

ETSI TS 126 512 V17.9.1 (2024-08)



**5G;
5G Media Streaming (5GMS);
Protocols
(3GPP TS 26.512 version 17.9.1 Release 17)**



Reference

RTS/TSGS-0426512vh91

Keywords

5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
ETSI [Search & Browse Standards application](#).

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#).

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2024.
All rights reserved.

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under <https://webapp.etsi.org/key/queryform.asp>.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights	2
Legal Notice	2
Modal verbs terminology.....	2
Foreword.....	10
1 Scope	12
2 References	12
3 Definitions of terms, symbols and abbreviations	14
3.1 Terms.....	14
3.2 Symbols.....	14
3.3 Abbreviations	14
4 Procedures for Downlink Media Streaming	15
4.1 General	15
4.2 APIs relevant to Downlink Media Streaming.....	16
4.3 Procedures of the M1 (5GMS Provisioning) interface	16
4.3.1 General.....	16
4.3.2 Provisioning Session procedures	17
4.3.2.1 General	17
4.3.2.2 Create Provisioning Session.....	17
4.3.2.3 Read Provisioning Session properties	17
4.3.2.4 Update Provisioning Session properties.....	17
4.3.2.5 Destroy Provisioning Session.....	17
4.3.3 Content Hosting Provisioning procedures	18
4.3.3.1 General	18
4.3.3.2 Create Content Hosting Configuration.....	18
4.3.3.3 Read Content Hosting Configuration properties	18
4.3.3.4 Update Content Hosting Configuration properties.....	18
4.3.3.5 Destroy Content Hosting Configuration.....	19
4.3.3.6 Purge Content Hosting cache	19
4.3.4 Content Protocols Discovery procedures	19
4.3.4.1 General	19
4.3.4.2 Create Content Protocols.....	19
4.3.4.3 Read Content Protocols.....	19
4.3.4.4 Update Ingest Protocols	19
4.3.4.5 Destroy Ingest Protocols	19
4.3.5 Content Preparation Template Provisioning procedures.....	20
4.3.5.1 General	20
4.3.5.2 Create Content Preparation Template	20
4.3.5.3 Read Content Preparation Template	20
4.3.5.4 Update Content Preparation Template	20
4.3.5.5 Destroy Content Preparation Template	20
4.3.6 Server Certificate Provisioning procedures	21
4.3.6.1 General	21
4.3.6.2 Create Server Certificate	21
4.3.6.3 Reserve Server Certificate.....	21
4.3.6.4 Retrieve Server Certificate.....	22
4.3.6.5 Upload Server Certificate.....	22
4.3.6.6 Update Server Certificate.....	23
4.3.6.7 Destroy Server Certificate.....	23
4.3.7 Dynamic Policy Provisioning procedures.....	23
4.3.7.1 General	23
4.3.7.2 Create Policy Template	24
4.3.7.3 Read Policy Template	24
4.3.7.4 Update Policy Template.....	24
4.3.7.5 Destroy Policy Template.....	24

4.3.8	Consumption Reporting Configuration procedures	25
4.3.8.1	General	25
4.3.8.2	Create Consumption Reporting Configuration.....	25
4.3.8.3	Read Consumption Reporting Configuration.....	25
4.3.8.4	Update Consumption Reporting Configuration.....	25
4.3.8.5	Destroy Consumption Reporting Configuration	25
4.3.9	Metrics Reporting Provisioning procedures	26
4.3.9.1	General	26
4.3.9.2	Create Metrics Reporting Configuration.....	26
4.3.9.3	Read Metrics Reporting Configuration	26
4.3.9.4	Update Metrics Reporting Configuration.....	26
4.3.9.5	Destroy Metrics Reporting Configuration.....	26
4.3.10	Edge Resources Provisioning Procedures.....	26
4.3.10.1	General	26
4.3.10.2	Create Edge Resources Provisioning Configuration	27
4.3.10.3	Read Edge Resources Provisioning Configuration	27
4.3.10.4	Update Edge Resources Provisioning Configuration	27
4.3.10.5	Destroy Edge Resources Provisioning Configuration	27
4.3.11	Event Data Processing Provisioning procedures.....	28
4.3.11.1	General	28
4.3.11.2	Create Event Data Processing Configuration.....	28
4.3.11.3	Read Event Data Processing Configuration	28
4.3.11.3A	Update Event Data Processing Configuration.....	28
4.3.11.4	Destroy Event Data Processing Configuration.....	28
4.4	Procedures of the M2d (5GMS content ingest) interface	29
4.5	Procedures of the M3d interface.....	29
4.6	Procedures of the M4d (Media Streaming) interface.....	29
4.6.1	Procedures for DASH Session.....	29
4.6.2	Procedures for Progressive Download Session.....	29
4.7	Procedures of the M5 (Media Session Handling) interface.....	30
4.7.1	Introduction.....	30
4.7.2	Procedures for Service Access Information.....	30
4.7.2.1	General	30
4.7.2.2	Create Service Access Information	30
4.7.2.3	Retrieve Service Access Information properties	30
4.7.2.4	Update Service Access Information properties	31
4.7.2.5	Destroy Service Access Information properties	31
4.7.3	Procedures for dynamic policy invocation.....	31
4.7.4	Procedures for consumption reporting.....	32
4.7.5	Procedures for metrics reporting.....	33
4.7.6	Procedures for network assistance	34
4.8	Procedures of the M6d (UE Media Session Handling) interface.....	34
4.8.1	General.....	34
4.8.2	Consumption reporting procedures.....	34
4.9	Procedures of the M7d (UE Media Player) interface	35
4.9.1	General.....	35
4.9.2	Metrics reporting procedures	35
4.10	Procedures of the M8d interface.....	35
4.11	Data collection and reporting procedures at reference point R4.....	35
4.11.1	General.....	35
4.11.2	5GMS AS data collection and reporting client configuration.....	35
4.11.3	5GMS AS data reporting	36
4.12	Event Exposure procedures at reference points R5 and R6.....	36
4.12.1	General.....	36
4.12.2	Event Exposure subscription procedure.....	37
4.12.3	Event Exposure unsubscription procedure.....	37
4.12.4	Event Exposure notification procedure.....	37
4.13	Procedures for downlink media streaming via eMBMS.....	37
5	Procedures for Uplink Media streaming	38
5.1	General	38
5.2	APIs relevant to Uplink Media Streaming	39

6	General aspects of APIs for 5G Media Streaming	40
6.1	HTTP resource URIs and paths	40
6.2	Usage of HTTP	40
6.2.1	HTTP protocol version	40
6.2.1.1	5GMS AF	40
6.2.1.2	5GMS AS	40
6.2.2	HTTP message bodies for API resources	40
6.2.3	Usage of HTTP headers	41
6.2.3.1	General	41
6.2.3.2	User Agent identification	41
6.2.3.2.1	Media Stream Handler identification	41
6.2.3.2.2	Media Session Handler identification	41
6.2.3.3	Server identification	41
6.2.3.3.1	5GMS AF identification	41
6.2.3.4	Support for conditional HTTP GET requests	42
6.2.3.5	Support for conditional HTTP POST, PUT, PATCH and DELETE requests	42
6.3	HTTP response codes	42
6.4	Common API data types	42
6.4.1	General	42
6.4.2	Simple data types	42
6.4.3	Structured data types	43
6.4.3.1	IpPacketFilterSet type	43
6.4.3.2	ServiceDataFlowDescription type	43
6.4.3.3	M5QoSSpecification type	43
6.4.3.4	M1QoSSpecification type	43
6.4.3.5	ChargingSpecification type	44
6.4.3.6	TypedLocation type	44
6.4.3.7	OperationSuccessResponse type	44
6.4.3.8	EdgeProcessingEligibilityCriteria type	45
6.4.3.9	EndpointAddress type	45
6.4.4	Enumerated data types	45
6.4.4.1	CellIdentifierType enumeration	45
6.4.4.2	SdfMethod enumeration	46
6.4.4.3	ProvisioningSessionType enumeration	46
6.4.4.4	EASRelocationTolerance enumeration	46
6.4.4.4	CacheStatus enumeration	46
6.5	Explanation of API data model notation	47
7	Provisioning (M1) APIs	48
7.1	General	48
7.2	Provisioning Sessions API	48
7.2.1	Overview	48
7.2.2	Resource structure	48
7.2.3	Data model	49
7.2.3.1	ProvisioningSession resource	49
7.3	Server Certificates Provisioning API	50
7.3.1	Overview	50
7.3.2	Resource structure	50
7.3.3	Data model	51
7.3.3.1	Certificate Signing Request	51
7.3.3.2	Server Certificate resource	51
7.3.4	Operations	51
7.4	Content Preparation Templates Provisioning API	52
7.4.1	Overview	52
7.4.2	Resource structure	52
7.4.3	Data model	52
7.4.4	Operations	52
7.5	Content Protocols Discovery API	53
7.5.1	Overview	53
7.5.2	Resource structure	53
7.5.3	Data model	53
7.5.3.1	ContentProtocols resource	53

7.5.3.2	ContentProtocolDescriptor type	53
7.6	Content Hosting Provisioning API	54
7.6.1	Overview	54
7.6.2	Resource structure	54
7.6.3	Data model	54
7.6.3.1	ContentHostingConfiguration resource	54
7.6.3.2	DistributionNetworkType enumeration	59
7.6.3.3	DistributionMode enumeration	59
7.6.4	Operations	59
7.6.4.1	Overview	59
7.6.4.2	Content caching	59
7.6.4.3	Cache purging	60
7.6.4.4	Content processing	60
7.6.4.5	URL signing	60
7.6.4.6	Geofencing	61
7.7	Consumption Reporting Provisioning API	62
7.7.1	Overview	62
7.7.2	Resource structure	62
7.7.3	Data model	62
7.7.3.1	ConsumptionReportingConfiguration resource	62
7.8	Metrics Reporting Provisioning API	63
7.8.1	Overview	63
7.8.2	Resource structure	63
7.8.3	Data model	64
7.8.3.1	MetricsReportingConfiguration resource	64
7.9	Policy Templates Provisioning API	65
7.9.1	Overview	65
7.9.2	Resource structure	66
7.9.3	Data model	67
7.9.3.1	PolicyTemplate resource	67
7.10	Edge Resources Provisioning API	68
7.10.1	General	68
7.10.2	Resource structure	68
7.10.3	Data model	69
7.10.3.1	EdgeResourcesConfiguration resource type	69
7.10.3.2	EdgeManagementMode enumeration	69
7.10.3.3	EASRequirements type	70
7.10.3.4	M1EASRelocationRequirements type	70
7.11	Event Data Processing Provisioning API	71
7.11.1	General	71
7.11.2	Resource structure	71
7.11.3	Data model	72
7.11.3.1	EventDataProcessingConfiguration resource type	72
8	Media Ingest and Publish (M2) protocols	72
8.1	General	72
8.2	HTTP pull-based content ingest protocol	72
8.3	DASH-IF push-based content ingest protocol	73
9	Internal (M3) APIs	73
10	Media Streaming (M4) APIs	74
10.1	General	74
10.2	DASH Distribution	74
11	Media Session Handling (M5) APIs	75
11.1	General	75
11.2	Service Access Information API	75
11.2.1	General	75
11.2.2	Resource structure	75
11.2.3	Data model	76
11.2.3.1	ServiceAccessInformation resource type	76
11.2.3.2	EASDiscoveryTemplate type	82

11.2.3.3	M5EASRelocationRequirements type	82
11.2.4	Operations.....	82
11.3	Consumption Reporting API	83
11.3.1	General.....	83
11.3.2	Reporting procedure	83
11.3.3	Report format.....	83
11.3.3.1	ConsumptionReport format.....	83
11.3.3.2	ConsumptionReportingUnit type	84
11.4	Metrics Reporting API	84
11.4.1	General.....	84
11.4.2	Reporting procedure	84
11.4.3	Report format.....	85
11.5	Dynamic Policies API	85
11.5.1	Overview	85
11.5.2	Resource structure.....	85
11.5.3	Data model.....	86
11.5.3.1	DynamicPolicy resource	86
11.5.4	Operations.....	86
11.6	Network Assistance API	87
11.6.1	Overview	87
11.6.2	Resource structure.....	87
11.6.3	Data model.....	88
11.6.3.1	NetworkAssistanceSession resource	88
11.6.4	Operations.....	88
11.6.4.1	Create Network Assistance session.....	88
11.6.4.2	Retrieve Network Assistance session.....	89
11.6.4.3	Request bit rate recommendation.....	89
11.6.4.4	Request delivery boost.....	89
11.6.4.5	Update Network Assistance session.....	90
11.6.4.6	Destroy Network Assistance session.....	90
12	UE Media Session Handling (M6) APIs for uplink and downlink.....	90
12.1	General	90
12.2	Media Session Handling for Downlink media streaming – APIs and Functions.....	91
12.2.1	Overview	91
12.2.2	Media Session Handler model	92
12.2.2.1	State model.....	92
12.2.2.2	Media Session Handler internal properties	92
12.2.2.3	Media Session Handler internal operations.....	92
12.2.2.4	Starting and Stopping a Media Session Handler	92
12.2.3	General.....	92
12.2.4	Dynamic Policy Information.....	93
12.2.5	Network Assistance Information	93
12.2.6	Consumption Reporting Information.....	93
12.2.7	Metrics Reporting Information	94
12.3	Media Session Handling for Uplink Streaming – APIs and Functions.....	94
13	UE Media Stream Handler (M7) APIs for uplink and downlink	94
13.1	General	94
13.2	DASH Media Player – APIs and Functions	95
13.2.1	Overview	95
13.2.2	Media Player model.....	96
13.2.3	Methods	97
13.2.3.1	General	97
13.2.3.2	Initialize	98
13.2.3.3	Attach.....	98
13.2.3.4	Pre-load	99
13.2.3.5	Play	100
13.2.3.6	Pause	101
13.2.3.7	Seek.....	101
13.2.3.8	Reset.....	102
13.2.3.9	Destroy.....	102

13.2.4	Configurations and settings API	103
13.2.5	Notifications and error events	104
13.2.6	Status Information	106
13.2.7	Usage of M7d Information by Media Session Handler	107
14	Application (M8) APIs for uplink and downlink	107
15	Miscellaneous UE-internal APIs	108
15.1	General	108
15.2	RAN Signaling-based Network Assistance API.....	108
15.3	RAN-based Metrics Reporting API.....	108
16	Usage of 5GC interfaces and APIs	109
16.1	General	109
16.2	Usage of N5/N33 for AF-based Network Assistance.....	109
16.3	Usage of N5/N33 for dynamic policies	110
17	Media Streaming data reporting at R4.....	111
17.1	General	111
17.2	MediaStreamingAccessRecord type.....	112
18	Event exposure at R5 and R6	113
Annex A (informative): 5GMS Parameter propagation for DASH Streaming		114
A.1	End-to-end model.....	114
A.2	Premium QoS dynamic policy	115
A.2.1	General	115
A.2.2	Procedure.....	117
A.2.3	Example parameters	118
A.3	(Conditional) Zero Rating dynamic policy.....	119
A.3.1	General	119
A.3.2	Procedure.....	120
A.3.3	Example parameters	121
A.4	Background Download.....	122
A.4.1	General	122
A.4.2	Procedure.....	123
A.4.3	Example parameters	124
Annex B (informative): Content Hosting Configuration examples		125
B.1	Pull-based content ingest example	125
B.1.1	Overview	125
B.1.2	Desired URL mapping.....	125
B.1.3	Content Hosting Configuration	125
B.2	Push-based content ingest example	126
B.2.0	Overview	126
B.2.1	Desired URL mapping.....	126
B.2.2	Content Hosting Configuration	126
Annex C (normative): OpenAPI representation of the 5GMS HTTP REST APIs.....		127
C.1	General	127
C.2	Data Types applicable to several APIs.....	127
C.3	OpenAPI representation of the M1 APIs	130
C.3.1	M1_ProvisioningSessions API.....	130
C.3.2	M1_ServerCertificatesProvisioning API.....	132
C.3.3	M1_ContentPreparationTemplatesProvisioning API	134
C.3.4	M1_ContentProtocolsDiscovery API.....	136
C.3.5	M1_ContentHostingProvisioning API	137
C.3.6	M1_ConsumptionReportingProvisioning API	141

C.3.7	M1_MetricsReportingProvisioning API.....	143
C.3.8	M1_PolicyTemplatesProvisioning API.....	145
C.3.9	M1_EdgeResourcesProvisioning API.....	147
C.3.10	M1_EventDataProcessingProvisioning API.....	150
C.4	OpenAPI representation of the M5 APIs	152
C.4.1	M5_ServiceAccessInformation API.....	152
C.4.2	M5_ConsumptionReporting API.....	155
C.4.3	M5_MetricsReporting API.....	156
C.4.4	M5_DynamicPolicies API.....	157
C.4.5	M5_NetworkAssistance API.....	159
C.5	OpenAPI representation of data reporting records.....	162
C.5.1	R4 data reporting records	162
Annex D (informative): 5GMS AF API index.....		164
Annex E (normative): Controlled vocabularies of 5G Media Streaming UE data parameters..		166
E.1	General	166
E.2	Controlled vocabularies of DASH QoE metrics reporting parameters	166
E.2.1	Reporting parameters for 3GP-DASH metrics.....	166
E.2.2	Reporting parameters for VR metrics.....	166
E.3	Controlled vocabulary of 5GMS consumption reporting parameters	167
E.4	Controlled vocabulary of 5GMS Network Assistance reporting parameters	167
E.5	Controlled vocabulary of 5GMS Dynamic Policy reporting parameters	167
E.6	Controlled vocabulary of 5GMS media access activity parameters.....	168
Annex F (Informative): 5GMS AS Certificate provisioning and discovery		171
F.1	General	171
F.2	5GMS AS discovery and media streaming access with a Server Certificate created by the 5GMS System.....	171
F.3	5GMS AS discovery and service access with a Server Certificate owned by the 5GMS Application Provider	174
Annex G (informative): Change history		177
History		179

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.

1 Scope

The present document specifies the set of protocols and APIs for 5G Media Streaming (5GMS) services based on the 5G Media Streaming Architecture (5GMSA). 5GMS supports services including MNO and third-party Downlink Media Streaming Services, and MNO and third-party Uplink Media Streaming Services.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".
- [2] 3GPP TS 26.501: "5G Media Streaming (5GMS); General description and architecture".
- [3] DASH Industry Forum, "Specification of Live Media Ingest", <https://dashif-documents.azurewebsites.net/Ingest/master/DASH-IF-Ingest.pdf>
- [4] 3GPP TS 26.247: "Transparent end-to-end Packet-switched Streaming Service (PSS); Progressive Download and Dynamic Adaptive Streaming over HTTP (3GP-DASH)".
- [5] Standard ECMA-262, 5.1 Edition: "ECMAScript Language Specification", June 2011.
- [6] IETF RFC 6234: "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)".
- [7] 3GPP TS 23.003: "Numbering, addressing and identification".
- [8] ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005: "Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks".
- [9] IETF RFC 7230: "Hypertext-Transfer Protocol (HTTP/1.1): Message Syntax and Routing".
- [10] IETF RFC 4648: "The Base16, Base32, and Base64 Data Encodings".
- [11] IEEE Standard 1003.1™, Issue 7: "The Open Group Base Specifications", 2018. <https://pubs.opengroup.org/onlinepubs/9699919799/>
- [12] 3GPP TS 29.571: "Common Data Types for Service Based Interfaces; Stage 3".
- [13] 3GPP TS 38.321: "NR; Medium Access Control (MAC) protocol specification".
- [14] 3GPP TS 36.321: "Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification".
- [15] 3GPP TS 27.007: "AT Command set for User Equipment (UE)".
- [16] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3", August 2018.
- [17] IETF RFC 7468: "Textual Encodings of PKIX, PKCS, and CMS Structures", April 2015.
- [18] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions — Part 1: Country codes".
- [19] ISO 3166-2: "Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision code".

- [20] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", May 2008.
- [21] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".
- [22] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition; Stage 3".
- [23] OpenAPI: "OpenAPI 3.0.0 Specification", <https://github.com/OAI/OpenAPI-Specification/blob/master/versions/3.0.0.md>.
- [24] IETF RFC 7230: "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".
- [25] IETF RFC 7231: "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".
- [26] IETF RFC 7232: "Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests".
- [27] IETF RFC 7233: "Hypertext Transfer Protocol (HTTP/1.1): Range Requests".
- [28] IETF RFC 7234: "Hypertext Transfer Protocol (HTTP/1.1): Caching".
- [29] IETF RFC 7235: "Hypertext Transfer Protocol (HTTP/1.1): Authentication".
- [30] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".
- [31] IETF RFC 7540: "Hypertext Transfer Protocol Version 2 (HTTP/2)".
- [32] ISO/IEC 23009-1: "Information technology; Dynamic adaptive streaming over HTTP (DASH) — Part 1: Media presentation description and segment formats".
- [33] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS); Stage 2".
- [34] 3GPP TS 29.514: "5G System; Policy Authorization Service; Stage 3".
- [35] 3GPP TS 26.511: "5G Media Streaming (5GMS); Profiles, codecs and formats".
- [36] Void.
- [37] 3GPP TS 26.244: "Transparent end-to-end packet switched streaming service (PSS); 3GPP file format (3GP)".
- [38] IETF RFC 8259: "The JavaScript Object Notation (JSON) Data Interchange Format", December 2017.
- [39] ISO 14496-12: "Information technology – Coding of audio-visual objects – Part 12: ISO base media file format".
- [40] ISO 23000-19: "Information technology – Coding of audio-visual objects – Part 19: Common media application format (CMAF) for segmented media".
- [41] IETF RFC 3986: "URI Generic Syntax".
- [42] 3GPP TS 26.118: "Virtual Reality (VR) profiles for streaming applications".
- [43] 3GPP TS 24.558: "Enabling Edge Applications; Protocol specification".
- [44] 3GPP TS 29.558: "Enabling Edge Applications; Application Programming Interface (API) specification; Stage 3".
- [45] 3GPP TS 23.502: "Procedures for the 5G System (5GS); Stage 2".
- [46] 3GPP TS 29.517: "5G System; Application Function Event Exposure Service; Stage 3".
- [47] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".
- [48] 3GPP TS 26.531: "Data Collection and Reporting; General Description and Architecture".
- [49] 3GPP TS 26.532: "Data Collection and Reporting; Protocols and Formats".

- [50] 3GPP TS 29.522: "5G System. Network Exposure Function Northbound APIs; Stage 3".
- [51] 3GPP TS 26.346: "Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs".
- [52] 3GPP TS 26.347: "Multimedia Broadcast/Multicast Service (MBMS); Application Programming Interface and URL".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

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

3.2 Symbols

Void.

3.3 Abbreviations

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

5GMS	5G Media Streaming
5GMSd	5GMS downlink
5GMSu	5GMS uplink
5GMSA	5GMS Architecture
5GMS EAS	Edge-enabled 5GMS Application Server
BMFF	(ISO) Base Media File Format
ABR	Adaptive Bit Rate
ACR	Application Context Relocation
AF	Application Function
ANBR	Access Network Bit rate Recommendation
AS	Application Server
CDN	Content Delivery Network / Content Distribution Network
CGI	Cell Global Identifier
CMAF	Common Media Application Format
CRUD	Create, Read, Update, Delete
CNAME	Canonical Name
CORS	Cross-Origin Resource Sharing
CRL	Certificate Revocation List
DASH	Dynamic Adaptive Streaming over HTTP
DER	Distinguished Encoding Rule
DNN	Domain Name News
DNS	Domain Name Server
EAS	Edge Application Server
ECGI	E-UTRAN Cell Global Identifier
ECMA	European Computer Manufacturers Association
EES	Edge Enabler Server
FQDN	Fully Qualified Domain Name
GPSI	Generic Public Subscription Identifier
HLS	HTTP Live Streaming
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
LCID	Logical Channel Identifier
MFBR	Maximum Flow Bit Rate

MIME	Multipurpose Internet Mail Extensions
MNO	Mobile Network Operator
MPD	Media Presentation Description
MSISDN	Mobile Subscriber ISDN number
NCGI	NR Cell Global Identifier
NEF	Network Exposure Function
OAM	Operations, Administration and Maintenance
PCC	Policy Control and Charging
PCF	Policy Control Function
PEM	Privacy-Enhanced Mail
PFD	Packet Flow Description
PFDF	Packet Flow Description Function
QoE	Quality of Experience
QoS	Quality of Service
SDF	Service Data Flow
SHA	Secure Hash Algorithm
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Coordinated Universal Time

4 Procedures for Downlink Media Streaming

4.1 General

This clause defines all procedures for Downlink Media Streaming using the different 5G Media Streaming Reference Points.

NOTE: The descriptions of certain M1 interface procedures in clause 4.3, and of certain M5 interface procedures in clause 4.7, indicate applicability of those procedures to both downlink and uplink media streaming. This avoids redundant duplication of normative text in clause 5, regarding M1 and M5 procedures for uplink media streaming.

4.2 APIs relevant to Downlink Media Streaming

Table 4.2-1 summarises the APIs used to provision and use the various downlink media streaming features specified in TS 26.501 [2].

Table 4.2-1: Summary of APIs relevant to downlink media streaming features

5GMSd feature	Abstract	Relevant APIs		
		Interface	API name	Clause
Content protocols discovery	Used by the 5GMSd Application Provider to interrogate which content ingest protocols are supported by 5GMSd AS(s).	M1d	Content Protocols Discovery API	7.5
Content hosting	Content is ingested, hosted and distributed by the 5GMSd AS according to a Content Hosting Configuration associated with a Provisioning Session.	M1d	Provisioning Sessions API	7.2
			Server Certificates Provisioning API	7.3
			Content Preparation Templates Provisioning API	7.4
			Content Hosting Provisioning API	7.6
		M2d	HTTP-pull based content ingest protocol	8.2
		M2d	DASH-IF push based content ingest protocol	8.3
		M4d	DASH [4] or 3GP [37]	10
		M5d	Service Access Information API	11.2
Metrics reporting	The 5GMSd Client uploads metrics reports to the 5GMSd AF according to a provisioned Metrics Reporting Configuration it obtains from the Service Access Information for its Provisioning Session.	M1d	Provisioning Sessions API	7.2
			Metrics Reporting Provisioning API	7.8
		M5d	Service Access Information API	11.2
			Metrics Reporting API	11.4
Consumption reporting	The 5GMSd Client provides feedback reports on currently consumed content according to a provisioned Consumption Reporting Configuration it obtains from the Service Access Information for its Provisioning Session.	M1d	Provisioning Sessions API	7.2
			Consumption Reporting Provisioning API	7.7
		M5d	Service Access Information API	11.2
			Consumption Reporting API	11.3
Dynamic Policy invocation	The 5GMSd Client activates different traffic treatment policies selected from a set of Policy Templates configured in its Provisioning Session.	M1d	Provisioning Sessions API	7.2
			Policy Templates Provisioning API	7.9
		M5d	Service Access Information API	11.2
			Dynamic Policies API	11.5
Network Assistance	The 5GMSd Client requests bit rate recommendations and delivery boosts from the 5GMSd AF.	M5d	Service Access Information API	11.2
			Network Assistance API	11.6
Edge content processing	Edge resources are provisioned for processing content in 5GMS downlink media streaming sessions.	M1d	Provisioning Sessions API	7.2
			Edge Resources Provisioning API	7.10
		M5d	Service Access Information API	11.2
5GMS via eMBMS	The 5GMSd AF provisions the delivery of content via eMBMS.	M1d	Provisioning Sessions API	7.2
		M5d	Service Access Information API	11.2
		M4d	DASH [4] or 3GP [37] or HLS	10
UE data collection, reporting and exposure	UE data related to downlink 5G Media Streaming is reported to the Data Collection AF instantiated in the 5GMSd AF for exposure to Event consumers.	M1d	Event Data Processing Provisioning API	7.11
		R4	<i>Ndcaf_DataReporting</i> service	17
		R5, R6	<i>Naf_EventExposure</i> service	18

4.3 Procedures of the M1 (5GMS Provisioning) interface

4.3.1 General

A 5GMS Application Provider may use the procedures in this clause to provision the network for media streaming sessions that are operated by that 5GMS Application Provider. For downlink media streaming, these sessions may be DASH streaming sessions, progressive download sessions, or any other type of media streaming or distribution (e.g.

HLS) sessions. For uplink media streaming, the content format and delivery protocol are defined by the 5GMSu Application Provider, and may be either non-fully standardized or employ standardized HTTP-based streaming of ISO BMFF content fragments as profiled by CMAF [39].

The M1 interface offers three different sets of procedures:

- For downlink media streaming, configuration of content ingest at M2d for onward distribution by the 5GMSd AS over M4d or via other distribution systems such as eMBMS: designed as an API that is equivalent to the functionality of a public CDN. For uplink media streaming, configuration of content ingest at M2u for the media content received by the 5GMSu AS from the 5GMSu Client over M4u. The resource types involved in content hosting configuration are provisioning session (see clause 4.3.2), content hosting procedures (see clause 4.3.3), ingest protocols (see clause 4.3.4), content preparation template (see clause 4.3.5), and server certificates (see clause 4.3.6).
- Configuration of dynamic policies: allows the configuration of Policy Templates at M5 that can be applied to M4 downlink/uplink media streaming sessions.
- Configuration of reporting: permits the MNO to collect, at M5, QoE metrics and consumption reports about M4 downlink sessions, as well as permits the MNO to collect, at M5, QoE metrics reports about M4 uplink sessions.

A 5GMS Application Provider may use any of these procedures, in any combination, to support its media streaming sessions.

4.3.2 Provisioning Session procedures

4.3.2.1 General

Prior to configuring content hosting, dynamic policies, or reporting, the 5GMS Application Provider shall create a new Provisioning Session. The following CRUD operations are used to manage a provisioning session.

4.3.2.2 Create Provisioning Session

This procedure is used by the 5GMS Application Provider to create a new Provisioning Session. The 5GMS Application Provider shall use the HTTP `POST` method to create a new Provisioning Session. Upon successful creation, the 5GMS AF shall respond with a `201 (Created)` response message that includes the resource identifier of the newly created Provisioning Session in the body of the reply and the URL of the resource, including its resource identifier, shall be returned as part of the HTTP `Location` header field.

4.3.2.3 Read Provisioning Session properties

This procedure is used by the 5GMS Application Provider to obtain the properties of the Provisioning Session from the 5GMS AF. The 5GMS Application Provider uses the `GET` method for this purpose.

4.3.2.4 Update Provisioning Session properties

The Update operation is not allowed on Provisioning Sessions.

4.3.2.5 Destroy Provisioning Session

This procedure is used by the 5GMS Application Provider to destroy a Provisioning Session. The 5GMS AF will release any associated resources, purge any cached data, delete all QoS and reporting configurations associated with this Provisioning Session. The 5GMS AF shall use the HTTP `DELETE` method for this purpose.

4.3.3 Content Hosting Provisioning procedures

4.3.3.1 General

These procedures are used by the 5GMSd Application Provider and the 5GMSd AF on M1d to provision the content hosting feature for downlink streaming.

4.3.3.2 Create Content Hosting Configuration

This procedure is used by the 5GMSd Application Provider to create a new Content Hosting Configuration. The 5GMSd Application Provider shall use the HTTP `POST` method for this purpose and the request message body shall include a *ContentHostingConfiguration* resource, as specified in clause 7.6.3.1.

- 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 5GMSd Application Provider in the request message body. The 5GMSd 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 5GMSd AF and returned in the response message body. It shall not be set by the 5GMSd Application Provider in the request message body.

In all cases, the *DistributionConfiguration.baseURL* property is read-only: it shall be omitted from the creation request and shall be assigned by the 5GMSd AF, allowing the value to be inspected by the 5GMSd Application Provider in the returned *ContentHostingConfiguration* resource representation, or by using the procedure specified in clause 4.3.3.3 below.

If the procedure is successful, the 5GMSd AF shall generate a resource identifier representing the new Content Hosting Configuration. In this case, the 5GMSd AF shall respond with a `201 (Created)` HTTP response message and shall provide the URL to the newly created resource in the `Location` header field. The response message body may include a *ContentHostingConfiguration* resource (see clause 7.6.3.1) that represents the current state of the Content Hosting Configuration, including any fields set by the 5GMSd AF.

When both properties are set in a given distribution configuration by the 5GMSd Application Provider, it is a requirement that the value of *domainNameAlias* matches one of the Subject Alternative Names in the Server Certificate resource referenced by *certificateId* (allowing for wildcard matching). When the *certificateId* property is set, if the *domainNameAlias* does not match one of the Subject Alternative Names in the Server Certificate, the 5GMSd AF shall respond with a `400 (Bad Request)` response message.

If the procedure is otherwise unsuccessful, the 5GMSd AF shall provide a response code as defined in clause 6.3.

4.3.3.3 Read Content Hosting Configuration properties

This procedure is used by the 5GMSd Application Provider to obtain the properties of an existing Content Hosting Configuration resource from the 5GMSd AF. The HTTP `GET` method shall be used for this purpose.

If the procedure is successful, the 5GMSd AF shall respond with a `200 (OK)` response message that includes the *ContentHostingConfiguration* resource in the response message body.

If the procedure is not successful, the 5GMSd AF shall provide a response code as defined in clause 6.3.

4.3.3.4 Update Content Hosting Configuration properties

The update operation is invoked by the 5GMSd Application Provider to modify the properties of an existing *ContentHostingConfiguration* resource. All writable properties except *domainNameAlias* may be updated. The HTTP `PATCH` or HTTP `PUT` methods shall be used for the update operation.

If the procedure is successful, the 5GMSd AF shall respond with a `200 (OK)` and provide the content of the resource in the response, confirming the successful update operation.

When both properties are set in a given distribution configuration by the 5GMSd Application Provider, it is a requirement that the value of *domainNameAlias* matches one of the Subject Alternative Names in the Server Certificate

resource referenced by *certificateId* (allowing for wildcard matching). When the *certificateId* is set, if the *domainNameAlias* does not match one of the Subject Alternative Names in the Server Certificate, the 5GMSd AF shall respond with a *400 (Bad Request)* response message.

If the procedure is otherwise unsuccessful, the 5GMSd AF shall provide a response code as defined in clause 6.3.

4.3.3.5 Destroy Content Hosting Configuration

This operation is used by the 5GMSd Application Provider to destroy a Content Hosting Configuration resource and to terminate the related distribution. The HTTP `DELETE` method shall be used for this purpose. As a result, the 5GMSd AF will release any associated network resources, purge any cached content, and delete any corresponding configurations.

If the procedure is successful, the 5GMSd AF shall respond with a *200 (OK)* response message.

If the procedure is not successful, the 5GMSd AF shall provide a response code as defined in clause 6.3.

4.3.3.6 Purge Content Hosting cache

This operation is used by the 5GMSd Application Provider to purge content from the 5GMSd 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, as specified in clause 7.6.4.3. As a result, the 5GMSd AF purges any cached content whose URL matches the specified regular expression.

If the procedure is successful, the 5GMSd AF shall respond with a *200 (OK)* response message.

If the procedure is not successful, the 5GMSd AF shall provide a response code as defined in clauses 6.3 and 7.6.4.3.

4.3.4 Content Protocols Discovery procedures

4.3.4.1 General

The set of downlink content ingest or uplink content egest protocols supported by the 5GMS AS at interface M2 is described by the *ContentProtocols* resource at M1, as specified in clause 7.5.3.1.

4.3.4.2 Create Content Protocols

The Create operation is not permitted for the *ContentProtocols* resource.

4.3.4.3 Read Content Protocols

This procedure is used by the 5GMS Application Provider to retrieve a list of content ingest protocols supported by the 5GMS AS. The HTTP `GET` method shall be used for this purpose.

If the procedure is successful, the 5GMS AF shall respond with a *200 (OK)* response that includes a *ContentProtocols* resource in the response message body, as specified in clause 7.5.3.1. If the procedure is not successful, the 5GMS AF shall provide a response code as defined in clause 6.3.

4.3.4.4 Update Ingest Protocols

The Update operation is not permitted for the *ContentProtocols* resource.

4.3.4.5 Destroy Ingest Protocols

The Delete operation is not permitted for the *ContentProtocols* resource.

4.3.5 Content Preparation Template Provisioning procedures

4.3.5.1 General

For downlink media streaming, the 5GMSd AS may be required to process content ingested at interface M2d before serving it on interface M4d. For uplink media streaming, the 5GMSu AS may be required to process content it receives from the 5GMSu Client before passing it to the 5GMSu Application Provider on the egest interface M2u. The content processing operations are specified in a Content Preparation Template resource, as specified in clause 7.4.2.

4.3.5.2 Create Content Preparation Template

This procedure is used by the 5GMS Application Provider to register a new Content Preparation Template with a Provisioning Session. The 5GMS Application Provider shall use the HTTP `POST` method to upload a new Content Preparation Template resource. The MIME content type of the Content Preparation Template shall be supplied in the `Content-Type` HTTP request header.

Upon successful creation, the 5GMS AF shall respond with a *201 (Created)* response message and the URL of the newly created resource, including its resource identifier, shall be returned as part of the HTTP `Location` header field.

If the MIME content type indicated in `Content-Type` is not acceptable to the 5GMS AF, the creation of the Content Preparation Template resource shall fail with HTTP error response status code *415 (Unsupported Media Type)*.

If the 5GMS AF is unable to provision the resources indicated in the supplied Content Preparation Template, the creation operation shall fail with an HTTP response status code of *503 (Service Unavailable)*.

If the procedure is otherwise unsuccessful, the 5GMS AF shall provide a response code as defined in clause 6.3.

4.3.5.3 Read Content Preparation Template

This procedure is used by the 5GMS Application Provider to download a copy of a Content Preparation Template resource from the 5GMS AF. The 5GMS Application Provider shall use the `GET` method for this purpose.

If the procedure is successful, the 5GMS AF shall respond with *200 (OK)* and shall provide 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.

If the procedure is not successful, the 5GMS AF shall provide a response code as defined in clause 6.3.

4.3.5.4 Update Content Preparation Template

The update procedure is used by the 5GMS Application Provider to modify or replace an existing Content Preparation Template resource. The HTTP `PATCH` or HTTP `PUT` methods shall be used for the update operation.

If the procedure is successful, the 5GMS AF shall respond with a *200 (OK)* and provide the content of the resource in the response, reflecting the successful update operation.

If the MIME content type indicated in `Content-Type` is not acceptable to the 5GMS AF, the creation of the Content Preparation Template resource shall fail with HTTP error response status code *415 (Unsupported Media Type)*.

If the 5GMS AF is unable to provision the resources indicated in the supplied Content Preparation Template, the update operation shall fail with an HTTP response status code of *503 (Service Unavailable)*.

If the procedure is otherwise unsuccessful, the 5GMS AF shall provide a response code as defined in clause 6.3.

4.3.5.5 Destroy Content Preparation Template

This operation is used by the 5GMS Application Provider to destroy a Content Preparation Template resource. The HTTP `DELETE` method shall be used for this purpose.

If the procedure is successful, the 5GMS AF shall respond with a *200 (OK)* response message.

If the procedure is not successful, the 5GMS AF shall provide a response code as defined in clause 6.3. If the Content Preparation Template is in use as part of a Content Hosting Configuration, the procedure shall fail with HTTP error response status code 409 (*Conflict*).

