**3GPP TSG-S4 Meeting #114e *S4-210822***

 **Electronic Meeting, 19th May – 28th May 2021**

|  |
| --- |
| *CR-Form-v12.1* |
| **Pseudo CHANGE REQUEST** |
|  |
|  | **26.804** | **CR** | **<CR#>** | **rev** | **<Rev#>** | **Current version:** | **0.2.1** |  |
|  |
| *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 |  |

|  |
| --- |
|  |
| ***Title:***  | Clarification of Traffic Identification description and addition of identified open issues |
|  |  |
| ***Source to WG:*** | Ericsson LM |
| ***Source to TSG:*** | S4 |
|  |  |
| ***Work item code:*** | FS\_5GMS\_EXT |  | ***Date:*** | 2021-05-12 |
|  |  |  |  |  |
| ***Category:*** | **<Cat>** |  | ***Release:*** | Rel-17 |
|  | *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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | Different terms are used to describe the general traffic identification procedures in different SA2 and CT3 specifications. The description for the Traffic Identification aspect was confusing, since different terminology was used. The “open issue” around traffic identification was still empty. |
|  |  |
| ***Summary of change:*** | A short summary of terminology is added and the text is adjusted using terms more consistently. Some subsections are re-ordered to put the different technologies into a better sequence.Finds with respect to missing parameters on different interfaces is added.  |
|  |  |
| ***Consequences if not approved:*** |  |
|  |  |
| ***Clauses affected:*** |  |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  |  |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  |  |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  |  |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

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

# 2 References

[X] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS); Stage 2".

[Y] 3GPP TS 29.514: "5G System; Policy Authorization Service; Stage 3".

[Z] 3GPP TS 29.522: "5G System; Network Exposure Function Northbound APIs; Stage 3".

[Z2] 3GPP TS 29.512: "5G System; Session Management Policy Control Service; Stage 3".

\*\*\*\* Second Change \*\*\*\*

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

CDN Content Delivery Network

FAR Forward Action Rule

MAR Multi-Access Rule

PDR Packet Detection Rule

PFCP Packet Forwarding Control Protocol

QER QoS Enforcement Rule

PFD Packet Flow Description

SDF Service Data Flow

URL Uniform Resource Locator

URR Usage Reporting Rule

\*\*\*\* Third Change \*\*\*\*

### 5.3.1 Description

For different features within the 5G Media Streaming Architecture, it is necessary for the 5G System to identify the traffic flows. The increased usage of transport encryption (e.g. HTTPS) increases the difficulty of detecting the packets for certain application flows. Existing detection methods, such as using “significant parts of the URL to be matched” (contained in a Packet Flow Description, see below), are impractical for HTTPS traffic, since the URL is carried in the encrypted payload.

Multimedia streaming applications might not be able to uniquely identify the 5-tuple of the streaming session, since the 5-tuples are often changing. This is due to factors such as load balancing, CDN distribution, multiple concurrent requests for different types of resources, etc. This study will address how to properly configure the 5G System to enable efficient detection of application flows (service data flows) e.g. for event reporting, and QoS profile usage, etc.

Note that the TS 23.50x specifications use different terminology from the TS 29.xxx specifications. Furthermore, TS 23.503 [X] uses slightly different terms than TS 23.501 [23] and TS 23.502 [24]. The two common terms are defined in TS 23.503:

**- Packet flow:** A specific user data flow from and/or to the UE.

**- Service data flow**: An aggregate set of packet flows carried through the UPF that matches a service data flow template.

The terms *traffic detection* [23] and *application detection* [23] refer to the process of finding matching service data flows among all packet flows. This logic is defined in TS 23.503 as an *application detection filter*.

The procedures in TS 23.502 use the term *flow description*, which is only a subset of an *IP Packet Filter Set* (as defined in TS 23.501).

Figure 5.3.1-1 depicts the chain of functions (taken from TS 29.244 [26], Figure 5.2.1-1) within a UPF.

The steps are as follows:

1. The UPF always first looks up the Packet Forwarding Control Protocol (PFCP) session context to which a packet belongs. The PFCP session context is an individual PDU session or a standalone PFCP session not tied to any PDU session.

2. Then there are so-called Packet Detection Rules (PDR), which implement traffic detection of the service data flows with respect to different conditions.

NOTE: A PDR is direction specific. Thus, an Uplink (UL) PDR and a Downlink (DL) PDR are needed to detect a bidirectional Service Data Flow.

