**3GPP TSG-WG SA2 Meeting #154 *S2-2211362***

**Toulouse, France, November 14 – 18, 2022 (revision of S2-2211245)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **23.548** | **CR** | **0075** | **rev** | **2** | **Current version:** | **17.4.0** |  |
|  | | | | | | | | |
| *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:*** | KI#4 common EAS enforcement for set of UEs | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** |  | | | | | | | | | |
| ***Source to TSG:*** | SA2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | EDGE\_Ph2 | | | | |  | ***Date:*** | | | 2022-11-04 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-18 |
|  | *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-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.2.3.2.X, 6.2.3.2.Y (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | | **X** |  | Other core specifications | | | | TS23.501 CR3788, TS23.502 CR3625, TS23.503 CR0776 | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | | This CR to be implemented before 23.548CR0070 (S2-221364) | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

##### 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.

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

- Control Action: Performs at least one of control actions on the DNS message(s) as follows:

- Buffer the DNS message(s).

- Send the buffered DNS Response(s) message to UE.

- Discard cached DNS Response message(s).

When the EASDF forwards a DNS message (to the UE or towards a DNS server over N6), 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;

NOTE 7: 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 8: 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 9: 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 10: 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 the candidate DNAI for that FQDN for the UE location, or in a case a common DNAI is used for the UE collection, the information is determined based on the common DNAI of the set of the 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 an 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 TS 23.503 [4] clause 6.4 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 11: 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 12: 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 13: 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, SUPI, 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, SUPI, 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 in Step 8, 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 and determine the associated N6 traffic routing information for the DNAI. 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. The SMF can use the FQDN in Neasdf\_DNSContext\_Notify Request in Step 8 to find the Application ID configured for the application in the EAS Deployment Information and use the Application ID to find the corresponding PCC rule. If the SMF finds a PCC rule for the application, the SMF shall use the information in the PCC rule instead of the EAS Deployment Information for any overlapping parameters, such as list of DNAI(s).

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.

\*\*\* Next change \*\*\*

#### 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].

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.

\* \* \* Next change \* \* \* \*

##### 6.2.3.2.X Common EAS discovery for a set of UEs

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



Figure 6.2.3.2.X-1: Common EAS discovery for a set of UEs

1. The AF request in step 1 of figure 4.3.6.2-1 in TS 23.502 [9] is used to request selecting the common EAS for 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 UEs for correlated selection of EAS.

An EAS Correlation indication can be provided for selecting the same EAS for set of UEs accessing the same application.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 EAS.

In step 5 of figure 4.3.6.2-1 in TS 23.502 [9], PCF determines the UEs influenced by the AF Request, and based on AF request, PCF creates PCC rule with Application ID and EAS Correlation indication to SMF.

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

In step 9:

The SMF can use the FQDN in Neasdf\_DNSContext\_Notify Request in Step 8 to find the Application ID configured for the application in the EAS Deployment Information and use the Application ID to find the corresponding PCC rule. If FQDN in Neasdf\_DNSContext\_Notify Request is for the application indicated in PCC rule, and if EAS Correlation indication is set, SMF determines the UE belongs to set of UEs identified by Application ID and the UE accesses the application and determines the UE needs to use the common EAS for the set of UEs.

If the common EAS is not available for the set of UEs:

steps 12~16 are used for discovering an EAS, SMF could take multiple UEs into consideration for EAS discovery.

If the common EAS is available for the set of UEs:Step 12~Step 16 are skipped.

In step 17:

SMF sends DNS message handling rule with IP address for the common EAS and instructs EASDF to return the Common EAS IP address in a DNS response to UE directly.

In step 19:

EASDF sends DNS response with the IP address of the common EAS instructed in step 17 to UE.

\* \* \* \* Next change \* \* \* \*

##### 6.2.3.2.Y EAS discovery corresponding to Common DNAI for a set of UEs

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.Y-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 [9] is used to request selecting the common DNAI for 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 UEs for correlated selection of DNAI.

An indication of traffic correlation can be provided for indicating selecting the same DNAI (i.e. selecting EAS corresponding to the same DNAI) for set of UEs accessing the same application.

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 5 of figure 4.3.6.2-1 in TS 23.502 [9], PCF determines the UEs influenced by the AF Request, and based on AF request, PCF creates PCC rule with Application ID and indication of traffic correlation to SMF.

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

In step 10:

The SMF can use the FQDN in Neasdf\_DNSContext\_Notify Request in Step 8 to find the Application ID configured for the application in the EAS Deployment Information and use the Application ID to find the corresponding PCC rule. If FQDN in Neasdf\_DNSContext\_Notify Request is for the application indicated in PCC rule, and if indication of traffic correlation is set, SMF determines the UE belongs to set of UEs identified by the Application ID and the UE is accessing the application and determines the UE needs to connect to EAS corresponding to the common DNAI for the set of UEs.

If the common DNAI is not available, SMF determines the common DNAI and SMF could take multiple UEs into consideration for the determination of common DNAI.

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.

Editor's Note: It is FFS if and how the common DNAI can be changed during Edge relocation procedure.

\* \* \* \* End of changes \* \* \* \*