4.3.6 Server Certificate Provisioning procedures

4.3.6.1 General

Each X.509 server certificate [8] presented by the 5GMSd AS at reference point M4d or at reference point xMB-U is represented by a Server Certificate resource at M1d. The Server Certificates Provisioning API as specified in clause 7.3 enables a Server Certificate resource to be created within the scope of a Provisioning Session, and subsequently referenced by a Content Hosting 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 5GMS System operator on behalf of the 5GMSd Application Provider; the other in which a certificate is generated by the 5GMSd Application Provider from a Certificate Signing Request solicited from the 5GMSd AF. Both methods shall be supported by implementations of the 5GMSd AF.

NOTE: As a consumer of media from the 5GMSd AS in a combined architecture using 5GMS and eMBMS, the BM-SC needs to be able to trust the content it is receiving comes from a bona fide source. This issue is left to implementation.

4.3.6.2 Create Server Certificate

This procedure is used by the 5GMSd Application Provider to request that the 5GMS System generates a new X.509 certificate [8] on its behalf within the scope of a Provisioning Session. In this case, the certificate's Common Name (CN) is assigned in a domain under the control of the 5GMSd 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 5GMSd Application Provider shall use the HTTP POST method to create a new Server Certificate resource. Upon successful creation, the 5GMSd AF shall respond with a 201 (*Created*) response message and the URL of the resource, including its resource identifier, shall be returned in the HTTP Location header. The response message body may optionally include a copy of the X.509 certificate corresponding to the newly created Server Certificate resource, as specified in clause 7.3.3.2.

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 4.3.6.4 below for more details.

If the procedure is not successful, the 5GMSd AF shall provide a response code as defined in clause 6.3.

When the Server Certificate resource is subsequently referenced by a Content Hosting Configuration in the scope of the same Provisioning Session, the 5GMSd AF shall ensure that the canonical domain name of the 5GMSd AS is a Fully-Qualified Domain Name (FQDN) that matches the Common Name and the first Subject Alternative Name in the referenced Server Certificate resource.

4.3.6.3 Reserve Server Certificate

This procedure is used by the 5GMSd Application Provider to solicit a Certificate Signing Request (CSR) from the 5GMSd AF for the purpose of generating an X.509 certificate [8] independently of the 5GMSd System. In this case, the certificate's Common Name (CN) is assigned in a domain under the control of the 5GMSd 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 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 5GMSd 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 [20]), to resolve to the address of a 5GMSd AS in the target 5GMS System.

The 5GMSd Application Provider may specify additional domains in its certificate reservation request to the 5GMSd 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 [20]). In this case, the 5GMSd Application Provider is responsible for ensuring that any FQDN aliases it provisions in Content Hosting Configurations matching these additional domains resolve to the canonical domain name of the 5GMSd AS in the target 5GMS System.

The 5GMSd Application Provider shall use the HTTP `POST` method to create a new Server Certificate. Upon successful creation of the resource, the 5GMSd AF shall respond with a `201 (Created)` response message and the URL of the resource, including its resource identifier, shall be returned in the HTTP `Location` header. The `Content-Type` response header and the body of the HTTP response message shall be as specified in clause 7.3.3.1.

If the procedure is not successful, the 5GMSd AF shall provide a response code as defined in clause 6.3.

4.3.6.4 Retrieve Server Certificate

This procedure is used by the 5GMSd Application Provider to download a Server Certificate resource for inspection. The HTTP `GET` method shall be used for this purpose. If the requested resource exists and is populated with an X.509 certificate [8], the 5GMSd AF shall respond with `200 (OK)` and shall return the requested Server Certificate in accordance with clause 7.3.3.2.

In the case where the X.509 certificate was provisioned by the 5GMSd System on behalf of the 5GMSd Application Provider according to clause 4.3.6.2 above, the HTTP response `503 (Service Unavailable)` 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 5GMSd Application Provider from a Certificate Signing Request obtained according to clause 4.3.6.3 above, the HTTP response `204 (No Content)` shall be returned until such time as the X.509 certificate has been uploaded using the procedure specified in clause 4.3.6.5 below.

4.3.6.5 Upload Server Certificate

This procedure is used by a 5GMSd Application Provider to upload an X.509 certificate [8] that it has generated in response to a Certificate Signing Request solicited using the reservation procedure specified in clause 4.3.6.3 above. The HTTP `PUT` method shall be used for this purpose. The `Content-Type` request header and the body of the HTTP request message shall be as specified in clause 7.3.3.2.

The 5GMSd AF shall verify that the party originating the upload is the same party that reserved the Server Certificate resource using the procedure specified in clause 4.3.6.3 above before accepting the supplied X.509 certificate. The 5GMSd 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 on either count, the HTTP response `403 (Forbidden)` shall be returned.

Attempting to upload an X.509 certificate to a Server Certificate resource that has not been reserved shall elicit a `404 (Not Found)` HTTP response.

When the Server Certificate resource is subsequently referenced by a Content Hosting Configuration in the scope of the same Provisioning Session, the 5GMS Application Provider shall set the *domainNameAlias* property of all distribution configurations to a Fully-Qualified Domain Name (FQDN) that matches one of the Subject Alternative Names in the referenced Server Certificate resource.

NOTE: Even if multiple distribution configurations in the same Content Hosting Configuration reference the same Server Certificate resource, they may each choose a different matching domain name alias.

4.3.6.6 Update Server Certificate

Updating a previously uploaded Server Certificate is not permitted for security reasons. Any attempt to do so using the PUT method shall result in the HTTP response 405 (*Method Not Allowed*).

To supply a replacement X.509 certificate, for example when a previously supplied certificate is shortly due to expire, the 5GMSd Application Provider should instead use one of the procedures specified in clause 4.3.6.2 or 4.3.6.3 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.

4.3.6.7 Destroy Server Certificate

This procedure is used to remove a Server Certificate resource from a Provisioning Session. The HTTP DELETE method shall be used for this purpose. On success, the HTTP response 200 (*OK*) or 204 (*No content*) shall be returned and afterwards the identifier of the Service Certificate resource is no longer valid.

Only the party that created (see clause 4.3.6.2) or reserved (see clause 4.3.6.3) 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 if an attempt is made to destroy a Server Certificate resource that is currently referenced by a Content Hosting Configuration resource.

Attempting to destroy a Server Certificate resource that has been reserved but never uploaded shall elicit a 200 (*OK*) HTTP response. In this case, the 5GMSd AF should release any resources associated with the reservation.

If the procedure is not successful, the 5GMSd AF shall provide a response code as defined in clause 6.3.

4.3.7 Dynamic Policy Provisioning procedures

4.3.7.1 General

These procedures are used by the 5GMS Application Provider to configure the Policy Templates for streaming sessions of a particular Provisioning Session.

Figure 4.3.7.1-1 below is a state diagram showing the life-cycle of a Policy Template resource.

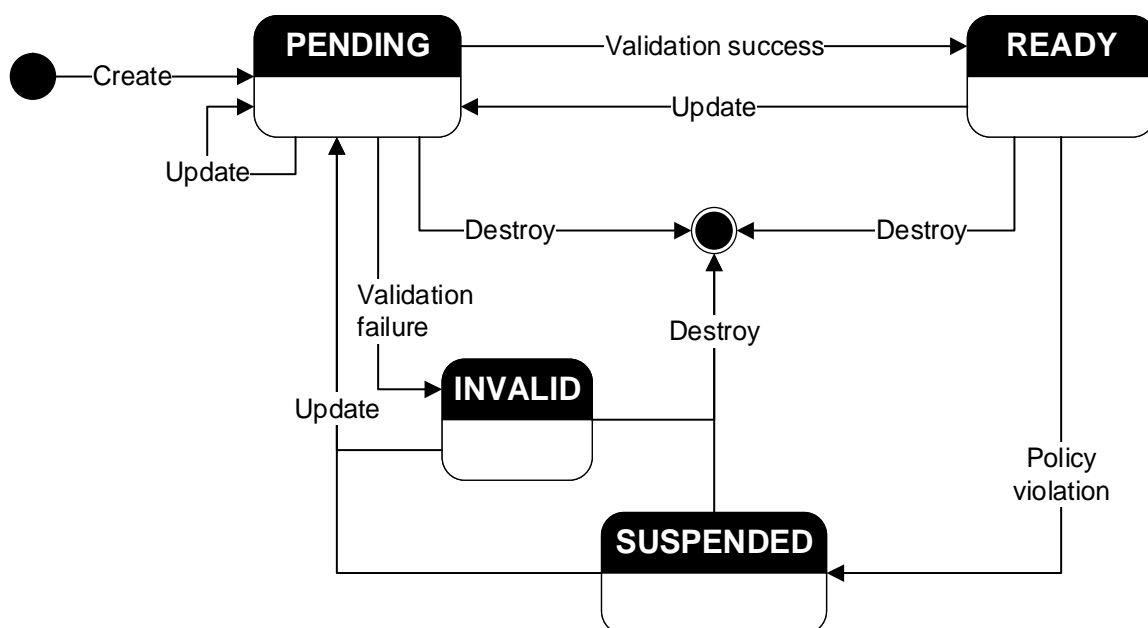


Figure 4.3.7.1-1: Policy Template Resource State Diagram

Since Policy Templates require 5GMS System operator verification, a Policy Template resource that is newly created cannot be used immediately. Upon creation, a Policy Template resource shall be in the *PENDING* state. Once all mandatory properties are provided, the 5GMS AF triggers validation. If the Policy Template is not deemed to be valid by the operator of the 5GMS System, it shall move to the *INVALID* state, from where it can be updated to remedy the defect. Once it has been successfully validated by the 5GMS System operator, a Policy Template resource shall take the *READY* state, indicating that it may be applied to media streaming sessions. If it is subsequently updated by the 5GMS Application Provider, a Policy Template resource shall return to the *PENDING* state, awaiting revalidation by the operator of the 5GMS System. Finally, a Policy Template resource may be *SUSPENDED* by the 5GMS 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 into *PENDING* and triggers revalidation.

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

The 5GMS 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 5GMS 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.

4.3.7.2 Create Policy Template

This procedure is used by the 5GMS Application Provider to create a new Policy Template resource. The HTTP `POST` method shall be used for this purpose.

If the procedure is successful, the 5GMS AF shall generate a resource identifier to uniquely identify the newly created Policy Template resource. In that case, it shall respond with a *201 (Created)* HTTP response message and provide the URL to the newly created resource in the `Location` header field.

If the procedure is not successful, the 5GMS AF shall provide a response code as defined in clause 6.3.

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.

4.3.7.3 Read Policy Template

This procedure is used by the 5GMS Application Provider and other 5GMS AFs to query the properties of an existing Policy Template resource from the 5GMS AF. The HTTP `GET` method shall be used for this purpose.

If the procedure is successful, the 5GMS AF shall respond with a *200 (OK)* response that includes a copy of the Policy Template resource in the response message body.

If the procedure is not successful, the 5GMS AF shall provide a response code as defined in clause 6.3.

4.3.7.4 Update Policy Template

The update operation is invoked by the 5GMS Application Provider to modify the properties of an existing Policy Template resource. All available properties except *state* may be updated. The HTTP `PATCH` or HTTP `PUT` methods shall be used for the update operation.

Any update to the Policy Template resource will change its state back to *PENDING*, which makes it temporarily unusable. If all mandatory property values have been provided, the Policy Template is eligible for revalidation.

If the procedure is successful, the 5GMS AF shall respond with a *200 (OK)* response message that includes a copy of the Policy Template resource in the response message body. Modifications to read-only properties, such as changes to the state of a Policy Template, shall be rejected with a *403 (Forbidden)* HTTP response.

If the procedure is not successful, the 5GMS AF shall provide a response code as defined in clause 6.3.

4.3.7.5 Destroy Policy Template

This operation is used by the 5GMS Application Provider to destroy a Policy Template resource. The HTTP `DELETE` method shall be used for this purpose. As a result, the 5GMS AF will remove the Policy Template from any Provisioning Sessions that reference it.

Currently active media streaming sessions using the destroyed Policy Template, if any exist, shall be stopped by the removal of the Policy Template.

If the procedure is successful, the 5GMS AF shall respond with a *200 (OK)* response message.

If the procedure is not successful, the 5GMS AF shall provide a response code as defined in clause 6.3.

4.3.8 Consumption Reporting Configuration procedures

4.3.8.1 General

These procedures are used by the 5GMSd Application Provider to activate and to configure consumption reporting. This clause defines the basic procedures. More details are provided in clause 7.7.

4.3.8.2 Create Consumption Reporting Configuration

This procedure is used by the 5GMSd Application Provider to activate consumption reporting for a particular Provisioning Session. The 5GMSd Application Provider shall use the HTTP `POST` method to activate the consumption reporting procedure and to transmit the Consumption Reporting Configuration to the 5GMSd AF. Upon successful operation, the 5GMSd AF shall respond with a *201 (Created)* response message and the same resource URL shall be returned in the `Location` header field.

If the procedure is not successful, the 5GMSd AF shall provide a response code as defined in clause 6.3.

4.3.8.3 Read Consumption Reporting Configuration

This procedure is used by the 5GMSd Application Provider to obtain the current Consumption Reporting Configuration from the 5GMSd AF. The 5GMSd Application Provider uses the `GET` method for this purpose.

4.3.8.4 Update Consumption Reporting Configuration

The update operation is invoked by the 5GMSd 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 the update operation.

If the procedure is successful, the 5GMSd AF shall respond with a *200 (OK)* reflecting the successful update operation.

If the procedure is not successful, the 5GMSd AF shall provide a response code as defined in clause 6.3.

4.3.8.5 Destroy Consumption Reporting Configuration

This operation is used by the 5GMSd Application Provider to terminate the related consumption reporting procedure. The HTTP `DELETE` method shall be used for this purpose. As a result, the 5GMSd AF will release any associated resources, purge any cached data, and delete any corresponding configurations.

If the procedure is successful, the 5GMSd AF shall respond with a *200 (OK)* response message. If the procedure is not successful, the 5GMSd AF shall provide a response code as defined in clause 6.3.

4.3.9 Metrics Reporting Provisioning procedures

4.3.9.1 General

These procedures are used by the 5GMS Application Provider to configure QoE metrics reporting functionality associated with downlink or uplink media streaming. This clause defines the basic procedures. More details are provided in clause 7.8.3.1.

A given instance of a Metrics Reporting Configuration resource is identified by the *metricsReportingConfigurationId* property of the *MetricsReportingConfiguration* resource. The properties of that resource, as described in clause 7.8.3.1, pertain to metrics collection and reporting by the Media Session Handler to the 5GMS AF.

4.3.9.2 Create Metrics Reporting Configuration

This procedure is used by the 5GMS Application Provider to create a Metrics Reporting Configuration resource for a particular Provisioning Session. The 5GMS Application Provider shall use the HTTP `POST` method for this purpose and the request message body may include a *MetricsReportingConfiguration* resource, as specified in clause 7.8.3.1. Upon successful operation, the 5GMS AF shall respond with a `201 (Created)` response message and the resource URL for the newly-created Metrics Reporting Configuration resource shall be returned in the `Location` header field. If the procedure is unsuccessful, the 5GMS AF shall provide a response code as defined in clause 6.3.

This procedure may be performed multiple times to provision different Metrics Reporting Configurations in the scope of a particular Provisioning Session. Each such configuration resource is represented by a different value of *metricsReportingConfigurationId*.

4.3.9.3 Read Metrics Reporting Configuration

This procedure is used by the 5GMS Application Provider to obtain the properties of an existing Metrics Reporting Configuration resource from the 5GMS AF. The 5GMS Application Provider shall use the `GET` method for this purpose. If successful, the 5GMS AF shall respond with a `200 (OK)` and the requested *MetricsReportingConfiguration* resource (see clause 7.8.3.1) shall be returned in the body of the HTTP response message. If the procedure is unsuccessful, the 5GMS AF shall provide a response code as defined in clause 6.3.

4.3.9.4 Update Metrics Reporting Configuration

The update operation is invoked by the 5GMS Application Provider to initially upload the Metrics Reporting Configuration resource, or in the case of an existing Metrics Reporting Configuration resource, to entirely replace or modify certain properties of that resource. All available properties may be updated. The HTTP `PATCH` or HTTP `PUT` methods shall be used for the update operation.

If the procedure is successful, the 5GMS AF shall respond with a `200 (OK)` reflecting the successful update operation. If the procedure is unsuccessful, the 5GMS AF shall provide a response code as defined in clause 6.3.

4.3.9.5 Destroy Metrics Reporting Configuration

This operation is used by the 5GMS Application Provider to destroy a Metrics Reporting Configuration resource and to terminate the related metrics reporting procedure. The HTTP `DELETE` method shall be used for this purpose. As a result, the 5GMS AF should release any associated resources, discard any pending metrics reports, and delete any corresponding configurations.

If the procedure is successful, the 5GMS AF shall respond with a `200 (OK)` response message. If the procedure is unsuccessful, the 5GMS AF shall provide a response code as defined in clause 6.3.

4.3.10 Edge Resources Provisioning Procedures

4.3.10.1 General

These procedures are used by the 5GMS Application Provider and the 5GMS AF at reference point M1d to provision edge resources for downlink streaming.

NOTE: The requirements on an edge-enabled 5GMS AF are defined in clause 4.5.2 of TS 26.501 [2].

4.3.10.2 Create Edge Resources Provisioning Configuration

This procedure is used by the 5GMS Application Provider to create a new Edge Resources Provisioning Configuration. The 5GMS Application Provider shall use the HTTP POST method for this purpose and the request message body shall include an *EdgeResourcesConfiguration* resource, as specified in clause 7.10.3.1.

- If the *edgeManagementMode* is set to *EM_AF_DRIVEN* (indicating AF-driven edge resource management), the 5GMS AF is responsible for requesting and managing the required edge resources and for handling EAS relocation in relation to media streaming 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 5GMS AF shall only request edge resources based on requests from the EEC instantiated in the Media Session Handler at reference point EDGE-1.

If the procedure is successful, the 5GMS AF shall generate a resource identifier representing the new Edge Resources Provisioning Configuration. In this case, the 5GMS AF shall respond with a *201 (Created)* HTTP response message and shall provide the URL to the newly created resource in the *Location* header field. The response message body may include an *EdgeResourcesConfiguration* resource (see clause 7.10.3.1) that represents the current state of the Edge Resources Provisioning Configuration, including any fields set by the 5GMS AF.

If the procedure is not successful, the 5GMS AF shall provide a response code as defined in clause 6.3.

4.3.10.3 Read Edge Resources Provisioning Configuration

This procedure is used by the 5GMS Application Provider to retrieve the current values of the properties of an existing Edge Resources Provisioning Configuration resource from the 5GMS AF. The HTTP GET method shall be used for this purpose.

If the procedure is successful, the 5GMS AF shall respond with a *200 (OK)* response message that includes the *EdgeResourcesConfiguration* resource in the response message body.

If the procedure is not successful, the 5GMS AF shall provide a response code as defined in clause 6.3.

4.3.10.4 Update Edge Resources Provisioning Configuration

The update operation is invoked by the 5GMS Application Provider to modify the properties of an existing *EdgeResourcesConfiguration* resource. All writeable properties except *edgeManagementMode* may be updated. The HTTP PATCH or HTTP PUT methods shall be used for the update operation.

If the procedure is successful, the 5GMS AF shall respond with a *200 (OK)* and provide the content of the resource in the response, confirming the successful update operation.

If the procedure is not successful, the 5GMS AF shall provide a response code as defined in clause 6.3.

4.3.10.5 Destroy Edge Resources Provisioning Configuration

This operation is used by the 5GMS Application Provider to destroy an Edge Resources Provisioning Configuration resource. The HTTP DELETE method shall be used for this purpose. This operation makes the configuration unusable for future media streaming sessions, but it does not affect any ongoing media streaming sessions.

If the procedure is successful, the 5GMS AF shall respond with a *200 (OK)* response message.

If the procedure is not successful, the 5GMS AF shall provide a response code as defined in clause 6.3.

4.3.11 Event Data Processing Provisioning procedures

4.3.11.1 General

These procedures are used by the 5GMS Application Provider to configure the collection and processing of UE data related to 5G Media Streaming over reference point M1 (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 5GMS AF (as defined in clause 4.7 of TS 26.501 [2]) with one or more Event Data Processing Configurations and Data Access Profiles for a particular Event ID.

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 5GMS event data are the NWDAF, the Event Consumer AF and the NEF.

The Event Data Processing Provisioning API is specified in clause 7.11.

4.3.11.2 Create Event Data Processing Configuration

This procedure is used by the 5GMS Application Provider to create a new Event Data Processing Configuration in the form of one or more Data Access Profiles. The 5GMS Application Provider shall use the HTTP POST method for this purpose and the request message body shall include an *EventDataProcessingConfiguration* resource, as specified in clause 7.11.3.

If the procedure is successful, the 5GMS AF shall generate a resource identifier representing the new Event Data Processing Configuration. In this case, the 5GMS AF shall respond with a 201 (*Created*) response message and shall provide the URL to the newly created resource in the `Location` header field.

If the procedure is unsuccessful, the 5GMS AF shall provide a response code as defined in clause 6.3.

4.3.11.3 Read Event Data Processing Configuration

This procedure is used by the 5GMS Application Provider to obtain the properties of an existing Event Data Processing Configuration resource from the 5GMS AF. The HTTP GET method shall be used for this purpose.

If the procedure is unsuccessful, the 5GMS AF shall provide a response code as defined in clause 6.3.

4.3.11.3A Update Event Data Processing Configuration

This operation is invoked by the 5GMS 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.

If the operation is successful, the 5GMS AF shall respond with 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 procedure is not successful, the 5GMS AF shall provide a response code as defined in clause 6.3.

4.3.11.4 Destroy Event Data Processing Configuration

This operation is used by the 5GMS Application Provider to destroy an existing Event Data Processing Configuration resource and to terminate the related distribution. The HTTP DELETE method shall be used for this purpose. 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.

If the procedure is successful, the 5GMS AF shall respond with a 200 (*OK*) response message.

If the procedure is unsuccessful, the 5GMS AF shall provide a response code as defined in clause 6.3.

4.4 Procedures of the M2d (5GMS content ingest) interface

The following 5GMS AS content ingest protocols are specified by the present document at reference point M2d to support downlink media streaming:

- An *HTTP pull-based content ingest protocol* is specified in clause 8.2, including specific handling for HTTP redirects issued to the 5GMS AS by the 5GMS Application Provider's origin server.
- A *DASH-IF push-based content ingest protocol* is specified in clause 8.3.

4.5 Procedures of the M3d interface

Interface M3d is internal and no procedures on this interface are specified.

4.6 Procedures of the M4d (Media Streaming) interface

4.6.1 Procedures for DASH Session

This procedure is used by a 5GMSd Client to establish a DASH session via the M4d interface. In order to establish such a session, the 5GMSd AS shall host an MPD as defined in ISO/IEC 23009-1 [32] or TS 26.247 [4] and the MPD URL is known to the 5GMSd Client typically using M8d.

The Media Player receives an MPD URL from the 5GMSd-Aware Application through M7d by methods defined in clause 13. The Media Player shall send an HTTP GET message to the 5GMSd AS including the URL of the MPD resource. On success, the 5GMSd AS shall respond with a 200 (OK) message that includes the requested MPD resource.

Additional procedures for reactions to different HTTP status codes are provided in TS 26.247 [4], clause A.7 and ISO/IEC 23009-1 [32] clause A.7.

Additional procedures for handling partial file responses are provided in TS 26.247 [4], clause A.9.

This information is provided through M7d to the application for selection. In addition, the currently used service description parameters are provided as status information through M7d in order for the Media Session Handler to make use of this information, for example for Dynamic Policy and Network Assistance.

The detailed handling of service description information is documented in clause 13.2 of the present document.

4.6.2 Procedures for Progressive Download Session

This procedure is used by a 5GMSd client to establish a Progressive Download session via the M4d interface. In order to establish such a session, the 5GMSd AS shall host a 3GP/MP4 file as defined in TS 26.247 [4]. The 3GP/MP4 URL is known to the Media Player (in this case a progressive download player), typically by using M8d.

The Media Player receives a URL from the 5GMSd-Aware Application through M7d by methods defined in clause 13. The Media Player shall send an HTTP GET message to the 5GMSd AS including the URL of the 3GP/MP4 resource. On success, the 5GMSd AS shall respond with a 200 (OK) message that includes the requested 3GP/MP4 resource.

Additional procedures for reactions to different HTTP status codes are provided in TS 26.247 [4].

4.7 Procedures of the M5 (Media Session Handling) interface

4.7.1 Introduction

The M5 APIs are used by a Media Session Handler within a 5GMS Client to invoke services relating to downlink or uplink media streaming at the 5GMS AF.

4.7.2 Procedures for Service Access Information

4.7.2.1 General

Service Access Information is the set of parameters and addresses needed by the 5GMSd Client to activate reception of a downlink media streaming session or by a 5GMSu Client to activate an uplink media streaming session for contribution. The data model of the *ServiceAccessInformation* resource acquired by the Media Session Handler of the 5GMS Client is shown in clause 11.2.3. Service Access Information additionally includes configuration information to allow the Media Session Handler to invoke procedures for dynamic policy (see clause 4.7.3), consumption reporting (clause 4.7.4), metrics reporting (clause 4.7.5) and network assistance (clause 4.7.6).

For downlink media streaming, the Media Session Handler may obtain Service Access Information from either the 5GMSd-Aware Application (via M6d) or the 5GMSd AF (via M5d). In the former case, the Service Access Information is initially acquired by the 5GMSd-Aware Application from the 5GMSd Application Provider via M8d. In the latter case, the Service Access Information is derived by the 5GMSd AF from the Provisioning Session established via M1d.

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 Player and is handed to the Media Player through M7d.

If an Edge Resources Configuration with client-driven management (*EM_CLIENT_DRIVEN*) is provisioned in the applicable Provisioning Session, the 5GMSd AF shall convey the *ClientEdgeResourcesConfiguration* to the Media Session Handler (via M5d) as part of the Service Access Information.

NOTE: The requirements on an edge-enabled Media Session Handler are defined in clause 4.5.2 of TS 26.501 [2].

For downlink media streaming exclusively via eMBMS and for hybrid 5GMSd/eMBMS services as defined in clauses 5.10.2 and 5.10.5 respectively of TS 26.501 [2], the Service Access Information indicates that the 5GMSd Client acts as an MBMS-Aware Application.

For dynamically provisioned downlink media streaming via eMBMS as defined in clause 5.10.6 of TS 26.501 [2], the 5GMSd AS creates a presentation manifest that is regularly polled by the Media Player for a potential update. When an eMBMS User Service carrying the 5GMSd content is dynamically provisioned or removed by the 5GMSd AF, the 5GMSd AS shall update the presentation manifest with the locations where the updated manifest and the media segments are now available, for example to add or change to the media server in the MBMS Client.

For uplink media streaming, the 5GMSu Client may obtain Service Access Information from either the 5GMSu-Aware Application (via M6u/M7u) or the 5GMSu AF (via M5u). In the former case, the Service Access Information is initially acquired by the 5GMSu-Aware Application from the 5GMSu Application Provider via M8u. In the latter case, the Service Access Information is derived by the 5GMSu AF from the Provisioning Session established via M1u.

This clause specifies the procedures whereby the 5GMS Client fetches Service Access Information from the 5GMS AF.

4.7.2.2 Create Service Access Information

The Create operation is not allowed on Service Access Information.

4.7.2.3 Retrieve Service Access Information properties

This procedure shall be used by the Media Session Handler to acquire Service Access Information from the 5GMS AF. The Media Session Handler uses the GET method for this purpose.

The downlink or uplink media streaming session for which the Media Session Handler is requesting data is identified by a unique reference contained in the path of the URL, as specified in clause 11.2.2.

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 containing either:

- an *If-None-Match* request header with the value of the entity tag (*ETag*) that was returned with the most recently acquired *ServiceAccessInformation* resource; or else
- an *If-Modified-Since* request header with the *Last-Modified* value of that most recently acquired resource.

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 procedure.

4.7.2.4 Update Service Access Information properties

The Update operation is not allowed on Service Access Information.

4.7.2.5 Destroy Service Access Information properties

The Destroy operation is not allowed on Service Access Information.

4.7.3 Procedures for dynamic policy invocation

This procedure is used by a Media Session Handler to manage Dynamic Policy Instance resources via the M5 interface. A dynamic policy invocation consists of a Policy Template Id, flow description(s), a 5GMS Application Service Configuration Id and potentially other parameters, according to TS 26.501 clause 5.7.

A Policy Template Id identifies the desired Policy Template to be applied to an application flow. A Policy Template includes properties such as specific QoS (e.g. background data) or different charging treatments. The 5GMS AF combines the information from the Policy Template with dynamic information from the Media Session Handler to gather a complete set of parameters to invoke the N33 or N5 API call. The Policy Template may contain for example the AF identifier.

The flow description allows the identification and classification of the media traffic, such as the packet filter sets given in clause 5.7.6 of [2].

In order to instantiate a new dynamic policy, the Media Session Handler shall first create a resource for the Dynamic Policy Instance on the 5GMS AF. When the Media Session Handler needs several dynamic policies, it repeats the step as often as needed.

The Media Session Handler creates a new Dynamic Policy Instance by sending an HTTP POST message to the 5GMS AF. The body of the HTTP POST message shall include a Provisioning Session Id, the Policy Template Id and the Service Data Flow description. The Service Data Flow description identifies the actual application flow(s) to be policed according to the Policy Template. If the operation is successful, the 5GMS AF creates a new resource URL representing the Dynamic Policy Instance. In this case, the 5GMS AF shall respond to the Media Session Handler with a 201 *Created* HTTP response message, including the URL for the newly created Dynamic Policy Instance resource as the value of the *Location* header field.

When the Dynamic Policy Instance is successfully instantiated, the 5GMS AF triggers the creation of a corresponding policy in the 5G System. Depending on the selected *sdfMethod*, the 5GMS AF fills in a *flowDescription* object and / or provides an application identifier referring to a *PF*D (Packet Flow Description) object containing the domain name.

NOTE 1: It is not defined in this Release how a 5GMS AF in an external Data Network provides an application identifier.

NOTE 2: It is not defined in this Release how a 5GMS AF in an external Data Network selects a specific DNN or S-NSSAI. The Media Session Handler can modify the parameters of an existing Dynamic Policy Instance resource using either the HTTP PUT or PATCH methods, as appropriate to the desired update. The 5GMS AF shall trigger the appropriate actions towards other Network Functions like PCF or NEF when all information is set.

The Media Session Handler can destroy a Dynamic Policy Instance resource using the HTTP DELETE method. As a result, the 5GMS AF shall trigger the appropriate actions towards other Network Functions like PCF or NEF to remove the associated PCC rule.

4.7.4 Procedures for consumption reporting

These procedures are used by the Media Session Handler and the Consumption Reporting functions of the 5GMSd Client to submit a consumption report via the M5d interface if Consumption Reporting is applied for a downlink streaming session.

The Service Access Information indicating whether Consumption Reporting is provisioned for downlink streaming sessions is described in clause 11.2.3. When the *clientConsumptionReportingConfiguration.samplePercentage* value is 100, the Media Session Handler shall activate the consumption reporting procedure. If the *samplePercentage* is less than 100, 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 report 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 5GMSd AF when any of the following conditions occur:

- Start of consumption of a downlink media streaming session;
- Stop of consumption of a downlink media streaming session;
- Upon determining the need to report ongoing 5GMS consumption at periodic intervals determined by the *clientConsumptionReportingConfiguration.reportingInterval* property.
- Upon determining a location change, if the *clientConsumptionReportingConfiguration.locationReporting* property is set to *True*.
- Upon determining an access network change (e.g., unicast to eMBMS, or *vice versa*), if the *clientConsumptionReportingConfiguration.accessReporting* property is set to *True*.

Whenever a consumption report is produced, the Media Session Handler shall reset its reporting interval timer to the value of the *clientConsumptionReportingConfiguration.reportingInterval* property and it shall begin countdown of the timer again. Whenever the Media Session Handler stops the consumption of a downlink streaming session, it shall disable its reporting interval timer.

In order to submit a consumption report, the Media Session Handler shall send an HTTP POST message to the 5GMSd AF. If several 5GMSd AF addresses are listed in the *clientConsumptionReportingConfiguration.serverAddresses* array (see table 11.2.3.1-1), the Media Session Handler shall choose one at random and shall send the consumption report to the selected server endpoint. The request body shall be a *ConsumptionReport* structure, as specified in clause 11.3.3.1. The server shall respond with a 200 (OK) message to acknowledge successful processing of the consumption report.

NOTE: If the connection via M5d for consumption reporting is temporarily unavailable, the consumption reports are expected to be stored on the UE for some time until connectivity to the 5GMSd AF is restored and sent later to the 5GMSd AF as a collection. Details are left to implementation.

The Consumption Reporting API, defining the data formats and structures and related procedures for consumption reporting, is described in clause 11.3.

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 5GMS 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 5GMS AF at the end of the downlink media streaming session therefore describes the last media consumed.

The location(s) of the UE when the media was consumed shall be included in the consumption reporting unit if the *locationReporting* property in the Client Consumption Reporting Configuration is set to *True*.

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 [7]. Otherwise, the reporting client identifier should be represented by a stable and globally unique string.

4.7.5 Procedures for metrics reporting

The M5 procedures for QoE metrics reporting pertain to the combination of the provisioning of metrics collection and reporting in the Media Session Handler using relevant Service Access Information, and the sending of collected metrics by the Media Session Handler to the 5GMS AF in accordance with the configured metrics scheme(s). A metrics scheme may be 3GPP-defined or non-3GPP-defined.

When the metrics collection and reporting feature is activated for a downlink media streaming session, one or more metrics configuration sets, each associated with a metrics scheme, may be provided to the 5GMS Client. A given metrics configuration set contains information such as the 5GMS AF address(es) to which metrics are to be sent by the Media Session Handler, metrics reporting interval, target percentage of media streaming sessions for which reports should be sent, and the set of metrics to be collected and reported. See TS 26.501 [2] for additional details.

For progressive download and DASH streaming services, the listed metrics in a given metrics configuration set are associated with the 3GPP metrics scheme and shall correspond to one or more of the metrics as specified in clauses 10.3 and 10.4, respectively, of TS 26.247 [4]. Metrics related to virtual reality media, as specified in clause 9.3 of TS 26.118 [42], may also be listed in the metrics configuration. Metrics related to eMBMS delivery, as specified in clause 9.4.6 of TS 26.346 [51], may also be listed in the metrics configuration.

Whenever a metrics report is produced for a given metrics 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 stops the consumption of a downlink streaming session, it shall disable its reporting interval timer for all metrics configurations.

In order to submit a metrics report, the Media Session Handler shall send an HTTP *POST* message to the 5GMS AF. If several 5GMS AF addresses are listed in the *clientMetricsReportingConfigurations[].serverAddresses* array (see table 11.2.3.1-1), the Media Session Handler shall choose one at random and shall send the metrics report to the selected server endpoint. The request body shall be formatted according to the metrics scheme indicated in *clientMetricsReportingConfigurations[].scheme* (see table 11.2.3.1-1), as specified in clause 11.4.3. The server shall respond with a *200 (OK)* message to acknowledge successful processing of the metrics report.

NOTE: If the connection via M5 for metrics reporting is temporarily unavailable, the metrics reports are expected to be stored on the UE for some time until connectivity to 5GMS AF is restored and sent later to the 5GMS AF as a collection. Details are left to implementation.

Details of the metrics reporting API are provided in clause 11.4, and for 3GP-DASH based downlink media streaming services, the 3GPP-defined metrics reporting scheme and metrics report format are defined in clause 11.4.3.

A reporting client identifier may be included in the metrics report. If available to the Media Session Handler, its value should be a GPSI value as defined by TS 23.003 [7]. Otherwise, the reporting client identifier should be represented by a stable and globally unique string.

4.7.6 Procedures for network assistance

These procedures are used by the 5GMS Client to request Network Assistance from one of the 5GMS AF instances listed in the *networkAssistanceConfiguration.serverAddresses* property of the Service Access Information resource retrieved using the procedure in clause 4.7.2.3. Details of the APIs supporting these procedures are specified in clause 11.6.

The 5GMS Client first creates a Network Assistance Session with its chosen 5GMS AF instance. It provides information that will later be used by the 5GMS 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 5GMS Client. This procedure is further specified in clause 11.6.4.1.

The *NetworkAssistanceSession* resource may be retrieved by the Media Session Handler using the procedure specified in clause 11.6.4.2.

When a Network Assistance Session is created, the responding 5GMS AF instance may nominate an MQTT endpoint URL in the *NetworkAssistanceSession.notificationURL* property. The Media Session Handler may subscribe to the MQTT channel provided at this endpoint and receive notifications with an up-to-date bit rate recommendation whenever this changes.

At any time after the Network Assistance Session resource is created, the 5GMS Client may use the Network Assistance Session identifier to explicitly request a bit rate recommendation by invoking a remote procedure call provided for this purpose by the 5GMS AF. This procedure is further specified in clause 11.6.4.3.

Using the Network Assistance identifier, the 5GMS 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 5GMS AF. This procedure is further specified in clause 11.6.4.4.

The information provided when first creating a Network Assistance Session may be modified subsequently by the Media Session Handler using the session modification procedure specified in clause 11.6.4.5.

In order to terminate a Network Assistance Session, the 5GMS Client deletes the Network Assistance session resource. This procedure is further specified in clause 11.6.4.6.

4.8 Procedures of the M6d (UE Media Session Handling) interface

4.8.1 General

This clause contains the procedures for the interaction between the 5GMSd-Aware application or the Media Player and the Media Session Handler through the M6d API. Details are provided in clause 12.

4.8.2 Consumption reporting procedures

Before a streaming session is started, the Media Session Handler shall check if the Service Access Information contains any Consumption reporting configuration, as specified in clause 4.7.3. If such a configuration is present, the Media Session Handler shall initiate consumption reporting based on this configuration for the current streaming session.

The Media Session Handler shall first determine whether consumption reporting is active for the session. The determination shall be based on the *samplePercentage* attribute specified in the consumption reporting configuration. When the *samplePercentage* is not present or its value is 100, consumption reporting is active for the session. If the *samplePercentage* is less than 100, the Media Session Handler generates a random number which is uniformly distributed in the range 0 to 100; consumption reporting is active for the session when the generated random number is of a lower value than the *samplePercentage* value.

If consumption reporting for this session is active, the Media Session Handler shall regularly determine the consumption reporting parameters defined in clause 11.3.2.4 from the Media Player through the M7d interface and shall report these values according to the *reportingInterval* specified in the Client Consumption Reporting Configuration.

4.9 Procedures of the M7d (UE Media Player) interface

4.9.1 General

This clause contains the procedures for the interaction between the 5GMSd-Aware Application or the Media Session Handler and the Media Player through the M7d API. Details are provided in clause 13.

4.9.2 Metrics reporting procedures

These procedures shall be used by the Media Session Handler function to control metrics reporting when such reporting is configured via metadata sent in-band via the media manifest.

