**SA WG2 Meeting #153eS2-220abcd**

**October 10th -17th 2022 ; Elbonia (revision of S2-220)**

**Source: Intel, AT&T, Deutsche Telekom(?)**

**Title: KI#1: Conclusion**

**Document for: Approval**

**Agenda Item: 9.1**

**Work Item / Release:** **FS\_SFC / Rel-18**

*Abstract of the contribution:*

# 1 Discussion

The conclusion proposal in this pCR is provided using S2-2205919r14 from SA2#152e meeting as the baseline, resolving several Editor’s Note as follows.

1. Editor’s Notes: it is FFS whether metadata are supported.

The benefit of using Metadata is that it can simplify the configuration of Service Function Paths. Without the use of metadata, the operator would need to configure multiple service function paths corresponding to all possible combinations of SF chains that could be applied to traffic flow based on the request from 3rd party AF. This is illustrated in Figure 1.



Figure 1: Illustration of SFC without Metadata

With the use of metadata the operator needs to configure a reduced number of Service Function Paths, noting that the Metadata that is provided in the user plane (within the NSH header associated with every user plane packet) can be used a selector inside the SFC to determine which SF should be invoked or skipped for the packet, as illustrated in Figure 2.



Figure 2: Illustration of SFC with Metadata

Furthermore, even when the same SF is invoked for packets carrying distinct Metadata (e.g. SF2 in Figure 2 handles user plane packets tagged with both Metadata Mx and My), the Metadata can further control the operations that the SF applies with finer granularity. Consider for instance the case where SF2 = “Gating function based on Deep Packet Inspection (DPI)”, while Metadata Mx and My stand for “Service Provider X” and “Service Provider Y”. Consider that Service Provider X would like to block voice traffic, whereas Service Provider Y would like to block VPN traffic. While packets tagged with Mx and My Metadata are both processed by the same service function (SF2), the DPI logic applied by SF2 is completely different and is determined by the Metadata caried in the NSH packet header.

**Observation 1: The use of Metadata allows for simplified network configuration by reducing the number of configured SFPs in the node implementing SFC.**

We think that the explanation above clearly illustrates the usefulness of Metadata in terms of simplifying network configuration.

1. Editor’s Note: It is FFS whether SFC ID needs to be provided per traffic direction.

Given that the sentence above the EN i.e., 5GC may receive from the AF policies associating for one UE, a group of UE(s) or all UE(s) some traffic (filter) to be associated with a SFC ID already considers one SFC ID provided from the AF, we delete this EN.

1. Editor’s Note: It is FFS whether NEF or PCF performs the check whether the indicated SFC IDs correspond to the agreed SLA.

To avoid the SFC specific function impact in NEF, we support the option where the PCF performs the check whether the indicated SFC IDs correspond to the agreed SLA.

Editor’s Note: It is FFS whether to progress the option where the SFC functionality is implemented in a UPF that can be dynamically inserted on N6 (only when requested by an AF) i.e., the option that does not have the constraint of static configuration as described in the bullet above.

Figure 3 and Figure 4 illustrate the use of SFC without and with the option where the SFC functionality is implemented in a UPF that can be dynamically inserted on N6.



Figure 3: Without dynamic insertion

As shown in Figure 3 (and also documented for TR 23.700-18 solutions relying on existing traffic steering mechanisms) all UPFs in the operator network serving as PSA for the DNN/S-NSSAI/DNAI that is used for traffic that is potentially subject to SFC controls need to be configured with traffic steering information towards all SFPs supported for that DNN/S-NSSAI/DNAI. Given that SFC control can (and most of the time will) be invoked on Internet traffic i.e. on the PDU Session associated with DNN = “Internet”, in real deployments all of the PSAs will need to be configured with pre-established tunnels. It is noted that the number of pre-established tunnels in this approach is proportional to the number of supported SFPs (as also illustrated in Figure 3).



