|  |  |
| --- | --- |
| 3GPP TS 26.510 V1.1.0 (2024-02) | |
| Technical Specification | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Media delivery;  interactions and APIs for provisioning and media session handling;  (Release 18) | |
|  | |
|  |  |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  <https://www.3gpp.org> |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 14

Introduction 15

1 Scope 16

2 References 16

3 Definitions of terms, symbols and abbreviations 18

3.1 Terms 18

3.2 Symbols 18

3.3 Abbreviations 18

4 Functions and roles 19

4.1 Media Application Provider 19

4.2 Media AF 19

4.3 Media Session Handler 19

5 Interactions 19

5.1 Summary 19

5.2 Provisioning (M1) interactions 21

5.2.1 Overview 21

5.2.2 Provisioning Session provisioning 22

5.2.2.1 General 22

5.2.2.1A Enumerate Provisioning Sessions collection operation 22

5.2.2.2 Create Provisioning Session resource operation 23

5.2.2.3 Retrieve Provisioning Session resource operation 23

5.2.2.4 Update Provisioning Session resource operation 23

5.2.2.5 Destroy Provisioning Session resource operation 23

5.2.3 Content protocols discovery 23

5.2.3.1 General 23

5.2.3.2 Create Content Protocols resource operation 24

5.2.3.3 Retrieve Content Protocols resource operation 24

5.2.3.4 Update Content Protocols resource operation 24

5.2.3.5 Destroy Content Protocols resource operation 24

5.2.4 Server Certificate provisioning 24

5.2.4.1 General 24

5.2.4.2 Create Server Certificate resource operation 24

5.2.4.3 Reserve Server Certificate resource operation 25

5.2.4.4 Upload Server Certificate resource operation 26

5.2.4.5 Retrieve Server Certificate resource operation 26

5.2.4.6 Update Server Certificate resource operation 26

5.2.4.7 Destroy Server Certificate resource operation 27

5.2.5 Content Preparation provisioning 27

5.2.5.1 General 27

5.2.5.2 Create Content Preparation Template resource operation 27

5.2.5.3 Retrieve Content Preparation Template resource operation 28

5.2.5.4 Update Content Preparation Template resource operation 28

5.2.5.5 Destroy Content Preparation Template resource operation 28

5.2.6 Edge Resources provisioning 28

5.2.6.1 General 28

5.2.6.2 Create Edge Resources Configuration resource operation 29

5.3.6.3 Retrieve Edge Resources Configuration resource operation 29

5.2.6.4 Update Edge Resources Configuration resource operation 29

5.2.6.5 Destroy Edge Resources Configuration resource operation 30

5.2.7 Dynamic Policy provisioning 30

5.2.7.1 General 30

5.2.7.2 Policy Template life-cycle 31

5.2.7.3 Create Policy Template resource operation 32

5.2.7.4 Retrieve Policy Template resource operation 32

5.2.7.5 Update Policy Template resource operation 32

5.2.7.6 Destroy Policy Template resource operation 33

5.2.8 Content Hosting provisioning 33

5.2.8.1 General 33

5.2.8.2 Create Content Hosting Configuration resource operation 33

5.2.8.3 Retrieve Content Hosting Configuration resource operation 34

5.2.8.4 Update Content Hosting Configuration resource operation 34

5.2.8.5 Destroy Content Hosting Configuration resource operation 35

5.2.8.6 Purge Content Hosting cache operation 35

5.2.9 Content Publishing provisioning 36

5.2.9.1 General 36

5.2.9.2 Create Content Publishing Configuration resource operation 36

5.2.9.3 Retrieve Content Publishing Configuration resource operation 37

5.2.9.4 Update Content Publishing Configuration resource operation 37

5.2.9.5 Destroy Content Publishing Configuration resource operation 37

5.2.9.6 Purge Content Publishing cache operation 38

5.2.10 Metrics Reporting provisioning 38

5.2.10.1 General 38

5.2.10.2 Create Metrics Reporting Configuration resource operation 38

5.2.10.3 Retrieve Metrics Reporting Configuration resource operation 39

5.2.10.4 Update Metrics Reporting Configuration resource operation 39

5.2.10.5 Destroy Metrics Reporting Configuration resource operation 39

5.2.11 Consumption Reporting provisioning 40

5.2.11.1 General 40

5.2.11.2 Create Consumption Reporting Configuration resource operation 40

5.2.11.3 Retrieve Consumption Reporting Configuration resource operation 40

5.2.11.4 Update Consumption Reporting Configuration resource operation 40

5.2.11.5 Destroy Consumption Reporting Configuration resource operation 41

5.2.12 Event Data Processing provisioning 41

5.2.12.1 General 41

5.2.12.2 Create Event Data Processing Configuration resource operation 41

5.2.12.3 Retrieve Event Data Processing Configuration resource operation 42

5.2.12.4 Update Event Data Processing Configuration resource operation 42

5.2.12.5 Destroy Event Data Processing Configuration resource operation 42

5.3 Network media session handling (M3, M5) interactions 43

5.3.1 Overview 43

5.3.2 Service Access Information acquisition 43

5.3.2.1 General 43

5.3.2.2 Create Service Access Information resource operation 43

5.3.2.3 Retrieve Service Access Information resource operation 44

5.3.2.4 Update Service Access Information resource operation 44

5.3.2.5 Destroy Service Access Information resource operation 44

5.3.3 Dynamic Policy invocation 44

5.3.3.1 Procedures 44

5.3.3.2 Create Dynamic Policy Instance resource operation 45

5.3.3.3 Retrieve Dynamic Policy Instance resource operation 46

5.3.3.4 Update Dynamic Policy Instance resource operation 46

5.3.3.5 Destroy Dynamic Policy Instance resource operation 46

5.3.4 Network Assistance invocation 47

5.3.4.1 Procedures 47

5.3.4.2 Create Network Assistance Session resource operation 47

5.3.4.3 Retrieve Network Assistance Session resource operation 49

5.3.4.4 Bit rate recommendation request operation 49

5.3.4.5 Delivery boost request operation 49

5.3.4.6 Update Network Assistance Session resource operation 49

5.3.4.7 Destroy Network Assistance Session resource operation 50

5.3.5 Metrics reporting 50

5.3.5.1 Procedures 50

5.3.5.2 Submit metrics report operation 51

5.3.6 Consumption reporting 52

5.3.6.1 Procedures 52

5.3.6.2 Submit consumption report operation 53

5.4 UE media session handling (M6, M11) interactions 53

5.4.1 Overview 53

5.4.2 Media session handling initiation/termination 54

5.4.2.1 Explicit media session handling initiation/termination 54

5.4.2.2 Implicit media session handling initiation/termination 54

5.4.3 Dynamic Policy invocation 55

5.4.4 Network Assistance invocation 55

5.4.5 Metrics reporting 55

5.4.6 Consumption reporting 56

5.5 5GC policy control (N5/N33) interactions 56

5.5.1 Overview 56

5.5.2 Policy control interactions for Dynamic Policies 56

5.5.3 Policy control interactions for AF-based Network Assistance 57

5.6 UE modem interactions 58

5.6.1 Overview 58

5.6.2 ANBR-based Network Assistance 58

5.6.3 RAN-based metrics reporting 59

6 3GPP Service URL 59

7 General aspects of network APIs 60

7.1 Usage of HTTP 60

7.1.1 HTTP protocol version 60

7.1.2 HTTP endpoint addresses 60

7.1.2.1 Default Media AF endpoint address at reference point M1 60

7.1.2.2 Default Media AF endpoint address at reference point M3 60

7.1.2.3 Default Media AF endpoint address at reference point M5 60

7.1.3 HTTP resource URIs and paths 60

7.1.4 Usage of HTTP headers 61

7.1.4.1 General 61

7.1.4.2 User Agent identification 61

7.1.4.3 Server identification 61

7.1.4.2 Cache control 61

7.1.4.3 Support for conditional HTTP GET requests 61

7.1.4.4 Support for conditional HTTP POST, PUT, PATCH and DELETE requests 61

7.1.5 HTTP message bodies for API resources 61

7.1.6 HTTP response codes 61

7.1.7 HTTP error response message bodies 61

7.2 Explanation of API data model notation 62

7.3 Common OpenAPI data types 63

7.3.1 General 63

7.3.2 Simple data types 63

7.3.3 Structured data types 64

7.3.3.1 IpPacketFilterSet type 64

7.3.3.2 ServiceDataFlowDescription type 64

7.3.3.3A M1UnidirectionalQoSSpecification type 64

7.3.3.3 M1QoSSpecification type 64

7.3.3.3A M5BitRateSpecification type 65

7.3.3.4 M5QoSSpecification type 65

7.3.3.5 ChargingSpecification type 65

7.3.3.6 TypedLocation type 65

7.3.3.7 OperationSuccessResponse type 65

7.3.3.8 EdgeProcessingEligibilityCriteria type 66

7.3.3.9 EndpointAddress type 66

7.3.3.10 UnidirectionalQoSSpecification data type 67

7.3.3.11 M1MediaEntryPoint type 67

7.3.4 Enumerated data types 67

7.3.4.1 CellIdentifierType enumeration 67

7.3.4.2 SdfMethod enumeration 68

7.3.4.3 ProvisioningSessionType enumeration 68

7.3.4.4 EASRelocationTolerance enumeration 68

7.3.4.5 ContentTransferMode enumeration 68

8 Maf\_Provisioning service 69

8.1 Overview 69

8.2 Provisioning Sessions API 71

8.2.1 Overview 71

8.2.2 Resource structure 71

8.2.3 Data model 72

8.2.3.1 ProvisioningSession resource 72

8.3 Content Protocols Discovery API 74

8.3.1 Overview 74

8.3.2 Resource structure 74

8.3.3 Data model 75

8.3.3.1 ContentProtocols resource 75

8.3.3.2 ContentProtocolDescriptor type 75

8.4 Server Certificates provisioning API 76

8.4.1 Overview 76

8.4.2 Resource structure 76

8.4.3 Data model 77

8.4.3.1 Certificate Signing Request 77

8.4.3.2 Server Certificate resource 77

8.5 Content Preparation Templates provisioning API 78

8.5.1 Overview 78

8.5.2 Resource structure 78

8.5.3 Data model 78

8.6 Edge Resources provisioning API 79

8.6.1 General 79

8.6.2 Resource structure 79

8.6.3 Data model 80

8.6.3.1 EdgeResourcesConfiguration resource type 80

8.6.3.2 EdgeManagementMode enumeration 80

8.6.3.3 EASRequirements type 81

8.6.3.4 M1EASRelocationRequirements type 81

8.7 Policy Templates provisioning API 82

8.7.1 Overview 82

8.7.2 Resource structure 82

8.7.3 Data model 83

8.7.3.1 PolicyTemplate resource 83

8.8 Content Hosting provisioning API 85

8.8.1 Overview 85

8.8.2 Resource structure 85

8.8.3 Data model 86

8.8.3.1 ContentHostingConfiguration resource 86

8.8.3.2 DistributionNetworkType enumeration 89

8.8.3.3 DistributionMode enumeration 89

8.9 Content Publishing provisioning API 90

8.9.1 Overview 90

8.9.2 Resource structure 90

8.9.3 Data model 91

8.9.3.1 ContentPublishingConfiguration resource 91

8.10 Metrics Reporting provisioning API 94

8.10.1 Overview 94

8.10.2 Resource structure 94

8.10.3 Data model 94

8.10.3.1 MetricsReportingConfiguration resource 94

8.11 Consumption Reporting provisioning API 96

8.11.1 Overview 96

8.11.2 Resource structure 96

8.11.3 Data model 97

8.11.3.1 ConsumptionReportingConfiguration resource 97

8.12 Event Data Processing provisioning API 98

8.12.1 General 98

8.12.2 Resource structure 98

8.12.3 Data model 99

8.12.3.1 EventDataProcessingConfiguration resource type 99

9 Maf\_SessionHandling service 100

9.1 Overview 100

9.2 Service Access Information API 101

9.2.1 General 101

9.2.2 Resource structure 101

9.2.3 Data model 102

9.2.3.1 ServiceAccessInformation resource type 102

9.2.3.2 EASDiscoveryTemplate type 106

9.2.3.3 M5EASRelocationRequirements type 106

9.3 Dynamic Policy API 107

9.3.1 Overview 107

9.3.2 Resource structure 107

9.3.3 Data model 108

9.3.3.1 DynamicPolicy resource 108

9.4 Network Assistance API 109

9.4.1 Overview 109

9.4.2 Resource structure 109

9.4.3 Data model 110

9.4.3.1 NetworkAssistanceSession resource 110

9.5 Metrics Reporting API 111

9.5.1 General 111

9.5.2 Reporting procedure 111

9.5.3 Report format 111

9.6 Consumption Reporting API 112

9.6.1 General 112

9.6.2 Reporting procedure 112

9.6.3 Report format 113

9.6.3.1 ConsumptionReport type 113

9.6.3.2 ConsumptionReportingUnit type 114

10 UE media session handling APIs 115

10.1 General 115

10.2 Session launch mechanisms 115

10.3 Media session handling APIs for downlink media streaming 115

10.3.1 General 115

10.3.2 Media Session Handler model 115

10.3.2.1 State model 115

10.3.2.2 Media Session Handler internal properties 116

10.3.2.3 Media Session Handler internal operations 116

10.3.2.4 Starting and Stopping a Media Session Handler 116

10.3.3 General 117

10.3.4 Dynamic Policy information 117

10.3.5 Network Assistance information 117

10.3.6 Consumption Reporting information 118

10.3.7 Metrics Reporting information 119

10.4 Media session handling APIs for uplink media streaming 120

10.5 Media session handling APIs for webRTC 120

Annex A (normative): OpenAPI representation of HTTP REST APIs 121

A.1 General 121

A.2 Data Types applicable to several APIs 121

A.3 OpenAPI representation of Maf\_Provisioning APIs 121

A.3.1 Maf\_Provisioning\_ProvisioningSessions API 121

A.3.2 Maf\_Provisioning\_ContentProtocols API 121

A.3.3 Maf\_Provisioning\_ServerCertificates API 121

A.3.4 Maf\_Provisioning\_ContentPreparationTemplates API 121

A.3.5 Maf\_Provisioning\_EdgeResources API 121

A.3.6 Maf\_Provisioning\_PolicyTemplates API 122

A.3.7 Maf\_Provisioning\_ContentHosting API 122

A.3.8 Maf\_Provisioning\_ContentPublishing API 122

A.3.9 Maf\_Provisioning\_MetricsReporting API 122

A.3.10 Maf\_Provisioning\_ConsumptionReporting API 122

A.3.11 Maf\_Provisioning\_EventDataProcessing API 122

A.4 OpenAPI representation of Maf\_SessionHandling APIs 122

A.4.1 Maf\_SessionHandling\_ServiceAccessInformation API 122

A.4.2 Maf\_SessionHandling\_DynamicPolicy API 122

A.4.3 Maf\_SessionHandling\_NetworkAssistance API 122

A.4.4 Maf\_SessionHandling\_MetricsReporting API 123

A.4.5 Maf\_SessionHandling\_ConsumptionReporting API 123

Annex B (normative): Controlled vocabularies 124

B.1 Media Delivery locator type 124

Annex C (informative): Usage of TOS/DSCP for traffic identification 125

C.1 General 125

C.2 Differentiated Services/TOS-enabled Collaboration Scenarios 125

C.3 Procedure for using TOS Traffic Class for traffic identification 126

Annex <D> (informative): Change history 129

# Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# Introduction

This clause is optional. If it exists, it shall be the second unnumbered clause.

# 1 Scope

This clause shall start on a new page.

The present document …

# 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".

[23501] 3GPP TS 23.501: "System architecture for the 5G System (5GS) ".

[23502] 3GPP TS 23.502: "Procedures for the 5G System (5GS); Stage 2".

[26501] 3GPP TS 26.501: "5G Media Streaming (5GMS); General description and architecture".

[26506] 3GPP TS 26.506: "5G Real-time Media Communication Architecture (Stage 2)".

[26512] 3GPP TS 26.512: "5G Media Streaming (5GMS); Protocols".

[26113] 3GPP TS 23.113: "Real-Time Media Communication; Protocols and APIs".

[26247] 3GPP TS 26.247: "Transparent end-to-end Packet-switched Streaming Service (PSS); Progressive Download and Dynamic Adaptive Streaming over HTTP (3GP-DASH)".

[29122] 3GPP TS 29.122: "T8 reference point for Northbound APIs".

[X.509] ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005: "Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks".

[RFC5280] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", May 2008.

[RFC7468] IETF RFC 7468: "Textual Encodings of PKIX, PKCS, and CMS Structures", April 2015.

[23558] 3GPP TS 23.558: "Architecture for enabling edge applications".

[24558] 3GPP TS 24.558: "Enabling Edge Applications; Protocol specification".

[29558] 3GPP TS 29.558: "Enabling Edge Applications; Application Programming Interface (API) specification; Stage 3".

[23503] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS); Stage 2".

[23003] 3GPP TS 23.003: "Numbering, addressing and identification".

[29514] 3GPP TS 29.514: "5G System; Policy Authorization Service; Stage 3".

[29522] 3GPP TS 29.522: "5G System. Network Exposure Function Northbound APIs; Stage 3".

[27007] 3GPP TS 27.007: "AT Command set for User Equipment (UE)".

[38321] 3GPP TS 38.321: "NR; Medium Access Control (MAC) protocol specification".

[36321] 3GPP TS 36.321: "Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification".

[HTTPsemantics] IETF RFC 9110: "HTTP Semantics", June 2022.

[HTTPcaching] IETF RFC 9111: "HTTP Caching", June 2022.

[HTTP11] IETF RFC 9112: "HTTP/1.1", June 2022.

[HTTP2] IETF RFC 9113: "HTTP/2", June 2022.

[HTTP3] Reserved for future use.

[TLS13] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3", August 2018.

[29500] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[29501] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition; Stage 3".

[OpenAPI300] OpenAPI: "OpenAPI 3.0.0 Specification", <https://github.com/OAI/OpenAPI-Specification/blob/master/versions/3.0.0.md>.

[29571] 3GPP TS 29.571: "Common Data Types for Service Based Interfaces; Stage 3".

[RFC3339] IETF RFC 3339: "Date and Time on the Internet: Timestamps", July 2002.

[RFC3986] IETF RFC 3986: "URI Generic Syntax".

[ECMA262] Standard ECMA-262, 5.1 Edition: "ECMAScript Language Specification", June 2011.

[JSON] IETF RFC 8259: "The JavaScript Object Notation (JSON) Data Interchange Format", December 2017.

[JSONSchema] IETF draft-bhutton-json-schema-validation: "JSON Schema Validation: A Vocabulary for Structural Validation of JSON", June 2022.

[26118] 3GPP TS 26.118: "Virtual Reality (VR) profiles for streaming applications".

[29517] 3GPP TS 29.517: "5G System; Application Function Event Exposure Service; Stage 3".

[26532] 3GPP TS 26.532: "Data Collection and Reporting; Protocols and Formats".

[26346] 3GPP TS 26.346: "Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs".

[26347] 3GPP TS 26.347: "Multimedia Broadcast/Multicast Service (MBMS); Application Programming Interface and URL".

[ISO3166-1] ISO 3166‑1: "Codes for the representation of names of countries and their subdivisions — Part 1: Country codes".

[ISO3166-2] ISO 3166‑2: "Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision code".

[RFC2474] IETF RFC 2474: "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".

[RFC2475] IETF RFC 2475: "An Architecture for Differentiated Services".

[RFC3246] IETF RFC 3246: "An Expedited Forwarding PHB (Per-Hop Behavior)".

[RFC2597] IETF RFC 2597: "Assured Forwarding PHB Group".

# 3 Definitions of terms, symbols and abbreviations

This clause and its three (sub) clauses are mandatory. The contents shall be shown as "void" if the TS/TR does not define any terms, symbols, or abbreviations.

## 3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1], TS 26.501 [26501], TS 26.506 [26506] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1], TS 26.501 [26501] or TS 26.506 [26506].

**Media EAS:** Media Application Server deployed as an Edge Application Server.

**Media Delivery System:** A deployment of a 5GMS System or RTC System.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

5GC 5G Core

AF Application Function

ANBR Access Network Bit rate Recommendation

API Application Programming Interface

AS Application Server

DN Data Network

DS Differentiated Services

DSCP DS Code Point

EAS Edge Application Server

EEC Edge Enabler Client

EES Edge Enabler Server

FQDN Fully Qualified Domain Name

GPSI Generic Public Subscription Identifier

JSON JavaScript Object Notation

MFBR Maximum Flow Bit Rate

NEF Network Exposure Function

OAM Operations, Administration and Maintenance

PCC Policy Control and Charging

PCF Policy Control Function

PDR Packet Detection Rule

PHB Per-Hop Behaviour

QoE Quality of Experience

QoS Quality of Service

QFI QoS Flow Identifier

TCP Transmission Control Protocol

TOS Type of Service

UE User Equipment

URI Uniform Resource Identifier

URL Uniform Resource Locator

# 4 Functions and roles

## 4.1 Media Application Provider

Editor's Note: Role of the Media Application Provider in provisioning media features.

## 4.2 Media AF

Editor's Note: Role of the Media AF.

## 4.3 Media Session Handler

Editor's Note: Role of the Media Session Handler from TS 26.512 clause 12.2.1.

# 5 Interactions

## 5.1 Summary

Table 5.1‑1 summarises the APIs used to provision and use the various Media Delivery features specified in TS 26.501 [26501] and TS 26.506 [26506].

Table 5.1‑1: Summary of APIs relevant to downlink media streaming features

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Media delivery feature | Abstract | Reference point | Interactions clause | Relevant APIs | |
| API name | API clause |
| Content protocols discovery | Used by the Media Application Provider to interrogate which content ingest protocols are supported by the Media Delivery System. | M1 | 5.2.2 | Content Protocols Discovery API | 8.2 |
| Content hosting | Content is ingested, hosted and distributed by the Media AS according to a Content Hosting Configuration associated with a Provisioning Session.  The Media AS may be instantiated in an Edge Data Network.  Ingested content may additionally be distributed via eMBMS and/or MBS. | M1 | 5.2.3 | Provisioning Sessions API | 8.3 |
| 5.2.4 | Server Certificates provisioning API | 8.4 |
| 5.2.5 | Content Preparation Templates provisioning API | 8.5 |
| 5.2.6 | Edge Resources provisioning API | 8.6 |
| 5.2.7 | Policy Templates provisioning API | 8.7 |
| 5.2.8 | Content Hosting provisioning API | 8.8 |
| M5 | 5.4.2 | Service Access Information API | 9.2 |
| Content publishing | Content is contributed to and egested from the Media AS according to a Content Hosting Publishing associated with a Provisioning Session.  The Media AS may be instantiated in an Edge Data Network. | M1 | 5.2.3 | Provisioning Sessions API | 8.3 |
| 5.2.4 | Server Certificates provisioning API | 8.4 |
| 5.2.5 | Content Preparation Templates provisioning API | 8.5 |
| 5.2.6 | Edge Resources provisioning API | 8.6 |
| 5.2.7 | Policy Templates provisioning API | 8.7 |
| 5.2.9 | Content Publishing provisioning API | 8.9 |
| M5 | 5.4.2 | Service Access Information API | 9.2 |
| Dynamic Policy instantiation | The Media Client activates different traffic treatment and charging policies, including Background Data Transfer, selected from a set of Policy Templates provisioned in its Provisioning Session. | M1 | 5.2.3 | Provisioning Sessions API | 8.3 |
| 5.2.7 | Policy Templates provisioning API | 8.7 |
| M5 | 5.4.2 | Service Access Information API | 9.2 |
| 5.4.3 | Dynamic Policies API | 9.3 |
| Network Assistance | The Media Client requests bit rate recommendations and delivery boosts from the Media AF. | M5 | 5.4.2 | Service Access Information API | 9.2 |
| 5.4.4 | Network Assistance API | 9.4 |
| Metrics reporting | The Media Client submits metrics reports to the Media AF according to a provisioned Metrics Reporting Configuration it obtains from the Service Access Information for its Provisioning Session. | M1 | 5.2.3 | Provisioning Sessions API | 8.3 |
| 5.2.10 | Metrics Reporting provisioning API | 8.10 |
| M5 | 5.4.2 | Service Access Information API | 9.2 |
| 5.4.5 | Metrics Reporting API | 9.5 |
| Consumption reporting | The Media Client submits consumption reports to the Media AF about content consumed from downlink media delivery sessions according to a provisioned Consumption Reporting Configuration it obtains from the Service Access Information for its Provisioning Session. | M1 | 5.2.3 | Provisioning Sessions API | 8.3 |
| 5.2.11 | Consumption Reporting provisioning API | 8.11 |
| M5 | 5.4.2 | Service Access Information API | 9.2 |
| 5.4.6 | Consumption Reporting API | 9.6 |
| UE data collection, reporting and exposure | UE data related to media delivery is reported to the Data Collection AF instantiated in the Media AF for exposure to Event consumers. | M1 | 5.2.12 | Event Data Processing provisioning API | 8.12 |

## 5.2 Provisioning (M1) interactions

### 5.2.1 Overview

A Media Application Provider may use the operations in this clause to provision the different features offered by the Media Delivery System in the Media AF. The Provisioning API exposed by the Media AF to the Media Application Provider at reference point M1 offers the following sets of operations:

1. Provisioning of *Provisioning Sessions* (see clause 5.2.2) to act as an umbrella for the following provisioning information. Each such Provisioning Session is uniquely identified by a system-dependent Provisioning Session identifier as well as by system-independent service identifier that is subsequently used by a Media-Aware Application to launch media session handling (see clause 10.2) via a 3GPP Service URL (see clause 6).

2. Discovery of the set of content ingest and/or egest protocols supported by the Media AS for a particular Provisioning Session (see clause 5.2.3):

- For downlink media delivery, discovery of the content ingest protocols available at reference point M2 and the content distribution protocols available at reference point M4.

- For uplink media delivery, discovery of the content contribution protocols available at reference point M4 and the content egest protocols available at reference point M2.

3. Provisioning of *Server Certificates* within the scope of a Provisioning Session (see clause 5.2.4) to be used by the Media AS to assert its identity to the Media Access Function in Media Clients during media delivery sessions at reference point M4.

4. Provisioning of *Content Preparation Templates* within the scope of a Provisioning Session (see clause 5.2.5) that can be used by the Media AS to manipulate media content ingested at reference point M2 or contributed at reference point M4.

5. Provisioning of *Edge Resources* within the scope of a Provisioning Session (see clause 5.2.6) to be used to instantiate the Media AS as a set of Edge Application Servers (EAS) in an Edge Data Network (EDN) using the APIs specified in TS 29.558 [29558].

5. Provisioning of *Policy Templates* within the scope of a Provisioning Session (see clause 5.2.7) that can be applied to M4 downlink/uplink media delivery sessions in order to realise different Service Operation Points as part of the Dynamic Policies feature (see clause 5.4.3).

7. Provisioning of media delivery by the Media AS within the scope of a Provisioning Session using the abovementioned building blocks:

- For downlink media streaming according to TS 26.512 [26512], provisioning of the *Content Hosting* feature of the Media AS (see clause 5.2.8), which offers functionality equivalent to that of a public Content Delivery Network (CDN): content ingest at reference point M2 for onward distribution by the Media AS to Media Clients via reference point M4 or via other distribution systems such as eMBMS or MBS.

After discovering the set of ingest and distribution content protocols supported by the Media AS (see clause 5.2.2), the Media Application Provider may provision a Server Certificate (see clause 5.2.4), Content Preparation Template (see clause 5.2.5) and/or Edge Resources Configuration (see clause 5.2.6) for each Content Hosting distribution configuration to reference. The Media Application Provider may also provision one or more Policy Templates (see clause 5.2.7) to realise Service Operation Points pertaining to downlink media delivery.

- For uplink media streaming according to TS 26.512 [26512], provisioning of the *Content Publishing* feature of the Media AS (see clause 5.2.9), including content contribution by Media Clients at reference point M4 and subsequent content egest of content at reference point M2 after optional manipulation by a Content Preparation Template.

After discovering the set of contribution and egest content protocols supported by the Media AS (see clause 5.2.2), the Media Application Provider may provision a Server Certificate (see clause 5.2.4), Content Preparation Template (see clause 5.2.5) and/or Edge Resources Configuration (see clause 5.2.6) for each Content Publishing contribution configuration to reference. The Media Application Provider may also provision one or more Policy Templates (see clause 5.2.7) to realise Service Operation Points relevant to the parent Provisioning Session.

Editor's Note: Add some words for RTC, referencing TS 26.114.

8. Provisioning of *QoE metrics reporting* within the scope of a Provisioning Session (see clause 5.2.10) to configure how and how often the Media Client should report Quality of Experience metrics to the Media AF during the course of media delivery sessions at reference point M4.

9. Provisioning of *consumption reporting* within the scope of a Provisioning Session (see clause 5.2.11) to configure how often the Media Client should report downlink media consumption to the Media AF during the course of media delivery sessions at reference point M4.

10. Provisioning of rules for processing of UE data (as defined in TS 26.531 [26531]) related to media delivery sessions by the Data Collection AF instantiated in the Media AF (as defined in clause 4.7 of TS 26.501 [26501]), and for restricting its exposure over reference points R5 and R6 by means of Event Data Processing Configurations and Data Access Profiles for a particular Event ID.

NOTE: The *Network Assistance* feature is not provisioned by the Media Application Provider at reference point M1. Instead, it is provisioned at the discretion of the Media Delivery System operator using means beyond the scope of the present document.

### 5.2.2 Provisioning Session provisioning

#### 5.2.2.1 General

Prior to configuring media delivery features specified in subsequent clauses of the present document, the Media Application Provider shall create a new Provisioning Session resource in the Media AF at reference point M1. The Media Application Provider shall nominate a globally unique *external service identifier* that will be used by the Media Session Handler to launch media delivery sessions and this identifier shall be associated with exactly one Provisioning Session in each Media Delivery System.

The operations specified in the following clauses are used to manage a Provisioning Session resource, as specified in clause 8.2.3.1.

HTTP responses for successful and operation-specific failure cases are specified in the following clauses. For all other failure cases, an HTTP response indicating a response code in accordance with clause 7.1.6 shall be returned to the API client. In all failure cases a message body in accordance with clause 7.1.7 shall be included in the response message.

#### 5.2.2.1A Enumerate Provisioning Sessions collection operation

This procedure is used by the Media Application Provider to enumerate the current set of Provisioning Sessions in the Media AF. The HTTP GET method shall be used for this purpose. The request URL shall be that of the Provisioning Sessions collection.

If the operation is successful, the Media AF shall return an HTTP 200 (OK) response. The resource body shall be a JSON array of Provisioning Session resource identifiers. The array shall contain only resource identifiers for Provisioning Sessions that the Media Application Provider is entitled to manipulate, according to the credentials supplied with the request. This may, for example, be the subset of Provisioning Sessions tagged with the Application Server Provider identifier of the Media Application Provider. The array shall be empty if no Provisioning Sessions visible to the invoker currently exist in the collection.

#### 5.2.2.2 Create Provisioning Session resource operation

This operation is used by the Media Application Provider to create a new Provisioning Session. The Media Application Provider shall use the HTTP POST method to create a new Provisioning Session.

Upon successful creation, the Media AF shall return a 201 (Created) response message that includes the resource identifier of the newly created Provisioning Session resource (the *Provisioning Session identifier*) in the body of the HTTP response message and the URL of the resource, including its resource identifier, shall be provided as the value of the Location HTTP header field. The response message body shall be a representation of the current state of the Provisioning Session resource (see clause 8.2.3.1), including any property values set by the Media AF.

If the request is acceptable but the Media AF is unable to create the Provisioning Session resource, the create operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Provisioning Session resource shall remain in an uncreated state in the Media AF.

This operation may be performed multiple times by a Media Application Provider to create different Provisioning Session resources. Each such resource is assigned a different Provisioning Session identifier by the Media AF.

#### 5.2.2.3 Retrieve Provisioning Session resource operation

This operation is used by the Media Application Provider to retrieve the current state of an existing Provisioning Session from the Media AF. The HTTP GET method shall be used for this purpose, citing the resource identifier of the target Provisioning Session in the request URL.

If the target Provisioning Session exists, the Media AF shall return an HTTP 200 (OK) response with a representation of the Provisioning Session resource in the response message body.

#### 5.2.2.4 Update Provisioning Session resource operation

The Update operation is not permitted for the Provisioning Sessions resource. Any attempt to do so using the HTTP PUT or PATCH methods shall result in the HTTP response 405 (Method Not Allowed) that includes an error message body per clause 7.1.7.

To achieve an equivalent outcome, the Media Application Provider should instead destroy the existing Provisioning Session resource using the operation specified in clause 5.2.2.5 and create a new one using the operation specified in clause 5.2.2.2.

#### 5.2.2.5 Destroy Provisioning Session resource operation

This operation is used by the Media Application Provider to destroy an existing Provisioning Session. The Media AF shall use the HTTP DELETE method for this purpose, citing the resource identifier of the target Provisioning Session in the request URL.

If the target Provisioning Session resource exists, the Media AF shall return a 204 (No Content) HTTP response message with an empty message body. The Media AF shall release any associated resources in the Media AF and Media AS, purge any cached data, and destroy any sub-resources associated with the target Provisioning Session.

Any subsequent operations citing the resource identifier of a destroyed Provisioning Session should result in a 410 (Gone) or else a 404 (Not Found) HTTP response message that includes an error message body per clause 7.1.7.

### 5.2.3 Content protocols discovery

#### 5.2.3.1 General

The set of downlink content ingest and/or uplink content egest protocols supported by the Media AS at reference point M2 is described by the Content Protocols resource exposed by the Media AF at reference point M1, as specified in clause 8.3.3.1. This resource shall exist in the Media AF as a sub-resource of each created Provisioning Session and may therefore be different for each one, for example to offer different content protocols depending on properties of the parent Provisioning Session or 5GMS Application Provider.

HTTP responses for successful and operation-specific failure cases are specified in the following clauses. For all other failure cases, an HTTP response indicating a response code in accordance with clause 7.1.6 shall be returned to the API client. In all failure cases a message body in accordance with clause 7.1.7 shall be included in the response message.

#### 5.2.3.2 Create Content Protocols resource operation

The Create operation is not permitted for the Content Protocols resource. Any usage of the HTTP POST method in relation to its well-known resource URL shall result in the HTTP response 405 (Method Not Allowed) that includes an error message body per clause 7.1.7.

#### 5.2.3.3 Retrieve Content Protocols resource operation

This operation is used by the Media Application Provider to retrieve from the Media AF a list of downlink content ingest protocols and/or uplink content egest protocols supported by the Media AS at reference point M2. The HTTP GET method shall be used for this purpose, citing the well-known URL of the Content Protocols resource.