When a streaming session is started, the Media Session Handler shall check if the manifest contains any metrics configuration, as specified in TS 26.247 clauses 10.4 and 10.5, or TS 26.118 [42] clause 9.3. If such a configuration is found, the Media Session Handler shall use it for the current streaming session.

The Media Session Handler shall first determine whether metrics from this session shall be reported. The determination shall be based on the *samplePercentage* attribute specified in the metrics configuration, according to TS 26.247 clause 10.5.

If metrics are reported for the session, the Media Session Handler shall request the Media Player to create a metrics collection job. The Media Player 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 collector job with the set of metrics which shall be collected during the session. The format of the configuration shall be according to TS 26.247 clause L.2, but note that 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 Player according to the *reportingInterval* specified in the metrics configuration. The metrics returned by the Media Player shall use the format as described in TS 26.247 clause 10.6, and (for virtual reality media) in TS 26.118 [42] clause 9.4 and the Media Session Handler shall forward these to the server address(es) specified in the metrics configuration using the specified *DNN* according to the procedures described in TS 26.247 clause 10.6.

When the session is finished the Media Session Handler shall delete the metrics collection job.

4.10 Procedures of the M8d interface

This clause defines basic procedures for M8d.

No specific procedures are defined but it is expected that the 5GMSd Application Provider can provide media session entry points to a 5GMSd-Aware Application through M8d. The 5GMSd-Aware Application would then initiate the media session by providing such an entry point to the 5GMSd Client through M7d.

4.11 Data collection and reporting procedures at reference point R4

4.11.1 General

These procedures are used by the 5GMS AS, as a type of data collection client, to acquire its data collection and reporting client configuration from, and subsequently report media streaming access activity to, the Data Collection AF instantiated in the 5GMS AF. It does so by invoking the *Ndcnf_DataReporting* service offered by the Data Collection AF at reference point R4, as specified in clause 7 of TS 26.532 [49].

4.11.2 5GMS AS data collection and reporting client configuration

The 5GMS AS shall use the service operations and procedures specified in TS 26.532 [49] to obtain its data collection and reporting client configuration from the Data Collection AF instantiated in the 5GMS AF at reference point R4:

- In the case where both the 5GMS AS and the 5GMS AF reside in the trusted domain, the 5GMS AS shall obtain its data collection client configuration directly from the Data Collection AF by invoking appropriate *Ndcnf_DataReporting* service operations as specified in clause 7.2 of [49] according to the procedures specified in clauses 4.2.5 of [49].
- Should the 5GMS AS and the 5GMS AF reside in different trust domains, the 5GMS AS shall instead obtain its configuration from the Data Collection AF indirectly via the NEF by invoking the equivalent operations on the *Nnef_DataReporting* service as defined in TS 26.531 [48].

In both cases, the 5GMS AS shall declare that it supports the *MS_ACCESS_ACTIVITY* data reporting domain in *DataReportingSession.supportedDomains* (see clauses 7.2.3.2.1 and 7.2.3.3.1 of TS 26.532 [49]) and the Data Collection AF instantiated in the 5GMS AF shall request reporting for this domain by including the same value as a key to the *DataReportingSession.reportingConditions* dictionary. The value of the *ReportingCondition.type* property at this key shall be *INTERVAL*, *THRESHOLD* or *OFF*.

No data packaging strategies are specified in this release for the data reporting domains associated with the 5GMS AS at reference point R4.

Default data packaging strategies for the data reporting domains associated with the 5GMS AS at reference point R4 are not specified in this release.

The 5GMS AS shall refresh its data collection and reporting client configuration according to the procedures specified in clause 4.2.5.3 of TS 26.532 [49].

4.11.3 5GMS AS data reporting

The 5GMS AS shall use the service operations and procedures specified in TS 26.532 [49] to report media streaming access activity to the Data Collection AF instantiated in the 5GMS AF at reference point R4:

- In the case where both the 5GMS AS and the 5GMS AF reside in the trusted domain, the 5GMS AS shall submit media streaming access activity reports directly to the Data Collection AF by invoking appropriate *Ndcnf_DataReporting* service operations as specified in clause 7.3 of [49] according to the procedures specified in clauses 4.2.7 of [49].
- Should the 5GMS AS and the 5GMS AF reside in different trust domains, the 5GMS AS shall instead submit media streaming access activity reports indirectly to the 5GMS AF via the NEF by invoking the equivalent operations on the *Nnef_DataReporting* service as defined in TS 26.531 [48].

In both cases, the conditions for sending a downlink media streaming access activity report by the 5GMSd AS and the parameters of such report are signalled in the data collection and reporting client configuration obtained using the procedure specified in clause 4.11.2.

In order to submit a media streaming access activity report, the 5GMS AS shall send an HTTP `POST` message to the Data Collection AF instantiated in the 5GMS AF. The request body shall be a JSON document of type *DataReport* (as defined in clause 7.3.3.2.1 of TS 26.532 [49]) containing one or more *MediaStreamingAccessRecord* structures, as specified in clauses 17.2 and C.5.1 of the present document.

The Data Collection AF shall respond with a `200 (OK)` message to acknowledge successful processing of the media streaming access activity report.

4.12 Event Exposure procedures at reference points R5 and R6

4.12.1 General

As specified in clauses 4.7.1 and 4.7.4 of TS 26.501 [2], Events relating to 5G Media Streaming are exposed to Event consumers at reference points R5 and R6 by the Data Collection AF instantiated in the 5GMS AF (playing the role of

Event service provider). Procedures for event exposure are specified in clauses 5.11.3 (for downlink media streaming) and 6.8.3 (for uplink media streaming) respectively of [2].

The following *Naf_EventExposure* service operations as defined in TS 23.502 [45] apply for such interactions between the Data Collection AF and consumer entities:

- *Naf_EventExposure_Subscribe*,
- *Naf_EventExposure_Unsubscribe*, and
- *Naf_EventExposure_Notify*.

In this release, eligible Event service consumers of 5GMS Event services are the NWDAF and NEF as NFs, and the Event Consumer AF of the 5GMS Application Provider.

4.12.2 Event Exposure subscription procedure

The definition of input and output parameters of the *Naf_EventExposure_Subscribe* service operation is identical to that specified in clause 5.2.19.2.2 of TS 23.502 [45], except that "AF" is replaced by "Data Collection AF" and "consumer NF" (or "NF consumer") is replaced by "Event service consumer".

4.12.3 Event Exposure unsubscription procedure

The definition of input and output parameters of the *Naf_EventExposure_Unsubscribe* service operation is identical to that specified in clause 5.2.19.2.3 of TS 23.502 [45], except that "AF" is replaced by "Data Collection AF" and "consumer NF" (or "NF consumer") is replaced by "Event service consumer".

4.12.4 Event Exposure notification procedure

The definition of input and output parameters of the *Naf_EventExposure_Notify* service operation is identical to that specified in clause 5.2.19.2.4 of TS 23.502 [45], except that "AF" is replaced by "Data Collection AF" and "consumer NF" (or "NF consumer") is replaced by "Event service consumer".

4.13 Procedures for downlink media streaming via eMBMS

This procedure is used by a 5GMSd Client to establish a 5GMSd session either completely, or at least partially, through eMBMS.

- For downlink media streaming exclusively via eMBMS and for hybrid 5GMSd/eMBMS services, as defined in clauses 5.10.2 and 5.10.5 respectively of TS 26.501 [2]:
 - The 5GMSd Application Provider shall provision a supplementary distribution network of type *DISTRIBUTION_NETWORK_EMBMS* in the Content Hosting configuration at reference point M1d, as specified in clause 7.6.3.1, with either *MODE_EXCLUSIVE* or *MODE_HYBRID* (as appropriate).
 - The 5GMSd Application Provider may additionally provision access reporting in the Consumption Reporting Configuration at M1d, as specified in clause 7.7.3.1.
 - The MBMS Client shall host an MPD as defined in ISO/IEC 23009-1 [32] or in TS 26.247 [4], or any other presentation manifest as the 5GMSd Media Entry Point such as an HLS Master Playlist.
 - The URL of this presentation manifest shall be signalled to the 5GMSd Client through the 5GMSd session establishment procedure.
 - The MBMS Client shall be invoked by the Media Session Handler via reference point MBMS-API-C using the procedures defined in TS 26.347 [52].

- For dynamically provisioned downlink media streaming via eMBMS as defined in clause 5.10.6 TS 26.501 [2]:
 - The 5GMSd Application Provider shall provision a supplementary distribution network of type *DISTRIBUTION_NETWORK_EMBMS* in the Content Hosting configuration at reference point M1d, as specified in clause 7.6.3.1, with *MODE_DYNAMIC*.
 - The 5GMSd Application Provider shall additionally provision access reporting in the Consumption Reporting Configuration at M1d, as specified in clause 7.7.3.1.
 - The 5GMSd AS shall host an MPD as defined in ISO/IEC 23009-1 [32] or in TS 26.247 [4], or any other presentation manifest as the 5GMSd Media Entry Point.
 - The URL of this presentation manifest shall be signalled to the 5GMSd Client through the 5GMSd session establishment procedure. If the 5GMSd service is currently available as an MBMS User Service, the 5GMSd Client forwards the manifest request to the MBMS Client; otherwise, it forwards the request to the 5GMSd AS via reference point M4d.

NOTE: The detailed execution of dynamically handling this decision is left to implementation.

- The MBMS Client shall be invoked dynamically, paused or destroyed by the Media Session Handler via reference point MBMS-API-C using the procedures defined in TS 26.347 [52].

Additional procedures for reactions to different HTTP status codes are provided in clause A.7 of TS 26.247 [4] and clause A.7 of ISO/IEC 23009-1 [32].

Additional procedures for handling partial file responses are provided in clause A.9 of TS 26.247 [4].

5 Procedures for Uplink Media streaming

5.1 General

Uplink media streaming functional entities in the 5GMS System include the 5GMSu Application Provider, 5GMSu AF, 5GMSu AS and the UE. To make use of these other entities, the UE includes a 5GMSu-Aware Application that is provided by the 5GMS Application Provider and a 5GMSu Client comprising the Media Session Handler and the Media Streamer.

The M1 Provisioning API enables the 5GMSu Application Provider to establish and manage the uplink media session handling and streaming options of the 5GMSu system.

The M2u Egest interface enables Uplink media streaming content sent by the 5GMSu Client to the 5GMSu AS over interface M4u to be subsequently delivered to the 5GMSu Application Provider. Uplink media streaming media transfer from the 5GMSu AS to the 5GMSu Application Provider may be either pull-based and initiated by the 5GMSu Application Provider using the HTTP *GET* method, or push-based and initiated by the 5GMSu AS using the HTTP *PUT* method. The resource identifier of the 5GMSu Application Provider for push-based streaming content delivery is provided to the 5GMSu AS by the 5GMSu AF over the M3u interface, as part of the M1 Provisioning Session.

The 5GMSu AF, having acquired M1 Provisioning information, sets up the M5 interface that the 5GMSu Client can use for Uplink media streaming session management, remote control, metrics reporting, network assistance and request for policy and/or charging treatment. Certain types of configuration and policy information accessed over M5 by the Media Session Handler, such as uplink metrics reporting, QoS policy, or support for AF-based network assistance are further passed to the Media Streamer via the M7u API.

Based on the configuration information received on M5 and a request from the Media Streamer received over the M6u interface, the Media Session Handler sets up an Uplink media streaming session with the 5GMSu AF. Upon successful session establishment, the Media Session Handler triggers the Media Streamer to begin Uplink media streaming of media content to the 5GMSu AS over the M4u interface.

Subscription to status and other event notification services are offered by the Media Session Handler to the 5GMSu-Aware Application and to the Media Streamer via the M6u APIs exposed by the Media Session Handler.

Subscription to status and other event notification services are also offered by the Media Streamer to the 5GMSu-Aware Application and to the Media Session Handler via the M7u APIs exposed by the Media Player.

5.2 APIs relevant to Uplink Media Streaming

Table 5.2-1 summarises the APIs used to provision and use the various uplink media streaming features specified in TS 26.501 [2].

Table 5.2-1: Summary of APIs relevant to uplink media streaming features

5GMSu feature	Abstract	Relevant APIs		
		Interface	API name	Clause
Content protocols discovery	Used by the 5GMSu Application Provider to query which content egest protocols are supported by 5GMSu AS(s).	M1u	Content Protocols Discovery API	7.5
Content preparation	Supports manipulation by the 5GMSu AS of streaming media content uploaded by 5GMSu Client over M4u, prior to egest of the manipulated content over M2u.	M1u	Content Preparation Templates Provisioning API	7.4
Metrics reporting	The 5GMSu Client uploads metrics reports to the 5GMSu AF according to a provisioned Metrics Reporting Configuration it obtains from the Service Access Information for its Provisioning Session.	M1u	Provisioning Sessions API	7.2
			Metrics Reporting Provisioning API	7.8
		M5u	Service Access Information API	11.2
			Metrics Reporting API	11.4
Dynamic Policy invocation	The 5GMSu Client activates different traffic treatment policies selected from a set of Policy Templates configured in its Provisioning Session.	M1u	Provisioning Sessions API	7.2
			Policy Templates Provisioning API	7.9
		M5u	Service Access Information API	11.2
			Dynamic Policies API	11.5
Network Assistance	The 5GMSu Client requests bit rate recommendations and delivery boosts from the 5GMSu AF.	M5u	Service Access Information API	11.2
			Network Assistance API	11.6
Edge content processing	Edge resources are provisioned for processing content in 5GMS uplink media streaming sessions.	M1u	Provisioning Sessions API	7.2
			Edge Resources Provisioning API	7.10
UE data collection, reporting and exposure	UE data related to uplink 5G Media Streaming is reported to the Data Collection AF instantiated in the 5GMSu AF for exposure to Event consumers.	M1u	Event Data processing Provisioning API	7.11
			R4	<i>Ndcaf_DataReporting</i> service
		R5, R6	<i>Naf_EventExposure</i> service	18

6 General aspects of APIs for 5G Media Streaming

6.1 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 [22], i.e.:

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

with the following components:

- *{apiRoot}* shall be set as described in TS 29.501 [22].
- *{apiName}* shall be set as defined by the following clauses.
- *{apiVersion}* shall be set to "v2" in this release of the specification.
- *{apiSpecificResourceUriPart}* shall be set as described in the following clauses.

6.2 Usage of HTTP

6.2.1 HTTP protocol version

6.2.1.1 5GMS AF

Implementations of the 5GMS AF shall expose both HTTP/1.1 [24] and HTTP/2 [31] endpoints at interfaces M1 and M5, including support for the HTTP/2 starting mechanisms specified in section 3 of RFC 7540 [31]. In both protocol versions, TLS [29] shall be supported and HTTPS interactions should be used on these interfaces in preference to cleartext HTTP.

The 5GMS Application Provider may use any supported HTTP protocol version at interface M1.

The Media Session Handler may use any supported HTTP protocol version at interface M5.

All responses from the 5GMS AF that carry a message body shall include 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 shall support the conditional HTTP requests `If-None-Match` and `If-Modified-Since`.

6.2.1.2 5GMS AS

Implementations of the 5GMS AS shall expose HTTP/1.1 [24] endpoints at interfaces M2 and M4 and may additionally expose HTTP/2 [31] endpoints at these interfaces. In both protocol versions, TLS [30] shall be supported and HTTPS interactions should be used on these interfaces in preference to cleartext HTTP.

For pull-based content ingest, the 5GMS Application Provider shall expose an HTTP/1.1-based origin endpoint to the 5GMSd AS at interface M2 and may additionally expose an HTTP/2-based origin endpoint.

For push-based content ingest, the 5GMS Application Provider may use any supported HTTP protocol version at interface M2.

The Media Stream Handler may use any supported HTTP protocol version at interface M4.

6.2.2 HTTP message bodies for API resources

The OpenAPI [23] specification of HTTP messages and their content bodies is contained in annex C.

6.2.3 Usage of HTTP headers

6.2.3.1 General

Standard HTTP headers shall be used in accordance with clause 5.2.2 of TS 29.500 [21] for both HTTP/1.1 and HTTP/2 messages.

6.2.3.2 User Agent identification

6.2.3.2.1 Media Stream Handler identification

The Media Stream Handler in the 5GMS Client shall identify itself to the 5GMS AS at interface M4 using a *User-Agent* request header (see section 5.5.3 of RFC 7231 [25]) that should include the *product* token 5GMSMediaStreamHandler. If this product identifier is supplied, the optional *product-version* suffix shall be present. This should indicate the version number of the present document (without the leading "V") with which the Media Stream Handler implementation complies and shall, at minimum, indicate the 3GPP release number with which the implementation complies.

The Media Stream Handler may additionally supply a *comment* element in the *User-Agent* request header containing vendor-specific information.

EXAMPLE 1: 5GMSMediaStreamHandler/17.5.0 (build2634) ExoPlayerLib/2.17.1

EXAMPLE 2: 5GMSMediaStreamHandler/17

6.2.3.2.2 Media Session Handler identification

The Media Session Handler in the 5GMS Client shall identify itself to the 5GMSd AF at interface M5d using a *User-Agent* request header (see section 5.5.3 of RFC 7231 [25]) in which the first element shall be a *product* identified by the token 5GMSMediaSessionHandler. The optional *product-version* suffix shall be present. This should indicate the version number of the present document (without the leading "V") with which the Media Session Handler implementation complies and shall, at minimum, indicate the 3GPP release number with which the implementation complies.

The Media Session Handler may supply additional vendor-specific product identifiers in the *User-Agent* request header and may additionally supply a *comment* element containing vendor-specific information.

EXAMPLE 1: 5GMSMediaSessionHandler/17.5.0 (build1536) lib5gmsclient/0.3.1

EXAMPLE 2: 5GMSMediaSessionHandler/17

6.2.3.3 Server identification

6.2.3.3.1 5GMS AF identification

The 5GMS AF shall identify itself at reference points M1 and M5 using a *Server* response header (see section 7.4.2 of RFC 7231 [25]) that includes a product string of the following form:

5GMSAF-*{FQDN}*/*{complianceInformation}*

where *{FQDN}* shall be the Fully-Qualified Domain Name of the 5GMSd AF exposed to the requesting client, and *{complianceInformation}* should indicate the version number of the present document (without the leading "V") with which the 5GMS AF implementation complies and shall, at minimum, indicate the 3GPP release number with which the implementation complies.

The *Server* response header may also include comments strings and vendor-specific subproduct strings compliant with the syntax and guidance provided in section 7.4.2 of [25].

EXAMPLE 1: 5GMSAF-vm10664.mno.net/17.4.0 (api=2.1.0) libsbi/2.1 libnf/1.2 libaf/1.1

EXAMPLE 2: 5GMSAF-vm10664.mno.net/17 (api=2.1.0) libsbi/2.1 libnf/1.2 libaf/1.1

6.2.3.4 Support for conditional HTTP GET requests

All responses from the 5GMS AF that carry a resource message body shall include:

- a strong entity tag for the resource, conveyed in an `ETag` response header,
- a resource modification timestamp, conveyed in a `Last-Modified` response header, and
- a predicted time-to-live period for the resource, conveyed in a `Cache-Control: max-age` response header.

All API endpoints on the 5GMS AF that expose the HTTP `GET` method shall support conditional requests using the `If-None-Match` and `If-Modified-Since` request headers. 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.

6.2.3.5 Support for conditional HTTP POST, PUT, PATCH and DELETE requests

All API endpoints on the 5GMS AF that expose the HTTP `POST`, `PUT`, `PATCH` or `DELETE` methods shall support conditional requests using the `If-Match` request header. The API client should supply a strong entity tag in an `ETag` request header when invoking any of these HTTP methods.

6.3 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 [22]. API-specific error responses are specified in the respective technical specifications.

6.4 Common API data types

6.4.1 General

The data types defined in this clause are intended to be used by more than one of the 5GMS APIs.

6.4.2 Simple data types

Table 6.4.2-1 below specifies common simple data types used within the 5GMS APIs, including a short description of each. In cases where types from other specifications are reused, a reference is provided.

Table 6.4.2-1: Simple data types

Type name	Type definition	Description	Reference
<i>ResourceId</i>	string	String chosen by the 5GMS AF to serve as an identifier in a resource URL.	
<i>Uri</i>	string	Uniform Resource Identifier conforming with the URI Generic Syntax.	TS 29.571 [12] table 5.2.2-1
<i>Url</i>	string	Uniform Resource Locator, conforming with the URI Generic Syntax.	IETF RFC 3986 [41]
<i>Percentage</i>	number	A percentage expressed as a floating point value between 0.0 and 100.0 (inclusive).	
<i>DurationSec</i>	integer	An unsigned integer identifying a period of time expressed in units of seconds.	TS 29.571 [12] table 5.2.2-1
<i>DateTime</i>	string	An absolute date and time expressed using the OpenAPI <i>date-time</i> string format.	TS 29.571 [12] table 5.2.2-1
<i>IPv4Addr</i>	string	IPv4 address formatted in "dotted decimal" notation	TS 29.571 [12] table 5.2.2-1.
<i>IPv6Addr</i>	string	IPv6 address formatted in colon-separated hexadecimal quartet notation.	TS 29.571 [12] table 5.2.2-1.
<i>UInteger</i>	Integer	Unsigned integer.	TS 29.571 [12] table 5.2.2-1.

6.4.3 Structured data types

6.4.3.1 IpPacketFilterSet type

Table 6.4.3.1-1: Definition of type IpPacketFilterSet

Property name	Data type	Cardinality	Usage	Description
<i>srcIp</i>	String	0..1		Source IP address or IPv6 prefix.
<i>dstIp</i>	String	0..1		Destination IP address or IPv6 prefix.
<i>protocol</i>	Integer	0..1		Protocol.
<i>srcPort</i>	Integer	0..1		Source port.
<i>dstPort</i>	Integer	0..1		Destination Port.
<i>toSTc</i>	String	0..1		Type of Service (TOS) (IPv4) / Traffic class (IPv6) and Mask.
<i>flowLabel</i>	Integer	0..1		Flow Label (IPv6).
<i>spi</i>	Integer	0..1		Security Parameter Index.
<i>direction</i>	String	1..1		Packet Filter Set Direction.

6.4.3.2 ServiceDataFlowDescription type

Table 6.4.3.2-1: Definition of type ServiceDataFlowDescription

Property name	Data type	Cardinality	Usage	Description
<i>flowDescription</i>	IpPacketFilterSet	0..1		Service Data Flow Description.
<i>domainName</i>	string	0..1		FQDN of the 5GMS AS.

NOTE: Exactly one property shall be populated in objects of this type.

6.4.3.3 M5QoSSpecification type

Table 6.4.3.2-1: Definition of type M5QoSSpecification

Property name	Data type	Cardinality	Usage	Description
<i>marBwDlBitRate</i>	BitRate	1..1		Maximum requested bit rate for the Downlink.
<i>marBwUlBitRate</i>	BitRate	1..1		Maximum requested bit rate for the Uplink.
<i>minDesBwDlBitRate</i>	BitRate	0..1		Minimum desired bit rate for the Downlink.
<i>minDesBwUlBitRate</i>	BitRate	0..1		Minimum desired bit rate for the Uplink.
<i>mirBwDlBitRate</i>	BitRate	1..1		Minimum requested bit rate for the Downlink.
<i>mirBwUlBitRate</i>	BitRate	1..1		Minimum requested bandwidth for the Uplink.
<i>desLatency</i>	Integer	0..1		Desire Latency.
<i>desLoss</i>	Integer	0..1		Desired Loss Rate.

6.4.3.4 M1QoSSpecification type

Table 6.4.3.2-1: Definition of type M1QoSSpecification

Property name	Data type	Cardinality	Usage	Description
<i>qosReference</i>	String	0..1		As defined in clause 5.6.2.7 of TS 29.514 [34].
<i>maxBtrUl</i>	BitRate	0..1	RO	Maximum Bitrate Uplink.
<i>maxBtrDl</i>	BitRate	0..1	RO	Maximum Bitrate Downlink.
<i>maxAuthBtrUl</i>	BitRate	0..1	RW	Maximum Authorized Bitrate Uplink by 5GMS Application Provider.
<i>maxAuthBtrDl</i>	BitRate	0..1	RW	Maximum Authorized Bitrate Downlink by 5GMS Application Provider.
<i>defPacketLossRateDl</i>	Integer	0..1		Default packet loss rate for Downlink.
<i>defPacketLossRateUl</i>	Integer	0..1		Default packet loss rate for Uplink.

6.4.3.5 ChargingSpecification type

Table 6.5.3.2-1: Definition of type ChargingSpecification

Property name	Data type	Cardinality	Usage	Description
<i>sponId</i>	SponId	0..1		As defined in clause 5.6.2.3 of TS 29.514 [34].
<i>sponStatus</i>	SponsoringStatus	0..1		
<i>gpsi</i>	Array(Gpsi)	0..1		List of UEs permitted to instantiate this Policy Template.

6.4.3.6 TypedLocation type

Table 6.4.3.6-1: Definition of TypedLocation type

Property name	Data type	Cardinality	Description
<i>locationIdentifierType</i>	CellIdentifierType	1..1	The type of cell location present in the <i>location</i> property.
<i>location</i>	string	1..1	Identifies the cell location.

6.4.3.7 OperationSuccessResponse type

The data model for the *OperationSuccessResponse* type is specified in table 6.4.3.7-1 below:

Table 6.4.3.7-1: Definition of OperationSuccessResponse type

Property name	Type	Cardinality	Description
<i>success</i>	Boolean	1..1	Indicates whether an operation was successful (<i>TRUE</i>) or not (<i>FALSE</i>).
<i>reason</i>	String	0..1	Optional explanation of the success or otherwise of the operation.

6.4.3.8 EdgeProcessingEligibilityCriteria type

The *EdgeProcessingEligibilityCriteria* type is specified in table 6.4.3.8-1 below:

Table 6.4.3.8-1: Definition of EdgeProcessingEligibilityCriteria type

Property name	Type	Cardinality	Description
<i>serviceDataFlowDescriptions</i>	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 <i>ServiceDataFlowDescription</i> elements: - <i>domainName</i> - <i>flowDescription.dstIp</i> and <i>flowDescription.dstPort</i> - <i>flowDescription.toSTc</i> - <i>flowDescription.flowLabel</i> Other <i>ServiceDataFlowDescription</i> settings shall be rejected by the 5GMS AF.
<i>ueLocations</i>	array(LocationArea5G)	1..1	A set of geographical areas in which edge media processing is to be triggered when a UE is present. If the set is empty, edge media processing may be invoked for an otherwise eligible media stream session in any location.
<i>timeWindows</i>	array(TimeWindow)	1..1	Edge media processing is triggered when the media streaming session is taking place during one of the indicated time windows. If the set is empty, edge media processing may be invoked for an otherwise eligible media stream session at any time.
<i>appRequest</i>	boolean	1..1	When set <i>TRUE</i> , 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 <i>LocationArea5G</i> and <i>TimeWindow</i> are defined in TS 24.558 [42].			

6.4.3.9 EndpointAddress type

Table 6.4.3.9-1: Definition of EndpointAddress type

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

6.4.4 Enumerated data types

6.4.4.1 CellIdentifierType enumeration

The data model for the *CellIdentifierType* enumeration which indicates the type of cell identifier as defined in TS 23.003 [7], is specified in Table 6.4.4.1-1 below:

Table 6.4.4.1-1: Definition of CellIdentifierType enumeration

Enumeration value	Description
<i>CGI</i>	Cell Global Identification.
<i>ECGI</i>	E-UTRAN Cell Global Identification.
<i>NCGI</i>	NR Cell Global Identity.

6.4.4.2 SdfMethod enumeration

The data model for the *SdfMethod* enumeration is specified in table 6.4.4.2-1 below:

Table 6.4.4.2-1: Definition of SdfMethod enumeration

Enumeration value	Description
<i>5_TUPLE</i>	The Media Session Handler shall use 5-Tuples for Service Data Flow descriptions. The 5-Tuple shall not contain a wildcard.
<i>2_TUPLE</i>	The Media Session Handler shall use a 2-Tuple of UE IP and Server IP as Service Data Flow Description.
<i>TYPE_OF_SERVICE_MARKING</i>	The Media Session Handler shall apply Type of Service (ToS) marking to the Service Data Flow.
<i>FLOW_LABEL</i>	The Media Session Handler shall apply IPv6 flow label marking and provide the IPv6 flow label of the Service Data Flow.
<i>DOMAIN_NAME</i>	The Media Session Handler shall provide the domain name of the 5GMSd AS.

6.4.4.3 ProvisioningSessionType enumeration

The data model for the *ProvisioningSessionType* enumeration is specified in Table 6.4.4.3-1 below:

Table 6.4.4.3-1: Definition of ProvisioningSessionType enumeration

Enumeration value	Description
<i>DOWNLINK</i>	Downlink media streaming
<i>UPLINK</i>	Uplink media streaming

6.4.4.4 EASRelocationTolerance enumeration

The *EASRelocationTolerance* enumeration is specified in table 6.4.4.4-1 below:

Table 6.4.4.4-1: Definition of EASRelocationTolerance enumeration

Enumeration value	Description
<i>RELOCATION_UNAWARE</i>	The application is not aware of any EAS relocation that may happen. Relocation procedures may be executed without any restrictions.
<i>RELOCATION_TOLERANT</i>	The application may tolerate EAS relocation, but requirements for the relocation procedure must be met. An application context may need to be transferred.
<i>RELOCATION_INTOLERANT</i>	The application does not tolerate relocation.

6.4.4.4 CacheStatus enumeration

Table 6.4.4.4-1: Definition of CacheStatus enumeration

Enumeration value	Description
<i>HIT</i>	The requested object is present in the 5GMS AS cache and is still valid.
<i>MISS</i>	The requested object is not present in the 5GMS AS cache.
<i>EXPIRED</i>	The requested object is present in the 5GMS AS cache but is stale.

6.5 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 [38] 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 [38].
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" (Read) and "U" (Update) refers to the CRUD procedure during which the property is present in the resource type. (The Delete operation never takes any input data type.)
 - "RO" signifies a read-only property. Only the API provider function is permitted to modify the property value. The API invoker can only read the value.
 - "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 Provisioning (M1) APIs

7.1 General

This clause defines the provisioning API used by a 5GMS Application Provider to configure downlink or uplink 5G Media Streaming services.

7.2 Provisioning Sessions API

7.2.1 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 4.3.2. Having created a Provisioning Session, the 5GMS Application Provider can then go on to provision other 5GMS features in the context of that Provisioning Session, using the APIs specified in clause 7.3 *et seq.* Certain of these features are only applicable to the type of Provisioning Session created.

7.2.2 Resource structure

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

{apiRoot}/3gpp-m1/{apiVersion}/provisioning-sessions/

Table 7.4.2-1 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 7.2.2-1: Operations supported by the Provisioning Sessions API

Operation	Sub-resource path	Allowed HTTP method(s)	Description
Create Provisioning Session		POST	Used to create a new Provisioning Session resource. If the operation succeeds, the URL of the created Provisioning Session resource shall be returned in the <code>Location</code> header of the response.
Retrieve Provisioning Session	<i>{provisioningSessionId}</i>	GET	Used to retrieve a Provisioning Session resource for inspection.
Destroy Provisioning Session		DELETE	Used to destroy an existing Provisioning Session resource.

7.2.3 Data model

7.2.3.1 ProvisioningSession resource

The data model for the *ProvisioningSession* resource is specified in table 7.2.3.1-1 below. Different properties are present in the resource depending on the type of Provisioning Session indicated in the *provisioningSessionType* property, and this is specified in the *Applicability* column.

Table 7.2.3.1-1: Definition of ProvisioningSession resource

Property name	Type	Cardinality	Usage	Description	Applicability
<i>provisioningSessionId</i>	ResourceId	1..1	C: R R: RO	A unique identifier for this Provisioning Session.	All types.
<i>provisioningSessionType</i>	ProvisioningSessionType	1..1	C: RW R: RO U: –	The type of Provisioning Session.	All types.
<i>aspld</i>	AspId	0..1	C: W R: RO	The identity of the Application Service Provider responsible for this Provisioning Session, as specified in clause 5.6.2.3 of TS 29.514 [34].	All types.
<i>appld</i>	ApplicationId	1..1	C: RW R: RO U: RO	The Application Identifier (see table 5.4.2-1 of TS 29.571 [12]) to which this Provisioning Session pertains. The same <i><aspld, appld></i> 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 [34]) 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.
<i>serverCertificateIds</i>	array(ResourceId)	0..1	C: – R: RO	A list of Server Certificate identifiers currently associated with this Provisioning Session.	<i>downlink</i>
<i>contentPreparationTemplateIds</i>	array(ResourceId)	0..1	C: – R: RO	A list of Content Preparation Template identifiers currently associated with this Provisioning Session.	<i>downlink, uplink</i>
<i>metricsReportingConfigurationIds</i>	array(ResourceId)	0..1	C: – R: RO	A list of Metrics Reporting Configuration identifiers currently associated with this Provisioning Session.	<i>downlink, uplink</i>
<i>policyTemplateIds</i>	array(ResourceId)	0..1	C: – R: RO	A list of Policy Template identifiers currently associated with this Provisioning Session.	<i>downlink, uplink</i>
<i>edgeResourcesConfigurationIds</i>	array(ResourceId)	0..1	C: – R: RO	A list of Edge Resources Configuration identifiers currently associated with this Provisioning Session.	<i>downlink, uplink</i>
<i>eventDataProcessingConfigurationIds</i>	array(ResourceId)	0..1	C: – R: RO	A list of Event Data Processing Configuration identifiers currently associated with this Provisioning Session.	<i>downlink, uplink</i>

7.3 Server Certificates Provisioning API

7.3.1 Overview

The Server Certificates Provisioning API is used to provision X.509 [8] server certificates that can be referenced by a Content Hosting Configuration and subsequently presented by the 5GMSd AS when it distributes content to 5GMSd Clients at interface M4d using Transport Layer Security [30]. Server Certificate resources are provisioned within the scope of an enclosing Provisioning Session.

7.3.2 Resource structure

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

```
{apiRoot}/3gpp-m1/{apiVersion}/provisioning-sessions/{provisioningSessionId}/
```

Table 7.3.2-1 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 7.3.2-1: Operations supported by the Server Certificates Provisioning API

Operation	Sub-resource path	Allowed HTTP method(s)	Description
Create Server Certificate	certificates	POST	<p>Invoked on the Server Certificates collection associated with a Provisioning Session to request that the 5GMS System creates a new Server Certificate on behalf of the 5GMSd Application Provider.</p> <p>The request message body shall be empty.</p> <p>If the operation succeeds, the URL of the created Server Certificate resource shall be returned in the <i>Location</i> header of the response and this shall comply with the sub-resource path specified below for manipulating Server Certificate resources in the collection.</p> <p>The body of the response message may include a copy of the created X.509 certificate, as specified in clause 7.3.3.2 below.</p>
Reserve Server Certificate	certificates?csr	POST	<p>Invoked on the Server Certificates collection associated with a Provisioning Session to solicit a Certificate Signing Request for a new Server Certificate.</p> <p>The request message body shall be a JSON array of domain name aliases or (if no domain name aliases are required) empty.</p> <p>If the operation succeeds, the URL of the reserved Server Certificate resource shall be returned in the <i>Location</i> header of the response and this shall comply with the sub-resource path specified below for manipulating Server Certificate resources in the collection.</p> <p>The body of the response shall be a PEM-encoded X.509 Certificate Signing Request, as specified in clause 7.3.3.1 below.</p>

Retrieve Server Certificate	certificates/{ <i>certificateId</i> }	GET	Used to retrieve a previously created or uploaded Server Certificate. If a Server Certificate resource has been reserved but not yet uploaded, this operation shall return <i>204 (No Content)</i> .
Upload Server Certificate		PUT	Used by the 5GMSd Application Provider to supply a new Server Certificate in response to a solicited Certificate Signing Request. The body of the request message shall be a PEM-encoded X.509 certificate signed with the public key of the Certificate Signing Request, as specified in clause 7.3.3 below. The 5GMSd AF shall associate the Server Certificate with the private key it generated alongside the Certificate Signing Request. Attempting to update a previously uploaded Server Certificate is an error.
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 { <i>certificateId</i> } differs from the serial number of the X.509 certificate.		

7.3.3 Data model

7.3.3.1 Certificate Signing Request

The Certificate Signing Request shall comply with the Privacy-Enhanced Mail (PEM) textual format specified in RFC 7468 [17], 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*.

7.3.3.2 Server Certificate resource

The Server Certificate resource shall comply with the Privacy-Enhanced Mail (PEM) textual format specified in RFC 7468 [17], i.e. a Base64-encoded DER certificate request or 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*.

7.3.4 Operations

Under no circumstances shall the 5GMSd AF reveal the private key associated with the Certificate Signing Request to the 5GMSd Application Provider.

7.4 Content Preparation Templates Provisioning API

7.4.1 Overview

Content Preparation Templates are used to specify manipulations applied by a 5GMS AS to downlink media resources ingested at interface M2d for distribution at interface M4d, or to uplink media resources contributed at interface M4u for egest at interface M2u. 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.

7.4.2 Resource structure

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

{apiRoot}/3gpp-m1/{apiVersion}/provisioning-sessions/{provisioningSessionId}/

Table 7.4.2-1 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 7.4.2-1: Operations supported by the Content Preparation Templates Provisioning API

Operation	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. If the operation succeeds, the URL of the newly created Content Preparation Template resource shall be returned in the <code>Location</code> header of the response and this shall comply with the sub-resource path specified below for manipulating Content Preparation Templates.
Retrieve Content Preparation Template	content-preparation-templates/ <i>{contentPreparationTemplateId}</i>	GET	Used to retrieve a Content Preparation Template resource.
Update Content Preparation Template		PUT, PATCH	Used to modify an existing Content Preparation Template resource.
Destroy Content Preparation Template		DELETE	Used to destroy an existing Content Preparation Template resource.

7.4.3 Data model

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

7.4.4 Operations

The operations shall be determined by the MIME content type of the Content Preparation Template resource.

7.5 Content Protocols Discovery API

7.5.1 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 5GMS AS instance(s) associated with a 5GMS AF. One of the supported ingest protocols is subsequently indicated in a Content Hosting Configuration for downlink media streaming.

7.5.2 Resource structure

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

```
{apiRoot}/3gpp-m1/{apiVersion}/provisioning-sessions/{provisioningSessionId}/
```

Table 7.5.2-1 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 7.5.2-1: Operations supported by the Ingest Protocols Discovery API

Operation	Sub-resource path	Allowed HTTP method(s)	Description
Fetch list of supported content protocols	<i>protocols</i>	GET	This operation is used to retrieve a list of supported content protocols.

7.5.3 Data model

7.5.3.1 ContentProtocols resource

The data model for the *ContentProtocols* resource is specified in Table 7.5.3.1-1 below:

Table 7.5.3.1-1: Definition of ContentProtocols resource

Property name	Data Type	Cardinality	Description
<i>downlinkIngestProtocols</i>	Array(Content Protocol Descriptor)	0..1	An array of <i>ContentProtocolDescriptor</i> objects, as specified in clause 7.5.3.2, each one uniquely identifying a content ingest protocol supported at interface M2d by the 5GMSd AS(s) associated with the corresponding 5GMSd AF.
<i>uplinkEgestProtocols</i>	Array(Content Protocol Descriptor)	0..1	An array of <i>ContentProtocolDescriptor</i> objects, as specified in clause 7.5.3.2, each one uniquely identifying a content egest protocol supported at interface M2u by the 5GMSu AS(s) associated with the corresponding 5GMSu AF.
<i>geoFencingLocatorTypes</i>	Array(Uri)	0..1	An array of fully-qualified term identifiers, each one indicating a content geo-fencing locator type supported by the 5GMS System. Every 5GMS System shall support at least the locator type <i>urn:3gpp:5gms:locator-type:iso3166</i> .