3. Based on the PDR result, the next rules are executed, namely Multi-Access Rule (MAR), Forward Action Rule (FAR), QoS Enforcement Rule (QER), and Usage Reporting Rule (URR).

NOTE: Only the Forward Action Rule (FAR) is mandatory. The QoS Enforcement Rule (QER) is only present for QoS Flows. The Usage Reporting Rule (URR) is only available when traffic volume measurements (e.g. for charging) are needed.

The Packet Detection Rule (PDR) is based on Service Data Flow Templates, which contain one or more Service Data Flow (SDF) Filters or an Application Identifier. An Application Identifier refers to one or more Packet Flow Descriptions (PFDs).

A Service Data Flow (SDF) Filter contains for IP PDU Sessions a single IP Packet filter, i.e. any combination of

- Source/destination IP address or IPv6 prefix.

- Source / destination port number.

- Protocol ID of the protocol above IP/Next header type.

- Type of Service (TOS) (IPv4) or Traffic class (IPv6) and Mask.

- Flow Label (IPv6).

- Security parameter index.

- Packet Filter direction.

compris

The application detection filter can be configured in the SMF and the SMF then provides it in the Service Data Flow Template to the UPF. Alternatively, the Service Data Flow Template for traffic handling in the UPF is received from the dynamic PCC Rule.

Besides, the Management of Packet Flow Descriptions enables the UPF to perform accurate application detection when PFD(s) are provided by an Application Service Provider (ASP) and then to apply enforcement actions as instructed in a PCC Rule.

The operator is able to configure pre-defined PCC Rules in the SMF or dynamic PCC Rules in the PCF. A PCC rule includes either a list of Service Data Flow filters or an application identifier for Service Data Flow detection. The PCC rule further includes charging control information, i.e. charging key and optionally a Sponsor identifier or an ASP identifier or both.

The application identifier references one or more PFDs, which are managed using the PFD Management API. Depending on the service level agreements between the operator and the Application Server Provider, it may be possible for the ASP to provide to the SMF individual PFDs or the full set of PFDs for each application identifier maintained by the ASP via the PFD Management service in the NEF (PFDF). The PFDs become part of the application detection filters in the SMF/UPF and are thereafter used as part of the logic to detect traffic generated by an application. The ASP may remove or modify some or all of the PFDs which have been provided previously for one or more application identifiers. The SMF may report the application stop to the PCF for an application instance identifier as defined in clause 5.8.2.8.4 of TS 23.501 [5] if the removed/modified PFD in SMF/UPF would result in an inability to detect traffic for that application instance.

The ASP manages (i.e. provisions, updates, deletes) the PFDs through the NEF (PFDF). The PFD(s) are transferred to the SMF through the NEF (PFDF). The PFDF is a logical functionality in the NEF which receives PFD(s) from the ASP through the NEF, stores the PFD(s) in the UDR and provides the PFD(s) to the SMF(s) either on the request from ASP PFD management through NEF (PFDF) (push mode) or on the request from SMF (pull mode). Finally, the PFDF functionality is a service provided by the NEF.

The ASP may provide/update/remove PFDs with an allowed delay to the NEF (PFDF). Upon reception of the request from the ASP, the NEF (PFDF) checks if the ASP is authorized to provide/update/remove those PFD(s) and request the allowed delay. The NEF (PFDF) may be configured with a minimum allowed delay based on SLA to authorize the allowed delay provided by the ASP. When both the requesting ASP and the requested allowed delay are successfully authorized, the NEF (PFDF) translates each external Application Identifier to the corresponding Application Identifier known in the core network. The NEF (PFDF) stores the PDF(s) into the UDR.

The Application Identifier is simply an index to a set of application detection rules configured in the UPF. It is an identifier that can be mapped to a specific application traffic detection rule.

The procedure is depicted Figure 5.3.1‑2 below:



Figure 5.3.1‑2:

The PFD (Packet Flow Description) is a set of information enabling the detection of application traffic.

Each PFD may be identified by a PFD ID. A PFD ID is unique in the scope of a particular Application Identifier. Conditions for when a PFD ID is included in the PFD are described in TS 29.551 [6]. There may be different PFD types associated with an Application Identifier.

### 5.3.2 Collaboration Scenarios

The 5GMSd Application Provider negotiates with the MNO an SLA to provide differentiated treatment, including network QoS and charging for its 5GMSd-Aware Application. The Application Provider provides the necessary information to the MNO to detect the traffic, to ensure its correct and exclusive identification. The MNO detects the traffic correctly and applies the agreed traffic treatment.