If the operation is successful, the Media AF shall return a 200 (OK) response that includes a Content Protocols resource in the response message body, as specified in clause 8.3.3.1.

#### 5.2.3.4 Update Content Protocols resource operation

The Update operation is not permitted for the Content Protocols resource. Any usage of the HTTP PUT or PATCH methods in relation to its well-known resource URL shall result in the HTTP response 405 (Method Not Allowed) that includes an error message body per clause 7.1.7.

#### 5.2.3.5 Destroy Content Protocols resource operation

The Destroy operation is not permitted for the Content Protocols resource. Any usage of the HTTP DELETE method in relation to its well-known resource URL shall result in the HTTP response 405 (Method Not Allowed) that includes an error message body per clause 7.1.7.

### 5.2.4 Server Certificate provisioning

#### 5.2.4.1 General

Each X.509 server certificate [X.509] presented by the Media AS to the Media Client at reference point M4 is represented by a Server Certificate resource at reference point M1. The Server Certificates Provisioning API specified in clause 8.4 enables a Server Certificate resource to be created within the scope of a Provisioning Session, and subsequently referenced by a Content Hosting Configuration or Content Publishing Configuration created in the scope of the same Provisioning Session. That API supports two alternative provisioning methods for Server Certificate resources: one in which a certificate is generated by the Media Delivery System operator on behalf of the Media Application Provider; the other in which a certificate is generated by the Media Application Provider from a Certificate Signing Request solicited from the Media AF. Both methods shall be supported by implementations of the Media AF.

Under no circumstances shall the Media AF reveal the private key associated with a Certificate Signing Request to the Media Application Provider.

HTTP responses for successful and operation-specific failure cases are specified in the following clauses. For all other failure cases, an HTTP response indicating a response code in accordance with clause 7.1.6 shall be returned to the API client. In all failure cases a message body in accordance with clause 7.1.7 shall be included in the response message.

#### 5.2.4.2 Create Server Certificate resource operation

This operation is used by the Media Application Provider to request that the Media Delivery System generates a new X.509 certificate [X.509] on its behalf within the scope of a Provisioning Session. In this case, the certificate’s Common Name (CN) and a single Subject Alternative Name (subjectAltName, see section 4.2.1.6 of RFC 5280 [RFC5280]) is assigned in a domain under the control of the Media Delivery System operator and the use of supplementary domain name aliases is not supported. The first Subject Alternative Name (subjectAltName) extension field of the certificate should be identical to its Common Name. Both fields may include a single wildcard ("\*") character at the start to indicate applicability to several different subdomains of the same domain.

NOTE 1: Modern TLS client implementations ignore the obsolete Common Name (CN) field of the X.509 certificate in favour of the first Subject Alternative Name (subjectAltName) extension field.

The Media Application Provider shall use the HTTP POST method to create a new Server Certificate resource in the Media AF. The request URL shall be a well-known sub-resource of the Provisioning Session resource representing its Server Certificates resource collection, as specified in clause 8.4.2. The HTTP request message body shall be omitted.

Upon successful creation, the Media AF shall return a 201 (Created) HTTP response message and the URL of the newly created Server Certificate resource, including its resource identifier, shall be provided in the HTTP Location header field. The response message body may optionally convey a copy of the X.509 certificate corresponding to the newly created Server Certificate resource, as specified in clause 8.4.3.2.

NOTE 2: The X.509 certificate corresponding to the newly created Server Certificate resource may not be available immediately for interrogation and use. See clause 5.2.4.5 below for more details.

If the request is acceptable but the Media AF is unable to provision the X.509 certificate, the create operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Server Certificate resource shall remain in an uncreated state in the Media AF.

This operation may be performed multiple times by a Media Application Provider to provision different Server Certificate resources within the scope of a Provisioning Session. Each such resource is assigned a different Server Certificate resource identifier by the Media AF.

#### 5.2.4.3 Reserve Server Certificate resource operation

This operation is used by the Media Application Provider to solicit a Certificate Signing Request (CSR) from the Media AF for the purpose of generating an X.509 certificate [X.509] independently of the Media Delivery System. In this case, the certificate's Common Name (CN) is assigned in a domain under the control of the Media Application Provider itself, or that of a third party acting on its behalf. The first Subject Alternative Name (subjectAltName) extension field of the certificate should be identical to its Common Name. The CN and subjectAltName fields may include a single wildcard ("\*") character at the start to indicate applicability to several different subdomains of the same domain.

NOTE: Modern TLS client implementations ignore the obsolete Common Name (CN) field of the X.509 certificate in favour of the first Subject Alternative Name (subjectAltName) extension field.

The Media Application Provider may specify additional domains in its certificate reservation request to the Media AF. If provided, these domain name aliases shall be included in the returned Certificate Signing Request using the Subject Alternative Name (subjectAltName) extension (see section 4.2.1.6 of RFC 5280 [RFC5280]). In this case, the Media Application Provider is responsible for ensuring that any FQDN aliases it subsequently provisions in Content Hosting Configurations or Content Publishing Configurations matching these additional domains resolve to the canonical domain name of the Media AS in the target Media Application System.

The Media Application Provider shall separately arrange for the FQDN carried in the Common Name of the certificate generated, or those of all Subject Alternative Name (subjectAltName) extensions in the same certificate (see section 4.2.1.6 of RFC 5280 [RFC5280]), to resolve to the address of a Media AS in the target Media Delivery System after provisioning the Content Hosting feature per clause 5.2.8.2 or the Content Publishing feature per clause 5.2.9.2.

The Media Application Provider shall use the HTTP POST method to create a new Server Certificate. The request URL shall be a well-known sub-resource of the Provisioning Session resource representing its Server Certificates resource collection, as specified in clause 8.4.2, including the query parameter specified there. Domain name aliases (if any) shall be conveyed in the HTTP request message body, encoded as a JSON array of strings; otherwise the request message body shall be omitted. Upon successful creation of the resource, the Media AF shall return a 201 (Created) response message and the URL of the resource, including the resource identifier of the reserved Server Certificate resource, shall be returned in the HTTP Location header. The HTTP response message shall provide a Certificate Signing Request as specified in clause 8.4.3.1.

If the list of additional domains in the HTTP request message is malformed, the Media AF shall return a 400 (Bad Request) response message.

If the request is acceptable but the Media AF is unable to generate a Certificate Signing Request, the creation operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Server Certificate resource shall remain in an uncreated state in the Media AF.

This operation may be performed multiple times by a Media Application Provider to provision different Server Certificate resources within the scope of a Provisioning Session. Each such resource is assigned a different Server Certificate resource identifier by the Media AF.

#### 5.2.4.4 Upload Server Certificate resource operation

This operation is used by a Media Application Provider to upload an X.509 certificate [X.509] to the Media AF that it has generated in response to a Certificate Signing Request solicited using the reservation operation specified in clause 5.2.4.3 above. The Media Application Provider shall use the HTTP PUT method for this purpose. The Content‑Type request header and the body of the HTTP request message shall be as specified in clause 8.4.3.2.

The Media AF shall verify that the party originating the upload is the same party that reserved the Server Certificate resource using the operations specified in clause 5.2.4.3 above before accepting the supplied X.509 certificate. The Media AF shall also verify that the X.509 certificate uploaded corresponds to the Certificate Signing Request it issued for the Server Certificate resource in question. If there is a mismatch, the HTTP response 403 (Forbidden) shall be returned.

Attempting to upload an X.509 certificate to a Server Certificate resource URL that has not been reserved using the operation specified in clause 5.2.4.3 above shall elicit a 404 (Not Found) HTTP response.

On success, the HTTP response 204 (No Content) shall be returned with an empty response body.

#### 5.2.4.5 Retrieve Server Certificate resource operation

This operation is used by the Media Application Provider to download a Server Certificate resource from the Media AF for inspection. The HTTP GET method shall be used for this purpose, citing the resource identifier of the target Server Certificate in the request URL.

If the requested resource exists and is populated with an X.509 certificate [X.509], the Media AF shall return 200 (OK) HTTP response message with a representation of the target Server Certificate in the response message body in accordance with clause 8.4.3.2.

In the case where the X.509 certificate was provisioned by the Media Delivery System on behalf of the Media Application Provider according to clause 5.2.4.2 above, the HTTP response 204 (No Content) shall be returned until such time as the X.509 certificate is generated and available for download. The optional HTTP response header Retry-After should be included in such a response, indicating when the certificate is expected to become available for inspection and use.

In cases where the X.509 certificate is to be generated by the Media Application Provider from a Certificate Signing Request obtained according to clause 5.2.4.3 above, the HTTP response 204 (No Content) shall be returned with an empty message response body until such time as the X.509 certificate has been uploaded using the operation specified in clause 5.2.4.4 above.

#### 5.2.4.6 Update Server Certificate resource operation

The Update operation is not permitted for the Server Certificate resource. Any attempt to do so using the HTTP PUT method shall result in the HTTP response 405 (Method Not Allowed) that includes an error message body per clause 7.1.7.

Updating a previously uploaded Server Certificate in the Media AF is not permitted for security reasons. To supply a replacement X.509 certificate, for example when a previously supplied certificate is shortly due to expire, the Media Application Provider should instead use one of the operations specified in clause 5.2.4.2 or 5.2.4.3 above to create or reserve a new Server Certificate resource and, once the certificate is available for use, update the Content Hosting Configuration to reference it.

#### 5.2.4.7 Destroy Server Certificate resource operation

This operation is used by the Media Application Provider to remove a Server Certificate resource from a Provisioning Session in the Media AF. The HTTP DELETE method shall be used for this purpose, citing the resource identifier of the target Server Certificate in the request URL.

On success, the HTTP response 204 (No Content) shall be returned with an empty response body and afterwards the identifier of the Service Certificate resource is no longer valid. The party that originally created (see clause 5.2.4.2) or reserved (see clause 5.2.4.3) the Server Certificate resource is responsible for ensuring that the serial number of the destroyed certificate is appropriately revoked. Only the party that created (see clause 5.2.4.2) or reserved (see clause 5.2.4.3) the Server Certificate resource is permitted to destroy it. Any attempt by another party to destroy a Server Certificate resource shall elicit the HTTP response 405 (Method Not Allowed).

The HTTP response 409 (Conflict) shall be returned with an error message body per clause 7.1.7 if an attempt is made to destroy a Server Certificate resource that is currently referenced by a Content Hosting Configuration or Content Publishing Configuration resource.

Attempting to destroy a Server Certificate resource that has been reserved but never uploaded shall elicit a 200 (OK) HTTP response with an empty message body. In this case, the Media AF should release any resources associated with the reservation.

Any subsequent operations citing the resource identifier of a destroyed Server Certificate should result in a 410 (Gone) or else a 404 (Not Found) HTTP response message that includes an error message body per clause 7.1.7.

### 5.2.5 Content Preparation provisioning

#### 5.2.5.1 General

For downlink media delivery, the Media AS may be required to process content ingested at reference point M2 before distributing it at reference point M4. For uplink media delivery, the Media AS may be required to process content contributed by Media Clients before publishing it to the Media Application Provider at reference point M2. These content processing operations are described by a Content Preparation Template resource provisioned in the Media AF by the Media Application Provider at reference point M1, as specified in clause 8.5, and subsequently configured in the Media AS by the Media AF at reference point M3 using an API outside the scope of the present document.

HTTP responses for successful and operation-specific failure cases are specified in the following clauses. For all other failure cases, an HTTP response indicating a response code in accordance with clause 7.1.6 shall be returned to the API client. In all failure cases a message body in accordance with clause 7.1.7 shall be included in the response message.

#### 5.2.5.2 Create Content Preparation Template resource operation

This operation is used by the Media Application Provider to register a new Content Preparation Template with a Provisioning Session in the Media AF. The Media Application Provider shall use the HTTP POST method to upload a new Content Preparation Template resource to the Media AF. The request URL shall be a well-known sub-resource of the Provisioning Session resource representing its Content Preparation Templates resource collection, as specified in clause 8.5.2. The HTTP request message body shall be a Content Preparation Template as specified in clause 8.5.3. The MIME content type of the Content Preparation Template shall be supplied in the Content-Type HTTP request header.

Upon successful creation, the Media AF shall respond with a 201 (Created) response message and the URL of the newly created resource, including its resource identifier, shall be provided as the value of the Location HTTP header field. The response message body shall be a representation of the current state of the Content Preparation Template resource (see clause 8.5.2.1), including any properties assigned by the Media AF.

This operation may be performed multiple times by a Media Application Provider to provision different Content Preparation Template resources within the scope of a Provisioning Session. Each such resource is assigned a different Content Preparation Template identifier by the Media AF.

If the MIME content type indicated in Content-Type is not understood by the Media AF, the creation of the Content Preparation Template resource shall fail with HTTP error response status code 415 (Unsupported Media Type) that includes an error message body per clause 7.1.7.

If the request is acceptable but the Media AF is unable to provision the resources required by the supplied Content Preparation Template, the create operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Content Preparation Template resource shall remain in an uncreated state in the Media AF.

#### 5.2.5.3 Retrieve Content Preparation Template resource operation

This operation is used by the Media Application Provider to retrieve the current state of a Content Preparation Template resource from the Media AF. The HTTP GET method shall be used for this purpose, citing the resource identifier of the target Server Certificate in the request URL.

If the operation is successful, the Media AF shall respond with 200 (OK) and shall provide a representation of the requested resource in the HTTP message response body. The Content-Type response header shall have the same value as that supplied when the Content Preparation Template resource was created using the operation specified in clause 5.2.5.2.

#### 5.2.5.4 Update Content Preparation Template resource operation

This operation is used by the Media Application Provider to modify or replace an existing Content Preparation Template resource. The HTTP PATCH or HTTP PUT methods shall be used for this purpose. The replacement Content Preparation Template resource representation shall be provided in the body of the HTTP request message.

If the HTTP request is acceptable but the operation results in no change to the resource representation, a 204 (No Content) HTTP response message with an empty body should be returned.

If the operation is otherwise successful, the Media AF shall return a 200 (OK) HTTP response message and shall provide a representation of the current state of the resource in the message body to confirm successful update.

If the Media AF does not support modification of the Content Preparation Template, the update operation shall fail with a 403 (Forbidden) HTTP response that includes an error message body per clause 7.1.7.

If the MIME content type indicated in Content-Type is not acceptable to the Media AF, the creation of the Content Preparation Template resource shall fail with HTTP error response status code 415 (Unsupported Media Type).

If the request is acceptable but the Media AF is unable to provision the resources required by the supplied Content Preparation Template, the update operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Content Preparation Template resource in the Media AF shall remain in the state immediately prior to the update operation.

#### 5.2.5.5 Destroy Content Preparation Template resource operation

This operation is used by the Media Application Provider to destroy a Content Preparation Template resource. The HTTP DELETE method shall be used for this purpose, citing the resource identifier of the target Content Preparation Template in the request URL.

If the operation is successful, the Media AF shall return a 204 (No Content) response message with an empty message body.

If the Content Preparation Template is still referenced by a Content Hosting Configuration or Content Publishing Configuration, the operation shall fail with HTTP error response status code 409 (Conflict) that includes an error message body per clause 7.1.7.

### 5.2.6 Edge Resources provisioning

#### 5.2.6.1 General

These operations are used by the Media Application Provider at reference point M1 to provision edge computing resources in the Media AF for the purpose of instantiating Edge Application Server (EAS) instances of the Media AS in an Edge Data Network (EDN), as defined in TS 23.558 [23558].

NOTE: The requirements for an edge-enabled Media AF are defined in clause 4.5.2 of TS 26.501 [26501].

HTTP responses for successful and operation-specific failure cases are specified in the following clauses. For all other failure cases, an HTTP response indicating a response code in accordance with clause 7.1.6 shall be returned to the API client. In all failure cases a message body in accordance with clause 7.1.7 shall be included in the response message.

#### 5.2.6.2 Create Edge Resources Configuration resource operation

This operation is used by the Media Application Provider to create a new Edge Resources Configuration resource in the Media AF. The HTTP POST method shall be used for this purpose. The request URL shall be a well-known sub‑resource of the Provisioning Session resource representing its Edge Resources Configurations resource collection, as specified in clause 8.6.2. The request message body shall be an Edge Resources Configuration resource representation, as specified in clause 8.6.3.1.

- If the edgeManagmentMode is set to EM\_AF\_DRIVEN (indicating AF-driven edge resource management), the Media AF is responsible for requesting and managing the required edge resources and for handling EAS relocation in relation to media delivery sessions that fall within the scope of the parent Provisioning Session.

- If the edgeManagementMode is set to EM\_CLIENT\_DRIVEN (indicating client-driven edge resource management), the Media AF shall only request edge resources based on requests from the Edge Enabler Client (EEC) instantiated in the Media Session Handler at reference point EDGE‑1 (as defined in clause 6 of TS 23.558 [23558]).

If the operation is successful, the Media AF shall generate a resource identifier representing the new Edge Resources Provisioning Configuration. In this case, the Media AF shall respond with a 201 (Created) HTTP response message and the URL of the newly created resource, including its resource identifier, shall be provided as the value of the Location HTTP header field. The response message body shall be a representation of the current state of the Edge Resources Configuration resource (see clause 8.6.3.1), including any properties assigned by the Media AF.

If the request is acceptable but the Media AF is unable to provision the resources required by the supplied Edge Resources Configuration, the create operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Edge Resources Configuration resource shall remain in an uncreated state in the Media AF.

This operation may be performed multiple times by a Media Application Provider to provision different Edge Resources Configuration resources within the scope of a Provisioning Session. Each such resource is assigned a different Edge Resources Configuration identifier by the Media AF.

#### 5.3.6.3 Retrieve Edge Resources Configuration resource operation

This operation is used by the Media Application Provider to retrieve the current state of an existing Edge Resources Provisioning Configuration resource from the Media AF. The HTTP GET method shall be used for this purpose.

If the procedure is successful, the Media AF shall return a 200 (OK) response message that includes a representation of the target Edge Resources Configuration resource (see clause 8.6.3.1) in the response message body.

#### 5.2.6.4 Update Edge Resources Configuration resource operation

This operation is invoked by the Media Application Provider to modify the properties of an existing Edge Resources Configuration resource. All writeable properties except edgeManagementMode may be updated. The HTTP PATCH or HTTP PUT methods shall be used for this purpose. The replacement Edge Resources Configuration resource representation shall be provided in the body of the HTTP request message.

If the HTTP request is acceptable but the operation results in no change to the resource representation, a 204 (No Content) HTTP response message with an empty body should be returned.

If the operation is otherwise successful, the Media AF shall return a 200 (OK) HTTP response message and shall provide a representation of the resulting state of the resource in the message body to confirm successful update.

Attempts to modify read-only properties of the target Edge Resources Configuration resource, such as the edge management mode, shall be rejected by the Media AF with a 403 (Forbidden) HTTP response that includes an error message body per clause 7.1.7.

If the request is acceptable but the Media AF is unable to provision the resources required by the supplied Edge Resources Configuration, the update operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Edge Resources Configuration resource in the Media AF shall remain in the state immediately prior to the update operation.

#### 5.2.6.5 Destroy Edge Resources Configuration resource operation

This operation is used by the Media Application Provider to destroy an Edge Resources Configuration resource in the Media AF. The HTTP DELETE method shall be used for this purpose, citing the resource identifier of the target Edge Resources Configuration in the request URL. This operation makes the configuration unusable for future media delivery sessions, but it does not affect any ongoing media delivery sessions.

If the operation is successful, the Media AF shall return a 204 (No Content) HTTP response message with an empty message body.

The HTTP response 409 (Conflict) shall be returned with an error message body per clause 7.1.7 if an attempt is made to destroy an Edge Resources Configuration resource that is currently referenced by a Content Hosting Configuration or Content Publishing Configuration resource.

Any subsequent operations citing the resource identifier of a destroyed Edge Resources Configuration should result in a 410 (Gone) or else a 404 (Not Found) HTTP response message that includes an error message body per clause 7.1.7.

### 5.2.7 Dynamic Policy provisioning

#### 5.2.7.1 General

These operations are used by the Media Application Provider to configure Policy Templates for the media delivery sessions of a particular Provisioning Session.

A Policy Template, identified by its policyTemplateId, represents a set of PCF/NEF API parameters which defines the service quality and/or associated charging for the corresponding media delivery session(s). The Policy Template is configured as part of the provisioning procedures with the Media AF using the API specified in clause 8.7 and is subsequently instantiated by a Media Session Handler using the interactions specified in clause 5.4.3. At this point, the parameters in the Policy Template are used by the Media AF to request specific QoS and/or charging policies from the PCF (either directly or via the NEF, as specified in clause 5.5.2) for that media delivery session.

When a Policy Template requires media to be delivered in a specific Data Network and/or network slice at reference point M4, the applicationSessionContext array shall be present with at least one of the following properties populated:

- The dnn property contains the name of the Data Network in which the Media AS is hosted.

- When Network Slicing is used, the sliceInfo property contains information about the network slice which is serving the UE.

When a Policy Template is intended to influence the network QoS of Service Data Flows used for media delivery, the qoSSpecification object (of type M1QoSSpecification, see clause 7.3.3.3) shall be present:

- The qosReference value, as specified in clause 5.6.2.7 of TS 29.514 [29514], is obtained with the Service Level Agreement. See TS 23.502 [23502] for detailed usage.

- The maximumBitRate properties of the downlink and uplink objects define the maximal bit rates which are permitted to be requested by a Media Session Handler on (respectively) downlink and uplink Service Data Flows. These values are defined by configuration of the 5G System and are therefore populated by the Media AF rather than by the Media Application Provider.

- The maximumAuthorisedBitRate properties of the downlink and uplink objects define the maximal bit rates which a Media Session Handler is authorised to request on (respectively) downlink and uplink Service Data Flows. Higher bit rates are not authorised by the Media Application Provider when the Policy Template is instantiated.

- The minimumPacketLossRate properties of the downlink and uplink objects define the minimal packet loss rates which are permitted to be requested by a Media Session Handler on (respectively) downlink and uplink Service Data Flows. Lower packet loss rates are not permitted by the Media Application Provider when the Policy Template is instantiated.

When a Policy Template is intended to be used for differential charging, the chargingSpecification property shall be present.

HTTP responses for successful and operation-specific failure cases are specified in the following clauses. For all other failure cases, an HTTP response indicating a response code in accordance with clause 7.1.6 shall be returned to the API client. In all failure cases a message body in accordance with clause 7.1.7 shall be included in the response message.

#### 5.2.7.2 Policy Template life-cycle

The state of a Policy Template is exposed by the Media AF in the state property of the Policy Template resource and has one of the values specified in table 5.2.7.2‑1.

Table 5.2.7.2‑1: Policy Template states

|  |  |
| --- | --- |
| Policy Template state | Meaning |
| PENDING | The Policy Template is awaiting validation by the Media Delivery System, potentially because not all required parameters have yet been provided. This is the default state after Policy Template creation. |
| INVALID | One or more of the Policy Template's properties failed validation by the Media Delivery System. |
| READY | After successful validation by the Media Delivery System the Policy Template moves into this state. |
| SUSPENDED | The Media Delivery System may move a Policy Template into this state under certain conditions defined within the Service Level Agreement. |

Figure 5.2.7.2‑1 below is a state diagram showing the life-cycle of a Policy Template resource in the Media AF.



Figure 5.2.7.2‑1: Policy Template Resource State Diagram

Policy Templates require Media Delivery System operator verification, and a Policy Template resource that is newly created cannot be used immediately.

1. Upon creation, a Policy Template resource shall be in the PENDING state. Once all mandatory properties are provided, the Media AF triggers validation.

2. If the Policy Template is not deemed to be valid by the operator of the Media Delivery System, it shall move to the INVALID state, from where it can be updated to remedy the defect.

3. Once it has been successfully validated by the Media Delivery System operator, a Policy Template resource shall take the READY state, indicating that it may be applied to media delivery sessions.

4. If it is subsequently updated by the Media Application Provider, a Policy Template resource shall return to the PENDING state, awaiting revalidation by the operator of the Media Delivery System.

5. Finally, a Policy Template resource may be SUSPENDED by the Media Delivery System operator, e.g., in case of a violation of the usage terms or for some other reasons, which renders it unusable. The update of any property moves the state from SUSPENDED into PENDING and triggers revalidation.

A Policy Template resource may be destroyed when it is in any of the abovementioned states.

The Media AF shall verify the status of a Policy Template resource prior to allowing a Dynamic Policy Instance to instantiate it. Only a Policy Template resource in the READY state is eligible to be instantiated in this way.

The Media AF shall indicate the current state of a Policy Template in the Policy Template resource in machine-readable form as well as indicating a human-readable reason for this state.

#### 5.2.7.3 Create Policy Template resource operation

This operation is used by the Media Application Provider to create a new Policy Template resource. The HTTP POST method shall be used for this purpose. The request URL shall be a well-known sub-resource of the Provisioning Session resource representing its Policy Templates resource collection, as specified in clause 8.7.2. The HTTP request message body shall be a Policy Template resource representation, as specified in clause 8.7.3.1.

If the procedure is successful, the Media AF shall generate a resource identifier to uniquely identify the newly created Policy Template resource. In that case, it shall return a 201 (Created) HTTP response message and the URL of the newly created resource, including its resource identifier, shall be provided as the value of the Location HTTP header field. The response message body shall be a representation of the current state of the Policy Template resource (see clause 8.7.3.1), including any property values set by the Media AF.

If the request is acceptable but the Media AF is unable to provision the resources required by the supplied Policy Template, the create operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Policy Template resource shall remain in an uncreated state in the Media AF.

This operation may be performed multiple times by a Media Application Provider to provision different Policy Template resources within the scope of a Provisioning Session. Each such resource is assigned a different Policy Template identifier by the Media AF.

The default state of a newly created Policy Template resource is PENDING. If all mandatory property values have been provided, the Policy Template resource is eligible for validation, as specified in clause 5.2.7.2.

#### 5.2.7.4 Retrieve Policy Template resource operation

This operation is used by the Media Application Provider to retrieve the current state of an existing Policy Template resource in the Media AF. The HTTP GET method shall be used for this purpose, citing the resource identifier of the target Policy Template in the request URL.

If the operation is successful, the Media AF shall return a 200 (OK) response that includes a representation of the target Policy Template resource (see clause 8.7.3.1) in the response message body.

#### 5.2.7.5 Update Policy Template resource operation

This operation is invoked by the Media Application Provider to modify the properties of an existing Policy Template resource in the Media AF. All available properties except state may be updated. The HTTP PATCH or HTTP PUT methods shall be used for this purpose. The replacement Policy Template resource representation shall be provided in the body of the HTTP request message.

Any update to the Policy Template resource shall automatically change its state back to PENDING, which makes it temporarily unusable by ongoing media delivery sessions. Accordingly, any attempt to instantiate the Policy Template (see clause 5.4.3) shall fail. If all mandatory property values have been provided by the Media Application Provider, the updated Policy Template is eligible for revalidation.

If the HTTP request is acceptable but the operation results in no change to the resource representation, a 204 (No Content) HTTP response message with an empty body should be returned.

If the operation is otherwise successful, the Media AF shall return a 200 (OK) response message that includes a representation of the target Policy Template resource in the response message body, confirming successful update.

Attempts to modify read-only properties of the target Policy Template resource, such as its state, shall be rejected by the Media AF with a 403 (Forbidden) HTTP response that includes an error message body per clause 7.1.7.

If the request is acceptable but the Media AF is unable to provision the resources required by the supplied Policy Template, the update operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Policy Template resource in the Media AF shall remain in the state immediately prior to the update operation.

#### 5.2.7.6 Destroy Policy Template resource operation

This operation is used by the Media Application Provider to destroy a Policy Template resource in the Media AF. The HTTP DELETE method shall be used for this purpose, citing the resource identifier of the target Policy Template in the request URL.

If the operation is successful, the Media AF shall return a 204 (No Content) response message with an empty message body.

All currently active media delivery sessions using the destroyed Policy Template shall revert to a default network QoS as a result of destroying the Policy Template resource.

Any subsequent operations citing the resource identifier of a destroyed Policy Template should result in a 410 (Gone) or else a 404 (Not Found) HTTP response message that includes an error message body per clause 7.1.7.

### 5.2.8 Content Hosting provisioning

#### 5.2.8.1 General

These operations are used by the Media Application Provider at reference point M1 to provision the Content Hosting feature for downlink media delivery.

HTTP responses for successful and operation-specific failure cases are specified in the following clauses. For all other failure cases, an HTTP response indicating a response code in accordance with clause 7.1.6 shall be returned to the API client. In all failure cases a message body in accordance with clause 7.1.7 shall be included in the response message.

#### 5.2.8.2 Create Content Hosting Configuration resource operation

This operation is used by the Media Application Provider at reference point M1 to activate the Content Hosting feature for a particular Provisioning Session. The Media Application Provider shall use the HTTP POST method for this purpose. The request URL shall be a well-known sub-resource of the Provisioning Session resource, as specified in clause 8.8.2. The HTTP request message body shall be a Content Hosting Configuration resource representation, as specified in clause 8.8.3.1. There is at most one Content Hosting Configuration at a time for a given Provisioning Session.

Regarding the configuration of content ingest by the Media AS from the Media Application Provider at reference point M2:

- If the Content Hosting Configuration uses the pull-based content ingest method, i.e., the pull attribute is set to true, then the ingestConfiguration.baseURL property shall be nominated by the Media Application Provider in the request message body. The Media AF shall return the IngestConfiguration.baseURL property value unchanged in its response message body.

- If the Content Hosting Configuration uses the push-based content ingest method, i.e., the pull attribute is set to false, then the ingestConfiguration.baseURL property shall be nominated by the Media AF and returned in the response message body. It shall not be set by the Media Application Provider in the request message body.

Regarding the configuration(s) of content distribution by the Media AS to the Media Client at reference point M4:

- In all cases, the distributionConfiguration.‌canonicalDomainName and distributionConfiguration.‌baseURL properties are read-only: they shall always be omitted from the creation request and shall be assigned by the Media AF, allowing their values to be inspected by the Media Application Provider in the returned Content Hosting Configuration resource representation, or by using the operation specified in clause 5.2.8.3 below.

- If the distributionConfiguration.‌certificateId property is present and valid, the Media AF shall assign a canonical domain name for the Media AS to expose at reference point M4 that matches the Common Name and the first Subject Alternative Name in the referenced Server Certificate resource (taking into account wildcard matching) regardless of whether the corresponding X.509 certificate was created using the operation specified in clause 5.2.4.2 or those specified in clauses 5.2.4.3 and 5.2.4.4.

- The Media Application Provider may nominate an alternative domain name to be advertised to the Media Client in the Service Access Information by setting the distributionConfiguration.‌domainNameAlias property when (and only when) creating the Content Hosting Configuration resource. If valid, the value of this property shall then appear in the distribution‌Configuration.‌baseURL assigned by the Media AF instead of distributionConfiguration.‌canonicalDomainName. The Media Application Provider shall ensure that this domain name alias resolves to the canonical domain name of the Media AS notified by the Media AF in its response by means of suitable DNS configuration.

If the operation is successful, the Media AF shall return a 201 (Created) HTTP response message and the request URL shall be returned as the value of the Location HTTP header field. The response message body shall be a representation of the current state of the Content Hosting Configuration resource (see clause 8.8.3.1), including any properties assigned by the Media AF.

If any resources referenced by the supplied Content Hosting Configuration resource representation are invalid, the create operation shall fail with an HTTP response status code of 400 (Bad Request) and an error message body per clause 7.1.7. In this case, the Content Hosting Configuration resource shall remain in an uncreated state in the Media AF.

If distributionConfiguration.‌domainNameAlias is set in the supplied Content Hosting Configuration resource representation but its value is not a syntactically valid Fully-Qualified Domain Name or if the distributionConfiguration.‌certificateId property is absent or if the supplied domain name alias does match any of one of the Subject Alternative Names listed in the Server Certificate referenced by the distributionConfiguration.‌certificateId property, the create operation shall fail with an HTTP response status code of 400 (Bad Request) and an error message body per clause 7.1.7. In this case, the Content Hosting Configuration resource shall remain in an uncreated state in the Media AF.

NOTE: Even if multiple distribution configurations in the same Content Hosting Configuration reference the same Server Certificate resource, they may each nominate a different domain name alias from among its Subject Alternative Names.

Attempting to create a Content Hosting Configuration in the scope of a Provisioning Session of any type other than DOWNLINK shall fail with an HTTP response status code of 403 (Forbidden) and an error message body per clause 7.1.7. In this case, the Content Hosting Configuration resource shall remain in an uncreated state in the Media AF.

If the request is acceptable but the Media AF is unable to provision the resources required by the supplied Content Hosting Configuration, the create operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Content Hosting Configuration resource shall remain in an uncreated state in the Media AF.

#### 5.2.8.3 Retrieve Content Hosting Configuration resource operation

This operation is used by the Media Application Provider to retrieve the current state of an existing Content Hosting Configuration resource from the Media AF. The HTTP GET method shall be used for this purpose.

If the operation is successful, the Media AF shall return a 200 (OK) response message that includes a representation of the target Content Hosting Configuration resource (see clause 8.8.3.1) in the response message body.

#### 5.2.8.4 Update Content Hosting Configuration resource operation

This operation is invoked by the Media Application Provider to modify the properties of an existing Content Hosting Configuration resource. All writeable properties except domainNameAlias may be updated. The HTTP PATCH or HTTP PUT methods shall be used for this purpose. The replacement Content Hosting Configuration resource representation shall be provided in the body of the HTTP request message.

If the HTTP request is acceptable but the operation results in no change to the resource representation, a 204 (No Content) HTTP response message with an empty body should be returned.

If the operation is otherwise successful, the Media AF shall return a 200 (OK) HTTP response message and shall provide a representation of the current state of the target resource in the message body to confirm successful update.

If any resources referenced by the supplied Content Hosting Configuration resource representation are invalid, the create operation shall fail with an HTTP response status code of 400 (Bad Request) and an error message body per clause 7.1.7. In this case, the Content Hosting Configuration resource shall remain in the state immediately prior to the update operation.

Attempts to modify read-only properties of the target Content Hosting Configuration resource, such as the canonical domain name of a distribution configuration, shall be rejected by the Media AF with a 403 (Forbidden) HTTP response that includes an error message body per clause 7.1.7.

If the request is acceptable but the Media AF is unable to provision the resources required by the supplied Content Hosting Configuration, the update operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Content Hosting Configuration resource in the Media AF shall remain in the state immediately prior to the update operation.