7.5.3.2 ContentProtocolDescriptor type

The data model for the *ContentProtocolDescriptor* type is specified in table 7.5.3.2-1 below:

Table 7.5.3.2-1: Definition of ContentProtocolDescriptor type

Property name	Data Type	Cardinality	Description
<i>termIdentifier</i>	Uri	1..1	A fully-qualified term identifier from the controlled vocabulary <i>urn:3gpp:5gms:content-protocol</i> , as specified in clause 8.
<i>descriptionLocator</i>	Url	0..1	The location of a description of the content protocol, for example the public web URL of its specification.

7.6 Content Hosting Provisioning API

7.6.1 Overview

This clause specifies the API that a 5GMSd Application Provider uses at interface M1d to provision and manage 5GMSd AS Content Hosting Configurations by interacting with a 5GMSd AF. Each such configuration is represented by a *ContentHostingConfiguration*, the data model for which is specified in clause 7.6.3 below. The RESTful resources for managing Content Hosting Configurations are specified in clause 7.6.2 and the operations on these resources are further elaborated in clause 7.6.4.

7.6.2 Resource structure

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

{apiRoot}/3gpp-m1/{apiVersion}/provisioning-sessions/{provisioningSessionId}/

Table 7.6.2-1 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 7.6.2-1: Operations supported by the Content Hosting Provisioning API

Operation	Sub-resource path	Allowed HTTP method(s)	Description
Create Content Hosting Configuration	content-hosting-configuration	POST	Used to create a Content Hosting Configuration resource.
Retrieve Content Hosting Configuration		GET	Used to retrieve an existing Content Hosting Configuration.
Update Content Hosting Configuration		PUT, PATCH	Used to modify an existing Content Hosting Configuration.
Destroy Content Hosting Configuration		DELETE	Used to delete an existing Content Hosting Configuration.
Purge Content Hosting Configuration cache	content-hosting-configuration/purge	POST	This operation is used to invalidate some or all cached media resources associated with this Content Hosting Configuration.

7.6.3 Data model

7.6.3.1 ContentHostingConfiguration resource

The data model for the *ContentHostingConfiguration* resource is specified in table 7.6.3.1-1 below:

Table 7.6.3.1-1: Definition of ContentHostingConfiguration resource

Property name	Data Type	Cardinality	Description
<i>name</i>	string	1..1	A name for this Content Hosting Configuration.
<i>ingestConfiguration</i>	object	1..1	Describes the 5GMSd Application Provider's origin server from which media resources will be ingested via interface M2d.
<i>pull</i>	boolean	1..1	Indicates whether to the 5GMSd AS shall use Pull or Push for ingesting the content.
<i>protocol</i>	Uri	1..1	A fully-qualified term identifier allocated in the name space <i>urn:3gpp:5gms:content-protocol</i> that identifies the content ingest protocol. The set of supported protocols is defined in clause 8.
<i>baseURL</i>	AbsoluteUrl	0..1	A base URL (i.e. one that includes a scheme, authority and, optionally, path

			<p>segments) from which content is ingested at reference point M2d for this ingest configuration.</p> <p>In the case of Pull-based content ingest (<i>pull</i> flag is set to <i>True</i>), the base URL shall be provided to the 5GMSd AF to indicate the location from which content is to be pulled for this Content Hosting Configuration. A request received at reference point M4d is mapped by the 5GMSd AS to a URL at reference point M2d whose base is the value of this property.</p> <p>In the case of Push-based content ingest (<i>pull</i> flag is set to <i>False</i>), this property is populated by the 5GMSd AF and returned to the 5GMSd Application Provider to indicate the base URL to which content for this Content Hosting Configuration is to be published.</p>
<i>distributionConfigurations</i>	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.
<i>entryPoint</i>	M1MediaEntry Point	0..1	The Media Entry Point when this distribution configuration is used to describe a single content item. Omitted when this distribution configuration describes multiple content items.
<i>relativePath</i>	RelativeUrl	1..1	<p>A relative path (i.e. without a scheme or any leading forward slash characters) to the resource for the Media Entry Point. The semantics are dependent on the value of <i>ingestConfiguration.protocol</i>, as specified in clause 8.</p> <p>The path shall be valid at reference point M2d when appended to the ingest base URL and at reference point M4d when appended to the distribution base URL.</p>
<i>contentType</i>	string	1..1	<p>The MIME content type of the Media Entry Point.</p> <p>Used by the 5GMS Client to select a distribution configuration.</p>
<i>profiles</i>	array(Uri)	0..1	<p>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.</p> <p>Used by the 5GMS Client to select a distribution configuration.</p> <p>If present, the array shall contain at least one item.</p>
<i>contentPreparationTemplateId</i>	ResourceId	0..1	Indicates that content preparation prior to distribution is requested by the 5GMSd Application Provider. It identifies the Content Preparation Template that shall be used as defined in clause 7.4.
<i>edgeResources ConfigurationId</i>	ResourceId	0..1	When present, the 5GMSd AS supporting this content distribution shall be deployed as a set of one or more EAS instances.
<i>supplementaryDistribution Networks</i>	array(<Distribution NetworkType,	0..1	Specifies 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

	DistributionMode		mapping a type of distribution network to a mode of distribution. The same <i>DistributionNetworkType</i> value shall appear at most once in the array.
<i>canonicalDomainName</i>	String	0..1	All resources of the current distribution shall be accessible through this <i>default</i> Fully Qualified Domain Name assigned by the 5GMSd AF.
<i>domainNameAlias</i>	string	0..1	The 5GMSd 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 5GMSd AS at reference point M4d. This domain name is used by the 5GMSd AS to set appropriate CORS HTTP response headers at reference point M4d. If this property is present, the 5GMSd Application Provider is responsible for providing in the DNS a <i>CNAME</i> record that resolves <i>domainNameAlias</i> to <i>canonicalDomainName</i> . If the <i>certificateId</i> property is also present in this distribution configuration, the provided domain name alias shall match one of the <i>subjectAltName</i> extension fields in the referenced Server Certificate resource, allowing for wildcard matching.
<i>baseURL</i>	AbsoluteUrl	0..1	A base URL (i.e. one that includes a scheme, authority and, optionally, path segments) from which content is made available to 5GMS Clients at reference point M4d for this distribution configuration. The value is chosen by the 5GMSd AF when the Content Hosting Configuration is provisioned. It is an error for the 5GMSd Application Provider to set this.
<i>pathRewriteRules</i>	array(object)	0..1	An ordered list of rules for rewriting the request URL paths of media resource requests handled by the 5GMSd AS. If multiple rules match a particular resource's path, only the first matching rule, in order of appearance in this array, shall be applied.
<i>requestPathPattern</i>	string	1..1	A regular expression [5] against which the path part of each 5GMSd 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 ingest, the M4d download request path is used in the comparison. In the case of Push-based ingest, the M2d 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 <i>mappedPath</i> shall be applied.
<i>mappedPath</i>	string	1..1	A replacement for the portion of the 5GMSd AS request path that matches <i>requestPathPattern</i> .

			<p>In the case of Pull-based ingest, <i>ingestConfiguration.entryPoint</i> is concatenated with the mapped path and any leaf path element from the original M4d download request to form the M2d origin request URL.</p> <p>In the case of Push-based ingest, <i>canonicalDomainName</i> (and, optionally, <i>domainNameAlias</i>) are concatenated with the mapped path and any leaf path element from the original M2d upload request to form the distribution URL(s) exposed over M4d.</p>
<i>cacheConfigurations</i>	array(object)	0..1	Defines a configuration of the 5GMSd AS cache for a matching subset of media resources ingested in relation to this Content Hosting Configuration.
<i>urlPatternFilter</i>	string	1..1	A pattern that will be used to match media resource URLs to determine whether a given media resource is eligible for caching by the 5GMSd AS. The format of the pattern shall be a regular expression as specified in [5].
<i>cacheDirectives</i>	object	1..1	If a <i>urlPatternFilter</i> applies to a resource, then the provided <i>cacheDirectives</i> shall be applied by the 5GMSd AS at M4d, potentially overwriting any origin caching directives ingested at M2d.
<i>statusCodeFilters</i>	array(integer)	0..1	The set of HTTP origin response status codes to which these <i>cacheDirectives</i> apply. The filter shall be provided as a regular expression as specified in [5]. If the list is empty, the <i>CacheDirectives</i> shall apply to all HTTP origin response status codes at M2d.
<i>noCache</i>	boolean	1..1	If set to <i>True</i> , this indicates that the media resources matching the filters shall not be cached by the 5GMSd AS and shall be marked as not to be cached when served by the 5GMSd AS at M4d.
<i>maxAge</i>	integer	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 5GMSd AS shall cache matching media resources as well as the time-to-live period signalled by the 5GMSd AS at interface M4d 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.
<i>geoFencing</i>	object	0..N	Limit access to the content to the indicated geographic areas.
<i>locatorType</i>	Uri	1..1	The type of the locators shall be indicated using a fully-qualified term identifier URI from the controlled vocabulary <i>urn:3gpp:5gms:locator-type</i> , as specified in clause 7.6.4.6, or else from a vendor-specific vocabulary.
<i>locators</i>	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 value of <i>locatorType</i> , as specified in clause 7.6.4.6.
<i>urlSignature</i>	object	0..1	Defines the URL signing scheme. Only correctly signed and valid URLs will be

			allowed to access the content resource at M4d.
<i>urlPattern</i>	string	1..1	A pattern that shall be used by the 5GMSd AS to match M4d media resource URLs. The 5GMSd AS shall not serve a matching media resource at M4d unless it includes a valid authentication token calculated over the portion of the M4d request URL that matches this pattern. The format of the pattern shall be a regular expression as specified in [5].
<i>tokenName</i>	string	1..1	The name of the M4d request query parameter that the Media Player should use to present the authentication token when required to do so.
<i>passphraseName</i>	string	1..1	The name of the query parameter that is used to refer to the passphrase when constructing the authentication token. Note that the token is not included in the cleartext part of the M4d URL query component.
<i>passphrase</i>	string	1..1	The shared secret between the 5GMSd Application Provider and the 5GMSd AS for this <i>distributionConfiguration</i> . The passphrase is used in the computation and verification of the M4d authentication token but is never sent in-the-clear over that interface.
<i>tokenExpiryName</i>	string	1..1	The name of the M4d request query parameter that the Media Player should use to present the token expiry field.
<i>useIPAddress</i>	boolean	1..1	If set to <i>True</i> , the IP address of the UE is included in the computation of the authentication token for resources that match <i>urlPattern</i> and access to matching media resources shall be allowed by the 5GMSd AF only when the M4d request is made from a UE with this IP address.
<i>ipAddressName</i>	string	0..1	The name of the M4d request query parameter that is encoded as part of the authentication token if the <i>useIPAddress</i> flag is set to <i>True</i> . Note that the IP address is not passed in the cleartext part of the M4d URL query component.
<i>certificateId</i>	ResourceId	0..1	When content is distributed using TLS [16], the X.509 [8] certificate for the origin domain is shared with the 5GMSd AF so that it can be presented by the 5GMSd AS in the TLS handshake at reference point M4d. This attribute indicates the identifier of the certificate to use.

7.6.3.2 DistributionNetworkType enumeration

The data model for the *DistributionNetworkType* enumeration is specified in Table 7.6.3.2-1 below:

Table 7.6.3.2-1: Definition of DistributionNetworkType enumeration

Enumeration value	Description
<i>DISTRIBUTION_NETWORK_EMBMS</i>	Downlink media streaming via eMBMS.

7.6.3.3 DistributionMode enumeration

The data model for the *DistributionMode* enumeration is specified in Table 7.6.3.3-1 below:

Table 7.6.3.3-1: Definition of DistributionMode enumeration

Enumeration value	Description
<i>MODE_EXCLUSIVE</i>	Downlink media streaming content ingested by the 5GMSd AS is distributed exclusively via a supplementary network and is not available at reference point M4d.
<i>MODE_HYBRID</i>	Downlink media streaming content ingested by the 5GMSd AS is available at reference point M4d and is additionally distributed via a supplementary network.
<i>MODE_DYNAMIC</i>	Downlink media streaming content ingested by the 5GMSd AS is available at reference point M4d and is additionally distributed via a supplementary network only when reported client demand exceeds a configured threshold.

7.6.4 Operations

7.6.4.1 Overview

This clause defines the behaviour that is expected from the 5GMSd AS when the Content Hosting Configuration has been successfully provisioned. The main operations that are performed affect the caching and purging of cached content as well as the processing for media preparation and at the edge.

7.6.4.2 Content caching

A Content Hosting Configuration may specify caching rules to be applied to media resources when they are distributed by the 5GMSd AS over interface M4d. The distribution shall use the *urlPatternFilter* in the *CachingConfiguration* object to determine which caching directives apply to that object. In case a media resource's URL matches the pattern filter of more than one *CachingConfiguration*, the first match shall apply. In case no *CachingConfiguration* is identified as a match, the 5GMSd AS shall apply the caching directives that were received from the origin. In the case where no match is found and the origin server does not supply caching directives at M2d, then default caching directives based on the media resource type shall be applied.

A caching directive shall either indicate that a matching media resource is not to be cached by the 5GMSd AS, nor by downstream M4d clients (*noCache* set to *True*), or that the 5GMSd AS and downstream M4d clients are to cache it for *maxAge* seconds. The *maxAge* value applies relative to the time when a media resource was ingested, *t_ingest*. For an HTTP-based ingest, this corresponds to the *Date* header field in the HTTP request/response that carries the media resource at M2d. At the time *t_ingest + maxAge*, the object is considered stale and should not be served at M4d from the 5GMSd AS cache. The 5GMSd AS shall compensate for any synchronization skew between the origin and its own clock. This can be for instance done by including the *max-stale* HTTP cache directive in its M4d responses.

The *maxAge* value may be signalled at M4d by the 5GMSd AS using the *Expires* HTTP response header or the HTTP *Cache-Control* directives *max-age* or *s-maxage*.

When distributing a media resource using HTTP, a *no-cache* request may be translated into a *no-cache* and *no-store* HTTP *Cache-Control* directive and/or a *max-age=0* HTTP *Cache-Control* directive.

By default, all origin HTTP header fields shall be assumed as not forwarded by the 5GMSd AS, unless specified otherwise by setting the flag *originCacheHeaders* to *True*.

7.6.4.3 Cache purging

The 5GMSd Application Provider may perform a purge operation to invalidate some or all cached media resources of a particular Content Hosting Configuration. A regular expression describing the set of media resource URLs to be purged from the 5GMSd AS cache for the Content Hosting Configuration in question shall be supplied in the body of the request. The 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 5GMSd AF shall immediately invalidate all media resources in the 5GMSd AS cache matching the regular expression by declaring them as stale. Any request at reference point M4d for a purged media resource will trigger the fetching (and possible caching) of the current version from the origin via M2d in case of a Pull-

based ingest. For Push-based ingest, M4d requests for purged content shall be responded to with a *404 (Not Found)* HTTP response, until a new version of the object is pushed by the origin to the 5GMSd AS via M2d.

If the procedure is successful, the 5GMSd AF shall respond with 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.
- *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 5GMSd AS instances distributing the Provisioning Session in question.

If the procedure is not successful, the 5GMSd AF shall provide a response code as defined in clause 6.3. In addition, 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 5GMSd AF to be syntactically malformed.

7.6.4.4 Content processing

The 5GMSd AS can perform various content processing tasks (such as repackaging, encryption, ABR transcoding) on media resources ingested at M2d prior to serving them at M4d. These processing tasks shall be specified in a Content Preparation Template resource referenced from the Content Hosting Configuration object.

7.6.4.5 URL signing

The URL signing procedure allows the 5GMSd Application Provider to prevent deep linking and unauthorized access to M4d media resources. It works by cryptographically signing some elements of the M4d request URL and then appending this authentication token to the URL as an additional query parameter. The token is generated by the 5GMSd Application Provider and supplied to the player, for example as part of an initial URL. When it receives a request that requires URL signing, the 5GMSd AS verifies the presence and validity of the token in the M4d request URL before allowing access to the requested media resource. The 5GMSd AS(s) and the origin share a secret that is encoded as part of the query parameter hash, but not shared with the 5GMSd Media Player.

The validity of the authentication token can also be limited to a single UE. If *useIPAddress* is set to True, then the public IP address of the UE as viewed by the 5GMSd AS, *ue_public_ip_address*, shall be incorporated into the token calculation. The parameter name shall be indicated by *ipAddressName*.

The shared secret shall be provided in *UrlSignature.passphrase* as a string of length between 6 and 50 characters. The parameter name for the passphrase shall be provided by *passphraseName*.

The expiry time of the signed URL, *tokenExpiry*, shall be included as an additional query parameter in the URL exposed at M4d with the name indicated in *tokenExpiryName*. The expiry time shall be the string representation of the number of seconds from 1970-01-01T00:00:00Z UTC until the specified UTC date/time, ignoring leap seconds, as defined in section 4.16 of POSIX.1 [11].

Given the above, the authentication token shall be calculated as:

$$\text{token} := \text{SHA512}(\text{url} \& \text{UrlSignature.tokenExpiryName}=\text{token_expiry} \& \text{UrlSignature.ipAddressName}=\text{ue_public_ip_address} \& \text{UrlSignature.passphraseName}=\text{passphrase})$$

where the SHA512 function shall be the SHA-512 hash [6] of the enclosed string. The *url* parameter shall be the original M4d media resource request URL, including the scheme, authority and path components but excluding any query and fragment components.

The resulting token value shall be "base64url" encoded, as specified in section 5 of RFC 4648 [10], prior to inclusion in the M4d URL.

The query part of the signed URL presented by the 5GMSd Media Player at M4d as proof of authenticity shall be composed as follows:

$$\text{query} := \text{UrlSignature.tokenExpiryName}=\text{token_expiry} \& \text{UrlSignature.tokenName}=\text{base64url}(\text{token})$$

For all media resources requested at reference point M4d that match the regular expression specified in *UrlSignature.urlPattern*, the 5GMSd AS shall validate the *query* presented in the request URL according to the following steps:

- 1) If the parameter indicated by *UriSignature.tokenName* is absent from *query*, or if the supplied *token* value is malformed, the 5GMSd AS shall respond with a *403 (Forbidden)* error response message and terminate further processing of the M4d request.
- 2) If the parameter indicated by *UriSignature.tokenExpiryName* is absent from *query*, or if the supplied *token_expiry* value has expired, or if the supplied *token_expiry* is malformed, the 5GMSd AS shall respond with a *403 (Forbidden)* error response message and terminate further processing of the M4d request.
- 3) The 5GMSd AS shall compute the authentication token according to the *token* production specified above using the requesting UE's public IP address as the value of *ue_public_ip_address* if required by *UriSignature.useIPAddress* being set to *True*. After applying "base64url" encoding, the 5GMSd AS shall compare this with the value supplied in the URL *query* parameter whose name is *UriSignature.tokenName*. If the two values differ, the 5GMSd AS shall respond with a *403 (Forbidden)* error response message and terminate further processing of the M4d request.
- 4) Otherwise, the presented authentication token is valid. The 5GMSd AS shall either return the media resource in a *200 (OK)* response message (if it is able to serve that media resource), or else return an appropriate error response, such as *404 (Not Found)* or *503 (Service Unavailable)*.

7.6.4.6 Geofencing

The 5GMSd Application Provider may wish to limit access to its media content at interface M2d to UEs located in certain geographical zones. Geofencing is used to configure the zone from which content is accessible.

Two different types of locator are specified here:

- **Administrative area locator:** the value of *GeoFencing.locatorType* shall be *urn:3gpp:5gms:locator-type:iso3166* and each member of the *GeoFencing.locators* array shall be either a string representation of an ISO 3166-1 alpha-2 country code [18] (e.g. *US, CN, KR, GB, FR*) or an ISO 3166-2 code [19] 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*).
- [- **Tracking Area locator:** the value of *GeoFencing.locatorType* shall be *urn:3gpp:5gms:locator-type:trackingAreaCode* and each member of the *GeoFencing.locators* array shall be the Fully-Qualified Domain Name representation of a Tracking Area Code, as defined in clause 19.4.2.3 of TS 23.003 [7].]

7.7 Consumption Reporting Provisioning API

7.7.1 Overview

The Consumption Reporting Provisioning API is a RESTful API that allows a 5GMSd Application Provider to configure the Consumption Reporting Procedure for a particular downlink media streaming Provisioning Session at interface M1d. The different procedures are described in clause 4.3.8. The Consumption Reporting Configuration is represented by a *ConsumptionReportingConfiguration*, the data model for which is specified in clause 7.7.3 below. The RESTful resources for managing the Consumption Reporting Configuration are specified in clause 7.7.2.

7.7.2 Resource structure

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

{apiRoot}/3gpp-m1/{apiVersion}/provisioning-sessions/{provisioningSessionId}/

Table 7.7.2-1 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 7.7.2-1: Operations supported by the Consumption Reporting Provisioning API

Operation	Sub-resource path	Allowed HTTP method(s)	Description
Activate Consumption Reporting procedure with a Consumption Reporting Configuration	consumption-reporting-configuration	POST	Activate the consumption reporting procedure and to set the Consumption Reporting Configuration.
Fetch Consumption Reporting Configuration		GET	Retrieve an existing Consumption Reporting Configuration.
Update Consumption Reporting Configuration		PUT, PATCH	Modify an existing Consumption Reporting Configuration.
Delete Consumption Reporting Configuration		DELETE	Deactivate the consumption reporting procedure for that particular session.

7.7.3 Data model

7.7.3.1 ConsumptionReportingConfiguration resource

The data model for the *ConsumptionReportingConfiguration* resource is specified in table 7.7.3.1-1.

Table 7.7.3.1-1: ConsumptionReportingConfiguration resource

Property name	Type	Cardinality	Description
<i>reportingInterval</i>	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.
<i>samplePercentage</i>	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.
<i>locationReporting</i>	boolean	0..1	Stipulates whether the Media Session Handler is required to provide location data to the 5GMSd AF in consumption reporting messages (in case of MNO or trusted third parties). If omitted, location reporting is disabled.

<i>accessReporting</i>	boolean	0..1	Stipulates whether the Media Session Handler is required to provide consumption reporting messages to the 5GMSd AF when the access network changes during a media streaming session. If omitted, access reporting is disabled.
------------------------	---------	------	---

7.8 Metrics Reporting Provisioning API

7.8.1 Overview

The Metrics Reporting Provisioning API allows an 5GMS System operator or a 5GMS Application Provider to configure the Metrics Collection and Reporting procedure for a particular downlink or uplink media streaming Provisioning Session at interface M1.

7.8.2 Resource structure

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

{apiRoot}/3gpp-m1/{apiVersion}/provisioning-sessions/{provisioningSessionId}/

Table 7.8.2-1 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 of the table shall be appended to the URL base path.

Table 7.8.2-1: Operations supported by the Metrics Reporting Provisioning API

Operation	Sub-resource path	Allowed HTTP method(s)	Description
Create Metrics Reporting Configuration	metrics-reporting-configurations	POST	Create and optionally provide a configuration. If the operation succeeds, the URL of the created Metrics Reporting Configuration resource shall be returned in the <code>Location</code> header of the response.
Read Metrics Reporting Configuration	metrics-reporting-configurations/ <i>{metricsReportingConfigurationId}</i>	GET	Retrieve the values of an existing Metrics Reporting Configuration.
Update Metrics Reporting Configuration		PUT, PATCH	Provide initial upload of a new configuration, or either the modification of, or replacement to an existing configuration.
Delete Metrics Reporting Configuration		DELETE	Delete a configuration, disables reporting.

7.8.3 Data model

7.8.3.1 MetricsReportingConfiguration resource

The data model for the *MetricsReportingConfiguration* resource is specified in table 7.8.3-1 below:

Table 7.8.3-1: Definition of MetricsReportingConfiguration resource

Property name	Type	Cardinality	Description
<i>metricsReportingConfigurationId</i>	ResourceId	1..1	An identifier for this Metrics Reporting Configuration assigned by the 5GMS AF that is unique within the scope of the enclosing Provisioning Session.
<i>sliceScope</i>	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 slices.
<i>scheme</i>	Uri	0..1	The QoE metrics scheme associated with this Metrics Reporting Configuration, which indicates the required format of metrics reports. A scheme may be associated with 3GPP or with a non-3GPP entity. For downlink media streaming, if omitted, the 3GPP metrics scheme <i>urn:3GPP:ns:PSS:DASH:QM10</i> specified in clause 10.6 of TS 26.247 [4] shall apply. For uplink media streaming, if omitted, the implication is that no associated uplink metrics reporting shall be performed.
<i>dataNetworkName</i>	Dnn	0..1	The Data Network Name (DNN) which shall be used when sending metrics reports. If not specified, the default DNN shall be used.
<i>reportingInterval</i>	DurationSec	0..1	The time interval between successive metrics reports. The value shall be greater than zero. If not specified, a single final report shall be sent after the media streaming session has ended.
<i>samplePercentage</i>	Percentage	0..1	The proportion of media streaming sessions for which 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 sessions.
<i>urlFilters</i>	array(String)	0..1	A non-empty list of Media Entry Point URL patterns for which metrics shall be reported. If not specified, reporting shall be done for all media streaming sessions initiated within the scope of the parent Provisioning Session.
<i>samplingPeriod</i>	DurationSec	1..1	The time interval the 5GMS Client should wait between sampling the QoE metrics specified by this metrics reporting configuration.

Property name	Type	Cardinality	Description
<i>metrics</i>	array(Uri)	0..1	<p>If present, a non-empty list of metrics which shall be collected and reported.</p> <p>In the case of downlink media streaming and for the 3GPP scheme <i>urn:3GPP:ns:PSS:DASH:QM10</i> the listed metrics shall correspond to one or more of the metrics as specified in clauses 10.3 and 10.4 of TS 26.247 [7], each indicated using a fully-qualified term identifier according to clause E.2.1, and the quality reporting scheme and quality reporting protocol as defined in clauses 10.5 and 10.6, respectively, of [7] shall be used to produce and send metrics reports.</p> <p>Metrics related to virtual reality media, as specified in TS 26.118 [42] clause 9.3, may also be listed in the metrics configuration, each indicated using a fully-qualified term identifier according to clause E.2.2, and shall be reported according to the quality reporting scheme defined in clause 9.4 of [42].</p> <p>In the case of uplink streaming, no standardized metrics nor metrics reporting protocol are defined in the present document. It is assumed that those quality metrics and reporting protocol are defined by the metrics scheme.</p> <p>If omitted, the complete (or default, as applicable) set of metrics associated with the specified scheme shall be collected and reported.</p>
NOTE: The <i>Snssai</i> data type is specified in TS 29.571 [12].			

7.9 Policy Templates Provisioning API

7.9.1 Overview

The Policy Templates Provisioning API allow a 5GMS Application Provider to configure a set of Policy Templates within the scope of a Provisioning Session that can subsequently be applied to downlink or uplink media streaming sessions belonging to that Application Provider using the Dynamic Policies API specified in clause 11.5. A Policy Template is used to specify the traffic shaping and charging policies to be applied to these media streaming sessions.

A Policy Template, identified by its *policyTemplateId*, represents a set of PCF/NEF API parameters which defines the service quality and associated charging for the corresponding downlink or uplink media streaming session(s). The Policy Template is configured as part of the provisioning procedures with the 5GMS AF and is then used by the 5GMS AF to request specific QoS and charging policies for that session from the PCF or NEF.

The state of a Policy Template can be:

- *pending*: The Policy Template is awaiting validation, 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 5GMS AF.
- *ready*: After successful validation by the 5GMS AF the Policy Template moves into this state.
- *suspended*: The 5GMS AF may move a Policy Template into this state under certain conditions defined within the Service Level Agreement.

When the Policy Template is used for QoS Flows, the *qoSSpecification* object (of type *M1QoSSpecification*) shall be present:

- The *qoSReference* value is obtained with the Service Level Agreement. See TS 23.502 [45] for detailed usage.
- The *maxBtrUl* and *maxBtrDl* properties define the maximal bit rate which can be used for QoS Flows. This value is defined by the 5G System.
- The *maxAuthBtrUl* and *MaxAuthBtrDl* properties define the maximal authorized bit rate values which can be requested by a Media Session Handler. Higher bit rate values are not authorized for use by the 5GMS Application Provider.
- The *minPacketLossRateDl* and *minPacketLossRateUl* properties define the minimal authorized packet loss rate, which can be requested by a Media Session Handler.

When the Policy Template is used for differential charging the *chargingSpecification* property shall be present.

applicationSessionContext is an optional child object.

- The *dnn* property contains the Data Network Name of the data network in which the 5GMS AF is hosted.
- When Network Slicing is used, the *sliceInfo* property contains information about the network slice which is serving the UE.

7.9.2 Resource structure

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

{apiRoot}/3gpp-m1/{apiVersion}/provisioning-sessions/{provisioningSessionId}/

Table 7.9.2-1 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 7.9.2-1: Operations supported by the Policy Template Provisioning API

Operation	Sub-resource path	Allowed HTTP method(s)	Description
Create a new Policy Template	<i>policy-templates</i>	POST	Used to create a new Policy Template resource. If the operation succeeds, the URL of the created Policy Template resource shall be returned in the <i>Location</i> header of the response.
Fetch a Policy Template	<i>policy-templates/{policyTemplateId}</i>	GET	Used to retrieve an existing Policy Template resource.
Update a Policy Template		PUT, PATCH	Used to modify the configuration of an existing Policy Template.
Delete a Policy Template		DELETE	Used to delete an existing Policy Template resource.

7.9.3 Data model

7.9.3.1 PolicyTemplate resource

The data model for the *PolicyTemplate* resource is specified in table 7.9.3-1 below:

Table 7.9.3.1-1: Definition of PolicyTemplate resource

Property	Type	Cardinality	Usage	Description
<i>policyTemplateId</i>	ResourceId	1..1	C: RO R: RO U: RO	Identifier of this Policy Template assigned by the 5GMS AF that is unique within the scope of the Provisioning Session.
<i>state</i>	string enum	1..1	C: RO R: RO U: RO	Current state of this Policy Template exposed to the 5GMS Application Provider by the 5GMS AF. A Policy Template may be in the <i>PENDING</i> , <i>INVALID</i> , <i>READY</i> , or <i>SUSPENDED</i> state. Only a Policy Template in the <i>READY</i> state may be instantiated as a Dynamic Policy Instance and applied to media streaming sessions.
<i>stateReason</i>	Problem Details	1..1	C: RO R: RO U: –	Additional details about the current state of this Policy Template exposed to the 5GMS Application Provider by the 5GMS AF. The <i>instance</i> sub-property shall be present and shall indicate the URL of this Policy Template resource. The <i>title</i> sub-property shall be present and shall indicate a human-readable representation of the <i>state</i> property specified above, e.g. "Policy Template ready for use" or "Policy Template invalid". The <i>detail</i> sub-property shall be present and shall indicate a human-readable status/error message. All other properties shall be omitted.
<i>externalReference</i>	string	1..1	C: RW R: RO U: RW	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".
<i>qoSSpecification</i>	MIQoS Specification	0..1	C: RW R: RO U: RW	Specifies the network quality of service to be applied to media streaming sessions at this Policy Template.
<i>applicationSessionContext</i>	object	0..1		Specifies information about the application session context at reference point M4 to which this Policy Template can be applied.
<i>sliceInfo</i>	Snsai	0..1	C: RW R: RW U: RW	As defined in clause 5.4.4.2 of TS 29.571 [12].
<i>dnn</i>	Dnn	0..1	C: RW R: RW U: RW	As defined in clause 5.3.2 of TS 29.571 [12].
<i>chargingSpecification</i>	Charging Specification	0..1	C: RW R: RW U: RW	Provides information about the charging policy to be used for this Policy Template.

7.10 Edge Resources Provisioning API

7.10.1 General

The Edge Resources Provisioning API is used by the 5GMS 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 5GMS AS EAS instance that will serve the media session to the UE.

7.10.2 Resource structure

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

{apiRoot}/3gpp-m1/{apiVersion}/provisioning-sessions/{provisioningSessionId}/

Table 7.10.2-1 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 7.10.2-1: Operations supported by the Edge Resources API

Operation	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. If the operation succeeds, the URL of the newly created Edge Resources Configuration resource shall be returned in the Location header of the response.
Retrieve Edge Resources Configuration	edge-resources-configurations/ <i>{edgeResourcesConfigurationId}</i>	GET	Used to retrieve a specific Edge Resources Configuration resource.
Modify Edge Resources Configuration		PUT, PATCH	Used to modify or replace an existing Edge Resources Configuration resource.
Destroy Edge Resources Configuration		DELETE	Used to destroy an existing Edge Resources Configuration resource.

7.10.3 Data model

7.10.3.1 EdgeResourcesConfiguration resource type

The data model for the Edge Resources Configuration resource is specified in table 7.10.3.1-1:

Table 7.10.3.1-1: Definition of EdgeResourcesConfiguration resource type

Property name	Type	Cardinality	Description
<i>edgeResourcesConfigurationId</i>	ResourceId	1..1	An identifier for this Edge Resources Configuration that is unique within the scope of the enclosing Provisioning Session.
<i>edgeManagementMode</i>	EdgeManagement Mode	1..1	Indicates whether the management of edge resources is client-driven or AF-driven. (See clause 7.10.3.2.)
<i>eligibilityCriteria</i>	EdgeProcessing Eligibility Criteria	0..1	Condition to activate edge resources for this Provisioning Session. If omitted, it shall be assumed that all media streaming sessions related to the parent Provisioning Session will use edge resources. (See clause 6.4.3.8.)
<i>easRequirements</i>	EASRequirements	1..1	Requirements on the EAS Profile used by the 5GMS AF or by the EEC to discover and select one or more 5GMS EAS instances to serve media streaming sessions. (See clause 7.10.3.3.)
<i>easRelocationRequirements</i>	M1EASRelocation Requirements	0..1	EAS relocation tolerance and requirements. If not present, the 5GMS AF shall assume that the application is unaware of context transfer and that transfers to a target 5GMS EAS are allowed. (See clause 7.10.3.4.)

7.10.3.2 EdgeManagementMode enumeration

The *EdgeManagementMode* enumeration is specified in table 7.10.3.2-1 below:

Table 7.10.3.2-1: Definition of EdgeManagementMode enumeration

Enumeration value	Description
<i>EM_AF_DRIVEN</i>	The 5GMS AF, in coordination with the Media Session Handler, assigns edge resources and directs application traffic to the 5GMS EAS instance transparently to the application running on the UE.
<i>EM_CLIENT_DRIVEN</i>	An Application Client running on the UE explicitly manages edge resources via the EES at reference point EDGE-1.

7.10.3.3 EASRequirements type

The *EASRequirements* type is specified in table 7.10.3.3-1 below:

Table 7.10.3.3-1: Definition of EASRequirements type

Property name	Type	Cardinality	Description
<i>easProviderIds</i>	array(string)	0..1	The set of acceptable providers of 5GMS EAS instances associated with this Provisioning Session. If empty, EAS instances from any provider are acceptable.
<i>easId</i>	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.
<i>easType</i>	string	0..1	The type of 5GMS EAS instances associated with this Provisioning Session.
<i>easFeatures</i>	array(string)	0..1	5GMS EAS service features required to be supported by EAS instances associated with this Provisioning Session. If empty, 5GMS EAS instances of the specified <i>easType</i> with any feature set are acceptable.
<i>serviceKpi</i>	EASServiceKPI	0..1	Service characteristics required to be satisfied by 5GMS AS EAS instances associated with this Provisioning Session. If absent, 5GMS EAS instances with any service characteristics are acceptable.
<i>serviceArea</i>	GeographicalServiceArea	0..1	The list of geographical areas that 5GMS EAS instances associated with this Provisioning Session are required to serve. If absent, 5GMS EAS instances shall serve all geographical areas whenever possible.
<i>serviceAvailabilitySchedule</i>	array(ScheduledCommunicationTime)	0..1	The required availability schedule for 5GMS EAS instances associated with this Provisioning Session. If omitted, 5GMS EAS instances are required to be available at all times.
<i>serviceContinuityScenarios</i>	array(ACRScenario)	0..1	The Application Context Relocation scenarios that 5GMS EAS instances associated with this Provisioning Session are required to support for service continuity. If omitted 5GMS EAS instances are not required to support service continuity across EAS relocation.
NOTE: Data types <i>ScheduledCommunicationTime</i> , <i>GeographicalServiceArea</i> , <i>EASServiceKPI</i> , and <i>ACRScenario</i> are defined in TS 29.558 [43].			

7.10.3.4 M1EASRelocationRequirements type

The *M1ACRRequirements* type is specified in table 7.10.3.4-1 below:

Table 7.10.3.4-1: Definition of M1EASRelocationRequirements type

Property name	Type	Cardinality	Description
<i>tolerance</i>	EASRelocationTolerance	1..1	Indicates whether the 5GMS EAS instance tolerates Application Context Relocation. (See clause 6.4.4.4.) If set to <i>RELOCATION_INTOLERANT</i> , the other properties in this data type shall be ignored.
<i>maxInterruptionDuration</i>	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 5GMS EAS instance shall not be performed.
<i>maxResponseTimeDifference</i>	UIntegerRm	0..1	The maximum allowed difference between the previously experienced average User Plane network latency to the source 5GMS EAS instance and the expected latency to the target 5GMS EAS instance, expressed in milliseconds.

7.11 Event Data Processing Provisioning API

7.11.1 General

The Event Data Processing Provisioning API is used by a 5GMS Application Provider to provide Event Data Processing Configurations to the Data Collection AF instantiated in the 5GMS AF. Each such configuration is represented by an *EventDataProcessingConfiguration* resource, the data model of which is specified in clause 7.11.3 below. It comprises processing rules and parameters expressed by Data Access Profiles 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 7.11.2.

7.11.2 Resource structure

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

{apiRoot}/3gpp-m1/{apiVersion}/provisioning-sessions/{provisioningSessionId}/

Table 7.11.2-1 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 7.11.2-1: Operations supported by the Data Exposure Restriction API

Operation	Sub-resource path	Allowed HTTP method(s)	Description
Create Event Data Processing Configuration	event-data-processing-configurations	POST	Used to create a new Event Data Processing Configuration resource.
Retrieve Event Data Processing Configuration	event-data-processing-configurations/{ <i>EventDataProcessingConfigurationId</i> }	GET	Used to retrieve an existing Event Data Processing Configuration.
Update Event Data Processing Configuration		PUT, PATCH	Used to modify an existing Event Data Processing Configuration.
Destroy Event Data Processing Configuration		DELETE	Used to destroy an existing Event Data Processing Configuration.