Due to privacy concerns, the content hosting is provided by the Application Provider in an external Data Network. However, the 5GMSd Application Provider leverages the network features either via a 5GMSd AF in the trusted Data Network (Figure 5.9.2‑1) or via a 5GMSd AF in the external Data Network (Figure 5.9.2‑2).



Figure 5.9.2-1: Collaboration 1 (Collaboration 3 of TS 26.501)



Figure 5.9.2-2: Collaboration 2 (Collaboration 4 of TS 26.501)

In order to use flow-based network features (such as different QoS classes or different charging policies), the 5G System needs to detect the relevant traffic.

### 5.3.3 Deployment Architectures

The following figure depicts a potential architecture design for the realization of traffic detection. The architecture shows the involved network functions in the traffic detection.



Figure 5.3.3-1: Relevant architecture components

### 5.3.4 Mapping to 5G Media Streaming and High-Level Call Flows

#### 5.3.4.1 General

The Service Data Flow Templates support multiple different combinations to define parameters for traffic detection. This clause describes the common parameter combinations to detect specifically media streaming application traffic.

The Service Data Flow Template can either be Service Data Flow Filters (i.e. IP Packet Filter Sets) or an application Id, referencing PFDs.

An IP Packet Filter Set can contain different combinations of parameter values. Unspecified parameter values in the IP Packet Filter Sets are used to match any value of the corresponding information in a packet. Common IP Packet Filter Set combinations are

* 5-Tuple: The Source/destination IP addresses, Source / destination port numbers (incl. small range) and the Protocol ID parameter values are specified.
* ToS: The Source IP address and the Type of Service (TOS) parameter values are specified.

Editor’s Note: Additional parameter value combinations such as 3-Tuple or usage of Flow Label (IPV6 only) can be beneficial

A Packet Flow Description (PFD) can contain different parameters. Common parameters are

* A Domain Name: The domain name parameter is present.

#### 2

Tapplicationbased on a pre-configured PCC rule (i.e. ) or a dynamic PCC rule (i.e. provided by the PCF)By interacting with the PCF (possibly via the NEF) ttraffic

theSet

identifier

 (uplink or downlink)

2the



2

the

the UE IP address, an IP Packet Filter Set with and the UE

#### 5.3.4.4 Usage of Packet Flow Descriptions for Traffic Identification

The following are potential and simplified call flows for the realization of the traffic identification.

In the first call flow (Figure 5.3.4.4‑1) the provisioning step is described, in which one or more PFDs for a single application are provisioned. The provisioned PFDs for a single application are identified by the Application Identifier.



Figure 5.3.4.4-1: PFD Provisioning using the PFD Management API (simplified)

In the second call flow (Figure 5.3.4.4‑2) the update procedure for the PFD to adjust to an actual session is described.



Figure 5.3.4.4-2: PFD usage within an application detection filter (simplified)

### 5.3.5 Potential open issues

The exact behaviour and information that needs to be provided to and by the 5GMSd AF as well as the MSH need to be specified.

The following open issues have been identified:

1. The Npcf\_PolicyAuthorization API as defined in TS 23.502 [24] only supports usage of a flow description or an application identifier. The flow description is not further defined in TS 23.501 or TS 23.502. In Stage 3 specifications, a flow description represents only a 5-tuple. Other information elements of the Service Data Flow Filter are not supported.

2. The Nnef\_ChargeableParty and Nnef\_AFsessionWithQOS APIs only support usage of a flow description. The flow description is not further defined in TS 23.501 or TS 23.502. Other information elements of the Service Data Flow Filter are not supported.

3. The Npcf\_PolicyAuthorization API Stage 3 as defined in TS 29.514 [Y], only supports a flow description and a ToS value. However, it is not possible to define whether the ToS value should be used in uplink traffic detection or downlink traffic detection.

4. The Nnef\_AFsessionWithQOS and Nnef\_ChargeableParty stage 3 APIs, as defined in TS 29.522 [Z], only supports a Packet Flow Description (through the FlowInfo Type). Other information elements of the Service Data Flow Filter are not supported. Note, the FlowInfo Type from TS 29.122 [?] is different from the FlowInformation Type in TS 29.512 [Z2]

### 5.3.6 Candidate Solutions

Editor’s Note: Provide candidate solutions (including call flows) for each of the identified issues.

\*\*\*\* Last Change \*\*\*\*