#### 5.2.8.5 Destroy Content Hosting Configuration resource operation

This operation is used by the Media Application Provider to destroy a Content Hosting Configuration resource in the Media AF and to terminate the related content distribution. The HTTP DELETE method shall be used for this purpose, citing the well-known sub-resource of the target Provisioning Session in the request URL. As a result, the Media AF shall release any associated network resources, purge any cached content in the Media AS, and remove any corresponding configurations.

If the procedure is successful, the Media AF shall return a 200 (OK) HTTP response message with an empty message body.

#### 5.2.8.6 Purge Content Hosting cache operation

This operation is used by the Media Application Provider to purge content from the Media AS Content Hosting cache. The HTTP POST method shall be used for this purpose with a regular expression describing the media resource URLs to be purged provided in the body of the request. The message request body shall be encoded using the application/x-www-form-urlencoded MIME content type as a key–value pair, with the key being the string pattern and the value being the regular expression.

On receiving a purge request, the Media AF shall immediately invalidate all media resources in the Media AS cache matching the regular expression by declaring them as stale. A subsequent Media Client request at reference point M4 for a purged media resource will trigger the fetching (and possible caching) of the current version from the Media Application Provider's content origin via reference point M2 in case of a Pull-based ingest. For Push-based ingest, M4 requests for purged content shall be responded to with a 404 (Not Found) HTTP response until such time as a new version of the object is published by the Media Application Provider to the Media AS via at reference point M2.

If the procedure is successful, the Media AF shall return one of the following response messages:

- 204 (No Content) if no cache entries were purged, for example because no current cache entries matched the regular expression supplied in the original request. The response message body shall be empty in this case.

- 200 (OK) if some cache entries were purged. The body of the response message shall indicate the total number of cache entries purged in all Media AS instances distributing the content.

The HTTP response 400 (Bad Request) shall be returned in the case where the request message body – or the regular expression contained in it – are found by the Media AF to be syntactically malformed.

### 5.2.9 Content Publishing provisioning

#### 5.2.9.1 General

These operations are used by the Media Application Provider at reference point M1 to provision the Content Publishing feature for uplink media delivery.

HTTP responses for successful and operation-specific failure cases are specified in the following clauses. For all other failure cases, an HTTP response indicating a response code in accordance with clause 7.1.6 shall be returned to the API client. In all failure cases a message body in accordance with clause 7.1.7 shall be included in the response message.

#### 5.2.9.2 Create Content Publishing Configuration resource operation

This operation is used by the Media Application Provider at reference point M1 to activate the Content Publishing feature for a particular Provisioning Session. The Media Application Provider shall use the HTTP POST method for this purpose. The request URL shall be a well-known sub-resource of the Provisioning Session resource, as specified in clause 8.9.2. The HTTP request message body shall be a Content Publishing Configuration resource representation, as specified in clause 8.9.3.1. There is at most one Content Publishing Configuration at a time for a given Provisioning Session.

Regarding the configuration of content egest from the Media AS to the Media Application Provider at reference point M2:

- If the Content Publishing Configuration uses the push-based content egest method, i.e., the pull attribute is set to false, then the egestConfiguration.baseURL property shall be nominated by the Media Application Provider in the request message body. The Media AF shall return the egestConfiguration.baseURL property value unchanged in its response message body.

- If the Content Publishing Configuration uses the pull-based content egest method, i.e., the pull attribute is set to true, then the egestConfiguration.baseURL property shall be nominated by the Media AF and returned in the response message body. It shall not be set by the Media Application Provider in the request message body.

Regarding the configuration(s) of content contribution by the Media Client to the Media AS at reference point M4:

- In all cases, the contributionConfiguration.‌canonicalDomainName and contributionConfiguration.‌baseURL properties are read-only: they shall always be omitted from the creation request and shall be assigned by the Media AF, allowing their values to be inspected by the Media Application Provider in the returned Content Publishing Configuration resource representation, or by using the operation specified in clause 5.2.9.3 below.

- If the contributionConfiguration.‌certificateId property is present and valid, the Media AF shall assign a canonical domain name for the Media AS to expose at reference point M4 that matches the Common Name and the first Subject Alternative Name in the referenced Server Certificate resource (taking into account wildcard matching) regardless of whether the corresponding X.509 certificate was created using the operation specified in clause 5.2.4.2 or those specified in clauses 5.2.4.3 and 5.2.4.4.

- The Media Application Provider may nominate an alternative domain name to be advertised to the Media Client in the Service Access Information by setting the contributionConfiguration.‌domainNameAlias property when (and only when) creating the Content Publishing Configuration resource. If valid, the value of this property shall then appear in the contribution‌Configuration.‌baseURL assigned by the Media AF instead of contributionConfiguration.‌canonicalDomainName. The Media Application Provider shall ensure that this domain name alias resolves to the canonical domain name of the Media AS notified by the Media AF in its response by means of suitable DNS configuration.

If the operation is successful, the Media AF shall return a 201 (Created) HTTP response message and the request URL shall be returned as the value of the Location HTTP header field. The response message body shall be a representation of the current state of the Content Publishing Configuration resource (see clause 8.9.3.1), including any properties assigned by the Media AF.

If any resources referenced by the supplied Content Publishing Configuration resource representation are invalid, the create operation shall fail with an HTTP response status code of 400 (Bad Request) and an error message body per clause 7.1.7. In this case, the Content Publishing Configuration resource shall remain in an uncreated state in the Media AF.

If contributionConfiguration.‌domainNameAlias is set in the supplied Content Hosting Configuration resource representation but its value is not a syntactically valid Fully-Qualified Domain Name or if the contributionConfiguration.‌certificateId property is absent or if the supplied domain name alias does match any of one of the Subject Alternative Names listed in the Server Certificate referenced by the contributionConfiguration.‌certificateId property, the create operation shall fail with an HTTP response status code of 400 (Bad Request) and an error message body per clause 7.1.7. In this case, the Content Publishing Configuration resource shall remain in an uncreated state in the Media AF.

NOTE: Even if multiple contribution configurations in the same Content Publishing Configuration reference the same Server Certificate resource, they may each nominate a different domain name alias from among its Subject Alternative Names.

Attempting to create a Content Publishing Configuration in the scope of a Provisioning Session of any type other than UPLINK shall fail with an HTTP response status code of 403 (Forbidden) and an error message body per clause 7.1.7. In this case, the Content Publishing Configuration resource shall remain in an uncreated state in the Media AF.

If the request is acceptable but the Media AF is unable to provision the resources required by the supplied Content Publishing Configuration, the create operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Content Publishing Configuration resource shall remain in an uncreated state in the Media AF.

#### 5.2.9.3 Retrieve Content Publishing Configuration resource operation

This operation is used by the Media Application Provider to retrieve the current state of an existing Content Publishing Configuration resource from the Media AF. The HTTP GET method shall be used for this purpose.

If the operation is successful, the Media AF shall return a 200 (OK) response message that includes a representation of the target Content Publishing Configuration resource (see clause 8.9.3.1) in the response message body.

#### 5.2.9.4 Update Content Publishing Configuration resource operation

This operation is invoked by the Media Application Provider to modify the properties of an existing Content Publishing Configuration resource. All writeable properties may be updated. The HTTP PATCH or HTTP PUT methods shall be used for this purpose.

If the HTTP request is acceptable but the operation results in no change to the resource representation, a 204 (No Content) HTTP response message with an empty body should be returned.

If the operation is otherwise successful, the Media AF shall return a 200 (OK) HTTP response message and shall provide a representation of the current state of the target resource in the message body to confirm successful update.

Attempts to modify read-only properties of the target Content Publishing Configuration resource, such as the canonical domain name of a contribution configuration, shall be rejected by the Media AF with a 403 (Forbidden) HTTP response that includes an error message body per clause 7.1.7.

If the request is acceptable but the Media AF is unable to provision the resources required by the supplied Content Publishing Configuration, the update operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Content Publishing Configuration resource in the Media AF shall remain in the state immediately prior to the update operation.

#### 5.2.9.5 Destroy Content Publishing Configuration resource operation

This operation is used by the Media Application Provider to destroy a Content Publishing Configuration resource and to terminate the related egest of content. The HTTP DELETE method shall be used for this purpose. As a result, the Media AF will release any associated network resources, purge any cached content, and delete any corresponding configurations.

If the procedure is successful, the Media AF shall return a 204 (No Content) HTTP response message with an empty message body.

#### 5.2.9.6 Purge Content Publishing cache operation

When pull-based content egest is provisioned in the Content Publishing Configuration, this operation is used by the Media Application Provider to purge content from the Media AS Content Publishing cache. The HTTP POST method shall be used for this purpose with a regular expression describing the media resource URLs to be purged provided in the body of the request. The message request body shall be encoded using the application/x-www-form-urlencoded MIME content type as a key–value pair, with the key being the string pattern and the value being the regular expression.

On receiving a purge request, the Media AF shall immediately invalidate all media resources in the Media AS cache matching the regular expression by declaring them as stale. Requests at reference point M2 for purged media resources should be responded to with a 410 (Gone) HTTP response or else a 404 (Not Found) response.

If the procedure is successful, the Media AF shall return one of the following response messages:

- 204 (No Content) if no cache entries were purged, for example because no current cache entries matched the regular expression supplied in the original request. The response message body shall be empty in this case.

- 200 (OK) if some cache entries were purged. The body of the response message shall indicate the total number of cache entries purged in all Media AS instances egesting the content.

The HTTP response 400 (Bad Request) shall be returned in the case where the request message body – or the regular expression contained in it – are found by the Media AF to be syntactically malformed.

### 5.2.10 Metrics Reporting provisioning

#### 5.2.10.1 General

These operations are used by the Media Application Provider at reference point M1 to provision QoE metrics reporting functionality associated with downlink or uplink media delivery. The Media Application Provider may provision several Metrics Reporting Configurations within the scope of a Provisioning Session with different properties which determine whether and how often the Media Session Handler submits QoE metrics reports to the Media AF as well as the format and contents of these reports. To this end, each Metrics Reporting Configuration shall specify a *metrics scheme*, which may be specified by 3GPP or by another party. The chosen metrics scheme URI is indicated in the scheme property of the Metrics Reporting Configuration. This clause defines the basic operations; more details are provided in clause 8.10.

A given Metrics Reporting Configuration is uniquely identified within the scope of its parent Provisioning Session by the metricsReportingConfigurationId property of the corresponding Metrics Reporting Configuration resource, as specified in clause 8.10.3.1.

Where metrics reporting is not required for the entire duration of a media delivery session, reportingStartOffset and/or reportingDuration parameters may additionally be specified for a Metrics Reporting Configuration indicating the portion of each media delivery session for which metrics reports are to be submitted by the Media Session Handler.

HTTP responses for successful and operation-specific failure cases are specified in the following clauses. For all other failure cases, an HTTP response indicating a response code in accordance with clause 7.1.6 shall be returned to the API client. In all failure cases a message body in accordance with clause 7.1.7 shall be included in the response message.

#### 5.2.10.2 Create Metrics Reporting Configuration resource operation

This operation is used by the Media Application Provider to create a Metrics Reporting Configuration resource within the scope of an existing Provisioning Session. The Media Application Provider shall use the HTTP POST method for this purpose. The request URL shall be a well-known sub-resource of the Provisioning Session resource representing its Metrics Reporting Configurations resource collection, as specified in clause 8.10.2. The HTTP request message body shall be a Metrics Reporting Configuration resource representation, as specified in clause 8.10.3.1.

Upon successful creation of the resource, the Media AF shall return a 201 (Created) response message and the resource URL for the newly-created Metrics Reporting Configuration resource, including its resource identifier, shall be returned as the value of the Location HTTP header field. The response message body shall be a representation of the current state of the Metrics Reporting Configuration resource (see clause 8.10.3.1), including any properties assigned by the Media AF.

If the metrics scheme or any of the metrics cited in the supplied Metrics Reporting Configuration is not supported by the Media AF, the create operation shall fail with an HTTP response status code of 400 (Bad Request) and an error message body per clause 7.1.7. In this case, the Metrics Reporting Configuration resource shall remain in an uncreated state in the Media AF.

If the request is acceptable but the Media AF is unable to provision the resources required by the supplied Metrics Reporting Configuration, the create operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Metrics Reporting Configuration resource shall remain in an uncreated state in the Media AF.

This operation may be performed multiple times by a Media Application Provider to provision different Metrics Reporting Configuration resources within the scope of a Provisioning Session. Each such resource is assigned a different Metrics Reporting Configuration identifier by the Media AF.

#### 5.2.10.3 Retrieve Metrics Reporting Configuration resource operation

This operation is used by the Media Application Provider to retrieve the current state of an existing Metrics Reporting Configuration resource in the Media AF. The HTTP GET method shall be used for this purpose, citing the resource identifier of the target Metrics Reporting Configuration in the request URL.

If successful, the Media AF shall return a 200 (OK) HTTP response message that includes a representation of the target Metrics Reporting Configuration resource (see clause 8.10.3.1) in the response message body.

#### 5.2.10.4 Update Metrics Reporting Configuration resource operation

This operation is invoked by the Media Application Provider to entirely replace or modify certain properties of an existing Metrics Reporting Configuration resource. All available properties may be updated. The HTTP PATCH or HTTP PUT methods shall be used for this purpose. The replacement Metric Reporting Configuration resource representation shall be provided in the body of the HTTP request message.

If the HTTP request is acceptable but the operation results in no change to the resource representation, a 204 (No Content) HTTP response message with an empty body should be returned.

If the operation is otherwise successful, the Media AF shall return a 200 (OK) HTTP response message that includes a representation of the current state of the target resource in the message body to confirm successful update.

If the metrics scheme or any of the metrics cited in the supplied Metrics Reporting Configuration is not supported by the Media AF, the update operation shall fail with an HTTP response status code of 400 (Bad Request) and an error message body per clause 7.1.7. In this case, the Metrics Reporting Configuration resource in the Media AF shall remain in the state immediately prior to the update operation.

Attempts to modify read-only properties of the target Metrics Reporting Configuration resource shall be rejected by the Media AF with a 403 (Forbidden) HTTP response that includes an error message body per clause 7.1.7.

If the request is acceptable but the Media AF is unable to provision the resources required by the supplied Metrics Reporting Configuration, the update operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Metrics Reporting Configuration resource in the Media AF shall remain in the state immediately prior to the update operation.

#### 5.2.10.5 Destroy Metrics Reporting Configuration resource operation

This operation is used by the Media Application Provider to destroy a Metrics Reporting Configuration resource and to terminate the related metrics reporting procedure by Media Clients. The HTTP DELETE method shall be used for this purpose, citing the resource identifier of the target Metrics Reporting Configuration in the request URL. As a result, the Media AF shall release any associated resources, discard any pending metrics reports, and remove any corresponding configurations.

If the operation is successful, the Media AF shall return a 204 (No Content) HTTP response message with an empty message body.

Any subsequent operations citing the resource identifier of a destroyed Metrics Reporting Configuration should result in a 410 (Gone) or else a 404 (Not Found) HTTP response message that includes an error message body per clause 7.1.7.

### 5.2.11 Consumption Reporting provisioning

#### 5.2.11.1 General

These operations are used by the Media Application Provider at reference point M1 to activate and to configure consumption reporting functionality associated with downlink media delivery. The Media Application Provider may provision a single Consumption Reporting Configuration within the scope of a Provisioning Session which determines whether and how often the Media Session Handler submits consumption reports to the Media AF. This clause defines the basic operations. More details are provided in clause 8.11.

HTTP responses for successful and operation-specific failure cases are specified in the following clauses. For all other failure cases, an HTTP response indicating a response code in accordance with clause 7.1.6 shall be returned to the API client. In all failure cases a message body in accordance with clause 7.1.7 shall be included in the response message.

#### 5.2.11.2 Create Consumption Reporting Configuration resource operation

This operation is used by the Media Application Provider to activate the Consumption Reporting feature for a particular Provisioning Session. The Media Application Provider shall use the HTTP POST method for this purpose. The request URL shall be a well-known sub-resource of the Provisioning Session resource, as specified in clause 8.11.2. The HTTP request message body shall be a Consumption Reporting Configuration resource representation, as specified in clause 8.11.3.1. There is at most one Consumption Reporting Configuration at a time for a given Provisioning Session.

Upon successful creation of the resource, the Media AF shall return a 201 (Created) response message and the request URL shall be returned as the value of the Location HTTP header field. The response message body shall be a representation of the current state of the Consumption Reporting Configuration resource (see clause 8.11.3.1), including any properties assigned by the Media AF.

If the supplied Consumption Reporting Configuration is not supported by the Media AF, the create operation shall fail with an HTTP response status code of 400 (Bad Request) and an error message body per clause 7.1.7. In this case, the Consumption Reporting Configuration resource shall remain in an uncreated state in the Media AF.

If the request is acceptable but the Media AF is unable to provision the resources required by the supplied Consumption Reporting Configuration, the create operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Consumption Reporting Configuration resource shall remain in an uncreated state in the Media AF.

#### 5.2.11.3 Retrieve Consumption Reporting Configuration resource operation

This operation is used by the Media Application Provider to obtain the current Consumption Reporting Configuration from the Media AF. The HTTP GET method shall be used for this purpose.

If successful, the Media AF shall return a 200 (OK) HTTP response message that includes a representation of the target Consumption Reporting Configuration resource (see clause 8.11.3.1) in the response message body.

#### 5.2.11.4 Update Consumption Reporting Configuration resource operation

This operation is invoked by the Media Application Provider to modify the current Consumption Reporting Configuration. All available parameters may be updated. The HTTP PATCH or HTTP PUT methods shall be used for this purpose. The replacement Consumption Reporting Configuration resource representation shall be provided in the body of the HTTP request message.

If the HTTP request is acceptable but the operation results in no change to the resource representation, a 204 (No Content) HTTP response message with an empty body should be returned.

If the operation is otherwise successful, the Media AF shall return a 200 (OK) HTTP response message that includes a representation of the current state of the Consumption Reporting Configuration resources to confirm successful update.

If the supplied Consumption Reporting Configuration is not acceptable to the Media AF, the update operation shall fail with an HTTP response status code of 400 (Bad Request) and an error message body per clause 7.1.7. In this case, the Consumption Reporting Configuration resource shall remain in the state immediately prior to the update operation.

Attempts to modify read-only properties of the target Consumption Reporting Configuration resource shall be rejected by the Media AF with a 403 (Forbidden) HTTP response that includes an error message body per clause 7.1.7.

If the request is acceptable but the Media AF is unable to provision the resources required by the supplied Consumption Reporting Configuration, the update operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Consumption Reporting Configuration resource in the Media AF shall remain in the state immediately prior to the update operation.

#### 5.2.11.5 Destroy Consumption Reporting Configuration resource operation

This operation is used by the Media Application Provider to destroy the Consumption Reporting Configuration resource and to terminate the related consumption reporting procedure by Media Clients. The HTTP DELETE method shall be used for this purpose, citing the well-known sub-resource of the target Provisioning Session in the request URL. As a result, the Media AF shall release any associated resources, purge any cached data, and remove any corresponding configurations.

If the operation is successful, the Media AF shall return a 204 (No Content) HTTP response message with an empty message body.

### 5.2.12 Event Data Processing provisioning

#### 5.2.12.1 General

These operations are used by the Media Application Provider at reference point M1 to configure the collection and processing of UE data related to media delivery (as defined in TS 26.531 [46]) and to restrict its exposure over reference points R5 and R6 by configuring the Data Collection AF instantiated in the Media AF (such as that defined in clause 4.7 of TS 26.501 [26501]) with one or more Event Data Processing Configurations and Data Access Profiles for a particular Event ID. The Media Application Provider may provision several Event Data Processing Configurations within the scope of a Provisioning Session with different properties.

Each instance of a Data Access Profile specifies a set of data processing operations to be performed by the Data Collection AF on its collected UE data in order to synthesize the event data to be exposed to a specific Event service consumer entity. In this release, eligible Event service consumer entities of Media Delivery event data are the NWDAF, the Event Consumer AF and the NEF.

The Event Data Processing Provisioning API is specified in clause 8.12.

HTTP responses for successful and operation-specific failure cases are specified in the following clauses. For all other failure cases, an HTTP response indicating a response code in accordance with clause 7.1.6 shall be returned to the API client. In all failure cases a message body in accordance with clause 7.1.7 shall be included in the response message.

#### 5.2.12.2 Create Event Data Processing Configuration resource operation

This operation is used by the Media Application Provider to create a new Event Data Processing Configuration within the scope of an existing Provisioning Session in the form of one or more Data Access Profiles. The HTTP POST method shall be used for this purpose. The request URL shall be a well-known sub-resource of the Provisioning Session resource representing its Event Data Processing Configurations resource collection, as specified in clause 8.12.2. The request message body shall be an Event Data Processing Configuration resource representation, as specified in clause 8.12.3.1.

If the operation is successful, the Media AF shall generate a resource identifier representing the new Event Data Processing Configuration. In this case, the Media AF shall return a 201 (Created) response message and the URL of the newly created resource, including its resource identifier, shall be provided as the value of the Location HTTP header field. The response message body shall be a representation of the current state of the Event Data Processing Configuration resource (see clause 8.12.3.1), including any properties assigned by the Media AF.

If the event identified in the supplied Event Data Processing Configuration is not supported by the Media AF, or if any of the data access profiles are unacceptable, the create operation shall fail with an HTTP response status code of 400 (Bad Request) and an error message body per clause 7.1.7. In this case, the Event Data Processing Configuration resource shall remain in an uncreated state in the Media AF.

If the Data Collection AF is not instantiated in the Media AF, the create operation shall fail with an HTTP response status code of 404 (Not Found) and an error message body per clause 7.1.7. In this case, the Event Data Processing Configuration resource shall remain in an uncreated state in the Media AF.

If the request is acceptable but the Media AF is unable to provision the resources required by the supplied Event Data Processing Configuration, the create operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Event Data Processing Configuration resource shall remain in an uncreated state in the Media AF.

This operation may be performed multiple times by a Media Application Provider to provision different Event Data Processing Configuration resources within the scope of a Provisioning Session. Each such resource is assigned a different Event Data Processing Configuration identifier by the Media AF.

#### 5.2.12.3 Retrieve Event Data Processing Configuration resource operation

This operation is used by the Media Application Provider to retrieve the current state of an existing Event Data Processing Configuration resource in the Media AF. The HTTP GET method shall be used for this purpose, citing the resource identifier of the target Event Data Processing Configuration in the request URL.

If successful, the Media AF shall return a 200 (OK) HTTP response message that includes a representation of the target Event Data Processing Configuration resource (see clause 8.12.3.1) in the response message body.

#### 5.2.12.4 Update Event Data Processing Configuration resource operation

This operation is invoked by the Media Application Provider to entirely replace or modify certain properties of an existing Event Data Processing Configuration resource. All available properties may be updated. The HTTP PATCH or HTTP PUT methods shall be used for this purpose. The replacement Event Data Processing Configuration resource representation shall be provided in the body of the HTTP request message.

If the HTTP request is acceptable but the operation results in no change to the resource representation, a 204 (No Content) HTTP response message with an empty body should be returned.

If the operation is otherwise successful, the Media AF shall return a 200 (OK) HTTP response message that includes a representation of the current state of the target resource in the message body to confirm successful update.

If the event identified in the supplied Event Data Processing Configuration is not supported by the Media AF, or if any of the data access profiles are unacceptable, the update operation shall fail with an HTTP response status code of 400 (Bad Request) and an error message body per clause 7.1.7. In this case, the Event Data Processing Configuration resource in the Media AF shall remain in the state immediately prior to the update operation.

Attempts to modify read-only properties of the target Event Data Processing Configuration resource shall be rejected by the Media AF with a 403 (Forbidden) HTTP response that includes an error message body per clause 7.1.7.

If the request is acceptable but the Media AF is unable to provision the resources required by the supplied Event Data Processing Configuration, the update operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Event Data Processing Configuration resource in the Media AF shall remain in the state immediately prior to the update operation.

#### 5.2.12.5 Destroy Event Data Processing Configuration resource operation

This operation is used by the Media Application Provider to destroy an existing Event Data Processing Configuration resource and to terminate the related collection of UE data and exposure of events to event consumer subscribers. The HTTP DELETE method shall be used for this purpose, citing the resource identifier of the target Event Data Processing Configuration in the request URL. As a result, the Data Collection AF shall process any reported UE data still outstanding and shall delete any corresponding data collection and reporting client configurations as well as any event subscriptions.

If the operation is successful, the Media AF shall return a 204 (No Content) HTTP response message with an empty message body.

Any subsequent operations citing the resource identifier of a destroyed Event Data Processing Configuration should result in a 410 (Gone) or else a 404 (Not Found) HTTP response message that includes an error message body per clause 7.1.7.

## 5.3 Network media session handling (M3, M5) interactions

### 5.3.1 Overview

This clause specifies the set of operations used by the Media Session Handler within a Media Client to invoke services on the Media AF at reference point M5 relating to downlink or uplink media delivery. A subset of these operations is also exposed by the Media AF to the Media AS at reference point M3.

### 5.3.2 Service Access Information acquisition

#### 5.3.2.1 General

Service Access Information is the set of parameters and addresses needed by the Media Client to activate reception of a downlink media delivery session or to activate an uplink media delivery session for content contribution.

The Media Session Handler may obtain Service Access Information in one of two ways:

1. From the Media-aware Application via reference point M6. In this case, the Service Access Information is initially acquired by the Media-aware Application from the Media Application Provider via reference point M8 and the Media-aware Application shall pass the parameters to the Media Session Handler using one of the session launch mechanisms specified in clause 10.2.

2. From the Media AF via reference point M5. In this case, the Service Access Information is derived by the Media AF from a Provisioning Session established at reference point M1 and the Media AF exposes this to the Media Session Handler using the operations specified in this clause. At the start of a media delivery session, a minimal set of baseline Service Access Information parameters is passed to the Media Session Handling using one of the session launch mechanisms specified in clause 10.2 and this causes it to fetch the full Service Access Information from the Media AF using the procedure specified in clause 5.3.2.3.

The data model of the Service Access Information resource acquired by the Media Session Handler of the Media Client is specified in clause 9.2.3.

Typically, the Service Access Information for downlink media streaming includes a media entry point (e.g. a URL to a DASH MPD or a URL to a progressive download file) that can be consumed by the Media Access Function and is handed to the Media Access Function via reference point M7.

Editor's Note: What about uplink media streaming?

Service Access Information additionally includes configuration information to allow the Media Session Handler to invoke procedures for dynamic policy (see clause 5.3.3), network assistance (clause 5.3.4), QoE metrics reporting (clause 5.3.5) and consumption reporting (clause 5.3.6).

If an Edge Resources Configuration with client-driven management (EM\_CLIENT\_DRIVEN) is provisioned in the applicable Provisioning Session (see clause 5.2.6), the Media AF shall convey a Client Edge Resources Configuration to the Media Session Handler as part of the Service Access Information it provides at reference point M5.

NOTE: The requirements for an edge-enabled Media Session Handler are defined in clause 4.5.2 of TS 26.501 [26501].

HTTP responses for successful and operation-specific failure cases are specified in the following clauses. For all other failure cases, an HTTP response indicating a response code in accordance with clause 7.1.6 shall be returned to the API client. In all failure cases a message body in accordance with clause 7.1.7 shall be included in the response message.

#### 5.3.2.2 Create Service Access Information resource operation

The Create operation is not permitted for the Service Access Information resource collection. Any usage of the HTTP POST method shall result in the HTTP response 405 (Method Not Allowed).

#### 5.3.2.3 Retrieve Service Access Information resource operation

This operation shall be used by the Media Session Handler to acquire Service Access Information from the Media AF. The Media Session Handler shall use the GET method for this purpose, citing the external service identifier associated with the target Provisioning Session (see clause 5.2.3) in the request URL. The request message body shall be empty.

If successful, the Media AF shall reply with a 200 (OK) HTTP response message that includes a representation of the Service Access Information associated with the target media streaming session resource in the response message body, along with HTTP response headers in line with clause 7.1.3.2.

Once it has obtained an initial set of Service Access Information, the Media Session Handler shall periodically check for updated Service Access Information by issuing a conditional HTTP GET request in line with clause 7.1.3.2. The periodicity of polling for updated Service Access Information shall be guided by the value of the Expires and/or Cache-control: max-age headers that shall be included along with every response message for this operation.

#### 5.3.2.4 Update Service Access Information resource operation

The Update operation is not permitted for members of the Service Access Information resource collection. Any usage of the HTTP PUT or PATCH methods in relation to the URLs of its members shall result in the HTTP response 405 (Method Not Allowed).

#### 5.3.2.5 Destroy Service Access Information resource operation

The Destroy operation is not permitted for members of the Service Access Information resource collection. Any usage of the HTTP DELETE method in relation to the URLs of its members shall result in the 405 (Method Not Allowed) HTTP response.

### 5.3.3 Dynamic Policy invocation

#### 5.3.3.1 Procedures

The following procedures are followed by a Media Session Handler to manage Dynamic Policy Instance resources in the Media AF via reference point M5. Instantiating a Policy Template as a dynamic policy requires a Policy Template identifier (provided in Service Access Information that is either retrieved from the Media AF using the operation specified in clause 5.3.2.3 or else supplied via reference point M6), a set of Service Data Flow description(s), an optional dynamic QoS specification and potentially other parameters defined in clause 5.7 of TS 26.501 [26501].

- The Policy Template identifier identifies the desired Policy Template (as previously provisioned per clause 5.2.7.3) to be applied to the specified application flow(s). A Policy Template includes properties such as specific QoS (e.g. background data) or different charging treatments. The Media AF combines the information from the Policy Template with dynamic QoS specification supplied by the Media Session Handler and uses this complete set of parameters to invoke the PCF according to clause 5.5.2.

- The set of Service Data Flow description(s) allow the identification and classification by the 5G System of the application traffic involved in a media delivery session. These take the form of an IP packet filter set (as defined in clause 5.7.6 of [23501]) or the Fully-Qualified Domain Name (FQDN) of a Media AS at reference point M4.

NOTE: It is not defined in this release how a Media AF in an external Data Network selects a specific DNN or S‑NSSAI.

Application Identifiers, referring to one or more Packet Flow Descriptions (PFDs), may be used as alternative traffic filtering parameters for dynamic policy invocation. The Media AF shall first provision a PFD in the NEF's PFD Function (PFDF) for one or more (external) Application IDs by sending an HTTP POST message to the NEF as specified in clause 4.4.10 of TS 29.122 [29122]. The mapping between the (external) Application Identifiers and PFDs stored in the PFDF will then be pushed to or pulled from the SMF and installed in the UPF for future traffic identification.

The Dynamic Policy Instance resource created as a result of instantiating a Policy Template shall include an MQTT endpoint address that allows the Media Session Handler to subscribe to receive asynchronous notifications from the Media AF concerning Background Data Transfer opportunities available in relation to that Dynamic Policy Instance.

HTTP responses for successful and operation-specific failure cases are specified in the following clauses. For all other failure cases, an HTTP response indicating a response code in accordance with clause 7.1.6 shall be returned to the API client. In all failure cases a message body in accordance with clause 7.1.7 shall be included in the response message.

#### 5.3.3.2 Create Dynamic Policy Instance resource operation

In order to instantiate a new dynamic policy, the Media Session Handler shall first create a resource for the Dynamic Policy Instance in the Media AF. The Media Session Handler shall use the HTTP POST message for this purpose. The body of the HTTP POST message shall be a Dynamic Policy Instance resource representation that includes a Provisioning Session identifier, the resource identifier of the target Policy Template and a set of Service Data Flow descriptions identifying the application flow(s) to be policed.

1. The provisioningSessionId property associates the Dynamic Policy Instance resource with a Provisioning Session.

2. The policyTemplateId property uniquely identifies the Policy Template on which the Dynamic Policy Instance is based.

3. The serviceDataFlowDescriptions property of the Dynamic Policy Instance resource representation is populated by the Media Session Handler and shall declare a set of Service Data Flow templates according to TS 23.503 [23503] that describe one or more application data flows comprising the media delivery session. Each Service Data Flow template contains exactly one of the following filtering specifications to identify traffic belonging to a media delivery application flow:

- a flowDescription object (including 5-tuples, Type of Service, Security Parameter Index, etc.).

- a domainName.

4. When the Media Session Handler attempts to activate a QoS-related Policy Template, the qosSpecification property shall be present in the Dynamic Policy Instance resource representation and it shall contain the following properties:

- marBwDlBitRate or marBwUlBitRate, indicating the maximum requested bit rate by the Media Session Handler.

- mirBwDlBitRate or mirBwUlBitRate, indicating the minimum requested bit rate by the Media Session Handler.

- minDesBwDlBitRate or minDesBwUlBitrate, indicating the minimum bit rate desired by the Media Session Handler.

5. When the 5G System employs a traffic enforcement function to ensure that traffic complies with the policy described by the qosSpecification property, the Media AF shall explicitly indicate this in the Dynamic Policy resource representation by setting the qosEnforcement property to true.

If the operation is successful, the Media AF shall create a new Dynamic Policy Instance resource. In this case, the Media AF shall return a 201 (Created) HTTP response message to the Media Session Handler, and the URL of the newly created Dynamic Policy Instance resource, including its resource identifier, shall be provided as the value of the Location HTTP header field. The response message body shall be a representation of the current state of the Dynamic Policy Instance resource (see clause 9.3.3.1), including any properties assigned by the Media AF.

When the Dynamic Policy Instance is successfully instantiated, the Media AF triggers the creation of a corresponding PCC rule in the 5G System according to clause 5.5.2 to enforce the required QoS and/or charging policy on the specified application flow(s). Depending on the ServiceDataFlowDescription objects in the received Dynamic Policy Instance resource representation and the sdfMethod indicated by each one, the Media AF shall populate for each one a flowDescription object and/or provide an Application Identifier referring to a PFD (Packet Flow Description) object containing the domain name of a Media AS instance.

NOTE: When the Media AF is deployed in an external Data Network, it is the responsibility of the NEF to map any external Application Identifier supplied by the Media AF into an internal Application Identifier that is known to the PCF.

If the supplied Dynamic Policy Instance is not acceptable to the Media AF, the create operation shall fail with an HTTP response status code of 400 (Bad Request) and an error message body per clause 7.1.7. In this case, the Dynamic Policy Instance resource shall remain in an uncreated state in the Media AF.

If the request is acceptable but the Media AF forbids the instantiation of the referenced Policy Template, for example because the UE is not permitted in the charging specification, the create operation shall fail with an HTTP response status code of 403 (Forbidden) and an error message body per clause 7.1.7. In this case, the Dynamic Policy Instance resource shall remain in an uncreated state in the Media AF.

If the request is acceptable but the Media AF is unable to provision the resources required by the supplied Dynamic Policy Instance, the create operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Dynamic Policy Instance resource shall remain in an uncreated state in the Media AF.

