**3GPP SA WG2 Meeting #162 S2-2404483**

**Changsha, China, April 15 – 19, 2024**

**Source: Ericsson**

**Title: KI#3: New solution**

**Document for: Approval**

**Agenda Item: 19.9**

**Work Item / Release: FS\_eEDGE\_5GC\_Ph3 / Rel-19**

*Abstract of the contribution: The contribution discusses and proposes updates to solution #12.*

# Proposal

It is proposed to add this solution to TS. 23.700-49

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* First changes (all new) \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 6.X Solution #X: Establishment of tunnel based on AF/EAS request

### 6.X.1 Key Issue mapping

This addresses the KI#3

### 6.X.2 Description

This solution is based on solution #21.

This solution does not impact EDI. Instead, the AF/EAS knows it has no connection to the central AS and by this the AF/EAS requests a connection e.g., from one DNAI to another DNAI, or to an address. The establishment of the connection between the UPFs connected to the DNAIs can use the principles in solution #21.

The solution does not care which about central or local. The important part is that 2 UPFs can connect to each other.

One of the major problems of any solution that needs to tunnel traffic between 2 separate IP network, is how to deal with the routing. In the IP network routers exchange information about how to reach a destination via routing protocols. Now if the 2 IP network are disjoint, no routing information will flow between these networks. And thus, one cannot use an IP address of another network if there is no connection between them. E.g., If EAS in IP network 1 need to send IP packets to AS in IP network 2 and IP network 1 and IP network 2 has not connection via routing, EAS cannot use the address of AS in its network. This means that EAS needs to use an address of IP network 1. Furthermore, any outgoing traffic from a UPF will in most deployments use NAT between UPF and the DN. See figure below for how an IP packet needs to travel in uplink. The arrow denoted X is the problematic one.

UE

IP Network 1

NAT

NAT

UPF

UPF

X

EAS

AS

IP Network 2

Figure 6.X.2-1: example of uplink packet flow

To solve the outline problem, the EAS/AF provides the 5GC with the set of tunnelling mechanisms it supports, e.g., GRE, IP in IP (both should be available in most OSes). Then SMF selects one and provides a tunnelling endpoint in UPF.

### 6.X.3 Procedures

UPF2

UPF1

SMF

NEF

AF/EAS

1. Get tunnel req. (DNAIs, supported tunneling mech).

2. Get tunnel req. (dito)

3. set-up tunnel

4. Get tunnel resp. (endpoint, tunnel mechanism)

5. Get tunnel resp. (dito)

+-

AS

Figure 6.x.3-1: Request tunnel over 5GC

1. AF/EAS requests 5GC to set up a tunnel between 2 DNAIs. One could also imagine that the EAS/AF only gives IP address ranges of EAS and AS, or even FQDNs of these. If not DNAIs are provided, NEF needs to translate the provided info to DNAIs. The AF/EAS provides which tunnelling protocol it supports, e.g.. IP in IP, GRE, etc. Also other relevant data related to the specific tunnel, such as e.g. which optional parameters in GRE to be used, and in case this Key in GRE is used, what value. If AF/EAS supports masque e.g. connect IP (IETF RFC 9484 [x], AF/EAS can also indicate this. This step can happen at any time e.g., at EAS boot up or restart, when a UE first access the EAS, or via a management procedure in an AF.

2. NEF finds a SMF supporting both DNAIs and sends a request to this SMF.

3. SMF follows steps 3-6 in solution #21. With the following differences:

- SMF selects one of the tunneling methods provided by the AF/EAS (if 5GC supports at least one of them, else SMF rejects the request)

- PDRs from Solution #21 needs to be updated, depending on technology used the PDEs may look different. The following table is an example:

PDRs and FARs for UPF1 and UPF2

|  |  |  |
| --- | --- | --- |
| UPF | Rule | Description |
| UPF2 (UL) | PDR-1 | Source Interface = access (N9) Packet Filter Set (optional): Incoming Tunnel ID / IP SA = L-EAS IP (range), GTP-U outer header removalFAR ID = FAR-1’s ID |
|  | FAR-1 | Rule IDAction = forwardDestination interface = N6 |
| UPF1 (UL) | PDR-2 | Source Interface = N6’ Tunnel outer header removalPacket Filter Set: Incoming Tunnel Info FAR ID = FAR-2’s ID |
|  | FAR-2 | Rule IDAction = forwardDestination interface = N9GTP-U outer header adding: GTP-u header that the SMF has received from the UPF2 |
| UPF1(DL) | PDR-3 | Source Interface = access N9 (optional)Packet Filter: incoming GTP-U tunnelGTP-U outer header removalTunnel Outer header adding FAR ID = FAR-3’s ID |
|  | FAR-3 | Rule IDAction = forwardDestination interface = N6’ |
| UPF2(DL) | PDR-4 | Source Interface = core (N6 (optional))Packet Filter Set: , IP DA = L-EAS IP (range)FAR ID = FAR-4’s ID |
|  | FAR-4 | Rule ID Action = forwardDestination interface = access (N9)GTP-U outer header adding: GTP-U header that the SMF has received from the UPF1 |

4. SMF responds with the selected tunneling mechanism and the tunnel endpoint address of UPF1 and also the tunnel specific information needed, e.g. if Key in GRE is to be used, the Key value. Or if masque is selected, the HTTP proxy address for masque control.

5. NEF forwards the received information from SMF to the AF/EAS

Editor's Note: it is FFS how to support 2 SMFs, e.g. as in a roaming case.

### 6.X.4 Impacts on services, entities and interfaces

SMF:

- Support a request to establish a tunnel

- select a termination tunnel mechanism

- establish the tunnels

UPF:

- Support termination of a tunnel e.g. GRE or IP in IP

NEF;

- Support request of tunnel

- optionally map IP address ranges to DNAIs

AF/EAS:

- Request an establishment of a tunnel

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

# 2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

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

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

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

[4] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS)".

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

[6] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[7] IETF RFC 792: "Internet Control Message Protocol".

[8] IETF RFC 4443: "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification".

[9] 3GPP TS 28.538: "Management and orchestration; Edge Computing Management".

[x] IETF RFC 9484: "Proxying IP in HTTP

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* 3rd changes (all new) \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |
| --- | --- |
| Solutions | Key Issues |
|  | 1 | 2 | 3 |
| #1: Edge computing handling by I-SMF | X |  |  |
| #2: Edge computing handling by local SMF | X |  |  |
| #3: Reducing impact of DNS message handling on central SMF for EAS (re)discovery based on offload to L-SMF | X |  |  |
| #4: Enhanced EC Architecture with SMF selecting local SMF storing EC related information | X |  |  |
| #5: Enhanced EC architecture with AMF selecting local SMF | X |  |  |
| #6: Local management of EAS Deployment Information with local SMF | X |  |  |
| #7: EAS deployment information report from L-UPF | X |  |  |
| #8: Selecting an EAS server leveraging analytics |  | X |  |
| #9: Solution of local UPF and EAS (re)selection jointly considering N6 delay and EAS load |  | X |  |
| #10: L-PSA and EAS (re)selection based on N6 one-way and two-way delay measurement |  | X |  |
| #11: Provision weight factor of DNAIs from AF |  | X |  |
| #12: NWDAF and SMF-based EAS and local UPF (re)selection |  | X |  |
| #13: EAS Discovery taking account of EAS load in EASDF |  | X |  |
| #14: EAS selection considering DNS historical handling records |  | X |  |
| #15: The local EASDF assist for the EAS and local UPF (re)selection based on the AF provided N6 delay and EAS load information |  | X |  |
| #16: Local UPF and EAS (re)selection considering access network delay and N6 delay information by 5GC or AF |  | X |  |
| #17: EC Traffic Routing between local part of DN and central part of DN with IP replacement in EAS |  |  | X |
| #18: Supporting traffic routing between local DN and central DN within a PDU Session |  |  | X |
| #19: Traffic Routing between local DN and central DN over session breakout model |  |  | X |
| #20: EC Traffic Routing between local part of DN and central part of DN via PDU session |  |  | X |
| #21: Solution to traffic routing between local and central part of DN via tunnel(s) |  |  | X |
| #22: Establishment of connectivity between the local DN and central part of DN based on OAM |  |  | X |
| #23: Traffic steering between different parts of a DN |  |  | X |
| #xx: Establishment of tunnel based on AF/EAS request |  |  | X |

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