EAS IP address(es) based on EASDF procedure and/or

list of candidate DNAI(s), SMF ID, number of PDU sessions it is serving for the set of UEs, Traffic Correlation ID.

2. If the NEF determines that there is currently no common EAS IP address and/or common DNAI available for the set of UEs identified by Traffic Correlation ID, it selects a common DNAI and/or common EAS using the list of DNAI(s), EAS IP address and number of PDU sessions each SMF is serving for the set of UEs received in step 1. Then the NEF updates traffic influence data with the 5GC determined common EAS/DNAI for the set of UEs.

   The update of traffic influence data triggers notifications to PCF(s) that in turn trigger associated PCC rule updates to the SMF(s), if any, with PDU Session(s) associated with the traffic correlation ID.

   The NEF maintains a list of SMFs serving the set of UEs and the associated data including common DNAI, common EAS, number of PDU sessions each SMF is serving for the set of UEs, Traffic Correlation ID.

3. NEF responds by acknowledging the notification to the SMF.

4. The update in UDR triggers notification to the PCF(s) that have subscribed for notification. The PCF(s) sends PCC rule(s) with NEF information, Traffic correlation ID and common EAS IP address and/or Common DNAI, as part of traffic influence data to the SMF(s) with PDU Session(s) associated with the Traffic Correlation ID.

   SMF(s) may select other candidate DNAI(s) for the PDU session(s) or a candidate new EAS IP address via the EASDF procedure e.g. due to UE(s) mobility. In this case, the SMF notifies to the NEF as in the above step 1, with the list of candidate DNAI(s) and/or EAS IP address. This may trigger NEF to re-select common DNAI and/or common EAS. NEF determines common EAS and/or common DNAI based on received EAS IP, list of candidate DNAI(s), number of PDU sessions SMF(s) serving for the set of UEs.

   If another DNAI/EAS IP address is selected by the NEF, it updates the common DNAI or common EAS in the UDR in the Traffic Influence data.

NOTE: How NEF determines a common EAS/DNAI is implementation.

6.2.3.3 EAS Re-discovery Procedure at Edge Relocation

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.

For PDU Session with Session Breakout connectivity, the UE may indicate its support for refreshing stale EAS information to the SMF during the PDU Session Establishment procedure or, when the UE moves from EPS to 5GS for the first time, by using the PDU Session Modification procedure. If the UE indicates such support, the SMF may send to the UE the EAS rediscovery indication, with an optional impact field, so that the UE may trigger to re-discover the EAS (see the step 2 of Figure 6.2.3.3-1) after the insertion/change/removal of an L-PSA based on AF influence or its local configuration using the PDU Session Modification procedure, or based on the AF triggered EAS relocation.

This procedure is used by the SMF to trigger the EAS rediscovery procedure when a new connection to EAS need to be established. It applies to both Session Breakout using ULCL and Session Breakout using BP.

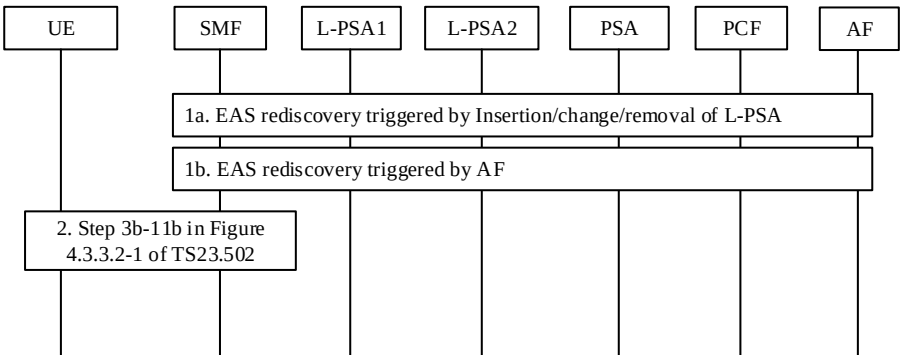

Figure 6.2.3.3-1: EAS re-discovery procedure at Edge relocation

During a previous EAS Discovery procedure on this PDU Session the UE may have EAS information (i.e. EAS IP address corresponding to an EAS FQDN) locally stored, e.g. acquired during the previous connection with the EAS (for more information see Annex C UE considerations for EAS (re)discovery).

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

The L-PSA insertion, change or removal for the PDU Session may be triggered due to update of a common DNAI.

1b. The AF triggers EAS relocation e.g. due to EAS load balance or maintenance, etc. and informs the SMF the related information indicating the EAS relocation, as described in clause 4.3.6 AF influence on traffic routing procedure in TS 23.502 [3].

AF may request to add/remove a UE to/from a set of UEs via AF influence on traffic routing procedure in TS 23.502 [3]. The PCF updates PCC rule to SMF (i.e. adding/removal of EAS Correlation indication/indication of traffic correlation and Traffic Correlation ID to/from the PCC rule). With the update of the PCC rule, the SMF detects that the UE is belonging to a set of UE(s) for a common EAS/DNAI, or the UE is not belonging to a set of UEs for common EAS/DNAI any longer and the common EAS/DNAI is not optimized for the UE, it may trigger EAS rediscovery.

If UE is belonging to a set of UE(s) for a common EAS/DNAI as instructed by the PCC rule, the SMF interacts with NEF for common EAS/DNAI selection as described in clauses 6.2.3.2.5 and 6.2.3.2.6.

2. This step may be performed as part of step 1a/1b. The SMF performs the network requested PDU Session Modification procedure from the step 3b-11b as defined in clause 4.3.3.2 TS 23.502 [3].

If the UE has indicated that it supports to refresh EAS information stored locally corresponding to the impact field per the EAS rediscovery indication from network, the SMF may send the impact field with the EAS rediscovery indication. SMF determines the impacted EAS(s) which need be rediscovered as the following:

- If an L-PSA is inserted/relocated/removed, the SMF determines the impact field, which is associated with the L-DN to be inserted, relocated or removed and identified by FQDN(s) or IP address range(s) of the old EAS, based on the association between FQDN(s)/IP address range(s) and DNAI provided by AF or SMF local configuration on the L-DN.

- For AF triggered EAS rediscovery, the AF may indicate the EAS rediscovery for the impacted applications, which are identified by Application Identifier(s), to the SMF via the AF influence on traffic routing procedure.

The SMF sends PDU Session Modification Command (EAS rediscovery indication, [impact field]) to UE. The EAS rediscovery indication indicates to refresh the cached EAS information. The impact field is used to identify which EAS(s) information need to be refreshed. The impact field includes the L-DN information corresponding to the impacted EAS(s), which are identified by FQDN(s) or IP address range(s) of the old EAS(s). If the impact field is not included, it means all EAS(s) information associated with this PDU Session need to be refreshed.

The SMF may choose new DNS settings for the PDU Session and if so, it provides them to the UE as new DNS server (see Option C in clause 6.2.3.2.3). Otherwise the UE uses the existing DNS server for EAS rediscovery.

For the following connection with the EAS(s) for which the EAS rediscovery needs to be executed per the received EAS rediscovery indication and impact field, the UE has been instructed not to use the old EAS information stored locally. Instead it should trigger EAS discovery procedure to get new EAS information as defined in clause 6.2.3.2.

For the Split-UE, it is not possible to provide the NAS level EAS rediscovery indication and the impact field to the TE. Annex C documents mitigations for this scenario.

NOTE 1: In case of EAS IP Replacement (see 6.3.3.1) the support for EAS rediscovery indication procedure is not required.

NOTE 2: Depending on the UE implementation, the EAS rediscovery indication triggers an EAS Rediscovery procedure. If the EAS rediscovery indication is not sent to the UE Application Layer or to the UE OS, then the DNS Query to discover a new EAS is triggered only if the IP flows are terminated or via application/OS implementation means, e.g. based on application redirection, other application server information or DNS cache time-to-live. If DNS cache has not expired in the Application Layer or the OS, the triggered re-discovery can lead to the old EAS. For more information see Annex C.

NOTE 3: The active connection(s) between the UE and the EAS(s) are not impacted.

6.2.3.4 EAS Deployment Information Management

6.2.3.4.1 General

EAS Deployment Information management refers to the capability to create, update or remove EAS Deployment Information from AF and the distribution to the SMF. The NEF is in charge of the management of EAS Deployment Information which may be stored in UDR.

The EAS Deployment Information indicates how edge services are deployed in each Local part of the DN, the description of EAS Deployment Information is shown in Table 6.2.3.4-1.

Table 6.2.3.4-1 Description of EAS Deployment Information

Parameters	Description
AF ID	Addressing information of Application Function responsible for the DNAI in the record. [Optional]. See NOTE 1.
DNN	DNN for the EAS Deployment Information. [optional]
S-NSSAI	S-NSSAI for the EAS Deployment Information. [optional]
External Group Identifier/Internal Group Identifier	Group ID for the EAS Deployment information. [optional]. See NOTE 2.
Application ID	Identifies the application for which the EAS Deployment Information corresponds to. [optional]
FQDN(s)	Supported FQDN(s) for application(s) deployed in the Local part of the DN.
DNAI(s)	DNAI(s) for the EAS Deployment information. [optional]
DNS Server Information	list of DNS server identifier (consisting of IP address and port) for each DNAI. [optional]
EAS IP address range Information	IP address(es) of the EASs in the Local part of the DN or the IP address ranges (IPv4 subnetwork(s) and/or IPv6 prefix(es) of the Local part of the DN where the EAS is deployed for each DNAI. [optional]
N6 traffic routing information	Information about how to forward edge traffic in the local part of DN corresponding to DNAI. [optional]
NOTE 1: When an AF ID is provided, all DNAI(s) correspond to the same EHE provider. NOTE 2: The AF may provide External Group Identifier, and NEF can map the External Group Identifier into Internal Group Identifier according to information received from UDM. For HR-SBO roaming scenario, External Group Identifier and Internal Group Identifier, cannot be used by AF in VPLMN. NOTE 3: AF ID can be used in case of AF(s) involving different EHE providers, and the source EHE is unaware of other/target EHE specific deployment details.	

The EAS Deployment Information management procedures are described in this clause, the procedures are independent of any PDU Session, including:

- The procedure for EAS Deployment Information management from AF via the NEF.
- The procedure for EAS Deployment Information management in the SMF.

- The procedure for BaselineDNSPattern management in the EASDF.

NOTE: In order to support EAS discovery when the Edge Hosting Environment is provided by a partner, an SLA is needed between current operator and the partner to provide e.g. the Address(es) and credentials for the DNS servers if the partner hosts the DNS server(s) for the related DNS resolution.

6.2.3.4.2 EAS Deployment Information Provision from AF via NEF

The AF provides non-PDU Session specific EAS Deployment information to 5GC via the procedure defined in this clause.

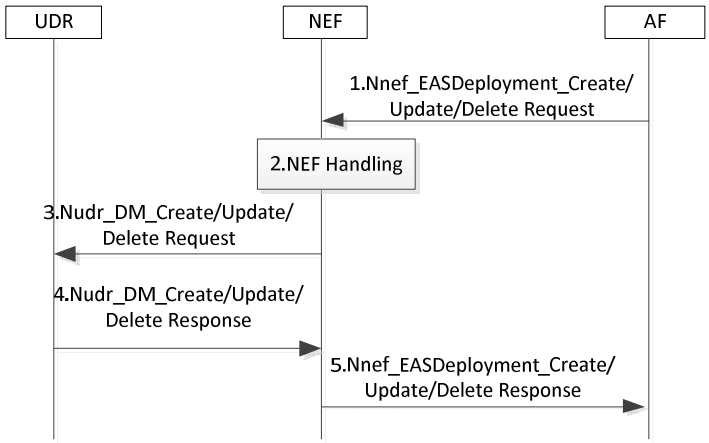

Figure 6.2.3.4.2-1 EAS Deployment Information management in the AF procedure

1. The AF invokes the Nnef_EASDeployment_Create/Update/Delete service operation.
2. NEF checks whether the AF is authorized to perform the request, and authorised to provision the EAS Deployment Information based on the operator policies. The NEF derives DNN and S-NSSAI from the AF Service Identifier if not received explicitly and translates received External Application Identifier to Application Identifier known inside MNO domain. If there is an existing EAS address information for a DNAI configured via OAM, NEF also ensures that any EAS IP address range Information per DNAI in EAS Deployment Information does not contradict with the existing information.
3. The NEF invokes the Nudr_DM_Create/Update/Delete to the UDR if it is authorized.
4. The UDR stores/updates/removes the corresponding information (and responds a Nudr_DM_Create/Update/Delete Response to the NEF.
5. The NEF sends Nnef_EASDeployment_Create/Update/Delete Response to the AF.

6.2.3.4.3 EAS Deployment Information Management in the SMF

The SMF may receive the EAS Deployment Information from NEF via Subscribe /Notify procedure defined in this clause. NEF may have stored the information in UDR.

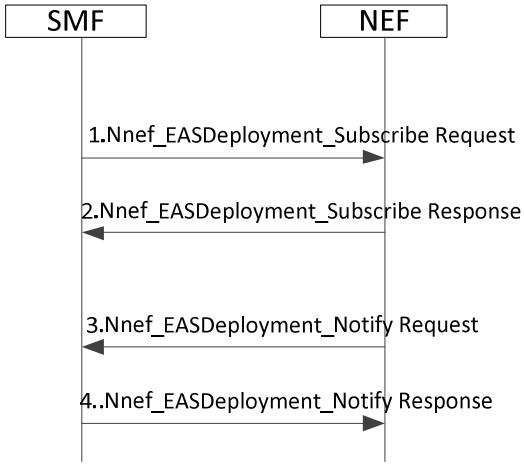

Figure 6.2.3.4.3-1: EAS Deployment Information management in the SMF procedure

1-2. As pre-requisite condition, the SMF subscribes to EAS Deployment Information Change Notification from the NEF by sending Nnef_EASDeployment_Subscribe message. The SMF may indicate that the current status of EAS Deployment Information shall be notified immediately (if available). The SMF may indicate for which (list of) DNN and/or S-NSSAI and/or application identifier and/or Internal Group Identifier (if available) it subscribes.

3-4. The NEF invokes Nnef_EASDeployment_Notify (EAS Deployment Information) to the SMF(s) to which the EAS Deployment Information shall be provided. If there is EAS Deployment Information available and immediate report is required, the NEF notifies the SMF(s) with such information.

6.2.3.4.4 BaselineDNSPattern Management in the EASDF

The SMF receives EAS Deployment Information as described in clause 6.2.3.4.1, and derives BaselineDNSPattern from the EAS Deployment Information. The BaselineDNSPattern is not dedicated to a specific PDU Session.

SMF may create/update/delete the BaselineDNSPattern in the EASDF.

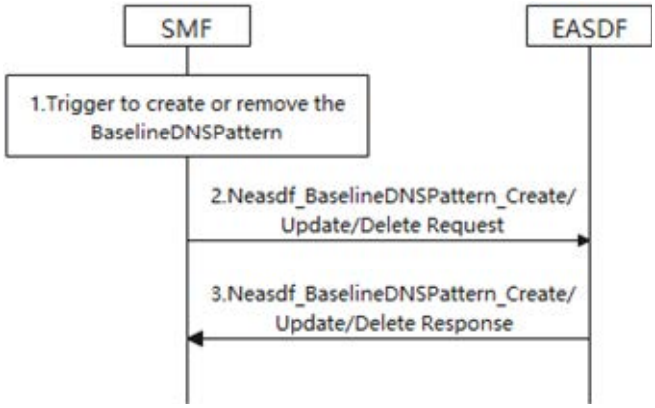

Figure 6.2.3.4.4-1: BaselineDNSPattern management in the EASDF procedure

1. The SMF may triggered to create/update/delete the BaselineDNSPattern.

   - When new EAS Deployment Information is received by the SMF.
   - When any update of the EAS Deployment Information is received by the SMF.

   The BaselineDNSPattern is deducted from the EAS Deployment Information. The BaselineDNSPattern has the form as per clause 6.2.3.2.2.

2. The SMF invokes Neasdf_BaselineDNSPattern_Create/Update/Delete service operation of the EASDF to create/update/delete the BaselineDNSPattern. This interaction with the EASDF is a node level procedure, i.e. independent of any PDU Session.

3. The EASDF updates the BaselineDNSPattern and acknowledges the SMF.

   For EAS Deployment Information management in HR-SBO roaming scenario, the SMF and EASDF in clause 6.2.3.4.4 are replaced by V-SMF and V-EASDF.

6.2.4 EDC Functionality based DNS Query to reach EASDF/DNS Resolver/DNS Server indicated by the SMF

In order to guarantee that the FQDN requested by the Application that intends to use EAS is resolved by the DNS Server (e.g. EASDF/DNS resolver) indicated by the SMF, the consumer in the UE uses the related EDC functionality to either:

1) Send a DNS Query to the DNS Server (e.g., EASDF/DNS resolver) indicated by the SMF.

   - The consumer in the UE provides to the EDC functionality the Domain Name to be resolved,
   - The EDC functionality shall send the DNS Query to the DNS Server (e.g., EASDF/DNS resolver) indicated by the SMF,
   - Once received, the EDC functionality shall forward the result of the DNS response (i.e., the IP address provided by the DNS resolver) to the consumer.

or:

2) Obtain the IP address of the DNS Server (e.g., EASDF/DNS resolver) indicated by the SMF (Optional).

   - The consumer in the UE requests the IP address of the DNS Server (e.g. EASDF/DNS resolver) indicated by the SMF. The EDC functionality shall send to the consumer in the UE the IP address of the DNS Server (e.g. EASDF/DNS resolver) or/and it shall notify the consumer in the UE of any update;
   - The consumer in the UE then generates and sends a DNS Query to the DNS Server (e.g. EASDF/DNS resolver) indicated via EDC functionality by the SMF.

6.3 Edge Relocation

6.3.1 General

Edge Relocation refers to the procedures supporting EAS changes and/or PSA UPF relocation.

Edge Relocation may be triggered by an AF request (e.g. due to the load balance between EAS instances in the EHE) or by the network (e.g. due to the UE mobility).

With Edge Relocation, the user plane path may be re-configured to keep it optimized. This may be done by PDU Session re-establishment using SSC mode 2/3 mechanisms or Local PSA UPF relocation using UL CL and BP mechanisms. The corresponding procedures are defined in TS 23.501 [2] and TS 23.502 [3].

Due to Edge Relocation, the UE may need to re-discover a new EAS and establish the connectivity to the new EAS to continue the service. The re-discovery of EAS is specified in clause 6.2.

Edge Relocation may result in AF relocation, for example, as part of initial PDU Session Establishment, a central AF may be involved. However, due to Edge Relocation another AF serving the Edge Applications is selected.

The trigger of Edge Relocation by the network is specified in clause 4.3.6.3 of TS 23.502 [3]. Some EAS (re-)Discovery procedures in clause 6.2 may also trigger Edge Relocation.

This clause further describes the following procedures:

- Edge Relocation involving AF change.
- Edge Relocation using EAS IP replacement.
- AF request for simultaneous connectivity for source and target PSA.

- Packet buffering for low Packet Loss.
- Edge Relocation considering User Plane Latency Requirements.
- Edge Relocation triggered by AF
- Edge Relocation for a set of UEs for common DNAI.

Annex F describes example procedure for EAS Relocation on Release 16 capabilities.

For non-roaming PDU Session, the 5GC functions in the following clauses are located in the HPLMN.

For LBO roaming PDU Session, the 5GC functions in the following clauses are located in the serving VPLMN.

For HR-SBO PDU Sessions specified in clause 6.7, the AF may send to V-NEF an AF request to influence traffic routing as described in clause 4.3.6 of TS 23.502 [3] for supporting Edge Relocation (e.g. for the purpose of subscription to UP path management events, especially for the change of local PSA UPF in VPLMN). In this case, the steps involving PCF in the following clauses are skipped.

6.3.2 Edge Relocation Involving AF Change

This clause is related to scenarios where distributed Edge Application Server (EAS) deployed in local part of a Data Network or a central AS are relocated, and where the (E)AS relocation also implies AF relocation i.e. AF instance change.

Application Function influence on traffic routing mechanism as described in clause 5.6.7 of TS 23.501 [2] can be applied for a relocation of the AF. In the case that AF sends AF request via NEF, the target AF may invoke Nnef_TrafficInfluence_Create to deliver the relocation related information, including notification target address based on the procedure described in clause 4.3.6.2 of TS 23.502 [3]. Also, the source AF or target AF may invoke Nnef_TrafficInfluence_Update service operation to deliver the relocation information, including AF ID and notification target address based on the procedure described in clause 4.3.6.2 of TS 23.502 [3].

Also if the AF relocation occurs during the early/late notification procedure described in clause 4.3.6.3 of TS 23.502 [3], the target AF invokes Nnef_TrafficIfluence_Create/Update at step 4e-a or Npcf_PolicyAuthorization_Create at step 4g-a to deliver the notification target address of the AF. In the case that AF directly interacts with PCF, the target AF may invoke Npcf_PolicyAuthorization _Create, or the source AF/target AF may invoke Npcf_PolicyAuthorization _Update service operation to deliver relocation information including notification target address based on the procedure described in clause 4.3.6.4 of TS 23.502 [3].

In the case of Edge relocation between two DNAI(s), an AF relocation may be triggered by SMF, e.g. due to UE mobility. In such cases, the SMF provides as described in clause 4.3.6.3 of TS 23.502 [3] during early/late notification procedure the source AF with target AF ID as defined in Table 6.2.3.4-1. Target AF ID is used by source AF to communicate with the target AF.

6.3.3 Edge Relocation Using EAS IP Replacement

EAS IP replacement enables the Local PSA UPF to replace the source/old Target EAS IP address and port number with the target/new target EAS IP address and port number for the Destination IP address and Destination Port number field of the uplink traffic and replace the target/new target EAS IP address and port number with the source/old Target EAS IP address and port number for the Source IP address and Source Port number field of the downlink traffic based on the enhanced AF Influence information for EAS IP replacement (i.e. source EAS IP address and port number, target EAS IP address and port number). The source AS IP address and port number are the destination IP address and port number of the uplink traffic, generated by UE, for a service subject to Edge Computing. The source EAS IP address is the one discovered by UE for a service subject to Edge Computing.

To support Edge Relocation using EAS IP address and Port number replacement, in this clause the SMF shall instruct the UPF to use the FAR that contains Information elements of "IP Address and Port Number Replacement".

EAS IP replacement requires support of TCP/TLS/QUIC context transfer between EASs.

NOTE: The feasibility of this requirement, i.e. TCP/TLS/QUIC context transfer between EASs, depends on whether third party platforms support an individual real time TCP/TLS/QUIC context transfer between EASs.

6.3.3.1 EAS IP Replacement Procedures

6.3.3.1.1 Enabling EAS IP Replacement Procedure by AF

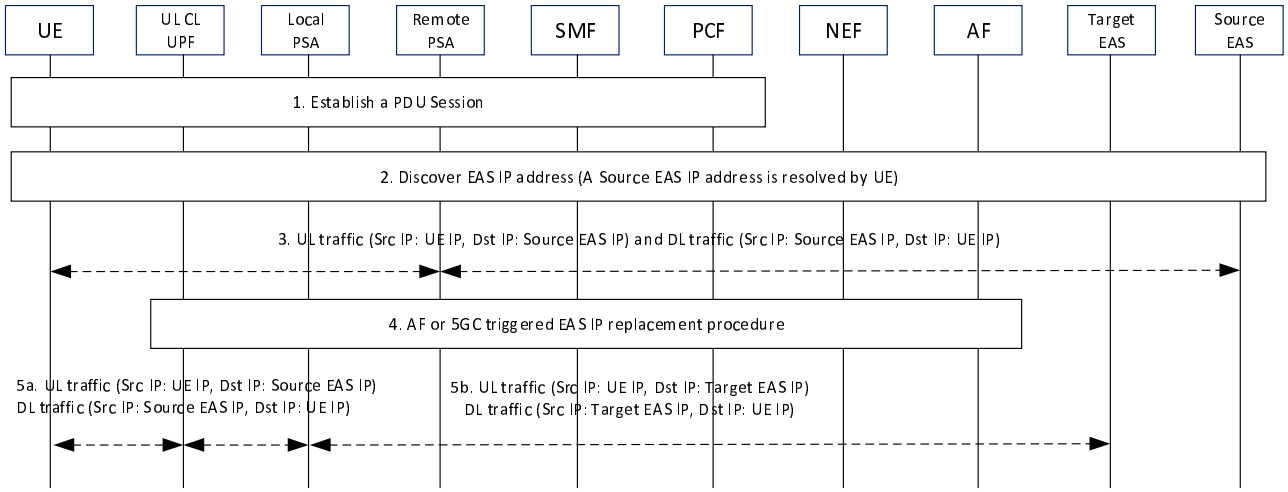

Figure 6.3.3.1.1-1: Enabling EAS IP replacement procedure by AF

NOTE 1: This procedure covers the scenarios that the UE moves from non-EC to EC or the AF decides to enable the EAS IP replacement in the middle of a session.