If the Media Session Handler needs to instantiate several dynamic policies, it may invoke this operation as often as needed.

#### 5.3.3.3 Retrieve Dynamic Policy Instance resource operation

This operation is used by the Media Session Handler to retrieve the current state of an existing Dynamic Policy Instance resource in the Media AF. HTTP GET method shall be used for this purpose, citing the resource identifier of the target Dynamic Policy Instance in the request URL.

If successful, the Media AF shall return a 200 (OK) HTTP response message that includes a representation of the target Dynamic Policy Instance resource (see clause 9.3.3.1) in the response message body.

#### 5.3.3.4 Update Dynamic Policy Instance resource operation

This operation is invoked by the Media Session Handler to entirely replace or modify certain properties of an existing Dynamic Policy resource. All available properties may be updated. The HTTP PATCH or HTTP PUT methods shall be used for this purpose, citing the resource identifier of an existing Dynamic Policy Instance in the request URL. The replacement Dynamic Policy Instance resource representation shall be provided in the body of the HTTP request message.

If all required information is set in the replacement Dynamic Policy Instance, the Media AF shall trigger the appropriate actions towards other Network Functions in the 5G System according to clause 5.5.2 to update the associated PCC rule in line with the modified QoS and charging policy.

If the HTTP request is acceptable but the operation results in no change to the resource representation, a 204 (No Content) HTTP response message with an empty body should be returned.

If the operation is otherwise successful, the Media AF shall return a 200 (OK) HTTP response message that includes a representation of the current state of the target resource in the message body to confirm successful update.

If the supplied Dynamic Policy Instance is not acceptable to the Media AF, the update operation shall fail with an HTTP response status code of 400 (Bad Request) and an error message body per clause 7.1.7. In this case, the Dynamic Policy Instance resource shall remain in the state immediately prior to the update operation.

Attempts to modify read-only properties of the target Dynamic Policy Instance resource shall be rejected by the Media AF with a 403 (Forbidden) HTTP response that includes an error message body per clause 7.1.7.

If the request is acceptable but the Media AF forbids the instantiation of the referenced Policy Template, for example because the UE is not permitted in the charging specification, the update operation shall fail with an HTTP response status code of 403 (Forbidden) and an error message body per clause 7.1.7. In this case, the Dynamic Policy Instance resource shall remain in the state immediately prior to the update operation.

If the request is acceptable but the Media AF is unable to provision the resources required by the supplied Dynamic Policy Instance, the update operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Dynamic Policy Instance resource shall remain in the state immediately prior to the update operation.

#### 5.3.3.5 Destroy Dynamic Policy Instance resource operation

This operation is invoked by the Media Session Handler to destroy an existing Dynamic Policy Instance resource. theThe HTTP DELETE method shall be used for this purpose, citing the resource identifier of the target Dynamic Policy Instance in the request URL. As a result, the Media AF shall trigger the appropriate actions towards other Network Functions in the 5G System according to clause 11.2.x to remove the associated PCC rule and to revert the affected application flow(s) to a default QoS and charging policy.

If the operation is successful, the Media AF shall return a 204 (No Content) HTTP response message with an empty message body.

Any subsequent operations citing the resource identifier of a destroyed Dynamic Policy Instance should result in a 410 (Gone) or else a 404 (Not Found) HTTP response message that includes an error message body per clause 7.1.7.

### 5.3.4 Network Assistance invocation

#### 5.3.4.1 Procedures

The following procedures are followed by the Media Session Handler to request Network Assistance from one of the Media AF instances listed in the serverAddresses property of the Network Assistance Configuration which is part of the Service Access Information that is either retrieved from the Media AF using the operation specified in clause 5.3.2.3 or else supplied via reference point M6.

1. The Media Client first creates a Network Assistance Session with its chosen Media AF instance. It provides information that will later be used by the Media AF to request a particular network QoS to be applied by the PCF to one or more application data flows, and to recommend a bit rate to the Media Client. The Media AF assigns a resource identifier to the Network Assistance Session at the point of creation. This procedure is further specified in clause 5.3.4.2.

When a Network Assistance Session is created, the responding Media AF instance may nominate an MQTT endpoint URL in the notificationURL property in the Network Assistance Session resource representation it returns to the Media Session Handler. If this property is present, the Media Session Handler shall subscribe to the MQTT channel provided at the indicated endpoint and shall expect to receive notifications from the Media AF of type M5QoSSpecification with an up-to-date bit rate recommendation whenever this changes.

2. The Network Assistance Session resource may be retrieved by the Media Session Handler using the procedure specified in clause 5.3.4.3.

3. At any time after the Network Assistance Session resource is created, the Media Client may use the Network Assistance Session resource identifier to explicitly request a bit rate recommendation by invoking a remote procedure call provided for this purpose by the Media AF. This procedure is further specified in clause 5.3.4.4.

4. Using the Network Assistance Session resource identifier, the Media Client may also request a delivery boost to be provided by the 5G System at any time by invoking a remote procedure call provided for this purpose by the Media AF. This procedure is further specified in clause 5.3.4.5.

5. The information provided when first creating a Network Assistance Session may be modified subsequently by the Media Session Handler using the session modification operation specified in clause 5.3.4.6.

6. In order to terminate a Network Assistance Session, the Media Client destroys the Network Assistance Session resource using the procedure specified in clause 5.3.4.7.

Details of the APIs supporting these procedures at reference point M5 are specified in clause 9.4.

HTTP responses for successful and operation-specific failure cases are specified in the following clauses. For all other failure cases, an HTTP response indicating a response code in accordance with clause 7.1.6 shall be returned to the API client. In all failure cases a message body in accordance with clause 7.1.7 shall be included in the response message.

#### 5.3.4.2 Create Network Assistance Session resource operation

This operation is used by the Media Session Handler to create a Network Assistance Session in the Media AF. The POST HTTP method shall be used for this purpose and the request message body shall be a Network Assistance Session resource representation as specified in clause 9.4.3.1.

1. The provisioningSessionId property associates the Network Assistance Session with a Provisioning Session.

2. The Media Session Handler shall populate the Network Assistance Session resource representation in the request with service data flow information and optionally the Policy Template identifier of the network QoS policy currently in force on the media streaming session for which Network Assistance operations are to be performed. (The Media AF subsequently uses this information to execute Network Assistance operations in the 5GC.)

The serviceDataFlowDescriptions property of the Network Assistance Session resource representation is populated by the Media Session Handler and shall declare a set of Service Data Flow templates according to TS 23.503 [33] that describe one or more application data flows comprising the media delivery session. Each Service Data Flow template contains exactly one of the following filtering specifications to identify traffic belonging to a media delivery application flow:

- a flowDescription object (including 5-tuples, Type of Service, Security Parameter Index, etc.).

- a domainName.

3. The requestedQoS property may be provided in the Network Assistance Session resource representation to specify an initial network QoS the Media Session Handler wishes to use for the media streaming session. If the policyTemplateId property is also populated in the Network Assistance Session resource representation, the Media AF shall return a 400 (Bad Request) HTTP response message if the requested network QoS lies outside the limits specified in the referenced Policy Template.

- If the requestedQoS property is omitted from the Network Assistance Session resource representation but the policyTemplateId is populated, the Media AF shall use the network QoS currently provisioned in the referenced Policy Template as the floor/ceiling for bit rate recommendations and delivery boosts within the scope of the Network Assistance Session.

- If neither a policyTemplateId nor a requestedQoS are supplied when creating a Network Assistance Session, operations invoked on the Media AF within the scope of the Network Assistance session are constrained only by the policies of the PCF. Upon successful creation, the Media AF shall return a 201 (Created) response message and the URL of the newly created resource, including its Network Assistance session resource identifier, shall be provided as the value of the Location HTTP header field. The response message body shall be a representation of the current state of the Network Assistance Session resource (see clause 9.4.3.1), including any properties assigned by the Media AF.

If the operation is successful, the Media AF shall create a new Network Assistance Session resource. In this case, the Media AF shall return a 201 (Created) HTTP response message to the Media Session Handler, and the URL of the newly created Network Assistance Session resource, including its resource identifier, shall be provided as the value of the Location HTTP header field. The response message body shall be a representation of the current state of the Network Assistance Session resource (see clause 9.4.3.1), including any properties assigned by the Media AF.

When the Network Assistance Session is successfully instantiated, the Media AF triggers the creation of a corresponding PCC rule in the 5G System according to clause 5.5.3 to enforce the required QoS on the specified application flow(s). Depending on the ServiceDataFlowDescripton objects in the received Network Assistance Session resource representation and the sdfMethod indicated by each one, the Media AF shall populate for each one a flowDescription object and/or provide an Application Identifier referring to a PFD (Packet Flow Description) object containing the domain name of a Media AS instance.

NOTE: When the Media AF is deployed in an external Data Network, it is the responsibility of the NEF to map any external Application Identifier supplied by the Media AF into an internal Application Identifier that is known to the PCF.

If the supplied Network Assistance Session is not acceptable to the Media AF, the create operation shall fail with an HTTP response status code of 400 (Bad Request) and an error message body per clause 7.1.7. In this case, the Network Assistance Session resource shall remain in an uncreated state in the Media AF.

If the request is acceptable but the Media AF forbids the use of the referenced Policy Template in a Network Assistance Session, for example because the UE is not permitted in the charging specification, the create operation shall fail with an HTTP response status code of 403 (Forbidden) and an error message body per clause 7.1.7. In this case, the Network Assistance Session resource shall remain in an uncreated state in the Media AF.

If the request is acceptable but the Media AF is unable to provision the resources required by the supplied Network Assistance Session, the create operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Network Assistance Session resource shall remain in an uncreated state in the Media AF.

The Media Client uses the Network Assistance Session resource identifier (naSessionId) provided by the Media AF to refer all subsequent API calls to the Media AF instance responsible for that Network Assistance Session.

#### 5.3.4.3 Retrieve Network Assistance Session resource operation

This operation is used by the Media Session Handler to retrieve the current state of a Network Assistance Session resource from the Media AF. The HTTP GET method shall be used for this purpose, citing the resource identifier of the target Network Assistance Session in the request URL.

If the operation is successful, the Media AF shall return 200 (OK) and shall provide a representation of the requested resource in the HTTP message response body.

#### 5.3.4.4 Bit rate recommendation request operation

This operation is used by the Media Session Handler to request a bit rate recommendation from the Media AF. the HTTP GET method shall be used for this purpose, citing the resource identifier of an existing Network Assistance Session in the request URL along with a sub-resource path indicting the bit rate recommendation operation.

If the operation is successful, the Media AF shall return a 200 (OK) HTTP response message and shall provide the recommended bit rate(s) in an HTTP response message body containing an M5QoSSpecification object that is populated as follows:

- For a downlink media delivery session, the recommended minimum and maximum downlink bit rates shall be indicated in the properties mirBwDlBitRate and marBwDlBitRate respectively. If a unique downlink bit rate is recommended by the Media AF, then this value shall be set identically in both of these properties. The Media Session Handler shall ignore the mandatory properties related to uplink media delivery, i.e., mirBwUlBitRate and marBwUlBitRate.

- For an uplink media delivery session, the recommended minimum and maximum uplink bit rates shall be indicated in the properties mirBwUlBitRate and marBwUlBitRate, respectively. If a unique uplink bit rate is recommended by the Media AF, then this value shall be set identically in both of these properties. The Media Session Handler shall ignore the mandatory properties related to downlink media delivery, i.e., mirBwDlBitRate and marBwDlBitRate.

The optional properties minDesBwDlBitRate, minDesBwUlBitRate, desLatency and desLoss shall not be included in the returned M5QoSSpecification object.

If the Media AF refuses to provide a bit rate recommendation, for example because the Provisioning Session in question currently lacks the rights required to receive this information, the operation shall fail with an HTTP response status code of 403 (Forbidden) and an error message body per clause 7.1.7.

#### 5.3.4.5 Delivery boost request operation

This operation is used by the Media Session Handler to request a delivery boost from the Media AF. the HTTP POST method shall be used for this purpose, citing the resource identifier of an existing Network Assistance Session in the request URL along with a sub-resource path indicating the delivery boost operation.

If the operation is successful, the Media AF shall return a 200 (OK) HTTP response message and shall provide an OperationSuccessResponse object in the message body indicating whether or not the delivery boost was successfully applied by the Media AF to the application data flow(s) described in the target Network Assistance Session.

If the Media AF refuses to provide the requested delivery boost, for example because the Provisioning Session in question currently lacks the rights required to receive a boost, the operation shall fail with an HTTP response status code of 403 (Forbidden) and an error message body per clause 7.1.7.

#### 5.3.4.6 Update Network Assistance Session resource operation

This operation is used by the Media Session Handler to replace the steaming session parameters in an existing Network Assistance Session resource with new values. The HTTP PUT or PATCH methods shall be used for this purpose, citing the resource identifier of an existing Network Assistance Session in the request URL. Any change to the Policy Template currently in force resulting from instantiation of a Dynamic Policy (see clause 5.3.3) should also be notified to the Media AF using this operation if a Network Assistance session has been created for the media delivery session in question.

If the HTTP request is acceptable but the operation results in no change to the resource representation, a 204 (No Content) HTTP response message with an empty body should be returned.

If the operation is otherwise successful, the Media AF shall return a 200 (OK) HTTP response message and shall provide a representation of the current state of the resource in the message body to confirm successful update.

If the supplied Network Assistance Session is not acceptable to the Media AF, the update operation shall fail with an HTTP response status code of 400 (Bad Request) and an error message body per clause 7.1.7. In this case, the Network Assistance Session resource shall remain in the state immediately prior to the update operation.

Attempts to modify read-only properties of the target Network Assistance Session resource shall be rejected by the Media AF with a 403 (Forbidden) HTTP response that includes an error message body per clause 7.1.7.

If the request is acceptable but the Media AF forbids the use of the referenced Policy Template in a Network Assistance Session, for example because the UE is not permitted in the charging specification, the update operation shall fail with an HTTP response status code of 403 (Forbidden) and an error message body per clause 7.1.7. In this case, the Network Assistance Session resource shall remain in the state immediately prior to the update operation.

If the request is acceptable but the Media AF is unable to provision the resources required by the supplied Network Assistance Session, the update operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Network Assistance Session resource shall remain in the state immediately prior to the update operation.

#### 5.3.4.7 Destroy Network Assistance Session resource operation

This operation is used by the Media Session Handler to terminate a Network Assistance Session. The HTTP DELETE method shall be used for this purpose, citing the resource identifier of the target Network Assistance Session in the request URL.

If the operation is successful, the Media AF shall return a 204 (No Content) HTTP response message with an empty message body.

Any subsequent operations citing the resource identifier of a destroyed Network Assistance Session should result in a 410 (Gone) or else a 404 (Not Found) HTTP response message that includes an error message body per clause 7.1.7.

### 5.3.5 Metrics reporting

#### 5.3.5.1 Procedures

These procedures are used by the Media AS at reference point M3 or else by the Metrics Reporting functions of the Media Client and subsequently by the Media Session Handler at reference point M5 to submit a metrics report to one of the Media AF instances listed in the client metrics reporting configuration of the Service Access Information resource previously retrieved using the procedure in clause 5.3.2.3.

When the metrics collection and reporting feature is provisioned for a media delivery session using the operations specified in clause 5.2.10, one or more client metrics reporting configurations, each associated with a provisioned Metrics Reporting Configuration, shall be provided to the Media Session Handler in the Service Access Information. A given client metrics reporting configuration contains information including:

1. The subset of metrics from the provisioned metrics scheme to be collected and reported by the Media Client;

2. The frequency at which these metrics are to be sampled by the Media Client;

3. The proportion of media delivery sessions for which reports are to be sent by the Media Session Handler;

4. The portion of the media session (represented by start offset and/or duration parameters) for which metrics reports are to be sent by the Media Session Handler if reporting is enabled for that media delivery session;

5. The interval at which metrics reports are to be sent by the Media Session Handler if reporting is enabled for a media delivery session; and

6. The Media AF address(es) to which metrics reports are to be sent.

Before a media delivery session is started, the Media Session Handler shall check if the Service Access Information includes any Metrics Reporting Configurations. If any such configurations are present, the Media Session Handler shall initiate the metrics reporting procedure for the media delivery session based on these configurations. During the media delivery session, the Media Session Handler shall periodically check if the Metrics Reporting Configurations are added to or removed from the Service Access Information and shall activate or deactivate the metrics reporting procedure as appropriate for the media delivery session in question. The Service Access Information indicating whether Metrics Reporting is provisioned for media delivery sessions is specified in clause 9.2.3.

Whenever a metrics report is produced for a given client metrics reporting configuration, the Media Session Handler shall reset its reporting interval timer for that configuration to the value of the clientMetrics‌Reporting‌Configurations[].‌reportingInterval property and it shall begin countdown of the timer again. Whenever the Media Session Handler terminates a media delivery session, it shall disable its reporting interval timer for all client metrics reporting configurations.

Details of the APIs supporting these procedures at reference points M3 and M5 are specified in clause 9.5.

HTTP responses for successful and operation-specific failure cases are specified in the following clauses. For all other failure cases, an HTTP response indicating a response code in accordance with clause 7.1.6 shall be returned to the API client. In all failure cases a message body in accordance with clause 7.1.7 shall be included in the response message.

#### 5.3.5.2 Submit metrics report operation

This operation is used by the Media Session Handler or Media AS to submit a metrics report to the Media AF If several Media AF addresses are listed in the serverAddresses array of the client metrics reporting configuration (see table 9.2.3.1-1), the Media Session Handler shall choose one at random and shall send the metrics report to the selected server endpoint. The HTTP POST method shall be used for this purpose, citing the address of the chosen Media AF in the request URL. The request body shall be formatted according to the metrics scheme indicated in scheme property of one of the Client Metrics Reporting Configurations (see clause 5.3.2.3 and table 9.2.3.1-1) and the Content-Type HTTP request header set accordingly. Details of individual metrics reporting schemes and their corresponding metrics report formats are beyond the scope of the present document.

A reporting client identifier should be included in the metrics report if the metrics scheme supports carriage of this data. Metrics schemes designed for use with this operation should specify a means to convey a reporting client identifier. If available to the Media Session Handler, its value should be a GPSI value as defined by TS 23.003 [23003]. Otherwise, the reporting client identifier should be represented by a stable and globally unique string.

If the HTTP request is acceptable but the Media AS has not yet fully processed the submitted metrics report, the Media AF may return a 202 (Accepted) HTTP response message with an empty body and process the report later.

If the operation is otherwise successful, the Media AF shall return a 200 (OK) HTTP response message with an empty body to acknowledge successful processing of the metrics report.

If metrics reporting is not provisioned for the Provisioning Session in question, the Media AF shall return a 403 (Forbidden) HTTP response message with an error message body per clause 7.1.7 and the Media AF shall not process the submitted report.

If the HTTP request message indicates a MIME content type in the Content-Type request header that is not consistent with one of the provisioned metrics reporting schemes, the Media AF shall return a 415 (Unsupported Media Type) HTTP response message with an error message body per clause 7.1.7 and shall not process the submitted metrics report.

If the target Media AF endpoint is temporarily unable to accept the submitted metrics report (e.g. because it is overloaded), it shall return a 503 (Service Unavailable) HTTP response message with an empty body. The optional HTTP response header Retry-After should be included in such a response, indicating when the Media AS expects to be able to accept new submissions. In this case, the Media Client should store outstanding metrics reports and reattempt submission when the endpoint later becomes available. Details are left to implementation.

### 5.3.6 Consumption reporting

#### 5.3.6.1 Procedures

These procedures are used by the Media AS at reference point M3 or else by the Consumption Reporting functions of the Media Client and subsequently by the Media Session Handler at reference point M5 to submit a consumption report to one of the Media AF instances listed in the Client Consumption Reporting Configuration of the Service Access Information resource previously retrieved using the procedure in clause 5.3.2.3.

When the Consumption Reporting feature is provisioned for a downlink media delivery session using the operations specified in clause 5.2.11, a Client Consumption Reporting Configuration shall be provided to the Media Session Handler in the Service Access Information.

Before a downlink media delivery session is started, the Media Session Handler shall check if the Service Access Information includes a Client Consumption Reporting Configuration. If such a configuration is present, the Media Session Handler shall initiate consumption reporting for the downlink media delivery session based on this configuration. During the course of the downlink media delivery session, the Media Session Handler shall periodically check if the Client Consumption Reporting Configuration is added to or removed from the Service Access Information and shall activate or deactivate the consumption reporting procedure as appropriate for the media delivery session in question.

The Service Access Information indicating whether Consumption Reporting is provisioned for a particular downlink media delivery session is specified in clause 9.2.3.

When the samplePercentage property in the Client Consumption Reporting Configuration has a value of 100 percent, the Media Session Handler shall activate the consumption reporting procedure. If the samplePercentage value is less than 100 percent, the Media Session Handler shall generate a random number which is uniformly distributed in the range of 0 to 100, and the Media Session Handler shall activate the consumption reporting procedure when the generated random number is of a lower value than the samplePercentage value.

If the consumption reporting procedure is activated, the Media Session Handler shall produce and submit a consumption report to the Media AF using the procedure specified in clause 5.3.6.2 when any of the following conditions are met:

- At the start of consumption of a downlink media delivery session;

- At the end of consumption of a downlink media delivery session;

- On determining the need to report ongoing content consumption at periodic intervals determined by the reportingInterval property in the Client Consumption Reporting Configuration.

- On detecting a location change, if the locationReporting property in the Client Consumption Reporting Configuration is set to True.

- On detecting a change of access network, if the accessReporting property in the Client Consumption Reporting Configuration is set to True.

Whenever a consumption report is produced, the Media Session Handler shall reset its consumption reporting interval timer to the value of the reportingInterval property of the Client Consumption Reporting Configuration and it shall begin countdown of the timer again. Whenever the Media Session Handler terminates a downlink media delivery session, it shall disable its consumption reporting interval timer.

Details of the APIs supporting these procedures at reference points M3 and M5 are specified in clause 9.6.

The consumption report shall comprise a time-ordered list of consumption reporting units. Each such unit shall describe the media selected for presentation during a continuous time period of a downlink media streaming session in terms of a start time and duration. The sequence of consumption reporting units shall be contiguous with no discontinuities in the reported timeline. When no media is being consumed (e.g., because the media streaming presentation is paused), the selected media shall still be indicated in the consumption reporting unit.

- A consumption reporting unit shall be included in exactly one consumption report, although delivery of this report may be attempted more than once by the Media Session Handler.

- A new consumption reporting unit shall be created when the media consumed changes or (if provisioned in the consumption reporting configuration per clause 4.3.8) when the network used to access media at reference point M4d changes.

- The last (or only) consumption reporting unit in every consumption report describes the media currently being consumed in the media streaming session and indicates in the duration property how long this media has been consumed so far.

- If there is no change in the media consumed when the next consumption report is sent to the Media AF, this consumption reporting unit shall be repeated as the first (and possibly only) consumption reporting unit in the next report with the same start time but with its duration updated to reflect the period of time that the media has been consumed up to the point of reporting.

- The last (or only) consumption reporting unit in the final consumption report sent to the Media AF at the end of the downlink media streaming session therefore describes the last media consumed.

HTTP responses for successful and operation-specific failure cases are specified in the following clauses. For all other failure cases, an HTTP response indicating a response code in accordance with clause 7.1.6 shall be returned to the API client. In all failure cases a message body in accordance with clause 7.1.7 shall be included in the response message.

#### 5.3.6.2 Submit consumption report operation

This operation is used by the Media Session Handler or Media AS to submit a consumption report to the Media AF If several Media AF addresses are listed in the serverAddresses array of the Client Consumption Reporting Configuration (see table 9.2.3.1-1), the Media Session Handler shall choose one at random and shall send the consumption report to the selected server endpoint. The HTTP POST method shall be used for this purpose, citing the address of the chosen Media AF in the request URL. The request body shall be a ConsumptionReport structure, as specified in clause 9.6.3.1.

A reporting client identifier shall be included in the consumption report. If available to the Media Session Handler, its value should be a GPSI value as defined by TS 23.003 [23003]. Otherwise, the reporting client identifier should be represented by a stable and globally unique string.

The location(s) of the UE when the media was consumed shall be included in every ConsumptionReportingUnit (see clause 9.6.3.2) if the locationReporting property in the Client Consumption Reporting Configuration is set to True.

If the HTTP request is acceptable but the Media AS has not yet fully processed the submitted consumption report, the Media AF may return a 202 (Accepted) HTTP response message with an empty body and process the report later.

If the operation is otherwise successful, the Media AF shall return a 200 (OK) HTTP response message with an empty body to acknowledge successful processing of the consumption report.

If consumption reporting is not provisioned for the Provisioning Session in question, the Media AF shall return a 403 (Forbidden) HTTP response message with an error message body per clause 7.1.7 and the Media AF shall not process the submitted consumption report.

If the target Media AF endpoint is temporarily unable to accept the submitted consumption report (e.g. because it is overloaded), it shall return a 503 (Service Unavailable) HTTP response message with an empty body. The optional HTTP response header Retry-After should be included in such a response, indicating when the Media AS expects to be able to accept new submissions. In this case, the Media Client should store outstanding consumption reports and reattempt submission when the endpoint subsequently becomes available. Details are left to implementation.

## 5.4 UE media session handling (M6, M11) interactions

### 5.4.1 Overview

This clause specifies the interactions between the Media-aware Application and the Media Session Handler at reference point M6 and those between the Media Access Function and the Media Session Handler at reference point M11. Details are provided in clause 10.

### 5.4.2 Media session handling initiation/termination

#### 5.4.2.1 Explicit media session handling initiation/termination

Media session handling of a new media delivery session may be explicitly initiated by a Media-aware Application invoking an appropriate API method on the Media Session Handler at reference point M6. An *external service identifier* shall be provided as input parameter to the API method.

In response, the Media Session Handler shall allocate a globally unique *media delivery session identifier* for use by the Media Client in its subsequent interactions with the Media AF and Media AS.

The Media Session Handler shall attempt to acquire full Service Access Information for the specified external service identifier from the Media AF using the operation defined in clause 5.3.2.3 and, if successful, shall return the media delivery session identifier to the invoker of the API method.

Subsequent interactions by the Media-aware Application with the Media Session Handler at reference point M6 shall cite the relevant media delivery session identifier.

a) If it initiates media delivery, the Media-aware Application shall also pass this media delivery session identifier to the Media Access Function at reference point M7 for subsequent use in interactions between the Media Access Function and the Media Session Handler at reference point M11.

b) Alternatively, if media delivery is initiated by the Media Session Handler on behalf of the Media-aware Application, the media delivery session identifier shall instead be passed to the Media Access Function at reference point M11 for use in subsequent interactions between them at this reference point.

Subsequent interactions by the Media Access Client with the Media AS at reference point M4 shall cite the relevant media delivery session identifier to enable media access logged by the Media AS to be correlated with media session handling operations logged by the Media AF.

The Media-aware Application may explicitly terminate media session handling of the media delivery session by invoking an appropriate API method on the Media Session Handler at reference point M6, citing the target media delivery session identifier as input parameter.

#### 5.4.2.2 Implicit media session handling initiation/termination

A UE entity may use the implicit service launch mechanism specified in clause 6 to initiate media session handling of a new media delivery session.

In response, the Media Session Handler shall allocate a globally unique *media delivery session identifier* for use by the Media Client in its subsequent interactions with the Media AF and Media AS.

The Media Session Handler shall attempt to acquire full Service Access Information for the specified external service identifier from the Media AF using the operation defined in clause 5.3.2.3.

The implicit service launch mechanism does not typically yield a return value, in which case it is not possible to return a media delivery session identifier to the invoker. Hence, it is not possible for the UE entity invoking the implicit service launch mechanism to take advantage of the UE media session handling APIs specified in clause 10. Nevertheless, the Media Session Handler is able to support a limited subset of media session handling on behalf of the UE entity – such as dynamic policy instantiation based on a Service Operation Point – if additional launch parameters are embedded in the Service URL.

When it has been initiated using the implicit method described in this clause, the media delivery session is implicitly terminated by the Media Session Handler after it detects an implementation-specific period of inactivity.

### 5.4.3 Dynamic Policy invocation

At the start of a media delivery session, the Media Session Handler shall determine the external reference and target QoS parameters of the initial Service Operation Point by invoking an appropriate API method on the Media Session Handler at reference point M11. Based on the parameter values supplied, the Media Session Handler shall attempt to instantiate a Dynamic Policy satisfying the Media Access Function’s requirements using the operation specified in clause 5.3.3.2 if the target QoS lies within the bounds of a Policy Template with the corresponding external reference advertised in the Service Access Information for the media delivery session.

The Media Session Handler shall subscribe to receive notifications from the Media Access Function at reference point M11 of changes to the Service Operation Point during the course of the media delivery session. When such a change occurs (e.g., when the Media Access Function selects a different MPEG‑DASH Representation), the Media Access Function shall send a notification to the Media Session Handler at reference point M11 citing the external reference and target QoS parameters of the new Service Operation Point. If the QoS of the new Service Operation Point is not satisfied by the currently instantiated Dynamic Policy, the Media Session Handler shall attempt to instantiate a Dynamic Policy satisfying the Media Access Function’s requirements using the operation specified in clause 5.3.3.2 if the target QoS lies within the bounds of a Policy Template with the corresponding external reference advertised in the Service Access Information for the media delivery session.

The Media-aware Application shall subscribe to receive notifications from the Media Session Handler at reference point M6 concerning Background Data Transfer opportunities. When such an opportunity is announced to the Media Session Handler by the Media AF at reference point M5, the Media Session Handler shall send a corresponding notification to the Media-aware Application at reference point M6 that includes an estimate of the opportunity window. If it wishes to avail itself of the Background Data Transfer opportunity, the Media-aware Application shall invoke a suitable API method on the Media Session Handler at reference point M6, providing an estimate of the data volume it intends to transfer over reference point M4. The Media Session Handler shall then attempt to instantiate a Dynamic Policy with Background Data Transfer network characteristics (including the data volume estimate supplied by the Media-aware Application) using the operation specified in clause 5.3.3.2 if a suitable Policy Template is advertised in the Service Access Information for the media delivery session.

### 5.4.4 Network Assistance invocation

At the start of a media delivery session, the Media Access Function shall determine an initial bit rate recommendation by invoking an appropriate API method on the Media Session Handler at reference point M11. The Media Session Handler shall invoke the operation specified in clause 5.3.4.2 to create a new Network Assistance Session and shall return to the Media Access Function the bit rate recommendation information in the response from the Media AF. The Media Access Function may use this information to set an initial bit rate for the media delivery session (e.g., by selecting an initial MPEG‑DASH Representation or contribution media encoding bit rate). The Media Access Function may also use this bit rate recommendation to select a different Service Operation Point, resulting in a change to the current Dynamic Policy (see clause 5.4.2).

The Media Session Handler shall subscribe to receive notifications from the Media AF at reference point M11 of bit rate recommendation updates. When such an update is received from the Media AF, the Media Session Handler shall send a notification to the Media Access Function at reference point M11 providing the new bit rate recommendation. As a result, the Media Access Function may modify the bit rate of the media delivery session (e.g., by switching to a different MPEG‑DASH Representation or by varying the rate controller of a contribution media encoder). The Media Access Function may also use this bit rate recommendation to select a different Service Operation Point, resulting in a change to the current Dynamic Policy (see clause 5.4.2).

During the course of the media delivery session the Media Access Function may request a delivery boost by invoking an appropriate API method on the Media Session Handler at reference point M11.

### 5.4.5 Metrics reporting

When metrics reporting is active for a given media delivery session, the Media Session Handler shall periodically sample the metrics required by the metrics scheme(s) configured per clause 5.3.5.1 by invoking an appropriate API method at reference point M11 on the Media Access Function and shall use these to populate metrics reports.

### 5.4.6 Consumption reporting

When consumption reporting is active for a given media delivery session, the Media Session Handler shall periodically determine the consumption reporting parameters required per clause 5.3.6.1 by invoking an appropriate API method on the Media Access Function at reference point M11 and shall use these to populate consumption reports.

## 5.5 5GC policy control (N5/N33) interactions

### 5.5.1 Overview

Certain features of the Media Delivery System rely on interfaces and APIs that are defined in the 5G Core. The interactions between the Media AF and the Network Functions in the 5GC to support these features are specified in the following clauses.

NOTE: The Media Delivery System architecture may be applied to an EPS although such application is not specified in the present document and is left to the discretion of deployments and implementations.

### 5.5.2 Policy control interactions for Dynamic Policies

The Dynamic Policies feature operates at reference point M5 between the Media Session Handler in the Media Client and a Media AF that has been appropriately provisioned with Policy Templates (see clause 5.2.7). The Dynamic Policy API at reference point M5 (see clauses 5.3.3 and 9.3) is specified in a generic way such that the associated functionality in the 5GC may be realised by various means.

NOTE 1: This clause does not limit the possible set of 5G System exposure functionalities for realising dynamic policies.

In this release, the Media AF converts Dynamic Policies API invocations received at reference point M5 into direct or indirect invocations of the Policy Authorization Service exposed by the PCF, and converts responses from the PCF into their equivalents at reference point M5 for return to the Media Session Handler.

To realise dynamic policies, the Media AF shall interact with the PCF using one of the following methods:

A. If the Media AF is deployed in the Trusted DN, it may directly invoke the Npcf\_Policy‌Authorization service at reference point N5, as specified in TS 29.514 [29514].

NOTE 2: It is the responsibility of the Media AF in this case to discover and track changes to the PCF instance responsible for the PDU Session supporting the media streaming session at reference point M4 using the discovery services provided by the NRF and/or BSF.

B. If the Media AF is deployed outside the Trusted DN, or if it is more convenient for a Media AF deployed in the Trusted DN to do so, it invokes the Nnef\_AFSession‌With‌QoS and/or Nnef\_Chargeable‌Party services exposed by the NEF, as specified in clauses 4.4.9 and 4.4.8 respectively of TS 29.522 [29522], to indirectly invoke the PCF at reference point N33.

NOTE 3: Per clause 4.4.9 of TS 29.522 [29522], the Nnef\_AFSession‌With‌QoS service is realised at reference point N33 by the AsSession‌With‌QoS exposure API. Similarly, the Nnef\_Chargeable‌Party service is realised by the Chargeable‌Party exposure API per clause 4.4.8 of [29522].

NOTE 4: Configuration of the NEF endpoint address and access credentials in the Media AF in this case is beyond the scope of the present document.

When a dynamic policy is instantiated by the Media Session Handler (per clause 4.7.3), the Media AF shall create an *AF application session context* in the PCF responsible for the PDU Session corresponding to the M4 application flows listed in the DynamicPolicy.‌serviceDataFlow‌Descriptions property.

