**3GPP TSG-SA4 Meeting 113-e *S4-210537***

**Electronic Meeting, 6th - 14th April 2021**

|  |
| --- |
| *CR-Form-v12.0* |
| **Pseudo CHANGE REQUEST** |
|  |
|  | **26.804** | **CR** | **<CR#>** | **rev** | **3** | **Current version:** | **0.1.1** |  |
|  |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Key Topic Traffic Identification |
|  |  |
| ***Source to WG:*** | Qualcomm Incorporated, Ericsson LM |
| ***Source to TSG:*** | SA4 |
|  |  |
| ***Work item code:*** | FS\_5GMS-EXT |  | ***Date:*** | 2021-02-23 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | The study item description identifes the key topic “Traffic Identification”. |
|  |  |
| ***Summary of change:*** | Adds the structure and description for this key topic |
|  |  |
| ***Consequences if not approved:*** | Key topic not addressed |
|  |  |
| ***Clauses affected:*** |  |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
| ***56***  |  |
| ***This CR's revision history:*** |  |

**===== CHANGE =====**

# 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 26.501: " 5G Media Streaming (5GMS); General description and architecture".

[3] 3GPP TS 26.511: "5G Media Streaming (5GMS); Profiles, codecs and formats".

[4] 3GPP TS 26.512: "5G Media Streaming (5GMS); Protocols".

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

[6] 3GPP TS 29.551: “5G System; Packet Flow Description Management Service; Stage 3"

**===== CHANGE =====**

# 4 Introduction to 5G Media Streaming

## 4.1 Introduction

## 4.2 Collaboration Scenarios

## 4.3 Architectures

## 4.4 Summary of Stage-3 enablers

**===== CHANGE =====**

# 5 Key Topics

## 5.1 Introduction

## 5.3 Traffic Identification

### 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. 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.

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 the PCC Rule.

The operator is able to configure pre-defined PCC Rules in the SMF or dynamic PCC Rules in the PCF that include at least an application identifier for service data flow detection, charging control information, i.e. charging key and optionally the Sponsor identifier or the A SP identifier or both. Depending on the service level agreements between the operator and the Application Server Provider, it may be possible for the ASP to provide individual PFDs or the full set of PFDs for each application identifier maintained by the ASP to the SMF via the PFD Management service in the NEF (PFDF). The PFDs become part of the application detection filters in the SMF/UPF and therefore are 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 a 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 results in that the stop of the application instance is not being able to be detected.

The ASP manages (provision, update, delete) 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). 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 by the following diagram:



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.

A PFD includes the following information:

- PFD ID; and one or more of the following:

- 3-tuple(s) including protocol, server-side IP address and port number;

- the significant parts of the URL to be matched, e.g. host name;

- a domain name matching criterion and information about applicable protocol(s).

### 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 identify the traffic, to ensure its correct and exclusive identification. The MNO identifies 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. The 5G System uses so-called **Packet Detection Rules** (PDRs) in the UPF to detect the traffic. The PDRs are created based on **Service Data Flow Templates**. The Service Data Flow Templates are provided by the 5GMSd AF.

### 5.3.3 Deployment Architectures

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



Figure 5.3.3-1: Relevant architecture components

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

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

In the first call flow (Figure 5.3.4‑1) 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 5.3.4-1: PFD Provisioning using the PFD Management API (simplified)

In the second call flow (Figure 5.3.4‑2) the update procedure for the PFD to adjust to an actual session is described.



Figure 5.3.4-2: PFD usage within an application traffic detection rule (simplified)

### 5.3.5 Potential open issues

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

### 5.3.6 Candidate Solutions

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