1. UE requests to establish a PDU Session.

2. UE is preconfigured with the Source EAS IP address or discovers the IP address of the application server for the service subject to Edge Computing and the Source EAS IP address is returned to the UE via EAS Discovery procedure as described in clause 6.2.

3. UE communicates with the Source EAS.

4a. EAS Relocation may be triggered by AF (e.g. due to the load balance between EAS instances in the EHE). When AF detects that the EAS is capable of runtime context mirroring and an optimal EAS is found, then AF decides to influence the traffic routing in 5GC. For the common DNAI case, the AF may determine that there is an optimal common DNAI (i.e. target common DNAI). The AF may select Target EAS corresponding to the target common DNAI for each UE belonging to the set of UEs. The EAS IP replacement information (i.e. source EAS IP address and port number, target EAS IP address and port number) is sent to the SMF within the AF Influence information and the SMF reconfigures the UL CL UPF for local traffic routing and Local PSA with EAS IP replacement information.

UL CL is configured by SMF to forward UL packet to Local PSA if the destination IP address is the Source EAS IP address.

Local PSA is configured by SMF to enforce the FAR as described in step 5.

Detailed enhancement to the AF Influence procedure is described in clause 6.3.3.2.

If a new Local PSA is selected by SMF, the SMF may configure the new Local PSA to buffer the uplink traffic per clause 6.3.5 and enforce the "Outer Header Creation" and "Outer Header Removal" as described in step 5.

If AF is not notified by 5GC that the 5GC supports EAS IP replacement mechanism, the AF does not include the target EAS identifier and does not initiate the AF triggered EAS IP replacement procedure.

If the 5GC does not support EAS IP replacement capability, the SMF should reject the AF request and step 5 is skipped.

4b. EAS Relocation may be also triggered by 5GC (e.g. due to UE Mobility). For the common DNAI case, a SMF may determine that there is an optimal common DNAI (i.e. target common DNAI). If target common DNAI is not available, the SMF determines Target Common DNAI.. The SMF selects the common DNAI according to clause 6.2.3.2.4. When Early/Late Notification procedure with enhancement described in clause 6.3.3.2 is triggered, the SMF notifies AF about the target DNAI or target common DNAI and may provide the capability

of supporting EAS IP replacement in 5GC. Based on the target DNAI or target common DNAI, the AF selects a proper target EAS, then the AF triggers to mirror the runtime context between Source EAS and Target EAS. Once the Target EAS is ready, AF responds to SMF about the EAS IP replacement information. During the addition or change of UL CL and Local PSA as described in clause 4.3.5.4, 4.3.5.6 or 4.3.5.7 of TS 23.502 [3], SMF may (re)configure Local PSA for EAS IP address replacement between Source EAS and Target EAS.

5. Local PSA starts to perform FARs as instructed by SMF, which results in EAS IP address replacement:

   - For UL traffic, the destination IP address and port number are replaced with the Target EAS IP address and port number;

   - For DL traffic, the source IP address and port number are replaced back with the Source EAS IP address and port number.

NOTE 2: In this solution, the PSA UPF need not to understand the logic of EAS IP replacement.

Then all subsequent uplink traffic of this EC service for this UE is forwarded to the target EAS.

NOTE 3: AF decides when and how to stop the Source EAS from serving the UE based on its local configuration.

6.3.3.1.2 EAS IP Replacement Update upon DNAI and EAS IP Change

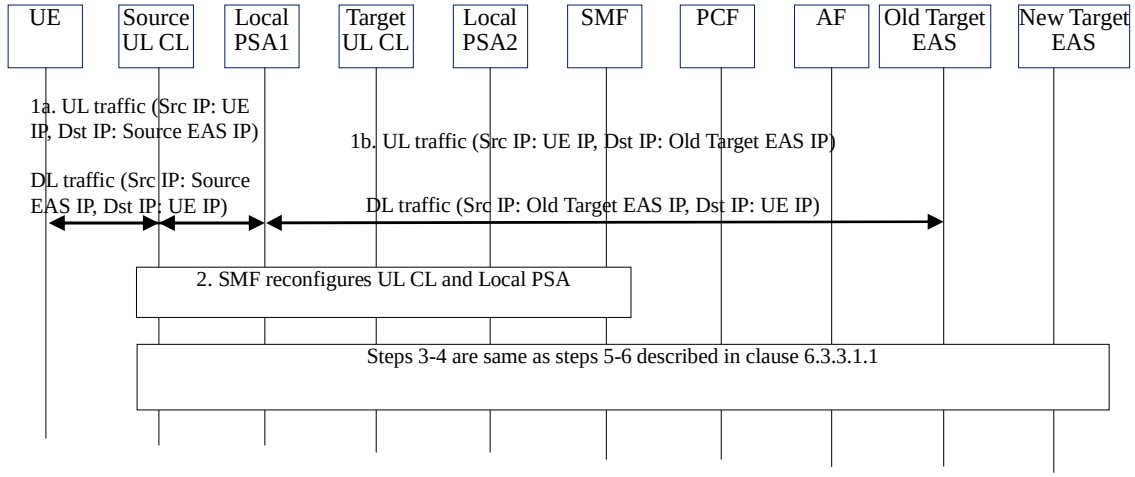

Figure 6.3.3.1.2-1: EAS IP replacement update upon DNAI and EAS IP change

1. For UL traffic, the destination IP address is replaced with the old Target EAS IP address at Local PSA; for DL traffic, the source IP address is replaced back with the Source EAS IP address at Local PSA.

2. SMF configures Target UL CL with forwarding rules and Local PSA2 with FARs, as described in step 4 of clause 6.3.3.1.1.

Steps 3-4 are same as steps 5-6 described in clause 6.3.3.1.1 except that the UL CL, Local PSA and Target EAS in clause 6.3.3.1.1 are replaced by Target UL CL, Local PSA2 and new Target EAS respectively.

6.3.3.1.3 Disabling EAS IP Replacement Procedure

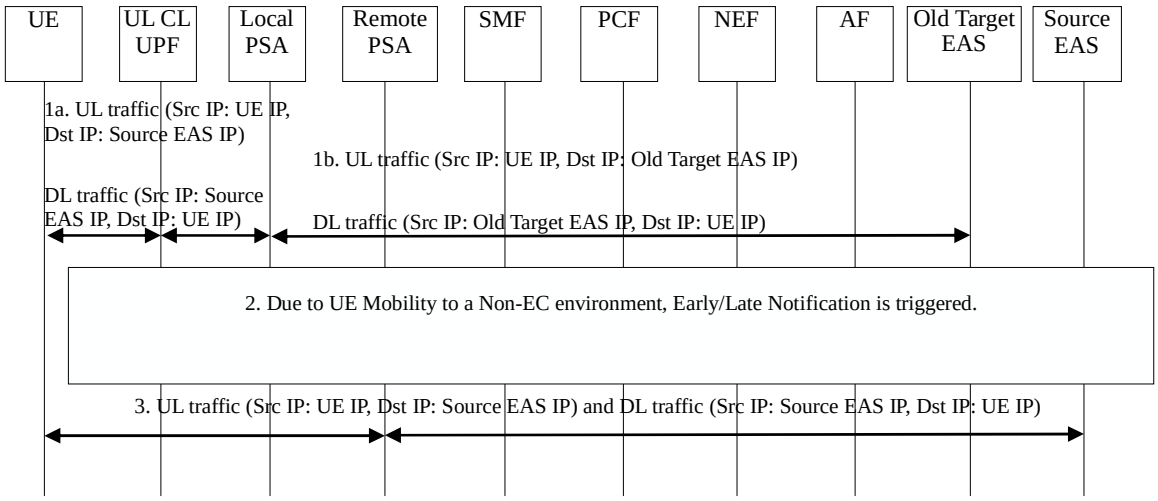

Figure 6.3.3.1.3-1: Disabling EAS IP replacement procedure

1. Local PSA performs FARs as instructed by SMF, which results in EAS IP address replacement:

   - For UL traffic, the destination IP address and port number are replaced with the old Target EAS IP address and port number;

   - For DL traffic, the source IP address and port number are replaced back with the Source EAS IP address and port number.

2. Due to UE Mobility to a Non-EC environment, when Early/Late Notification is triggered for the change from the UP path status where a DNAI applies to a status where no DNAI applies, AF knows the UE moves out of EC environment and mirrors the runtime session context from old Target EAS to Source EAS. Once ready, the AF indicates SMF without providing source/target EAS IP addresses and port numbers, so the SMF disables the local routing at UL CL and the EAS IP replacement at Local PSA for this PDU Session.

3. UL and DL traffic goes through Remote PSA, no EAS IP address replacement happens at Remote PSA.

NOTE 1: AF decides when and how to stop the old Target EAS from serving the UE based on its local configuration. In case of AF relocation, AF doesn't have to disable the EAS IP Replacement in 5GC.

6.3.3.2 Enhancement to AF Influence

The AF may additionally include Source and Target EAS IP address(es) and Port number(s) in the Nnef_TrafficInfluence_Create/Update or Nnef_TrafficInfluence_AppRelocationInfo or Nsmf_EventExposure_AppRelocationInfo request. Based on the Source EAS IP address(es) and Port number(s), the SMF knows which service flow(s) is(are) subject to EAS IP Replacement.

Using Early/Late Notification procedure, the SMF may notify the AF about the capability of supporting EAS IP replacement in 5GC, the AF sends an/a early/late notification response to the SMF when EAS relocation is completed. The SMF sends the FARs to (target) Local PSA UPF and (target) Local PSA UPF starts the EAS IP address replacement as described in clause 6.3.3.1.

For load balancing purpose, the AF may move some UE(s) from the old Target EAS to the New Target EAS in the same L-DN identified by the DNAI. For the abnormal condition of EAS, the AF may move all the UEs being served by the source EAS to a target EAS in the same L-DN. For those purposes, the AF needs to include List of UEs, the source/old Target EAS IP address and port number for the impacted DNAI, the (new) Target EAS IP address and port number for the impacted DNAI in the Nnef_TrafficInfluence_Create/Update request. If 5GC does not support EAS IP replacement capability, the SMF should reject this AF request.

The additional parameters for enabling the EAS IP Replacement are defined in clause 5.6.7.1 of TS 23.501 [2] and clauses 4.3.6.3 and 4.3.6.4 of TS 23.502 [3].

6.3.4 AF Request for Simultaneous Connectivity over Source and Target PSA at Edge Relocation

EAS relocation can make use of network capabilities that, at PSA change, provide simultaneous connectivity over the source and the target PSA during a transient period. This is described in Annex F.

AF may issue a request to the network on whether to provide simultaneous connectivity over the source and the target PSA at edge relocation. This may trigger the SMF to use a re-anchoring procedure that provides simultaneous connectivity over the source and target PSA, as described in TS 23.502 [3]:

- For Session Breakout, in clause 4.3.5.7 for Simultaneous change of Branching Point or UL CL and additional PSA for a PDU Session. This could involve the establishment of a temporary N9 forwarding tunnel between the source UL CL and target UL CL.

The AF request may include the following information:

- "Keep existing PSA" indication: If this indication is included, the SMF may decide to use a re-anchoring procedure that provides simultaneous connectivity over the source and target PSA, as described above.

- "Keep existing PSA timer": its value indicates the minimum time interval to be considered for inactivity for the traffic described. It may overwrite the SMF configurable period of time for how long the existing PSA is to be maintained after all active traffic ceases to flow on it.

AF traffic influence request via NEF is described in clause 5.2.6.7 of TS 23.502 [3]. The request to PCF is described in clauses 5.2.5.3.2 and 5.2.5.3.3 of TS 23.502 [3].

Once the simultaneous connectivity over the source and the target PSA at relocation requested by AF is authorized by the NEF, the AF request including the requirements is informed to the SMF via AF influenced Traffic Steering Enforcement Control (see clause 6.3.1 of TS 23.503 [4]) in PCC rules.

If SMF determines that simultaneous connectivity over the source and the target PSA at relocation is not possible (e.g. the PDU Session is neither session breakout nor SSC mode 3) while it is requested, the SMF issues a failure notification towards the AF.

6.3.5 Packet Buffering for Low Packet Loss

This procedure aims at synchronizing between EAS relocation and UL traffic from the UE, ensuring that UL traffic from the UE is sent to the new EAS only when EAS context transfer has been carried out.

This procedure may be applied at change of local PSA. It consists of buffering uplink packets in the target PSA in order to prevent there is packet loss if the application client sends UL packets to a new EAS before the new EAS is prepared to handle them. During the buffering, the old EAS may continue to serve the UE over the former PSA.

Buffering starts upon request by AF and continues till AF indicates otherwise. The EAS relocation procedure (e.g. the migration of the service context) happens at the application layer. That is outside the scope of 3GPP.

As an alternative to this procedure, upper layer solutions can provide the needed synchronization between EAS relocation and UL traffic from the UE.

NOTE 1: Upper layer solutions may still be needed when there are other EAS relocation scenarios (e.g. EAS (re)selection upon DNS cache entry expiry) not related to PSA change.

Buffering of uplink packets is not meant to apply to all traffic being offloaded at the new PSA. AF may request the buffering for the UL traffic of applications that require so. When the AF subscribes Early/Late Notification of UP path change for a specific application, Traffic Description for this application is provided as described in clause 5.6.7 of TS 23.501 [2]. When AF receives such an Early/Late Notification and indicates that uplink traffic buffering is needed in the response (step 2 in Figure 6.3.5-1), this uplink traffic buffering is then activated for the traffic described by Traffic Description provided in the subscription to Early/Late Notification.

NOTE 2: To request uplink traffic buffering, the AF is expected to subscribe both Early and Late Notifications.

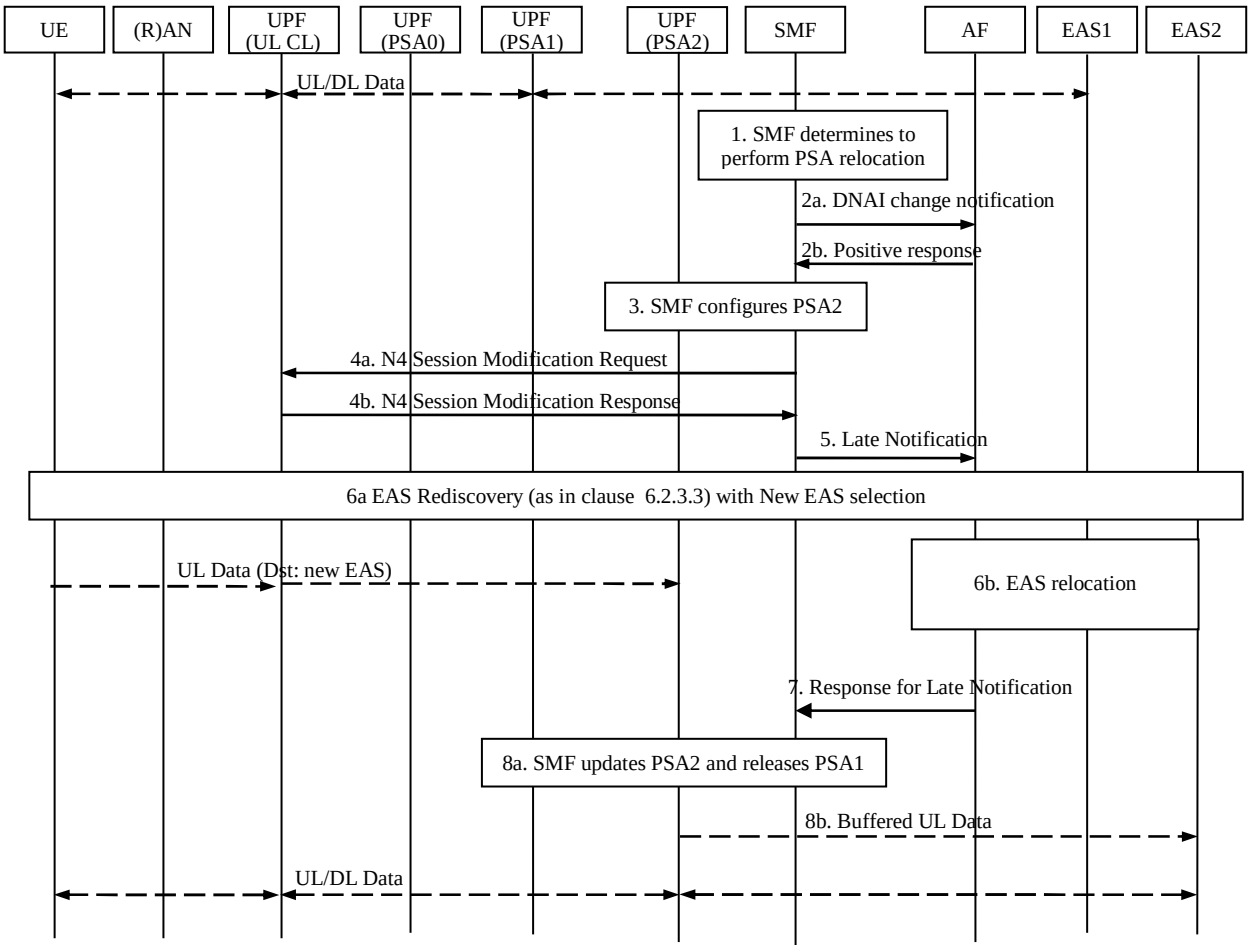

Figure 6.3.5-1: Packet buffering for low packet loss

1. The SMF decides to change the local PSA of a PDU Session with UL CL or SSC mode 3.

2. The SMF may send an early notification to the AF after target PSA (i.e. PSA2) is selected and waits for a notification response from the AF. The AF may reply in positive to the notification by indicating that buffering of uplink traffic to the target DNAI is needed as long as traffic to the target DNAI is not authorized by the AF. This is e.g. as defined in steps 1 and 2 of TS 23.502 [3] Figure 4.3.6.3-1.

3. For the procedures with ULCL/BP, the SMF configures the PSA2 as specified in step 2 in clause 4.3.5.6 and step 2 in clause 4.3.5.7 of TS 23.502 [3], which may request the PSA2 to buffer uplink traffic. The PSA1 (i.e. source PSA) keeps receiving downlink traffic from EAS1 and send it to the UE until it is released in step 7.

   For the procedures with SSC mode 3, the SMF configures the PSA2 as specified in step 4 in clause 4.3.5.2 and in step 5-6 in clause 4.3.5.4 of TS 23.502 [3], which may request the PSA2 to buffer uplink traffic.

4. For the procedures with ULCL/BP, the SMF sends an N4 Session Modification Request to the UL CL to update the UL CL rules regarding to the traffic flows that the SMF tries to steer to PSA2. This is e.g. as defined in TS 23.502 [3] Figure 4.3.5.7-1 step 3.

5. The SMF sends a Late Notification to the AF. This corresponds e.g. to step 4a-c of TS 23.502 [3] Figure 4.3.6.3-1 and is e.g. also described in step 9 of TS 23.502 [3] Figure 4.3.5.7-1.

6a. A new EAS is selected by the application (e.g. at DNS cache entry expiry, the DNS Query is resolved and the response includes a new EAS that is near the new PSA (PSA2)). Any traffic sent to the new EAS is buffered at PSA2.

6b. The application layer completes the EAS relocation (This corresponds to step 4d of TS 23.502 [3] Figure 4.3.6.3-1). The UE context is completely relocated from the old EAS to new EAS. The old EAS stops to serve the UE

NOTE 3: Steps 6a and 6b are related which implies there is some sort of coordination at application layer that is outside of 3GPP scope.

7. When EAS relocation is completed, the AF sends a notification response to the SMF. This corresponds to step 4e-g of TS 23.502 [3] Figure 4.3.6.3-1(and is e.g. also described in step 6 or 7 of TS 23.502 [3] Figure 4.3.5.7-1) and may indicate that buffering of uplink traffic to the target DNAI is no more needed as traffic to the target DNAI /EAS is now authorized by the AF.

   If the AF is changed during EAS relocation, see the details indicated in clause 6.3.2.

8. (if AF has indicated that buffering of uplink traffic to the target DNAI is no more needed as traffic to the target DNAI /EAS is now authorized by the AF) The SMF updates the PSA2 by indicating the PSA2 to send the buffered uplink packets (step 8b) and to stop buffering.

   The SMF releases PSA1.

6.3.6 Edge Relocation Considering User Plane Latency Requirement

Edge relocation may be performed considering user plane latency requirements provided by the AF.

In a network deployment where the estimated user plane latency between the UE and the potential PSA-UPF is known to the SMF, the 5GC provides the enhancement of AF influence to consider the user plane latency requirements requested by the AF so that the SMF decides to relocate the PSA-UPF based on AF requested requirements.

The AF may provide user plane latency requirements to the network via AF traffic influence request as described in clause 5.2.6.7 of TS 23.502 [3]. The user plane latency requirements may include the following information:

- Maximum allowed user plane latency: The value of this information is the target user plane latency. The SMF may use this value to decide whether edge relocation is needed to ensure that the user plane latency does not exceed the value. The SMF may decide whether to relocate the PSA UPF to satisfy the user plane latency.

The AF request on the user plane latency requirements are authorized by PCF. The PCF checks whether the AF has an authority to make such a request.

Once the user plane latency requirements requested by AF is authorized by the PCF, the AF request including the requirements is informed to the SMF via AF influenced Traffic Steering Enforcement Control (see clause 6.3.1 of TS 23.503 [4]) in PCC rules. After receiving the user plane latency requirements from AF via PCF, the SMF may take appropriate actions to meet the requirements e.g. by reconfiguring the user plane of the PDU Session as described in the step 6 of Figure 4.3.6.2-1 in TS 23.502 [3] with the following considerations:

- In the case that the maximum allowed user plane latency is requested, the SMF decides not to perform PSA UPF relocation if the serving PSA satisfies the maximum allowed user plane latency. Otherwise, the SMF may decide to perform PSA UPF relocation if the target PSA UPF satisfies the maximum user plane latency. The SMF may select the PSA UPF with the shortest user plane latency among the PSA UPFs satisfying the maximum user plane latency requirements.

6.3.7 Edge Relocation Triggered by AF

The AF may invoke the AF request targeting an individual UE address procedure as described in clause 4.3.6.4 of TS 23.502 [3], due to EAS relocation. The EAS relocation may be due to AF internal triggers e.g. EAS load balance or maintenance, etc. or due to UP path change notification from SMF. The EAS relocation may include AF change or AF not change. The EAS relocation can happen with or without DNAI change. The AF may include the following information: Indication for EAS Relocation, target DNAI, traffic descriptor information and N6 routing information at target DNAI in the Nnef_TrafficInfluence_Create/Update Request to the NEF, or Npcf_PolicyAuthorization_Create/Update Request to the PCF. When the PCF receives an AF request for the same application, then the latest AF request message take precedence over any previous request if the traffic descriptor information is same.

The AF may invoke the AF request targeting a set of UEs as described in clause 4.3.6.2 of TS 23.502 [3], due to change of common EAS/common DNAI used by the set of UEs. Similar as the Edge relocation triggered by AF with target DNAI, the common DNAI is included instead of the target DNAI.

6.4 Network Exposure to Edge Application Server

6.4.1 General

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

NOTE 1: Local PSA UPF can expose the QoS monitoring results to local AF via N6. How to deliver the information on N6 is out of the scope of the present document.

NOTE 2: Sending QoS monitoring information that has not been properly integrated over time, i.e. with over-high frequency, can increase risk that the application may over-react to instantaneous radio events/conditions e.g. leading to service instability.

6.4.2 Network Exposure to Edge Application Server

6.4.2.1 Usage of Nupf_EventExposure to Report QoS Monitoring results

The UPF may be instructed to report information about a PDU Session directly i.e. bypassing the SMF and the PCF. This reporting may target an Edge Application Server (EAS) or a local AF that itself interfaces the EAS.

Local NEF deployed at the edge may be used to support network exposure with low latency to local AF. The local NEF may support one or more of the functionalities described in clause 6.2.5.0 of TS 23.501 [2]. and may support a subset of the APIs specified for capability exposure based on local policy. In order to support the network exposure locally, the local NEF shall support Nnef_AFSessionWithQoS service operation for the local AF. The local NEF selection by AF is described in clauses 6.2.5.0 and 6.3.14 of TS 23.501 [2].

The local AF subscribes the direct notification of QoS Monitoring results from the PCF via a local NEF or NEF. If the NEF detects that it is not the most suitable NEF instance to serve the local AF request, it may redirect the AF to a local NEF instance.

NOTE 1: If the notifications need to go via the local NEF, then the local NEF needs to be involved in order to be able to map these notifications to the URI where the AF expects to receive them.

The local AF may also use the Npcf_PolicyAuthorization_Create or Update service of the PCF directly. In this case, reporting is done directly from the UPF to the local AF.