If no corresponding AF application session context already exists, the Media AF shall use the Npcf\_‌Policy‌Authorization\_‌Create operation at reference point N5 (or, if deployed outside the Trusted DN, the equivalent AsSession‌WithQoS service operation) with the appropriate service information to create and provision a new AF application session context. The information in the AppSessionContext‌ReqData shall be derived from the service data flow descriptions in the dynamic policy resource and/or the requested QoS.

The AF application session context shall declare exactly one media component per media streaming session. A separate sub-component shall be declared for each M4 application flow listed in the NetworkAssistanceSession.‌serviceDataFlow‌Descriptions array.

For each of the dynamic policies it is managing, the Media AF shall subscribe to the following PCF notifications on the corresponding AF application session context:

- Service Data Flow QoS notification control;

- Service Data Flow deactivation;

- Resources allocation outcome.

When requesting QoS provisioning for a media streaming session, the Media AF shall use the configured Policy Template of the dynamic policy to determine the list of the QoS references within altSerReqs. The lowest priority index shall be assigned to the policy template with the lowest QoS requirement, and the highest priority shall be assigned to the requested operation point by the UE (if the UE is allowed to use that operation point).

When a dynamic policy is subsequently destroyed by the Media Session Handler (per clause 4.7.3), the Media AF shall destroy the corresponding AF application session context in the relevant PCF instance.

### 5.5.3 Policy control interactions for AF-based Network Assistance

The AF-based Network Assistance feature operates at reference point M5 between the Media Session Handler in the Media Client and a Media AF that provides Network Assistance capabilities. The Network Assistance API at reference point M5 (see clauses 5.3.4 and 9.4) is specified in a generic way such that the associated Network Assistance functionality in the 5GC may be realised by various means.

NOTE 1: This clause does not limit the possible set of 5G System exposure functionalities for obtaining Network Assistance information.

In this release, the Media AF converts Network Assistance API invocations received at reference point M5 into direct or indirect invocations of the Policy Authorization Service exposed by the PCF, and converts responses and notifications from the PCF into their equivalents at reference point M5 for delivery to the Media Session Handler.

If it supports the Network Assistance feature, the Media AF shall offer the bit rate recommendation (throughput estimation) and delivery boost request API based on existing Policy Templates that match the filtering criteria for a media streaming session, and the Media AF shall interact with the PCF using one of the following methods:

A. If the Media AF is deployed in the Trusted DN, it may directly invoke the Npcf\_Policy‌Authorization service at reference point N5, as specified in TS 29.514 [29514].

NOTE 2: It is the responsibility of the Media AF in this case to discover and track changes to the PCF instance responsible for the PDU Session supporting the media streaming session at reference point M4 using the discovery services provided by the NRF and/or BSF.

B. If the Media AF is deployed outside the Trusted DN, or if it is more convenient for a Media AF deployed in the Trusted DN to do so, it invokes the Nnef\_AFSessionWithQoS service exposed by the NEF, as specified in clause 4.4.9 of TS 29.522 [29522], to indirectly invoke the PCF at reference point N33.

NOTE 3: Per clause 4.4.9 of TS 29.522 [29522], the Nnef\_AFSession‌With‌QoS service is realised at reference point N33 by the AsSession‌With‌QoS exposure API.

NOTE 4: Configuration of the NEF endpoint address and access credentials in the Media AF in this case is beyond the scope of the present document.

When a Network Assistance session is created by the Media Session Handler (per clauses 4.7.6 and 11.6.4.1), the Media AF shall create an *AF application session context* in the PCF responsible for the PDU Session corresponding to the M4 application flows listed in the NetworkAssistanceSession.‌serviceDataFlow‌Descriptions property.

If no corresponding AF application session context already exists, the 5GMS AF shall use the Npcf\_‌Policy‌Authorization\_‌Create operation at reference point N5 (or, if deployed outside the Trusted DN, the equivalent AsSession‌WithQoS service operation) with the appropriate service information to create and provision a new AF application session context. The information in the AppSessionContext‌ReqData shall be derived from the service data flow descriptions in the Network Assistance session resource, as well as from the referenced Policy Template (if any) and/or the requested QoS.

The AF application session context shall declare exactly one media component per media streaming session. A separate sub-component shall be declared for each M4 application flow listed in the NetworkAssistanceSession.‌serviceDataFlow‌Descriptions array.

For each of the Network Assistance sessions it is managing, the 5GMS AF shall subscribe to the following PCF notifications on the corresponding AF application session context:

- Service Data Flow QoS notification control;

- Service Data Flow deactivation;

- Resources allocation outcome.

When requesting QoS provisioning for a media streaming session, the Media AF shall use the configured Policy Templates of the Provisioning Session to determine the list of the QoS references within altSerReqs. The lowest priority index shall be assigned to the policy template with the lowest QoS requirement, and the highest priority shall be assigned to the requested operation point by the UE (if the UE is allowed to use that operation point).

When a Network Assistance session is subsequently destroyed by the Media Session Handler (per clauses 5.3.4.7 and 11.6.4.6), the Media AF shall destroy the corresponding AF application session context in the relevant PCF instance.

## 5.6 UE modem interactions

### 5.6.1 Overview

Certain features of the Media Delivery System rely on interfaces and APIs that are essentially UE-internal. The interactions between the Media Session Handler and the UE modem to support these features are specified in the following clauses.

### 5.6.2 ANBR-based Network Assistance

If ANBR-based Network Assistance is supported, the Media Session Handler may use an interface to the Medium Access Control entity in the UE modem to send and receive bit rate recommendation messages. This interface may be based on the AT commands +CGBRRREQ and +CGBRRREP as defined in TS 27.007 [27007].

Furthermore, messaging across that interface corresponds to the logical translations of the *Bit Rate Recommendation* and/or *Bit Rate Recommendation Query* messages, carried by the Recommended bit rate MAC CE, exchanged between the RAN Modem and the RAN, as specified in TS 38.321 [38321] for 5G NR and TS 36.321 [36321] for LTE. The association between the LCID for which the recommendation applies and the actual flow (including the intermediate RLC channel) is performed by the modem.

NOTE: The +C5GQOSRDP=? command may be used to obtain a list of CID values that are associated with QoS flows (both network and MT/TE initiated). When used to request a bit rate boost, the query shall not request a bit rate that may exceed the MFBR for the corresponding QoS Flow. Failure to ensure this may result in unexpected congestion-induced packet delays and packet dropping.

The *Bit Rate Recommendation Query* shall indicate the bit rate desired by the application, as described by [38321] and [36321]. This request may be used by the Media Session Handler to request for a temporary increase in bit rate for the corresponding flow ("bit rate boost"). The RAN responds with a Bit Rate Recommendation message that confirms the recommended bit rate after the boost grant. Once the bit rate drops again after a boost grant, the network shall inform the Media Session Handler about the new recommended bit rate by means of an ANBR message.

Whenever the Media Session Handler receives a message from the UE modem corresponding to the logical translation of the *Bit Rate Recommendation* message for the associated RAN uplink or downlink, it shall notify the Media Access Function (via a suitable reference point M11 notification) of the new bit rate recommendation associated with the indicated PDU session.

Furthermore, whenever the Media Session Handler receives a request for a bit rate boost from the Media Access Function (via a suitable reference point M11 method invocation) relating to a PDU session in use for Media Delivery, it may send a bit rate boost message to the UE modem. That bit rate boost request is logically translated by the modem to the *Bit Rate Recommendation Query* message which is then sent to the RAN on the associated RAN uplink or downlink.

It is left to the implementer of the Media Access Function to decide how to best use the bit rate recommendation and the bit rate recommendation query information for individual media delivery sessions.

### 5.6.3 RAN-based metrics reporting

These procedures shall be used by the Media Session Handler to control metrics reporting when such reporting is configured by the OAM via the 5G control plane signalling.

As described in clause L.1 of TS 26.247 [26247], the metrics configuration is delivered to the UE as a container from the OAM via RAN and the Media Session Handler should obtain its metrics configuration , e.g. using the AT Command +CAPPLEVMC or +CAPPLEVMCNR. This configuration may also include virtual reality metrics as specified in clause 9.3 of TS 26.118 [26118]. When a metrics configuration is received, the Media Session Handler shall store this configuration and use it for all subsequent media delivery sessions.

When a media delivery session is started the Media Session Handler shall determine whether metrics from this session shall be reported. The determination shall be based on the *sample percentage*, *slice scope* and *streaming source filter* specified in the stored metrics configuration, according to clause 10.5 of TS 26.247 [26247].

If metrics are to be reported for the session, the Media Session Handler shall request the Media Access Function to create a metrics collection job. The Media Access Function shall return a reference to the created job, which the Media Session Handler shall use in all subsequent actions related to this job.

The Media Session Handler shall configure the metrics collection job with the set of metrics to be collected during the media delivery session. The format of the configuration shall be according to clause L.2 of [26247], but only the metrics attribute in the configuration shall be used for this purpose.

The Media Session Handler shall regularly request the collected metrics from the Media Access Function according to the reportingInterval specified in the metrics configuration. The metrics returned by the Media Access Function shall use the format as described in clause 10.6 of [26247], and (for Virtual Reality media) in clause 9.4.3 of TS 26.118 [26118]. The Media Session Handler should forward these to the UE modem, e.g. using the AT command +CAPPLEVMR or +CAPPLEVMRNR. As a result, the UE modem sends metrics reports to the RAN which are then forwarded to the OAM according to clause L.1 of [26247].

When the media delivery session is finished the Media Session Handler shall destroy the metrics collection job.

# 6 3GPP Service URL

Editor’s Note: General design of 3GPP Service URLs, which may be factored out into its own TS in future.

# 7 General aspects of network APIs

## 7.1 Usage of HTTP

### 7.1.1 HTTP protocol version

Implementations of the Media AF shall expose both HTTP/1.1 [HTTP11] and HTTP/2 [HTTP2] endpoints at reference points M1, M3 and M5, including support for the HTTP/2 starting mechanisms specified in section 3 of RFC 9113 [HTTP2]. In both protocol versions, TLS version 1.3 [TLS13] shall be supported and HTTPS interactions should be used on these interfaces in preference to cleartext HTTP.

- The Media Application Provider may use any supported HTTP protocol version at reference point M1.

- The Media AS may use any supported HTTP protocol version at reference point M3.

- The Media Session Handler may use any supported HTTP protocol version at reference point M5.

All responses from the Media AF that carry a message body shall provide a strong entity tag in the form of an ETag response header and a modification timestamp in the form of a Last-Modified response header.

All endpoints exposed at reference points M1, M3 and M5 shall support the conditional HTTP requests If-None-Match and If-Modified-Since.

### 7.1.2 HTTP endpoint addresses

#### 7.1.2.1 Default Media AF endpoint address at reference point M1

The present document does not specify a default endpoint address for the Maf\_Provisioning service exposed to the Media Application Provider at reference point M1.

#### 7.1.2.2 Default Media AF endpoint address at reference point M3

The present document does not specify a default endpoint address for the Maf\_SessionHandling service exposed to the Media AS at reference point M3.

#### 7.1.2.3 Default Media AF endpoint address at reference point M5

The present document does not specify a default endpoint address for the Maf\_SessionHandling service exposed to the Media Session Handler at reference point M5.

### 7.1.3 HTTP resource URIs and paths

The resource URI used in each HTTP request to the API provider shall have the structure defined in subclause 4.4.1 of TS 29.501 [29501], i.e.:

{apiRoot}/{apiName}/{apiVersion}/{apiSpecificResourceUriPart}

with the following components:

- {apiRoot} shall be set as described in [29501].

- {apiName}shall be set as defined by the following clauses.

- {apiVersion} shall be set to "v1" in this release of the specification.

- {apiSpecificResourceUriPart} shall be set as described in the following clauses.

### 7.1.4 Usage of HTTP headers

#### 7.1.4.1 General

Standard HTTP headers shall be used in accordance with clause 5.2.2 of TS 29.500 [29500] for both HTTP/1.1 and HTTP/2 messages.

#### 7.1.4.2 User Agent identification

Individual specifications referencing the present document shall specify the User-Agent HTTP request header used by the Media Session Handler to identify itself.

#### 7.1.4.3 Server identification

Individual specifications referencing the present document shall specify the Server HTTP response header used by the Media AF to identify itself.

#### 7.1.4.2 Cache control

All responses from the Media AF that carry a resource message body shall include:

- a strong entity tag for the resource, conveyed in an ETag response header as specified in section 8.8.3 of RFC 9110 [HTTPsemantics],

- a resource modification timestamp, conveyed in a Last-Modified response header as specified in section 8.8.2 of [HTTPsemantics], and

- a predicted time-to-live period for the resource, conveyed in a Cache-Control: max-age response header as specified in section 5.2.1.1 of RFC 9111 [HTTPcaching].

#### 7.1.4.3 Support for conditional HTTP GET requests

All API endpoints on the Media AF that expose the HTTP GET method shall support conditional requests using the If-None-Match and If-Modified-Since request headers as specified in section 13 of [HTTPsemantics]. API clients should not attempt to revalidate their cached copy of a resource using a conditional GET request before the indicated time-to-live period has elapsed.

#### 7.1.4.4 Support for conditional HTTP POST, PUT, PATCH and DELETE requests

All API endpoints on the Media AF that expose the HTTP POST, PUT, PATCH or DELETE methods shall support conditional requests using the If-Match request header as specified in section 13.1.1 of RFC 9110 [HTTPsemantics]. The API client should supply a strong entity tag previously obtained per clause 7.1.4.2 in this request header when invoking any of these HTTP methods.

### 7.1.5 HTTP message bodies for API resources

The OpenAPI [OpenAPI300] specification of request and response HTTP messages is contained in annex A.

### 7.1.6 HTTP response codes

Guidelines for error responses to the invocation of APIs of NF services are specified in clause 4.8 of TS 29.501 [29501]. API-specific error responses are specified in the respective clauses of the present document.

### 7.1.7 HTTP error response message bodies

Error messages shall be conveyed to the API client using an HTTP response body of type ProblemDetails, as specified in clause 4.8.2 of TS 29.501 [29501].

## 7.2 Explanation of API data model notation

The data models in the following API clauses are specified using the following notational conventions:

1. Data models are expressed as an unordered list of JSON properties [JSON] with one property defined in each row of the data model table.

2. The *Data type* column defines the type of the property, according to JSON notation [JSON].

3. The keyword "Array" in the *Data type* column indicates that zero or more elements of the data type in brackets are included. The number of elements in the array may additionally be constrained by normative text in the *Description* column.

4. The *Cardinality* column defines whether a property is optional or mandatory. An array with cardinality 0 indicates that the array property is optional in the data structure. An array with cardinality 1 indicates that the property is mandatory in the data structure, even when the array is empty.

5. The keyword "Object" in the *Data type* column indicates a structured sub-object of an unnamed type whose properties are defined inline in the indented table rows immediately afterwards. The "Object" type may be combined with the "Array" type.

6. In the case of data types specifying RESTful resources, the additional *Usage* column defines the property behaviour for each CRUD Operation as follows:

- "C" (Create), "R" (Retrieve) and "U" (Update) refers to the CRUD procedure during which the property is present in the resource type. (A Destroy operation never takes any input data type in the body of the request message, nor does it return any response message body.)

- "RO" signifies a read-only property. Only the API provider function is permitted to modify the property value. Any value supplied by the API invoker in the body of a request message is ignored by the API provider function. The property may be omitted from request message bodies, even if it is a mandatory property of the data type, i.e., the property is only mandatory in response message bodies.

- "WO" signifies a write-only property. Only the API invoker is permitted to modify the property value. The API provider function should not populate this property in the body of any response message returned to the API invoker, even if it is a mandatory property of the data type, i.e., the property is only mandatory in request message bodies.

- "RW" signifies a read/write property. The API provider and API invoker may both modify the property value.

7. An additional read-only property is included at the start of all data models defining resources that are members of a RESTful collection. This property is populated with the unique identifier of the resource within its parent collection, and corresponds to the leaf path element in the RESTful URL of that resource.

## 7.3 Common OpenAPI data types

### 7.3.1 General

The data types defined in this clause are intended to be used by more than one of the Media Delivery APIs.

### 7.3.2 Simple data types

Table 7.3.2-1 below specifies common simple data types used within the Media Delivery APIs, including a short description of each. In cases where types from other specifications are reused, a reference is provided.

Table 7.3.2-1: Simple data types

|  |  |  |  |
| --- | --- | --- | --- |
| Type name | Type definition | Description | Reference |
| Uint6 | integer | Integer where the allowed values correspond to the value range of an unsigned 6-bit integer. | Clause A.2 |
| Uint8 | integer | Integer where the allowed values correspond to the value range of an unsigned 8-bit integer. | Clause A.2 |
| Uint20 | integer | Integer where the allowed values correspond to the value range of an unsigned 20-bit integer. | Clause A.2 |
| ResourceId | string | String chosen by the 5GMS AF to serve as an identifier in a resource URL. | Clause A.2. |
| Percentage | number | A percentage expressed as a floating-point value between 0.0 and 100.0 (inclusive). | Clause A.2. |
| DurationSec | integer | An unsigned integer identifying a period of time expressed in units of seconds. | TS 29.571 [12] table 5.2.2‑1 |
| Duration | string | A period of time expressed as a string compliant with the duration format specified in section 7.3.1 of the JSON Schema specification [JSONSchema]. | Clause A.2.  IETF RFC 3339 [RFC3339] appendix A. |
| DateTime | string | An absolute date and time expressed using the OpenAPI date-time string format. | TS 29.571 [12] table 5.2.2‑1 |
| Uri | string | Uniform Resource Identifier conforming with the URI-reference production of the URI Generic Syntax. | TS 29.571 [12] table 5.2.2‑1 |
| Url | string | Uniform Resource Locator, conforming with the URI Generic Syntax. | RFC 3986 [41] section 4.1 |
| RelativeUrl | string | Relative Uniform Resource Locator, conforming with the relative-ref production of the URI Generic Syntax.  Both query and fragment suffixes are permitted. | RFC 3986 [RFC3986], section 4.2 |
| AbsoluteUrl | string | Absolute Uniform Resource Locator, conforming with the absolute-URI production of the URI Generic Syntax in which the scheme part is http or https.  The query suffix is permitted but the fragment suffix is not. | RFC 3986 [RFC3986], section 4.3 |
| IPv4Addr | string | IPv4 address formatted in "dotted decimal" notation | TS 29.571 [29571] table 5.2.2‑1. |
| IPv6Addr | string | IPv6 address formatted in colon-separated hexadecimal quartet notation. | TS 29.571 [29571] table 5.2.2‑1. |
| Uinteger | integer | Unsigned integer. | TS 29.571 [29571] table 5.2.2‑1. |
| UintegerRm | integer | Unsigned integer (nullable). | TS 29.571 [29571] table 5.2.2‑1. |
| Uint32 | integer | Unsigned integer between 0 and 4294967295 (232 − 1). | TS 29.571 [29571] table 5.2.2‑1. |
| Dnn | string | Data Network Name. | TS 29.571 [29571] table 5.3.2‑1. |
| BitRate | string | A bit rate expressed as a string-encoded decimal value and unit. | TS 29.571 [29571]  table 5.5.2‑1. |
| Media‌Delivery‌Session‌Id | string | A unique identifier for a media delivery session.  This should not contain any user-identifiable data. | Clause A.2. |

### 7.3.3 Structured data types

#### 7.3.3.1 IpPacketFilterSet type

Table 7.3.3.1-1: Definition of type IpPacketFilterSet

|  |  |  |  |
| --- | --- | --- | --- |
| Property name | Data type | Cardinality | Description |
| sourceAddress | IpAddr | 0..1 | Source IP address or IPv6 prefix. |
| destinationAddress | IpAddr | 0..1 | Destination IP address or IPv6 prefix. |
| protocolNumber | Uint8 | 0..1 | Transport layer protocol number as it appears in the Protocol field of the IPv4 packet header or the Next Header field of the IPv6 packet header. |
| sourcePort | Uint16 | 0..1 | Source port number. |
| destinationPort | Uint16 | 0..1 | Destination port number. |
| differentiated‌Services‌Code‌Point | Uint6 | 0..1 | Differentiated Services Code Point. |
| flowLabel | Uint20 | 0..1 | IPv6 Flow Label. |
| security‌Parameters‌Index | Uint32 | 0..1 | IPv6 Security Parameters Index (SPI). |
| direction | string | 1..1 | Packet Filter Set direction. |

#### 7.3.3.2 ServiceDataFlowDescription type

Table 7.3.3.2-1: Definition of type ServiceDataFlowDescription

|  |  |  |  |
| --- | --- | --- | --- |
| Property name | Data type | Cardinality | Description |
| sdfMethod | SdfMethod | 1..1 | The filtering method used to identify packets belonging to this Service Data Flow (see clause 7.3.4.2). |
| flowDescription | IpPacketFilterSet | 0..1 | Service Data Flow Description (see NOTE). |
| domainName | string | 0..1 | FQDN of the Media AS (see NOTE). |
| NOTE: Exactly one of these properties shall be populated. | | | |

#### 7.3.3.3A M1UnidirectionalQoSSpecification type

Table 7.3.3.3A-1: Definition of type M1UnidirectionalQoSSpecification

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property name | Data type | Cardinality | Usage | Description |
| maximumBitRate | BitRate | 1..1 | RO | Maximum bit rate supported by the 5G System.  Populated by the Media AF. |
| maximumAuthorisedBitRate | BitRate | 0..1 | RW | Maximum bit rate authorised by the Media Application Provider. |
| minimumPacketLossRate | Percentage | 0..1 | RW | Minimum packet loss rate permitted by the Media Application Provider, expressed as a floating-point percentage between 0.0 and 100.0. |

#### 7.3.3.3 M1QoSSpecification type

Table 7.3.3.3-1: Definition of type M1QoSSpecification

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property name | Data type | Cardinality | Usage | Description |
| qosReference | string | 0..1 |  | As specified in clause 5.6.2.7 of TS 29.514 [29514]. |
| downlink | M1Unidirectional‌QoS‌Specification | 0..1 |  | QoS specification in the downlink direction. |
| uplink | M1Unidirectional‌QoS‌Specification | 0..1 |  | QoS specification in the uplink direction. |

#### 7.3.3.3A M5BitRateSpecification type

Table 7.3.3.3A-1: Definition of type M5BitRateSpecification

|  |  |  |  |
| --- | --- | --- | --- |
| Property name | Data type | Cardinality | Description |
| maximumRequestedBitRate | BitRate | 1..1 | Maximum requested bit rate. |
| minimumDesiredBitRate | BitRate | 0..1 | Minimum desired bit rate. |
| minimumRequestedBitRate | BitRate | 1..1 | Minimum requested bit rate. |

#### 7.3.3.4 M5QoSSpecification type

Table 7.3.3.4-1: Definition of type M5QoSSpecification

|  |  |  |  |
| --- | --- | --- | --- |
| Property name | Data type | Cardinality | Description |
| downlinkBitRates | M5BitRate‌Specification | 1..1 | Bit rate specification for the downlink direction. |
| uplinkBitRates | M5BitRate‌Specification | 1..1 | Bit rate specification for the uplink direction. |
| desiredPacketLatency | Float | 0..1 | Desired packet latency in milliseconds, expressed as a positive floating-point value. |
| desiredPacketLossRate | Percentage | 0..1 | Desired packet loss rate expressed as a floating-point percentage between 0.0 and 100.0. |

#### 7.3.3.5 ChargingSpecification type

Table 7.3.3.5-1: Definition of type ChargingSpecification

|  |  |  |  |
| --- | --- | --- | --- |
| Property name | Data type | Cardinality | Description |
| sponsorId | SponId | 0..1 | As defined in clause 5.6.2.3 of TS 29.514 [29514]. |
| sponsoringStatus | SponsoringStatus | 0..1 |
| permittedUes | array(Gpsi) | 0..1 | List of UEs permitted to instantiate the parent Policy Template.  If present, the array shall contain at least one member.  If absent, all UEs are permitted. |

#### 7.3.3.6 TypedLocation type

Table 7.3.3.6-1: Definition of TypedLocation type

|  |  |  |  |
| --- | --- | --- | --- |
| Property name | Data type | Cardinality | Description |
| locationIdentifierType | CellIdentifierType | 1..1 | The type of cell location present in the location property. |
| location | string | 1..1 | Identifies the cell location. |

#### 7.3.3.7 OperationSuccessResponse type

Table 7.3.3.7-1: Definition of OperationSuccessResponse type

| Property name | Type | Cardinality | Description |
| --- | --- | --- | --- |
| success | boolean | 1..1 | Indicates whether an operation was successful (TRUE) or not (FALSE). |
| reason | string | 0..1 | Optional explanation of the success or otherwise of the operation. |

#### 7.3.3.8 EdgeProcessingEligibilityCriteria type

Table 7.3.3.8-1: Definition of EdgeProcessingEligibilityCriteria type

| Property name | Type | Cardinality | Description |
| --- | --- | --- | --- |
| service‌DataFlow‌Descriptions | array(Service‌DataFlow‌Description) | 1..1 | A set of Service Data Flow descriptions that are to be used as triggers for invoking edge media processing (see NOTE 1).  If the set is empty, edge media processing may be invoked for an otherwise eligible media stream session on any service data flow.  Valid ServiceDataFlowDescription elements:  - domainName  - flowDescription.destinationAddress and flowDescription.destinationPort  - flowDescription.differentiatedServices  - flowDescription.flowLabel  Other ServiceDataFlowDescription settings shall be rejected by the Media AF. |
| ueLocations | array(Location‌Area5G) | 1..1 | A set of geographical areas in which edge media processing is to be triggered when a UE is present (see NOTE 2).  If the set is empty, edge media processing may be invoked for an otherwise eligible media stream session in any location. |
| timeWindows | array(TimeWindow) | 1..1 | Edge media processing is triggered when the media streaming session is taking place during one of the indicated time windows (see NOTE 2).  If the set is empty, edge media processing may be invoked for an otherwise eligible media stream session at any time. |
| appRequest | boolean | 1..1 | When set TRUE, edge media processing is to be triggered based on application request only. |
| NOTE 1: The usage of these fields to influence route selection and EAS re-selection are for future study.  NOTE 2: Data types LocationArea5G and TimeWindow are defined in TS 24.558 [24558]. | | | |

#### 7.3.3.9 EndpointAddress type

Table 7.3.3.9-1: Definition of EndpointAddress type

| Property name | Type | Cardinality | Description |
| --- | --- | --- | --- |
| domainName | string | 0..1 | Internet domain name of the endpoint. |
| ipv4Addr | Ipv4Addr | 0..1 | IPv4 address of the endpoint. |
| ipv6Addr | Ipv6Addr | 0..1 | IPv6 address of the endpoint. |
| portNumber | Uint16 | 1 | Port number of the endpoint. |
| NOTE: Either domainName or at least one of ipv4Addr or ipv6Addr shall be present. | | | |

#### 7.3.3.10 UnidirectionalQoSSpecification data type

The UnidirectionalQoSSpecification data type describes a network Quality of Service specification for media delivery in one direction.

Table 7.3.3.10‑1: Definition of UnidirectionalQoSSpecification data type

| Property name | Data Type | Cardinality | Description |
| --- | --- | --- | --- |
| maximum‌Requested‌BitRate | BitRate | 1..1 | The maximum requested bit rate. |
| minimum‌Desired‌BitRate | BitRate | 0..1 | The minimum desired bit rate. |
| minimum‌Requested‌BitRate | BitRate | 1..1 | The minimum requested bit rate. |
| desired‌Packet‌Latency | Uinteger | 0..1 | The desired packet latency in milliseconds, expressed as a positive floating-point value. |
| desired‌Packet‌Loss‌Rate | Uinteger | 0..1 | The desired packet loss rate expressed as a floating-point percentage between 0.0 and 100.0. |

#### 7.3.3.11 M1MediaEntryPoint type

Editor's Note: Move common data type into TS26510\_ConnonDataTypes.yaml now it is shared between ContentHostingConfiguration and ContentPublishingConfiguration.

Table 7.3.3.11-1: Definition of type M1MediaEntryPoint

|  |  |  |  |
| --- | --- | --- | --- |
| Property name | Data type | Cardinality | Description |
| relativePath | RelativePath | 1..1 | A relative path (i.e., without a scheme or any leading forward slash characters) to the Media Entry Point document resource.  The semantics are dependent on the value of the contentType property. |
| contentType | string | 1..1 | The MIME content type of this Media Entry Point. |
| profiles | array(Uri) | 0..1 | An optional list of conformance profile identifiers associated with this Media Entry Point, each one expressed as a URI. A profile URI may indicate an interoperability point, for example.  If present, the array shall contain at least one item. |

### 7.3.4 Enumerated data types

Editor's Note: The CacheStatus enumeration is intentionally *not* ported from TS 26.512.

#### 7.3.4.1 CellIdentifierType enumeration

The CellIdentifierType enumeration indicates the type of cell identifier as defined in TS 23.003 [7].

Table 7.3.4.1‑1: Definition of CellIdentifierType enumeration

|  |  |
| --- | --- |
| Enumeration value | Description |
| CGI | Cell Global Identification. |
| ECGI | E-UTRAN Cell Global Identification. |
| NCGI | NR Cell Global Identity. |

#### 7.3.4.2 SdfMethod enumeration

Table 7.3.4.2‑1: Definition of SdfMethod enumeration

|  |  |
| --- | --- |
| Enumeration value | Description |
| 5\_TUPLE | Service Data Flow described by source (Media Access Function) IP address and port number, destination (Media AS) IP address and port number and protocol number.  Wildcard values are not permitted in the Service Data Flow description. |
| 2\_TUPLE | Service Data Flow described by source (Media Access Function) IP address and destination (Media AS) IP address duple. |
| TYPE\_OF\_SERVICE\_MARKING | Service Data Flow described by Type of Service (TOS) marking. |
| FLOW\_LABEL | Service Data Flow described by IPv6 flow label marking. |
| DOMAIN\_NAME | Service Data Flow described by a domain name. |

#### 7.3.4.3 ProvisioningSessionType enumeration

Table 7.3.4.3‑1: Definition of ProvisioningSessionType enumeration

|  |  |
| --- | --- |
| Enumeration value | Description |
| DOWNLINK | Downlink media streaming |
| UPLINK | Uplink media streaming |

#### 7.3.4.4 EASRelocationTolerance enumeration

Table 7.3.4.4‑1: Definition of EASRelocationTolerance enumeration

|  |  |
| --- | --- |
| Enumeration value | Description |
| RELOCATION\_UNAWARE | The application is not aware of any EAS relocation that may happen. Relocation procedures may be executed without any restrictions. |
| RELOCATION\_TOLERANT | The application may tolerate EAS relocation, but requirements for the relocation procedure must be met. An application context may need to be transferred. |
| RELOCATION\_INTOLERANT | The application does not tolerate relocation. |

#### 7.3.4.5 ContentTransferMode enumeration

Table 7.3.4.5‑1: Definition of ContentTransferMode enumeration

|  |  |
| --- | --- |
| Enumeration value | Description |
| PULL | Content is pulled by or from the Media AS. |
| PUSH | Content is pushed into or by the Media AS. |

# 8 Maf\_Provisioning service

## 8.1 Overview

This clause defines the provisioning API used by a Media Application Provider at reference point M1 to configure downlink or uplink Media Delivery services. The corresponding OpenAPI definitions for the Maf\_Provisioning service are specified in clause A.3. A summary of the resource structure is shown in table 8.1‑1 below. The default endpoint address of the Media AF at reference point M1 is specified in clause 7.1.2.1.

Table 8.1‑1: Resource structure of Maf\_Provisioning APIs

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| HTTP request path element hierarchy | Description | Allowed HTTP methods | | | | | Resource | OpenAPI |
| Create | Retrieve | Update | Destroy | Non-RESTful operation | structure definition clause | definition clause |
| provisioning-sessions | Provisioning Sessions collection | POST | GET |  |  |  | 8.2.2 | A.3.1 |
| {provisioningSessionId} | Provisioning Session resource |  | GET |  | DELETE |  |
| content-protocols | Content Protocols resource |  | GET |  |  |  | 8.3.2 | A.3.2 |
| certificates | Server Certificates collection | POST |  |  |  |  | 8.4.2 | A.3.3 |
| {certificateId} | Server Certificate resource |  | GET | PUT | DELETE |  |
| content-preparation-templates | Content Preparation Templates collection | POST |  |  |  |  | 8.5.2 | A.3.4 |
| {contentPreparationTemplateId} | Content Preparation Template resource |  | GET | PUT, PATCH | DELETE |  |
| edge-resources-configurations | Edge Resources Configurations collection | POST |  |  |  |  | 8.6.2 | A.3.5 |
| {edgeResourcesConfigurationId} | Edge Resources Configuration resource |  | GET | PUT, PATCH | DELETE |  |
| policy-templates | Policy Templates collection | POST |  |  |  |  | 8.7.2 | A.3.6 |
| {policyTemplateId} | Policy Template resource |  | GET | PUT, PATCH | DELETE |  |
| content-hosting-configuration | Content Hosting Configuration resource | POST | GET | PUT, PATCH | DELETE |  | 8.8.2 | A.3.7 |
| purge | Content Hosting cache purge operation |  |  |  |  | POST |
| content-publishing-configuration | Content Publishing Configuration resource | POST | GET | PUT, PATCH | DELETE |  | 8.9.2 | A.3.8 |
| purge | Content Publishing cache purge operation |  |  |  |  | POST |
| metrics-reporting-configuration | Metrics Reporting Configuration collection | POST |  |  |  |  | 8.10.2 | A.3.9 |
| {metricsReportingConfigurationId} | Metrics Reporting Configuration resource |  | GET | PUT, PATCH | DELETE |  |
| consumption-reporting-configuration | Consumption Reporting Configuration resource | POST | GET | PUT, PATCH | DELETE |  | 8.11.2 | A.3.10 |
| event-data-processing-configurations | Event Data Processing Configuration collection | POST |  |  |  |  | 8.12.2 | A.3.11 |
| {event‌Data‌Processing‌ConfigurationId} | Event Data Processing Configuration resource |  | GET | PUT, PATCH | DELETE |  |

## 8.2 Provisioning Sessions API

### 8.2.1 Overview

The Provisioning Sessions API is used by the 5GMS Application Provider to instantiate and manipulate Provisioning Sessions in the 5GMS System, as described in clause 5.2.2. Having created a Provisioning Session, the 5GMS Application Provider then goes on to discover the content protocols it supports using the API specified in clause 8.3, and to provision other Media Delivery features in the context of that Provisioning Session, using the APIs specified in clause 8.4 *et seq*. Certain of these features are only applicable to the type of Provisioning Session created.