7.11.3 Data model

7.11.3.1 EventDataProcessingConfiguration resource type

The data model for the *EventDataProcessingConfiguration* resource is specified in table 7.11.3-1 below:

Table 7.11.3-1: Definition of EventDataProcessingConfiguration resource

Property name	Type	Cardinality	Description
<i>eventDataProcessingConfigurationId</i>	ResourceId	1..1	An identifier for this Event Data Processing Configuration that is unique within the scope of the enclosing Provisioning Session.
<i>eventId</i>	AfEvent	1..1	One of the enumerated values specified in clause 5.6.3.3 of TS 29.517 [46] relating to 5G Media Streaming.
<i>authorizationUrl</i>	Url	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.
<i>dataAccessProfiles</i>	Array(Data Access Profile)	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 [47].) The controlled vocabularies to be used with <i>DataAccessProfile.parameters</i> are specified in annex E of the present document.

8 Media Ingest and Publish (M2) protocols

8.1 General

The set of content protocols supported by the 5GMS AS is listed in table 8.1-1 below:

Table 8.1-1: Supported content protocols

Description	Term identifier	Clause
Content ingest protocols at interface M2d		
HTTP pull-based content ingest protocol	<i>urn:3gpp:5gms:content-protocol:http-pull-ingest</i>	8.2
DASH-IF push-based content ingest protocol	<i>urn:3gpp:5gms:content-protocol:dash-if-ingest</i>	8.3
Content egest protocols at interface M2u		

8.2 HTTP pull-based content ingest protocol

If *IngestConfiguration.protocol* is set to *urn:3gpp:5gms:content-protocol:http-pull-ingest* in the Content Hosting Configuration, media resources shall be ingested by the 5GMSd AS using HTTP [9]. The *IngestConfiguration.pull* property shall be set to *True*, indicating that a Pull-based protocol is used. The *IngestConfiguration.baseURL* property shall point at the 5GMSd Application Provider's origin server, as specified in table 7.6.3.1-1, and may indicate the use of HTTPS [16].

When the 5GMSd AS receives a request for a media resource at interface M4d that cannot be satisfied from its content cache, the request shall be transformed into a corresponding HTTP GET request directed to the 5GMSd Application Provider's origin server via interface M2d as follows:

1. The prefix of the request URL indicated in the *DistributionConfiguration.baseURL* of the applicable Content Hosting Configuration is replaced with that of the corresponding *IngestConfiguration.baseURL*.

NOTE 1: It is the responsibility of the 5GMSd AF to assign unique M4d base URLs to each provisioned Content Hosting Configuration so as to ensure that this substitution is unambiguous.

2. The path rewrite rules (if provisioned in *DistributionConfiguration.PathRewriteRules*) are applied in strict order to the remainder of the request URL (i.e., the path segments following *DistributionConfiguration.baseURL*). The *requestPathPattern* of the first matching path rewrite rule is replaced with the corresponding *mappedPath*.

In the case where the 5GMSd Application Provider's origin server issues an HTTP 3xx redirect at reference point M2d pointing to another location, the 5GMSd AS shall issue an equivalent HTTP redirect to the Media Player via reference point M4d whose location is a dynamically generated M4d endpoint. Requests to this location shall be rewritten by the 5GMSd AS to the target location of the M2d redirection.

- NOTE 2: This explicit handling of HTTP redirects received by the 5GMSd AS at reference point M2d ensures that it is not bypassed by the Media Player. The general concept underlying this is commonly referred to as a "reverse mapping rule" by HTTP reverse proxies.

8.3 DASH-IF push-based content ingest protocol

If *IngestConfiguration.protocol* is set to *urn:3gpp:5gms:content-protocol:dash-if-ingest* in the Content Hosting Configuration, media resources shall be ingested by the 5GMSd AS as specified by the DASH-IF Live Media Ingest specification [3]. The *IngestConfiguration.pull* property shall be set to *False*, indicating that a Push-based protocol is used. The *IngestConfiguration.baseURL* property shall be set by the 5GMSd AF to the base URL that is to be used by the 5GMSd Application Provider to upload the DASH segments and MPD(s) to the 5GMSd AS at reference point M2d.

9 Internal (M3) APIs

APIs of this reference point are not specified within this release.

10 Media Streaming (M4) APIs

10.1 General

This clause deals with the interface and APIs for media streaming for different distribution formats and protocols. TS 26.511 [35] defines the integration of several media codecs into 5G Media Streaming, and provides requirements and recommendations for the support of these media profiles in specific 5G Media Streaming profiles. However, 5GMS is not restricted to the media profiles defined in TS 26.511 [35]. Any CMAF media profile may be used and distributed within 5G Media Streaming as long as it can be used with APIs and interfaces defined in this specification.

10.2 DASH Distribution

In the case of DASH distribution, M4d is relevant for the distribution as shown in figure 10.2-1.

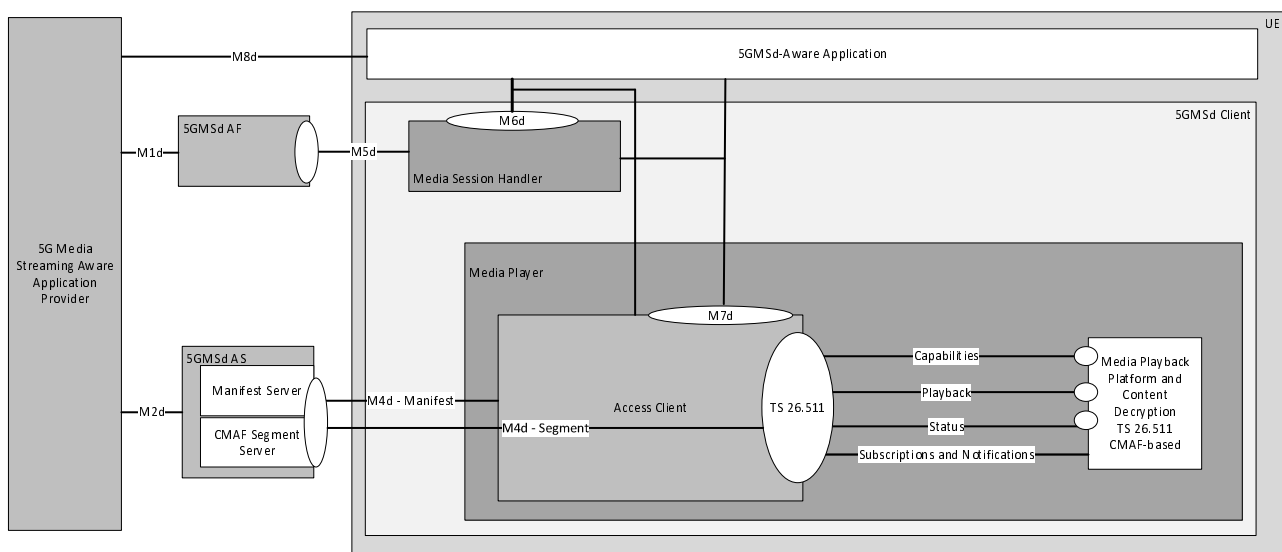


Figure 10.2-1: M4d usage for DASH distribution

For DASH-based distribution according to TS 26.247 [4] and ISO/IEC 23009-1 [32], two main formats are of relevance:

- 1) The Media Presentation Description (MPD) that is processed in the DASH Access Client.
- 2) The Segment formats that are passed through the DASH Access Client and processed in the Media Playback and Content Decryption Platform. Note that the DASH Access Client may parse Segments to extract for example Inband Events or producer reference times.

Other resources may be referenced in the MPD, for example DRM related information.

The Segment formats for DASH Streaming in the context of 5G Media Streaming are defined in TS 26.511 [35] based on the CMAF encapsulation. The DASH Access Client downloads the Segments from the SGMSd AS based on the instructions in the MPD and the instructions from the SGMSd-Aware Application through M7d (see clause 13 for details).

The interface between the DASH Access Client and the Media Playback and Content Decryption Platform as well as the SGMSd Client requirements for media codecs are documented in TS 26.511 [35].

The following requirements apply for M4d:

- 1) The Media Presentation Description (MPD) and Segments shall conform to an MPD according to ISO/IEC 23009-1 [32] or TS 26.247 [4].
- 2) The Segment formats should conform to CMAF addressable resources as well as to the requirements in TS 26.511 [35].

- 3) The Media Presentation should conform to the 5G Media Streaming DASH Interoperability Point as defined in clause 7.3.11 of TS 26.247 [4].

A 5GMSd Client shall support the 5G Media Streaming DASH Interoperability Point as defined in TS 26.247 [4], clause 7.3.11. A 5GMSd Client may support additional DASH profiles and interoperability points.

The MPD may contain a one or several **ServiceDescription** elements that include operational parameters. The MPD may also include multiple configurations for the media (different codecs, different content protection, different resolutions, etc.), for example for playback under different operating policies. The handling of this information is documented in clause 13.2.

11 Media Session Handling (M5) APIs

11.1 General

This clause defines the Media Session Handling APIs used by the Media Session Handler to access resources exposed by the 5GMS AF at interface M5.

NOTE: While the entirety of the Media Session Handling APIs apply to downlink media streaming, only a subset is applicable to uplink media streaming. Specifically, the Consumption Reporting API is not applicable to uplink media streaming.

11.2 Service Access Information API

11.2.1 General

The Service Access Information API is used by the Media Session Handler to obtain configuration information from the 5GMS AF that enables it to use the other Media Session Handling APIs specified in clause 11.3 *et seq.*

11.2.2 Resource structure

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

{apiRoot}/3gpp-m5/{apiVersion}/service-access-information/

The operations and the corresponding HTTP methods in Table 11.2.2-1 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	Sub-resource path	Allowed HTTP method(s)	Description
Fetch Service Access Information	<i>{provisioningSessionId}</i>	GET	Used to acquire the Service Access Information resource for the specified Provisioning Session. The <i>{provisioningSessionId}</i> uniquely identifies the Service Access Information Resource and is allocated by the 5GMS AF during creation of a Provisioning Session.

11.2.3 Data model

11.2.3.1 ServiceAccessInformation resource type

The data model for the *ServiceAccessInformation* resource is specified in table 11.2.3.1-1 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 11.2.3.1-1: Definition of ServiceAccessInformation resource

Property name	Type	Cardinality	Usage	Description	Applicability
<i>provisioningSessionId</i>	ResourceId	1..1	RO	Unique identification of the M1 Provisioning Session.	All types
<i>provisioningSessionType</i>	ProvisioningSessionType	1..1	RO	The type of Provisioning Session.	All types.
<i>streamingAccess</i>	object	0..1	RO	Present if Content Hosting is provisioned by the 5GMS Application Provider.	<i>downlink</i>
<i>entryPoints</i>	Array(M5MediaEntryPoint)	0..1	RO	A list of alternative Media Entry Points for the 5GMS Client to choose between.	
<i>locator</i>	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.	
<i>contentType</i>	string	1..1	RO	The MIME content type of this Media Entry Point.	
<i>profiles</i>	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.	
<i>eMBMSServiceAnnouncementLocator</i>	AbsoluteUrl	0..1	RO	A pointer to a document that defines a User Service Announcement for eMBMS where the service announcement file is available.	

Property name	Type	Cardinality	Usage	Description	Applicability
<i>clientConsumptionReportingConfiguration</i>	object	0..1	RO	Present if consumption reporting is provisioned by the 5GMS Application Provider.	<i>downlink</i>
<i>reportingInterval</i>	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.	
<i>serverAddresses</i>	array(AbsoluteUrl)	1..1	RO	A list of 5GMSd AF addresses (URLs) where the consumption reporting messages are sent by the Media Session Handler. See NOTE. Each address shall be an opaque base URL, following the 5GMS URL format specified in clause 6.1 up to and including the <i>{apiVersion}</i> path element.	

Property name	Type	Cardinality	Usage	Description	Applicability
<i>locationReporting</i>	boolean	1..1	RO	Stipulates whether the Media Session Handler is required to provide location data to the 5GMSd AF in consumption reporting messages (in case of MNO or trusted third parties). Shall be set false if <i>locationReporting</i> parameter is omitted from the <i>ConsumptionReporting Configuration</i> , as specified in table 7.7.3-1.	
<i>accessReporting</i>	boolean	1..1	RO	Stipulates whether the Media Session Handler is required to provide consumption reporting messages to the 5GMSd AF when the access network changes during a media streaming session. Shall be set false if <i>accessReporting</i> parameter is omitted from the <i>ConsumptionReporting Configuration</i> , as specified in table 7.7.3-1.	
<i>samplePercentage</i>	Percentage	1..1	RO	The percentage of media streaming 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 <i>samplePercentage</i> parameter is omitted from the <i>ConsumptionReporting Configuration</i> , as specified in table 7.7.3-1.	
<i>dynamicPolicyInvocation Configuration</i>	object	0..1	RO	Present if Policy Templates have been provisioned by the 5GMS Application Provider and at least one of them is in the <i>READY</i> state.	<i>downlink, uplink</i>
<i>serverAddresses</i>	array(AbsoluteUrl)	1..1	RO	A list of 5GMSd AF addresses (URLs) which offer the APIs for dynamic policy invocation sent by the Media Session Handler. See NOTE. Each address shall be an opaque base URL, following the 5GMS URL format specified in clause 6.1 up to and including the <i>{apiVersion}</i> path element.	
<i>policyTemplateBindings</i>	array(object)	1..1	RO	A list of duples, each one binding an external reference to a Policy Template resource identifier.	

Property name	Type	Cardinality	Usage	Description	Applicability
<i>externalReference</i>	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".	
<i>policyTemplateId</i>	ResourceId	1..1	RO	The resource identifier of a Policy Template tagged with <i>externalReference</i> that is in the <i>READY</i> state.	
<i>sdfMethods</i>	array(SdfMethod)	1..1	RO	A list of recommended service data flow description methods (descriptors), e.g. 5-tuple, ToS, 2-tuple, etc., which should be used by the Media Session Handler to describe the service data flows for the traffic to be policed.	

Property name	Type	Cardinality	Usage	Description	Applicability
<i>clientMetricsReportingConfigurations</i>	array(object)	0..1	RO	Present if metrics reporting is provisioned by the 5GMS application Provider. If present, contains one or more client metrics reporting configurations.	<i>downlink, uplink</i>
<i>metricsReportingConfigurationId</i>	ResourceId	1..1	RO	The identifier of this metrics reporting configuration, unique within the scope of <i>provisioningSessionId</i> . The value shall be the same as the corresponding identifier provisioned at reference point M1.	
<i>serverAddresses</i>	array(AbsoluteUrl)	1..1	RO	A list of 5GMS AF addresses to which metrics reports shall be sent. See NOTE 1. Each address shall be an opaque base URL, following the 5GMS URL format specified in clause 6.1 up to and including the <i>{apiVersion}</i> path element.	
<i>sliceScope</i>	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 slices.	
<i>scheme</i>	Uri	1..1	RO	A URI identifying the metrics reporting scheme that metrics reports shall use (see clause 4.7.5).	
<i>dataNetworkName</i>	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.	
<i>reportingInterval</i>	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.	
<i>samplePercentage</i>	Percentage	1..1	RO	The percentage of media streaming sessions that shall report metrics, expressed as a floating point value between 0.0 and 100.0.	

Property name	Type	Cardinality	Usage	Description	Applicability
<i>urlFilters</i>	array(string)	0..1	RO	A non-empty list of Media Entry Point URL patterns for which metrics reporting shall be done. The format of each pattern shall be a regular expression as specified in [5]. If not specified, reporting shall be done for all media streaming sessions.	
<i>samplingPeriod</i>	DurationSec	1..1	RO	The time interval the 5GMS Client should wait between sampling the QoE metrics specified by this metrics reporting configuration.	
<i>metrics</i>	array(Uri)	1..1	RO	A list of metrics which shall be reported, each indicated using a fully-qualified term identifier per clause E.2. If empty, the complete (or default if applicable) set of metrics associated with the specified <i>scheme</i> shall be collected and reported.	
<i>networkAssistance Configuration</i>	object	0..1	RO	Present if network assistance is provisioned by the 5GMS System Operator.	<i>downlink, uplink</i>
<i>serverAddresses</i>	array(AbsoluteUrl)	1..1	RO	A list of 5GMS AF addresses (URLs) that offer the APIs for 5GMS AF-based Network Assistance, for access by the 5GMSd Media Session Handler. See NOTE 1. Each address shall be an opaque URL, following the 5GMS URL format specified in clause 6.1 up to and including the { <i>apiVersion</i> } path element.	
<i>clientEdgeResources Configuration</i>	object	0..1	RO	Present only for Provisioning Sessions with client-driven edge computing management mode provisioned.	<i>Downlink, uplink</i>
<i>eligibilityCriteria</i>	EdgeProcessing Eligibility Criteria	0..1	RO	Conditions for activating edge resources for media streaming sessions in the scope of this Service Access Information. (See clause 6.4.3.8.)	
<i>easDiscoveryTemplate</i>	EASDiscovery Template	1..1	RO	A template for the EAS discovery filter that shall be used by the EEC to discover and select a 5GMS EAS instance to serve media streaming sessions in the scope of this Service Access Information. (See clause 11.2.3.2.)	

Property name	Type	Cardinality	Usage	Description	Applicability
<i>easRelocation Requirements</i>	M5EASRelocation Requirements	0..1	RO	EAS relocation tolerance and requirements. If absent, the EEC shall assume that relocation is tolerated by all 5GMS EAS instances in the scope of this Service Access Information. (See clause 11.2.3.3.)	
NOTE 1: In deployments where multiple instances of the 5GMSd AF expose the Media Session Handling APIs at 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 AF instance.					
NOTE 2: The <i>Snssai</i> data type is specified in TS 29.571 [12].					

11.2.3.2 EASDiscoveryTemplate type

Table 11.2.3.2-1 Definition of EASDiscoveryTemplate type

Property name	Type	Cardinality	Description
<i>easId</i>	string	0..1	The application identifier of the EAS, e.g. FQDN, URI. If omitted, any 5GMS EAS instance matching the other criteria specified in the template are acceptable. Corresponding to <i>EasCharacteristics.easId</i> , as specified in clause 6.3.5.2.7 of TS 24.558 [43].
<i>easType</i>	string	0..1	If present, a non-empty string indicating the type of 5GMS EAS required to support media streaming sessions in the scope of this discovery template. Corresponding to <i>EasCharacteristics.easType</i> , as specified in clause 6.3.5.2.7 of TS 24.558 [43].
<i>easProviderIds</i>	array(string)	0..1	The set of acceptable EAS provider identifiers. If omitted, 5GMS EAS instances of the specified <i>easType</i> from any provider are acceptable. Corresponding to <i>EasCharacteristics.easProvId</i> , as specified in clause 6.3.5.2.7 of TS 24.558 [43].
<i>easFeatures</i>	array(string)	0..1	The required service features for the EAS to serve this session. If omitted, 5GMS EAS instances of the specified <i>easType</i> with any feature set are acceptable. Corresponding to <i>EasCharacteristics.svcFeats</i> , as specified in clause 6.3.5.2.7 of TS 24.558 [43].
NOTE: At least one of the properties shall contain a value.			

11.2.3.3 M5EASRelocationRequirements type

Table 11.2.3.3-1: Definition of M5EASRelocationRequirements type

Property name	Type	Cardinality	Description
<i>tolerance</i>	EASRelocation Tolerance	1..1	Indicates whether the 5GMS EAS instance tolerates relocation. (See clause 6.4.4.4.)
<i>maxInterruptionDuration</i>	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 5GMS AS EAS instance shall not be performed.

11.2.4 Operations

This clause defines the behaviour that is expected from the 5GMS AF when a Service Access Information resource is acquired by the Media Session Handler. The main operation that is performed is to look up or generate the Service Access Information corresponding to the requested Provisioning Session.

11.3 Consumption Reporting API

11.3.1 General

The Consumption Reporting API allows the Media Session Handler to report downlink media consumption to the 5GMSd AF. The API defines data models, resources and the related procedures for the creation and management of the consumption reporting procedures. This procedure is configured by the *ServiceAccessInformation* resource, as defined in clause 11.2.3.

11.3.2 Reporting procedure

Consumption reports shall be submitted to a 5GMSd AF endpoint according to the following general URL format:

```
{apiRoot}/3gpp-m5/{apiVersion}/consumption-reporting/{provisioningSessionId}
```

where the first three 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 11.2.3.1) and *{provisioningSessionId}* shall be substituted with the relevant Provisioning Session identifier obtained from Service Access Information (see clause 11.2.3).

The only HTTP method supported by this endpoint is POST.

11.3.3 Report format

11.3.3.1 ConsumptionReport format

This type represents the format of consumption report instance. This structure is used by the Media Session Handler to report the consumption.

Table 11.3.3.1-1: Definition of ConsumptionReport format

Property name	Data type	Cardinality	Description
<i>mediaPlayerEntry</i>	AbsoluteUrl	1..1	Identifies the Media Entry Point. In the case of DASH [32], this shall be the URL of the MPD at reference point M4d. For other types of media streaming, the content of this property is undefined.
<i>reportingClientId</i>	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.
<i>consumptionReportingUnits</i>	array(ConsumptionReportingUnit)	1..1	A list of consumption reporting units, ordered by start time. In the case of DASH [32], separate consumption reporting units shall be reported for each Adaptation Set selected for presentation by the Media Player.

11.3.3.2 ConsumptionReportingUnit type

This type represents a single consumption reporting unit.

Table 11.3.3.2-1: Definition of type ConsumptionReportingUnit

Property name	Data type	Cardinality	Description
<i>mediaConsumed</i>	string	1..1	Identifies the media consumed. In the case of DASH, the value of the Representation@id attribute shall be quoted. For other types of media streaming, the content of this property is undefined.
<i>clientEndpointAddress</i>	EndpointAddress	0..1	The IP address and port number of the Media Player endpoint used to access the media consumed. Present only if access reporting is enabled in the Consumption Reporting Configuration.
<i>serverEndpointAddress</i>	EndpointAddress	0..1	The IP address, port number and host name of the 5GMS AS endpoint used to access the media consumed. Present only if access reporting is enabled in the Consumption Reporting Configuration.
<i>startTime</i>	DateTime	1..1	The time when this consumption reporting unit started.
<i>duration</i>	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.
<i>locations</i>	array(TypedLocation)	0..1	A time-ordered list of 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 AF). The cardinality of objects in this array is 1..N.

11.4 Metrics Reporting API

11.4.1 General

The Metrics Reporting API allows the Media Session Handler to send QoE metrics reports to the 5GMS AF. This procedure is configured by the *ServiceAccessInformation* resource, as defined in clause 11.2.3. Note that multiple metrics configurations can be active at the same time, each identified by a unique *metricsReportingConfigurationId*.

11.4.2 Reporting procedure

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

```
{apiRoot}/3gpp-m5/{apiVersion}/metrics-reporting/{provisioningSessionId}/{metricsReportingConfigurationId}
```

where the first three elements shall be substituted by the 5GMS Client with one of the base URLs selected from the *clientMetricsReportingConfigurations.serverAddresses* array of the *ServiceAccessInformation* resource (see clause 11.2.3.1), *{provisioningSessionId}* shall be substituted with the relevant Provisioning Session identifier obtained from Service Access Information (see clause 11.2.3) and *{metricsReportingConfigurationId}* shall be substituted with the relevant Metrics Reporting Configuration identifier.

The only HTTP method supported by this endpoint is POST.

11.4.3 Report format

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

NOTE: For downlink media streaming, TS 26.247 [7] clauses 10.6.1 and 10.6.2 specify the required MIME content type and metrics report format for the 3GPP `urn:3GPP:ns:PSS:DASH:QM10` metrics reporting scheme. For virtual reality media the report format is further extended as defined in TS 26.118 [42] clause 9.4.

In XML documents representing metrics reports for 3GP-DASH downlink media streaming services, the `ReceptionReport@clientID` attribute, if present and is available to the Media Session Handler, should be a GPSI value as defined by TS 23.003 [7]. Otherwise, this attribute should be represented by a stable and globally unique string.

11.5 Dynamic Policies API

11.5.1 Overview

The Dynamic Policies 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 streaming session by invoking RESTful operations on the 5GMS AF at interface M5. The API defines a set of data models, resources and the related procedures for the creation and management of the dynamic policy request.

Application Identifiers, referring to one or more Packet Flow Description (PFD), may be used as alternative traffic filtering parameters for dynamic policy invocation. The 5GMSd AF shall first provision a PFD in the 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 [12]. 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 identifications.

NOTE: The PFDF is a functionality within the NEF.

11.5.2 Resource structure

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

`{apiRoot}/3gpp-m5/{apiVersion}/dynamic-policies/`

where the first three elements shall be substituted by the 5GMS Client with one of the URLs selected from the `dynamicPolicyInvocationConfiguration.serverAddresses` array of the `ServiceAccessInformation` resource (see clause 11.2.3.1).

Table 11.5.2-1 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 11.5.2-1: Operations supported by the Dynamic Policies API

Resource name	Sub-resource path	Allowed HTTP methods	Description
Dynamic Policies		POST	Create a new Dynamic Policy resource. If the operation succeeds, the URL of the created Dynamic Policy Instance resource shall be returned in the <code>Location</code> header of the response.
Dynamic Policy	<code>{dynamicPolicyId}</code>	GET	Retrieve an existing Dynamic Policy resource.
		PUT	Replace an existing Dynamic Policy resource.
		PATCH	Modify an existing Dynamic Policy resource.
		DELETE	Delete an existing Dynamic Policy resource.

11.5.3 Data model

11.5.3.1 DynamicPolicy resource

The *DynamicPolicy* resource is specified in table 11.5.3.1-1 below.

Table 11.5.3.1-1: Definition of Dynamic Policy resource

Property name	Data type	Cardinality	Usage	Description
<i>dynamicPolicyId</i>	ResourceId	1..1	RO	Unique identifier for this Dynamic Policy.
<i>policyTemplateId</i>	ResourceId	1..1	C: RW R: RO U: RW	Identifies the Policy Template which should be applied to the application flow(s).
<i>serviceDataFlowDescriptions</i>	array(ServiceDataFlowDescription)	1..1	C: RW R: RO U: RW	Describes the service data flows managed by this Dynamic Policy.
<i>mediaType</i>	MediaType	0..1	C: RW R: RO U: RW	The type of media carried by the application flows listed in <i>serviceDataFlowDescriptions</i> .
<i>provisioningSessionId</i>	ResourceId	1..1	C: RW R: RO U: RW	Provisioning Session identifier obtained from Service Access Information (see clause 11.2.3). Uniquely identifies Provisioning Session, which is linked to the Application Service Provider.
<i>qosSpecification</i>	M5QoSSpecification	0..1	C: RW R: RO U: RW	Describes the network Quality of Service properties of this Dynamic Policy.
<i>enforcementMethod</i>	string	0..1	C: RO R: RO U: RO	Description of the Policy Enforcement Method. The parameter is set by the 5GMSd AF.
<i>enforcementBitRate</i>	integer	0..1	C: RO R: RO U: RO	Description of the enforcement bit rate.

11.5.4 Operations

This clause defines the behaviour that is expected when activating a Dynamic Policy Instance.

The *policyTemplateId* property uniquely identifies the Policy Template with which the Dynamic Policy Instance is associated.

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

The Dynamic Policy resource contains a *serviceDataFlowDescriptions* property which contains a set of service data flow templates according to TS 23.503 [33]. Each service data flow template contains one of:

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

When the Media Session Handler is attempting to activate a QoS-related Dynamic Policy Template, then the *qosSpecification* property shall be present and it shall contain the following properties:

- *marBwDIBitRate* or *marBwUIBitRate*, indicating the maximum requested bit rate by the Media Session Handler.
- *mirBwDIBitRate* or *mirBwUIBitRate*, indicating the minimum requested bit rate by the Media Session Handler.
- *minDesBwDIBitRate* or *minDesBwUIBitrate*, indicating the minimum bit rate desired by the Media Session Handler.

When the 5G System employs a traffic enforcement function to ensure that the traffic is complying a certain traffic policy, the Dynamic Policy resource may contain the following two properties:

- an *enforcementMethod*, indicating the type of enforcement method (like leaky bucket).
- an *enforcementBitrate* property, indicating the maximal permitted bit rate.

11.6 Network Assistance API

11.6.1 Overview

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

11.6.2 Resource structure

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

{apiRoot}/3gpp-m5/{apiVersion}/network-assistance/

where the first three elements shall be substituted by the 5GMS Client with one of the URLs selected from the *networkAssistanceConfiguration.serverAddresses* array of the *ServiceAccessInformation* resource (see clause 11.2.3.1).

Table 11.6.2-1 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 11.6.2-1: Operations supported by the Network Assistance API

Operation	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.
Fetch a Network Assistance Session resource	<i>{naSessionId}</i>	GET	Fetch the properties of an existing Network Assistance Session.
Update a Network Assistance Session resource	<i>{naSessionId}</i>	PUT, PATCH	Update the properties of an existing Network Assistance Session.
Request a bit rate recommendation	<i>{naSessionId}/recommendation</i>	GET	Obtain a bit rate recommendation for the next recommendation window.
Request a delivery boost	<i>{naSessionId}/boost-request</i>	POST	Request a delivery boost for the next recommendation window.
Terminate Network Assistance Session	<i>{naSessionId}</i>	DELETE	Terminate a Network Assistance session.

11.6.3 Data model

11.6.3.1 NetworkAssistanceSession resource

The *NetworkAssistanceSession* resource is specified in table 11.6.3.1-1 below.

Table 11.6.3.1-1: Definition of NetworkAssistanceSession resource

Property name	Type	Cardinality	Usage	Description
<i>naSessionId</i>	ResourceId	1..1	C: RO R: RO U: RO	Unique identifier for this Network Assistance Session.
<i>provisioningSessionId</i>	ResourceId	1..1	C: RW R: RO U: RW	Provisioning Session identifier obtained from Service Access Information (see clause 11.2.3). Uniquely identifies Provisioning Session, which is linked to the Application Service Provider.
<i>serviceDataFlowDescriptions</i>	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).
<i>mediaType</i>	MediaType	0..1	C: RW R: RO U: RW	The type of media carried by the application flows listed in <i>serviceDataFlowDescriptions</i> .
<i>policyTemplateId</i>	ResourceId	0..1	C: RW R: RO U: RW	Identification of the policy (if any) that is in force for the media streaming session.
<i>requestedQoS</i>	M5QoSSpecification	0..1	C: RW R: RO U: RW	The requested QoS parameters.
<i>recommendedQoS</i>	M5QoSSpecification	0..1	C: RO R: RO U: RO	The QoS parameters currently recommended by the 5GMS AF.
<i>notificationURL</i>	AbsoluteUrl	0..1	C: RO R: RO U: RO	A URL to the MQTT channel over which notifications are to be sent by the 5GMS AF for this session. When set, the Media Session Handler shall subscribe to this channel. The notification messages shall be in the form of the <i>M5QoSSpecification</i> data type.

11.6.4 Operations

11.6.4.1 Create Network Assistance session

This clause defines the behaviour that is expected when creating a Network Assistance session.

The Media Session Handler uses the `POST` HTTP method to create a Network Assistance session with the 5GMS AF. The request includes a *NetworkAssistanceSession* resource representation in the message body.

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

The Media Session Handler populates the *NetworkAssistanceSession* 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 5GMS AF subsequently uses this information to execute Network Assistance operations in the 5GC.)

The *serviceDataFlowDescriptions* property contains a set of service data flow templates according to TS 23.503 [33]. Each service data flow template contains one of:

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

The *requestedQoS* property is used by the Media Session Handler to specify a network QoS it initially wishes to use for the media streaming session. If the *policyTemplateId* property is also populated in the *NetworkAssistanceSession* resource, the 5GMS 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 *NetworkAssistanceSession* resource but the *policyTemplateId* is populated, the 5GMS 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 5GMS AF within the scope of the Network Assistance session are constrained only by the policies of the PCF.

The 5GMS AF returns the Network Assistance session identifier if session setup was successful, otherwise an error code is returned without a Network Assistance session identifier.

The 5GMS Client uses the Network Assistance session resource identifier (*naSessionId*) provided by the 5GMS AF to refer all subsequent API calls to the 5GMS AF applicable to that Network Assistance session.

11.6.4.2 Retrieve Network Assistance session

The 5GMS Client uses the GET HTTP method with the Network Assistance Session resource identifier to retrieve a Network Assistance Session resource from the 5GMS AF. The 5GMS AF returns the Network Assistance Session resource if retrieval was successful, otherwise an appropriate error code is returned without the session resource in case of failure.

11.6.4.3 Request bit rate recommendation

The Media Session Handler uses the GET HTTP method with the sub-resource path specified in table 11.6.2-1 to request a bit rate recommendation from the 5GMS AF. The 5GMS AF shall return the recommended bit rate in an HTTP response body of type *M5QoSSpecification* if a bit rate recommendation could be obtained, otherwise an appropriate HTTP error code shall be returned with no response body.

- For a downlink media streaming session, the recommended minimum and maximum downlink bit rates shall be indicated in the properties *mirBwDIBitRate* and *marBwDIBitRate* respectively. The 5GMSd Client shall ignore the mandatory properties related to uplink streaming, i.e. *mirBwUIBitRate* and *marBwUIBitRate*.
- For an uplink media streaming session, the recommended minimum and maximum uplink bit rates shall be indicated in the properties *mirBwUIBitRate* and *marBwUIBitRate*, respectively. The 5GMSu Client shall ignore the mandatory properties related to downlink streaming, i.e. *mirBwDIBitRate* and *marBwDIBitRate*.

If a unique recommendation is given by the 5GMS AF then this recommended bit rate shall be set in both of these properties. The optional properties *minDesBwDIBitRate*, *minDesBwUIBitRate*, *desLatency* and *desLoss* shall not be included in the response.

11.6.4.4 Request delivery boost

The Media Session Handler uses the POST HTTP method with the sub-resource path specified in table 11.6.2-1 to request a delivery boost from the 5GMS AF. The 5GMS AF shall respond with the *OperationSuccessResponse* data type indicating whether or not the delivery boost will be attempted by the network within an upcoming nominal time period.

11.6.4.5 Update Network Assistance session

The Media Session Handler uses the `PUT` or `PATCH` HTTP methods to replace the existing steaming session parameters with new settings. For example, any change to the Policy Template currently in force resulting from an invocation of the Dynamic Policies API (see clause 11.5) should also be notified to the 5GMS AF using this operation if a Network Assistance session has been created for the media streaming session in question.

The 5GMS AF returns the *NetworkAssistanceSession* resource with settings resulting from the `PUT` or `PATCH` update operation.

11.6.4.6 Destroy Network Assistance session

The Media Session Handler uses the `DELETE` HTTP method to terminate the indicated Network Assistance session. The 5GMS AF returns an appropriate response code. If the termination was successful, then any subsequent calls referring to the terminated session will result in the error *404 (Not Found)*.

12 UE Media Session Handling (M6) APIs for uplink and downlink

12.1 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.

12.2 Media Session Handling for Downlink media streaming – APIs and Functions

12.2.1 Overview

In the following, it is assumed that the Media Session Handler for downlink media streaming adheres to a basic set of functionalities as shown in Figure 12.2.1-1.

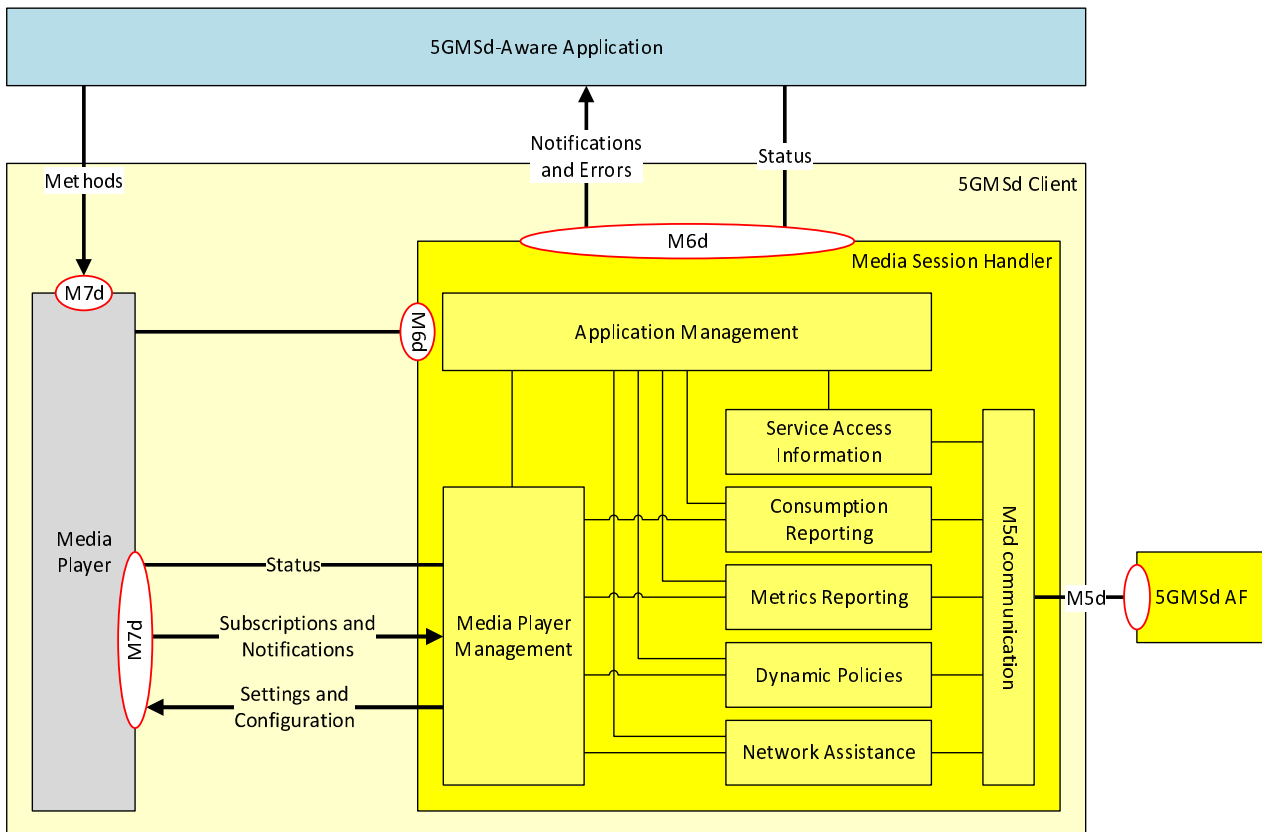


Figure 12.2.1-1: Usage of M6d in Media Downlink Streaming

The Media Session Handler is considered to run as a service in the background, and is invoked for a media session once a media player in the 5GMSd streaming client is activated with an MPD URL of media MIME type "application/dash+xml". Based on the MPD URL, the Media Session Handler may initiate communication with the 5GMSd AF through M5d.

NOTE: The initiation of the Media Session Handler for other media types than DASH is for further study.

For an ongoing 5G Media Streaming session, the Media Session Handler is given the following authorizations:

- 1) The ability to do status query on M7d. For details see clause 13.
- 2) The ability to process notifications and error on M7d. For details see clause 13.
- 3) The ability to configure certain parameters on the media player based on M7d. For details again see clause 13.