Based on the indication of direct event notification and operator's policy, the PCF includes Direct event notification method and the Target of reporting (including target local NEF address or target AF address) within the PCC rule that it provides to the SMF as described in clause 6.1.3.21 of TS 23.503 [4].

The SMF sends the QoS monitoring request to the RAN and N4 rules to the L-PSA UPF. If the L-PSA UPF supports such reporting, N4 rules indicate that the QoS flow needs direct notification of QoS Monitoring. When QoS monitoring of GTP-U Path(s) is used, it is also activated if needed. This is as defined in clause 5.33.3 of TS 23.501 [2]. When N4 rules indicate that the QoS flow needs direct notification of QoS Monitoring results, upon the detection of the QoS monitoring event (e.g. when threshold for the packet delay of the QoS flow is reached as defined in clause 5.33.3 of TS 23.501 [2]), the L-PSA UPF notifies the QoS Monitoring event information to the AF (directly or via Local NEF). If the L-PSA UPF supports the Nupf_EventExposure_Notify service operation, as defined in clause 5.2.26 of TS 23.502 [3], the L-PSA UPF sends the Nupf_EventExposure_Notify to the Notification Target Address indicated by the Session Reporting Rule received from the SMF. The Notification Target Address may correspond to the AF or to a local NEF. When the Notification Target Address corresponds to a Local NEF, the local NEF reports the QoS Monitoring result to the AF.

During UE mobility, the SMF may trigger the L-PSA UPF relocation/reselection and then send the N4 rules to the new L-PSA UPF to indicate the QoS flow needs direct notification of QoS Monitoring. The UE mobility may also trigger AF relocation or local NEF reselection, then the local AF should update the subscription for local exposure with QoS monitoring results possibly via local NEF, towards the PCF. This updated /new subscription is then propagated via SMF (via PCC rule updates) and then to the L-PSA UPF via N4 rules.

NOTE 2: The new local AF can subscribe direct notification of QoS Monitoring if Edge Relocation Involving AF Change happens as described in clause 6.3.2.

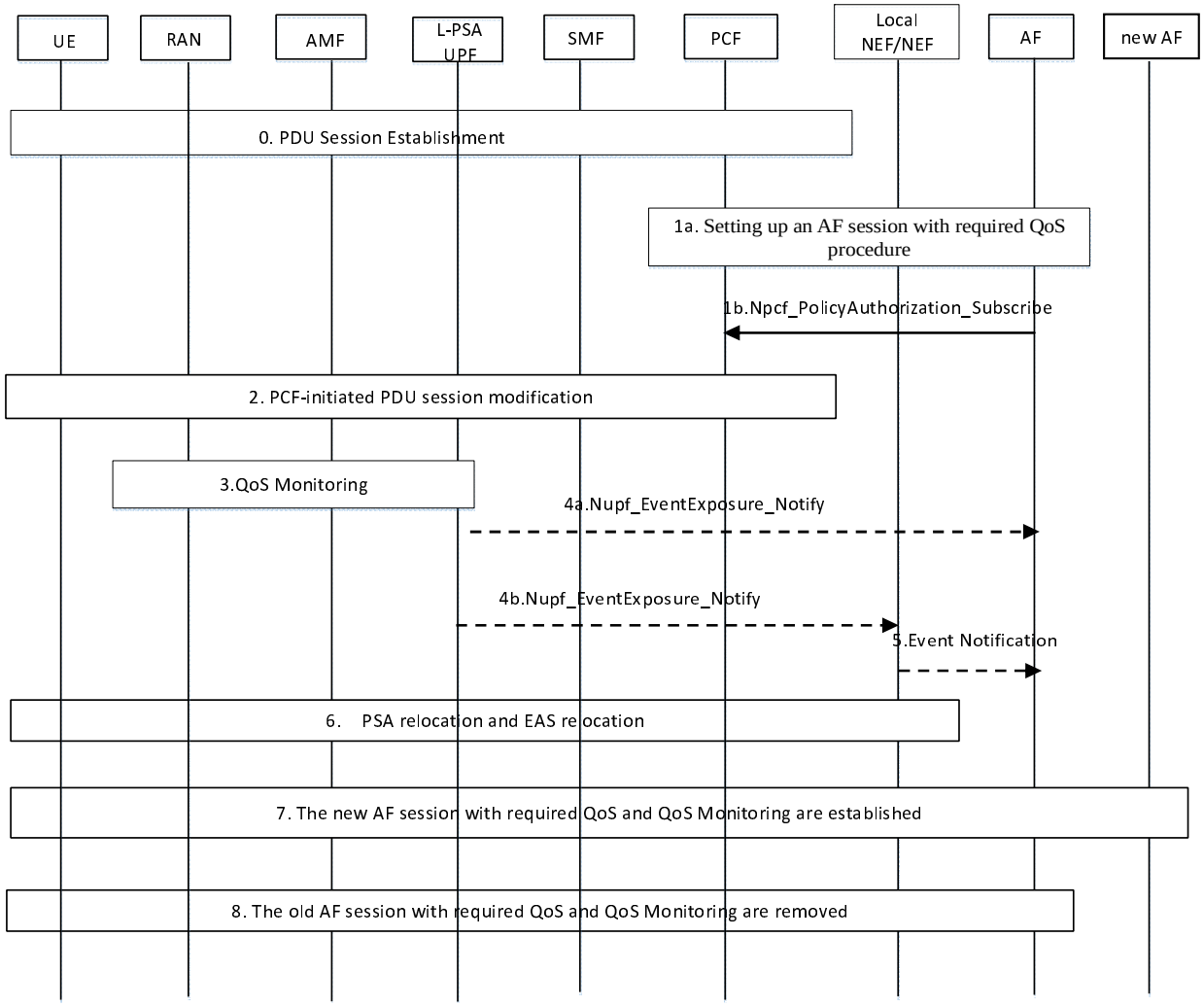

Figure 6.4.2.1-1: Network exposure to Edge Application Server

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

   In the request, the AF may subscribe to direct notification of QoS monitoring results for the service data flow to PCF possibly via Local NEF or NEF. If so, the AF shall include the corresponding QoS monitoring parameters as defined in clause 6.1.3.21 of TS 23.503 [4] and in TS 23.502 [3].

   The AF may also first initiate an AF Session with PCF and later subscribe to direct notification of QoS monitoring to PCF by invoking Npcf_PolicyAuthorization_Update service operation.

   The local AF or NEF may discover a local NEF as specified in clause 6.2.5.0 of TS 23.501 [2] and using parameters as specified in clause 6.3.14. Alternatively, if the NEF detects that it is not the most suitable NEF instance to serve the local AF request, the NEF may redirect the AF to a (more) local NEF. The NEF may use information on the L-PSA UPF for this determination.

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 [3], steps 1b, 3b, 4-8b.

   If the direct notification of QoS monitoring results is subscribed, the PCF includes the Direct event notification method and the Target of reporting (including target local NEF or local AF address) in the PCC rule of the service data flow as described in clause 6.1.3.21 of TS 23.503 [4].

If the SMF receives the Direct event notification form the PCF and the SMF determines that the L-PSA UPF supports such reporting, the SMF determines the QoS monitoring parameters based on the information received from the PCF and/or local configuration and provides them to the L-PSA UPF via N4 rules as described in clause 5.33.3.1 of TS 23.501 [2]. Otherwise the SMF activates N4 reporting for the QoS monitoring results. The PCF may determine that the duplicated notification is required, i.e. both, direct notification to the AF (i.e. sent from UPF) and notification sent to the PCF/SMF is required and indicate it to the SMF using the Direct event notification method in the PCC rule as described in clause 6.1.3.21 of TS 23.503 [4]. In this case, the SMF shall activate the N4 reporting together with the direct reporting to the local NEF/AF.

NOTE 2: The details of the parameters for the control of the QoS monitoring as well as the PCF and SMF behaviour are described in clause 6.1.3.21 of TS 23.503 [4] and in clause 5.33.3.1 of TS 23.501 [2], respectively.

3. The L-PSA UPF obtains QoS monitoring information as defined in clause 5.33.3 of TS 23.501 [2].

4. The L-PSA UPF sends the notification related with QoS monitoring information over Nupf_EventExposure_Notify service operation. The notification is sent to Notification Target Address that may correspond (4a) to the local AF or (4b) to the local NEF.

5. If Local NEF is used, it reports the real-time network information to local AF by invoking Nnef_EventExposure_Notify service operation.

6. Due to e.g. UE mobility, the PSA relocation and/or EAS relocation may happen as described in clause 6.3. During the PSA and/or EAS relocation (if the event was subscribed e.g. as in step 1), the SMF notifies the (local) NEF or the AF with the PSA and/or EAS relocation, and the AF may trigger a new L-NEF discovery as in step 1. During this step, the application mechanisms may involve a new AF for this session.

7. The new AF may initiate a new AF session to (re-)subscribe the direct notification of QoS monitoring as described in steps 1-4.

8. The old AF revokes the AF session.

NOTE 3: Step 8 can take place before step 7.

6.4.2.2 Local NEF Discovery

As specified in clause 6.2.5.0 of TS 23.501 [2], the NRF may be used by the AF to discover the L-NEF. To become discoverable, the L-NEF registers with an NRF deployed within the operator's domain where the AF resides.

The AF uses existing procedures as described in clause 4.17.4 of TS 23.502 [3] to discover the L-NEF. If the AF only knows the NEF and it initiates a Nnef_AFSessionWithQoS_Create/Update_request procedure with an indication of direct event notification as described in clause 6.4.2.1 and clause 6.1.3.21 of TS 23.503 [4], the NEF may decide that it is not suitable for local exposure, and re-direct the request to an L-NEF as described in TS 29.500 [9]. NEF may use NRF to find a suitable L-NEF for the re-direction.

6.5 Support of 3GPP Application Layer Architecture for Enabling Edge Computing

6.5.1 General

The 3GPP application layer architecture for Enabling Edge Computing that is specified in TS 23.558 [5] includes the following functional entities:

- Edge Enabler Client (EEC).
- Edge Configuration Server (ECS).
- Edge Enabler Server (EES).

A UE may host EEC(s) as defined in TS 23.558 [5] and support the ability to receive ECS address(es) from the 5GC and to transfer the ECS address(es) to the EEC(s). In this case, the ECS address provisioning via 5GC is described in clause 6.5.2.

NOTE: The features described in the other clauses of this specification do not require the UE and the network to support the 3GPP application layer architecture for Enabling Edge Computing that is specified in TS 23.558 [5].

6.5.2 ECS Address Provisioning

6.5.2.1 ECS Address Configuration Information

The ECS Address Configuration Information consists of one or more ECS Configuration Information as defined in clause 8.3.2.1 of TS 23.558 [5]. The ECS Configuration Information may contain Spatial Validity Conditions, which includes one of the following alternatives:

- a Geographical Service Area (see TS 23.558 [5]);
- a list of TA(s); or
- a list of countries (list of MCC);
- a list of PLMN IDs (see Table 4.15.6.3d-1 of TS 23.502 [3]).

A UE may receive multiple instances of ECS Address Configuration Information e.g., corresponding to different ECSPs (e.g., the MNO or a 3rd party service provider).

The ECS Address Configuration Information is sent to the UE on a per PDU Session basis. The same PDU session can be used by multiple ECS providers.

The SMF does not need to be aware of the internal structure of the ECS Address Configuration Information.

6.5.2.2 ECS Address Configuration Information Provisioning to the UE

If the UE hosts an EEC and supports transferring the ECS address received from the 5GC to the EEC, the UE indicates in the PCO at PDU Session establishment that it supports the ability to receive ECS address(es) via NAS and to transfer the ECS Address(es) to the EEC(s) (see TS 23.502 [3]). As described in TS 23.502 [3], if the UE supports the ability to receive ECS Address Configuration Information via NAS and to transfer the ECS address(es) to the EEC(s), the UE may receive ECS Address Configuration Information from the SMF via PCO during PDU Session Establishment and/or during PDU Session Modification procedures. If Spatial Validity Condition of ECS is provided, the UE uses the appropriate ECS as defined in TS 23.558 [5].

The SMF may receive ECS Address Configuration Information and associated spatial validity conditions from the UDM together with SM subscription information. The UDM in the HPLMN may provide the SMF (in HPLMN in HR case, in VPLMN in LBO case) with ECS address configuration information that depends on the serving PLMN of the UE.

The SMF determines the ECS Address Configuration Information to be sent to the UE based on UE subscription information received from UDM (as described in clause 4.15.6.3d-2 of TS 23.502 [3]).

The SMF may decide to send updated ECS Address Configuration Information to the UE based on locally configured policy or updated UE subscription information. The PDU Session Modification procedure is used to send updated ECS Address Configuration Information to the UE as described in clause 4.3.3 of TS 23.502 [3].

NOTE 1: In home routed sessions, the ECS Address Configuration Information comes from the H-SMF. The traffic to the indicated Edge Configuration Server(s) can be transmitted via a PDU Session with local breakout.

NOTE 2: Although the Service Provisioning procedure with the ECS can take place over a HR session, if the HR-SBO PDU Session is not supported for the UE, an LBO PDU Session to access the EES(s) and EAS(s) in VPLMN needs to be established. As the UE is not aware of whether a PDU Session is working in LBO or in HR mode, in this case the PDU Session used to access the EES(s) would need to use another combination of (DNN, S-NSSAI) than the PDU Session working in HR mode. If the HR-SBO PDU Session is supported for the UE, the same combination of DNN and S-NSSAI working in HR mode can be also used to access the EES(s) and EAS(s) in VPLMN.

NOTE 3: The Service Provisioning procedure is described in TS 23.558 [5].

6.5.2.3 ECS Address Provisioning by a 3rd Party AF

As described in TS 23.558 [5], the Edge Configuration Server can be deployed in a 3rd party domain by a service provider. An AF in the MNO domain or, if the Edge Configuration Server is deployed in a 3rd party domain by a service provider, a 3rd party AF can use Nnef_ParameterProvision to provide, update, or delete AF provided ECS Address Configuration Information applying on a DNN and/or S-NSSAI for a group of UE, or any UE (See clause 4.15.6.2 of TS 23.502 [3]).

When the AF uses Nnef_ParameterProvision to send a new AF provided ECS Address Configuration Information to the UDM (e.g. because on Application layer activity, etc.), the UDM may notify the impacted SMF(s) of the updated Subscription provided ECS Address Configuration Information and the new ECS Address Configuration Information will be sent to the UE(s) in a PDU Session Modification procedure.

NOTE 1: Mechanisms to avoid signalling overload when the AF uses Nnef_ParameterProvision to send new ECS Address Information to many UEs are defined in TS 23.502 [3].

NOTE 2: The AF provides ECS Address Configuration Information to 5GC that target any UEs or a group of UE.

6.5.2.4 ECS Address Provisioning by MNO

The ECS Address Configuration Information can be provisioned by the MNO subscription provisioning in UDM.

6.5.2.5 Interworking with EPC

In interworking scenarios, if the UE hosts an EEC and supports transferring the ECS address received from the 5GC to the EEC, the UE indicates in the PCO at PDN Connection establishment that it supports the ability to receive ECS address(es) via NAS and to transfer the ECS Address(es) to the EEC(s) (see TS 23.502 [3]) and the bearer modification procedure without bearer QoS update procedure is used to send updated ECS Address Configuration Information to the UE as described in clause 4.11.0a.5 of TS 23.502 [3].

6.5.2.6 ECS Address Provisioning in Roaming

6.5.2.6.1 General

For both LBO and HR case, the subscription data of the ECS Address Configuration Information in UDM or UDR is stored per PLMN ID.

For the LBO case, an AF in the visited PLMN may provide the EACI via External Parameter Provisioning procedure as described in clause 4.15.6.3d in TS 23.502 [3] to UDM via H-NEF. This ECS Address Configuration Information is further provided to SMF as part of subscription information.

For the HR case when access to EHE in VPLMN is allowed:

- The HPLMN has the knowledge of EACI in the VPLMN: For this scenario, the AF is able to interact with NEF in HPLMN. The AF may provide the VPLMN EACI to H-NEF via External Parameter Provisioning procedure as described in clause 4.15.6.3d in TS 23.502 [3], and further to the UDM. During the HR PDU session establishment procedure, the H-SMF sends the VPLMN EACI to V-SMF and then to UE. The V-SMF does not modify, but just delivers the EACI provided by the H-SMF.

- HPLMN does not have the knowledge of EACI in VPLMN: For this scenario, the AF can't interact with NEF in HPLMN. As defined in clauses 6.5.2.6.2 and 6.5.2.6.3, V-NEF stores the VPLMN EACI received from AF deployed in the VPLMN in V-UDR, and V-SMF subscribes from V-NEF to retrieve the VPLMN EACI. During the HR PDU Session establishment, the V-SMF sends the VPLMN EACI obtained from V-NEF to the H-SMF, and H-SMF decides the VPLMN ECS Address Configuration Information sent to V-SMF and then to UE according to the PLMN ID additionally.

NOTE: It depends on the PLMN operation that the HPLMN can decide the EACI if both VPLMN and UDM provides the EACI.

6.5.2.6.2 ECS Address Configuration Information Provision from AF via NEF in VPLMN

The AF provides non-PDU Session specific ECS Address Configuration Information via NEF in VPLMN to 5GC is defined in this clause.

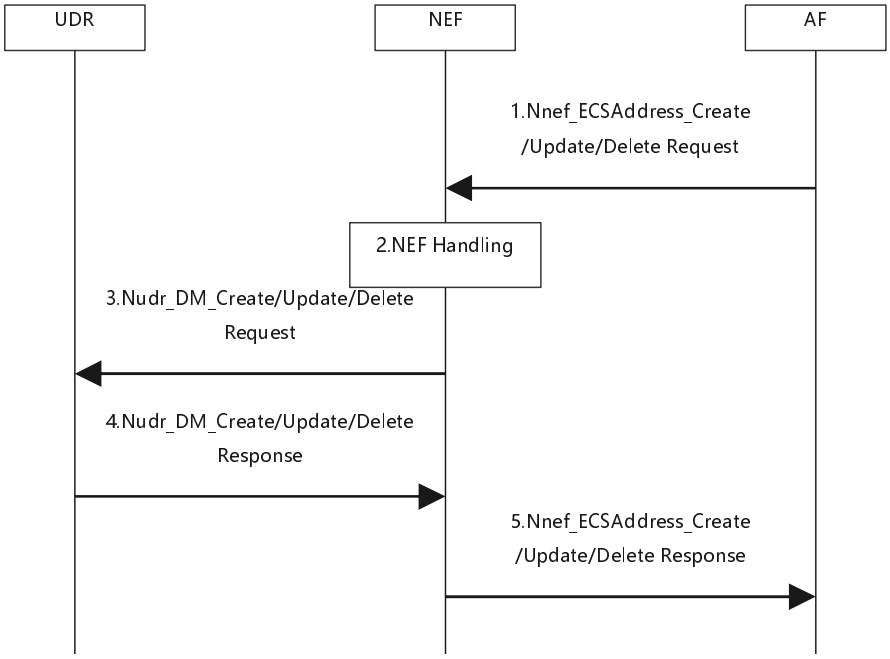

Figure 6.5.2.6.2-1 ECS Address Configuration Information provisioning to UDR via NEF in VPLMN

1. The AF invokes the Nnef_ECSAddress_Create /Update/Delete service operation to provide ECS Address Configuration Information to the NEF in VPLMN.
2. NEF checks whether the AF is authorized to perform the request based on the operator policies.

NOTE: External Group Identifier and Internal Group Identifier cannot be used by AF in VPLMN for the HR-SBO case.

3. The NEF invokes the Nudr_DM_Create/Update/Delete to the UDR in VPLMN if it is authorized.
4. The UDR stores/updates/removes the corresponding information (and responds a Nudr_DM_Create/Update/Delete Response to the NEF).
5. The NEF sends Nnef_ECSAddress_Create/Update/Delete Response to the AF.

6.5.2.6.3 ECS Address Configuration Information Provision to the SMF in VPLMN

V-SMF supporting HR-SBO may receive the ECS Address Configuration Information from NEF in VPLMN via Subscribe/Notify procedure is defined in this clause.

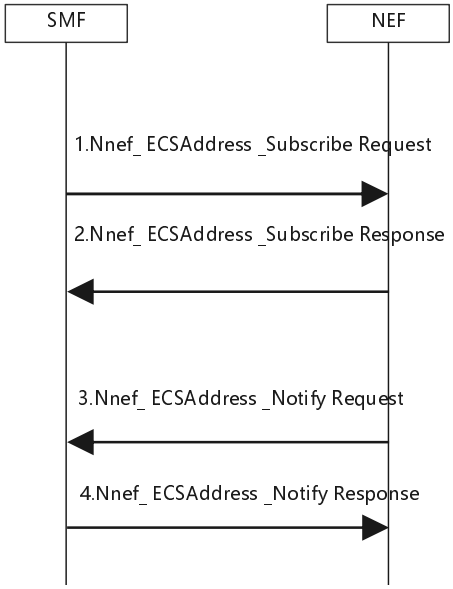

Figure 6.5.2.6.3-1: ECS Address Configuration Information provisioning to SMF in VPLMN

1-2. As pre-requisite condition, the SMF subscribes to ECS Address Configuration Information Change Notification from the NEF by sending Nnef_ECSAddress_Subscribe message. The SMF may indicate that the current status of ECS Address Configuration Information shall be notified immediately (if available). The SMF may indicate for which (list of) DNN and/or S-NSSAI it subscribes. NEF may further subscribe to ECS Address Configuration Information Change Notification from the UDR using Nudr_DM_Subscribe.

3-4. The NEF invokes Nnef_ECSAddress_Notify (ECS Address Configuration Information) to the SMF if the ECS Address Configuration Information is updated. If there is ECS Address Configuration Information available and immediate report is required, the NEF notifies the SMF(s) with such information immediately. NEF may retrieve the ECS Address Configuration Information from UDR using Nudr_DM_Query/Notify.

6.6 Support of AF Guidance to PCF Determination of Proper URSP Rules

This clause describes how an Edge Computing related AF may send guidance to PCF determination of proper URSP rules to send to the UE.

NOTE 1: This clause can apply in all deployment models.

An AF related with Edge computing may need to guide PCF determination of proper URSP rules. The guidance sent by the AF may apply to any UE or to a set of UE(s) e.g. identified by a Group Id. The AF may belong to the operator or to a third party.

NOTE 2: Some examples of the delivery of such AF guidance are shown in Annex D.

An AF may deliver such guidance to the PCF via application guidance for URSP rules determination mechanisms defined in clause 4.15.6.10 of TS 23.502 [3]. This mechanism is defined only to deliver the guidance to a PCF of the HPLMN of the UE.

The PCF may use the AF guidance received from different AFs, UE subscription data and local operator policy to determine the URSP rules to send to a UE. If received guidance information is not consistent with UE subscription data, or the local operator policy do not allow the specific S-NSSAI and DNN provided by the AF guidance, the corresponding AF guidance shall not be used to determine URSP rules.

- Application traffic descriptor from the application guidance is used to set the URSP Traffic Descriptor (e.g. Destination FQDNs or a regular expression in the Domain descriptor), and the PCF determines the URSP rules precedence in the URSP rule (defined in TS 23.503 [4] Table 6.6.2.1-2);

NOTE 3: When multiple Edge Computing specific parameters for the same application are received, the PCF decides the traffic matching priority Rule precedence value of the URSP rule (defined in TS 23.503 [4] Table 6.6.2.1-2).

- Route selection parameter from the application guidance is used to set a Route Selection Descriptor as follows:
  - DNN and S-NSSAI from the Route selection parameter from the application guidance are used to set the DNN selection, Network Slice selection components in the Route Selection Descriptor of the URSP rule, respectively (defined in TS 23.503 [4] Table 6.6.2.1-3) based on the UE subscription data;
  - Route selection precedence from the application guidance is used to set the Route Selection Descriptor Precedence in the Route Selection Descriptor (defined in TS 23.503 [4] Table 6.6.2.1-3);
  - The spatial validity condition for the Route selection precedence from the application guidance if any are used to set the Location Criteria in the Route Selection Descriptor of the URSP rule (defined in TS 23.503 [4] Table 6.6.2.1-3).

NOTE 4: Since the Validation Criteria are not required to be checked during the lifetime of the PDU Session, it may be left to UE implementation (e.g. URSP re-evaluation at mobility change) how well spatial validity conditions in URSPs restrict the access to a specific (DNN, S-NSSAI) to certain locations.

URSP rules based on AF guidance should not be set as the URSP rules with the "match all" traffic descriptor.

6.7 Support of the local traffic routing in VPLMN for Home Routed PDU Session for roaming (HR-SBO)

6.7.1 General

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 local traffic routing (i.e. session breakout performed by V-SMF also called HR-SBO) in VPLMN for the home routed session.

After establishing the HR-SBO PDU Session, the UE can access EAS deployed in EHE in VPLMN while the UE can also access the data network in the Home PLMN.