### 8.2.2 Resource structure

The Provisioning Sessions API is accessible through the following URL base path:

{apiRoot}/3gpp-maf-provisioning/{apiVersion}/provisioning-sessions/

Table 8.2.2‑1 specifies the operations and the corresponding HTTP methods that are supported by this API. In each case, the sub-resource path specified in the second column of the table shall be appended to the above URL base path.

Table 8.2.2‑1: Operations supported by the Provisioning Sessions API

|  |  |  |  |
| --- | --- | --- | --- |
| Operation name | Sub‑resource path | Allowed HTTP method(s) | Description |
| Enumerate Provisioning Sessions |  | GET | Enumerate the resource identifiers of the Provisioning Session collection. |
| Create Provisioning Session |  | POST | Create a new Provisioning Session resource. |
| Retrieve Provisioning Session | {provisioningSessionId} | GET | Retrieve an existing Provisioning Session resource for inspection. |
| Destroy Provisioning Session | DELETE | Destroy an existing Provisioning Session resource. |

### 8.2.3 Data model

#### 8.2.3.1 ProvisioningSession resource

Different properties are present in the ProvisioningSession resource depending on the type of Provisioning Session indicated in the provisioningSessionType property, and this is specified in the *Applicability* column.

Table 8.2.3.1‑1: Definition of ProvisioningSession resource

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Property name | Type | Cardinality | Usage | Description | Applicability |
| provisioningSessionId | ResourceId | 1..1 | C: RO  R: RO U: – | A unique identifier for this Provisioning Session. | All types. |
| provisioningSession‌Type | Provisioning‌Session‌Type | 1..1 | C: RW R: RW U: – | The type of Provisioning Session. | All types. |
| externalServiceId | string | 1..1 | C: RW R: RO  U: RW | An identifier, nominated by the Media Application Provider, that identifies this Provisioning Session to the Media Client. Every Provisioning Session in a Media Delivery System shall have a different service identifier.  Takes the form of a reverse FQDN e.g., com.‌provider.‌service to ensure global applicability across different Media Delivery Systems.  Used by the Media Session Handler to invoke the network media session handling operations specified in clause 5.3 and clause 9, in particular to fetch full Service Access Information from the Media AF (see clauses 5.3.2 and 9.2). | All types. |
| aspId | AspId | 0..1 | C: RW  R: RW U: – | The identity of the Application Service Provider responsible for this Provisioning Session, as specified in clause 5.6.2.3 of TS 29.514 [29514]. | All types. |
| appId | ApplicationId | 1..1 | C: RW R: RW U: – | The Application Identifier (see table 5.4.2‑1 of TS 29.571 [29571]) to which this Provisioning Session pertains.  The same <aspId, ‌appId> duple may be present in several Provisioning Sessions in a given 5GMS System.  Used as the AF Application identifier (see clause 5.6.2.3 of TS 29.514 [29514]) for PCF interactions. When a 5GMS AF in the Trusted DN is provisioned from outside the Trusted DN, the NEF is responsible for mapping an external Application Identifier to the corresponding internal AF Application Identifier known to the PCF. | All types. |
| serverCertificateIds | array(ResourceId) | 0..1 | C: RO  R: RO U: – | A list of Server Certificate identifiers currently associated with this Provisioning Session. | DOWNLINK, UPLINK |
| contentPreparation‌TemplateIds | array(ResourceId) | 0..1 | C: RO  R: RO U: – | A list of Content Preparation Template identifiers currently associated with this Provisioning Session. | DOWNLINK, UPLINK |
| metricsReporting‌ConfigurationIds | array(ResourceId) | 0..1 | C: RO  R: RO U: – | A list of Metrics Reporting Configuration identifiers currently associated with this Provisioning Session. | DOWNLINK, UPLINK |
| policyTemplateIds | array(ResourceId) | 0..1 | C: RO  R: RO U: – | A list of Policy Template identifiers currently associated with this Provisioning Session. | DOWNLINK, UPLINK |
| edgeResources‌ConfigurationIds | array(ResourceId) | 0..1 | C: RO  R: RO U: – | A list of Edge Resources Configuration identifiers currently associated with this Provisioning Session. | DOWNLINK, UPLINK |
| eventDataProcessing‌ConfigurationIds | array(ResourceId) | 0..1 | C: RO  R: RO U: – | A list of Event Data Processing Configuration identifiers currently associated with this Provisioning Session. | DOWNLINK, UPLINK |

## 8.3 Content Protocols Discovery API

### 8.3.1 Overview

The Content Protocols Discovery API is used by a 5GMS Application Provider to find out which content ingest or egest protocols are supported by the Media AS instance(s) associated with a Provisioning Session in the Media AF.

### 8.3.2 Resource structure

The Content Protocols Discovery API is accessible through the following URL base path:

{apiRoot}/3gpp-maf-provisioning/{apiVersion}/provisioning-sessions/{provisioningSessionId}/

Table 8.3.2‑1 below specifies the operations and the corresponding HTTP methods that are supported by this API. In each case, the Provisioning Session identifier shall be substituted into {provisioningSessionId} in the above URL template and the sub-resource path specified in the second column of the table shall be appended to the URL base path.

Table 8.3.2‑1: Operations supported by the Ingest Protocols Discovery API

|  |  |  |  |
| --- | --- | --- | --- |
| Operation name | Sub‑resource path | Allowed HTTP method(s) | Description |
| Fetch list of supported content protocols | content-protocols | GET | Retrieve a list of supported content protocols. |

### 8.3.3 Data model

#### 8.3.3.1 ContentProtocols resource

Table 8.3.3.1-1: Definition of ContentProtocols resource

| Property name | Data Type | Cardinality | Description |
| --- | --- | --- | --- |
| downlinkIngestProtocols | array(Content‌Protocol‌Descriptor) | 0..1 | An array of ContentProtocolDescriptor objects, as specified in clause 8.3.3.2, each one uniquely identifying a content ingest protocol supported at reference point M2 by the Media AS(s) associated with the target Media AF. |
| uplinkEgestProtocols | array(Content‌Protocol‌Descriptor) | 0..1 | An array of ContentProtocolDescriptor objects, as specified in clause 8.3.3.2, each one uniquely identifying a content egest protocol supported at reference point M2 by the Media AS instance(s) associated with the target Media AF. |
| geoFencingLocatorTypes | array(Uri) | 0..1 | An array of fully-qualified term identifiers, each one indicating a content geo-fencing locator type supported at reference point M2 by the Media AS instance(s) associated with the target Media AF. (See clause B.1.) |

#### 8.3.3.2 ContentProtocolDescriptor type

Table 8.2.3.2-1: Definition of ContentProtocolDescriptor type

|  |  |  |  |
| --- | --- | --- | --- |
| Property name | Data Type | Cardinality | Description |
| termIdentifier | Uri | 1..1 | A fully-qualified term identifier indicating support for a content protocol (see NOTE). |
| descriptionLocator | AbsoluteUrl | 0..1 | The location of a description of the content protocol, for example the public web URL of its specification. |
| NOTE: The controlled vocabulary of terms identifying 5G Media Streaming content ingest and content egest protocols at reference point M2 is specified in clause 8 of TS 26.512 [26512]. | | | |

## 8.4 Server Certificates provisioning API

### 8.4.1 Overview

The Server Certificates Provisioning API is used to provision X.509 [X.509] server certificates that can be referenced by a Content Hosting Configuration and subsequently presented by the Media AS when it distributes content to Media Clients at reference point M4 using Transport Layer Security [TLS13]. Server Certificate resources are provisioned within the scope of an enclosing Provisioning Session.

### 8.4.2 Resource structure

The Server Certificates Provisioning API is accessible through the following URL base path:

{apiRoot}/3gpp-maf-provisioning/{apiVersion}/provisioning-sessions/{provisioningSessionId}/

Table 8.4.2‑1 specifies the operations and the corresponding HTTP methods that are supported by this API. In each case, the Provisioning Session identifier shall be substituted into {provisioningSessionId} in the above URL template and the sub-resource path specified in the second column shall be appended to the URL base path.

Table 8.4.2‑1: Operations supported by the Server Certificates Provisioning API

|  |  |  |  |
| --- | --- | --- | --- |
| Operation name | Sub‑resource path | Allowed HTTP method(s) | Description |
| Create Server Certificate | certificates | POST | Invoked on the Server Certificates collection associated with a Provisioning Session to request that the Media AF creates a new Server Certificate on behalf of the Media Application Provider. |
| Reserve Server Certificate | certificates?csr | POST | Invoked on the Server Certificates collection associated with a Provisioning Session to solicit a Certificate Signing Request for a new Server Certificate. |
| Retrieve Server Certificate | certificates/{certificateId} | GET | Used to retrieve a previously created or uploaded Server Certificate. |
| Upload Server Certificate | PUT | Used by the Media Application Provider to supply a new Server Certificate in response to a Certificate Signing Request previously solicited from the Media AF. |
| Destroy Server Certificate | DELETE | Removes the specified Server Certificate from the set of certificates associated with the Provisioning Session. |
| NOTE: The Server Certificate resource identifier {certificateId} may differ from the serial number of the X.509 certificate. | | | |

### 8.4.3 Data model

#### 8.4.3.1 Certificate Signing Request

The Certificate Signing Request shall comply with the Privacy-Enhanced Mail (PEM) textual format specified in RFC 7468 [RFC7468], i.e. a Base64-encoded DER certificate request or certificate, including leading and trailing encapsulation boundary lines.

The MIME content type shall be application/x-pem-file.

#### 8.4.3.2 Server Certificate resource

The Server Certificate resource shall comply with the Privacy-Enhanced Mail (PEM) textual format specified in RFC 7468 [RFC7468], i.e. a Base64-encoded DER certificate, including leading and trailing encapsulation boundary lines. The resource shall include only the public parts of the X.509 certificate. In particular, the private key shall not be included.

The MIME content type shall be application/x-pem-file.

## 8.5 Content Preparation Templates provisioning API

### 8.5.1 Overview

Content Preparation Templates are used to specify manipulations applied by a Media AS to downlink media resources ingested at reference point M2 for distribution at reference point M4, or to uplink media resources contributed at reference point M4 for egest at reference point M2. The Content Preparation Templates Provisioning API is used to provision a Content Preparation Template within the scope of a Provisioning Session that can subsequently be referenced from a Content Hosting Configuration or Content Publishing Configuration.

### 8.5.2 Resource structure

The Content Preparation Templates Provisioning API is accessible through the following URL base path:

{apiRoot}/3gpp-maf-provisioning/{apiVersion}/provisioning-sessions/{provisioningSessionId}/

Table 8.5.2‑1 specifies the operations and the corresponding HTTP methods that are supported by this API. In each case, the Provisioning Session identifier shall be substituted into {provisioningSessionId} in the above URL template and the sub-resource path specified in the second column shall be appended to the URL base path.

Table 8.5.2‑1: Operations supported by the Content Preparation Templates Provisioning API

|  |  |  |  |
| --- | --- | --- | --- |
| Operation name | Sub‑resource path | Allowed HTTP method(s) | Description |
| Create Content Preparation Template | content-preparation-templates | POST | Invoked on a Content Preparation Templates collection when supplying a new Content Preparation Template resource. |
| Retrieve Content Preparation Template | content‑preparation‑templates/‌{contentPreparationTemplateId} | GET | Retrieve a specific Content Preparation Template resource. |
| Update Content Preparation Template | PUT, PATCH | Modify an existing Content Preparation Template resource. |
| Destroy Content Preparation Template | DELETE | Destroy an existing Content Preparation Template resource. |

### 8.5.3 Data model

The data model of the Content Preparation Template resource shall be determined by its MIME content type.

## 8.6 Edge Resources provisioning API

### 8.6.1 General

The Edge Resources Provisioning API is used by the Media Application Provider to provision edge resource usage for media streaming sessions associated with the parent Provisioning Session. The information serves as a template to select or instantiate the appropriate Media AS EAS instance that will serve the media session to the UE.

### 8.6.2 Resource structure

The Edge Resources API is accessible through the following URL base path:

{apiRoot}/3gpp-maf-provisioning/{apiVersion}/provisioning-sessions/{provisioningSessionId}/

Table 8.6.2-1 specifies the operations and the corresponding HTTP methods that are supported by the Edge Resources API. In each case, the Provisioning Session identifier shall be substituted into {provisioningSessionId} in the above URL template and the sub-resource path indicated by the second column of the table shall be appended to the resulting URL base path.

Table 8.6.2-1: Operations supported by the Edge Resources API

|  |  |  |  |
| --- | --- | --- | --- |
| Operation name | Sub‑resource path | Allowed HTTP method(s) | Description |
| Configure Edge Resources | edge-resources-configurations | POST | Invoked on the Edge Resources Configurations collection to create a new Edge Resources Configuration resource. |
| Retrieve Edge Resources Configuration | edge-resources-configurations/‌{edgeResourcesConfigurationId} | GET | Retrieve a specific Edge Resources Configuration resource. |
| Modify Edge Resources Configuration | PUT, PATCH | Modify or replace an existing Edge Resources Configuration resource. |
| Destroy Edge Resources Configuration | DELETE | Destroy an existing Edge Resources Configuration resource. |

### 8.6.3 Data model

#### 8.6.3.1 EdgeResourcesConfiguration resource type

Table 8.6.3.1-1: Definition of EdgeResourcesConfiguration resource type

| Property name | Type | Cardinality | Description |
| --- | --- | --- | --- |
| edgeResourcesConfigurationId | ResourceId | 1..1 | A resource identifier for this Edge Resources Configuration that is unique within the scope of the enclosing Provisioning Session. |
| edgeManagementMode | Edge‌Management‌Mode | 1..1 | Indicates whether the management of edge resources is client-driven or AF-driven. (See clause 8.6.3.2.) |
| eligibilityCriteria | Edge‌Processing‌Eligibility‌Criteria‌ | 0..1 | Condition to activate edge resources for this Provisioning Session. If the activationTrigger property of the object is not present, it shall be assumed that all media delivery sessions related to the parent Provisioning Session use edge resources. (See clause 7.3.3.8.) |
| easRequirements | EASRequirements | 1..1 | Requirements on the EAS Profile used by the Media AF or by the EEC to discover and select one or more Media EAS instances to serve media streaming sessions. (See clause 8.6.3.3.) |
| eas‌Relocation‌Requirements | M1EAS‌Relocation‌Requirements | 0..1 | EAS relocation tolerance and requirements.  If not present, the Media AF shall assume that the application is unaware of context transfer and that transfers to a target Media EAS are allowed. (See clause 8.6.3.4.) |

#### 8.6.3.2 EdgeManagementMode enumeration

Table 8.6.3.2‑1: Definition of EdgeManagementMode enumeration

|  |  |
| --- | --- |
| Enumeration value | Description |
| EM\_AF\_DRIVEN | The Media AF, in coordination with the Media Session Handler, assigns edge resources and directs application traffic to the Media EAS instance transparently to the application running on the UE. |
| EM\_CLIENT\_DRIVEN | An Application Client running on the UE explicitly manages edge resources via the EES at reference point EDGE‑1. |

#### 8.6.3.3 EASRequirements type

Table 8.6.3.3-1: Definition of EASRequirements type

|  |  |  |  |
| --- | --- | --- | --- |
| Property name | Type | Cardinality | Description |
| easProviderIds | array(string) | 0..1 | The set of acceptable providers of Media EAS instances associated with this Provisioning Session.  If empty, EAS instances from any provider are acceptable. |
| easId | string | 0..1 | The Application Identifier (e.g., in the form of a URI or Fully-Qualified Domain Name) of a set of EAS instances, or of a particular EAS instance associated with this Provisioning Session. |
| easType | string | 0..1 | The type of Media EAS instances associated with this Provisioning Session. |
| easFeatures | array(string) | 0..1 | Media EAS service features required to be supported by EAS instances associated with this Provisioning Session.  If empty, Media EAS instances of the specified easType with any feature set are acceptable. |
| serviceKpi | EASServiceKPI | 0..1 | Media AS service characteristics required to be satisfied by EAS instances associated with this Provisioning Session.  If omitted, Media EAS instances with any service characteristics are acceptable. |
| serviceArea | Geographical‌Service‌Area | 0..1 | The list of geographical areas that Media EAS instances associated with this Provisioning Session are required to serve.  If omitted, Media EAS instances shall serve all geographical areas whenever possible. |
| service‌Availability‌Schedule | array(Scheduled‌Communication‌Time) | 0..1 | The required availability schedule for Media EAS instances associated with this Provisioning Session.  If omitted, Media EAS instances are required to be available at all times. |
| service‌Continuity‌Scenarios | array(ACRScenario) | 0..1 | The Application Context Relocation scenarios that Media EAS instances associated with this Provisioning Session are required to support for service continuity.  If omitted Media EAS instances are not required to support service continuity across EAS relocation. |
| NOTE: Data types ScheduledCommunicationTime, GeographicalServiceArea, EASServiceKPI, and ACRScenario are defined in TS 29.558 [29558]. | | | |

#### 8.6.3.4 M1EASRelocationRequirements type

Table 8.6.3.4-1: Definition of M1EASRelocationRequirements type

| Property name | Type | Cardinality | Description |
| --- | --- | --- | --- |
| tolerance | EAS‌Relocation‌Tolerance | 1..1 | Indicates whether the Media EAS instance tolerates Application Context Relocation. (See clause 7.3.4.4.)  If set to RELOCATION\_INTOLERANT, the other properties in this data type shall be ignored. |
| max‌Interruption‌Duration | UintegerRm | 0..1 | The maximum downtime (expressed in milliseconds) that an application can tolerate during Media EAS relocation.  If the expected downtime of the application is expected to exceed this duration, relocation of the Media EAS instance shall not be performed. |
| maxResponseTime‌Difference | UintegerRm | 0..1 | The maximum allowed difference between the previously experienced average User Plane network latency to the source Media EAS instance and the expected latency to the target Media EAS instance, expressed in milliseconds. |

## 8.7 Policy Templates provisioning API

### 8.7.1 Overview

The Policy Templates Provisioning API allows a Media Application Provider to configure a set of Policy Templates within the scope of a Provisioning Session that may subsequently be applied to downlink or uplink media delivery sessions belonging to that Media Application Provider using the Dynamic Policy API specified in clause 9.3. A Policy Template is used to specify the traffic shaping and charging policies to be applied to these media streaming sessions, as specified in clause 5.2.7.1.

### 8.7.2 Resource structure

The Policy Templates Provisioning API is accessible through the following URL base path:

{apiRoot}/3gpp-maf-provisioning/{apiVersion}/provisioning-sessions/{provisioningSessionId}/

Table 8.7.2‑1 below specifies the operations and the corresponding HTTP methods that are supported by this API. In each case, the Provisioning Session identifier shall be substituted into {provisioningSessionId} in the above URL template and the sub-resource path specified in the second column shall be appended to the URL base path.

Table 8.7.2‑1: Operations supported by the Policy Template Provisioning API

|  |  |  |  |
| --- | --- | --- | --- |
| Operation name | Sub‑resource path | Allowed HTTP method(s) | Description |
| Create Policy Template | policy-templates | POST | Create a new Policy Template resource within the scope of a Provisioning Session. |
| Fetch Policy Template | policy-templates/‌{policyTemplateId} | GET | Retrieve an existing Policy Template resource. |
| Update Policy Template | PUT, PATCH | Modify the configuration of an existing Policy Template. |
| Destroy Policy Template | DELETE | Destroy an existing Policy Template resource. |

### 8.7.3 Data model

#### 8.7.3.1 PolicyTemplate resource

Table 8.7.3.1-1: Definition of PolicyTemplate resource

| Property | | Type | Cardinality | Usage | Description |
| --- | --- | --- | --- | --- | --- |
| policyTemplateId | | ResourceId | 1..1 | C: RO R: RO U: RO | Resource identifier of this Policy Template assigned by the Media AF that is unique within the scope of the Provisioning Session. |
| state | | string enum | 1..1 | C: RO R: RO U: RO | Current state of this Policy Template (see clause 5.2.7.2) exposed to the 5GMS Application Provider by the Media AF.  Only a Policy Template in the READY state may be instantiated as a Dynamic Policy Instance and applied to media streaming sessions. |
| stateReason | | Problem‌Details | 1..1 | C: RO R: RO U: RO | Additional details about the current state of this Policy Template exposed to the Media Application Provider by the Media AF.  The instance sub-property shall be present and shall indicate the URL of this Policy Template resource at reference point M1.  The title sub-property shall be present and shall indicate a human-readable representation of the state property specified above, e.g., "Policy Template ready for use" or "Policy Template invalid".  The detail sub-property shall be present and shall indicate a human-readable status/error message.  All other properties shall be omitted. |
| externalReference | | string | 1..1 | C: RW R: RW U: RW | Additional identifier for this Policy Template, unique within the scope of its Provisioning Session, that may be cross-referenced with external metadata about a media delivery session.  Example: "HD\_Premium". |
| application‌Session‌Contexts | | array(object) | 0..1 | C: RW R: RW U: RW | Exactly one application session context at reference point M4 to which this Policy Template may be applied.  Each object in the array shall specify at least one property. If more than one property is specified, instantiation of the Policy Template is restricted to the conjunction of all the object's properties. |
|  | sliceInfo | Snssai | 0..1 | C: RW R: RW  U: RW | A Network Slice on which this Policy Template may be instantiated. See clause 5.4.4.2 of TS 29.571 [29571]. |
|  | dnn | Dnn | 0..1 | C: RW R: RW  U: RW | A Data Network on which this Policy Template may be instantiated. (See clause 7.3.2.) |
| qoSSpecification | | M1‌QoS‌Specification | 0..1 | C: RW R: RW U: RW | The network Quality of Service policy to be applied to media delivery sessions that instantiate this Policy Template (see NOTE and clause 7.3.3.3). |
| charging‌Specification | | Charging‌Specification | 0..1 | C: RW R: RW  U: RW | The charging policy to be applied to media delivery sessions that instantiate this Policy Template is instantiated (see NOTE). |
| NOTE: At least one of qoSSpecification and charging‌Specification shall be present. | | | | | |

## 8.8 Content Hosting provisioning API

### 8.8.1 Overview

This clause specifies the API that a Media Application Provider uses by interacting with a Media AF at reference point M1 to provision and manage Media AS Content Hosting Configurations for downlink media delivery. Each such configuration is represented by a ContentHostingConfiguration, the data model for which is specified in clause 8.8.3 below. The RESTful resources for managing Content Hosting Configurations are specified in clause 8.8.2 and the operations on these resources are further elaborated in clause 5.2.8.

### 8.8.2 Resource structure

The Content Hosting Provisioning API is accessible through this URL base path:

{apiRoot}/3gpp-maf-provisioning/{apiVersion}/provisioning-sessions/{provisioningSessionId}/

Table 8.8.2-1 below specifies the operations and the corresponding HTTP methods that are supported by this API. In each case, the Provisioning Session identifier shall be substituted into {provisioningSessionId} in the above URL template and the sub-resource path specified in the second column shall be appended to the URL base path.

Table 8.8.2‑1: Operations supported by the Content Hosting Provisioning API

|  |  |  |  |
| --- | --- | --- | --- |
| Operation name | Sub‑resource path | Allowed HTTP method(s) | Description |
| Create Content Hosting Configuration | content-hosting-configuration | POST | Create the Content Hosting Configuration resource within the context of a parent Provisioning Session. |
| Retrieve Content Hosting Configuration | GET | Retrieve an existing Content Hosting Configuration resource. |
| Update Content Hosting Configuration | PUT, PATCH | Modify an existing Content Hosting Configuration resource. |
| Destroy Content Hosting Configuration | DELETE | Destroy an existing Content Hosting Configuration resource. |
| Purge Content Hosting Configuration cache | content-hosting-configuration/purge | POST | Invalidate some or all cached media resources associated with the specified Content Hosting Configuration. |

### 8.8.3 Data model

#### 8.8.3.1 ContentHostingConfiguration resource

Table 8.8.3.1-1: Definition of ContentHostingConfiguration resource

| Property name | | | | Data Type | Cardinality | Description |
| --- | --- | --- | --- | --- | --- | --- |
| name | | | | string | 1..1 | A name for this Content Hosting Configuration. |
| ingestConfiguration | | | | object | 1..1 | Parameters for ingesting media content into the Media AS at reference point M2. |
|  | mode | | | Content‌Transfer‌Mode | 1..1 | Indicates whether media content is pulled by the Media AS from the Media Application Provider's origin server or pushed into the Media AS by the Media Application Provider (see clause 7.3.4.5). |
|  | protocol | | | Uri | 1..1 | A fully-qualified term identifier URL that identifies the content ingest protocol.  The controlled vocabulary of content ingest protocols is not specified in the present document. |
|  | baseURL | | | AbsoluteUrl | 0..1 | A base URL (i.e., one that includes a scheme, authority and, optionally, path segments) from which content is ingested at reference point M2 for this ingest configuration.  In the case of Pull-based content ingest (method is set to PULL), the base URL shall be provided to the Media AF to indicate the location from which content is to be pulled. A request received at reference point M4 is mapped by the Media AS to a URL at reference point M2 whose base is the value of this property.  In the case of Push-based content ingest (method is set to PUSH), this property shall be populated by the Media AF and returned to the Media Application Provider to indicate the base URL to which content for this Content Hosting Configuration is to be published. |
| distributionConfigurations | | | | array(Object) | 1..1 | Specifies the distribution method and configuration for the ingested content.  More than one distribution may be configured for the ingested content, e.g. to offer different distribution configurations such as DASH and HLS. |
|  | supplementary‌Distribution‌Networks | | | array(<Distribution‌NetworkType, DistributionMode> | 0..1 | Indicates that the content for this distribution configuration is to be distributed via one of more supplementary networks. Each member of the array is a duple mapping a type of distribution network to a mode of distribution.  The same DistributionNetworkType value shall appear at most once in this array. |
|  | edgeResources‌ConfigurationId | | | ResourceId | 0..1 | A reference to an Edge Resources Configuration resource (see clause 8.6.2).  When present, indicates that the Media AS supporting this content distribution shall be realised as a set of one or more EAS instances. |
|  | content‌Preparation‌TemplateId | | | ResourceId | 0..1 | A reference to a Content Preparation Template resource (see clause 8.5.2).  Indicates that content preparation prior to distribution is required by the Media Application Provider. |
|  | certificateId | | | ResourceId | 0..1 | A reference to a Server Certificate resource (see clause 8.4.3.2).  When content is distributed using TLS [TLS13], the referenced X.509 [X509] certificate for the origin domain is presented by the Media AS in the TLS handshake at reference point M4. This attribute indicates the identifier of the certificate to use. |
|  | canonical‌Domain‌Name | | | string | 1..1 | All resources exposed at reference point M4 shall be accessible through this default Fully-Qualified Domain Name assigned by the Media AF. |
|  | domainNameAlias | | | string | 0..1 | The Media Application Provider may assign another Fully-Qualified Domain Name (FQDN) through which media resources within the scope of this distribution configuration are additionally accessible from the Media AS at reference point M4.  This domain name is used by the Media AS to set appropriate CORS HTTP response headers at reference point M4.  If this property is present, the Media Application Provider is responsible for providing in the DNS a CNAME record that resolves domainNameAlias to canonical‌Domain‌Name.  If the certificateId property is also present in this distribution configuration, the provided domain name alias shall match one of the subjectAltName extension fields in the referenced Server Certificate resource, allowing for wildcard matching. |
|  | baseURL | | | AbsoluteUrl | 1..1 | A base URL (i.e., one that includes a scheme, authority and, optionally, path segments) from which content is made available to Media Clients at reference point M4 for this distribution configuration.  The value is chosen by the Media AF when the Content Hosting Configuration is provisioned. It is an error for the Media Application Provider to set this. |
|  | entryPoint | | | M1‌Media‌Entry‌Point | 0..1 | The Media Entry Point nominated by the Media Application Provider for this distribution configuration when it is used to describe a single content item.  Omitted when this distribution configuration describes multiple content items. |
|  |  | relativePath | | RelativeUrl | 1..1 | A relative path (i.e., without a scheme or any leading forward slash characters) to the Media Entry Point document resource. The semantics are dependent on the value of ingestConfiguration.protocol.  The path shall be valid at reference point M2 when appended to the ingest base URL and at reference point M4 when appended to the distribution base URL. |
|  |  | contentType | | string | 1..1 | The MIME content type of the Media Entry Point.  Used by the Media Client to select a Media Entry Point. |
|  |  | profiles | | array(Uri) | 0..1 | An optional list of conformance profile identifiers associated with the Media Entry Point, each one expressed as a URI. A profile URI may indicate an interoperability point, for example.  Used by the Media Client to select a Media Entry Point.  If present, the array shall contain at least one item. |
|  | pathRewriteRules | | | array(object) | 0..1 | An ordered list of rules for rewriting the request URL paths of media resource requests handled by the Media AS at reference point M4 and translating them to URL paths at reference point M2.  If multiple rules match a particular resource’s path, only the first matching rule, in order of appearance in this array, shall be applied. |
|  |  | requestPathPattern | | string | 1..1 | A regular expression [ECMA262] against which the path part of each Media AS request URL, including the leading “/”, and up to and including the final “/”, shall be compared. (Any leaf path element following the final “/” shall be excluded from this comparison.)  In the case of Pull-based content ingest, the M4 download request path is used in the comparison.  In the case of Push-based content ingest, the M2 upload request path is used in the comparison.  In either case, if the request path matches this pattern, the path mapping specified in the corresponding mappedPath shall be applied. |
|  |  | mappedPath | | string | 1..1 | A replacement for the portion of the Media AS request path that matches requestPathPattern.  In the case of Pull-based content ingest, ingestConfiguration.entryPoint is concatenated with the mapped path and any leaf path element from the original M4 download request to form the M2 origin request URL.  In the case of Push-based content ingest, canonical‌Domain‌Name (and, optionally, domain‌Name‌Alias) are concatenated with the mapped path and any leaf path element from the original M2 upload request to form the distribution URL(s) exposed over reference point M4. |
|  | cachingConfigurations | | | array(object) | 0..1 | Defines a configuration of the Media AS content cache for a matching subset of media resources ingested in relation to this Content Hosting Configuration. |
|  |  | urlPatternFilter | | string | 1..1 | A pattern used to match media resource URLs at reference point M2 to determine whether a given media resource ingested by the Media AS is eligible to be cached by it. The format of the pattern shall be a regular expression as specified in [ECMA262]. |
|  |  | cachingDirectives | | object | 1..1 | If a urlPatternFilter applies to a resource, then the provided cachingDirectives shall be applied by the Media AS at reference point M4, potentially overwriting any origin caching directives provided by the Media Application Provider when that resource is ingested at reference point M2. |
|  |  |  | statusCodeFilters | array(integer) | 0..1 | The set of HTTP origin response status codes at reference point M2 to which these cachingDirectives apply.  If the property is present, the set shall contain at least one item.  If absent, the enclosing cachingDirectives shall apply to all HTTP origin response status codes. |
|  |  |  | noCache | boolean | 1..1 | If set to True, indicates that the media resources matching the filters shall not be cached by the Media AS and shall be marked by the Media AS as not to be cached when it servers such media resources at reference point M4. |
|  |  |  | maxAge | Uint32 | 0..1 | The caching time-to-live period that shall be set on ingested media resources matching the filters. This determines the minimum period for which the Media AS shall cache matching media resources as well as the time-to-live period signalled by the Media AS at reference point M4 when it serves such media resources.  The time-to-live for a given media resource shall be calculated relative to the time it was ingested. |
|  | geoFencing | | | object | 0..1 | Directives limiting access to the content to the indicated geographic areas (see NOTE 1). |
|  |  | locatorType | | Uri | 1..1 | The type of the members of the locators array shall be indicated using a fully-qualified term identifier URI from the controlled vocabulary specified in clause B.1, or else from a vendor-specific vocabulary. |
|  |  | locators | | array(string) | 1..1 | Array of locators from which access to the resources is to be allowed. The format of the locator strings shall be determined by the semantics of the term identifier indicated in locatorType. |
|  | urlSignature | | | object | 0..1 | Defines the URL signing scheme to be enforced by the Media AS at reference point M4 (see NOTE 2). When present, only correctly signed and valid URLs are permitted to access the content resources within the scope of the enclosing distribution configuration. |
|  |  | urlPattern | | string | 1..1 | A pattern that shall be used by the Media AS to match M4 media resource request URLs. The Media AS shall not serve a matching media resource at reference point M4 unless it includes a valid authentication token calculated over the portion of the M4 request URL that matches this pattern. The format of the pattern shall be a regular expression as specified in [ECMA262]. |
|  |  | tokenName | | string | 1..1 | The name of the query parameter that the Media Access Function shall use to present the authentication token in the M4 request URL when required to do so. |
|  |  | passphraseName | | string | 1..1 | The name of the token parameter to be used to refer to the passphrase when constructing the M4 authentication token. |
|  |  | passphrase | | string | 1..1 | A string of between 6 and 50 characters to be used as the shared secret between the Media Application Provider and the Media AS for this distributionConfiguration.  (This secret is used in the computation and verification of the M4 authentication token but is never sent in the cleartext part of the M4 request URL.) |
|  |  | tokenExpiryName | | string | 1..1 | The name of the token parameter to be used to refer to the token expiry time point when constructing the M4 authentication token.  The name of the query parameter that the Media Access Function shall use to present the token expiry time point in the cleartext part of the M4 request URL. |
|  |  | useIPAddress | | boolean | 1..1 | If set to True, the IP address of the Media Access Function is included in the computation of the authentication token for resources that match urlPattern and access to matching media resources shall be allowed by the Media AF only when the M4 request is made from this IP address. |
|  |  | ipAddressName | | string | 0..1 | The name of the token parameter that is encoded as part of the M4 authentication token if the useIPAddress flag is set to True.  (The IP address is not passed in the cleartext part of the M4 request URL.) |
| NOTE 1: The geofencing feature used to restrict content requests to the Media AS at reference point M4 is specified in clause 7.6.4.6 of TS 26.512 [26512].  NOTE 2: The format of the authentication token used to sign content requests to the Media AS at reference point M4 is specified in clause 7.6.4.5 of TS 26.512 [26512]. | | | | | | |

#### 8.8.3.2 DistributionNetworkType enumeration

Table 8.8.3.2‑1: Definition of DistributionNetworkType enumeration

|  |  |
| --- | --- |
| Enumeration value | Description |
| DISTRIBUTION\_NETWORK\_EMBMS | Downlink media streaming via eMBMS. |
| DISTRIBUTION\_NETWORK\_MBS | Downlink media streaming via MBS. |

#### 8.8.3.3 DistributionMode enumeration

Table 8.8.3.3‑1: Definition of DistributionMode enumeration

|  |  |
| --- | --- |
| Enumeration value | Description |
| MODE\_EXCLUSIVE | Content ingested by the Media AS is distributed exclusively via a supplementary network and is not available at reference point M4. |
| MODE\_HYBRID | Content ingested by the Media AS is available at reference point M4 and is additionally distributed via a supplementary network. |
| MODE\_DYNAMIC | Content ingested by the Media AS is available at reference point M4 and is additionally distributed via a supplementary network only when reported client demand exceeds a configured threshold. |

## 8.9 Content Publishing provisioning API

### 8.9.1 Overview

This clause specifies the API that a Media Application Provider uses with a Media AF at reference point M1 to provision and manage Media AS Content Publishing Configurations for uplink media delivery. Each such configuration is represented by a ContentPublishingConfiguration, the data model for which is specified in clause 8.9.3 below. The RESTful resources for managing Content Publishing Configurations are specified in clause 8.9.2 and the operations on these resources are further elaborated in clause 5.2.9.

