**3GPP TSG-WG SA2 Meeting #164 *S2-2408401r2***

**Maastricht, Netherlands, 2024-08-19 — 2024-08-23**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0248** | **rev** | **-** | **Current version:** | **18.6.0** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Addition of N6 delay measurement based EAS (re-)discovery enhancement | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson, Huawei?, HiSilicon?, China Mobile?, CATT?, Samsung?, Nokia? | | | | | | | | | |
| ***Source to TSG:*** | SA2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eEDGE\_5GC\_Ph3 | | | | |  | ***Date:*** | | | 2024-08-07 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-19 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)  Rel-20 (Release 20)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | TR 23.700-49 concluded for KI#2 that “SMF can select local PSA UPF considering N6 delay when available”, and “SMF can collect N6 delay measurement from candidate UPF per pair of 5GC N6 termination point (i.e. UPF) and the measurement endpoint at application side” and also that “SMF determines the measurement protocol based on the protocol supported by UPF and the measurement protocol(s) supported by application side (e.g. Pre-configuration in SMF or via AF request).”  TR 23.700-49 also specifies: “5GC may enable the N6 delay measurement via AF influence procedure per clause 4.3.6 in TS 23.502[3] or via EAS Deployment Information Management defined in clause 6.2.3.4 in TS 23.548 [5].” and “NOTE 1: For the enabling of SMF to measure N6 delay aspect, whether one mechanism between AF influence and EDI is enough will be determined in normative phase.”  The current CR proposes extensions to TS 23.548 that enable the SMF select local PSA UPF considering N6 delay, where AF is assumed to provide to the SMF the information for N6 latency measurements in the EAS Deployment Information (EDI). | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clause 6.2.3.4 “EAS Deployment Information Management” is extended with the information needed to support N6 delay measurements (note: the current CR does not provide any extensions related to extend AF influence mechanisms for the above purpose).  A new clause “N6 Delay Measurement Functionality” is added describing the new functionality and the impacted procedures.  Clause 6.2.3.2.2 is updated to show that SMF considers N6 daley information when creating/updating the DNS message handling rules. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The new feature proposed in the conclusion for KI#2 specified in TR23.700-49 will not be implemented. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.2.3.4.1, 6.2.3.2.2, 5.x (new clause) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\* \* \* \* First change \* \* \* \*

##### 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). N6 delay measurement may be performed for EAS discovery (see clause 6.2.3.2.x).

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).

\* \* \* \* Second change \* \* \* \*

##### 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] |
| N6 delay measurement information | Details about IP address(es), protocol information and security credentials of the measurement endpoint(s) in the Local part of the DN for each 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.

\*\*\* 2nd Change (all new)\*\*\*

## 6.x Use of N6 Delay Measurement

To enhance EAS and local UPF (re)selection by considering the fulfilment of end-to-end service delay requirements, the SMF may initiate N6 delay measurements per pair of 5GC N6 termination point (i.e. UPF/L-PSA) and the measurement endpoint at application side, as described in TS 23.502 [3], clause x.y.z. The N6 delay measurement information received from the UPF may be used by the SMF in the following way:

- The SMF may update the DNS message handling rule on EASDF, e.g., update the EDNS Client Subnet (ECS) option or Local DNS Server to be used for a given FQDN, as well as update the reporting action (Clause 6.2.3.2).

- The SMF may also update the DNS message handling rule on EASDF for a given DNS response, in response to the DNS message reporting received from the EASDF (Step 17 of Clause 6.2.3.2.2). In this case, the SMF may indicate which EAS IP address(es) are to be sent to the UE in the DNS response from the list of EASes received.

- For an already established connection to an EAS, the SMF may perform an edge relocation (Clause 6.3.6) and then it may also trigger an EAS re-discovery procedure (Clause 6.2.3.3) if the service requirements on the current connection are not met.

\*\*\* 3rd Change

##### 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

- N6 delay measurement from candidate L-PSA(s) and L-DN locations; 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, (if available) N6 delay measurements between the candidate UPF(s) and DNAI as described in clause 5.8.2.X of 23.501 [2], 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, EAS deployment and N6 delay measurement results, 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.

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]. The SMF may perform local PSA selection based on the N6 delay as determind via N6 delay measurement procedure defined in TS 23.502 [3], clause x.y.z. 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.