The reference architecture supporting this scenario is depicted in Figure 4.2-5 in clause 4.2.

6.7.2 Procedure

6.7.2.1 General

This clause describes the authorization procedure of the local traffic offloading using HR PDU Session and EAS discovery procedure supporting HR-SBO.

6.7.2.2 PDU Session establishment for supporting HR-SBO in VPLMN

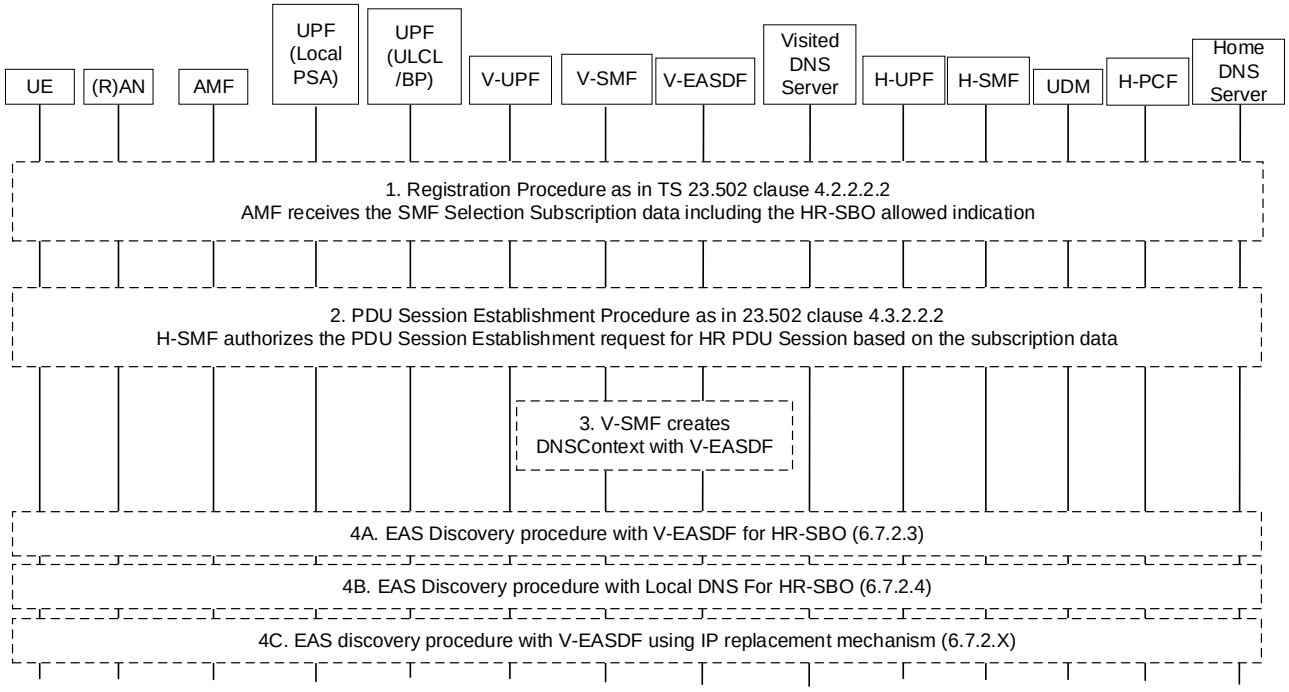

Figure 6.7.2.2-1: Procedure for PDU Session establishment supporting HR-SBO in VPLMN

1. During the Registration procedure, the AMF receives the HR-SBO allowed indication per DNN/S-NSNAI from the UDM in the step 14b of the procedure in the clause 4.2.2.2.2 of TS 23.502 [3].

2. During the PDU Session Establishment procedure for Home-routed roaming as in clause 4.3.2.2.2 of TS 23.502 [3], if the UE is roaming and if the AMF had received in SMF Selection Subscription data from UDM the HR-SBO allowed indication for the DNN/S-NSSAI in the step 1, the AMF selects a V-SMF supporting HR-SBO and sends an HR-SBO allowed indication to the V-SMF in the step 2 and the step3a of the procedure in figure 4.3.2.2.2-1 in clause 4.3.2.2.2 of TS 23.502 [3].

   If the V-SMF supporting the HR-SBO receives the HR-SBO allowed indication from AMF, the V-SMF may:

   - select UL CL/BP UPF and L-PSA UPF based on UE location information and this indication in the step 4 of the Figure 4.3.2.2.2-1 of TS 23.502 [3].

NOTE 1: The UL CL/BP UPF and L-PSA UPF can be co-located in the single V-UPF.

   - select a V-EASDF;

   - obtain the V-EASDF IP address based on local configuration, or invoke Neasdf_DNSContext_Create Request including the DNN, S-NSSAI, HPLMN ID and the UE IP address set to unspecified address or to a mapped address as specified in clause 7.1.2.2 to obtain the V-EASDF IP address;

   - may obtain V-EASDF DNS security information based on local configuration or via interaction with EASDF; and

NOTE 2: The network needs to ensure that EASDF can disambiguate the DNS traffic of different UEs that would be allocated with same private UE IP address. This can be done by implementation and/or deployment specific means, e.g. tunnelling on N6, network instance or UE source IP address mapping. To disambiguate the DNS traffic of different UEs allocated with same private UE IP address, the V-SMF can update the Local PSA-UPF with N4 PDR and FAR including either N6 traffic routing information or network instance (as described in clause 5.6.12 of 23.501 [2]) to forward the DNS traffic to the V-EASDF. When N6 traffic routing tunnel is used, the V-SMF can configure V-EASDF with the N6 traffic routing information towards the Local PSA-UPF. Alternatively, the V-SMF can update the local UPF to translate the UE source IP address with the replaced IP address in the IP pool of the Local PSA UPF.

- send the request for the establishment of the PDU Session supporting HR-SBO in VPLMN and optionally send the IP address and (if exists) DNS security information of V-EASDF/Local DNS Server/Resolver to the H-SMF in the Nsmf_PDUSession_Create Request in the step 6 of the procedure in figure 4.3.2.2.2-1 in clause 4.3.2.2.2 of TS 23.502 [3].

The H-SMF authorizes the request for HR-SBO based on SM subscription data (i.e. HR-SBO authorization indication) in the step 7 of the procedure in the clause 4.3.2.2.2-1 of TS 23.502 [3].

Once the HR-SBO is authorized, the H-SMF requests and retrieves the optional VPLMN Specific Offloading Policy from H-PCF by SM Policy Association Establishment/Modification with the HR-SBO support indication as indicated in clause 5.2.5.4.2 of TS 23.502 [3].. The H-SMF generates VPLMN Specific Offloading Information (i.e. IP range(s) and/or FQDN(s) allowed to be routed to the local part of DN in VPLMN, and/or Authorized DL Session AMBR for Offloading) based on the VPLMN Specific Offloading Policy. Each VPLMN Specific Offloading Policy may be provided with an Offload Identifier. The Offload Identifier is assigned by H-PCF, and is unique in the HPLMN.

NOTE 3: To ensure that the Offload Identifier is unique within the HPLMN, PCF instances can be configured to assign Offload Identifier with different ranges.

If HR-SBO is authorized for the PDU session, the H-SMF provides in the Nsmf_PDUSession_Create Response in the step 13 of the procedure in figure 4.3.2.2.2-1 in clause 4.3.2.2.2 of TS 23.502 [3] with the following information:

- optionally, VPLMN Specific Offloading Information that may include FQDN range, IP range, session AMBR for the local part of DN and charging policy.

  The VPLMN specific Offloading Information may refer to either allowed or not allowed traffic for HR-SBO (the latter is being used when the HPLMN would like to ensure that certain traffic are not allowed for HR-SBO). The VPLMN Specific Offloading Information for the allowed and not allowed traffic should be mutually exclusive, i.e., either a list of allowed or a list of not allowed traffic descriptors should be sent, but not both. The VPLMN Specific Offloading Policy can be configured in the H-SMF and tagged with Offload Identifier(s), and which VPLMN Specific Offloading Information to be sent to V-SMF can be indicated by these Offload Identifier(s) received from H-PCF.

  H-SMF may send the Offload Identifier(s) alone or together with the VPLMN Specific Offloading Information:

  - If the given V-SMF has already received the VPLMN Specific Offloading Information corresponding to certain Offload Identifier(s), this could be indicated to the H-SMF in any subsequent request to another HR-PDU Session from the same V-SMF, and the H-SMF will in this case send only the Offload Identifier(s) as a response;

  - If the VPLMN Specific Offloading Information for a given Offload Identifier is changed, for each V-SMF using the Offload Identifier, the H-SMF chooses one existing HR-SBO PDU Session using the Offload Identifier to update VPLMN Specific Offloading Information and corresponding Offload Identifier to the V-SMF via PDU Session Modification procedure as described in clause 4.3.3.3 of TS 23.502 [3];

NOTE 4: V-SMF keeps track for which HPLMN each Offload indicator is related to since the Offload Indicators are unique per HPLMN.

NOTE 5: An Offload identifier can include a version number. In this case, a VPLMN Specific Offloading Information provided by H-SMF with a higher version number will overwrite the one with lower version number.

- During PDU Session Release procedure as described in clause 4.3.4.3 of TS 23.502 [3], if the PDU Session is the last HR-SBO PDU Session using a given Offload Identifier on the V-SMF, the V-SMF may remove the Offload Identifier and corresponding VPLMN Specific Offloading Information based on roaming agreements.

NOTE 6: In this Release, the HPLMN allows HR-SBO for a PDU session only if the UE IP address of the PDU Session has not been allocated in a range that may overlap with other PDU sessions to the same DNN and S-NSSAI of that HPLMN.

- the V-EASDF IP address (corresponding to clause 6.7.2.3) or Local DNS Server/Resolver IP address (corresponding to clause 6.7.2.4) or DNS server IP address of HPLMN (corresponding to clause 6.7.2.5) as DNS server address to be sent to the UE via PCO; and

- the DNS security information of V-EASDF/Local DNS Server/Resolver to be sent to the UE via PCO, if the UE indicate DNS server security information indicator in PDU Session Establishment Request and if supported in V-EASDF/Local DNS Server/Resolver (see TS 24.501 [11] and TS 33.501 [12]);

- optionally, the DNS server address provided by HPLMN to be used for DNS requests related with traffic not to be subject to HR-SBO, including to configure V-EASDF corresponding to clause 6.7.2.3, or configure the UPF in VPLMN to perform IP replacement as described in clause 6.7.2.5;

NOTE 7: In this Release, only public IP address can be used as the DNS server address provided by HPLMN.

- optionally, the HPLMN address information (e.g. H-UPF IP address on N6) to be used by V-EASDF to build EDNS Client Subnet option for target FQDN of the DNS query which is not authorized for HR-SBO as described in clause 6.7.2.3;

- the HR-SBO authorization result (i.e. whether HR-SBO request is authorized or not).

The 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.

If the request for HR-SBO is not authorized and DNS context has been created, the V-SMF delete the DNS context from the selected V-EASDF, and the subsequent steps related to the EASDF in this procedure are skipped.

If the request for HR-SBO is not authorized, the DNS server address provided by HPLMN is configured to UE as DNS server address. Step 3 to step 4 are skipped.

The detailed information of VPLMN Specific Offloading Policy is described in clause 6.4 of TS 23.503 [4].

NOTE 8: The VPLMN Specific Offloading Policy can be prior configured in HPLMN based on the service level agreement between the VPLMN and HPLMN.

3. The V-SMF configures the V-EASDF with the DNS handling rules using the VPLMN Specific Offloading Information received from H-SMF or corresponding to Offload Identifier(s) received from H-SMF.

   The V-SMF optionally configures the V-EASDF with the DNS server address provided by the HPLMN as default DNS server (corresponding to clause 6.7.2.3), after the step 13 of the procedure in figure 4.3.2.2.2-1 in clause 4.3.2.2.2 of TS 23.502 [3] if they are received from H-SMF in the step 2. If V-SMF has not received the DNS server address provided by HPLMN from H-SMF in step 2, a default DNS server may be configured to V-EASDF.

   If HPLMN address information is received, the V-SMF may also configure the V-EASDF to build EDNS Client Subnet option based on this HPLMN address information for target FQDN of DNS query which is not authorized for HR-SBO.

   If the V-SMF has interacted with the V-EASDF in step 2, then the V-SMF invokes Neasdf_DNSContext_Update Request including UE IP address to complete the configuration of the context in the V-EASDF.

   The V-SMF configures the UL CL UPF and PSA UPF selected in the step 2 to forward DNS messages to V-EASDF.

   If the Authorized DL Session AMBR for Offloading is provided from the H-SMF, the V-SMF configures the Authorized DL Session AMBR for Offloading on the UL CL UPF in the VPLMN and additionally local PSA(s) terminating the N6 interface toward the local part of DN in the VPLMN.

   At N4 session establishment for a PDU Session working in HR SBO mode, the SMF in VPLMN provides to any UPF in VPLMN acting as (local) PSA for that PDU Session and capable of enforcing NAT on N6 traffic: the HPLMN ID of UE, andthe DNN/S-NSSAI of the PDU Session in HPLMN for the PDU Session.

4A. EAS Discovery procedure with V-EASDF is performed as described in clause 6.7.2.3.

4B. EAS Discovery procedure with Local DNS Server/Resolver is performed as described in clause 6.7.2.4.

4C. EAS discovery procedure with V-EASDF using IP replacement mechanism as described in clause 6.7.2.5.

6.7.2.3 EAS Discovery Procedure with V-EASDF for HR-SBO

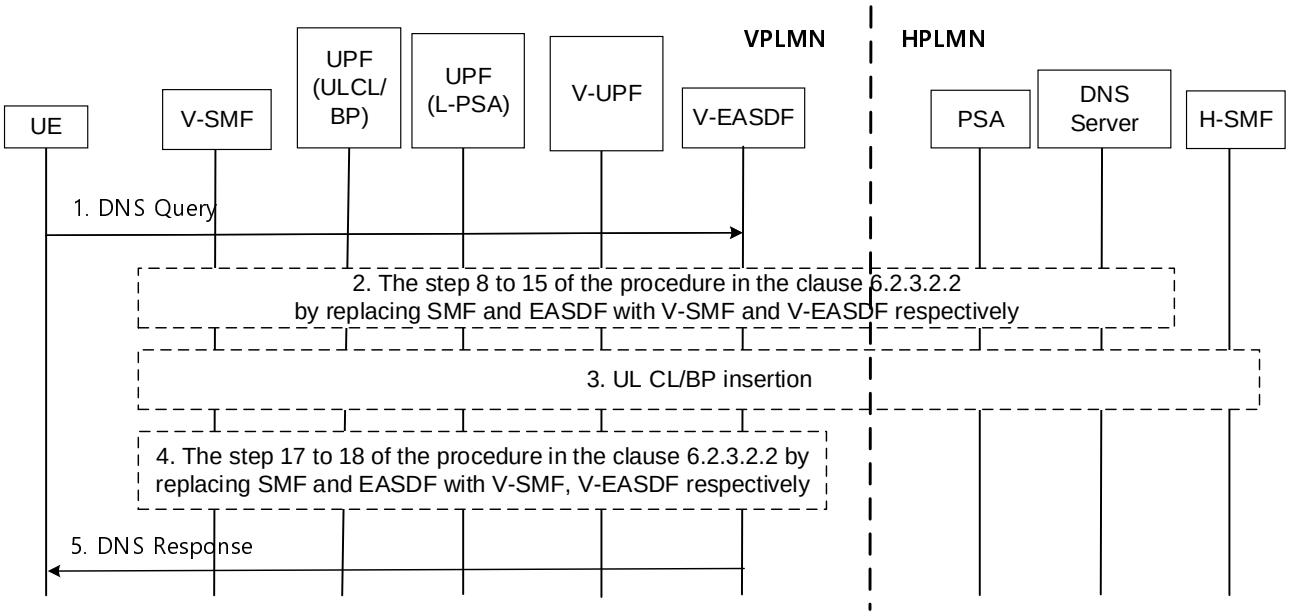

Figure 6.7.2.3-1: Procedure for EAS Discovery with V-EASDF for HR-SBO roaming scenario

1. The DNS query sent by the UE reaches the UL CL UPF in VPLMN selected in step 2 of clause 6.7.2.2. The UL CL UPF forwards it to Local PSA UPF then V-EASDF, or to H-UPF as described below.

   If the target FQDN of the DNS query is not part of the FQDN authorized by the H-SMF in step 2 of clause 6.7.2.2, the following a) or b) may be performed:

   a) Based on SMF instruction in step 3 of clause 6.7.2.2, the V-EASDF proceeds to step 12 of clause 6.2.3.2.2 where it sends the DNS query which may include the HPLMN address information as the EDNS Client Subnet option. The DNS query is sent to the DNS server address according to the DNS message handling rules provided by the V-SMF or to the default DNS server configured in the V-EASDF. Upon receiving the DNS response, the procedure proceeds immediately to step 5.

NOTE 1: If HPLMN DNS or the default DNS server does not support the EDNS Client Subnet option, it cannot be ensured that an AS close to H-UPF will be resolved.

   b) The UL CL/BP UPF sends the DNS query to the DNS server address provided by HPLMN via V-UPF (if exists) and H-UPF (through N9), by modifying the packet's destination IP address (corresponding to V-EASDF) to the DNS server address provided by HPLMN on UL CL or H-UPF. For the corresponding DNS response received by H-UPF, the H-UPF or UL CL modifies the packets' source IP address to that of the V-EASDF.

      This assumes that the UL CL is able to detect FQDN(s) in traffic sent to the IP address of the EASDF. It is thus incompatible with usage of DoT (DNS over TLS) or DoH to protect the DNS traffic exchanged between the UE and the PLMN.

   If the VPLMN Specific Offloading Information only includes IP range, the V-SMF can configure the V-EASDF to resolve all DNS queries using a VPLMN address (e.g. an IP address associated with the L-PSA UPF in the VPLMN) as EDNS Client Subnet option.

The rest of the procedure assumes the target FQDN of the DNS query is part of the FQDN authorized by the H-SMF in step 2 of clause 6.7.2.2.

2. The steps 8 to 15 of the procedure in the clause 6.2.3.2.2 by replacing SMF and EASDF with V-SMF and V-EASDF respectively.

If VPLMN Specific Offloading Information does not include FQDN range and the EAS IP address of the DNS response is not part of the IP range(s) authorized in step 2 of clause 6.7.2.2, the following may be performed:

- If the V-EASDF is not configured with the DNS server address provided by the HPLMN as default DNS server, The V-SMF indicates the V-EASDF to construct and to send another DNS query with the same FQDN and the HPLMN address information as the EDNS Client Subnet option, to the DNS server address as described in step 1) bullet a). Otherwise V-SMF indicates the V-EASDF to construct and send another DNS query with the same FQDN to the DNS server provided by HPLMN.

3. The V-SMF selects UL CL/BP and local PSA in VPLMN based on the V-EASDF notification, EAS Deployment Information in the VPLMN, VPLMN Specific Offloading Information and UE location. The V-SMF may perform insertion or change of UL CL/BP and local PSA in VPLMN.

   The V-SMF configures the UL CL/BP and local PSA for the traffic to be offloaded to the local part of DN based on the VPLMN Specific Offloading Information received from H-SMF.

   If the Authorized DL Session AMBR for Offloading is provided from the H-SMF, the V-SMF configures the Authorized DL Session AMBR for Offloading on the UL CL/BP in the VPLMN and additionally the local PSA(s) terminating the N6 interface toward the local part of DN in the VPLMN.

   In the case of UL CL, the V-SMF configures the traffic detection rules and traffic routing rules on the UL CL UPF based on the EAS Deployment Information and the EAS addresses included in VPLMN Specific Offloading Information.

   If there is no other V-UPF between the selected UL CL/BP in this step and H-UPF, the V-SMF sets up user plane between this UL CL/BP and H-UPF via the interaction with H-SMF. Otherwise, the V-SMF sets up user plane between this ULCL/BP and the existing V-UPF.

   The V-SMF sets up user plane between the selected UL CL/BP in this step and RAN (if no other V-UPF exists between RAN and this UL CL/BP) or the V-UPF (if exists between this UL CL/BP and RAN).

NOTE 2: If the selected UL CL/BP and local PSA in this step is the UL CL/BP and PSA selected by V-SMF in the step 2 of clause 6.7.2.2, the insertion of UL CL/BP and local PSA in VPLMN will not be performed in this step.

NOTE 3: In the home routed roaming scenario, the V-UPF selected during PDU Session establishment procedure can be deployed at a central area within VPLMN. In this case, the V-UPF is located in the user plane path between UL CL/BP UPF in VPLMN and PSA-UPF in HPLMN. In some deployments, the UL CL/BP UPF can be collocated with the V-UPF.

   If the EAS IP address is not part of the IP address authorized by H-SMF, the UL CL/BP V-UPF is instructed by V-SMF to send the packet from UE to the H-UPF.

4. The steps 17 to 18 of the procedure in clause 6.2.3.2.2 by replacing SMF and EASDF with V-SMF and V-EASDF respectively.

5. V-EASDF sends the DNS Response to the UE.

6.7.2.4 EAS Discovery Procedure with Local DNS for HR-SBO

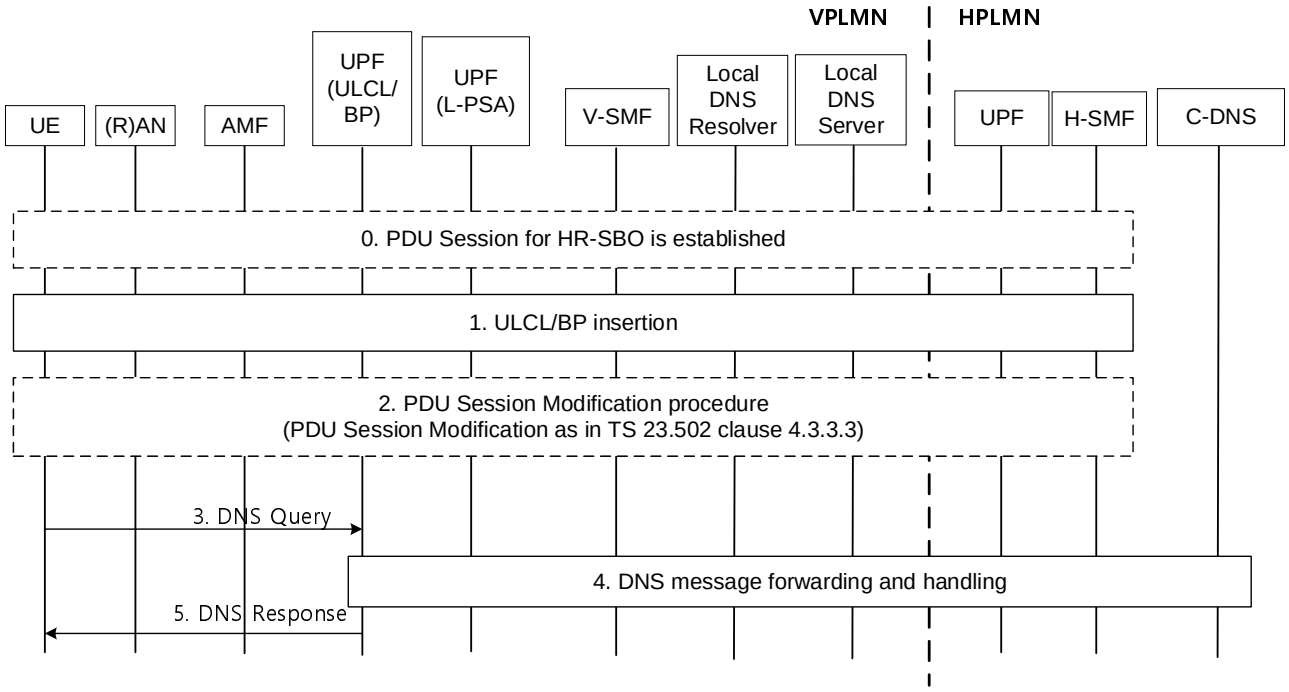

Figure 6.7.2.4-1: Procedure for EAS Discovery with local DNS for HR-SBO roaming scenario

The procedure in this clause assumes that the UL CL is able to detect FQDN(s) in traffic sent to the IP address of the local DNS Server. It is thus incompatible with usage of DoT (DNS over TLS) or DoH to protect the DNS traffic exchanged between the UE and the PLMN.

If the target FQDN of the DNS query is not part of the FQDN authorized by the H-SMF in step 2 of Figure 6.7.2.2-1, the UL CL/BP UPF is instructed to send the DNS request to the DNS server address provided by HPLMN via V-UPF (if it exists) and H-UPF (through N9), by modifying the packet's destination IP address (corresponding to local DNS Server) to the DNS server address provided by HPLMN on UL CL or H-UPF . For the corresponding DNS response received by H-UPF, the H-UPF or UL CL modifies the packets' destination IP address to that of the local DNS Server.