In addition, the MSH can provide information on M6d to the application and possibly delegated to Media Player using M6d for each of the Media Session Handler functionalities, namely providing:

- 1) Notification and Error Events;
- 2) Status Information.

12.2.2 Media Session Handler model

12.2.2.1 State model

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

12.2.2.2 Media Session Handler internal properties

The Media Session Handler maintains internal properties as defined Table 12.2.2.2-1. Note that the parameters are conceptual and internal and only serve for the purpose to describe message generation on the API calls.

Table 12.2.2.2-1: Parameters of Media Session Handler

States and Parameters	Definition
<i>_Configuration</i>	
<i>_networkAssistance</i>	Network Assistance configuration.
<i>_policyTemplate</i>	Policy Template configuration.
<i>_consumptionReporting</i>	Consumption reporting configuration.
<i>_metricsReporting</i>	Metrics reporting configuration.
<i>_status[]</i>	The Media Session Handler maintains a status record.

12.2.2.3 Media Session Handler internal operations

This aspect is for further study.

12.2.2.4 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.

12.2.3 General

Table 12.2.3-1 provides a list status information that can be obtained from the Media Session Handler through reference point M6d.

Table 12.2.3-1: General Status Information

Status	Type	Parameter	Definition

Table 12.2.3-2 provides a list of general notification events exposed at reference point M6d.

Table 12.2.3-2: General Notification Events

Event	Definition	Payload
<i>SESSION_HANDLING_ACTIVATED</i>	Triggered when media session handling was activated for a specific Media Entry Point.	Media Entry Point URL.
<i>SESSION_HANDLING_STOPPED</i>	Triggered when media session handling stopped for a specific Media Entry Point.	Media Entry Point URL.

Table 12.2.3-3 provides a list of general error events exposed at reference point M6d.

Table 12.2.3-3: General Error Events

Status	Definition	Payload
<i>ERROR_SESSION_HANDLING</i>	Triggered when there is an error in the media session handling.	Not applicable.

12.2.4 Dynamic Policy Information

Details are for further study.

12.2.5 Network Assistance Information

Details are for further study.

12.2.6 Consumption Reporting Information

Table 12.2.6-1 provides a list status information that can be obtained from the Media Session Handler through reference point M6d.

Table 12.2.6-1: Status Information relating to Consumption Reporting

Status	Type	Parameter	Definition
<i>consumptionReport</i>	Object		The most recently sent consumption report.

Table 12.2.6-2 provides a list of general notification events exposed by the Media Session Handler at reference point M6d.

Table 12.2.6-2: Notification Events relating to Consumption Reporting

Status	Definition	Payload
<i>CONSUMPTION_REPORTING_ACTIVATED</i>	Consumption reporting has been activated.	Not applicable.
<i>CONSUMPTION_REPORTING_STOPPED</i>	Consumption reporting has been stopped.	Not applicable.
<i>NEW_CONSUMPTION_REPORT</i>	A new consumption report is available and has been sent.	Not applicable.

Table 12.2.6-3 provides a list of general error events exposed by the Media Session Handler at reference point M6d.

Table 12.2.6-3: Error Events relating to Consumption Reporting

Status	Definition	Payload
<i>ERROR_CONSUMPTION_REPORTING</i>	Error in consumption reporting occurred.	Server address, Provisioning Session Id, HTTP response code Error message.

12.2.7 Metrics Reporting Information

Table 12.2.7-1 provides a list of status information that can be obtained from the Media Session Handler through M6d.

Table 12.2.7-1: Status Information relating to Metrics Reporting

Status	Type	Definition
<i>lastMetricsReport</i>	Object	Status information relating to the last sent metrics report.
<i>provisioningSessionId</i>	ResourceId	The Provisioning Seession identifier for this metrics report.
<i>metricsReportingConfigurationId</i>	ResourceId	The metrics reporting configuration identifier for this report.
<i>scheme</i>	Uri	The metrics reporting scheme used by this metrics report (see clause 4.7.5).
<i>metricsReport</i>	Object	The most recently sent metrics report.

Table 12.2.7-2 provides a list of general notification events exposed at reference point M6d.

Table 12.2.7-2: Notification Events relating to Metrics Reporting

Event	Definition	Payload
<i>METRICS_REPORTING_ACTIVATED</i>	Metrics reporting has been activated.	Not applicable.
<i>METRICS_REPORTING_STOPPED</i>	Metrics reporting has been stopped.	Not applicable.
<i>NEW_METRICS_REPORT</i>	A new metrics report is available and has been sent.	Not applicable.

Table 12.2.7-3 provides a list of general error events exposed at reference point M6d.

Table 12.2.7-3: Error Events relating to Metrics Reporting

Error event	Definition	Payload
<i>ERROR_METRICS_REPORTING</i>	Error in metrics reporting occurred.	Server address, Provisioning Session Id, Metrics Reporting Configuration Id, HTTP response code Error message.

Details of status information for RAN-based metrics reporting are for further study.

12.3 Media Session Handling for Uplink Streaming – APIs and Functions

Details are for further study.

13 UE Media Stream Handler (M7) APIs for uplink and downlink

13.1 General

This clause defines a set of APIs and methods that permit an application or other UE functions to communicate with a Media Player or Media Streamer. The main focus of this clause is to formalize and harmonize commonly available proprietary APIs in order to support the usage of a Media Player or a Media Streamer in a 5G Media Streaming context.

The APIs specified in this clause are language- and runtime-independent. Implementations are expected to provide language bindings appropriate to the UE runtime environment.

13.2 DASH Media Player – APIs and Functions

13.2.1 Overview

In the following, it is assumed that the Media Player (in this case a DASH client) adheres to a basic set of functionalities as shown in Figure 13.2-1. The DASH client downloads, processes and presents a DASH Media Presentation by instruction of a 5GMSd-Aware Application using the M7d interface.

The 5GMSd-Aware Application can, in addition, configure the presentation of the media, can receive notifications on events, or can query the internal status of the DASH Player, also supported through M7d. Different functions of the DASH Access Client that are typically necessary to process a DASH Media Presentation, are shown in Figure 13.2-1. Additional functions may be available as well.

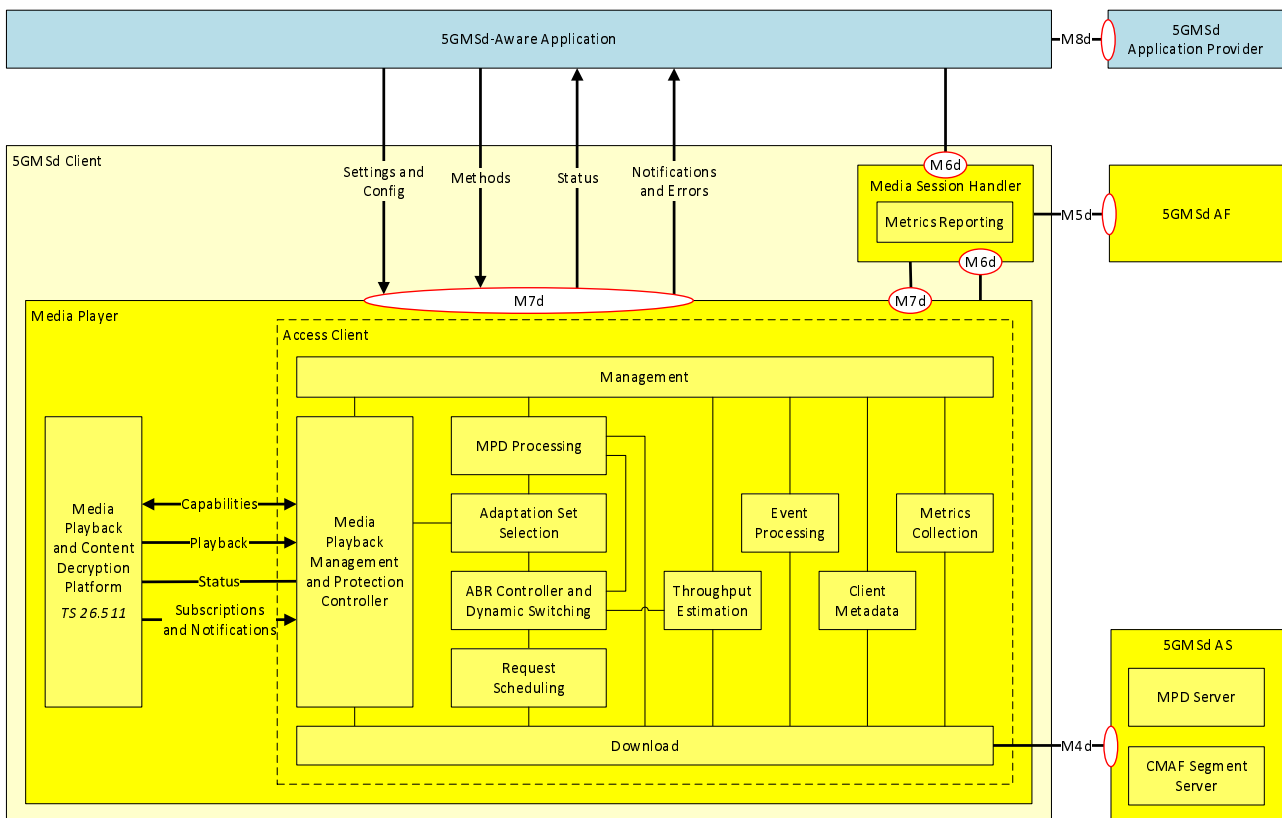


Figure 13.2.1-1: DASH Client Architecture

The key functionalities of each of the functions as shown in Figure 13.2-1 are summarized in the following:

- *5GMSd-Aware Application*: Application that makes use of the DASH/Media Player to playback a DASH Media Presentation using the APIs defined in this clause.
- *Media Player*: A complete player for the playback of a Media Presentation, including the Media Playback and Content Decryption Platform as defined in TS 26.511 [35].
- *Access Client*: A part of the DASH Player that accesses and downloads of the resources and provides the downloaded resources to the Media Playback Platform and Content Decryption for the playback of DASH content.
- *Management*: Controls all internal processes and the communication with the 5GMSd-aware application. In particular this includes the handling of service descriptions and operation points.
- *MPD Processing*: parses and processes the MPD and extracts the relevant information.
- *Adaptation Set Selection*: selects the Adaptation Set based on user, application and/or device capability information. Information provided through M7d may be used.

- *ABR Controller and Dynamic Switching*: runs adaptive bit rate logic and triggers adaptive switching of Representations. Information provided to the DASH client through M7d may be used.
- *Throughput Estimation*: estimates the throughput from the 5GMSd Application Server.
- *Metrics Logging*: logs relevant low-level metrics and provides those to the metrics aggregation and reporting functions in the Media Session Handler.
- *Media Playback Management and Protection Controller*: manages the media playback by moving downloaded information into media playback platform and also addresses handling of protection and DRM related information.
- *Media Playback and Content Decryption Platform*: plays back CMAF-based media content according to the playback requirements in TS 26.511 [35]. It also provides status information as well as events that maybe be provided through M7d.
- *Event Processing*: Processes DASH events and provides information to application as defined in TS 26.247 [4].

This clause focuses on Media Player related communication through M7d. In particular, the following aspects of M7d are defined:

- 1) Methods to interact with the Media Player are defined in clause 13.2.3.
- 2) Notification and Error Events are defined in clause 13.2.4.
- 3) Configuration and Settings APIs are defined in clause 13.2.5.
- 4) Status Information API is defined in clause 13.2.6.

The communication to the media playback platform is defined through the details in TS 26.511 [35].

A 5GMSd client for DASH distribution shall support the APIs defined in this clause 13.

NOTE: The initial APIs have largely been designed based on the dash.js APIs documented here: <http://cdn.dashjs.org/latest/jsdoc>.

13.2.2 Media Player model

Figure 13.2.2-1 provides an informative client state model in order to appropriately describe the messages on the Media streaming service API. Six different states are defined.

State changes may happen based on:

- Calls from application.
- Information provided in the Media Presentation Description (MPD).

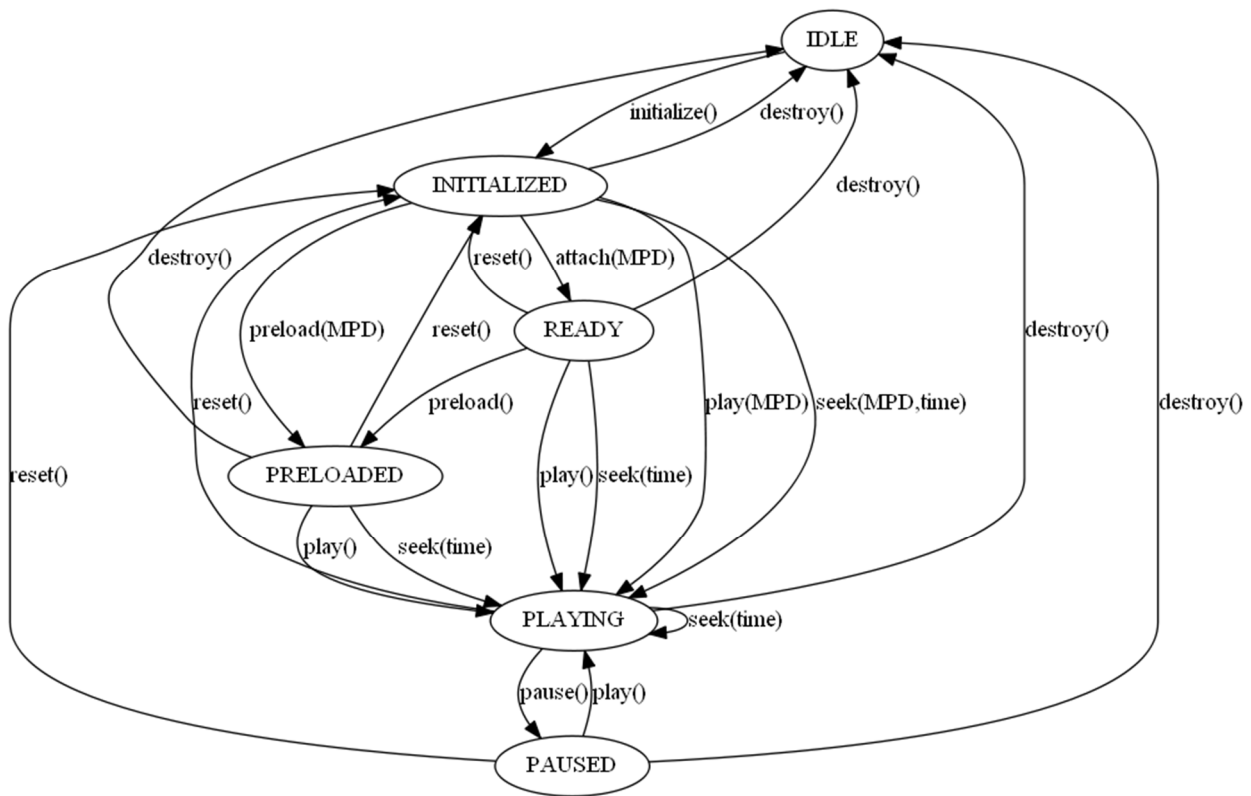


Figure 13.2.2-1: State Diagram for Media Player

Table 13.2.2-1 defines states for the Media Player. Detailed descriptions are provided in the following subclauses.

Table 13.2.2-1: States of Media Player

States	Definition
<i>IDLE</i>	The Media Player is not associated with any application.
<i>INITIALIZED</i>	The Media Player is associated with an application and the M7d API communication is established.
<i>READY</i>	The Media Player has loaded an MPD and is able to playback the media in this Media Presentation. It also updates the MPD according to the MPD update mechanism.
<i>PRELOADED</i>	The Media Player has pre-loaded all media information in order to start playback instantaneously. It also updates the MPD according to the MPD update mechanism.
<i>PLAYING</i>	The Media Player is playing the Media Presentation. It also updates the MPD according to the MPD update mechanism.
<i>PAUSED</i>	The playback of the Media Presentation is paused. It also updates the MPD according to the MPD update mechanism.

It is assumed that the DASH Access Client manages the playback of at most one CMAF track for each media type, namely one for video, one for audio and one for subtitles as defined in TS 26.511 [35]. Playback of multiple CMAF tracks of the same media type is not excluded for 5GMS, but details is for further study.

13.2.3 Methods

13.2.3.1 General

Based on the state model in clause 13.2.2, this clause introduces relevant procedures and API calls.

Table 13.2.3.1-1 provides an overview over the methods defined for the DASH-based streaming API. Note that in implementations, additional methods may be supported.

Table 13.2.3.1-1: Methods defined for DASH Streaming API

Method	State after success	Brief description	Clause
initialize()	<i>INITIALIZED</i>	The Media Player is created.	13.2.3.2
attach(MPD)	<i>READY</i>	sets a source URL to an MPD file or a previously downloaded and parsed MPD.	13.2.3.3
preload(MPD)	<i>PRELOADED</i>	Streaming the media is initiated.	13.2.3.4
play(MPD)	<i>PLAYING</i>	Playback of the media is initiated.	13.2.3.5
pause()	<i>PAUSED</i>	Playback of the media is paused.	13.2.3.6
seek(MPD, time)	<i>PLAYING</i>	The playback time of the media is altered.	13.2.3.7
reset()	<i>INITIALIZED</i>	All media related information is reset.	13.2.3.8
destroy()	<i>IDLE</i>	All media player related information is reset and API communication is stopped.	13.2.3.9

13.2.3.2 Initialize

This clause defines the `initialize()` method.

The Media Player is created by initializing using the `initialize()` method. The following functions are initialized:

- Media Playback Management in order to enable API-based communication through M7d. In particular, the M7d *Notifications and Errors API* (see clause 13.2.4) and the *Status Query* (see clause 13.2.5) are established.

13.2.3.3 Attach

This clause defines the `attach()` method.

The following pre-conditions apply:

- The MediaPlayer is be in *INITIALIZED* state.

An 5GMSd-Aware Application calls `attachMPD()` to set a source URL to an MPD file or a previously downloaded and parsed MPD.

The parameters of the method are defined in Table 13.2.3.3-1.

Table 13.2.3.3-1: Parameters for `attachMPD()`

Name	Type	Description
<i>urlOrMPD</i>	string Object	A URL to a valid MPD or a valid MPD as defined in ISO/IEC 23009-1 [32] or TS 26.247 [4]. The URL may be augmented by MPD Anchors as defined in ISO/IEC 23009-1 [32], clause C.4.

The following Media Player Actions are expected:

- The *Request Scheduling* and *Download* functions are established.
- If the input is a URL, the Media Player requests the MPD at the corresponding URL through M4d.
- If the MPD is not found after multiple retries, an error *ERROR_MPD_NOT_FOUND* is returned and the process is terminated.
- The *MPD Processing* function is established and the MPD parsed.
- If the MPD is not valid, an error *ERROR_MPD_NOT_VALID* is returned and the process is terminated.
- If the DASH Player does not support the profiles as indicated in the MPD, an error *ERROR_PROFILE_NOT_SUPPORTED* is returned and the process is terminated.

- Depending on the type of the MPD, possibly present anchors as well as the wall-clock time, the Media Player selects the Period in the content that is expected to be played next.
- The *Media Playback Management and Protection Controller* is established.
- The MPD is parsed for available Service Descriptions (including Media Subsets and Adaptation Sets). By using capability mechanisms defined in TS 26.511 [35] as well as using other information (language settings, output capabilities, accessibility settings), the Media Player identifies a set of permissible Service Descriptions including Media Subsets and Adaptation Sets. If no Adaptation Sets are capable to be played, an error *ERROR_MEDIA_NOT_SUPPORTED* is returned and the process is terminated.
- The available Service Descriptions including included Adaptation Sets are provided to the application through M7d.
- The application may select a Service Description instance as well as Adaptation Sets. Additional Service Descriptions parameters may be configured through M7d.
- Based on the service description parameters and selected Adaptation Sets:
 - the Operation Point parameters are set.
 - the *Media Playback Platform and Content Decryption* is established using the methods defined in TS 26.511.
 - The selected Adaptation Sets are initialized by downloading the relevant Initialization Segments/CMAF Headers through M4d in the Media Playback Platform as in TS 26.511 [35] establishing a track buffer for each selected media type.
- Depending on the MPD information and/or M7d configuration, one or more of the following functions may be established:
 - Metrics Logging and Collection
 - Event Processing and Notification
 - Client Metadata handling
- The Media Player is left in the *READY* state.

An application may use this method to load an MPD and in order to prepare playback. In case of errors notifications, it is up to the application to initiate appropriate actions.

13.2.3.4 Pre-load

This clause defines the `preload()` method.

The following pre-conditions apply:

- The MediaPlayer is in *INITIALIZED* or *READY* state.

An 5GMSd-Aware Application calls `preload()` to cause the player to begin streaming the media as set by the `attach()` method in preparation for playing.

The parameters of the method are defined in Table 13.2.3.4-1.

Table 13.2.3.4-1: Parameters for `attachSource()`

Name	Type	Description
<i>uriOrMPD</i>	string Object	A URL to a valid MPD or a valid MPD as defined in ISO/IEC 23009-1 [32] or TS 26.247 [4]. The URL may be augmented by MPD Anchors as defined in ISO/IEC 23009-1 [32], clause C.4.

The following Media Player Actions are expected:

- If in *INITIALIZED* state, the `attach()` method is invoked.

- Depending on the type of the MPD, possibly present anchors as well as the wall-clock time, and other MPD information, the earliest media time span for pre-loading is identified.
- The Access Client schedules and generates requests for the relevant media segments based on the ABR Controller information, as well as the throughput estimation and downloads this media.
- The Segments are downloaded from the corresponding URLs through M4d earliest at the segment availability start time of the Segments.
- The Segments are appropriately appended to the track buffers as established according to *Media Playback Platform and Content Decryption APIs*, following the description in TS 26.511 [35] for playback requirements.
- Configuration and service description parameters are taken into account, for example the content is continuously loaded to remain at the live edge following the latency requirements provided in the service description setting. Content not at the live edge is removed. For static services, the content is loaded from the beginning up to a suitable buffer duration, possibly as configured, and then downloading is stopped.
- Appropriate notifications and error messages are generated. For details refer to clause 13.2.5.
- Appropriate Status Information is generated. For details refer to clause 13.2.6.
- The Media Player is in *PRELOADED* state.

An application may use this method to preload media into the player in order to minimize the start-up time.

13.2.3.5 Play

This clause defines the `play()` method.

The following pre-conditions apply:

- The MediaPlayer is in *INITIALIZED* or *READY* or *PRELOADED* or *PAUSED* state.

An 5GMSd-Aware Application calls `play()` to cause the player to begin playback of the media as set by the `attach()` method.

The parameters of the method are defined in Table 13.2.3.5-1.

Table 13.2.3.5-1: Parameters for `play()`

Name	Type	Description
<i>urlOrMPD</i>	string Object	A URL to a valid MPD or a valid MPD as defined in ISO/IEC 23009-1 [32] or TS 26.247 [4]. The URL may be augmented by MPD Anchors as defined in ISO/IEC 23009-1 [32], clause C.4.

The following Media Player Actions are expected:

- If in *INITIALIZED* state, the `attach()` method is invoked.
- If in *PAUSED* state, the earliest media time is *MEDIA_TIME* (for details see clause 13.2.3.6), else, depending on the type of the MPD, possibly present anchors as well as the wall-clock time, and other MPD information, the earliest media time for start-up is identified.
- The Access Client checks the available buffer state of media in the Media Playback Platform. Based on this, the Access Client schedules and generates requests for the relevant media segments based on the ABR Controller information, as well as the throughput estimation and downloads this media.
- The Segments are downloaded from the corresponding URLs through M4d earliest at the segment availability start times.
- The media is appropriately appended to the *Media Playback Platform and Content Decryption APIs*, following the description in TS 26.511 [35] for playback requirements.

- Once a threshold for sufficient buffering is reached, the Media Playback platform is initiated to be started, i.e. a playback is initiated, following the description in TS26.511 [35] for playback requirements.
- The content is continuously streamed, downloaded and played back.
- Appropriate notifications and error messages are generated. For details refer to clause 13.2.4.
- Appropriate Status Information is generated. For details refer to clause 13.2.5.
- The Media Player is in *PLAYING* state.

An application may use this method to initiate playback of media.

13.2.3.6 Pause

This clause defines `pause()` method.

The following pre-conditions apply:

- The Media Player is in *PLAYING* state.

An 5GMSd-Aware Application calls `pause()` to cause the Media Playback Platform to pause playback.

No parameters are attached.

The following Media Player Actions are expected:

- The playback on the playback platform is paused and the media time is maintained as *MEDIA_TIME*.
- The Access Client checks the available buffer state of media in the Media Playback Platform. Based on this, the Access Client schedules and generates requests for the relevant media segments based on the ABR Controller information, as well as the throughput estimation and downloads this media.
- The media is downloaded from the corresponding URL through M4d earliest at the segment availability start time of the media.
- The media is appropriately appended to the *Media Playback Platform and Content Decryption* APIs, following the description in TS 26.511 [35] for playback requirements.
- Once the buffers are sufficiently filled, the client stops downloading.
- Appropriate notifications and error messages are generated. For details refer to clause 13.2.4.
- Appropriate Status Information is generated. For details refer to clause 13.2.5.
- The Media Player is in *PAUSED* state.

An application may use this method to play back media.

13.2.3.7 Seek

This clause defines `seek()` method.

The following pre-conditions apply:

- The MediaPlayer is in *INITIALIZED*, *READY*, *PRELOADED* or *PAUSED* state.

An 5GMSd-Aware Application calls `seek()` to cause the player to go a specific media time.

The parameters of the method are defined in Table 13.2.3.7-1.

Table 13.2.3.7-1: Parameters for seek()

Name	Type	Description
<i>urlOrMPD</i>	string Object	A URL to a valid MPD or a valid MPD. The URL may be augmented by MPD Anchors as defined in ISO/IEC 23009-1 [32], clause C.4.
<i>mediaTime</i>	Unsigned integer	The media time in milliseconds for playback.

The following Media Player Actions are expected:

- If in *INITIALIZED* state, the `attach()` method is carried out.
- If the `mediaTime` is not accessible return an error *ERROR_MEDIA_TIME_NOT_ACCESSIBLE* and terminate the process.
- The earliest media time is set to the `mediaTime`.
- The state is set to *PAUSED*.
- The `play()` command is issued.

An application may use this method to initiate playback of media.

13.2.3.8 Reset

This clause defines the `reset()` method.

The following pre-conditions apply:

- The Media Player may be in any state.

An 5GMSd-Aware Application calls `reset()` resets all information related to the media and the Media Presentation described by the MPD is destroyed.

No parameters are attached.

The following Media Player Actions are expected:

- The playback on the playback platform terminated.
- All open requests are cancelled.
- All scheduled requests are deleted.
- The current MPD is removed.
- The Media Player is left in the *INITIALIZED* state.

An application may use this method to terminate the playback of any media.

13.2.3.9 Destroy

This clause defines `destroy()` method.

The following pre-conditions apply:

- The Media Player may be in any state.

An 5GMSd-Aware Application calls `destroy()` resets all information related to the media and the network.

No parameters are attached.

The following Media Player Actions are expected:

- The playback on the playback platform terminated.
- All open requests are cancelled.
- All scheduled requests are deleted.
- The current MPD is removed.
- All network information is history is cleared.
- The Media Player is left in the *IDLE* state.

An application may use this method to terminate the playback of any media clear and download related information.

13.2.4 Configurations and settings API

DASH streaming may be configured with the parameters provided in Table 13.2.4-1. Note that these parameters may be set and they may also be observed.

Table 13.2.4-1: Configuration API

Status	Type	Definition
<i>source</i>	Object	Provides the MPD and all contained information.
<i>consumptionMode</i>	Enum	Defines two modes: <i>live</i> : in this case the target latency is maintained, if specified in the service description, according to the parameters <i>vod</i> : in this case the latency is set by the application and the latency settings are ignored.
<i>maxBufferTime</i>	Integer	Maximum buffer time in milliseconds for the service.
<i>serviceDescriptionId</i>	id	Selects a service description by selecting an identifier.
<i>serviceDescriptions[]</i>	Service description parameters	Configures a service description as defined in ISO/IEC 23009-1 [32], Annex K. This allows the application to define additional service descriptions beyond those defined in the MPD.
<i>id</i>	id	Sets a service description identifier different from the ones available in the service descriptions in the MPD or modifies existing service descriptions.
<i>serviceLatency</i>	Object	Sets service description parameters for the service latency, as defined in ISO/IEC 23009-1 [32], Table K.1.
<i>playBackRate</i>	Object	Sets service description parameters for the playback rate, as defined in ISO/IEC 23009-1 [32], Table K.2 when the service is consumed in live mode.
<i>operatingQuality</i>	Object	Sets service description parameters for the operating quality, as defined in ISO/IEC 23009-1 [32], Table K.3.
<i>operatingBandwidth</i>	Object	Sets service description parameters for the operating bandwidth, as defined in ISO/IEC 23009-1 [32], Table K.4.
<i>mediaSettings[]</i>	Media type audio, video, subtitle	Sets the selected Adaptation Set based on the available Adaptation Sets for each media type.
<i>metricsConfiguration[]</i>	Object	Defines the setting for collecting metrics.

13.2.5 Notifications and error events

Table 13.2.5-1 provides a list of notification events that are provided by the Media Player.

Table 13.2.5-1: Notification events

Status	Definition	Payload
<i>AST_IN_FUTURE</i>	Triggered when playback will not start yet as the MPD's availabilityStartTime is in the future.	Time before playback will start.
<i>AVAILABLE_MEDIA_CHANGED</i>	The list of available media has changed.	Media type: video, audio, subtitle, all
<i>BUFFER_EMPTY</i>	Triggered when the media playback platform's buffer state changes to stalled.	Media Type
<i>BUFFER_LOADED</i>	Triggered when the media playback platform's buffer state changes to loaded.	Media Type
<i>CAN_PLAY</i>	Sent when enough data is available that the media can be played.	Not applicable.
<i>MANIFEST_LOADED</i>	Triggered when the manifest load is complete	Not applicable.
<i>METRIC_ADDED</i>	Triggered every time a new metric is added.	
<i>METRIC_CHANGED</i>	The minimum bit rate that the ABR algorithms will choose. Use NaN for no limit.	
<i>METRIC_UPDATED</i>	Set to true if you would like DASH Client to keep downloading fragments in the background when the video element is paused.	
<i>METRICS_CHANGED</i>	Triggered whenever there is a change to the overall metrics.	
<i>OPERATION_POINT_CHANGED</i>	Triggered whenever there is a change of an operation point parameter.	External reference identifier of currently selected Service Operation Point.
<i>PLAYBACK_ENDED</i>	Sent when playback completes.	
<i>PLAYBACK_ERROR</i>	Sent when an error occurs. The element's error attribute contains more information.	Error attribute.
<i>PLAYBACK_PAUSED</i>	Sent when playback is paused.	
<i>PLAYBACK_PLAYING</i>	Sent when the media begins to play (either for the first time, after having been paused, or after ending and then restarting).	
<i>PLAYBACK_SEEKED</i>	Sent when a seek operation completes.	
<i>PLAYBACK_SEEKING</i>	Sent when a seek operation begins.	
<i>PLAYBACK_STALLED</i>	Sent when the media playback platform reports stalled	
<i>PLAYBACK_STARTED</i>	Sent when playback of the media starts after having been paused; that is, when playback is resumed after a prior pause event.	
<i>PLAYBACK_WAITING</i>	Sent when the media playback has stopped because of a temporary lack of data.	
<i>SERVICE_DESCRIPTION_SELECTED</i>	sent when the DASH client has selected a service description.	
<i>SERVICE_DESCRIPTION_CHANGED</i>	Sent when the DASH client has changed a service description.	
<i>SERVICE_DESCRIPTION_VIOLATED</i>	Provides notification that the service description parameters are currently not met.	Parameters of service description that are not met.
<i>SOURCE_INITIALIZED</i>	Triggered when the source is setup and ready.	

Table 13.2.5-2 provides a list of error events.

Table 13.2.5-2: Error events

Status	Definition	Payload
<i>ERROR_MPD_NOT_FOUND</i>	Triggered when the MPD is not found.	
<i>ERROR_MEDIA_PLAYBACK</i>	Triggered when there is an error from the media playback platform buffer.	
<i>ERROR_MPD_NOT_VALID</i>	The provided MPD is not valid according to the XML schema and schematron rules.	Detailed error information.
<i>ERROR_MEDIA_TIME_NOT_ACCESSIBLE</i>	After seek operation, the media time is not accessible.	
<i>ERROR_PROFILE_NOT_SUPPORTED</i>	The profile of the Media Presentation is not supported.	

13.2.6 Status Information

Table 13.2.6-1 provides a list of dynamically changing status information that can be obtained from the client.

Table 13.2.6-1: Dynamic Status information

Status	Type	Parameter	Definition
<i>state</i>	Enumeration		An enumerated value from table 13.2.2-1 indicating the current state of the Media Player.
<i>averageThroughput</i>	float	none	Current average throughput computed in the ABR logic in bit/s.
<i>bufferLength</i>	float	MediaType "video", "audio" and "subtitle"	Current length of the buffer for a given media type, in seconds. If no type is passed in, then the minimum of video, audio and subtitle buffer length is returned. NaN is returned if an invalid type is requested, the presentation does not contain that type, or if no arguments are passed and the presentation does not include any adaption sets of valid media type.
<i>liveLatency</i>	float	none	Current live stream latency in seconds based on the latency measurement.
<i>mediaSetting[]</i>	MPDAdaptationSet	MediaType "video", "audio" and "subtitle"	Current media settings for each media type based on the CMAF Header and the MPD information based on the selected Adaptation Set for this media type.
<i>mediaTime</i>	float	None	Current media playback time from media playback platform. The media time is in seconds and is relative to the start of the playback and provides the media that is actually rendered.
<i>playbackRate</i>	float	None	The current rate of playback. For a video that is playing twice as fast as the default playback, the <i>playbackRate</i> value should be 2.00.
<i>availableServiceDescriptions[]</i>	Provides the available service descriptions		Provides the list of available selectable service descriptions with an id to select from. Those are either configured ones or the ones in the MPD.
<i>availableMediaOptions[]</i>	List of Adaptation Set or Preselection ids	MediaType "video", "audio" "subtitle" "all"	Provides the list of available media options that can be selected by the application based on the capability discovery and the subset information.
<i>serviceOperationPoints</i>	Array(Service OperationPoint)		The set of Service Operation Points declared in the presentation manifest (e.g. DASH MPD) of the current media presentation.
<i>operativeServiceOperation Point</i>	integer		A zero-based index into the <i>service OperationPoints</i> array indicating the Service Operation Point currently operative in the playback session. Set to -1 if the array is empty.
<i>metrics[][]</i>	Metrics		A data blob of metrics for each configured metrics collecting scheme.

Table 13.2.6-2 provides a list of configured operation point information that can be obtained from the client. Any change to a parameter below shall be announced with a notification *OPERATION_POINT_CHANGED*.

Table 13.2.6-2: Service Operation Point Information

Parameter	Type	Definition
<i>ServiceOperationPoint</i>	Object	The currently configured operation point parameters according to which the DASH client is operating.
<i>externalIdentifier</i>	String	The external identifier uniquely identifying this Operation Point in the presentation manifest (e.g. DASH MPD).
<i>mode</i>	Enum	The following operation modes are defined: <i>live</i> : The DASH client operates to maintain configured target latencies using playback rate adjustments and possibly resync. <i>Vod</i> : The DASH client operates without latency requirements and rebuffering may result in additional latencies
<i>maxBufferTime</i>	Integer	maximum buffer time in milliseconds for the service.
<i>switchBufferTime</i>	Integer	buffer time threshold below which the DASH clients attempts to switch Representations.
<i>latency</i>	Object	Defines the latency parameters used by the DASH client when operating in live mode.
<i>target</i>	Integer	The target latency for the service in milliseconds.
<i>max</i>	Integer	The maximum latency for the service in milliseconds.
<i>min</i>	Integer	The maximum latency for the service in milliseconds.
<i>playbackRate</i>	Media Type <i>audio, video, all</i>	Defines the playback rate parameters used by the DASH client for catchup mode and deceleration to avoid buffer underruns and maintaining target latencies.
<i>max</i>	Real	The maximum playback rate for the purposes of automatically adjusting playback latency and buffer occupancy during normal playback, where 1.0 is normal playback speed.
<i>min</i>	Real	The minimum playback rate for the purposes of automatically adjusting playback latency and buffer occupancy during normal playback, where 1.0 is normal playback speed.
<i>bitRate</i>		Defines the operating bandwidth parameters used by the DASH client used for a specific media type or aggregated. The values are on IP level.
<i>target</i>	Integer	The target bandwidth for the service in bit/s that the client is configured to consume.
<i>max</i>	Integer	The maximum bandwidth for the service in bit/s that the client is configured to consume.
<i>min</i>	Integer	The minimum bandwidth for the service in bit/s that the client is configured to consume.
<i>playerSpecificParameters</i>		Player-specific parameters may be provided, for example about the used algorithm, etc.

13.2.7 Usage of M7d Information by Media Session Handler

The media session handler may use the notifications, errors and status information provided through M7d to execute relevant tasks.

14 Application (M8) APIs for uplink and downlink

APIs of this reference point are not specified within this release.

15 Miscellaneous UE-internal APIs

15.1 General

While the core functionality of 5GMS is specified in terms of the dedicated system interfaces and APIs that impact the UE, specified in clauses 10 to 14 (M4 to M8 respectively), certain features of 5GMS rely on interfaces and APIs that are essentially UE-internal.

Each usage of a UE-internal interface is specified in subsequent sub-clauses of the present clause.

15.2 RAN Signaling-based Network Assistance API

If RAN Signaling-based Network Assistance is supported, the Media Session Handler uses an interface to the RAN Modem (specifically, the UE MAC entity in the modem) to send and receive bit rate recommendation messages. The interface to the modem may be based on the AT commands `+CGBRRREQ` and `+CGBRRREP` as defined in [15].

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 [13] for 5G NR and [14] 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 get a list of CID values that are associated with QoS flows (both network and MT/TE initiated). When used for requesting 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 dropping.

The *Bit Rate Recommendation Query* shall indicate the bit rate desired by the application, as described by [13] and [14]. This request may be used by the 5GMSd 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 RAN Modem, corresponding to the logical translation of the *Bit Rate Recommendation* message for the associated RAN uplink or downlink, it shall indicate the associated bit rate recommendation to either the Media Player (via M7d, in the case of downlink streaming) or Media Streamer (via M7u, in the case of uplink streaming) function of an affiliated PDU session. Furthermore, whenever the Media Session Handler receives a request for a bit rate boost from either the Media Player (via M6d in the case of downlink streaming) or the Media Streamer (via M6u, in the case of uplink streaming) function of an affiliated PDU session, it may send a bit rate boost message to the RAN 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 player to decide how to best use the bit rate recommendation and the bit rate recommendation query information for the media streaming sessions.

15.3 RAN-based Metrics Reporting API

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 [4], the metrics configuration is delivered to the UE modem 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 [42]. When a metrics configuration is received, the Media Session Handler shall store this configuration and use it for all subsequent media streaming sessions.

When a streaming 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 [4].