### 8.9.2 Resource structure

The Content Publishing Provisioning API is accessible through this URL base path:

{apiRoot}/3gpp-maf-provisioning/{apiVersion}/provisioning-sessions/{provisioningSessionId}/

Table 8.9.2-1 below specifies the operations and the corresponding HTTP methods that are supported by this API. In each case, the Provisioning Session identifier shall be substituted into {provisioningSessionId} in the above URL template and the sub-resource path specified in the second column shall be appended to the URL base path.

Table 8.9.2‑1: Operations supported by the Content Publishing Provisioning API

|  |  |  |  |
| --- | --- | --- | --- |
| Operation | Sub‑resource path | Allowed HTTP method(s) | Description |
| Create Content Publishing Configuration | content-publishing-configuration | POST | Create the Content Publishing Configuration resource within the context of a parent Provisioning Session. |
| Retrieve Content Publishing Configuration | GET | Retrieve an existing Content Publishing Configuration resource. |
| Update Content Publishing Configuration | PUT,  PATCH | Modify an existing Content Publishing Configuration resource. |
| Destroy Content Publishing Configuration | DELETE | Destroy an existing Content Publishing Configuration resource. |
| Purge Content Publishing Configuration cache | content-publishing-configuration/purge | POST | Invalidate some or all cached media resources associated with the specified Content Publishing Configuration. Applicable to pull-based content egest only. |

### 8.9.3 Data model

#### 8.9.3.1 ContentPublishingConfiguration resource

Table 8.9.3.1-1: Definition of ContentPublishingConfiguration resource

| Property name | | | | Data type | Cardinality | Description |
| --- | --- | --- | --- | --- | --- | --- |
| name | | | | string | 1..1 | A name for this Content Publishing Configuration. |
| contribution‌Configurations | | | | array(object) | 1..1 | Specifies the Media Entry Point and content preparation required for the egested content.  More than one contribution may be configured. |
|  | edgeResources‌ConfigurationId | | | ResourceId | 0..1 | A reference to an Edge Resources Configuration resource (see clause 8.6.2).  When present, indicates that the Media AS supporting this content contribution shall be realised as a set of one or more EAS instances. |
|  | content‌Preparation‌TemplateId | | | ResourceId | 0..1 | A reference to a Content Preparation Template resource (see clause 8.5.2).  Indicates that content preparation prior to egest is required by the Media Application Provider. |
|  | certificateId | | | string | 0..1 | A reference to a Server Certificate resource (see clause 8.4.3.2).  When content is contributed using TLS [TLS13], the referenced X.509 [X509] certificate for the origin domain is presented by the Media AS in the TLS handshake at reference point M4. This attribute indicates the identifier of the certificate to use. |
|  | canonical‌Domain‌Name | | | string | 1..1 | All resources exposed at reference point M4 shall be accessible through this default Fully-Qualified Domain Name assigned by the Media AF. |
|  | domainNameAlias | | | string | 0..1 | The Media Application Provider may assign another Fully-Qualified Domain Name (FQDN) through which media resources within the scope of this contribution configuration are additionally accessible from the Media AS at reference point M4.  This domain name is used by the Media AS to set appropriate CORS HTTP response headers at reference point M4.  If this property is present, the Media Application Provider is responsible for providing in the DNS a CNAME record that resolves domainNameAlias to canonicalDomainName.  If the certificateId property is also present in this contribution configuration, the provided domain name alias shall match one of the subjectAltName extension fields in the referenced Server Certificate resource, allowing for wildcard matching. |
|  | baseURL | | | AbsoluteUrl | 0..1 | A base URL (i.e. one that includes a scheme, authority, and, optionally, path segments) to which content is contributed by Media Clients at reference point M4 for this contribution configuration.  Nominated by the Media AF when the Content Publishing Configuration is provisioned. It is an error for the Media Application Provider to set this. |
|  | entryPoint | | | M1‌Media‌Entry‌Point | 1..1 | The Media Entry Point nominated by the Media Application Provider for this contribution configuration. |
|  |  | relativePath | | Relative‌Url | 1..1 | A relative path (i.e., without a scheme or any leading forward slash characters) to the Media Entry Point document resource. The semantics are dependent on the value of the contentType property.  Nominated by the Media AF. |
|  |  | contentType | | string | 1..1 | The MIME content type of this Media Entry Point.  Used by the Media Client to select a contribution configuration.  Nominated by the Media Application Provider. |
|  |  | profiles | | array(Uri) | 0..1 | An optional list of conformance profile identifiers associated with this Media Entry Point, each one expressed as a URI. A profile URI may indicate an interoperability point, for example.  Used by the Media Client to select a contribution configuration.  Nominated by the Media Application Provider and, if present, the array shall contain at least one item. |
| egestConfiguration | | | | object | 1..1 | Parameters for egesting media content from the Media AS at reference point M2. |
|  | mode | | | Content‌Transfer‌Mode | 1..1 | Indicates whether content is pulled from the Media AS by the Media Application Provider or pushed to the Media Application Provider by the Media AS (see clause 7.3.4.5).  Nominated by the Media Application Provider. |
|  | protocol | | | Uri | 1..1 | A fully-qualified term identifier URI that identifies the content egest protocol.  Nominated by the Media Application Provider.  The controlled vocabulary of content egest protocols is not specified in the present document. |
|  | baseURL | | | Absolute‌URL | 0..1 | A base URL (i.e., one that includes a scheme, authority, and, optionally, path segments) to which content is published at reference point M2 for this publishing configuration.  In the case of Pull-based content egest (*method* is set to *PULL*), this property shall be populated by the Media AF to indicate the location on the Media AS from which content is to be pulled. An uplink media streaming request received at reference point M4 is mapped by the Media AS to a URL at reference point M2 whose base is the value of this property.  In the case of Push-based content egest (*method* is set to PUSH), this property shall be provided to the Media AF and indicates the base URL to which content for this Content Publishing Configuration is to be published. |
|  | entryPoint | | | M1‌Media‌Entry‌Point | 0..1 | The Media Entry Point for content egest used by the Media Application Provider at reference point M2.  In the case of Pull-based content egest (*method* is set to PULL), this object shall be provided by the Media AF.  In the case of Push-based content egest (*method* is set to PUSH), this object may be provided by the Media Application Provider.  The semantics of the entry point are dependent on the value of the contentType property. |
|  |  | relativePath | | Relative‌URL | 1..1 | A relative path (i.e., without a scheme or any leading forward slash characters) to the Media Entry Point document resource.  Nominated by the Media AF for Pull-based content egest.  Nominated by the Media Application Provider for Push-based content egest. |
|  |  | contentType | | string | 1..1 | The MIME content type of this Media Entry Point.  Nominated by the Media Application Provider. |
|  |  | profiles | | array(Uri) | 0..1 | An optional list of conformance profile identifiers associated with this Media Entry Point, each one expressed as a URI. A profile URI may indicate an interoperability point, for example.  Nominated by the Media Application Provider and, if present, the array shall contain at least one item. |
|  | cachingConfigurations | | | array(object) | 0..1 | Defines a configuration of the Media AS cache for a matching subset of media resources intended for pull-based egest at reference point M2 in relation to this Content Publishing Configuration.  Applicable only for Pull-based content egest (*method* is set to PULL). For Push-based egest (*method* is set to PUSH), this property shall not be present.  Nominated by the Media Application Provider. |
|  |  | urlPatternFilter | | string | 1..1 | A pattern used to match media resource URLs to determine whether a given media resource is eligible for caching by the Media AS. The format of the pattern shall be a regular expression as specified in [ECMA262]. |
|  |  | cachingDirectives | | object | 1..1 | If a urlPatternFilter applies to a resource, then the provided cachingDirectives shall be applied by the Media AS at reference point M2.  Any caching directives set by the Media Streamer on content contributed at reference point M4 which define a shorter lifetime for the content shall take precedence over these parameters. |
|  |  |  | noCache | boolean | 1..1 | If set to True, this indicates that the media resources matching the filters shall not be cached by the Media AS and shall be marked by the Media AS as not to be cached when it serves such media resources at reference point M2. |
|  |  |  | maxAge | Unit32 | 0..1 | The caching time-to-live period that shall be set on media resources matching the filters. This determines the minimum period for which the Media AS shall cache matching media resources as well as the time-to-live period signalled by the Media AS at reference point M2 when it serves such media resources.  The time-to-live for a given media resource shall be calculated relative to the time it was contributed. |

## 8.10 Metrics Reporting provisioning API

### 8.10.1 Overview

The Metrics Reporting Provisioning API allows an Media Application Provider to configure the Metrics Collection and Reporting procedure for a particular downlink or uplink media delivery Provisioning Session at reference point M1.

### 8.10.2 Resource structure

The Metrics Reporting Provisioning API is accessible through the following URL base path:

{apiRoot}/3gpp-maf-provisioning/{apiVersion}/provisioning-sessions/{provisioningSessionId}/

Table 8.10.2‑1 below specifies the operations and the corresponding HTTP methods that are supported by this API. In each case, the Provisioning Session identifier shall be substituted into {provisioningSessionId} in the above URL template and the sub-resource path specified in the second column of the table shall be appended to the URL base path.

Table 8.10.2-1: Operations supported by the Metrics Reporting Provisioning API

| Operation name | Sub‑resource path | Allowed HTTP method(s) | Description |
| --- | --- | --- | --- |
| Create Metrics Reporting Configuration | metrics‑reporting‑configurations | POST | Create and provide a metrics reporting configuration. |
| Read Metrics Reporting Configuration | metrics‑reporting‑configurations/‌{metricsReportingConfigurationId} | GET | Retrieve the values of an existing Metrics Reporting Configuration. |
| Update Metrics Reporting Configuration | PUT, PATCH | Modify or replace an existing metrics reporting configuration. |
| Destroy Metrics Reporting Configuration | DELETE | Destroy a metrics reporting configuration. |

### 8.10.3 Data model

#### 8.10.3.1 MetricsReportingConfiguration resource

Table 8.10.3‑1: Definition of MetricsReportingConfiguration resource

| Property name | Type | Cardinality | Description |
| --- | --- | --- | --- |
| metricsReportingConfigurationId | ResourceId | 1..1 | An identifier for this Metrics Reporting Configuration assigned by the Media AF that is unique within the scope of the enclosing Provisioning Session. |
| *sliceScope* | array(Snssai) | 0..1 | The set of network slice(s) for which metrics collection and reporting shall be executed in connection with this metrics reporting configuration (see NOTE).  If present, the array shall identify at least one network slice.  If absent, metrics shall be collected and reported for media delivery sessions within the scope of the parent Provisioning Session regardless of network slice. |
| scheme | Uri | 0..1 | The QoE metrics scheme associated with this Metrics Reporting Configuration.  Omitting this property signals to the Media AF that metrics reporting is currently disabled for the Provisioning Session in question. |
| dataNetworkName | Dnn | 0..1 | Identifies the Data Network which shall be used when sending metrics reports.  If not specified, the default Data Network shall be used. |
| *reportingStartOffset* | DurationSec | 0..1 | The time offset (expressed in seconds) from the start of a media delivery session when the Media Client is required to begin submitting metrics reports.  If omitted, the value of this parameter is assumed to be zero, i.e., directing the Media Client to start reporting metrics from the start of the media delivery session. |
| *reportingDuration* | DurationSec | 0..1 | The period of time (expressed in seconds) measured relative to the reporting start point, after which the Media Client is required to stop reporting metrics.  If omitted, reporting is required to continue until the end of the media delivery session. |
| reportingInterval | DurationSec | 0..1 | The time interval between successive metrics reports to be sent by the Media Session Handler. The value shall be greater than zero.  If not specified, a single final report shall be sent after the media delivery session has ended. |
| samplePercentage | Percentage | 0..1 | The proportion of media delivery sessions for which QoE metrics shall be reported, expressed as a floating-point value between 0.0 and 100.0.  If not specified, reports shall be sent for all media delivery sessions. |
| urlFilters | array(string) | 0..1 | If present, a non-empty list of Media Entry Point URL patterns for which QoE metrics shall be reported.  If not specified, reporting shall be done for all media delivery sessions initiated within the scope of the parent Provisioning Session. |
| samplingPeriod | DurationSec | 1..1 | The time interval the Media Client should wait between sampling the QoE metrics specified by this Metrics Reporting Configuration. |
| metrics | array(string) | 0..1 | If present, a non-empty list of QoE metrics which shall be collected and reported by the Media Client.  A controlled vocabulary of QoE metrics shall be specified by each metrics scheme for use with this property.  If omitted, the complete (or default, as applicable) set of metrics associated with the specified metrics scheme shall be collected and reported. |
| NOTE: The Snssai data type is specified in TS 29.571 [29571]. | | | |

## 8.11 Consumption Reporting provisioning API

### 8.11.1 Overview

The Consumption Reporting Provisioning API is a RESTful API that allows a Media Application Provider to configure the Consumption Reporting Procedure for a particular downlink media delivery Provisioning Session at reference point M1. The different interactions are described in clause 5.2.11. The Consumption Reporting Configuration is represented by a ConsumptionReportingConfiguration resource, the data model for which is specified in clause 8.11.3 below. The RESTful resources for managing the Consumption Reporting Configuration are specified in clause 8.11.2.

### 8.11.2 Resource structure

The Consumption Reporting Provisioning API is accessible through the following URL base path:

{apiRoot}/3gpp-maf-provisioning/{apiVersion}/provisioning-sessions/{provisioningSessionId}/

Table 8.11.2‑1 below specifies the operations and the corresponding HTTP methods that are supported by this API. In each case, the Provisioning Session identifier shall be substituted into {provisioningSessionId} in the above URL template and the sub-resource path specified in the second column shall be appended to the URL base path.

Table 8.11.2‑1: Operations supported by the Consumption Reporting Provisioning API

|  |  |  |  |
| --- | --- | --- | --- |
| Operation name | Sub‑resource path | Allowed HTTP method(s) | Description |
| Create Consumption Reporting Configuration resource | consumption‑reporting‑configuration | POST | Activate the consumption reporting procedure for a Provisioning Session by providing the Consumption Reporting Configuration. |
| Retrieve Consumption Reporting Configuration resource | GET | Retrieve an existing Consumption Reporting Configuration. |
| Update Consumption Reporting Configuration resource | PUT, PATCH | Replace or modify an existing Consumption Reporting Configuration. |
| Destroy Consumption Reporting Configuration resource | DELETE | Deactivate the consumption reporting procedure for the parent Provisioning Session. |

### 8.11.3 Data model

#### 8.11.3.1 ConsumptionReportingConfiguration resource

Table 8.11.3.1-1: ConsumptionReportingConfiguration resource

|  |  |  |  |
| --- | --- | --- | --- |
| Property name | Type | Cardinality | Description |
| reportingInterval | DurationSec | 0..1 | The interval between two consecutive consumption reports. The value shall be greater than zero.  If absent, a single final report shall be sent immediately after the media streaming session has ended. |
| samplePercentage | Percentage | 0..1 | The proportion of media streaming clients that shall report media consumption, expressed as a floating-point value between 0.0 and 100.0.  If not specified, all clients shall send consumption reports. |
| locationReporting | boolean | 0..1 | Stipulates whether the Media Session Handler is required to provide location data to the Media AF in consumption reporting messages (in case of MNO or trusted third parties).  If omitted, location reporting is disabled. |
| accessReporting | boolean | 0..1 | Stipulates whether the Media Session Handler is required to provide consumption reporting messages to the Media AF when the access network changes during a media streaming session.  If omitted, access reporting is disabled. |

## 8.12 Event Data Processing provisioning API

### 8.12.1 General

The Event Data Processing Provisioning API is used by a Media Application Provider to provide Event Data Processing Configurations to the Data Collection AF instantiated in the Media  AF. Each such configuration is represented by an EventDataProcessingConfiguration resource, the data model of which is specified in clause 8.12.3 below. It comprises processing rules and parameters expressed using Data Access Profiles (specified in TS 26.532 [26532]), each of which defines a level of access by Event consumers to the UE data collected by the Data Collection AF. The RESTful structure of the Data Exposure Restriction Configuration resource collection, along with the operations and corresponding HTTP methods for managing resources of this type are defined in clause 8.12.2.

### 8.12.2 Resource structure

The Event Data Processing Provisioning API is accessible through the following URL base path:

{apiRoot}/3gpp-maf-provisioning/{apiVersion}/provisioning-sessions/{provisioningSessionId}/

Table 8.12.2-1 below specifies the operations and the corresponding HTTP methods that are supported by this API. In each case, the Provisioning Session identifier shall be substituted into {provisioningSessionId} in the above URL template and the sub-resource path specified in the second column shall be appended to the URL base path.

Table 8.12.2‑1: Operations supported by the Data Exposure Restriction API

|  |  |  |  |
| --- | --- | --- | --- |
| Operation name | Sub‑resource path | Allowed HTTP method(s) | Description |
| Create Event Data Processing Configuration | event-data-processing-configurations | POST | Create a new Event Data Processing Configuration resource. |
| Retrieve Event Data Processing Configuration | event-data-processing-configurations/‌{event‌Data‌Processing‌ConfigurationId} | GET | Retrieve an existing Event Data Processing Configuration. |
| Update Event Data Processing Configuration | PUT,  PATCH | Modify or replace an existing Event Data Processing Configuration. |
| Destroy Event Data Processing Configuration | DELETE | Destroy an existing Event Data Processing Configuration. |

### 8.12.3 Data model

#### 8.12.3.1 EventDataProcessingConfiguration resource type

Table 8.12.3‑1: Definition of EventDataProcessingConfiguration resource

| Property name | Type | Cardinality | Description |
| --- | --- | --- | --- |
| eventDataProcessing‌ConfigurationId | ResourceId | 1..1 | An identifier for this Event Data Processing Configuration assigned by the Media AF that is unique within the scope of the enclosing Provisioning Session. |
| eventId | AfEvent | 1..1 | One of the enumerated values specified in clause 5.6.3.3 of TS 29.517 [29517] relating to Media Delivery. |
| authorizationUrl | AbsoluteUrl | 0..1 | A URL that may be used to authorize the Event consumer entity to enable its subscription to the Data Collection AF for event notification, subject to the data access restrictions of a Data Access Profile. |
| dataAccessProfiles | array(Data‌Access‌Profile) | 1..1 | One or more Data Access Profile definitions, each one describing a set of data processing instructions to be applied by the Data Collection AF when exposing events to an associated Event consumer entity. (See clause 6.3.3.2 of TS 26.532 [26532].)  The controlled vocabularies to be used with DataAccessProfile.‌parameters are not specified in the present document. |

# 9 Maf\_SessionHandling service

## 9.1 Overview

This clause defines the network media session handling API used by a Media AS at reference point M3 or by a Media Session Handler at reference point M5 to access Service Access Information and to invoke the session handling features provisioned using the APIs in clause 8. The corresponding OpenAPI definitions for the Maf\_SessionHandling service are specified in clause A.4. A summary of the resource structure is shown in table 9.1‑1 below. The default endpoint address of the Media AF at reference point M3 is specified in clause 7.1.2.2 and that at reference point M5 is specified in clause 7.1.2.3.

Table 9.1‑1: Resource structure of Maf\_SessionHandling APIs

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| HTTP request path element hierarchy | Description | Allowed HTTP methods | | | | | Resource | OpenAPI |
| Create | Retrieve | Update | Destroy | Non-RESTful operation | structure definition clause | definition clause |
| service-access-information | Service Access Information collection |  |  |  |  |  | 9.2.2 | A.4.1 |
| {*externalService*Id} | Service Access Information resource |  | GET |  |  |  |
| provisioning-sessions | Provisioning Sessions collection |  |  |  |  |  |  |  |
| {provisioningSessionId} | Provisioning Session path element |  |  |  |  |  |  |  |
| dynamic-policies | Dynamic Policies collection | POST |  |  |  |  | 9.3.2 | A.4.2 |
| {dynamicPolicyId} | Dynamic Policy resource |  | GET | PUT, PATCH | DELETE |  |
| network-assistance-sessions | Network Assistance Sessions collection | POST |  |  |  |  | 9.4.2 | A.4.3 |
| {naSessionId} | Network Assistance Session resource |  | GET | PUT, PATCH | DELETE |  |
| recommendation | Bit rate recommendation request operation |  |  |  |  | GET |
| boost | Delivery boost request operation |  |  |  |  | POST |
| metrics-reporting | Metrics Reporting endpoint collection |  |  |  |  |  | 9.5.2 | A.4.4 |
| {metricsReportingConfgurationId} | Metrics Reporting operation |  |  |  |  | POST |
| consumption-reporting | Consumption Reporting endpoint |  |  |  |  | POST | 9.6.2 | A.4.5 |

## 9.2 Service Access Information API

### 9.2.1 General

The Service Access Information API is used by the Media Session Handler to obtain configuration information from the Media AF that enables it to use the other Media Session Handling APIs specified in clause 9.3 *et seq.*

### 9.2.2 Resource structure

The Service Access Information API is accessible through the following URL base path:

{apiRoot}/3gpp-maf-session-handling/{apiVersion}/service-access-information/

The operations and the corresponding HTTP methods in table 9.2.2-1 are supported. In each case, the sub-resource path specified in the second column shall be appended to the URL base path.

Table 11.2.2‑1: Operations supported by the Service Access Information API

|  |  |  |  |
| --- | --- | --- | --- |
| Operation name | Sub-resource path | Allowed HTTP method(s) | Description |
| Retrieve Service Access Information | {*external‌Service*Id} | GET | Acquire the Service Access Information resource for the specified Provisioning Session. |

### 9.2.3 Data model

#### 9.2.3.1 ServiceAccessInformation resource type

The data model for the ServiceAccessInformation resource is specified in table 9.2.3.1-1 below. Different properties are present in the resource depending on the type of Provisioning Session from which the Service Access Information is derived (as indicated in the provisioningSessionType property) and this is specified in the *Applicability* column.

Table 9.2.3.1‑1: Definition of ServiceAccessInformation resource

| Property name | | | Type | Cardinality | Usage | Description | Applicability |
| --- | --- | --- | --- | --- | --- | --- | --- |
| provisioningSessionId | | | ResourceId | 1..1 | RO | Unique identification of the M1 Provisioning Session. | All types |
| provisioningSession‌Type | | | Provisioning‌Session‌Type | 1..1 | RO | The type of Provisioning Session. | All types. |
| streamingAccess | | | object | 0..1 | RO | Present if Content Hosting or Content Publishing is provisioned in the parent Provisioning Session. | DOWNLINK |
|  | entryPoints | | Array(M5‌Media‌Entry‌Point) | 0..1 | RO | A list of alternative Media Entry Points for the Media Client to choose between. |
|  |  | locator | AbsoluteUrl | 1..1 | RO | A pointer to a document at reference point M2 that defines a media presentation e.g. MPD for DASH content or URL to a video clip file. |
|  |  | contentType | string | 1..1 | RO | The MIME content type of resource at locator. |  |
|  |  | profiles | array(Uri) | 0..1 | RO | An optional list of conformance profile URIs with which this Media Entry Point is compliant.  If present, the array shall contain at least one item. |  |
|  | eMBMS‌Service‌Announcement‌Locator | | AbsoluteUrl | 0..1 | RO | A pointer to an eMBMS User Service Announcement document. |  |
|  | mbs‌External‌Service‌Identifier | | string | 0..1 | RO | The external service identifier of an MBS User Service. |  |
| clientConsumptionReporting‌Configuration | | | object | 0..1 | RO | Present if consumption reporting is activated for this Provisioning Session. | DOWNLINK |
|  |  | reportingInterval | DurationSec | 0..1 | RO | The time interval, expressed in seconds, between consumption report messages being sent by the Media Session Handler. The value shall be greater than zero.  When this property is omitted, a single final report shall be sent immediately after the media streaming session has ended. |
|  |  | serverAddresses | array(AbsoluteUrl) | 1..1 | RO | A list of Media AF addresses (URLs) where the consumption reporting messages are sent by the Media Session Handler. (See NOTE 1).  Each address shall be an opaque base URL, following the format specified in clause 7.1.3 up to and including the {apiVersion} path element. |
|  |  | locationReporting | boolean | 1..1 | RO | Indicates whether the Media Session Handler is required to provide location data in consumption reporting messages (in case of MNO or trusted third parties).  Shall be set false if the locationReporting parameter is omitted from the Consumption‌Reporting‌Configuration, as specified in table 8.11.3.1‑1. |
|  |  | accessReporting | boolean | 1..1 | RO | Indicates whether the Media Session Handler is required to supply consumption reporting units whenever the access network changes during a media delivery session.  Shall be set false if the accessReporting parameter is omitted from the Consumption‌Reporting‌Configuration, as specified in table 8.11.3.1‑1. |
|  |  | samplePercentage | Percentage | 1..1 | RO | The percentage of media delivery sessions that shall send consumption reports, expressed as a floating-point value between 0.0 and 100.0.  Shall be set to 100.0 if the samplePercentage parameter is omitted from the Consumption‌Reporting‌Configuration, as specified in table 8.11.3.1‑1. |
| dynamicPolicyInvocation‌Configuration | | | object | 0..1 | RO | Present if Policy Templates have been provisioned in the parent Provisioning Session and at least one of them is in the READY state. | DOWNLINK, UPLINK |
|  | serverAddresses | | array(AbsoluteUrl) | 1..1 | RO | A list of Media AF addresses (URLs) which offer the APIs for dynamic policy invocation sent by the Media Session Handler. (See NOTE 1.)  Each address shall be an opaque base URL, following the format specified in clause 7.1.3 up to and including the {apiVersion} path element. |  |
|  | policyTemplateBindings | | array(object) | 1..1 | RO | A list of duples, each one binding an external reference to a Policy Template resource identifier. |  |
|  |  | externalReference | string | 1..1 | RO | Additional identifier for this Policy Template, unique within the scope of its Provisioning Session, that can be cross-referenced with external metadata about the media streaming session.  Example: "HD\_Premium". |  |
|  |  | policyTemplateId | ResourceId | 1..1 | RO | The resource identifier of a Policy Template tagged with externalReference that is in the READY state. |  |
|  | sdfMethods | | array(SdfMethod) | 1..1 | RO | A list of Service Data Flow description methods, e.g. 5-tuple, ToS, 2-tuple, etc., which should be used by the Media Session Handler to describe the Service Data flows at reference point M2 for media delivery sessions. |  |
| clientMetricsReporting‌Configurations | | | array(object) | 0..1 | RO | Present if QoE metrics reporting is provisioned in the parent Provisioning Session.  If present, contains one or more client metrics reporting configurations. | DOWNLINK, UPLINK |
|  | metricsReporting‌ConfigurationId | | ResourceId | 1..1 | RO | The identifier of this metrics reporting configuration, unique within the scope of the parent Provisioning Session.  The value shall be the same as the corresponding identifier provisioned at reference point M1 (see clause 8.10.3.1). |
|  | serverAddresses | | array(AbsoluteUrl) | 1..1 | RO | A list of Media AF addresses to which metrics reports shall be sent. (See NOTE 1).  Each address shall be an opaque base URL, following the format specified in clause 7.1.3 up to and including the {apiVersion} path element. |
|  | *sliceScope* | | array(Snssai) | 0..1 | RO | The set of network slice(s) for which metrics collection and reporting shall be executed in connection with this metrics reporting configuration (see NOTE 2).  If present, the array shall identify at least one network slice.  If absent, metrics shall be collected and reported for media delivery sessions within the scope of the parent Provisioning Session regardless of network slice. |
|  | scheme | | Uri | 1..1 | RO | A URI identifying the metrics scheme that metrics reports shall use (see clause 5.2.10). |
|  | dataNetworkName | | Dnn | 0..1 | RO | The name of the Data Network which shall be used to send metrics reports.  If not specified, the default DN shall be used. |
|  | *reportingStartOffset* | | DurationSec | 0..1 | RO | The time offset (expressed in seconds) from the start of a media delivery session when the Media Client is required to begin submitting metrics reports.  If omitted, the value of this parameter is assumed to be zero, i.e., directing the Media Client to start reporting metrics from the start of the media delivery session. |
|  | *reportingDuration* | | DurationSec | 0..1 | RO | The period of time (expressed in seconds) measured relative to the reporting start point, after which the Media Client is required to stop reporting metrics.  If omitted, reporting is required to continue until the end of the media delivery session. |
|  | reportingInterval | | DurationSec | 0..1 | RO | The time interval, expressed in seconds, between metrics reports being sent by the Media Session Handler. The value shall be greater than zero.  When this property is omitted, a single final report shall be sent immediately after the media streaming session has ended. |
|  | samplePercentage | | Percentage | 1..1 | RO | The percentage of media delivery sessions that shall report QoE metrics, expressed as a floating-point value between 0.0 and 100.0. |
|  | urlFilters | | array(string) | 0..1 | RO | A non-empty list of Media Entry Point URL patterns for which QoE metrics shall be reported. The format of each pattern shall be a regular expression as specified in [ECMA262].  If not specified, reporting shall be done for all media delivery sessions. |
|  | samplingPeriod | | DurationSec | 1..1 | RO | The time interval the Media Client should wait between sampling the QoE metrics specified by this metrics reporting configuration. |
|  | metrics | | array(string) | 1..1 | RO | A list of QoE metrics which shall be reported.  If empty, the complete (or default if applicable) set of metrics associated with the specified scheme shall be collected and reported. |
| networkAssistance‌Configuration | | | object | 0..1 | RO | Present if Network Assistance is provisioned in the parent Provisioning Session. | DOWNLINK, UPLINK |
|  | serverAddresses | | array(AbsoluteUrl) | 1..1 | RO | A list of Media AF addresses (URLs) that offer the APIs for AF-based Network Assistance at reference point M5. (See NOTE 1.)  Each address shall be an opaque URL, following the format specified in clause 7.1.3 up to and including the {apiVersion} path element. |
| client‌EdgeResources‌Configuration | | | object | 0..1 | RO | Present only for Provisioning Sessions with client-driven edge computing management mode provisioned. | DOWNLINK, UPLINK |
|  | eligibilityCriteria | | Edge‌Processing‌Eligibility‌Criteria | 0..1 | RO | Conditions for activating edge resources for media delivery sessions in the scope of the parent Provisioning Session. (See clause 7.3.3.8.) |
|  | easDiscoveryTemplate | | EAS‌Discovery‌Template | 1..1 | RO | A template for the EAS discovery filter that shall be used by the EEC to discover and select a Media EAS instance to serve media delivery sessions at reference point M4 in the scope of the parent Provisioning Session. (See clause 9.2.3.2.) |
|  | easRelocation‌Requirements | | M5EAS‌Relocation‌Requirements | 0..1 | RO | EAS relocation tolerance and requirements.  If absent, the EEC shall assume that relocation is tolerated by all Media EAS instances in the scope of the parent Provisioning Session. (See clause 9.2.3.3.) |
| NOTE 1: In deployments where multiple instances of the Media AF expose the Media Session Handling APIs at reference point M5, the 5G System may use a suitable mechanism (e.g., HTTP load balancing or DNS-based host name resolution) to direct requests to a suitable Media AF instance.  NOTE 2: The Snssai data type is specified in TS 29.571 [29571]. | | | | | | | |

#### 9.2.3.2 EASDiscoveryTemplate type

Table 9.2.3.2-1  Definition of EASDiscoveryTemplate type

|  |  |  |  |
| --- | --- | --- | --- |
| Property name | Type | Cardinality | Description |
| easId | string | 0..1 | The application identifier of the EAS, e.g. reverse FQDN, URI.  If omitted, any Media EAS instance matching the other criteria specified in the template are acceptable.  Corresponding to EasCharacteristics.easId, as specified in clause 6.3.5.2.7 of TS 24.558 [24558]. |
| easType | string | 0..1 | If present, a non-empty string indicating the type of Media EAS required to support media delivery sessions in the scope of this discovery template.  Corresponding to EasCharacteristics.easType, as specified in clause 6.3.5.2.7 of TS 24.558 [24558]. |
| easProviderIds | array(string) | 0..1 | The non-empty set of acceptable Media EAS provider identifiers, each expressed as a non-empty string.  If omitted, Media EAS instances of the specified easType from any provider are acceptable.  Corresponding to EasCharacteristics.easProvId, as specified in clause 6.3.5.2.7 of TS 24.558 [24558]. |
| easFeatures | array(string) | 0..1 | The non-empty set of required service features for the Media EAS to serve media delivery sessions, each expressed as a non-empty string.  If omitted, Media EAS instances of the specified easType with any feature set are acceptable.  Corresponding to EasCharacteristics.svcFeats, as specified in clause 6.3.5.2.7 of TS 24.558 [24558]. |
| NOTE: At least one of the properties shall be populated. | | | |

#### 9.2.3.3 M5EASRelocationRequirements type

Table 11.2.3.3-1: Definition of M5EASRelocationRequirements type

| Property name | Type | Cardinality | Description |
| --- | --- | --- | --- |
| tolerance | EASRelocation‌Tolerance | 1..1 | Indicates whether the Media EAS instance tolerates relocation. (See clause 7.3.4.4.) |
| maxInterruptionDuration | UintegerRm | 0..1 | The maximum downtime (expressed in milliseconds) that an application can tolerate during EAS relocation.  If the expected downtime of the application is expected to exceed this duration, relocation of the Media EAS instance shall not be performed. |

## 9.3 Dynamic Policy API

### 9.3.1 Overview

The Dynamic Policy API allows the Media Session Handler to request a specific policy and charging treatment to be applied to a particular application data flow of a downlink or uplink media delivery session by invoking RESTful operations on the Media AF at reference point M5. The API defines a set of data models, resources and the related operations for the creation and management of the dynamic policy request.

### 9.3.2 Resource structure

The Dynamic Policies API is accessible through the following URL base path:

{apiRoot}/3gpp-maf-session-handling/{apiVersion}/provisioning-sessions/{provisioningSessionId}/dynamic-policies/

where the first three path elements shall be substituted by the Media Session Handler with one of the URLs selected from the dynamicPolicy‌Invocation‌Configuration.serverAddresses array of the ServiceAccessInformation resource (see clause 9.2.3.1) and the fifth path element shall be substituted with the value of the relevant Provisioning Session identifier obtained from the same resource.