NOTE: This procedure only applies when both FQDN range and IP range are included in the VPLMN Specific Offloading Information. The V-SMF can use IP range included in the VPLMN Specific Offloading Information to configure ULCL/BP in V-UPF.

The steps 0 to 5 are the same as the steps 0 to 6 of Figure 6.2.3.2.3-1 with following differences:

- SMF is replaced with V-SMF.
- UE, (R)AN, AMF, UL CL/BP UPF, L-PSA UPF, V-SMF, Local DNS Resolver/Server are located in VPLMN.
- UPF, H-SMF, C-DNS are located in HPLMN.

0. The HR-SBO PDU Session is established. See the procedure in clause 6.7.2.2.
1. UL CL/BP insertion. See the step 1 of the procedure in Figure 6.2.3.2.3.
2. After UL CL/BP insertion is performed, the V-SMF sends new local DNS server address to the UE by performing PDU Session Modification procedure as in clause 4.3.3.3 of TS 23.502 [3] with following additions:
   - V-SMF sends Local DNS Server/Resolver to the H-SMF in the step 1a of the procedure as in clause 4.3.3.3 of TS 23.502 [3].
   - H-SMF sends the Local DNS Server/Resolver to be sent to the UE via PCO to the V-SMF in the step 3 of the procedure in clause 4.3.3.3 of TS 23.502 [3].

3-5. See the steps 4-6 of the procedure in Figure 6.2.3.2.3.

6.7.2.5 EAS discovery procedure with V-EASDF/Local DNS Server using IP replacement mechanism for supporting HR-SBO

Based on the operator's configuration and local regulations, the IP replacement mechanism may be used for EAS discovery supporting HR-SBO:

- The H-SMF sends DNS server address provided by the HPLMN included in PCO to UE via V-SMF during PDU Session Establishment/Modification procedure. The DNS query related to the edge computing (corresponding to FQDNs) can be routed to V-EASDF/Local DNS server in the VPLMN using IP replacement mechanism.

NOTE 1: This EAS discovery procedure requests modification of IP address of DNS messages. Whether this is allowed or not is subject to local regulations. As this procedure for EAS discovery requires an UPF to detect target FQDN in DNS message, it cannot apply when DNS security applies e.g. it does not apply to usage of DoH or DoT.

NOTE 2: This clause only applies when FQDN range is included in the VPLMN Specific Offloading Information. If Local DNS Server is used for the EAS discovery (i.e. not involving V-EASDF), it is assumed that IP address range is also provided in the VPLMN Specific Offloading Information.

To support IP replacement mechanism, in this clause the SMF shall instruct the UPF to use the FAR that contains Information elements of "IP Address and Port Number Replacement".

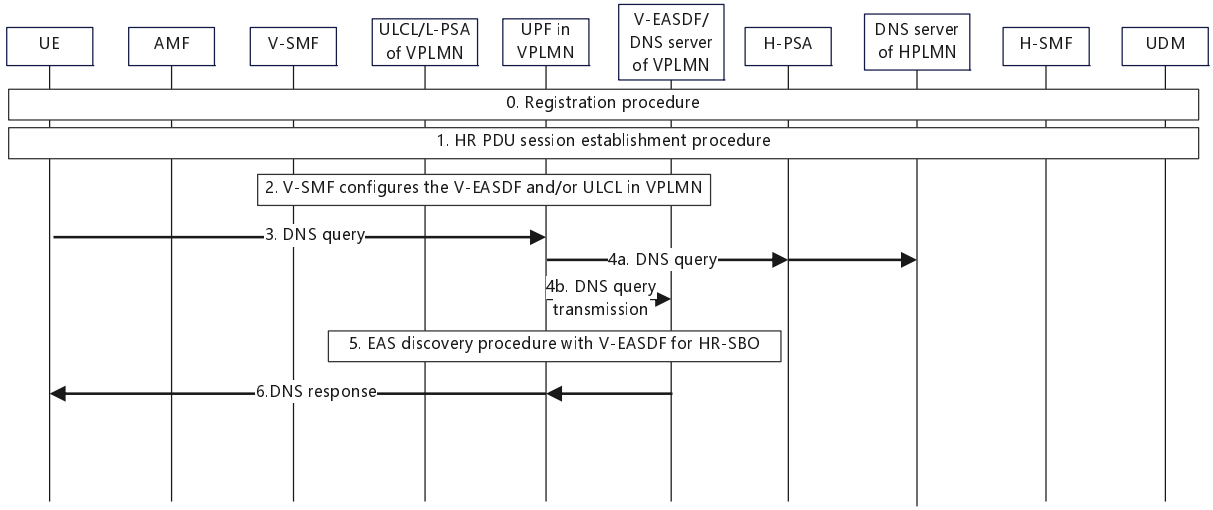

Figure 6.7.2.5-1: EAS discovery procedure with V-EASDF/Local DNS Server using IP replacement mechanism for supporting HR-SBO

NOTE 3: This clause assumes the V-SMF has received the HR-SBO allowed indication from the AMF and supports IP replacement mechanism for HR-SBO, it also assumes the HPLMN authorizes HR-SBO in the VPLMN.

0. The Registration procedure is described in step 1 of clause 6.7.2.2.

1. The HR-SBO PDU Session Establishment is described in the step 2 of clause 6.7.2.2 with the following differences:

   - After step 3 in clause 4.3.2.2.2 of TS 23.502 [3], the V-SMF selects a UPF in VPLMN supporting UL CL/BP and PSA functionalities based on UE location information.

NOTE 4: Based on the deployment of VPLMN, the selected UPF in VPLMN can support both UL CL and PSA functionalities in case that the UL CL UPF and PSA UPF are co-located. This UPF in VPLMN can be the V-UPF selected in the step 4 of clause 4.3.2.2.2 of TS 23.502 [3].

   - The V-SMF sends the request for establishment of the PDU session supporting HR-SBO in VPLMN without the V-EASDF/Local DNS server IP address in the step 6 of clause 4.3.2.2.2 of TS 23.502 [3].

   - If the Nsmf_PDUSession_Create Request received by the H-SMF does not include the V-EASDF/Local DNS server IP address, the H-SMF constructs PCO with DNS server address field set to DNS server address

provided by the HPLMN and sends the PCO to UE via V-SMF in the step 13 of clause 4.3.2.2.2 of TS 23.502 [3].

NOTE 5: The V-SMF can select the V-EASDF and create the DNS context in the V-EASDF or select the Local DNS server before sending Nsmf_PDUSession_Create Request or after having received Nsmf_PDUSession_Create response.

2. The V-SMF configures the UPF in VPLMN as described in step 3 of clause 6.7.2.2 with the following differences:

   - Based on the FQDN(s) received from the VPLMN Specific Offloading Information, the V-SMF indicates the UPF in VPLMN to route DNS queries for the FQDN (range) query to V-EASDF/Local DNS server. In the case of UL CL, the V-SMF configures the UPF in VPLMN with IP replacement information (i.e. DNS server IP address and port number of HPLMN, V-EASDF/Local DNS server IP address and port number). In uplink direction, UPF in VPLMN replaces the destination address of the DNS query targeting an FQDN eligible for HR-SBO related offload from DNS server IP address of HPLMN to V-EASDF/Local DNS server IP address; In downlink direction, UPF in VPLMN replaces the source address of the DNS response targeting an FQDN eligible for HR-SBO related offload from V-EASDF/Local DNS server IP address to DNS server IP address of HPLMN.

   If V-EASDF is used, the V-SMF also configures the V-EASDF as described in step 3 of clause 6.7.2.2.

NOTE 6: For the DNS query requiring DNS resolution in the HPLMN, the DNS resolution path is same as the normal path in the HR PDU Session.

3. UE sends DNS query to DNS server of HPLMN.

4a. If the DNS query does not match the FQDN range eligible for HR-SBO related offload, UPF in VPLMN delivers the DNS query via H-PSA through N9 and H-PSA delivers the DNS query to the DNS server of HPLMN.

4b. If the DNS query matches the FQDN range eligible for HR-SBO related offload, the UPF in VPLMN delivers the DNS query to V-EASDF/Local DNS server using IP replacement mechanism. The following EAS discovery procedure is based on step 4b.

5. The EAS discovery procedure described in steps 8-18 of clause 6.2.3.2.2 or steps 4-6 of clause 6.2.3.2.3 applies with the following differences:

   - This EAS discovery procedure with IP replacement is implemented in the VPLMN.

   - In step 16 of clause 6.2.3.2.2, the V-SMF may perform insertion or change of UL CL/BP and local PSA in VPLMN as described in the step 3 of clause 6.7.2.3.

6. The V-EASDF/Local DNS server sends the DNS response including FQDN to the UPF in VPLMN. The UPF in VPLMN replaces the source address from V-EASDF/Local DNS server to DNS server of HPLMN in the DNS response based on the V-SMF instructions and sends this DNS response to the UE directly or via UL CL/BP of VPLMN if existing in this PDU Session.

6.7.2.6 N2 Handover with V-SMF insertion/change/removal in HR-SBO case

This clause defines the procedure for intra-VPLMN and inter-PLMN N2-based handover for HR-SBO PDU Sessions with V-SMF insertion/change/removal. This procedure is based on Inter NG-RAN node N2-based handover with I-SMF insertion/change/removal defined in TS 23.502 [3] clause 4.23.7.3 by replacing the I-SMF as V-SMF and replacing the SMF as H-SMF.

The procedure assumes the UE has an HR-SBO PDU Session established as described in clause 6.7.2.2 using a source serving PLMN (e.g. involving a source V-SMF) and there is a handover to a same or different serving PLMN (e.g. involving a target V-SMF) with V-SMF change. The procedure also applies to the scenario where source or target serving network (before or after an inter-PLMN handover) is the HPLMN thus V-SMF insertion or removal happens.

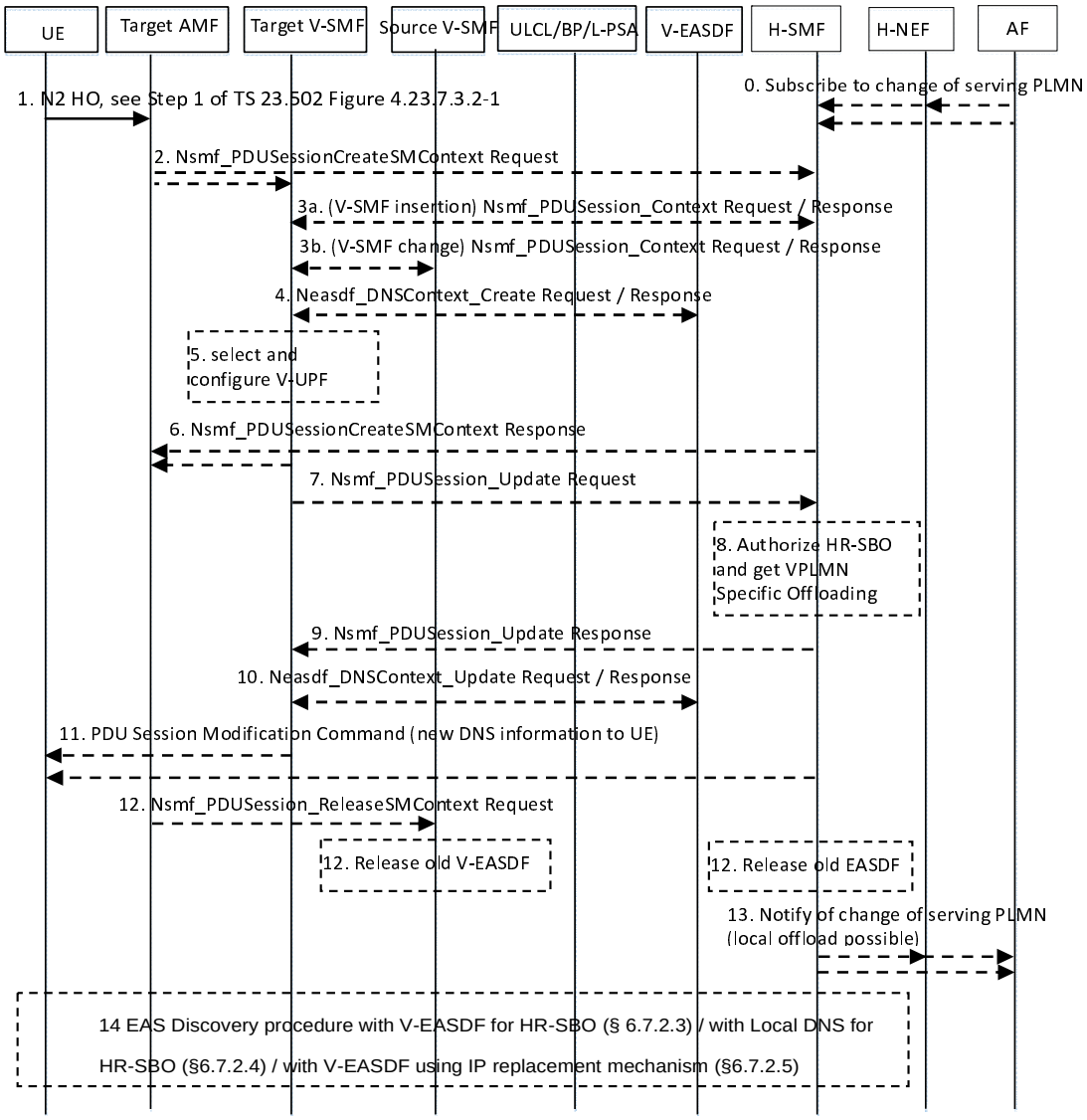

Figure 6.7.2.6-1: N2-based handover with V-SMF insertion/change/removal in HR-SBO case

NOTE 1: The flow above does not show all steps in clause 4.23.7.3 of TS 23.502 [3] but only those that are impacted by the support of HR-SBO.

The procedure described in clauses 4.23.17 and 4.23.7.3 of TS 23.502 [3] (N2-based handover with I-SMF insertion/change/removal) is performed by replacing I-SMF with V-SMF and SMF with H-SMF with following modifications:

0. The untrusted AF may subscribe via the H-NEF to the H-PCF or the trusted AF may directly subscribe to the H-PCF, then the H-PCF subscribe to the H-SMF for the event related with a mobility of the PDU Session towards a serving PLMN where local traffic offload is possible, i.e. mobility of the PDU Session either towards HPLMN or towards a VPLMN where HR-SBO is possible i.e. supported and allowed.

1. Step 1 in Figure 4.23.7.3.2-1 of TS 23.502 [3] (initiation of the N2-based handover).

   For an intra VPLMN HO, the source AMF provides the target AMF with whether HR-SBO is allowed for each PDU Session of the UE.

   For an inter PLMN HO, the target T-AMF uses local policies related to the SLA with the HPLMN of the UE to determine whether HR-SBO allowed indication is sent to the V-SMF(s) for the PDU Sessions of the UE.

NOTE 2: This means that if HR-SBO is allowed only for some users of the HPLMN and is not allowed for the UE being handed over, this will only be detected at a later step of the procedure i.e. at step 8.

2. Step 2 in Figure 4.23.7.3.2-1 of TS 23.502 [3] takes place.

   If the T-AMF considers that HR-SBO is possible, the T-AMF selects a V-SMF supporting HR-SBO.

2a (V-SMF insertion or V-SMF change) step 2 in Figure 4.23.7.3.2-1 of TS 23.502 [3] takes place.

   For V-SMF insertion and inter VPLMN V-SMF change case, the T-AMF sends an HR-SBO allowed indication to the target V-SMF in Nsmf_PDUSession_CreateSMContext Request as part of the step 3 of the procedure in Figure 4.23.7.3.2 of TS 23.502 [3].

2b (V-SMF removal) steps 9 to 12b in Figure 4.23.7.3.2-1of TS 23.502 [3] take place.

   The target AMF sends to H-SMF a Nsmf_PDUSession_CreateSMContext request as in step 9 in Figure 4.23.7.3.2-1 of TS 23.502 [3].

   For EAS discovery with EASDF, the H-SMF selects an EASDF in HPLMN and configures the DNS context in this EASDF (Neasdf_DNSContext_Create) and may select and configure UPF(s) in HPLMN.

   For EAS discovery with Local DNS Server, the H-SMF selects a Local DNS Server.

Steps 3 to 5 are skipped if the UE moves with V-SMF removal.

3. (V-SMF insertion or V-SMF change) step 4 or step 5 in Figure 4.23.7.3.2-1 of TS 23.502 [3].

3a. (V-SMF insertion case) The (target) V-SMF retrieves SM context from H-SMF using Nsmf_PDUSession_Context Request, followed by the Nsmf_PDUSession_Context Response.

3b. (V-SMF change case) The target V-SMF retrieves SM context from the source V-SMF using Nsmf_PDUSession_Context Request/Response.

   In step 3b, if source and target V-SMFs belong to same VPLMN, the SM context includes Authorization Result for HR-SBO, VPLMN Specific Offloading Information and/or corresponding Offload Identifier(s), the SM context also includes (if previously received by source V-SMF from H-SMF in the case of V-SMF change) the HPLMN address information, and the DNS Server address provided by the HPLMN.

   The SM context may also include EAS information to be refreshed for EAS re-discovery, i.e. FQDN(s) corresponding to the old target DNAI selected by the source V-SMF (V-SMF change case).

   If source and target V-SMFs belong to same VPLMN, the SM context may also include EAS IP replacement information (i.e. source EAS IP address and port number, target EAS IP address and port number) and the target DNAI.

4. (V-SMF insertion or V-SMF change) The (target) V-SMF selects a new V-EASDF e.g. based on the target UE location. The (target) V-SMF invokes Neasdf_DNSContext_Create including the DNN, S-NSSAI and HPLMN ID to obtain the new V-EASDF address.

   In the case of V-SMF insertion, the UE IP address is set to the unspecified address in Neasdf_DNSContext_Create as specified in clause 7.1.2.2.

   In the case of V-SMF change with inter PLMN mobility or intra PLMN mobility, the target V-SMF shall select a new V-EASDF if it is configured to use an EASDF for the PDU Session.

   To support EAS discovery with local DNS server as described in clause 6.7.2.4, the (target) V-SMF (re-)selects a local DNS server, e.g. based on the target UE location.

5. (V-SMF insertion or V-SMF change) The (target) V-SMF may perform UL CL/BP and local PSA insertion/change/removal as described in step 2 of Figure 6.7.2.2-1.

NOTE 3: When there are other V-UPF(s) between UL CL/BP and H-UPF, the (target) V-SMF sets up user plane between this ULCL/BP and the V-UPF.

6. The H-SMF (V-SMF removal) or the target V-SMF (V-SMF insertion or V-SMF change) responses to the target AMF with a Nsmf_PDUSession_CreateSMContext Response as in step 8 (V-SMF insertion or V-SMF change) or step 13 in Figure 4.23.7.3.2-1 of TS 23.502 [3] (V-SMF removal).

The handover procedure further continues as defined in steps 14 onwards of Figure 4.23.7.3.2-1 of TS 23.502 [3] and then per clause 4.23.7.3.3 of TS 23.502 [3], with clause 4.23.7.3.3 of TS 23.502 [3] modified as follows:

7 (V-SMF insertion or V-SMF change) when the T-AMF sends to the Target V-SMF an indication of Handover Complete within Nsmf_PDUSession_UpdateSMContext Request (at step 2 in Figure 4.23.7.3.3-1 of TS 23.502 [3]) the target V-SMF invokes Nsmf_PDUSession_Update Request to the H-SMF.

If a V-EASDF or a local DNS server has been selected in step 4, the selected V-EASDF or local DNS server address is provided in the request. The target V-SMF needs not provide the selected V-EASDF or local DNS server address if the target V-SMF is configured to use EAS discovery with V-EASDF using IP replacement mechanism corresponding to clause 6.7.2.5.

If the UE indicated support of refreshing stale EAS information, the V-SMF may also provide an EAS rediscovery indication and EAS information to be refreshed for EAS re-discovery if received in step 3 to the H-SMF.

This Nsmf_PDUSession_UpdateSMContext Request triggers steps 8 to 11.

8. (V-SMF insertion or V-SMF change): If the UE has changed of serving VPLMN or has moved from HPLMN to a VPLMN, the H-SMF:

- invokes Nudm_SDM_Get service to get subscription data from UDM by providing serving PLMN ID to get subscription data specific to the Serving PLMN;
- authorizes the request for HR-SBO based on the SM subscription data (i.e., HR-SBO authorization indication); and
- If the HR-SBO is authorized, retrieves the VPLMN Specific Offloading Policy from H-PCF.

9. (V-SMF insertion or V-SMF change): As defined in step 8 in clause 4.23.7.3.3 of TS 23.502 [3], the H-SMF invokes Nsmf_PDUSession_Update Response, providing the same HR-SBO related information as sent by the H-SMF in step 2 of Figure 6.7.2.2-1.

The H-SMF furthermore provides V-SMF with PCO including EAS rediscovery indication and impact field based on the EAS information to be refreshed for EAS re-discovery if received at step 7.

The target V-SMF stores the PCO including the V-EASDF address/local DNS server address, EAS rediscovery, impact field for the UE until it receives an indication of HO completion as described in step 2 in Figure 4.23.7.3.3-1 of TS 23.502 [3] or in step 11.

If the request for HR-SBO is not authorized and a V-EASDF context had been created, the V-SMF deletes the DNS context from the selected V-EASDF, and the subsequent steps related to the HR-SBO in this procedure are skipped.

10. (V-SMF insertion or V-SMF change): The (target) V-SMF configures the V-EASDF with the DNS handling rules as defined in step 3 of Figure 6.7.2.2-1.

If the (target) V-SMF has interacted with the V-EASDF in step 4, the V-SMF invokes Neasdf_DNSContext_Update Request including UE IP address to complete the configuration of the context in the V-EASDF.

The (target) V-SMF may configure the ULCL/L-PSA selected in the step 5 to forward DNS messages to V-EASDF.

When the V-SMF is configured to use EAS discovery with V-EASDF using IP replacement mechanism as described in clause 6.7.2.5, the (target) V-SMF configures the UL CL/L-PSA in the VPLMN with the IP replacement information (i.e. IP address of the DNS server provided by the HPLMN, the selected V-EASDF IP address and port number and DNS traffic filtering rules related with when IP replacement applies).

11. (V-SMF insertion or V-SMF change): The target V-SMF sends the PCO for the UE (received at step 9) in a PDU Session Modification Command sent to the UE.

(V-SMF removal): At step 10 in Figure 4.23.7.3.3-1 of TS 23.502 [3], when receiving Nsmf_PDUSession_UpdateSMContext Request (Handover Complete indication), the H-SMF sends the PCO including the V-EASDF or Local DNS Server address selected in step 2b in a PDU Session Modification

Command sent to the UE. If the UE indicated support of refreshing stale EAS information, the PCO may include EAS rediscovery indication.

12. (V-SMF change or removal): When the S-AMF invokes Nsmf_PDUSession_ReleaseSMContext Request to inform the Source V-SMF to release the SM context of the PDU Session, e.g. at step 3a or 11a in Figure 4.23.7.3.3-1 of TS 23.502 [3], the DNS context in the old (V-)EASDF is removed by the (source) V-SMF using Neasdf_DNSContext_Delete service.

    (V-SMF insertion): When the target V-SMF sends Nsmf_PDUSession_Update Request with a Handover Complete Indication at step 6 in Figure 4.23.7.3.3-1 of TS 23.502 [3], the DNS context in the old EASDF is removed by the H-SMF using Neasdf_DNSContext_Delete service.

NOTE 4: Re-selecting the old V-EASDF to reuse the existing DNS context in the case of intra-PLMN inter V-SMF mobility is not supported in this release of the specification.

13. If the AF had subscribed in step 0 and a serving PLMN change occurred towards a PLMN where local traffic offload is possible for the PDU Session, the H-SMF notifies the H-PCF then either via H-NEF or directly notify the AF indicating the target serving PLMN ID and DNN, S-NSSAI of the HPLMN. This may take place as soon as the H-SMF has received an indication of Handover Complete.

14. EAS discovery procedure by UE may take place:

    (V-SMF change or V-SMF insertion): EAS Discovery procedure with V-EASDF for HR-SBO (according to clause 6.7.2.3), with Local DNS for HR-SBO (according to clause 6.7.2.4), or with V-EASDF using IP replacement mechanism (according to clause 6.7.2.5); or

    (V-SMF removal): EAS Discovery procedure with EASDF or Local DNS Server (according to clause 6.2.3.2).

6.7.2.7 Inter V-SMF mobility registration update procedure in HR-SBO case

This clause defines the procedure for inter V-SMF intra-VPLMN and inter-PLMN mobility registration update procedure for HR-SBO PDU Sessions. This procedure is based on I-SMF insertion/change/removal defined in clauses 4.23.3 and 4.23.4.3 of TS 23.502 [3] by replacing the I-SMF as V-SMF and replacing the SMF as H-SMF.