If metrics are to be reported for the session, the Media Session Handler shall request the Media Player to create a metrics collection job. The Media Player 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 that shall be collected during the session. The format of the configuration shall be according to TS 26.247 [4] clause L.2, but note that 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 Player according to the *reportingInterval* specified in the metrics configuration. The metrics returned by the Media Player shall use the format specified in clause 10.6.2 of TS 26.247, and (for Virtual Reality media) in clause 9.4.3 of TS 26.118 [42], and 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 TS 26.247 [4].

When the session is finished the Media Session Handler shall delete the metrics collection job.

16 Usage of 5GC interfaces and APIs

16.1 General

While the core functionality of 5GMS is specified in terms of the dedicated system interfaces and APIs specified in clauses 7 to 14 (for M1 to M8 respectively), certain features of 5GMS rely on interfaces and APIs defined within the scope of the 5GC.

Each such case of usage of a 5GC interface and API is documented in subsequent sub-clauses of the present clause.

NOTE: The 5GMS architecture may be applied to an EPS although such an application is not specified in the present document and is left to the discretion of deployments and implementations.

16.2 Usage of N5/N33 for AF-based Network Assistance

The AF-based Network Assistance feature operates at reference point M5 between the Media Session Handler in the 5GMS Client and a 5GMS AF that provides Network Assistance capabilities. The Network Assistance API at reference point M5 (see clause 11.6) 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 5GMS 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 5GMS 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 5GMS AF shall interact with the PCF using one of the following methods:

A. If the 5GMS 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 [34].

NOTE 2: It is the responsibility of the 5GMS 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 5GMS AF is deployed outside the Trusted DN, or if it is more convenient for a 5GMS 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 [50], to indirectly invoke the PCF at reference point N33.

NOTE 3: Per clause 4.4.9 of TS 29.522 [50], 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 5GMS 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 5GMS 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 5GMS AF shall use the configured Policy Templates of the Provisioning Session to determine the list of the QoS references within the "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 4.7.6 and 11.6.4.6), the 5GMS AF shall destroy the corresponding AF application session context in the relevant PCF instance.

16.3 Usage of N5/N33 for dynamic policies

The dynamic policies feature operates at reference point M5 between the Media Session Handler in the 5GMS Client and a 5GMS AF that has been appropriately provisioned with Policy Templates. The Dynamic Policies API at reference point M5 (see clause 11.5) 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 5GMS 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 5GMS AF shall interact with the PCF using one of the following methods:

- A. If the 5GMS 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 [34].

NOTE 2: It is the responsibility of the 5GMS 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 5GMS AF is deployed outside the Trusted DN, or if it is more convenient for a 5GMS 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 [50], to indirectly invoke the PCF at reference point N33.

NOTE 3: Per clause 4.4.9 of TS 29.522 [50], 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 [50].

NOTE 4: Configuration of the NEF endpoint address and access credentials in the 5GMS 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 5GMS 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 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 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 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 5GMS AF shall use the configured Policy Template of the dynamic policy to determine the list of the QoS references within the "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 5GMS AF shall destroy the corresponding AF application session context in the relevant PCF instance.

17 Media Streaming data reporting at R4

17.1 General

The following record types shall be used with the *Ndcnf_DataReporting_Report* service operation specified in clause 7.2.3.4.1 of TS 26.532 [47]. In each case, one or more records are included in a *DataReport*, as specified in clause 7.3.3.2.1 of [47].

The OpenAPI definitions of the record types are found in clause C.5.1 of the present document.

17.2 MediaStreamingAccessRecord type

As specified in clause 4.11.3, the *MediaStreamingAccessRecord* type shall be used by the 5GMS AS to report media streaming access.

Table 17.2-1: Definition of MediaStreamingAccessRecord type

Property name	Data Type	Cardinality	Description
<i>timestamp</i>	DateTime	1..1	The date and time of the media access. (See table 6.4.2-1.)
<i>mediaStreamHandlerEndpointAddress</i>	Endpoint Address	1..1	The endpoint address of the Media Stream Handler accessing the 5GMS AS. (See clause 6.4.3.8.)
<i>applicationServerEndpointAddress</i>	Endpoint Address	1..1	The service endpoint on the 5GMS AS to which the Media Stream Handler is connected. (See clause 6.4.3.8.)
<i>sessionIdentifier</i>	string	0..1	An identifier for the HTTP session on which the Media Stream Handler request was made. This should not contain any user-identifiable data. It may, for example, be a one-way hash of the transport connection identifier, if available from the underlying transport protocol. Alternatively, it could be a one-way hash of the 5-tuple formed from the Media Stream Handler and 5GMSd AS endpoint addresses and a transport protocol identifier.
<i>requestMessage</i>	Object	1..1	Details of the HTTP request message submitted to the 5GMS AS by the Media Stream Handler for this media access.
<i>method</i>	string	1..1	The request method.
<i>url</i>	AbsoluteUrl	1..1	The request URL. (See table 6.4.2-1.)
<i>protocolVersion</i>	string	1..1	The HTTP protocol version, e.g. "HTTP/1.1".
<i>range</i>	string	0..1	The value of the <i>Range</i> request header, if present.
<i>size</i>	UInteger	1..1	The total number of bytes in the request message.
<i>bodySize</i>	UInteger	1..1	The number of bytes supplied by the Media Stream Handler in the HTTP request message body. Zero if there is no request body.
<i>contentType</i>	string	0..1	The MIME content type of the request message, if any.
<i>userAgent</i>	string	0..1	A string describing the requesting Media Stream Handler, if it supplies a <i>User-Agent</i> request header.
<i>userIdentity</i>	String	0..1	A string identifying the user that made the access, if supplied.
<i>referrer</i>	AbsoluteUrl	0..1	The URL that the Media Player reports being referred from, if the <i>Referer</i> request header is supplied. (See table 6.4.2-1.)
<i>cacheStatus</i>	CacheStatus	0..1	An indication of whether the 5GMS AS is able to serve an object corresponding to <i>requestMessage,url</i> from cache (<i>HIT</i>) or whether there is a stale object cached (<i>EXPIRED</i>) or the requested object is not present in cache (<i>MISS</i>). (See table 6.4.4.4.) For non-caching implementations of the 5GMS AS, the property shall be omitted.
<i>responseMessage</i>	Object	1..1	Details of the HTTP response message returned by the 5GMS AS to the Media Stream Handler for this media access.
<i>responseCode</i>	UInteger	1..1	The HTTP response code.
<i>size</i>	UInteger	1..1	The total number of bytes in the response message.
<i>bodySize</i>	UInteger	1..1	The number of bytes in the HTTP response message body.
<i>contentType</i>	string	0..1	The MIME content type of response message, if any.
<i>processingLatency</i>	Float	1..1	The time, expressed in milliseconds, taken by the 5GMS AS to respond to the Media Stream Handler request, measured from the first byte of the HTTP request being processed by the 5GMS AS to the last byte of the response being sent.

Property name	Data Type	Cardinality	Description
<i>connectionMetrics</i>	Object	0..1	Metrics about the performance of the transport connection underlying the HTTP session serving this media access.
<i>meanNetworkRoundTripTime</i>	Float	1..1	A rolling mean average, expressed in milliseconds, of the network round-trip time for the HTTP session.
<i>networkRoundTripTimeVariation</i>	Float	1..1	The variation in <i>meanNetworkRoundTripTime</i> , expressed in milliseconds, during the averaging period.
<i>congestionWindowSize</i>	UInteger	1..1	The current size (in bytes) of the congestion window for the transport connection underlying the HTTP session.

18 Event exposure at R5 and R6

The *Naf_EventExposure* service specified in TS 29.517 [46] shall be used by event consumer to subscribe to the following types of 5G Media Streaming event notifications, identified by their respective Event IDs, from the Data Collection AF instantiated in the 5GMS AF, and subsequently to receive such notifications:

1. Media Streaming QoE Event, as specified in clause 5.6.2.23 of [46], comprising
 - a) 3GPP-defined QoE metrics information, and
 - b) non-3GPP-defined QoE metrics information.
2. Media Streaming Consumption Event, as specified in clause 5.6.2.24 of [46].
3. Media Streaming Network Assistance Invocation Event, as specified in clause 5.6.2.25 of [46].
4. Media Streaming Dynamic Policy Invocation Event, as specified in clause 5.6.2.26 of [46].
5. Media Streaming Access Event, as specified in clause 5.6.2.27 of [46].

In this release, eligible event consumer subscribers to the *Naf_EventExposure* service as specified in [46] are the following:

- The NWDAF defined in TS 23.288 [47].
- The Event Consumer AF defined in TS 26.531 [46] when it is deployed in the Trusted DN.
- The NEF defined in TS 23.501 [2] when it is used to expose the *Naf_EventExposure* service to functions outside the Trusted DN via the *Nnef_EventExposure* service defined in TS 23.502 [45].

Implementations of the Data Collection AF instantiated the 5GMS AF shall support negotiation of the optional features relating to 5G Media Streaming specified in table 5.8-1 of TS 29.517 [46]. Feature negotiation by event consumers is achieved as specified in clause 5.8 of [46].

Annex A (informative): 5GMS Parameter propagation for DASH Streaming

A.1 End-to-end model

Figure A.1-1 below depicts an end-to-end model for the 5GMS parameter propagation for DASH streaming with dynamic policy. The arrows indicate the main information flow. The interfaces specified in TS 26.501 [2] are used throughout. However, there are additional interfaces (i.e. P1 or U1), which are not in the 5GMS Architecture.

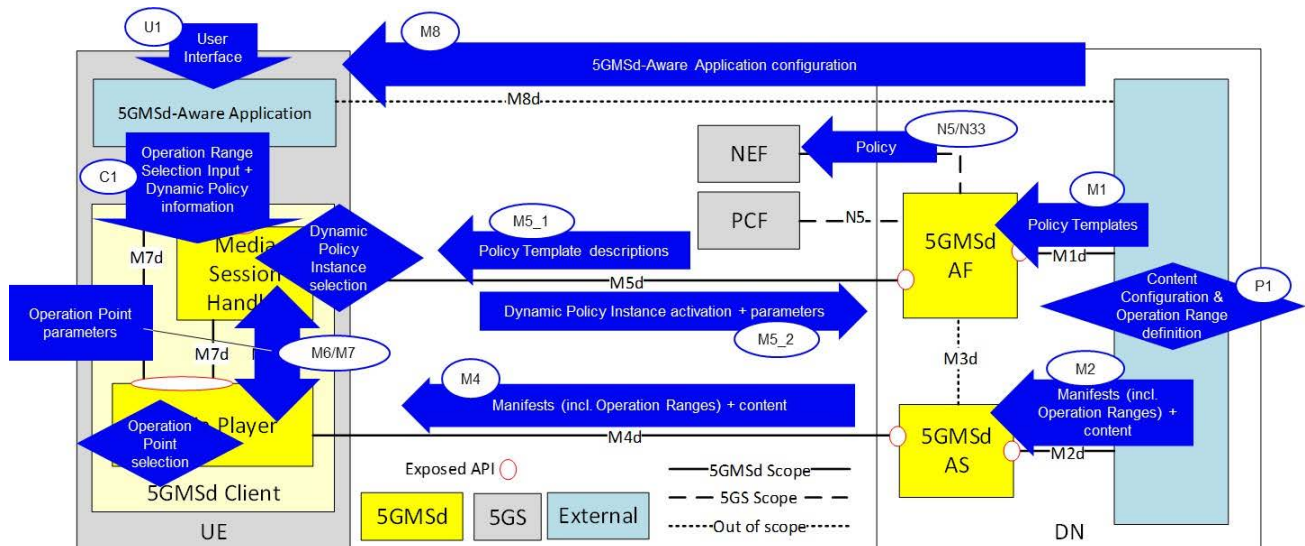


Figure A.1-1: End-to-end model for dynamic policy parameter propagation

The interfaces involved and their roles in this feature are as follows:

- M1: Provisioning interface between the 5GMS Application Provider and the 5GMS AF.
- P1: The 5GMS Application Provider provisions the DASH MPD generator, e.g. by annotating the MPD with Service Descriptions.
- U1: User Interface to the 5GMS-Aware Application.

NOTE: The 5GMS Application Provider controls the application, i.e. controls the GUI choices.

- M8: Non-standardized input from the 5GMS Application Provider to the 5GMS-Aware Application, such as country-specific application behaviours (languages, on-demand catalogue, etc).
- Input on subscriptions (e.g. 4K subscription versus SD subscription).
- Device-specific content selection rules (e.g. SmartPhone versus Smart TV).
- Additional service offering features (e.g. background download possible).
- C1 (one of M6 or M7): Information from the 5GMS-Aware Application to the 5GMS Client, e.g. user content selections.
- M6: Information flow from the DASH Player to the Media Session Handler.
- M7: Information flow from the Media Session Handler to the DASH Player.
- M5_1: Information flow into the Media Session Handler for parameter provisioning (Policy Descriptions, which originate from 5GMS AF and 5GMS Application Provider). The Policy Descriptions contain or reference the detailed Service Access Information, i.e. URLs to activate a certain policy.

- M5_2: Information flow from the Media Session Handler to the 5GMS AF. This includes:
 - input to create the Service Data Flow Templates (see TS 23.503 [33]) for identifying the application data flows within a PDU Session,
 - an identifier for the Dynamic Policy instance (e.g. QoS, Conditional Zero-rating, charging, etc) and
 - optionally, Network Assistance information, e.g. bit rate recommendations.

In its Annex K, the DASH standard [32] specifies so-called "Service Descriptions". The purpose of Service Descriptions is to provide additional information to a DASH player to influence its "Selection Logic", e.g. a DASH player should prefer a certain set of representations within an adaptation set. It is assumed in the following that the DASH MPD can be annotated using Service Descriptions to give hints for subscription models and different device types.

The 5G System specifies a number of different means to detect application flows. When activating a Dynamic Policy, the Media Session Handler provides a Service Data Flow Template to the 5GMS System, which identifies the application flow(s) of interest. It is assumed here that multiple applications are executing simultaneously on a given UE and that each application may independently access the network. Therefore, the Media Session Handler needs to provide (and update) these Service Data Flow Templates in order that the application traffic can be treated according to the corresponding Dynamic Policy.

In the following clauses, the parameter propagation for a number of different use cases is described.

A.2 Premium QoS dynamic policy

A.2.1 General

To realise a Premium QoS service offering, the 5GMS Client should activate a QoS Flow with characteristics matching the service needs. It is assumed that the DASH content is prepared for different subscription levels, e.g. 4K, HDR or SD, and for different target device types, e.g. SmartPhone or SmartTV. When commencing playback of a DASH presentation according to a particular subscription level (e.g. 4K), the 5GMS Client needs to activate a QoS Flow with a matching bit rate setting.

NOTE: The 5GMS Client may choose to activate a QoS Flow with a lower bit rate than the maximum supported by the 5G System, e.g. a small screen SmartPhone may select different QoS settings from a large screen device.

The per-title quality and the subscription levels of an example on-demand catalogue are illustrated in the figure below. The subscription levels in this example are 4K, FullHD, HD, SD and 480p. Only devices entitled to activate a 4K quality should actually select the according representations from the MPDs. In this example, all titles are available in SD and HD quality. Often, not all titles are available in 4K quality. Thus, a device with a 4K subscription can only activate reception of the HD or SD representations.

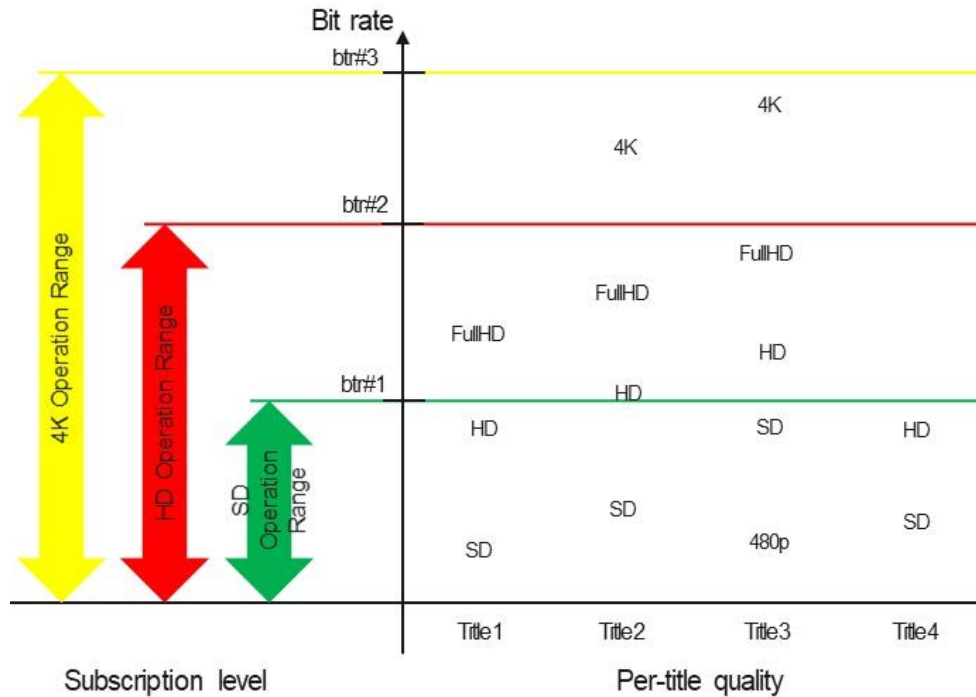


Figure A.2.1-1: Subscription Levels for Premium QoS

The bit rate required to sustain a certain quality varies from title to title. In the figure, the bit rate needed for *Title4* in HD is in the same range as SD quality of *Title3*.

The various consumer-facing Network Subscription Levels define a set of bounded Operation Ranges, as illustrated on the right side of the figure. Each such Operation Range is conveniently modelled in the 5GMS architecture as a Policy Template. The Policy Template for SD subscription level (*SD Operation Range*) is authorized to activate a maximal bit rate of *btr#1*. The Policy Template for 4K subscription level is authorized to activate between any low bit rate and a maximal bit rate of *btr#3*.

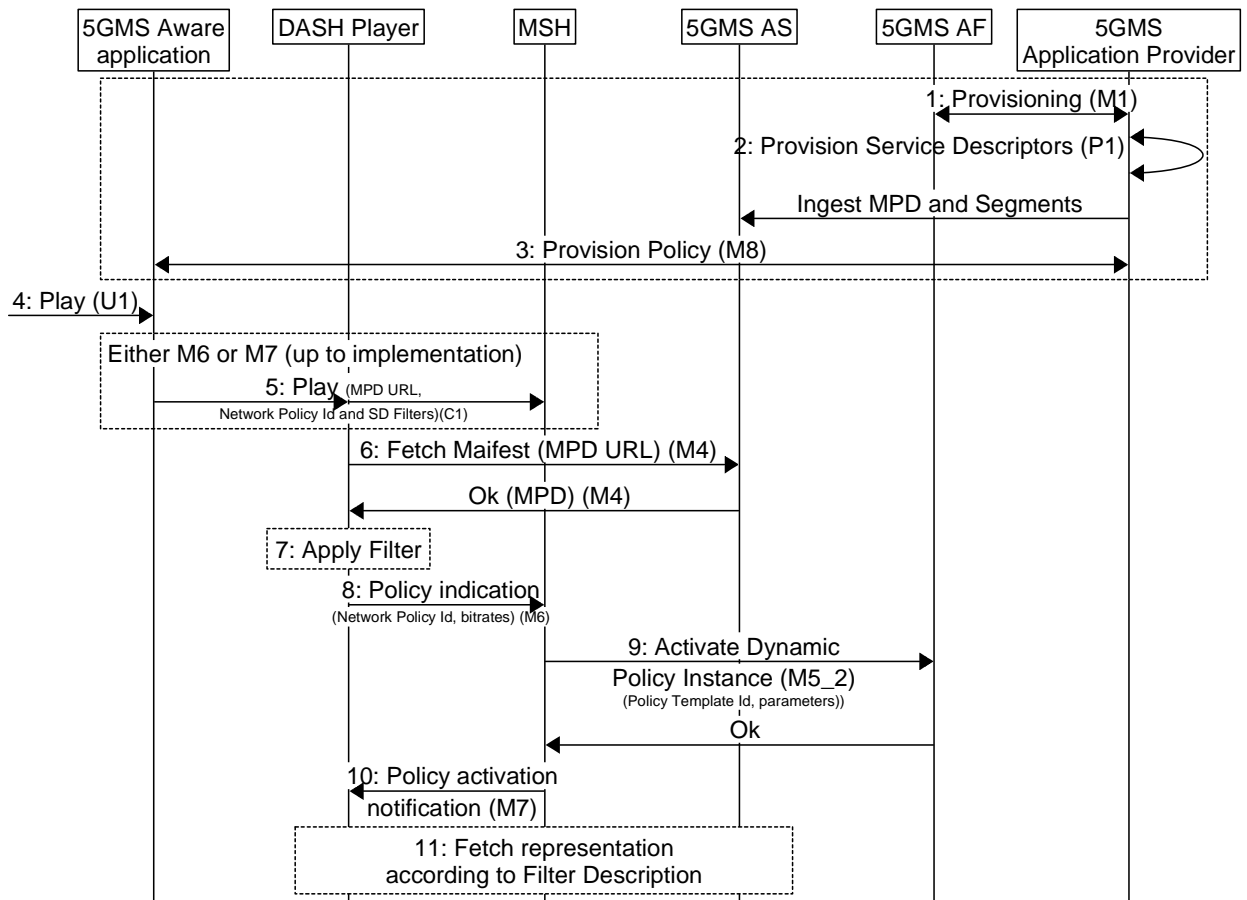
When activating a Dynamic Policy instance, the 5GMSd Client provides a desired bit rate for the selected title. The desired bit rate can be smaller than the maximal bit rate allowed by the Policy Template. The 5GMSd Client always activates a Dynamic Policy instance from its assigned Network Subscription Level, even when the desired bit rate justifies a different Policy Template.

When activating a QoS Flow for a certain subscription level and title, the 5GMSd Client should preferably select a desired bit rate matching the quality needed. For example, a device with an *HD Operation Range* subscription needs a higher desired bit rate when consuming *Title3* in HD quality and a lower desired bit rate when consuming *Title4* in HD quality.

In some cases, the system rejects a requested QoS Flow or drops an established QoS Flow due to insufficient available network resource. The 5GMSd Client can then try to activate a different QoS Flow with a lower desired bit rate.

A.2.2 Procedure

The procedure for activating a Premium Qos dynamic policy is illustrated in figure A.2.2-1 below.



<http://msc-generator.sourceforge.net v6.3.7>

Figure A.2.2-1: Procedure for activating Premium QoS dynamic policy

Steps:

1. The 5GMS Application Provider interacts with the 5GMS AF to set up one or more Policy Templates (using M1). Each Policy Template is identified by a Policy Template identifier and contains information about how to activate the corresponding policy within the 5G System (e.g. N5 URLs and parameters).
2. The 5GMS Application Provider interacts with its DASH content generation function (e.g. an MPD provider) to annotate the DASH MPD with Service Descriptions (using P1). The Service Descriptions define the Operational Ranges within the Media Player should operate. The DASH MPD and the DASH Media Segments are then ingested by the 5GMS AS.
3. The 5GMS-Aware Application is configured via M8 (step 3) with information about the available content catalogue (e.g. resolving MPD URLs), the available subscription identifiers (e.g. the user has a 4K subscription or the user has an SD subscription), device type identifiers and network policy identifiers.

The subscription identifiers and the device type identifiers are collectively referred to as Service Description Filters in the following.

NOTE 1: It is for further study whether network policy identifiers are embedded in the MPD Service Descriptions or derived from the Service Descriptions.

NOTE 2: The network policy identifier can be equal to a Policy Template identifier when the 5GMS-Aware Application is aware about its usage (e.g. for QoS streaming or background download). It is assumed here, that a unique Network Policy identifier is assigned to each subscription level.

4. When the user selects an item via the User Interface (U1), the 5GMS-Aware Application translates the input to the needed 5GMSd API calls.
5. The 5GMS-Aware Application provides input (via C1) on the selected presentation entry (i.e. MPD URL) together with a Network Policy Identifier (the value indicates here a "HD Premium QoS" policy (alternative Network Policy Identifiers can refer to e.g. 4K quality), i.e. make the Media Session Handler request a QoS Flow) and Service Description Filters. The Service Description Filter is used by the Media Player to identify the usable Service Descriptions from the MPD. The Network Policy Identifier is used by the Media Session Handler to find the according Policy Description containing information on the Dynamic Policy instantiation method (i.e. procedure and parameters such as Policy Template identifier).
6. The DASH player fetches the MPD.
7. The Media Player selects the Service Description and applies the Service Description Filter.
8. The DASH player indicates to the Media Session Handler (M6) that a "HD Premium QoS" network service should be activated (value of the Network Policy Identifier). The DASH player provides input on bit rate ranges (which may depend on the device type and the title quality). The Media Session Handler has received one or more Policy Descriptions together with matching Service Access Information (via M5_1). When the Media Session Handler has received the policy indication, the Media Session Handler uses the Network Policy Identifier to find the procedure and the parameters to activate the Dynamic Policy instance (i.e. find the matching Policy Description). The Media Session Handler activates a Dynamic Policy instance in the 5GMS AF, providing Service Data Flow Templates identifying the DASH media flows (audio, video, etc) and to provide the desired bit rate of the video.
9. The Media Session Handler activates a Dynamic Policy instance with the 5GMS AF. The 5GMS AF uses the Policy Template identifier to look up the matching Policy Template in order to create the PCF or NEF API invocation. As result, the Media Session Handler receives the enforcement bit rate in the 5GMS AF response. The 5GMS Client should not exceed this bit rate threshold.

The Service Access Information (via M5_1) includes a list of recommended traffic detection methods. The Media Session Handler selects a Service Data Flow description method (e.g. 5-Tuples). When the Media Session Handler selects:

- 5-Tuples: For each new TCP connection, the Media Session Handler updates the Dynamic Policy instances and adds a new 5-Tuple. For each closed TCP connection, the Media Session Handler updates the Dynamic Policy instances and removes the 5-Tuple of the closed TCP connection.
- TOS or Traffic Class: The Media Session Handler sets the TOS or Traffic Class for each new TCP connection.
- Domain name: The Media Session Handler provides the domain name with the Dynamic Policy Instance.

A.2.3 Example parameters

Table A.2.3-1: M5_1 parameters for Policy Descriptions (used by the Media Session Handler)

Parameter	Type	Purpose	Example Values
Policy Description	Object		
Network Policy Identifier	String	Identifies the Policy Description.	"4K Premium QoS", "HD Premium QoS".
Service Access Information URL	URL	References the associated Service Access Information.	

Table A.2.3-2: M5_1 parameters for Service Access Information

Parameter	Type	Purpose	
Service Access Information	Object		
Policy Template identifier	String	Identifies the Policy Template.	"HD QoS".
5GMS AF URL	URL	Used to invoke the 5GMS AF.	
Mandatory Request M5 information	List	Desired bit rate, which should be provided by the network for the application.	Policy Template identifier, Desired Bit Rate, Packet Detection Filters.
M5 Response information	List	Information to the Media Session Handler on the response parameters.	OK (requested bit rate is accepted), Proposed Lower Bit rate (requested bit rate cannot be provided).
sdfMethod	[String]	Indicates which Service Data Flow Description methods are recommended to be used by the Media Session Handler.	"5-Tuple", "domainName", "TOS=xx", etc.

A.3 (Conditional) Zero Rating dynamic policy

A.3.1 General

In the case of (Conditional) Zero Rating, the quality of a video streaming service should not exceed a certain bit rate threshold (called the policy threshold). This can be realized by deploying a traffic shaper in the network (e.g. a policing function in the UPF) or by instructing the DASH Player not to exceed a certain policy threshold bit rate. The policy threshold may be network-specific, i.e. depending on the 5G System. The following realization assumes the latter, i.e. the DASH Player is not exceeding the bit rate policy and the UPF is just monitoring the compliance of the application flows (one or more TCP and/or UDP flows). The MPD is annotated using DASH Service Descriptions in such a way that the DASH Player can identify which maximal representation bit rates still comply with the policy threshold.

Figure A.3.1-1 below illustrates the per-title quality and the policy threshold. For *Title1* and *Title2*, the 5GMSd Client can activate the SD and HD representations. For *Title3*, the 5GMSd Client can activate the 480p and the SD representations. For *Title4*, the 5GMSd Client can activate all available representations (i.e. SD and HD).

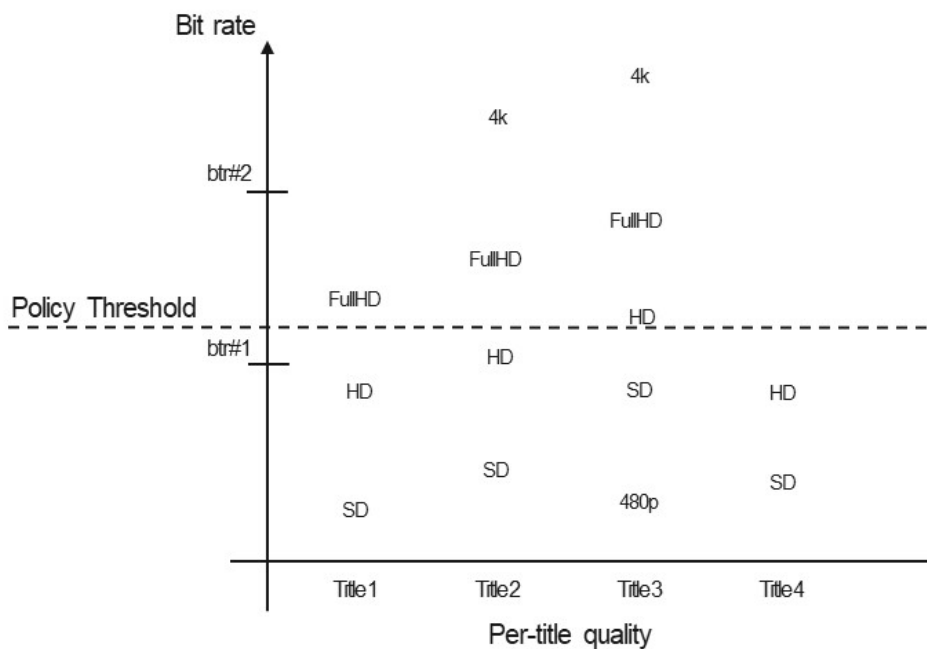
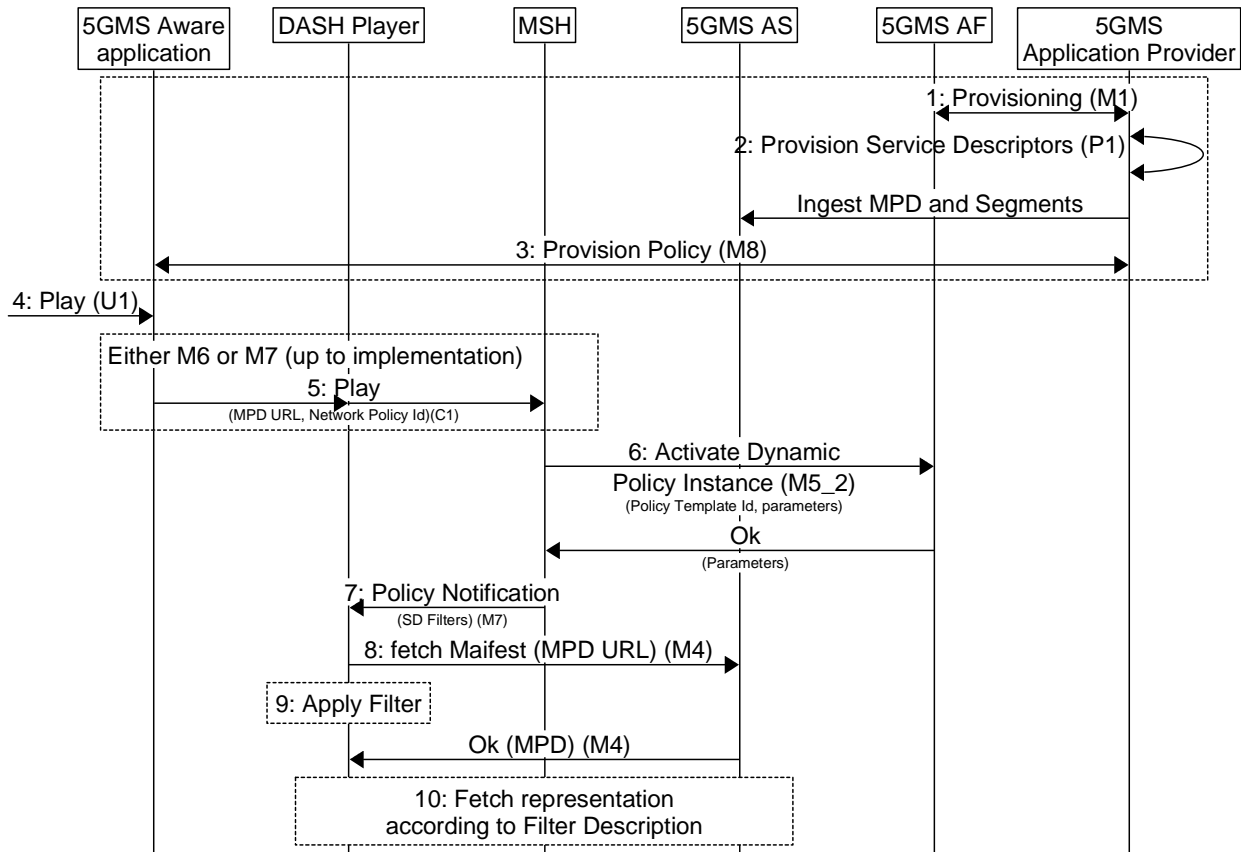


Figure A.3.1-1: Policy threshold versus quality

When the 5GMSd Client receives the bit rate of the policy threshold from the network, the 5GMSd Client filters the MPD for policy-compliant representations (i.e. those that lie at or below the policy threshold).

A.3.2 Procedure

The procedure for activating a (Conditional) Zero Rating dynamic policy is illustrated in figure A.3.2-1 below.



<http://msc-generator.sourceforge.net v6.3.7>

Figure A.3.2-1: Procedure for activating (Conditional) Zero Rating dynamic policy

Steps:

1. The 5GMS Application Provider interacts with the 5GMS AF to set up one or more Policy Templates. Each Policy Template is identified by a Policy Template identifier and contains information about how to activate the corresponding policy within the 5G System (e.g. N5 URLs and parameters).
2. The 5GMS Application Provider interacts with its DASH content generation function (e.g. an MPD provider) to annotate the DASH MPD with Service Descriptions (step 2). The intention of the Service Descriptions here is that the DASH Player can identify those representation combinations which do not exceed the bit rate requirement.
3. The 5GMSAware Application is configured via M8 with information about the available content catalogue (e.g. resolving MPD URLs), the available subscription identifiers (e.g. the user has a 4K content subscription or the user has an SD subscription), device type identifiers.

The 5GMSd-Aware Application is configured via M8 about the available (Conditional) Zero Rating policy. This includes the Network Policy Ids.

4. When a user selects an item via the User Interface (UI), the 5GMS-Aware Application translates the input to the needed 5GMSd API calls.

5. The 5GMS Aware Application provides input (via C1) on the selected presentation entry (i.e. MPD URL) and also on the Network Policy Id (the value in this case indicates a (Conditional) Zero-Rating policy, i.e. make the Media Session Handler request the policy threshold parameter from the network).

NOTE: C1 is an abstract interface and indicates that the 5GMS-Aware Application may either first use M6 or M7 for the interactions with the 5GMS Client.

6. The Media Session Handler uses the Network Policy Identifier to find the procedure and the parameters to activate the Dynamic Policy Instance (here a (Conditional) Zero Rating policy). The Media Session Handler has received one or more Policy Descriptions together with matching Service Access Information (via M5_1). The Media Session Handler uses the Network Policy Identifier as a key to find the correct Policy Description. Here, the Network Policy Identifier indicates a (Conditional) Zero Rating policy. The Media Session Handler should activate a dynamic policy in the 5GMS AF, providing Service Data Flow Template information about the DASH media flows (audio, video, etc.) and retrieving the bit rate threshold, which cannot be exceeded to comply with the policy. The Media Session Handler receives (as result of the Dynamic Policy activation) some information on the policy enforcement (*enforcementMethod* and/or *enforcementBitrate*), so that the representation selection logic (bit rate adaptation function) in the DASH Player can consider the effects of the enforcement scheme.
7. The Media Session Handler activates the Dynamic Policy instance on M5, providing a Policy Template identifier. Upon positive response, the Media Session Handler notifies the DASH Player, providing Service Descriptor Filters. The Media Session Handler may receive these Service Descriptor Filters with the response, or it may look up the Service Descriptor Filter values by a response value. Alternatively, the Media Session Handler receives a maximum bit rate with the response and the Media Session Handler derives the Service Descriptor Filter. The Media Session Handler may also receive information about Policy Enforcement, e.g. what type of traffic shaper will throttle the bit rate.

The Media Session Handler may need to update the Dynamic Policy instance, depending on the selected traffic detection method. For example, when the Media Session Handler uses 5-Tuples, the Media Session Handler needs to update the Dynamic Policy instance with every newly opened and every closed TCP connection.

8. The DASH Player fetches the MPD of the selected content.
9. The Service Descriptor Filter is used by the DASH Player to filter policy-compliant Service Descriptions from the MPD. The DASH Access Engine or Selection Logic (see ISO/IEC 23009-1 [32] figure K.1) selects only adaptation sets and representations according to the filter. Here, the DASH Player fetches the MPD after the notification from the Media Session Handler.

A.3.3 Example parameters

Table A.3.3-1: M5_1 parameters for Policy Descriptions (used by the Media Session Handler)

Parameter	Type	Purpose	Example Values
Policy Description	Object		
Network Policy Id	String	Identifies the Policy Description.	"(Conditional) Zero Rating".
Service Access Information URL	URL	References the associated Service Access Information.	

Table A.3.3.-2: M5_1 parameters for Service Access Information

Parameter	Type	Purpose	
Service Access Information	Object		
Policy Template Id	String	Identifies the Policy Template.	"not exceed bit rate"
5GMS AF URL	URL	Used to invoke the 5GMS AF.	
sdfMethods	[String]	Indicates which Service Data Flow Description methods are recommended for use by the Media Session Handler.	"5-Tuple", "domainName", "TOS=xx", etc.
Mandatory M5 Request information	List		Policy Template identifier, Service Data Flow Template.
M5 Response information	List	Information to the Media Session Handler on the response parameters.	Bit rate Policy Threshold (upper bit rate bound, which should not be exceeded).

A.4 Background Download

A.4.1 General

In the case of Background Download, the asset is acquired in the background, prior to viewing. Many application services offer the capability of acquiring a VoD item for later consumption. The 5GMS-Aware Application triggers the Media Session Handler to acquire the item, providing a background download network policy id.

NOTE: Here, the DASH Player is handling the acquisition, since the DASH Player contains the MPD processing and the DASH Access engine parts. Other realizations would use a separate background download agent, which is not even try to decode and render the video.