Table 9.3.2‑1 below specifies the operations and the corresponding HTTP methods that are supported by this API. The sub-resource path specified in the second column shall be appended to the URL base path.

Table 9.3.2-1: Operations supported by the Dynamic Policies API

|  |  |  |  |
| --- | --- | --- | --- |
| Operation name | Sub-resource path | Allowed HTTP methods | Description |
| Create Dynamic Policy resource |  | POST | Create a new Dynamic Policy resource. |
| Retrieve Dynamic Policy resource | {dynamicPolicyId} | GET | Retrieve an existing Dynamic Policy resource. |
| Update Dynamic Policy resource | PUT | Replace an existing Dynamic Policy resource. |
| PATCH | Modify an existing Dynamic Policy resource. |
| Destroy Dynamic Policy resource | DELETE | Remove an existing Dynamic Policy resource. |

### 9.3.3 Data model

#### 9.3.3.1 DynamicPolicy resource

Table 9.3.3.1-1: Definition of Dynamic Policy Instance resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property name | Data type | Cardinality | Usage | Description |
| dynamicPolicyId | ResourceId | 1..1 | RO | Unique identifier for this Dynamic Policy assigned by the Media AF. |
| provisioningSessionId | ResourceId | 1..1 | C: RO R: RO U: RO | Uniquely identifies the parent Provisioning Session, which is linked to the Application Service Provider. |
| session‌Id | MediaDelivery‌SessionId | 1..1 | C: RW R:RO U: RO | Unique identifier of the current media delivery session assigned by the Media Session Handler. |
| policyTemplateId | ResourceId | 1..1 | C: RW R: RO U: RW | Identifies the Policy Template to be applied to the application flow(s). |
| serviceDataFlowDescriptions | array(Service‌Data‌Flow‌Description) | 1..1 | C: RW R: RO U: RW | Describes the Service Data Flows managed by this Dynamic Policy. |
| mediaType | MediaType | 0..1 | C: RW R: RO U: RW | The type of media carried by the application flows listed in service‌DataFlow‌Descriptions. |
| qosSpecification | M5‌QoS‌Specification | 0..1 | C: RW R: RO U: RW | The network Quality of Service requirements of this Dynamic Policy (see clause 7.3.3.4). |
| qosEnforcement | boolean | 1..1 | C: RO R: RO U: RO | Indication that the Quality of Service described in qosSpecification is being enforced by the 5G System. |

## 9.4 Network Assistance API

### 9.4.1 Overview

If AF-based Network Assistance is supported by the Media AF, then the Network Assistance API, as defined in the present sub-clause, is first used to provision a Network Assistance Session resource at reference point M5. The Network Assistance resource can then be used to obtain bit rate recommendations and to issue delivery boost requests during the ongoing media delivery session.

### 9.4.2 Resource structure

The Network Assistance API is accessible via the following URL base path:

{apiRoot}/3gpp‑maf-session-handling/{apiVersion}/provisioning-sessions/{provisioningSessionId}/network-assistance-sessions/

where the first three path elements shall be substituted by the Media Session Handler with one of the URLs selected from the network‌Assistance‌Configuration.‌serverAddresses array of the ServiceAccessInformation resource (see clause 9.2.3.1) and the fifth path element shall be substituted with the relevant Provisioning Session identifier obtained from the same resource..

Table 9.4.2‑1 below specifies the operations and the corresponding HTTP methods that are supported by this API. In each case, the sub-resource path specified in the second column of the table shall be appended to the URL base path.

Table 9.4.2-1: Operations supported by the Network Assistance API

|  |  |  |  |
| --- | --- | --- | --- |
| Operation name | Sub‑resource path | Allowed HTTP method(s) | Description |
| Create Network Assistance Session resource |  | POST | Provision a new Network Assistance Session.  If the operation succeeds, the URL of the created Network Assistance Session resource shall be returned in the Location header of the response. |
| Retrieve Network Assistance Session resource | {naSessionId} | GET | Fetch the properties of an existing Network Assistance Session. |
| Bit rate recommendation request | {naSessionId}/recommendation | GET | Obtain a bit rate recommendation. |
| Delivery boost request | {naSessionId}/boost-request | POST | Request a delivery boost. |
| Update Network Assistance Session resource | {naSessionId} | PUT,  PATCH | Update the properties of an existing Network Assistance Session. |
| Destroy Network Assistance Session | {naSessionId} | DELETE | Terminate a Network Assistance session. |

### 9.4.3 Data model

#### 9.4.3.1 NetworkAssistanceSession resource

Table 9.4.3.1-1: Definition of NetworkAssistanceSession resource

| Property name | Type | Cardinality | Usage | Description |
| --- | --- | --- | --- | --- |
| naSessionId | ResourceId | 1..1 | C: RO  R: RO  U: RO | Unique identifier for this Network Assistance Session assigned by the Media AF. |
| provisioningSessionId | ResourceId | 1..1 | C: RO R: RO U: RO | Uniquely identifies the parent Provisioning Session, which is linked to the Application Service Provider. |
| session‌Id | MediaDelivery‌SessionId | 1..1 | C: RW R:RO U: RO | Unique identifier of the current media delivery session assigned by the Media Session Handler. |
| serviceDataFlowDescriptions | array(Service‌Data‌Flow‌Description) | 1..1 | C: RW  R: RO  U: RW | Identifying one or more application flows for which Network Assistance is sought, e.g. 2‑tuple (IP addresses) or 5-tuple (IP Addresses, protocol and ports). |
| mediaType | MediaType | 0..1 | C: RW  R: RO  U: RW | The type of media carried by the application flows listed in service‌DataFlow‌Descriptions. |
| policyTemplateId | ResourceId | 0..1 | C: RW  R: RO  U: RW | Identification of the policy (if any) that is currently in force for the media delivery session. |
| requestedQoS | M5QoSSpecification | 0..1 | C: RW  R: RO  U: RW | The QoS parameters requested by the Media Session Handler. |
| recommendedQoS | M5QoSSpecification | 0..1 | C: RO  R: RO  U: RO | The QoS parameters currently recommended by the Media AF. |
| notficationURL | AbsoluteUrl | 0..1 | C: RO  R: RO  U: RO | A URL to the MQTT channel, nominated by the Media AF, over which notifications are to be sent by the Media AF for this session. |

## 9.5 Metrics Reporting API

### 9.5.1 General

The Metrics Reporting API allows the Media Session Handler to send QoE metrics reports to the Media AF. This procedure is configured by the ServiceAccessInformation resource, as defined in clause 9.2.3.1. Multiple metrics reporting configurations may be active at the same time, each identified by a unique metrics‌Reporting‌ConfigurationId.

### 9.5.2 Reporting procedure

Metrics reports related to a specific metricsReportingConfigurationId shall be submitted according to the following general format:

{apiRoot}/3gpp-maf-session-handling/{apiVersion}/provisioning-sessions/{provisioningSessionId}/metrics-reporting/‌{metricsReporting‌ConfigurationId}

where the first three path elements shall be substituted by the Media Session Handler with one of the base URLs selected from the client‌Metrics‌Reporting‌Configurations.‌serverAddresses array of the ServiceAccessInformation resource (see clause 9.2.3.1), the fifth path element shall be substituted with the relevant Provisioning Session identifier obtained from the same resource and {metricsReportingConfigurationId} shall be substituted with the relevant Metrics Reporting Configuration identifier.

The only HTTP method supported by this endpoint is POST.

### 9.5.3 Report format

Metrics reports shall be submitted by the Media Session Handler in a format specified by the metrics scheme in question. The Content-Type HTTP request header shall be set in accordance with the specification of the relevant metrics scheme.

Metrics schemes specified by 3GPP shall make provision to convey the media delivery session identifier in their metrics reports. For metrics reporting formats specified elsewhere, the 3GPP specification referencing the metrics scheme should specify a means to convey the media delivery session identifier in metrics reports where practicable.

## 9.6 Consumption Reporting API

### 9.6.1 General

The Consumption Reporting API allows the Media Session Handler to report downlink media consumption to the Media AF. The API defines data models, resources and the related operations for the creation and management of the consumption reporting procedures. This feature is configured by the ServiceAccessInformation resource, as defined in clause 9.2.3.1.

### 9.6.2 Reporting procedure

Consumption reports shall be submitted to a Media AF endpoint according to the following general URL format:

{apiRoot}/3gpp-maf-session-handling/{apiVersion}/provisioning-sessions/{provisioningSessionId}/consumption-reporting/

Where the first three path elements shall be substituted by the 5GMSd Client with one of the base URLs selected from the client‌Consumption‌Reporting‌Configuration.‌serverAddresses array of the ServiceAccessInformation resource (see clause 9.2.3.1) and the fifth path element shall be substituted with the relevant Provisioning Session identifier obtained from the same resource.

The only HTTP method supported by this endpoint is POST.

### 9.6.3 Report format

#### 9.6.3.1 ConsumptionReport type

This data type specifies the root object of a consumption report instance document used by the Media Session Handler to report media consumption.

Table 9.6.3.1-1: Definition of ConsumptionReport format

|  |  |  |  |
| --- | --- | --- | --- |
| Property name | Data type | Cardinality | Description |
|  |  |  |  |
| reportingClientId | string | 1..1 | Identifier of the reporting client that consumed the streaming media service associated with this consumption report.  If available to the Media Session Handler, a GPSI value (see clause 28.8 of TS 23.003 [7]); otherwise, a stable and globally unique string. |
| session‌Id | MediaDelivery‌SessionId | 1..1 | Unique identifier of the current media delivery session assigned by the Media Session Handler. |
|  |  |  |  |
| consumptionReportingUnits | array(Consumption‌Reporting‌Unit) | 1..1 | A list of consumption reporting units, ordered by start time.  The content of this property is not specified in the present document. |

#### 9.6.3.2 ConsumptionReportingUnit type

This data type represents a single consumption reporting unit.

Table 9.6.3.2-1: Definition of type ConsumptionReportingUnit

|  |  |  |  |
| --- | --- | --- | --- |
| Property name | Data type | Cardinality | Description |
| mediaConsumed | string | 1..1 | Identifies the media consumed.  The content of this property is not specified in the present document. |
| clientEndpointAddress | EndpointAddress | 0..1 | The IP address and port number of the Media Access Function endpoint used to access the media consumed.  Present only if access reporting is enabled in the Consumption Reporting Configuration. |
| serverEndpointAddress | EndpointAddress | 0..1 | The IP address, port number and host name of the Media AS endpoint used to access the media consumed.  Present only if access reporting is enabled in the Consumption Reporting Configuration. |
| startTime | DateTime | 1..1 | The time when this consumption reporting unit started. |
| duration | DurationSec | 1..1 | The duration of this consumption reporting unit.  For consumption reporting units describing the currently consumed media, this shall indicate the duration so far. |
| locations | array(TypedLocation) | 0..1 | A time-ordered list of one or more UE location(s) where the media was consumed during the period of this consumption reporting unit.  Present only if location reporting is enabled in the Consumption Reporting Configuration (only for trusted Media AF). |

# 10 UE media session handling APIs

## 10.1 General

This clause defines the client APIs exposed by the Media Session Handler to the Media-aware Application at reference point M6 and to the Media Access Function at reference point M11.

NOTE: Client-driven management of edge processing resources via reference point M6 is not specified in this release.

## 10.2 Session launch mechanisms

Editor’s Note: Specify an explicit session launch API as an alternative to the 3GPP Service URL specified in clause 6?

## 10.3 Media session handling APIs for downlink media streaming

Editor’s Note: port clause 12.2 from TS 26.512. (Functional model in 12.2.1 should be migrated to TS 26.501.)

### 10.3.1 General

This clause defines the client APIs for Media Session Handling to be used by other 5G System components such as a Media Player in a 5GMSd Client or the Media Streamer in a 5GMSu Client.

NOTE: Client-driven management of edge processing resources via reference point M6 is not specified in this release.

### 10.3.2 Media Session Handler model

#### 10.3.2.1 State model

An informative state model for the Media Session Handler is for further study.

#### 10.3.2.2 Media Session Handler internal properties

The Media Session Handler maintains internal properties as defined table 10.3.2.2-1. Note that the parameters are conceptual and internal. They serve only for the purpose of defining the media session handling APIs.

Table 10.3.2.2-1: Parameters of Media Session Handler

|  |  |  |
| --- | --- | --- |
| States and Parameters | | Definition |
| \_Configuration[externalServiceId] | | The Media Session Handler maintains a separate configuration for each set of Service Access Information it has knowledge of, indexed by its external service identifier. |
|  | \_networkAssistance | Network Assistance configuration. |
|  | \_policyTemplate | Policy Template configuration. |
|  | \_consumptionReporting | Consumption reporting configuration. |
|  | \_metricsReporting | Metrics reporting configuration. |
| \_status[mediaDeliverySessionIdentifier] | | The Media Session Handler maintains a separate status record for each currently active media delivery session. |
|  | \_generalStatus | General status information. (See table 10.3.3‑1.) |
|  |  | Dynamic Policy status information is for further study. |
|  |  | Network Assistance status information is for further study. |
|  | \_consumptionReportingStatus | Consumption Reporting status information. (See table 10.3.6‑1.) |
|  | \_metricsReportingStatus | Metrics Reporting status information. (See table 10.3.7‑1.) |

#### 10.3.2.3 Media Session Handler internal operations

This aspect is for further study.

#### 10.3.2.4 Starting and Stopping a Media Session Handler

There are different ways to start a Media Session Handler. The most typical one is that the start is bound to the call of a Media Player with an MPD URL. That start method offers a client–server like interface realized by M6d. The service is bound such that the Media Session Handler communicates back to the Media Player.

### 10.3.3 General

Table 10.3.3-1 specifies the status information that can be obtained from the Media Session Handler through reference point M6d.

Table 10.3.3-1: General Status Information

|  |  |  |  |
| --- | --- | --- | --- |
| Status | Type | Parameter | Definition |
|  |  |  |  |

Table 10.3.3-2 provides a list of general notification events exposed at reference point M6d.

Table 10.3.3-2: General Notification Events

|  |  |  |
| --- | --- | --- |
| Event | Definition | Payload |
| SESSION\_HANDLING\_ACTIVATED | Triggered when media session handling was activated for a specific Media Entry Point. | Media Entry Point URL. |
| SESSION\_HANDLING\_STOPPED | Triggered when media session handling stopped for a specific Media Entry Point. | Media Entry Point URL. |

Table 10.3.3-3 provides a list of general error events exposed at reference point M6d.

Table 10.3.3-3: General Error Events

|  |  |  |
| --- | --- | --- |
| Status | Definition | Payload |
| ERROR\_SESSION\_HANDLING | Triggered when there is an error in the media session handling. | None. |

### 10.3.4 Dynamic Policy information

Editor's Note: Expose status information and asynchronous notifications relating to most recent dynamic policy invocation and Background Data Transfer.

Details are for further study.

### 10.3.5 Network Assistance information

Editor's Note: Expose status information and asynchronous notifications relating to most recent bit rate recommendation and delivery boost.

Details are for further study.

### 10.3.6 Consumption Reporting information

Table 10.3.6-1 specifies the status information relating to Consumption Reporting that is exposed by the Media Session Handler through reference point M6.

Table 10.3.6-1: Status Information relating to Consumption Reporting

|  |  |  |  |
| --- | --- | --- | --- |
| Status | Type | Parameter | Definition |
| consumptionReport | object |  | The most recently sent consumption report. |

Table 10.3.6-2 provides a list of general notification events exposed by the Media Session Handler at reference point M6.

Table 10.3.6-2: Notification Events relating to Consumption Reporting

|  |  |  |
| --- | --- | --- |
| Status | Definition | Payload |
| CONSUMPTION\_REPORTING\_ACTIVATED | Consumption reporting has been activated. | Media delivery session identifier. |
| CONSUMPTION\_REPORTING\_STOPPED | Consumption reporting has been stopped. | Media delivery session identifier. |
| NEW\_CONSUMPTION\_REPORT | A new consumption report is available and has been sent. | Media delivery session identifier. |

Table 10.3.6-3 provides a list of general error events exposed by the Media Session Handler at reference point M6d.

Table 10.3.6-3: Error Events relating to Consumption Reporting

|  |  |  |
| --- | --- | --- |
| Status | Definition | Payload |
| ERROR\_CONSUMPTION\_REPORTING | Error in consumption reporting occurred. | Media delivery session identifier, Provisioning Session Id, Server address, HTTP response code Error message. |

### 10.3.7 Metrics Reporting information

Table 10.3.7-1 specifies the status information relating to Metrics Reporting that is exposed by the Media Session Handler through reference point M6.

Table 10.3.7-1: Status Information relating to Metrics Reporting

|  |  |  |
| --- | --- | --- |
| Status | Type | Definition |
| lastMetricsReport | object | Status information relating to the last sent metrics report. |
| provisioningSessionId | ResourceId | The Provisioning Session identifier for this metrics report. |
| metricsReportingConfigurationId | ResourceId | The metrics reporting configuration identifier for this report. |
| scheme | Uri | The metrics reporting scheme used by this metrics report (see clause 5.3.5). |
| metricsReport | object | The most recently sent metrics report. |

Table 10.3.7-2 provides a list of general notification events exposed at reference point M6.

Table 10.3.7-2: Notification Events relating to Metrics Reporting

|  |  |  |
| --- | --- | --- |
| Event | Definition | Payload |
| METRICS\_REPORTING\_ACTIVATED | Metrics reporting has been activated. | Media delivery session identifier. |
| METRICS\_REPORTING\_STOPPED | Metrics reporting has been stopped. | Media delivery session identifier. |
| NEW\_METRICS\_REPORT | A new metrics report is available and has been sent. | Media delivery session identifier. |

Table 10.3.7-3 provides a list of general error events exposed at reference point M6.

Table 10.3.7-3: Error Events relating to Metrics Reporting

|  |  |  |
| --- | --- | --- |
| Error event | Definition | Payload |
| ERROR\_METRICS\_REPORTING | Error in metrics reporting occurred. | Media delivery session identifier, Provisioning Session Id, Server address, Metrics Reporting Configuration Id, HTTP response code Error message. |

Details of status information for RAN-based metrics reporting are for further study.

## 10.4 Media session handling APIs for uplink media streaming

Details are for further study.

## 10.5 Media session handling APIs for webRTC

Editor’s Note: New Clause.

Annex A (normative):  
OpenAPI representation of HTTP REST APIs

# A.1 General

The normative code specifying the APIs defined in clauses 7.3, 8 and 9 of the present document, including JSON Schema representations of HTTP message bodies to be used with these APIs, is published on 3GPP Forge according to the OpenAPI 3.0.0 specification [OpenAPI300]. The YAML files corresponding to this version of the present document shall be published to the following location:

https://forge.3gpp.org/rep/all/5G\_APIs/-/tags/TSG103-Rel18

Informative copies of these YAML files shall be distributed with the present document for the convenience only. Where any discrepancy exisits, the version on 3GPP Forge shall be considered definitive.

# A.2 Data Types applicable to several APIs

For the purpose of referencing entities specified in this clause, it shall be assumed that the OpenAPI definitions are contained in a physical file named "TS26510\_CommonData.yaml".

# A.3 OpenAPI representation of Maf\_Provisioning APIs

## A.3.1 Maf\_Provisioning\_ProvisioningSessions API

For the purpose of referencing entities specified in this clause, it shall be assumed that the OpenAPI definitions are contained in a physical file named "TS26510\_Maf\_Provisioning\_ProvisioningSessions.yaml".

## A.3.2 Maf\_Provisioning\_ContentProtocols API

For the purpose of referencing entities specified in this clause, it shall be assumed that the OpenAPI definitions are contained in a physical file named "TS26510\_Maf\_Provisioning\_ContentProtocols.yaml".

## A.3.3 Maf\_Provisioning\_ServerCertificates API

For the purpose of referencing entities specified in this clause, it shall be assumed that the OpenAPI definitions are contained in a physical file named "TS26510\_Maf\_Provisioning\_ServerCertificates.yaml".

## A.3.4 Maf\_Provisioning\_ContentPreparationTemplates API

For the purpose of referencing entities specified in this clause, it shall be assumed that the OpenAPI definitions are contained in a physical file named "TS26510\_Maf\_Provisioning\_ContentPreparationTemplates.yaml".

## A.3.5 Maf\_Provisioning\_EdgeResources API

For the purpose of referencing entities specified in this clause, it shall be assumed that the OpenAPI definitions are contained in a physical file named "TS26510\_Maf\_Provisioning\_EdgeResources.yaml".

## A.3.6 Maf\_Provisioning\_PolicyTemplates API

For the purpose of referencing entities specified in this clause, it shall be assumed that the OpenAPI definitions are contained in a physical file named "TS26510\_Maf\_Provisioning\_PolicyTemplates.yaml".

## A.3.7 Maf\_Provisioning\_ContentHosting API

For the purpose of referencing entities specified in this clause, it shall be assumed that the OpenAPI definitions are contained in a physical file named "TS26510\_Maf\_Provisioning\_ContentHosting.yaml".

## A.3.8 Maf\_Provisioning\_ContentPublishing API

For the purpose of referencing entities specified in this clause, it shall be assumed that the OpenAPI definitions are contained in a physical file named "TS26510\_Maf\_Provisioning\_ContentPublishing.yaml".

## A.3.9 Maf\_Provisioning\_MetricsReporting API

For the purpose of referencing entities specified in this clause, it shall be assumed that the OpenAPI definitions are contained in a physical file named "TS26510\_Maf\_Provisioning\_MetricsReporting.yaml".

## A.3.10 Maf\_Provisioning\_ConsumptionReporting API

For the purpose of referencing entities specified in this clause, it shall be assumed that the OpenAPI definitions are contained in a physical file named "TS26510\_Maf\_Provisioning\_ConsumptionReporting.yaml".

## A.3.11 Maf\_Provisioning\_EventDataProcessing API

For the purpose of referencing entities specified in this clause, it shall be assumed that the OpenAPI definitions are contained in a physical file named "TS26510\_Maf\_Provisioning\_EventDataProcessing.yaml".

# A.4 OpenAPI representation of Maf\_SessionHandling APIs

## A.4.1 Maf\_SessionHandling\_ServiceAccessInformation API

For the purpose of referencing entities specified in this clause, it shall be assumed that the OpenAPI definitions are contained in a physical file named "TS26510\_Maf\_SessionHandling\_ServiceAccessInformation.yaml".

## A.4.2 Maf\_SessionHandling\_DynamicPolicy API

For the purpose of referencing entities specified in this clause, it shall be assumed that the OpenAPI definitions are contained in a physical file named "TS26510\_Maf\_SessionHandling\_DynamicPolicy.yaml".

## A.4.3 Maf\_SessionHandling\_NetworkAssistance API

For the purpose of referencing entities specified in this clause, it shall be assumed that the OpenAPI definitions are contained in a physical file named "TS26510\_Maf\_SessionHandling\_NetworkAssistance.yaml".

## A.4.4 Maf\_SessionHandling\_MetricsReporting API

For the purpose of referencing entities specified in this clause, it shall be assumed that the OpenAPI definitions are contained in a physical file named "TS26510\_Maf\_SessionHandling\_MetricsReporting.yaml".

## A.4.5 Maf\_SessionHandling\_ConsumptionReporting API

For the purpose of referencing entities specified in this clause, it shall be assumed that the OpenAPI definitions are contained in a physical file named "TS26510\_Maf\_SessionHandling\_ConsumptionReporting.yaml".

Annex B (normative):  
Controlled vocabularies

# B.1 Media Delivery locator type

This controlled vocabulary is used to indicate the type of a locator in conjunction with the geofencing feature of the Content Hosting Configuration specified in clause 8.8.3.1.

Table B.1‑1: Media Delivey locator type controlled vocabulary

|  |  |  |
| --- | --- | --- |
| Term identifier | Term name | Semantic |
| urn:3gpp:media-delivery:locator-type:iso3166 | ISO 3166 administrative area | String representation of an ISO 3166‑1 alpha‑2 country code [ISO3166-1] (e.g. US, CN, KR, GB, FR) or an ISO 3166‑2 code [ISO3166-2] comprising an alpha‑2 country code and a country subdivision code valid for that country (e.g. US-CA, CN-GD, KR-26, GB-ENG, GB-WSM, FR-IDF, FR-75). |
| urn:3gpp:media-delivery:locatortype:trackingAreaCode | 3GPP Tracking Area Code | The Fully-Qualified Domain Name representation of a Tracking Area Code, as defined in clause 19.4.2.3 of TS 23.003 [23003]. |

Annex C (informative):  
Usage of TOS/DSCP for traffic identification

# C.1 General

This annex provides guidelines on the usage of the Type of Service (TOS) field of the IPv4 header or Traffic Class field of the IPv6 header for the purpose of traffic identification in the Media Delivery System as part of different features, such as Dynamic Policies and AF-based Network Assistance. The IP Packet Filter Set defined in TS 23.501 [23501] allows traffic filtering based on this field within the IP header.

# C.2 Differentiated Services/TOS-enabled Collaboration Scenarios

Differentiated Services (DS) as specified in RFC 2474 [RFC2474] is a scalable scheme for managing application traffic by classifying the traffic into a set of coarse-grained traffic classes. A *Differentiated Service (DS) domain* is a continuous set of DS-capable routers, which are operated with a common set of configurations. Each IP packet in a DS domain is marked and conditioned according to its traffic class. A 6-bit *DS Code Point* (DSCP) of the 8-bit differentiated services field (DS field) is used for marking. The DS field replaces the TOS field in the IPv4 packet headers and the Traffic Class field in the IPv6 header.

End host systems may mark IP packets with a specific DSCP value prior to transmission. DS-enabled routers treat the packet according to the DSCP value when performing routing operations on it. Border gateway routers typically mark packets with a DSCP value based on some traffic policy, overriding any value set by hosts.

NOTE: Usage of Differentiated Services across administrative borders is technically possible. The preservation of the DSCP field by networks between the MNO network and the external Data Networks hosting the Media Delivery functions is assumed to be governed by an SLA and by transport-level arrangements that are outside 3GPP scope. When the DSCP field is used only for traffic identification, preservation of the DSCP field could be achieved by using a tunnelling solution.

The RFCs defining Differentiated Services recommend a set of Per-Hop Behaviors (PHB), namely:

- *Default Forwarding (DF) PHB*, defined in section 4.1 of RFC 2474 [RFC2474], is used for traffic without special treatment.

- *Class Selector PHB*, defined in section 4.2.2.2 of RFC 2474 [RFC2474] is used for maintaining backwards compatibility with the IP precedence field of TOS.

- *Expedited Forwarding (EF) PHB*, defined by RFC 3246 [RFC3246], is dedicated to low loss or low latency traffic.

- *Assured Forwarding (AF) PHB*, defined by RFC 2597 [RFC2597], offers different levels of forwarding assurances.

The DS domain operator can also implement additional custom PHBs.

In the context of TOS-based traffic identification and separation, it is reasonable to assume the Data Network north of the UPF (N6) is DS-enabled. The 5G System is embedded in a larger DS domain, using same TOS values across multiple devices in order to provide Quality of Service Support like a DSCP-enabled link. However, it is not required to deploy DS capable routers for using in order to use the TOS field in the IP packet filter set for traffic identification.

According to clause 4.1 of TS 26.501 [26501], the 5GMS functions may be deployed within the trusted Data Network or an external Data network. As noted above, DS Code Points are often reset at network domain borders, but not always. There may be deployments e.g., with localized Edge Computing or with direct peering realizations, where the DSCP values can be used up to the Media AF and/or Media AS in an external Data Network. In this case, the logical DS domain is extended to include those externally-deployed Media Delivery functions.

Figure C.2-1 illustrates a deployment with a DS domain between the 5G System and the Media Delivery functions deployed in the external DN. (The model is also valid for deployments in which the Media Delivery functions both reside in the trusted DN.)



Figure C.2-1: Media Delivery System deployment within a DS domain

Figure C.2-2 illustrates a deployment with a DS domain between the 5G System and an externally deployed Media AS. The Media AF is deployed in the trusted DN.



Figure C.2-2: Media Delivery System deployment within a DS domain

# C.3 Procedure for using TOS Traffic Class for traffic identification

This call flow focuses on a scenario where both downlink and uplink traffic for a particular application flow within a PDU Session shared by several application flows needs to be mapped to a specific QoS Flow and handled separately by the 5G System. In this call flow, the Media Client initiates the QoS Flow establishment by using specific TOS values in the uplink traffic. A TOS-based QoS rule is already provisioned, so that the Uplink Traffic is mapped to the correct QoS Flow.

It is assumed here that the QoS flow should be used (e.g. for Premium QoS) as described in annex A of TS 26.501 [26501].



Figure C.3-1: High-level call flow for using TOS Traffic Class for traffic identification

Prerequisites:

- It is assumed that the Media Delivery System is already provisioned for Dynamic Policy usage as specified in clause 5.2.7 of the present document. As result, various functions of the 5G System are provisioned for QoS usage.

The steps are as follows:

1. The Media Delivery Client acquires Service Access Information (through reference points M8+M6 and/or M5 according to clause 5.3.2.3 of the present document), providing the information needed to use the Dynamic Policy API (see clause 5.3.3). Here, the sdfMethod indicates the usage of TOS.

2. The Media Delivery Client activates a Dynamic Policy (see clause 9.3). The serviceDataFlowDescriptions array contains objects of data type IpPacketFilterSet, where the srcIp, toSTc, dstIP properties are present. The filter for a bi-directional Service Data Flow requires two objects, one with direction set to in and one with direction set to out.

3. As a result of the previous step, the Media AF provisions the information for a Dynamic PCC rule with either the PCF or the NEF.

- When using the NEF AF Session with required QoS API, the TOS value is provided within the tosTC attribute within the FlowInfo data type.

- When using the PCF Policy Authorization Service API, the TOS value is provided within the tosTrCl attribution of the MediaSubComponent data type.

4. The PCF authorizes the request and creates a PCC rule. The PCF compiles and notifies the SMF about the PCC rule (containing the flow descriptions and providing parameters for policy control and/or charging control), has and the SMF forwards the QoS rule to the UE and (in the form of a PDR) to the UPF. The information contains, among other things, the QFI value and the TOS value.

During a media delivery session:

5. The Media Client initiates connection establishment by sending a TCP SYN packet. The TOS value in the TCP SYN packet is set by the Media Client to the same value as provided to the Media AF in earlier step 2.

6. The UE SDAP entity detects a matching TOS value in the uplink traffic.

7. The UE SDAP entity (Layer 2) encapsulates the IP packet into the according radio protocols, including the QFI marking.

8. The Media AS reads the TOS value from the uplink packet. The Media AS uses the uplink TOS value to mark all downlink packets in that TCP connection.

NOTE: When the 5G System employs an N6 NAT, the N6 NAT may set the downlink TOS value to the same value as the uplink TOS value.

9. The Media AS marks its acknowledgement IP packet (conveying the TCP SYN–ACK) with the same TOS value as the incoming packet.

10. The Media AS sends the TCP SYN–ACK packet back to the UE. The packet reaches the UPF on its path to the UE.

11. The UPF detects a match for the PDR rule configured in step 4 above containing the UE's IP address and TOS value.

12. The UPF encapsulates the downlink IP packet into an GTP‑U packet, and sets the QFI value in the GTP‑U packet header.

13. The UPF sends the GTP‑U-encapsulated packet to the RAN via reference point N3 and the RAN marks the QFI value in the SDAP layer, sending the packet to the UE. The UE SDAP entity (Layer 2) forwards the TCP SYN–ACK to the 5GMS Client.

14. The Media Client sends the TCP ACK (again with the TOS field set in the IP header) to complete the TCP connection handshake.

15. The UE SDAP entity (Layer 2) detects a TOS match for the UE.

16. The UE SDAP entity (Layer 2) encapsulates the IP packet into the according radio protocols, including the QFI marking.

The Media Client continues to use the established TCP connection.

Annex <D> (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Change history | | | | | | | |
| Date | Meeting | TDoc | CR | Rev | Cat | Subject/Comment | New version |
| 2023-08-24 | SA4#125 | S4-231500 |  |  |  | Initial document skeleton proposal. | 0.0.1 |
| 2023-10-24 | ad hoc post SA4#125 | S4aI230151 |  |  |  | Added assigned TS number to cover page.  Ported provisioning and session handling operations to clause 5. | 0.1.0 |
| 2023-11-03 | SA4#126 | S4-231638 |  |  |  | Resubmitted for discussion. | 0.2.0 |
| 2023-11-14 | SA4#126 | S4-231918 |  |  |  | Implemented pCRs:  S4-231637: Consumption reporting clarifications (tracking changes to TS 26.512 Rel‑17).  S4-231834: Content Publishing provisioning operations. | 0.3.0 |
| 2023-11-15 | SA4#126 | S4-231942 |  |  |  | Editorial fixes to porting from TS 26.512. | 0.3.1 |
| 2023-11-16 | SA4#126 | S4-232002 |  |  |  | Clean version for presentation to WG Closing Plenary. | 0.4.0 |
| 2024-01-08 | ad hoc post SA4#126 | S4aI230188 |  |  |  | * Comprehensive overhaul of HTTP error responses in clauses 5.2 and 5.3 to achieve uniformity across APIs. * 5G Core interactions ported to clause 5.5. * ANBR interactions ported to clause 5.6. * Common data types ported to clause 7.3.   + Added missing *sdfMethod* property to *Service‌Data‌Flow‌Description* data type. * Provisioning APIs ported to clause 8. * Network media session handling APIs ported to clause 9. * UE media session handling APIs ported to clause 10. | 1.0.1 |
| 2024-01-18 | ad hoc post SA4#126 | S4aI230209 |  |  |  | Clean version agreed as the basis of further work. | 1.0.2 |
| 2024-02-02 | SA4#127 | S4-240103 |  |  |  | S4-240099: API changes to support 3GPP Service URL.  S4-240100: Media delivery session identification and life-cycle.  S4-240101: Add provisioning Sessions enumeration operation.  S4-240102: *Maf\_SessionHandling* endpoint rationalisation.  S4-240373: Content Publishing Configuration.  S4-240374: Relax name space restriction on metrics reporting scheme identifier URIs.  S4-240380: Corrections on RAN-based metrics reporting.  S4-240382: Supplementary media distribution over MBS.  S4-240386: Traffic identification annex.  S4-240414: QoE metrics reporting range.  Alignment of clause 5.2.7.1 text with *M1QoSSpecification*.  Alignment of packet latency and loss data types with TS 29.114. | 1.1.0 |