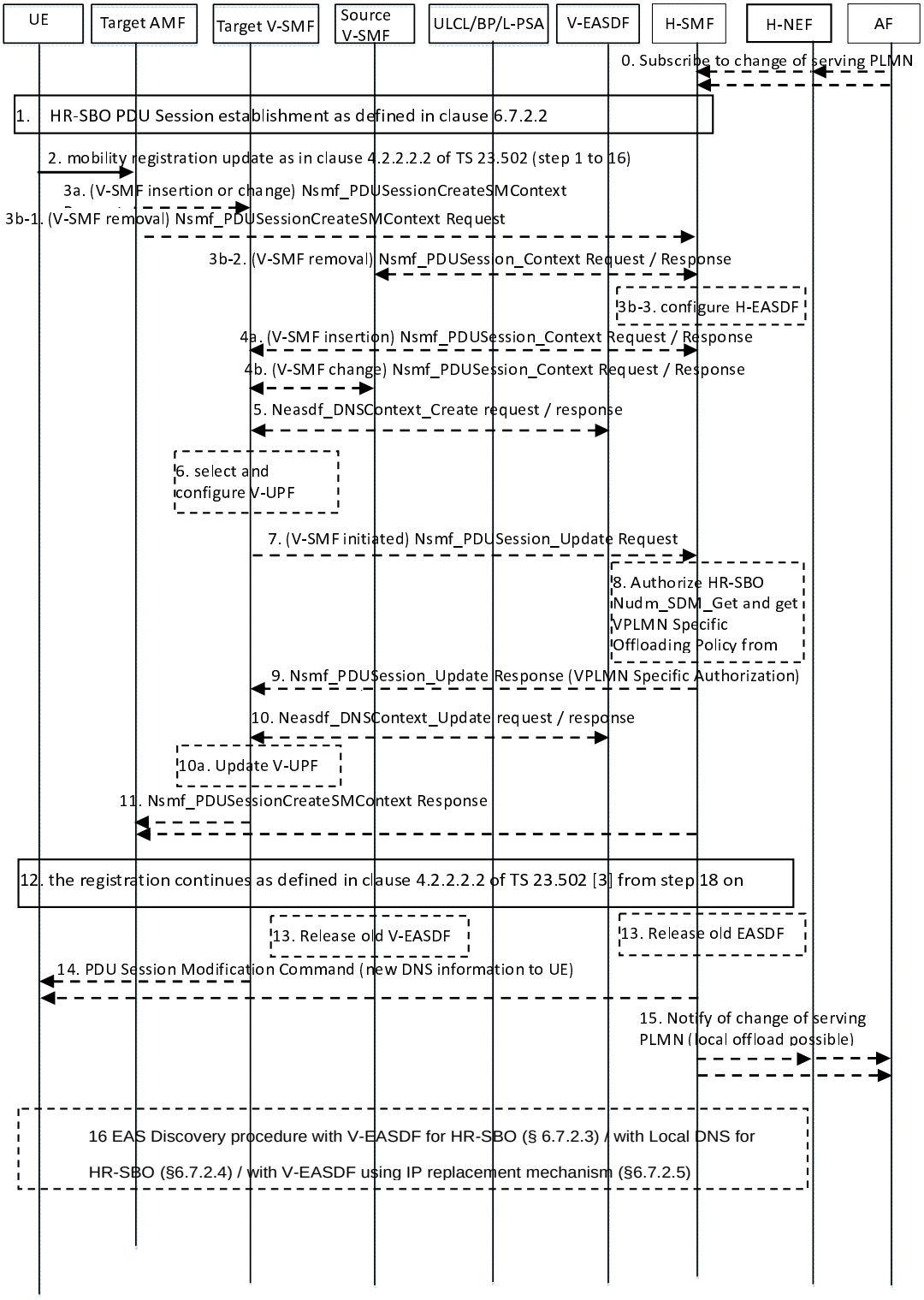

Figure 6.7.2.7-1: Inter V-SMF mobility registration update in HR-SBO

0. Same as step 0 of Figure 6.7.2.6-1.

1. The UE establishes a HR-SBO PDU Session as described in clause 6.7.2.2.

2. The UE initiates Mobility Registration Update procedure to the Target AMF as described in clauses 4.23.3 and 4.2.2.2.2 of TS 23.502 [3]. During the registration procedure, the target AMF (in roaming case) receives the SMF selection data including HR-SBO allowed indication per DNN/S-NSSAI from the UDM in the step 14b of the procedure in clause 4.2.2.2.2 of TS 23.502 [3].

3a. (V-SMF insertion or V-SMF change): at step 17 of clause 4.2.2.2.2 of TS 23.502 [3], the Target AMF selects and inserts a V-SMF supporting HR-SBO and provides the received HR-SBO allowed indication for the established Session for DNN, S-NSSAI in the PDUSession_CreateSMContext Request sent to the target V-SMF.

3b. (V-SMF removal) in case the Target AMF is an AMF of HPLMN (the UE moves from a VPLMN to HPLMN), in step 3b-1, the Target AMF sends a PDUSession_CreateSMContext Request sent to the H-SMF. In step 3b-2, the H-SMF retrieves SM Context from the V-SMF by invoking Nsmf_PDUSession_Context Request. The H-SMF may select an EASDF in HPLMN and configure the DNS context in this EASDF (Neasdf_DNSContext_Create) and may select and configure UPF(s) in HPLMN as in step 3b-3. For the V-SMF removal case, the steps 4 to 10 are skipped.

4a. (V-SMF insertion case) The (target) V-SMF retrieves SM context from H-SMF using Nsmf_PDUSession_Context Request/Response, followed by the Nsmf_PDUSession_Context Request/Response.

4b. (V-SMF change case) The target V-SMF retrieves SM context from the source V-SMF using Nsmf_PDUSession_Context Request/Response indicating HR-SBO support in the Request in the case of an intra-PLMN V-SMF case.

In step 4b, if source and target V-SMFs belong to same VPLMN, the SM context from the source V-SMF includes Authorization Result for HR-SBO, VPLMN Specific Offloading Information and/or corresponding Offload Identifier(s) and (if previously received by source V-SMF from H-SMF) the HPLMN address information, and the DNS Server address provided by the HPLMN.

NOTE 1: Step 4b in inter PLMN case (the target V-SMF retrieves SM context from the source V-SMF) assumes inter PLMN agreements on context exchange at both AMF and V-SMF levels.

5. As in step 4 of Figure 6.7.2.6-1, the (target) V-SMF may invoke Neasdf_DNSContext_Create.

6. As in step 5 of Figure 6.7.2.6-1, the (target) V-SMF may perform UL CL/BP and local PSA insertion/change/removal.

7. The target V-SMF invokes Nsmf_PDUSession_Update Request to the H-SMF as in step 7 of Figure 6.7.2.6-1.

8. As in step 8 of Figure 6.7.2.6-1, the H-SMF invokes Nudm_SDM_Get service, authorizes the request for HR-SBO based on the SM subscription data, and retrieves the VPLMN Specific Offloading Policy from H-PCF in case the HR-SBO is authorized.

9. As in step 9 of Figure 6.7.2.6-1, once the HR-SBO is authorized, the H-SMF sends the VPLMN Specific Offloading Information in the Nsmf_PDUSession_Update Response message to the target V-SMF.

NOTE 2: For the inter-PLMN case, the H-SMF sends VPLMN Specific Offloading Information related with the target VPLMN, which could be different from the one for source VPLMN.

10. As in step 9 of Figure 6.7.2.6-1, the (target) V-SMF may configure the V-EASDF based on the received VPLMN Specific Offloading Information.

10a. The (target) V-SMF may also update the configuration of the V-UPF based on the received VPLMN Specific Offloading Information.

11. As in step 6 of Figure 6.7.2.6-1, the target V-SMF (in the case of V-SMF removal, the H-SMF) answers to the target AMF with PDUSession_CreateSMContext Response.

12. The registration procedure continues as defined in clause 4.2.2.2.2 of TS 23.502 [3] from step 18 on.

13. In the case of V-SMF removal or change, when, at step 17a of clause 4.23.4.3 of TS 23.502 [3], receiving Nsmf_PDUSession_ReleaseSMContext Request from the source AMF, the source V-SMF initiates a Neasdf_DNSContext_Delete if a V-EASDF was used for the PDU Session.

In the case of V-SMF insertion, when at step 9 the H-SMF sends to the V-SMF VPLMN Specific Offloading Information in Nsmf_PDUSession_Update Response, the DNS context in the old EASDF may be removed by the H-SMF using Neasdf_DNSContext_Delete service.

14. (V-SMF insertion or V-SMF change): The target V-SMF sends the DNS information for the UE (received at step 9) and EAS rediscovery indication via PCO in a PDU Session Modification Command sent to the UE.

(In the case of V-SMF removal): the H-SMF sends the DNS information (received at step 3) for the UE and EAS rediscovery indication via PCO in a PDU Session Modification Command sent to the UE.

15. As in step 13 of Figure 6.7.2.6 -1, notification from H-SMF to the AF either via H-NEF or directly to the AF.

16. As in step 14 of Figure 6.7.2.6 -1: EAS discovery procedure by UE may take place.

6.7.2.8 N2 Handover without V-SMF change in HR-SBO case

This clause defines the procedure for intra-VPLMN N2-based handover without V-SMF change for HR-SBO PDU Session. This procedure is based on Inter NG-RAN node N2-based handover without I-SMF change defined in TS 23.502 [3] clause 4.23.7.2.

The procedure described in clauses 4.23.17, 4.23.7.2, 4.9.1.3.2 and 4.9.1.3.3 of TS 23.502 [3] is performed by replacing I-SMF with V-SMF and SMF with H-SMF with following modifications:

- Preparation phase, step 3 of clause 4.9.1.3.2: the source AMF provides the target AMF with whether HR-SBO is allowed for each PDU Session of the UE.

- Preparation phase, after step 4 of clause 4.9.1.3.2:

  For EAS discovery with V-EASDF as described in clause 6.7.2.3, the V-SMF may (re-)select a new V-EASDF or reuse the existing V-EASDF based on the target UE location. The V-SMF may invoke Neasdf_DNSContext_Create including the DNN, S-NSSAI and HPLMN ID to obtain the new V-EASDF address.

  For EAS discovery with local DNS server as described in clause 6.7.2.4, the V-SMF may (re-)select a local DNS server, e.g. based on the target UE location.

- Preparation phase, steps 5-6 of clause 4.9.1.3.2:

  The V-SMF may perform UL CL/BP and local PSA insertion/change/removal as described in step 2 of Figure 6.7.2.2-1.

NOTE: When there are other V-UPF(s) between UL CL/BP and H-UPF, the V-SMF sets up user plane between this ULCL/BP and the V-UPF.

- Execution phase, after step 7 of clause 4.9.1.3.3:

  The V-SMF removes the DNS Context in the old V-EASDF if a new V-EASDF is selected.

- Execution phase, step 10a of clause 4.23.7.2.3and 4.9.1.3.3:

  The V-SMF invokes Nsmf_PDUSession_Update Request toward the H-SMF.

  If a V-EASDF or a local DNS server has been selected, the selected V-EASDF or local DNS server address is provided in the request. The V-SMF needs not provide the selected V-EASDF or local DNS server address if the V-SMF is configured to use EAS discovery with V-EASDF using IP replacement mechanism corresponding to clause 6.7.2.5.

  If the UE indicated support of refreshing stale EAS information, the V-SMF may also provide an EAS rediscovery indication and EAS information to be refreshed for EAS re-discovery corresponding to the old target DNAI if it has been inserted by the V-SMF.

  The H-SMF invokes Nsmf_PDUSession_Update Response toward the V-SMF including the PCO for the UE. The PCO may includes V-EASDF or local DNS Server address, EAS rediscovery indication and impact field which is generated based on EAS information to be refreshed for EAS re-discovery.

- Execution phase, after step 10 of clause 4.9.1.3.3:

  The V-SMF sends the PCO in a PDU Session Modification Command sent to the UE.

6.7.2.9 Xn Handover with V-SMF change in HR-SBO case

This clause defines the procedure for Xn handover with intra-PLMN V-SMF change for HR-SBO PDU Session. This procedure is based on Xn based handover with re-allocation of I-SMF defined in TS 23.502 [3] clause 4.23.11.3.

The procedure described in clauses 4.23.17 and 4.23.11.3 of TS 23.502 [3] is performed by replacing I-SMF with V-SMF and SMF with H-SMF with following modifications:

- step 4 of clause 4.23.11.3:

  The target V-SMF retrieves SM context from the source V-SMF.

  - The SM context includes Authorization Result for HR-SBO, VPLMN Specific Offloading Information. It may also include Offload Identifier(s).

  - The SM context also includes (if previously received by source V-SMF from H-SMF) the HPLMN address information, and the DNS Server address provided by the HPLMN.

  - The SM context also includes EAS information to be refreshed for EAS rediscovery, i.e. the FQDN(s) corresponding to the old target DNAI if it has been inserted by the source V-SMF.

  The V-SMF selects a new V-EASDF, e.g. based on the target UE location. The V-SMF may invoke Neasdf_DNSContext_Create including the DNN, S-NSSAI and HPLMN ID to obtain the new V-EASDF address.

  To support EAS discovery with local DNS server as described in clause 6.7.2.4, the V-SMF selects a local DNS server, e.g. based on the target UE location.

  The V-SMF may perform UL CL/BP and local PSA insertion as described in step 2 of Figure 6.7.2.2-1.

  NOTE: When there are other V-UPF(s) between UL CL/BP and H-UPF, the V-SMF sets up user plane between this ULCL/BP and the V-UPF.

- step 6 of clause 4.23.11.3:

  If a V-EASDF or a local DNS server has been selected in step 4, the selected V-EASDF or local DNS server address is provided in the Nsmf_PDUSession_Update Request.

  The target V-SMF needs not provide the selected V-EASDF or local DNS server address if the target V-SMF is configured to use EAS discovery with V-EASDF using IP replacement mechanism corresponding to clause 6.7.2.5.

  If the UE indicated support of refreshing stale EAS information, the target V-SMF may also provide an EAS rediscovery indication and EAS information to be refreshed for EAS re-discovery if received in step 4 to the H-SMF.

- step 9 of clause 4.23.11.3: the H-SMF includes the same HR-SBO related information as sent by the H-SMF in step 2 of Figure 6.7.2.2-1.

  The H-SMF furthermore provides the target V-SMF with EAS rediscovery indication to be sent to the UE and also impact field based on the EAS information to be refreshed for EAS re-discovery if received at step 6.

  The target V-SMF configures the V-EASDF with the DNS handling rules as defined in step 3 of Figure 6.7.2.2-1.

  If the target V-SMF has interacted with the V-EASDF in step 4, the target V-SMF invokes Neasdf_DNSContext_Update Request including UE IP address to complete the configuration of the context in the V-EASDF.

  The target V-SMF may configure the V-UPF selected in the step 4 to forward DNS messages to V-EASDF.

  When the target V-SMF is configured to use EAS discovery with V-EASDF using IP replacement mechanism as described in clause 6.7.2.5, the V-SMF configures the UPF in the VPLMN with the IP replacement information (i.e. IP address of the DNS server provided by the HPLMN, the selected V-EASDF IP address and port number and DNS traffic filtering rules related with when IP replacement applies).

The target V-SMF sends the PCO including the V-EASDF address/local DNS server address, EAS rediscovery, impact field for the UE in a PDU Session Modification Command sent to the UE.

- step 12a of clause 4.23.11.3:

  When the AMF invokes Nsmf_PDUSession_ReleaseSMContext Request to inform the Source V-SMF to release the SM context of the PDU Session, the DNS context in the old V-EASDF is removed by the source V-SMF using Neasdf_DNSContext_Delete service.

6.7.2.10 Xn Handover without V-SMF change in HR-SBO case

This clause defines the procedure for Xn handover without V-SMF change for HR-SBO PDU Session. This procedure is based on Xn based handover without change of I-SMF defined in TS 23.502 [3] clause 4.23.11.5.

The procedure described in clauses 4.23.17 and 4.23.11.5 of TS 23.502 [3] is performed by replacing I-SMF with V-SMF and SMF with H-SMF with following modifications:

- step 2 of clause 4.23.11.5:

  When the V-SMF receives Nsmf_PDUSession_UpdateSMContext Request, the V-SMF may (re-)select a new V-EASDF or reuse the existing V-EASDF based on the target UE location. The V-SMF may invoke Neasdf_DNSContext_Create including the DNN, S-NSSAI and HPLMN ID to obtain the new V-EASDF address.

  For EAS discovery with local DNS server as described in clause 6.7.2.4, the V-SMF may (re-)select a local DNS server, e.g. based on the target UE location.

  The V-SMF may perform UL CL/BP and local PSA insertion/change/removal as described in step 2 of Figure 6.7.2.2-1.

NOTE: When there are other V-UPF(s) between UL CL/BP and H-UPF, the V-SMF sets up user plane between this ULCL/BP and the V-UPF.

  The V-SMF invokes Nsmf_PDUSession_Update Request toward the H-SMF.

    If a V-EASDF or a local DNS server has been selected, the selected V-EASDF or local DNS server address is provided in the request. The V-SMF needs not provide the selected V-EASDF or local DNS server address if the V-SMF is configured to use EAS discovery with V-EASDF using IP replacement mechanism corresponding to clause 6.7.2.5.

    If the UE indicated support of refreshing stale EAS information, the V-SMF may also provide an EAS rediscovery indication and EAS information to be refreshed for EAS re-discovery corresponding to the old target DNAI if it has been inserted by the V-SMF.

    The V-SMF is responsible of when to remove the context in the old V-EASDF.

- step 6 of clause 4.23.11.5:

  The Nsmf_PDUSession_Update Response sent by the H-SMF towards the V-SMF includes the PCO for the UE. The PCO may include V-EASDF or local DNS Server address, EAS rediscovery indication and impact field which is generated based on EAS information to be refreshed for EAS re-discovery.

  The V-SMF sends the PCO in a PDU Session Modification Command sent to the UE.

6.7.3 EAS Re-discovery and Edge Relocation Procedure

6.7.3.1 General

The EAS re-discovery and edge relocation in VPLMN can be triggered due to UE mobility, AF interacting with HPLMN, or AF interacting with VPLMN.

6.7.3.2 Network triggered EAS change in HR-SBO context

Figure 6.7.3.2-1 shows the procedure of EAS re-discovery and edge relocation when HR-SBO is supported and allowed in the target serving PLMN.

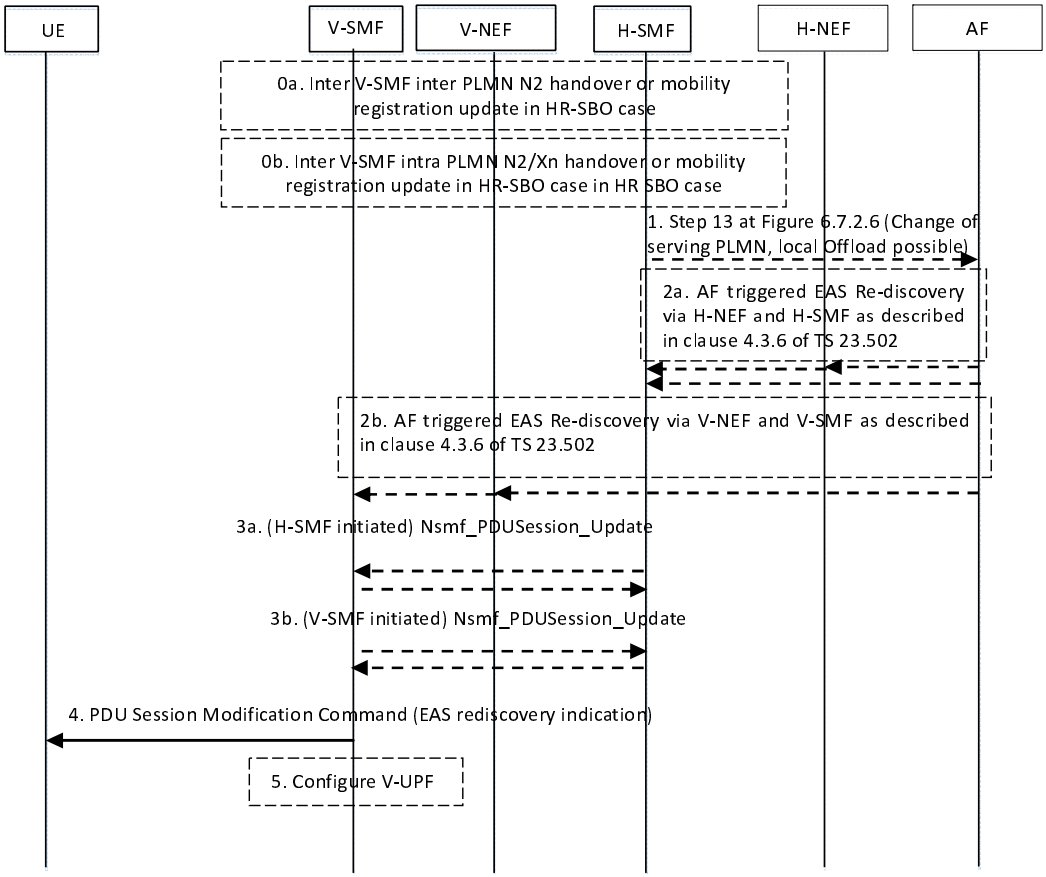

Figure 6.7.3.2-1: Network triggered EAS rediscovery and edge relocation in HR-SBO context procedure

0. The procedures described in clauses 6.7.2.6, 6.7.2.7 and 6.7.2.9 are performed: inter V-SMF inter-PLMN N2 handover or mobility registration (0a) in the HR-SBO case; or inter V-SMF intra-PLMN N2 handover or Xn handover or mobility registration update (0b) in the HR-SBO case.

1. In the case of the procedures happened in step 0a, if the AF had subscribed to the corresponding event and a serving PLMN change occurred towards a PLMN where local traffic offload is possible for the PDU Session, the H-SMF notifies the AF, indicating the new serving PLMN ID as well as HPLMN DNN and S-NSSAI for HR-SBO session and H-SMF may include capability of supporting EAS IP replacement in 5GC with PLMN ID of VPLMN. This may take place as soon as the H-SMF has received an indication of Handover Complete (see step 13 of Figure 6.7.2.6-1).

NOTE: Via this mechanism, the AF is aware of the PLMN to contact to issue traffic influence requests for HR-SBO sessions, if available, with HPLMN DNN and S-NSSAI information. The AF is assumed to check whether it has an SLA with the new serving PLMN. If the AF has no SLA with the new serving VPLMN, the AF interacts with H-NEF to issue traffic influence requests.

This may trigger the AF triggered edge relocation / EAS rediscovery as defined in step 1b of Figure 6.2.3.3-1 and in step 4a of Figure 6.3.3.1.1-1.

2a. For AF triggered EAS re-discovery and edge relocation via interacting with HPLMN, the AF may indicate the EAS rediscovery for the impacted applications, which are identified by Application Identifier(s), to the H-PCF via the H-NEF for the H-AF untrusted, or directly to the H-PCF for the AF trusted, then transfer to the H-SMF and optional H-NEF, H-UDR using the AF influence on traffic routing procedure as described in clause 4.3.6 of TS 23.502 [3]. The AF may also provide EAS IP replacement information and target DNAI together with an

indication of the PLMN associated with this target DNAI, i.e. the serving PLMN ID in the case that the VPLMN (V-SMF) supports EAS IP replacement capability and has already notified this capability information to AF (directly or via H-SMF/H-NEF).

NOTE: V-SMF providing the capability of supporting EAS IP replacement to AF can happen either:

- during V-SMF insertion/change phase where the capability information is provided to H-SMF and then to AF via H-NEF as noted in step 1; or
- as part of PDU session update respond procedure that is initiated by H-SMF in step 3a.

2b. For AF triggered EAS re-discovery and edge relocation via interacting with serving VPLMN, the AF may indicate the EAS rediscovery for the impacted applications via the V-NEF using the procedure described in clause 4.3.6 of TS 23.502 [3].

This may trigger step 2 of Figure 6.2.3.3-1 where the SMF that initiates PDU Session modification is the V-SMF that initiates Nsmf_PDUSession_Update request with the requested PCO.

The AF may also provide EAS IP replacement information and target DNAI to the VPLMN (i.e. V-SMF). In this case, steps 3-4 are skipped. If the V-SMF cannot serve the target DNAI, it triggers V-SMF change/removal, and the EAS IP replacement information and target DNAI may be provided in SM context as described in clause 6.7.2.6.

