**3GPP TSG SA WG2 Meeting #153E *S2-220xxxx***

**Elbonia, October 10 – 17, 2022**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **23.503** | **CR** | **x** | **rev** | **-** | **Current version:** | **17.6.0** |  |
|  |
| *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:***  | Basic description of Service Function Chaining |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | SA2 |
|  |  |
| ***Work item code:*** | SFC |  | ***Date:*** | 2022-08-30 |
|  |  |  |  |  |
| ***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 canbe 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:*** | Capture the conclusions from FS\_SFC study. |
|  |  |
| ***Summary of change:*** | Capture the basic descriotion of service function chaining |
|  |  |
| ***Consequences if not approved:*** | Incomplete specification |
|  |  |
| ***Clauses affected:*** | 4.3.7, 6.1.3.14 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** | **Y** |  |  Other core specifications  | TS 23.501 ... 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:*** |  |

*This CR captures KI#1 aspects. KI#2 aspects in separate CR*

\*\*\*\* First Change \*\*\*\*

### 4.3.7 Traffic steering control

Traffic Steering Control refers to the capability to activate/deactivate traffic steering policies from the PCF in the SMF for the purpose of:

- steering the subscriber's traffic to appropriate operator or 3rd party service functions (e.g. NAT, antimalware, parental control, DDoS protection) in the N6-LAN or 5G-LAN type of services, e.g. to support service function chaining. This is supported in non-roaming and home-routed scenarios only.

- AF influenced traffic diversion which enables the routing of the user traffic matching the traffic filters provided in the PCC rule to a local Data Network identified by the DNAI per AF request. This is supported in non-roaming and LBO scenarios only, as described in clause 5.6.7 of TS 23.501 [2].

\*\*\*\* Next Change \*\*\*\*

#### 6.1.3.14 Traffic steering control

Traffic steering control is triggered by the PCF initiated request and consists of steering the detected service data flows matching application detection filters or service data flow filter(s) in PCC Rules. The traffic steering control consists in one of the following:

- AF influenced Traffic Steering: diverting (at DNAI(s) provided in PCC rules) traffic matching traffic filters provided by the PCF, as described in clause 5.6.7 of TS 23.501 [2].

- N6-LAN Traffic Steering: applying a specific N6 traffic steering policy for the purpose of steering the subscriber's traffic to appropriated N6 service functions deployed by the operator or a 3rd party service provider, also referred to as service function chaining.

The PCF uses one or more pieces of information such as network operator's policies, user subscription, user's current RAT, network load status, application identifier, time of day, UE location, DNN, related to the subscriber session and the application traffic as input for selecting a traffic steering policy.

The PCF controls traffic steering by provisioning and modifying traffic steering control information in PCC rules. Traffic steering control information consists of a traffic description and in the case of N6-LAN Traffic Steering, a reference to a traffic steering policy that is configured in the SMF or, in the case of AF influenced Traffic Steering, per DNAI a reference to a traffic steering policy and/or N6 traffic routing information as well as other parameters described in clause 6.3.1 a reference to a traffic steering policy that is configured in the SMF.

The SMF instructs the UPF to perform necessary actions to enforce the traffic steering policy referenced by the PCF. This is further detailed in TS 23.501 [2], clause 5.6.X and clause 5.8.2.11. The actual traffic steering applies at the UPF. For enforcing the traffic steering policy, the UPF may support traffic steering related functions as defined by other standard organizations. The mechanism used for routing the traffic over N6 is out of 3GPP scope.

\*\*\*\* Next Change \*\*\*\*

#### 6.2.2.6 Traffic steering

The SMF shall support traffic steering control as defined in clause 6.1.3.14 and in the case of AF influenced Traffic Steering, also as defined in clause 5.6.7 of TS 23.501 [2.

The SMF may be configured with the traffic steering policy IDs related to the mechanism enabling traffic steering to the N6-LAN, DN and/or DNAIs associated with N6 traffic routing requirements.

Upon receiving a PCC rule which contains the traffic steering control information, the SMF shall provide the information to the UPF for the enforcement.

In the case of AF influenced Traffic Steering, the traffic steering control information in the PCC rule may include a set of DNAI(s) and for each DNAI a traffic steering policy identifier and/or N6 traffic routing information dynamically provided by the AF. Based on the received traffic steering policy identifier(s), the UPF may remove or insert VLAN tags on N6 interface for downlink and uplink frames, respectively. The details of the scenario is defined in clause 5.6.10.2 of TS 23.501 [2].

NOTE: The UPF can, for example, perform marking packets in order to indicate a certain type of traffic to the DN side of the N6 reference point which enables those packets to be steered in the DN. As another example the UPF can forward, i.e. offload, traffic identified by the traffic descriptor to a local tunnel.

\*\*\*\* End of Changes \*\*\*\*