Figure 4: With dynamic insertion of UPF implementing SFC

In contrast, with the dynamic insertion of UPF implementing SFC, as illustrated in Figure 4, there is no need for pre-configured tunnels between the PSA and the SFC node. Only when there is a request from a third party AF for a specific traffic flow, the SMF dynamically creates a GTP-U tunnel between the PSA and the UPF implementing SFC functionality (dashed blue line in Figure 4) in order to steer that traffic flow towards the SFC.

It is noted that there is no impact on the already deployed PSAs, because the establishment of a GTP-U tunnel towards another UPF node is already supported in the specification today. In reference to Figure 4, to establish a dynamic GTP-U tunnel the SMF needs to provide a FAR including an F-TEID to both the PSA and the UPF implementing SFC (F-TEID=X and F-TEID=Y, respectively). The selected Service Function Path to be applied (indicated via SFP ID), as well as the Metadata to be applied on that SFP, is only conveyed in the FAR going to the UPF implementing SFC functionality.

**Observation 2: The dynamic insertion of UPF implementing SFC avoids the burden of preconfigured tunnels in the existing PSAs and has no specification impact on the PSA.**

On the other hand, the N4 interface connecting the SMF to the UPF implementing SFC functionalities needs to be enhanced to carry the SFP ID and the Metadata in the FAR.

**Observation 3: In order to benefit from the advantages described in the previous observations (namely, reduced number of SFPs and no pre-established tunnels in the PSA), the FAR needs to be enhanced to carry the SFP ID and the Metadata.**

The updates to the conclusion corresponding to this EN is provided below.

# 2 Proposal

**It is proposed to update TR** **23.700-18 as follows.**

*Start of change*

# 8 Conclusions

## 8.1 Key Issue #1: Traffic Steering Policy and SFC Enhancements

It is recommended to use the following principles and procedures as the basis for the normative work.

- Support the N6-LAN traffic steering control and AF-influenced traffic steering control to be applicable to the same traffic simultaneously.

- 5GC may receive from the AF policies associating for one UE, a group of UE(s) or all UE(s) some traffic (filter) to be associated with a SFC ID.

- The PCF determines a policy per SDF/application for the purpose of steering the subscriber's traffic to appropriated N6 service functions deployed by the operator or a 3rd party service provider. The policy is expressed in a Traffic Steering Policy (TSP) IDs or SFP IDs that may be different in UL and DL directions.

- PCF checks whether the indicated SFC IDs correspond to an authorized SFC policy for the AF.

- The PCF maps the SFC IDs into a TSP ID(s) (possibly one per direction) that refers to a traffic steering behaviour that is configured in the SMF/UPF or SFP IDs that can be different for uplink and downlink directions that apply to PDU Session. The SMF/UPF don’t need to be aware of SFC IDs.

- The PCF provides the TSP ID(s) or SFP IDs and optionally Metadata (as provided by the AF) in the PCC rules to SMF. The TSP ID refers to a traffic steering behaviour that is configured in the SMF/UPF.- If the PCC rule includes TSP IDs, the SMF provisions corresponding PDRs, FARs, QERs to support SFC creating a FAR with the Forwarding Policy parameters set to the TSP ID. The UPF serving as PSA uses TSP ID to steer traffic over N6. In this case, the TSP ID identifies a specific Service Function Path in the SFC. It is assumed that all UPFs in the operator network serving as PSA for the DNN/S-NSSAI/DNAI subject to SFC control need to be configured with the same traffic steering information for SFC processing.

- If the PCC rule includes SFP IDs, the SMF provisions corresponding PDRs, FARs to PSA and UPF implementing SFC functionality that is different from the PSA.

- The SMF configures the PSA via N4 message including PDR and FAR. The FAR includes F-TEID (existing parameters) to establish the GTP-U tunnel towards the UPF implementing the SFC functionality.

- The SMF configures the UPF implementing the SFC functionality via N4 message including PDR and FARs. The first FAR includes the SFP ID to steer traffic to and from the Service Function Chain and the second FAR includes F-TEID (existing parameters) to establish the GTP-U tunnel towards the PSA.

- The UPF with SFC capability uses the SFP ID and optionally Metadata received in the PCC rule is used by the traffic classifier in the SFC and also in the SFC encapsulation header as defined in RFC 8300 [ref].