3a. (For AF triggered EAS re-discovery and edge relocation via interacting with HPLMN case): The AF traffic influence request information is sent to H-SMF via PCC rule. This may trigger step 2 of Figure 6.2.3.3-1 where the SMF that initiates the PDU Session modification is the H-SMF. The H-SMF issues a Nsmf_PDUSession_Update request . The Nsmf_PDUSession_Update request includes policies due to AF provided traffic influence information, which may also contain EAS IP replacement information and target DNAI provided by AF in step 2. If the V-SMF cannot serve the target DNAI, it invokes a Nsmf_PDUSession_SMContextStatusNotify service operation to send the target DNAI to AMF, and the AMF selects a target V-SMF based on the target DNAI as described in clause 4.23.5.4 of TS 23.502 [3] by replacing I-SMF with V-SMF. The target V-SMF retrieves SM context from the source V-SMF using Nsmf_PDUSession_Context Request/Response, containing Authorization Result for HR-SBO, EAS IP replacement information and target DNAI in the Request. The target V-SMF may select a new V-EASDF as described from steps 2 to 12 in Figure 6.7.2.6-1.

3b. (For AF triggered EAS re-discovery and edge relocation via interacting with VPLMN case): The V-SMF initiates Nsmf_PDUSession_Update request with the EAS rediscovery indication and the impact field to the H-SMF, and the H-SMF initiates Nsmf_PDUSession_Update Response towards the (target) V-SMF including the PCO information to be sent to the UE as described in step 2 of Figure 6.2.3.3-1. In intra-PLMN V-SMF change, the target V-SMF may use the source and target DNAI to determine the Impact field to be sent to the UE. In inter-PLMN mobility, the target V-SMF provides EAS rediscovery information without an Impact field.

4. The V-SMF may initiate PDU Session Modification command including the PCO to the UE.

The PCO may include EAS rediscovery indication (optional) and the impact field (optional).

5 The V-SMF may configure the V-UPF (UL CL and L-PSA) with EAS IP replacement information.

6.7.4 AF request on PDU Sessions supporting HR-SBO

For HR-SBO PDU Sessions, the AF may interact with VPLMN or HPLMN in order to send an AF request to influence traffic routing. The AF is assumed to check whether it has an SLA with the serving PLMN. If the AF has no SLA with the serving VPLMN, the AF interacts with HPLMN (H-NEF or H-PCF) to issue traffic influence requests.

Ife the AF has an SLA with the serving VPLMN, the AF in VPLMN may send to V-NEF an AF request to influence traffic routing. The AF request for the HR-SBO PDU Session from the AF is stored as Application Data (Data Subset = AF traffic influence request information) in the UDR of VPLMN as described in clause 4.3.6 of TS 23.502 [3]. NEF determine if HR-SBO is applicable as described in clause 4.3.6 of TS 23.502 [3]). To obtain the AF traffic influence request information, the V-SMF managing the PDU Session supporting HR-SBO subscribes to the NEF in VPLMN for notification of Application Data modification as specified in clause 4.3.6 of TS 23.502 [3].

If the AF has no SLA with the serving VPLMN, the AF in HPLMN may send to H-NEF (or H-PCF directly) an AF request to influence traffic routing (e.g. for the purpose of subscription to UP path management events on HR-SBO

Sessions in VPLMN) for HR-SBO session in VPLMN. In response to receiving the traffic influence request, the H-PCF may generate or update one or more PCC rules based on the traffic influence request. PCC rule that may contain information about the VPLMN DNAI(s) towards which the traffic routing should apply, and H-PCF sends an update notification to H-SMF.

The H-SMF may send to the V-SMF the received Application Function influence on traffic routing Enforcement Control (i.e. received in PCC rules from the H-PCF).

The H-SMF may also determine Application Function influence on traffic routing Enforcement Control information related to the VPLMN and provides the VPLMN-related Application Function influence on traffic routing Enforcement Control information to the V-SMF due to AF triggered EAS re-discovery or edge relocation as described in step 3a of Figure 6.7.3.2-1.

6.8 Support for mapping between EAS address Information and DNAI

6.8.1 General

In order to make sure the AF can query for DNAIs, the 5GS may help determine proper DNAI(s) and notify the information to AF based on AF request providing EAS address information (i.e. IP address(es), EAS IP range(s) or FQDN(s)).

NEF/UDR is configured by OAM with the mapping information between EAS IP address information and DNAI. AF may subscribe the mapping information modification to NEF. AF may request immediate reporting. When the configuration information (relationship between DNAI and EAS address information) is changed, the UDR can notify the new mapping information to NEF. When the mapping information is stored in UDR, NEF may subscribe to mapping information in UDR, where NEF may request immediate reporting. If subscribed to information change, the UDR notifies the NEF with all the corresponding mapping information it has stored for the relevant DNN and/or S-NSSAI, and the NEF notifies the AF.

The EAS address and DNAI Mapping Information record in UDR is shown Table 6.8.1-1. The information elements for the NEF service Nnef_DNAIMapping_Subscribe is specified in clause 5.2.6.8 of TS 23.502 [3].

Table 6.8.1-1: Description of EAS address and DNAI Mapping Information

Parameters	Description
EAS address information	IP address(es) of the EASs or the IP address ranges (IPv4 subnetwork(s) and/or IPv6 prefix(es)) or FQDN(s) where the EAS is deployed for each DNAI. [Mandatory]
DNAI(s)	DNAI(s) for the EAS Deployment information. [Mandatory]
DNN	DNN for the EAS Deployment Information. [Conditional] (NOTE 1)
S-NSSAI	S-NSSAI for the EAS Deployment Information. [Conditional] (NOTE 1)
NOTE 1: At least one of DNN or S-NSSAI shall be present.	

6.8.2 AF request for DNAI Procedures

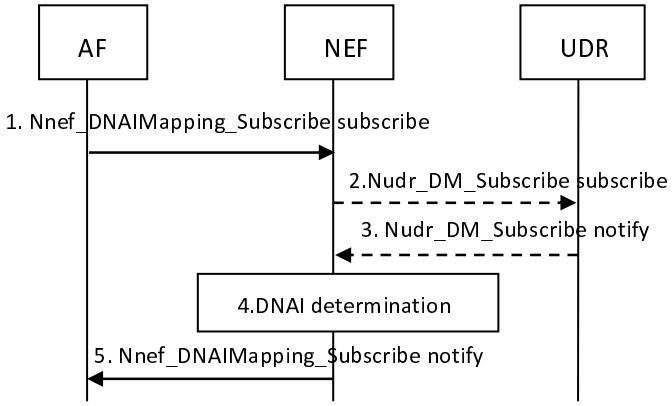

Figure 6.8.2-1: AF request for DNAI based on AF request

1. AF invokes Nnef_DNAIMapping_Subscribe service to request the DNAI information. The request includes EAS address information and optionally: DNN, S-NSSAI and AF Identifier.

   If mapping information is stored in NEF, skip step 2-3.

2. If the mapping information is stored in UDR, the NEF determines the DNN and/or the S-NSSAI if not received from the AF, potentially using the AF identifier. If the NEF has not yet received the DNAI mapping information for this DNN and/or S-NSSAI, NEF invokes the Nudr_DM_Subscribe service to subscribe to DNAI mapping information for this DNN and/or S-NSSAI.

3. UDR notifies the NEF with all the DNAI mapping information for the requested DNN/S-NSSAI.

4. NEF determines the suitable DNAI(s) using the DNAI mapping information.

5. NEF notifies the DNAI(s) or the updated DNAI information to AF corresponding to the request in step 1.

   If DNAI information is stored in the UDR, whenever the DNAI mapping information change, steps 3 to 5 take place.

7 Network Function Services and Descriptions

7.1 EASDF Services

7.1.1 General

The following table illustrates the EASDF Services and Service Operations.

Table 7.1.1-1: NF services provided by the EASDF

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Neasdf_DNSContext	Create	Request/Response	SMF
	Update	Request/Response	SMF
	Delete	Request/Response	SMF
	Notify	Subscribe/Notify	SMF
Neasdf_BaselineDNSPattern	Create	Request/Response	SMF
	Update	Request/Response	SMF
	Delete	Request/Response	SMF

7.1.2 Neasdf_DNSContext Service

7.1.2.1 General

Service description: This service enables the consumer to create, update, or delete DNS context in EASDF and to Subscribe to DNS message related reporting from EASDF.

DNS contexts in EASDF include rules on how EASDF is to handle DNS messages.

This service also can be supported by V-EASDF in VPLMN for HR scenario supporting HR-SBO.

7.1.2.2 Neasdf_DNSContext_Create Service Operation

Service operation name: Neasdf_DNSContext_Create

Description: Create a DNS context in EASDF.

Input, Required: UE IP address, DNN, S-NSSAI, Notification Endpoint.

Input, Optional: HPLMN ID, DNS message handling rules, N6 traffic routing information (towards the Local PSA-UPF).

NOTE 1: In HR-SBO scenario, the V-SMF can invoke Neasdf_DNSContext_Create service in order to obtain the IP address of the V-EASDF while the UE UP address has not yet been determined. If the V-SMF is not aware of the UE IP address when invoking this service operation, the V-SMF can set UE IP address as unspecified such as zero value.

DNS message detection and Actions(s) are specified in clause 6.2.3.2.2.

NOTE 2: N6 traffic routing information can contain the IP address the Local PSA-UPF.

Output, Required: If successful, IP address of the EASDF, EASDF Context ID, Result Indication.

Output, Optional: DNS Security Information of EASDF.

7.1.2.3 Neasdf_DNSContext_Update Service Operation

Service operation name: Neasdf_DNSContext_Update

Description: Update the DNS context in EASDF, or indicate EASDF to forward the DNS Response to UE.

Input, Required: EASDF Context ID, updated DNS message handling rules.

Input, Optional: UE IP address, N6 traffic routing information (towards the Local PSA-UPF).

NOTE: In HR-SBO scenario, the V-SMF can provide the UE IP address received from the H-SMF to update DNS Context of the V-EASDF via this Service Operation.

Output, Required: Result Indication.

Output, Optional: None.

7.1.2.4 Neasdf_DNSContext_Delete Service Operation

Service operation name: Neasdf_DNSContext_Delete

Description: Delete the DNS context in EASDF.

Input, Required: EASDF Context ID.

Input, Optional: None.

Output, Required: Result Indication.

Output, Optional: None.

7.1.2.5 Neasdf_DNSContext_Notify Service Operation

Service operation name: Neasdf_DNSContext_Notify

Description: EASDF reports DNS message related information to the consumer when receiving DNS Query or DNS Response.

Input, Required: DNS message reporting information (DNS message content specified in clause 6.2.3.2.2 and corresponding DNS message type), Notification Endpoint.

Input, Optional: DNS message identifier.

Output, Required: Result Indication.

Output, Optional: None.

7.1.3 Neasdf_BaselineDNSPattern Service

7.1.3.1 General

This service provides the capability to create, update or remove BaselineDNSPattern in EASDF. See clause 6.2.3.4.4 for detailed procedure.

7.1.3.2 Neasdf_BaselineDNSPattern_Create Service Operation

Service operation name: Neasdf_BaselineDNSPattern_Create

Description: Create the BaselineDNSPattern in EASDF.

Input, Required: BaselineDNSPattern.

Input, Optional: None.

Output, Required: Success or Failure.

Output, Optional:

7.1.3.3 Neasdf_BaselineDNSPattern_Update Service Operation

Service operation name: Neasdf_BaselineDNSPattern_Update

Description: Update the BaselineDNSPattern in EASDF.

Input, Required: Updated BaselineDNSPattern.

Input, Optional: None.

Output, Required: Success or Failure.

Output, Optional: None.

7.1.3.4 Neasdf_BaselineDNSPattern_Delete Service Operation

Service operation name: Neasdf_BaselineDNSPattern_Delete

Description: Delete the BaselineDNSPattern in EASDF.

Input, Required: Baseline DNS message detection template ID and/or Baseline DNS handling actions ID.

Input, Optional: None.

Output, Required: Result.

Output, Optional: None.

Annex A (Informative): EAS Discovery Using 3rd Party Mechanisms

There are different IP discovery mechanisms existing in the application layer. For example, the application client can generate the DNS Query outside of DNS libraries in the OS with DoT, DoH or other over the top mechanisms.

The third party can also deploy a service scheduling server to determine the (E)AS IP address based on the UE's HTTP(S) request. In this case, the DNS firstly resolves the FQDN in the DNS Query of the UE into the IP address of the service scheduling server and then the UE contacts the service scheduling server that can provide the IP address of the EAS that the UE is then to contact.

For the Distributed Anchor Point connectivity model, in order to enable EAS discovery by third party mechanisms, the DNS Server or service scheduling server in the third party could be pre-configured with mapping information between the IP address range which can correspond to the Central PSA UPF or other entities (e.g. a NAT server) on the N6 interface and EAS information. In this case, the DNS Server or service scheduling server in the third party can take the source IP address of the UE request as the location information of UE. The DNS and/or service scheduling server pre-configuration can be based on the agreement between the MNO and service provider.

For the Session Breakout connectivity model, based on agreement with the operator, a possible solution for the service scheduling server is as follows:

- The IP address of the service scheduling server can be set as a condition in the ULCL UPF to offload traffic. The IP address of service scheduling server can be pre-configured or resolved by the EASDF based on procedure defined in clause 6.2.2.2.

- NAT server can be deployed in the L- DN or local N6 interface, in order that the source IP address of the UE request sent to the service scheduling server can correspond to the UE location related information.

NOTE: Otherwise, the source IP address of the UE request message sent to the third party DNS server / service scheduling server is bound with the central PSA UPF, so it's impossible for the third party DNS server / service scheduling server to know which local EAS address could be allocated to the UE.

Based on the mapping relationship between the IP ranges of UE request and the EAS information, the EAS IP address can be allocated to the UE. The above example is briefly shown in Figure A-1.

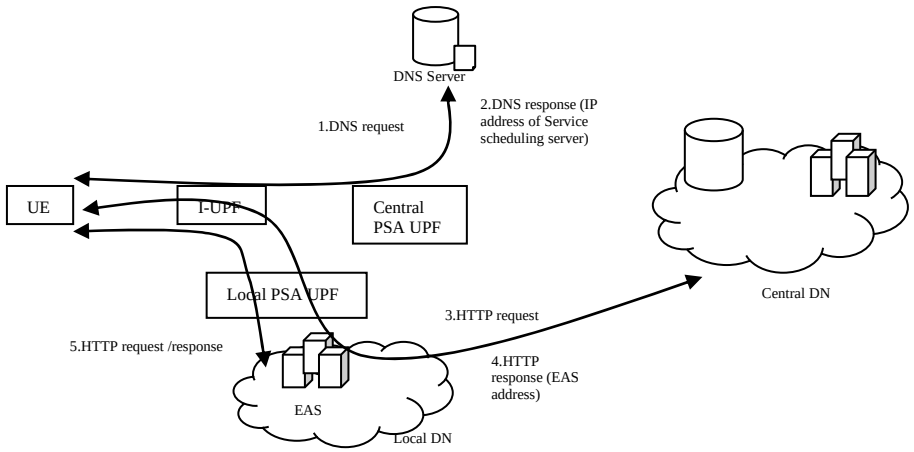

Figure A-1: Service scheduling server mechanism for Session Breakout connectivity model

Annex B (Informative): Application Layer based EAS (Re-)Direction

During the application relocation, the AF can reselect a new EAS for the UE. Reselection can be triggered by the AF when it receives a UP path change notification or by an internal trigger of the AF (e.g. load balancing, UE location change, etc.). When the new EAS is reselected, the UE is provided the new EAS address via application layer signalling. For example, the UE can receive the URL or FQDN of the new EAS once the application context relocation is complete and then use DNS to resolve the URL or FQDN. The UE can also obtain the new EAS address via HTTP redirection.

NOTE: The Application layer signalling between the AF (or Old EAS) and UE is application specific and is outside the scope of this specification.

Annex C (Informative): Considerations for EAS (re)Discovery

C.1 General

DNS records obtained from a DNS resolver in the network contains a time-to-live (TTL) value. This is a hint provided by the DNS resolver and can be used to determine the length of time that the record is to be cached. DNS records can be cached in the UE system wide (in OS) and/or applications. The application cache is managed on a per application basis while the system cache is common to applications. Name resolution caches in various applications also have different policies and behaviours. Some applications cache the DNS records for the length of the application session while others have a time limit. The recommendations in this TS will only work if the UE application (in case of DNS cache at the application layer) or the UE OS (in case of DNS cache shared by applications) consider indications from the UE modem layer with respect to DNS settings and DNS caching. Whether and how the UE (and application) considers the indication depends on implementation.

C.2 Impact of IP Addresses for DNS Resolver on UE

The UE can be configured by the 5GC with an IP address for the DNS resolver using ePCO or IPv6 Router Advertisement (RA), DHCPv4 or DHCPv6 as described in clause 5.8.2 of TS 23.501 [2]. 5GC can reconfigure the DNS resolver IP address using NAS or IPv6 Router Advertisement (RA). In case of anycast IP address is used for the DNS resolver, the 5GC can use UL CL/BP to branch out the DNS messages and the DN is responsible to route them to the closest instance of the MNO DNS resolver without having to reconfigure the DNS resolver IP address in the UE.

NOTE: 5GC is likely not to be able to reconfigure the DNS resolver IP address when DHCP is used to configure this information on the UE, e.g. in case of UE split. Applications in the UE can request the DNS resolver configured on the UE to resolve an FQDN. However, applications can also be configured with their own DNS resolver addresses and can use encrypted messaging based e.g. on DNS over HTTPS (DoH) or, DNS over TLS (DoT). Configuration of application DNS resolvers is out of scope of 5GC. DNS messages delivered over DoT, or DoH might be forwarded transparently to the destination addresses of the messages. The application DNS resolver can be operated by the 5GC operator or by a third party.

A network interface change, or NAS SM EAS rediscovery indication (explicitly as described in clause 6.2.3.3) or reconfiguration of DNS server address in NAS SM message that implicitly indicating EAS rediscovery as described in 6.2.3.2.3 can and should result in the UE OS/application clearing name/IP address translations in its DNS cache.

If a network interface change or NAS SM EAS rediscovery explicit indication or reconfiguration of DNS server address using NAS SM (i.e. implicit EAS rediscovery indication) does not result in the UE OS/application clearing name to IP address translations in its DNS cache, a subsequent DNS EAS address resolution request can result to address of old EAS.

During EPC to 5GC mobility without N26 interface, the UE can receive a new DNS server address different from the one received from the SMF+PGW-C during the PDN connection initiated in EPC. This can result in the UE OS clearing name/IP address translations in its DNS cache. During 5GC to EPC mobility without N26 interface, the UE can perform the same if it receives a new DNS server address from the SMF+PGW-C.

C.3 UE Considerations for EAS Re-discovery

A UE that complies with EAS (re-)discovery described in this specification is not recommended to override operator-provided DNS settings. This is necessary for the "closest" EAS server to be selected. Overriding the operator-provided DNS settings means that procedures requiring operator provided DNS server will not work.

NOTE 1: If the user overrides the DNS configuration set by the network using ePCO, for example if the user configures a private DNS configuration via UI, the network DNS configuration configured using ePCO could remain inactive until the user configured DNS setting is revoked by the user.

NOTE 2: If an OS, user or applications override the operator-provided DNS settings, the DNS resolvers or servers in the third party can take the source IP address of the DNS Query as the location information of UE, which can correspond to the remote PSA UPF or other entities (e.g. a NAT server) on the remote/central N6 interface which can lead to a non-optimal choice of the EAS server address.

NOTE 3: If the DNS server configuration in an OS overrides the operator provided DNS, the DNS Queries continue to be sent over the correct PDU Session for the application.

NOTE 4: If the UE (OS or application) uses a DNS resolver that is different than the one provided by the 5GC, then the Session Breakout connectivity mode, option A and B in clause 6.2.3.2 will not work if the EASDF is not in the DNS resolver chain for recursive DNS resolution.

C.4 UE Procedures for Session Breakout

In the session breakout connectivity model, the selection of a new session breakout path does not result in a new network interface indication at the UE.

NOTE: In the case of multiple sessions or distributed anchor point connectivity models, when there is a change of network interface, indication of network interface change can and should be used to flush the UE OS DNS cache.

Session breakout results in a NAS SM message indicating the need to redo DNS lookup sent by the SMF to the UE modem. Thus, in order to support some solutions of this specification, it is necessary for the operating system to receive information of EAS rediscovery from the modem when such signalling has been received and clear the DNS cache in UE OS.

C.5 Split-UE Considerations for EAS (Re-)discovery

For the split-UE (i.e. the TE and MT are separated), information provided by the SMF in the NAS message during the PDU Session Establishment, Modification and Command is provided to the MT and MTs cannot provide the NAS provided IP parameters to the TE, i.e. the TE cannot receive that information from the MT because of separation between the TE and MT. Example of information are the DNS configuration or Rediscovery indication.

The TE gets LAN side IP parameters configuration from the MT, i.e. using DHCPv4 (for IPv4) or IPv6 Router Advertisement/DHCPv6 (for IPv6). MT hosts the DNS resolver for TE and its address can be obtained from MT using DHCP or IPv6 RA. When TE uses DNS resolver in MT, the MT in turn uses its configured network DNS resolver (e.g. EASDF, L-DNS) which is the expected DNS resolution chain and it results in the discovery of the correct EAS. An application in the TE that complies with EAS (re-)discovery described in this specification is not recommended to override operator-provided DNS settings as described in clause C.3.

For the split-UE and MTs cannot provide the NAS information requesting UE to redo DNS lookup received from the SMF to the TE or the TE OS. In such cases, the closest EAS is still reachable, for example, if anycast EAS address is used.

For the Split-UE in the option C case, if the new address of Local DNS Server cannot be provided to the TE or the TE OS from the MT, so the TE continues to use the old DNS Server to perform the EAS discovery and cannot receive the DNS Query/Response from the 5GC (e.g. the BP will route the DNS Query to the L-PSA). After no DNS Query response is received from the 5GC for serval times or an information indicating the old DNS Server unreachable (e.g. ICMP message of Host Not Reachable), the TE initiates a new DNS Server Discovery via a DHCP message to the 5GC, and the SMF may send the same new DNS Server IP address to the UE in the DHCP response message than sent via PCO in the PDU Session Command. After the UE gets the new DNS Server IP address, the UE uses the new DNS Server IP address to perform the EAS (re-)discovery.

C.6 Detection of UE not using 5GC provided DNS server

The UPF Traffic detection and traffic reporting capabilities specified in clause 5.8 in TS 23.501 [2] can be used to monitor if the UE uses a DNS resolver that is different than the one provided by the 5GC, e.g.:

- the SMF can install Packet Detection Rule(s) in the UPF to report when the traffic matches certain well known public DNS service IP addresses;

- the UPF can have an Application Filter defined to detect DNS ports as well as if the DNS traffic not destined to operator provided DNS servers (e.g. EASDF). The SMF can refer to this filter using an application ID.

Annex D (Informative): Examples of AF Guidance to PCF for Determination of URSP Rules

a) The UE is to use a specific (DNN, S-NSSAI) (e.g. working in SSC mode 2 or 3 with the Distributed Anchor deployment) when trying to reach some domains while it should use another (DNN, S-NSSAI) (e.g. working in SSC mode 1) for other domains. In this example, the AF can indicate two FQDN filters, optionally with corresponding filtering rule priorities, if the FQDN filters overlap. For each FQDN filter, the AF can indicate a corresponding DNN, S-NSSAI.

b) Corporate applications only reachable via a specific (DNN, S-NSSAI) negotiated with the operator; corresponding URSP rules (URSP rules referring to domains of these corporate applications) shall only point to this specific (DNN, S-NSSAI). In this example, the AF can indicate one FQDN filter for the corporate applications. Optionally, the AF can indicate also the corresponding DNN, S-NSSAI for the FQDN filter. If DNN, S-NSSAI is not provided by the AF, the NEF can determine it based on the AF identity.

c) Corporate applications reachable via a (DNN, S-NSSAI) but only in some location; e.g. the corporate applications are only accessible when the UE is in some location corresponding to the corporate premises. In this example, the AF can provide information as in bullet b) and additionally provides where the corporate applications are accessible. URSP Rules will guide the UE select the (DNN, S-NSSAI) when the UE is in the geographical zone.

d) Internet applications not reachable via a specific (DNN, S-NSSAI) negotiated with the operator but that should be only reachable via a general purpose (DNN, S-NSSAI); e.g. traffic of UE(s) of a third party targeting Internet applications is not to be sent to a specific (DNN, S-NSSAI) negotiated with the operator as this traffic is not expected to cross the Intranet of the corporate. In this example, the default operator rules are used generate a "match all" URSP rule with a low filtering rule priority and a corresponding generic purpose DNN, S-NSSAI.

e) Internet applications reachable via both a specific (DNN, S-NSSAI) negotiated with the operator and via a general purpose (DNN, S-NSSAI) for which the third party may want to set preferences between these 2 kinds of connectivity. These preferences may depend on the UE location. In this example, the AF can indicate FQDN filters as in bullet b), but the FQDN filters are for Internet applications. In addition, the AF can indicate where the Internet applications are accessible via the specific DNN, S-NSSAI. In addition, the default operator rules are used generate a "match all" URSP rule with a low filtering rule priority and a generic purpose DNN, S-NSSAI.

f) Combination of bullets c) and e). In this example, the AF can indicate one FQDN filter for corporate applications as in bullet c) and another FQDN filter for Internet applications as in bullet c), In addition, the AF can indicate filtering rule priorities for the FQDN filters, if the FQDN filters overlap.

g) Corporate applications reachable via a (DNN, S-NSSAI) in some location and via another DNN, S-NSSAI in another location; e.g. the corporate applications are only accessible via a location specific corporate DNN, S-NSSAI. In this example, the AF can indicate an FQDN filter as in bullet c), but indicates two or more sets of location conditions for the FQDN filter and indicates different DNN, S-NSSAI for each. In addition, if the geographical zones overlap, the AF can indicate a Route Selection Descriptor Precedence for each of them.

The examples b) to e) above can correspond to different AF(s) representing different corporate that have different policies. How the rule precedence between rules for different AFs are set in the URSP rules is up to the operator policy.

In the examples above, when a location specific corporate DNN, S-NSSAI has been agreed, as an alternative, the location area where the DNN is accessible can also be set as part of the SLA agreement configured on the NEF.

Annex E (informative): EPS Interworking Considerations

E.1 General

5GC is specified to support interworking with EPC. Edge Computing deployments that use interworking need to consider the aspects outlined in this Annex.

E.2 Distributed Anchor

SSC mode 3 cannot be used when the UE is registered in EPC as 5G-NAS is not available. Re-establishing a PDN connection after releasing an old one can be done in EPS using the "reactivation requested" cause value in EPS bearer context deactivation (see clause 6.4.4.2 of TS 24.301 [7]), if the feature is supported by the EPS network.

E.3 Multiple Sessions

The URSP rules provided by 5GC to the UE are defined to cover both 5GS as well as EPS when interworking is applied. In EPS there is no possibility to provide new URSP rules to the UE, instead according to clauses 5.15.5.3 and 5.17.1.2 of TS 23.501 [2], the URSP rules provided to the UE when it was registered in 5GC can also be used when the UE is registered in EPC if HPLMN uses URSP (see TS 24.526 [8]).

AF guidance of URSPs may not take effect if the UE is in EPS and the UE does not use the URSP rules on EPS (see TS 24.526 [8] 4.4.2 for the use of URSP in EPS). Therefore, it is not deterministic when they will take effect, since PCF could have issued the URSP rules when the UE was on EPS (where URSP rules cannot be sent).

E.4 Session Breakout

As traffic offload via UL CL/BP is not supported over EPC, when a PDN connection is initiated in EPS or a PDU Session is handed-over to EPS, the SMF+PGW-C can send to the EASDF DNS message handling rules requesting the EASDF to transparently forward any DNS traffic. The SMF+PGW-C can send to the EASDF new DNS message handling rules (with actual reporting and actions as defined in clause 6.2.3.2.2) when the PDU Session/PDN connection is handed-over (back) to 5GS.

When a PDN connection is initiated in EPS, the SMF+PGW-C can also select a normal DNS Server (i.e. different from an EASDF) to serve the PDN Connection, and then indicate to the UE to use the EASDF as DNS Server when the PDU Session/PDN connection is moved to 5GS.

Annex F (Informative): EAS Relocation on Simultaneous Connectivity over Source and Target PSA

This annex describes how EAS relocation can make use of network capabilities that, at PSA change, provide simultaneous connectivity over the source and the target PSA during a transient period.

At PSA change, simultaneous connectivity to Application over former and new PSA allows the application to build its own EAS relocation solution and minimize the impact on latency:

- If the decision for when to start using a target EAS is taken by the application, this decision can consider application specific aspects, like for example, the time interval between packets or end of a video frame to minimize impact on latency.
- When there are multiple applications on a PDU Session, if connectivity over the former PSA is maintained for some time, each application can schedule EAS relocation to suit the application specific needs without interfering with the other applications.

The procedure is shown in below Figure F-1:

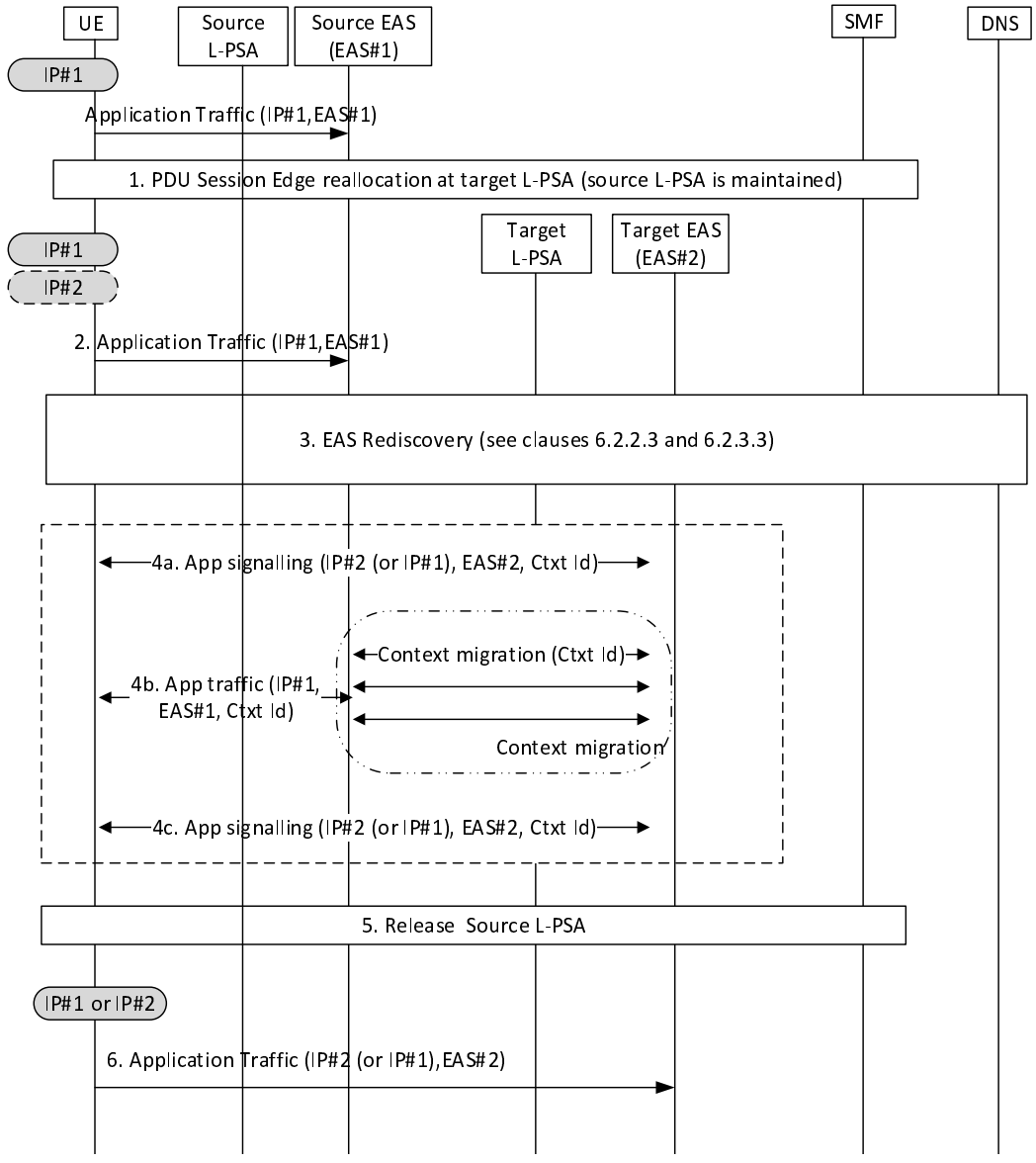

Figure F-1: EAS relocation on simultaneous connectivity over source and target PSA

The user has established a PDU Session. This PDU Session has a local PSA (source L-PSA), which could be the PSA of a PDU Session with Distributed Anchor connectivity or one additional local PSA of a PDU Session with Session Breakout. There has been an EAS Discovery procedure as described in clauses 6.2.2.2 and 6.2.3.2 (the procedure is conditioned to the connectivity model) for one or more applications. Application traffic is served by source EAS over the Local PSA.

1. User mobility triggers SMF to select a new Local PSA (target L-PSA) that is closer to current user location. In this scenario, the re-anchoring procedures that provide Simultaneous Connectivity over Source and Target PSA are described in TS 23.502 [3]:

   - For Distributed Anchor, in clause 4.3.5.2 for Change of SSC mode 3 PDU Session Anchor with multiple PDU Sessions and in clause 4.3.5.3 for Change of SSC mode 3 PDU Session Anchor with IPv6 Multi-homed PDU Session.

   - For Session Breakout, in clause 4.3.5.7 for Simultaneous change of Branching Point or UL CL and additional PSA for a PDU Session.

   The SMF may notify an AF for the early and/or late notifications on the UP-path change event as described in clause 4.3.6.3 in TS 23.502 [3].

2. When the connectivity is available on target L-PSA, the connectivity via source L-PSA is still available during certain time (that is provisioned and controlled as described in these TS 23.502 [3] procedures). The application traffic can continue to run over the established UE-EAS connections.

3. The EAS Rediscovery Procedures described in clauses 6.2.2.3 and 6.2.3.3 allow the UE to discover a new EAS (i.e. target EAS) for the application that is closer to the UE over the new path (there could be multiple triggers as described in those respective clauses). If multiple applications are being served by this PDU Session, each of them performs rediscovery. This discovery procedure may lead to EAS reselection.

4. New L4 connections may now be established between the UE and the target EAS with the following considerations:

   - For Distributed anchor or session breakout with MH, the UE uses the IP address /prefix associated with the target PSA (that is referred to as IP#2 in Figure F-1).

   - For Session breakout with ULCL, there has not been connection/IP address change. Same IP address is still used by UE (that is referred to as IP#1 in Figure F-1).

NOTE 1: If Session Breakout is used for connectivity and if the application wants to build service continuity on simultaneous connections, source EAS and target EAS cannot share the same IP address (e.g. by using anycast).

EAS Relocation may involve EAS context migration in the case of stateful applications. The following examples are part of the application implementation details and fall out of 3GPP specification scope:

- In case that SMF notifies an AF for the early and/or late notification in Step 1, based on the notifications, the AF can interact with the source Application server, which can recreate the context to the target EAS and then provide switching instructions to the Application client.

- The Application server can recreate the service context when first contacted by the client using a Context Id: when suitable, the application client sets up a connection to the target EAS including a Context Id. The target EAS uses this Context Id to retrieve the latest service context available and subsequent updates, if needed.

- The Application server can recreate the context when first contacted by the client using a Context Id: the application client sets up a connection to the target EAS but for some time it sends traffic to both source and target EAS. In this way it triggers the context migration before the actual EAS switch.

- The source Application server is able to provide the client with switching instructions when a new EAS is selected: upon UE request (if UE selected) or as an EAS initiative (if server selected), the source EAS provides the Application client with switching instructions while it continues to serve traffic and drives any context migration towards the selected target EAS.

NOTE 2: This application procedure may be designed to solve EAS relocation in all scenarios, not only when triggered by Edge Relocation, which may simplify the application design.

5. At some points all traffic for all applications in this session are sending traffic to their target EAS only and traffic ceases over the source L- PSA. The source L-PSA is then released. The timers should be set to allow EAS relocation.

6. UE only maintains connection(s) to target EAS(s).

Annex G (Informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2021-03	SA2#143E	S2-2100114	-	-	-	Proposed skeleton approved at S2#143E	0.0.0
2021-06	SA#92E	SP-210365	-	-	-	MCC editorial update for presentation to TSG SA#92E for information	1.0.0
2021-09	SA#93E	SP-210942	-	-	-	MCC editorial update for presentation to TSG SA#93E for approval	2.0.0
2021-09	SA#93E	-	-	-	-	MCC editorial update for publication after SA#93E approval	17.0.0
2021-12	SA#94E	SP-211290	0001	3	F	Correction related to uniqueness of Update related to a buffered DNS message in EASDF	17.1.0
2021-12	SA#94E	SP-211290	0003	-	F	Correction and removal of misleading Note	17.1.0
2021-12	SA#94E	SP-211290	0005	1	F	Not all EC scenarios requires EASDF	17.1.0
2021-12	SA#94E	SP-211290	0014	1	F	Clarify the local AF subscription for the QoS Monitoring during UE mobility	17.1.0
2021-12	SA#94E	SP-211290	0017	4	F	Updates on EAS Discovery Procedure with EASDF	17.1.0
2021-12	SA#94E	SP-211290	0018	3	F	Mega CR for minor fixes to TS 23.548	17.1.0
2021-12	SA#94E	SP-211290	0024	-	F	Update Neasdf_DNSContext services	17.1.0
2021-12	SA#94E	SP-211290	0030	4	C	EAS rediscovery: Edge DNS Client based EAS (re-)discovery	17.1.0
2021-12	SA#94E	SP-211290	0031	3	F	UE authorization for 5GC assisted EAS discovery	17.1.0
2021-12	SA#94E	SP-211290	0034	1	F	Updating related to EAS Discovery Procedure	17.1.0
2021-12	SA#94E	SP-211290	0035	1	F	Corrections on enabling EAS IP Replacement procedure by AF	17.1.0
2021-12	SA#94E	SP-211290	0036	1	F	Improvements and correction to annex C	17.1.0
2021-12	SA#94E	SP-211290	0038	1	F	Change of DNS server address during EPC IWK	17.1.0
2021-12	SA#94E	SP-211290	0039	1	F	Alignment of EASDF functional description	17.1.0
2021-12	SA#94E	SP-211290	0040	1	F	Added the situation of AF relocation to uplink Packet Buffer	17.1.0
2021-12	SA#94E	SP-211290	0042	1	F	Local NEF selection	17.1.0
2022-03	SA#95E	SP-220055	0043	1	F	Corrections on enabling EAS IP Replacement procedure by AF	17.2.0
2022-03	SA#95E	SP-220055	0046	1	F	Correction related EHE in EC architecture	17.2.0
2022-03	SA#95E	SP-220055	0047	1	F	Update of EAS discovery procedure and BaselineDNSPattern management in EASDF	17.2.0
2022-03	SA#95E	SP-220055	0048	1	F	On NAT between PSA UPF and EASDF	17.2.0
2022-03	SA#95E	SP-220055	0050	1	F	Removing inconsistency in the definition of ECS Address Configuration Information	17.2.0
2022-03	SA#95E	SP-220055	0051	1	F	Corrections of EDC functionality description	17.2.0
2022-06	SA#96	SP-220398	0052	1	F	Correction related to EAS IP Address in EDI	17.3.0
2022-06	SA#96	SP-220398	0053	-	F	Corrections on enabling EAS IP Replacement procedure by AF	17.3.0
2022-06	SA#96	SP-220398	0054	1	F	Correction of EAS Deployment Information Management procedures and services	17.3.0
2022-06	SA#96	SP-220398	0056	1	F	Parameter supplement of EDI	17.3.0
2022-06	SA#96	SP-220398	0061	1	F	Alignment of ECS Address Configuration Information to SA6's definition	17.3.0
2022-09	SA#97E	SP-220777	0062	1	F	EDNS Client Subnet option correction	17.4.0
2022-12	SA#98E	SP-221069	0063	-	F	Clarifications for local event notification control	17.5.0
2022-12	SA#98E	SP-221086	0070	2	B	Support of influencing UPF and EAS (re)location for collections of UEs	**18.0.0**
2022-12	SA#98E	SP-221086	0075	2	B	KI#4 common EAS enforcement for set of UEs	18.0.0
2022-12	SA#98E	SP-221086	0079	3	B	Procedure for PDU Session supporting HR-SBO in VPLMN	18.0.0
2022-12	SA#98E	SP-221086	0082	3	B	Influencing UPF and EAS (re)location for collections of UEs	18.0.0
2023-03	SA#99	SP-230059	0073	7	B	EAS Re-discovery Procedure with EASDF in HR roaming scenario	18.1.0
2023-03	SA#99	SP-230059	0083	4	B	Edge Relocation within the same hosting PLMN's EHEs	18.1.0
2023-03	SA#99	SP-230059	0084	13	B	Home Routed-Session Breakout (HR-SBO) support	18.1.0
2023-03	SA#99	SP-230059	0087	4	B	KI#4: AF traffic influence for common EAS, DNAI selection	18.1.0
2023-03	SA#99	SP-230059	0088	4	B	The EAS discovery procedure with V-EASDF using IP replacement mechanism for supporting HR-SBO	18.1.0
2023-03	SA#99	SP-230059	0089	4	B	Handling AF traffic influence for HR-SBO PDU Sessions	18.1.0
2023-03	SA#99	SP-230059	0092	9	B	DNAI mapping based on conclusions in TR 23.700-48	18.1.0
2023-03	SA#99	SP-230059	0093	5	B	KI#4 23.548 common EAS enforcement for set of UEs	18.1.0
2023-03	SA#99	SP-230059	0094	1	B	KI#5 EDI extension for EAS discovery for GSMA OPG scenario	18.1.0
2023-03	SA#99	SP-230059	0095	1	B	Common DNAI relocation	18.1.0
2023-03	SA#99	SP-230059	0096	1	B	ECS Address Configuration Information delivery in roaming	18.1.0
2023-03	SA#99	SP-230059	0098	1	B	Information sharing between PLMN to support GSMA OPG	18.1.0
2023-03	SA#99	SP-230059	0101	1	B	Select common DNAI/EAS for a set of UEs	18.1.0
2023-03	SA#99	SP-230059	0105	1	B	EASDF functional description update	18.1.0
2023-03	SA#99	SP-230059	0109	1	B	UL CL/BP insertion for common EAS Discovery	18.1.0
2023-04	SA#99	-	-	-	-	MCC correction to implementation of CR0095R1	18.1.1
2023-06	SA#100	SP-230462	0112	4	B	Home Routed-Session Breakout (HR-SBO) - offload policy structure	18.2.0
2023-06	SA#100	SP-230462	0120	7	B	KI#1 EAS Discovery: Resolve ENs	18.2.0
2023-06	SA#100	SP-230462	0122	2	B	KI#1 EACI provisioning from VPLMN	18.2.0
2023-06	SA#100	SP-230462	0123	3	B	KI#1 EDI provision for HR-SBO	18.2.0

2023-06	SA#100	SP-230462	0124	1	B	KI#4 DNS cache refresh triggered by common EAS-DNAI requests	18.2.0
2023-06	SA#100	SP-230462	0125	1	C	Clarification on ECS Address Provisioning in roaming scenarios	18.2.0
2023-06	SA#100	SP-230462	0137	4	B	HR SBO and DNS security	18.2.0
2023-06	SA#100	SP-230462	0140	1	B	Clarification for geographic area in DNAI mapping	18.2.0
2023-06	SA#100	SP-230462	0142	5	C	Corrections on handling the AF traffic influencing request for HR-SBO PDU Sessions	18.2.0
2023-06	SA#100	SP-230462	0146	2	B	Common EAS/DNAI determination for a set of UEs	18.2.0
2023-06	SA#100	SP-230462	0149	3	F	Solving ENs on multiple SMF coordination	18.2.0
2023-06	SA#100	SP-230462	0150	-	F	Correction on UL CL/BP insertion	18.2.0
2023-06	SA#100	SP-230462	0152	1	B	Update to edge relocation for HR-SBO	18.2.0
2023-06	SA#100	SP-230462	0155	3	B	EAS Re-discovery in HR-SBO context	18.2.0
2023-09	SA#101	SP-230846	0160	3	F	how to route the DNS traffic between the UE and the V-EASDF where multiple DNN networks with the same IP address range are deployed	18.3.0
2023-09	SA#101	SP-230846	0161	2	F	Inter V-SMF mobility registration update procedure in HR-SBO case	18.3.0
2023-09	SA#101	SP-230846	0162	2	F	NEF determination of the HR-SBO condition when receiving an AF request targeting an individual UE address	18.3.0
2023-09	SA#101	SP-230846	0163	3	F	Clarification on common DNAI selection with local DNS server	18.3.0
2023-09	SA#101	SP-230846	0165	1	F	Enforcement of VPLMN specific offloading information for IP range(s)	18.3.0
2023-09	SA#101	SP-230846	0167	-	F	Service correction related to traffic correlation	18.3.0
2023-09	SA#101	SP-230846	0169	1	F	Clarification of SMF behaviour if no common EAS IP address present in PCC rule	18.3.0
2023-09	SA#101	SP-230846	0171	1	F	DNS server reselection based on common DNAI	18.3.0
2023-09	SA#101	SP-230846	0172	2	F	Clarification on procedure of Handling of Common EAS, CommonDNAI for set of UEs	18.3.0
2023-09	SA#101	SP-230846	0173	2	F	Updates on EAS change procedure	18.3.0
2023-09	SA#101	SP-230846	0174	2	F	Updates on common DNAI selection with Local DNS Server/Resolver	18.3.0
2023-09	SA#101	SP-230846	0175	2	F	Updates on coordination among SMFs for common EAS/DNAI determination	18.3.0
2023-09	SA#101	SP-230846	0176	2	F	Clarification and editorial regarding common EAS/DNAI	18.3.0
2023-09	SA#101	SP-230846	0178	2	F	Clarification on EAS discovery procedure	18.3.0
2023-09	SA#101	SP-230846	0179	2	F	Updates on EAS rediscovery procedure	18.3.0
2023-09	SA#101	SP-230846	0180	2	F	KI#4 DNS cache refresh triggered by UE quitting or joining UE set	18.3.0
2023-09	SA#101	SP-230846	0181	-	D	Editorial Fix in the Network triggered EAS change in HR-SBO context procedure	18.3.0
2023-12	SA#102	SP-231256	0186	5	F	Enhancement on offloading information enforcement	18.4.0
2023-12	SA#102	SP-231256	0199	2	F	Update on Network triggered EAS change procedure	18.4.0
2023-12	SA#102	SP-231256	0206	2	F	Remove EN on DNS traffic routing	18.4.0
2024-03	SA#103	SP-240098	0187	3	F	EASDF functional description update	18.5.0
2024-03	SA#103	SP-240098	0189	3	F	Clarifications on EAS address and DNAI mapping information stored in UDR	18.5.0
2024-03	SA#103	SP-240098	0190	3	F	Clarifications on Common DNAI/EAS discovery/selection procedure	18.5.0
2024-03	SA#103	SP-240098	0192	2	F	HR-SBO Authorization failure in HR-SBO	18.5.0
2024-03	SA#103	SP-240098	0193	2	F	Clarification on DL Session AMBR for Offloading in HR-SBO Sessions	18.5.0
2024-03	SA#103	SP-240098	0200	2	F	Update on general descriptions for EAS discovery	18.5.0
2024-03	SA#103	SP-240098	0202	2	F	KI#1 Corrections on Offload Identifier and misalignments in services	18.5.0
2024-03	SA#103	SP-240098	0205	6	F	KI#1 Applicability of VPLMN specific offloading information and Offload ID	18.5.0
2024-03	SA#103	SP-240098	0207	5	F	Clarifications on the case AF interacts with HPLMN to influence HR-SBO traffic at VPLMN	18.5.0
2024-03	SA#103	SP-240463	0212	5	F	Support for the case where the EAS IP address is not part of the IP address authorized by H-SMF	18.5.0
2024-03	SA#103	SP-240098	0213	1	F	KI#1 Corrections on AF traffic influence and related information transmission in HR-SBO case	18.5.0
2024-03	SA#103	SP-240098	0214	-	F	Corrections to Neasdf_DNSContext Service and EASDF-related Description	18.5.0
2024-03	SA#103	SP-240098	0216	2	F	KI#4 Clarifications on common EAS/DNAI procedure	18.5.0
2024-03	SA#103	SP-240098	0218	1	F	Corrections to Procedures in 6.7.2.6, 6.7.2.7	18.5.0
2024-06	SA#104	SP-240602	0191	6	F	Correction of Outer Header Creation and Outer Header Removal in edge relocation	18.6.0
2024-06	SA#104	SP-240960	0198	5	F	Clarification on AF request for simultaneous connectivity	18.6.0
2024-06	SA#104	SP-240594	0219	-	F	EAS Configuration Address Information provisioning in roaming	18.6.0
2024-06	SA#104	SP-240594	0221	3	F	Security for EAS discovery procedure via (V-)EASDF	18.6.0
2024-06	SA#104	SP-240594	0222	2	F	KI#1 Clarification on EAS discovery with local DNS server using IP replacement	18.6.0

2024-06	SA#104	SP-240594	0224	1	F	Clarification of VPLMN specific offloading policy	18.6.0
2024-06	SA#104	SP-240594	0226	1	F	Corrections to HR-SBO	18.6.0

History

Document history		
V18.5.0	May 2024	Publication
V18.6.0	July 2024	Publication