Figure A.4.1-1 below illustrates the representation marking for background download. The MPD may be annotated with Service Descriptions clearly identifying representations intended for download. Here, *Title1* should be downloaded in Full HD quality and all other titles in regular HD quality.

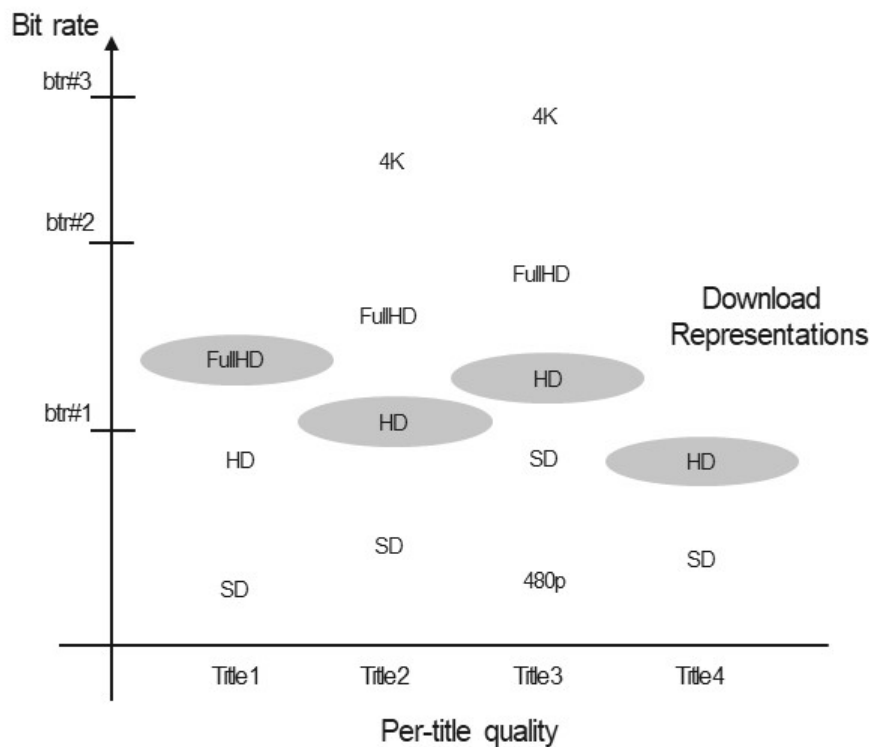
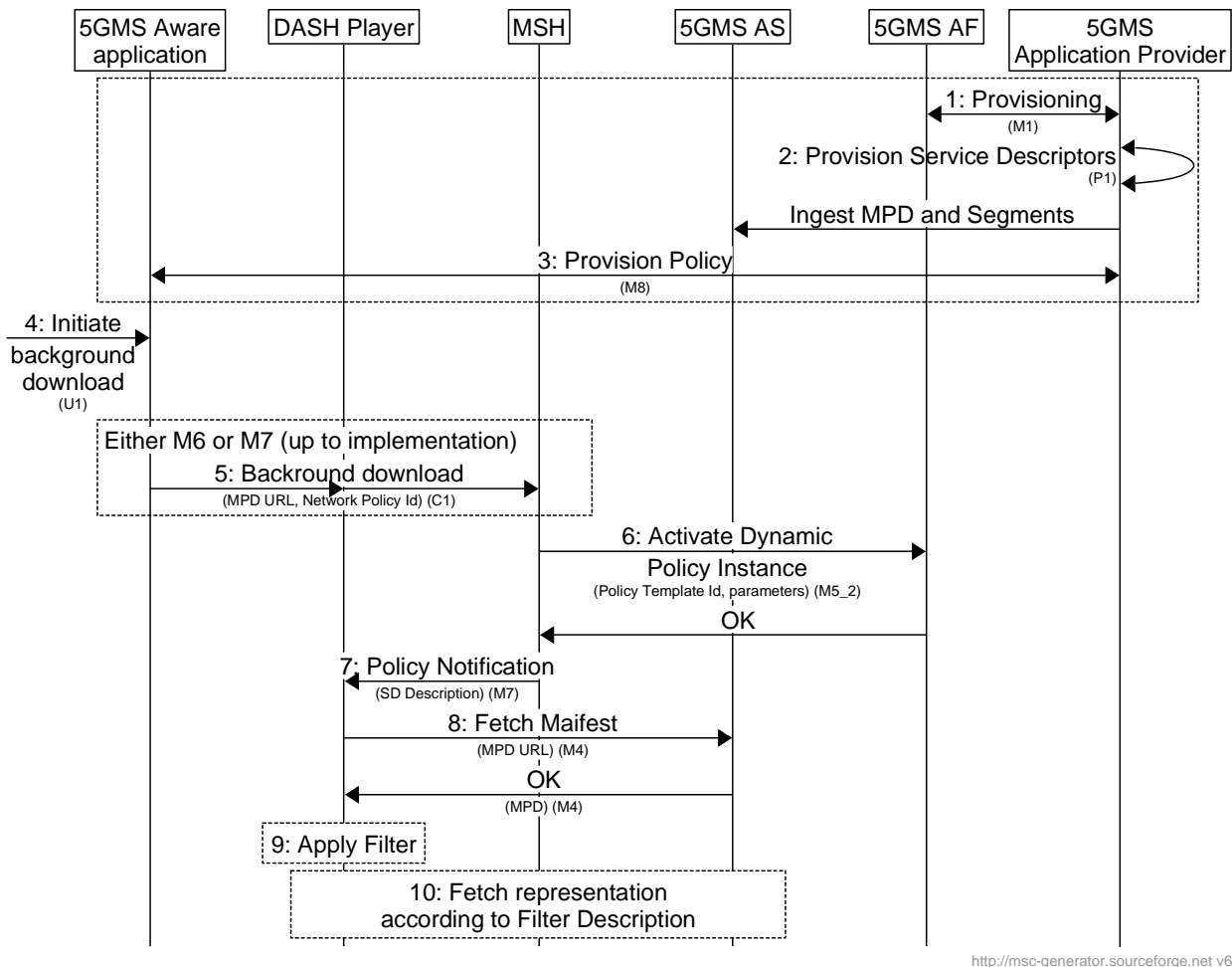


Figure A.4.1-1: Background Download Representations

A.4.2 Procedure

The procedure for activating a Background Download dynamic policy is illustrated in figure A.3.2-1 below.



<http://msc-generator.sourceforge.net> v6.3.7

Figure A.3.2-1: Procedure for activating Background Download dynamic policy

Steps:

1. The 5GMS Application Provider interacts with the 5GMS AF to set up one or more Policy Templates (M1). Each Policy Template is identified by a Policy Template identifier and contains information about how to activate the according policy within the 5G System (e.g. N5 URLs and parameters).
2. The 5GMS Application Provider also interacts with its DASH content generation function (e.g. an MPD provider) to annotate the DASH MPD with Service Descriptions, e.g. to identify, which representation is intended for background download.
3. The 5GMS-Aware Application is configured via M8 with information about the available content catalogue (e.g. resolving MPD URLs), the available subscription identifiers (e.g. the user has a 4K subscription or the user has an SD subscription), device type identifiers.

The 5GMSd-Aware Application is configured via M8 about the available background download policy. This includes the Network Policy Id which hints a background download policy.

4. When a user selects an item via the User Interface (U1) for Background Download the 5GMS-Aware Application translates the input to the needed 5GMSd API calls.
5. The 5GMS-Aware Application provides input (via C1) on the selected presentation entry (i.e. MPD URL) and also on the Network Policy Identifier (indicating a background download policy, i.e. make the Media Session Handler request a bearer suitable for Background Download).

NOTE: C1 is an abstract interface and indicates that the 5GMS-Aware Application may either first use M6 or M7 for the interactions with the 5GMS Client.

6. The Media Session Handler uses the Network Policy Identifier to find the procedure and the parameters to activate the Dynamic Policy Instance (here a Background Download policy). The Media Session Handler has received one or more Policy Descriptions together with matching Service Access Information (via M5_1). The Media Session Handler uses the Network Policy Identifier as a key to find the correct Policy Description. The Media Session Handler should activate a Dynamic Policy in the 5GMS AF, providing Service Data Flow Template information of the media flows (audio, video, etc). The Media Session Handler can also receive information on a bit rate policing (*enforcementMethod* and/or *enforcementBitrate*), e.g. that the bit rate is actively limited.
7. The Media Session Handler activates the Dynamic Policy instance on M5, providing the Policy Template identifier and additional parameters. Upon positive response, the Media Session handler notifies the DASH Player to start the Background Download. The notification contains a Service Descriptor Filters, which is used by the DASH Player to filter policy-compliant Service Descriptions from the MPD. The Media Session Handler may receive the Service Descriptor Filters with the response or may look up the Service Descriptor Filter values by a response value (e.g. derived from a maximum bit rate indication).

The Media Session Handler may need to update the Dynamic Policy instance, depending on the selected traffic detection method. For example, when the Media Session Handler uses 5-Tuples, it needs to update the Dynamic Policy instance with every newly opened and every closed TCP connection.

8. The DASH Player fetches the MPD of the selected content.
9. The DASH Access Engine / Selection Logic (see ISO 23009-1 [32] figure K.1) selects only adaptation sets and representations according to the filter (i.e. suitable for Background Download). Here, the DASH Player fetches the MPD after the notification from the Media Session Handler.

A.4.3 Example parameters

Table A.4.3-1: M5_1 Parameters for Policy Descriptions (used by the Media Session Handler)

Parameter	Type	Purpose	Example Values
Policy Description	Object		
Network Policy Id	String	Identifies the Policy Description.	"Background Download".
Service Access Information URL	URL	References the associated Service Access Information.	

Table A.4.3-2: M5_1 Parameters for Service Access Information

Parameter	Type		
Service Access Information	Object		
Policy Template Id	String	Identifies the Policy Template.	"backgrounddata".
5GMS AF URL	URL	Used to invoke the 5GMS AF.	
sdfMethods	[String]	Indication, which Service Data Flow Description methods are recommended to use by the media session handler.	"5-Tuple", "domainName", "TOS=xx", etc.
Mandatory M5 Request information	List	Desired bit rate, to be provided by the network for the application.	Policy Template Id, Average Bit rate, Service Data Flow Template.
M5 Response information	List	Information to the Media Session Handler on the response parameters.	

Annex B (informative): Content Hosting Configuration examples

B.1 Pull-based content ingest example

B.1.1 Overview

1. The 5GMSd Client on the UE requests a media resource via M4d.
2. The 5GMSd AS determines that it does not have a cached copy of the requested media resource.
3. The 5GMSd AS transforms the M4d request URL into a request to the 5GMSd Application Provider's origin server via M2d.

B.1.2 Desired URL mapping

In the example shown in table B.1.2-1 below, media resources are exposed at M4d from a default canonical domain `5gmsd-as.mno.net` determined by the 5GMSd System operator, and also from a custom domain name alias `mno-cdn.5gmsd-ap.com` that has been configured by the 5GMSd Application Provider.

Table B.1.2-1: Example URL mapping for pull-based ingest

M4d request from 5GMSd Client	Mapped M2d request to origin server on 5GMSd AS cache miss
<code>https://5gmsd-as.mno.net/m4d/provisioning-session9876/asset123456/video1/segment1000.mp4</code>	<code>https://origin.5gmsd-ap.com/media/asset123456/video1/segment1000.mp4</code>
<code>https://mno-cdn.5gmsd-ap.com/m4d/provisioning-session9876/asset123456/video1/segment1000.mp4</code>	
<code>https://5gmsd-as.mno.net/m4d/provisioning-session9876/asset123456/video2/segment1000.mp4</code>	<code>https://origin.5gmsd-ap.com/media/asset123456/video2/segment1000.mp4</code>
<code>https://mno-cdn.5gmsd-ap.com/m4d/provisioning-session9876/asset123456/video2/segment1000.mp4</code>	
<code>https://5gmsd-as.mno.net/m4d/provisioning-session9876/asset123456/audio1/segment1000.mp4</code>	<code>https://origin.5gmsd-ap.com/media/asset123456/audio1/segment1000.mp4</code>
<code>https://mno-cdn.5gmsd-ap.com/m4d/provisioning-session9876/asset123456/audio1/segment1000.mp4</code>	

B.1.3 Content Hosting Configuration

Table B.1.3-1 below shows the relevant Content Hosting Configuration parameters needed to achieve the example mapping described in table B.1.2-1 above.

Table B.1.3-1: Content Hosting Configuration properties relevant to pull-based ingest

Property	Example value	Set by
<i>IngestConfiguration</i>		
<i>protocol</i>	<code>urn:3gpp:5gms:content-protocol:http-pull-ingest</code>	5GMSd Application Provider
<i>pull</i>	<code>true</code>	
<i>baseURL</i>	<code>https://origin.5gmsd-ap.com/media</code>	
<i>DistributionConfiguration</i>		
<i>canonicalDomainName</i>	<code>5gmsd-as.mno.net</code>	5GMSd AF (M1d response)
<i>domainNameAlias</i>	<code>mno-cdn.5gmsd-ap.com</code>	5GMSd Application Provider
<i>baseURL</i>	<code>https://mno-cdn.5gmsd-ap.com/m4d/provisioning-session9876/</code>	5GMSd AF (M1d response)

B.2 Push-based content ingest example

B.2.0 Overview

1. The 5GMSd Application Provider uploads content to the 5GMSd AS via M2d.
2. The 5GMSd AS rewrites the M2d upload URL to an M4d downlink URL that is exposed to the 5GMSd Client on the UE.

B.2.1 Desired URL mapping

In the example shown in table B.2.1-1, media resources are pushed into the 5GMSd AS at M2d by the 5GMSd Application Provider and exposed to the 5GMSd Client at M4d using the canonical name of the 5GMSd AF `5gmsd-as.mno.net` and an additional domain name alias `mno-cdn.5gmsd-ap.com` configured by the 5GMSd Application Provider.

Table B.2.1-1: Example URL mapping for pull-based ingest

M2d ingest URL pushed to 5GMSd AS	M4d URL exposed to 5GMSd Client
https://5gmsd-as.mno.net/m2d/provisioning-session9876/asset123456/video1/segment1000.mp4	https://5gmsd-as.mno.net/m4d/provisioning-session9876/asset123456/video1/segment1000.mp4
	https://mno-cdn.5gmsd-ap.com/m4d/provisioning-session9876/asset123456/video1/segment1000.mp4
https://5gmsd-as.mno.net/m2d/provisioning-session9876/asset123456/video2/segment1000.mp4	https://5gmsd-as.mno.net/m4d/provisioning-session9876/asset123456/video2/segment1000.mp4
	https://mno-cdn.5gmsd-ap.com/m4d/provisioning-session9876/asset123456/video2/segment1000.mp4
https://5gmsd-as.mno.net/m2d/provisioning-session9876/asset123456/audio1/segment1000.mp4	https://5gmsd-as.mno.net/m4d/provisioning-session9876/asset123456/audio1/segment1000.mp4
	https://mno-cdn.5gmsd-ap.com/m4d/provisioning-session9876/asset123456/audio1/segment1000.mp4

B.2.2 Content Hosting Configuration

Table B.2.2-1 below shows the relevant Content Hosting Configuration parameters needed to achieve the example mapping described in table B.2.1-1 above.

Table B.2.2-1: Content Hosting Configuration properties relevant to push-based ingest

Property	Example value	Set by
<i>IngestConfiguration</i>		
<i>protocol</i>	urn:3gpp:5gms:content-protocol:dash-if-ingest	5GMSd Application Provider (M1d request)
<i>pull</i>	false	
<i>baseURL</i>	https://5gmsd-as.mno.net/m2d/provisioning-session9876/	
<i>DistributionConfiguration</i>		
<i>canonicalDomainName</i>	5gmsd-as.mno.net	5GMSd Application Provider (M1d response)
<i>domainNameAlias</i>	mno-cdn.5gmsd-ap.com	5GMSd Application Provider (M1d response)
<i>baseURL</i>	https://5gmsd-as.mno.net/m4d/provisioning-session9876/	5GMSd Application Provider (M1d response)

Annex C (normative): OpenAPI representation of the 5GMS HTTP REST APIs

C.1 General

This annex is based on the OpenAPI 3.0.0 specification [23] and provides corresponding representations of all APIs defined in the present document.

NOTE 1: An OpenAPIs representation embeds JSON Schema representations of HTTP message bodies.

This Annex shall take precedence when being discrepant to other parts of the present document with respect to the encoding of information elements and methods within the API(s).

NOTE 2: The semantics and procedures, as well as conditions, e.g. for the applicability and allowed combinations of attributes or values, not expressed in the OpenAPI definitions but defined in other parts of the specification also apply.

C.2 Data Types applicable to several APIs

For the purpose of referencing entities defined in this clause, it shall be assumed that the OpenAPI definitions below are contained in a physical file named "TS26512_CommonData.yaml".

```

openapi: 3.0.0
info:
  title: 5GMS Common Data Types
  version: 2.0.2
  description: |
    5GMS Common Data Types
    © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
tags:
  - name: 5GMS Common Data Types
    description: '5G Media Streaming: Common Data Types'
externalDocs:
  description: 'TS 26.512 V17.6.0; 5G Media Streaming (5GMS); Protocols'
  url: 'https://www.3gpp.org/ftp/Specs/archive/26_series/26.512/'
paths: {}
components:
  schemas:
    #####
    # Clause 6.4.2: Simple data types
    #####
    ResourceId:
      type: string
      description: String chosen by the 5GMS AF to serve as an identifier in a resource URI.
    Percentage:
      type: number
      minimum: 0.0
      maximum: 100.0
    #DurationSec is defined in TS29571_CommonData
    #DateTime is defined in TS29571_CommonData
    #Uri is defined in TS29571_CommonData
    Url:
      type: string
      format: uri-reference
      description: 'Uniform Resource Locator, conforming with the "URI-reference" production
specified in IETF RFC 3986, section 4.1.'
    RelativeUrl:
      type: string
      format: uri-reference
      description: 'Relative Uniform Resource Locator, conforming with the "relative-ref"
production specified in IETF RFC 3986, section 4.2. Note that both "query" and "fragment" suffixes
are permitted by this production.'
    AbsoluteUrl:
      type: string
      format: uri

```



```

description: 'Absolute Uniform Resource Locator, conforming with the "absolute-URI"
production specified in IETF RFC 3986, section 4.3 in which the scheme part is "http" or "https".
Note that the "query" suffix is permitted by this production but the "fragment" suffix is not.'

```

```

#####
# Clause 6.4.3: Structured data types
#####
IpPacketFilterSet:
  type: object
  required:
    - direction
  properties:
    srcIp:
      type: string
    dstIp:
      type: string
    protocol:
      type: integer
    srcPort:
      type: integer
    dstPort:
      type: integer
    toSTc:
      type: string
    flowLabel:
      type: integer
    spi:
      type: integer
    direction:
      type: string

ServiceDataFlowDescription:
  type: object
  properties:
    flowDescription:
      $ref: '#/components/schemas/IpPacketFilterSet'
    domainName:
      type: string

M5QoSSpecification:
  type: object
  required:
    - marBwDlBitRate
    - marBwUlBitRate
    - mirBwDlBitRate
    - mirBwUlBitRate
  properties:
    marBwDlBitRate:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
    marBwUlBitRate:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
    minDesBwDlBitRate:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
    minDesBwUlBitRate:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
    mirBwDlBitRate:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
    mirBwUlBitRate:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
    desLatency:
      type: integer
      minimum: 0
    desLoss:
      type: integer
      minimum: 0

M1QoSSpecification:
  type: object
  properties:
    qosReference:
      type: string
    maxBtrUl:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
    maxBtrDl:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
    maxAuthBtrUl:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
    maxAuthBtrDl:

```

```

    $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
  defPacketLossRateDl:
    type: integer
    minimum: 0
  defPacketLossRateUl:
    type: integer
    minimum: 0

ChargingSpecification:
  type: object
  properties:
    sponId:
      type: string
    sponStatus:
      $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/SponsoringStatus'
    gpsi:
      type: array
      items:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Gpsi'

TypedLocation:
  type: object
  required:
    - locationIdentifierType
    - location
  properties:
    locationIdentifierType:
      $ref: '#/components/schemas/CellIdentifierType'
    location:
      type: string

OperationSuccessResponse:
  type: object
  required:
    - success
  properties:
    success:
      type: boolean
    reason:
      type: string

EndpointAddress:
  type: object
  required:
    - portNumber
  properties:
    hostname:
      type: string
    ipv4Addr:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
    ipv6Addr:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Addr'
    portNumber:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Uint16'

EdgeProcessingEligibilityCriteria:
  type: object
  required:
    - serviceDataFlowDescriptions
    - ueLocations
    - timeWindows
    - appRequest
  properties:
    serviceDataFlowDescriptions:
      type: array
      items:
        $ref: '#/components/schemas/ServiceDataFlowDescription'
    ueLocations:
      type: array
      items:
        $ref: 'TS29122_CommonData.yaml#/components/schemas/LocationArea5G'
    timeWindows:
      type: array
      items:
        $ref: 'TS29122_CommonData.yaml#/components/schemas/TimeWindow'
    appRequest:
      type: boolean

```

```
#####
# Clause 6.4.4: Enumerated data types
#####
CellIdentifierType:
  anyOf:
    - type: string
      enum: [CGI, ECGI, NCGI]
    - type: string
      description: >
        This string provides forward-compatibility with future
        extensions to the enumeration but is not used to encode
        content defined in the present version of this API.

SdfMethod:
  anyOf:
    - type: string
      enum: [5_TUPLE, 2_TUPLE, TYPE_OF_SERVICE_MARKING, FLOW_LABEL, DOMAIN_NAME]
    - type: string
      description: >
        This string provides forward-compatibility with future
        extensions to the enumeration but is not used to encode
        content defined in the present version of this API.

ProvisioningSessionType:
  anyOf:
    - type: string
      enum: [DOWNLINK, UPLINK]
    - type: string
      description: >
        This string provides forward-compatibility with future
        extensions to the enumeration but is not used to encode
        content defined in the present version of this API.

CacheStatus:
  anyOf:
    - type: string
      enum: [HIT, MISS, EXPIRED]
    - type: string
      description: >
        This string provides forward-compatibility with future
        extensions to the enumeration but is not used to encode
        content defined in the present version of this API.

EASRelocationTolerance:
  anyOf:
    - type: string
      enum: [RELOCATION_UNAWARE, RELOCATION_TOLERANT, RELOCATION_INTOLERANT]
    - type: string
      description: >
        This string provides forward-compatibility with future
        extensions to the enumeration but is not used to encode
        content defined in the present version of this API.
```

C.3 OpenAPI representation of the M1 APIs

C.3.1 M1_ProvisioningSessions API

```
openapi: 3.0.0
info:
  title: M1_ProvisioningSessions
  version: 2.1.0
  description: |
    5GMS AF M1 Provisioning Sessions API
    © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
tags:
  - name: M1_ProvisioningSessions
    description: '5G Media Streaming: Provisioning (M1) APIs: Provisioning Sessions'
externalDocs:
  description: 'TS 26.512 V17.7.0; 5G Media Streaming (5GMS); Protocols'
  url: 'https://www.3gpp.org/ftp/Specs/archive/26_series/26.512/'
servers:
```

```

- url: '{apiRoot}/3gpp-m1/v2'
  variables:
    apiRoot:
      default: https://example.com
      description: See 3GPP TS 29.512 clause 6.1.
  paths:
    /provisioning-sessions:
      post:
        operationId: createProvisioningSession
        summary: 'Create a new Provisioning Session'
        responses:
          '201':
            description: 'Provisioning Session Created'
            headers:
              Location:
                description: 'URL including the resource identifier of the newly created Provisionin
g Session.'
                required: true
                schema:
                  $ref: 'TS26512_CommonData.yaml#/components/schemas/AbsoluteUrl'
            content:
              application/json:
                schema:
                  $ref: '#/components/schemas/ProvisioningSession'
    /provisioning-sessions/{provisioningSessionId}:
      parameters:
        - name: provisioningSessionId
          in: path
          required: true
          schema:
            $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
          description: 'The resource identifier of an existing Provisioning Session.'
      get:
        operationId: getProvisioningSessionById
        summary: 'Retrieve an existing Provisioning Session'
        responses:
          '200':
            description: 'Success'
            content:
              application/json:
                schema:
                  $ref: '#/components/schemas/ProvisioningSession'
      delete:
        operationId: destroyProvisioningSession
        summary: 'Destroy an existing Provisioning Session'
        responses:
          '204':
            description: 'Provisioning Session Destroyed'
            # No Content
  components:
    schemas:
      ProvisioningSession:
        type: object
        description: "A representation of a Provisioning Session."
        required:
          - provisioningSessionId
          - provisioningSessionType
          - appId
        properties:
          provisioningSessionId:
            $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
          provisioningSessionType:
            $ref: 'TS26512_CommonData.yaml#/components/schemas/ProvisioningSessionType'
          aspId:
            $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/AspId'
          appId:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/ApplicationId'
          serverCertificateIds:
            type: array
            items:
              $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
            minItems: 1
            uniqueItems: true
          contentPreparationTemplateIds:
            type: array
            items:
              $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
            minItems: 1

```

```

    uniqueItems: true
  metricsReportingConfigurationIds:
    type: array
    items:
      $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
    minItems: 1
    uniqueItems: true
  policyTemplateIds:
    type: array
    items:
      $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
    minItems: 1
    uniqueItems: true
  edgeResourcesConfigurationIds:
    type: array
    items:
      $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
    minItems: 1
    uniqueItems: true
  eventDataProcessingConfigurationIds:
    type: array
    items:
      $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
    minItems: 1
    uniqueItems: true

```

C.3.2 M1_ServerCertificatesProvisioning API

```

openapi: 3.0.0
info:
  title: M1_ServerCertificatesProvisioning
  version: 2.1.1
  description: |
    5GMS AF M1 Server Certificates Provisioning API
    © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
tags:
  - name: M1_ServerCertificatesProvisioning
    description: '5G Media Streaming: Provisioning (M1) APIs: Server Certificates Provisioning'
externalDocs:
  description: 'TS 26.512 V17.5.0; 5G Media Streaming (5GMS); Protocols'
  url: 'https://www.3gpp.org/ftp/Specs/archive/26_series/26.512/'
servers:
  - url: '{apiRoot}/3gpp-m1/v2'
    variables:
      apiRoot:
        default: https://example.com
        description: See 3GPP TS 29.512 clause 6.1.
paths:
  /provisioning-sessions/{provisioningSessionId}/certificates:
    parameters:
      - name: provisioningSessionId
        in: path
        required: true
        schema:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        description: 'The resource identifier of an existing Provisioning Session.'
    post:
      operationId: createOrReserveServerCertificate
      summary: 'Create or reserve a Service Certificate resource'
      description: 'Without the optional csr query parameter, an X.509 certificate is generated and this is returned. If the csr query parameter is present, a Certificate Signing Request is instead generated and returned, allowing the X.509 certificate to be generated by the invoker and later uploaded.'
      parameters:
        - in: query
          name: csr
          schema:
            type: string
          description: 'When present, return a Certificate Signing Request instead of generating an X.509 certificate'
      requestBody:
        description: 'An optional list of domain name aliases to be included in the returned Certificate Signing Request'
        content:

```

```

      'application/json':
        schema:
          type: array
          items:
            type: string
    responses:
      '200':
        description: 'Server Certificate Created'
        headers:
          Location:
            description: 'URL of the newly created Server Certificate resource'
            required: true
            schema:
              $ref: 'TS26512_CommonData.yaml#/components/schemas/AbsoluteUrl'
        content:
          'application/x-pem-file':
            schema:
              type: string

/provisioning-sessions/{provisioningSessionId}/certificates/{certificateId}:
  parameters:
    - name: provisioningSessionId
      in: path
      required: true
      schema:
        $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
      description: 'The resource identifier of an existing Provisioning Session.'
    - name: certificateId
      in: path
      required: true
      schema:
        $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
      description: 'The resource identifier of an existing Server Certificate'
  put:
    operationId: uploadServerCertificate
    summary: "Upload the X.509 certificate for a previously reserved Server Certificate resource"
    requestBody:
      required: true
      content:
        application/x-pem-file:
          schema:
            type: string
    responses:
      '204':
        description: 'Server Certificate Updated'
  get:
    operationId: retrieveServerCertificate
    summary: 'Retrieve the X.509 certificate representation of the specified Server Certificate resource'
    responses:
      '200':
        description: 'Success'
        content:
          'application/x-pem-file':
            schema:
              type: string
      '204':
        description: 'Awaiting Upload'
      '404':
        description: 'Not Found'
  delete:
    operationId: destroyServerCertificate
    summary: 'Destroy an existing Server Certificate resource'
    responses:
      '200':
        # OK
        description: 'Server Certificate Destroyed'
        content:
          'application/x-pem-file':
            schema:
              type: string
      '204':
        # No Content
        description: 'Server Certificate Destroyed'
      '404':
        # Not Found
        $ref: 'TS29571_CommonData.yaml#/components/responses/404'

```

```

'409':
  # Conflict
  $ref: 'TS29571_CommonData.yaml#/components/responses/409'
'410':
  # Gone
  $ref: 'TS29571_CommonData.yaml#/components/responses/410'

```

C.3.3 M1_ContentPreparationTemplatesProvisioning API

```

openapi: 3.0.0
info:
  title: M1_ContentPreparationTemplatesProvisioning
  version: 2.1.1
  description: |
    5GMS AF M1 Content Preparation Templates Provisioning API
    © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
tags:
  - name: M1_ContentPreparationTemplatesProvisioning
    description: '5G Media Streaming: Provisioning (M1) APIs: Content Preparation Templates Provisioning'
externalDocs:
  description: 'TS 26.512 V17.7.0; 5G Media Streaming (5GMS); Protocols'
  url: 'https://www.3gpp.org/ftp/Specs/archive/26_series/26.512/'
servers:
  - url: '{apiRoot}/3gpp-m1/v2'
    variables:
      apiRoot:
        default: https://example.com
        description: See 3GPP TS 29.512 clause 6.1.
paths:
  /provisioning-sessions/{provisioningSessionId}/content-preparation-templates:
    parameters:
      - name: provisioningSessionId
        in: path
        required: true
        schema:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        description: 'The resource identifier of an existing Provisioning Session.'
    post:
      operationId: createContentPreparationTemplate
      summary: 'Create (and optionally upload) a new Content Preparation Template for the specific Provisioning Session'
      requestBody:
        description: 'A Content Preparation Template of any supported type'
        required: true
        content:
          '*/*':
            schema:
              type: string
      responses:
        '201':
          description: 'Content Preparation Template Created'
          headers:
            Location:
              description: 'URL of the newly created Content Preparation Template.'
              required: true
              schema:
                $ref: 'TS26512_CommonData.yaml#/components/schemas/AbsoluteUrl'
        '415':
          # Unsupported Media Type
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
        '503':
          # Service Unavailable
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
  /provisioning-sessions/{provisioningSessionId}/content-preparation-templates/{contentPreparationTemplateId}:
    parameters:
      - name: provisioningSessionId
        in: path
        required: true
        schema:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        description: 'The resource identifier of an existing Provisioning Session.'

```

```

- name: contentPreparationTemplateId
  in: path
  required: true
  schema:
    $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
  description: 'The resource identifier of an existing Content Preparation Template.'
get:
  operationId: retrieveContentPreparationTemplate
  summary: 'Retrieve the specified Content Preparation Template of the specified Provisioning
Session'
  responses:
    '200':
      description: 'Success'
      content:
        '*/*':
          schema:
            type: string
put:
  operationId: updateContentPreparationTemplate
  summary: 'Update the specified Content Preparation Template for the specified Provisioning S
ession'
  requestBody:
    description: 'A Content Preparation Template of any type'
    required: true
    content:
      '*/*':
        schema:
          type: string
  responses:
    '204':
      description: 'Updated Content Preparation Template'
    '404':
      description: 'Not Found'
    '415':
      # Unsupported Media Type
      $ref: 'TS29571_CommonData.yaml#/components/responses/415'
    '503':
      # Service Unavailable
      $ref: 'TS29571_CommonData.yaml#/components/responses/503'
patch:
  operationId: patchContentPreparationTemplate
  summary: 'Patch the specified Content Preparation Template for the specified Provisioning Se
ssion'
  requestBody:
    description: 'A Content Preparation Template patch of any type'
    required: true
    content:
      application/merge-patch+json:
        schema:
          type: string
      application/json-patch+json:
        schema:
          type: string
  responses:
    '200':
      description: 'Patched Content Preparation Templates'
      content:
        '*/*':
          schema:
            type: string
    '404':
      description: 'Not Found'
    '415':
      # Unsupported Media Type
      $ref: 'TS29571_CommonData.yaml#/components/responses/415'
    '503':
      # Service Unavailable
      $ref: 'TS29571_CommonData.yaml#/components/responses/503'
delete:
  operationId: destroyContentPreparationTemplate
  summary: 'Destroy the specified Content Preparation Template of the specified Provisioning S
ession'
  responses:
    '200':
      # OK
      description: 'Content Preparation Template Destroyed'
      content:
        '*/*':

```



```

    schema:
      type: string
  '204':
    # No Content
    description: 'Content Preparation Template Destroyed'
  '404':
    # Not Found
    $ref: 'TS29571_CommonData.yaml#/components/responses/404'
  '409':
    # Conflict
    $ref: 'TS29571_CommonData.yaml#/components/responses/409'
  '410':
    # Gone
    $ref: 'TS29571_CommonData.yaml#/components/responses/410'

```

C.3.4 M1_ContentProtocolsDiscovery API

```

openapi: 3.0.0
info:
  title: M1_ContentProtocolsDiscovery
  version: 2.0.0
  description: |
    5GMS AF M1 Content Protocols Discovery API
    © 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
tags:
  - name: M1_ContentDiscovery
    description: '5G Media Streaming: Provisioning (M1) APIs: Content Protocols Discovery'
externalDocs:
  description: 'TS 26.512 V17.2.0; 5G Media Streaming (5GMS); Protocols'
  url: 'https://www.3gpp.org/ftp/Specs/archive/26_series/26.512/'
servers:
  - url: '{apiRoot}/3gpp-m1/v2'
    variables:
      apiRoot:
        default: https://example.com
        description: See 3GPP TS 29.512 clause 6.1.
paths:
  /provisioning-sessions/{provisioningSessionId}/protocols:
    parameters:
      - name: provisioningSessionId
        in: path
        required: true
        schema:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        description: 'The resource identifier of an existing Provisioning Session.'
    get:
      operationId: retrieveContentProtocols
      summary: 'Retrieve the set of Content Protocols supported by the specified Provisioning Session'
      responses:
        '200':
          description: 'Success'
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/ContentProtocols'
components:
  schemas:
    ContentProtocolDescriptor:
      type: object
      description: "A descriptor describing a content protocol."
      required:
        - termIdentifier
      properties:
        termIdentifier:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        descriptionLocator:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/Url'
    ContentProtocols:
      type: object
      description: "A representation of the Content Protocols resource."
      properties:
        downlinkIngestProtocols:

```

```

    type: array
    items:
      $ref: '#/components/schemas/ContentProtocolDescriptor'
    minItems: 1
  uplinkEgestProtocols:
    type: array
    items:
      $ref: '#/components/schemas/ContentProtocolDescriptor'
    minItems: 1
  geoFencingLocatorTypes:
    type: array
    items:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
    minItems: 1

```

C.3.5 M1_ContentHostingProvisioning API

```

openapi: 3.0.0
info:
  title: M1_ContentHostingProvisioning
  version: 2.2.3
  description: |
    5GMS AF M1 Content Hosting Provisioning API
    © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
tags:
  - name: M1_ContentHostingProvisioning
    description: '5G Media Streaming: Provisioning (M1) APIs: Content Hosting Provisioning'
externalDocs:
  description: 'TS 26.512 V17.7.0; 5G Media Streaming (5GMS); Protocols'
  url: 'https://www.3gpp.org/ftp/Specs/archive/26_series/26.512/'
servers:
  - url: '{apiRoot}/3gpp-m1/v2'
    variables:
      apiRoot:
        default: https://example.com
        description: See 3GPP TS 29.512 clause 6.1.
paths:
  /provisioning-sessions/{provisioningSessionId}/content-hosting-configuration:
    parameters:
      - name: provisioningSessionId
        in: path
        required: true
        schema:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        description: 'The resource identifier of an existing Provisioning Session.'
    post:
      operationId: createContentHostingConfiguration
      summary: 'Create (and optionally upload) the Content Hosting Configuration for the specified Provisioning Session'
      requestBody:
        description: 'A JSON representation of a Content Hosting Configuration'
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/ContentHostingConfiguration'
      responses:
        '201':
          description: 'Content Hosting Configuration Created'
          headers:
            Location:
              description: 'URL of the newly created Content Hosting Configuration (same as request URL).'
              required: true
              schema:
                $ref: 'TS26512_CommonData.yaml#/components/schemas/AbsoluteUrl'
    get:
      operationId: retrieveContentHostingConfiguration
      summary: 'Retrieve the Content Hosting Configuration of the specified Provisioning Session'
      responses:
        '200':
          description: 'Success'
          content:
            application/json:

```

```

        schema:
          $ref: '#/components/schemas/ContentHostingConfiguration'
      '404':
        description: 'Not Found'
    put:
      operationId: updateContentHostingConfiguration
      summary: 'Update the Content Hosting Configuration for the specified Provisioning Session'
      requestBody:
        description: 'A JSON representation of a Content Hosting Configuration'
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/ContentHostingConfiguration'
      responses:
        '204':
          description: 'Updated Content Hosting Configuration'
        '404':
          description: 'Not Found'
    patch:
      operationId: patchContentHostingConfiguration
      summary: 'Patch the Content Hosting Configuration for the specified Provisioning Session'
      requestBody:
        description: 'A JSON representation of a Content Hosting Configuration'
        required: true
        content:
          application/merge-patch+json:
            schema:
              $ref: '#/components/schemas/ContentHostingConfiguration'
          application/json-patch+json:
            schema:
              $ref: '#/components/schemas/ContentHostingConfiguration'
      responses:
        '200':
          description: 'Patched Content Hosting Configuration'
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/ContentHostingConfiguration'
        '404':
          description: 'Not Found'
    delete:
      operationId: destroyContentHostingConfiguration
      summary: 'Destroy the current Content Hosting Configuration of the specified Provisioning Session'
      responses:
        '204':
          description: 'Destroyed Content Hosting Configuration'
        '404':
          description: 'Not Found'

/provisioning-sessions/{provisioningSessionId}/content-hosting-configuration/purge:
  parameters:
    - name: provisioningSessionId
      in: path
      required: true
      schema:
        $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
      description: A unique identifier of the Provisioning
  post:
    operationId: purgeContentHostingCache
    summary: 'Purge the content of the cache for the Content Hosting Configuration of the specified Provisioning Session'
    requestBody:
      description: 'The regular expression pattern for resources to purge from the cache'
      required: true
      content:
        application/x-www-form-urlencoded:
          schema:
            properties:
              pattern:
                description: 'The regular expression'
                type: string
    responses:
      '200':
        # OK
        description: 'Content Purged'
        content:

```

```

    application/json:
      schema:
        description: 'The aggregate number of cache entries purged in all 5GMSd AS
instances distributing content for the requested Provisioning Session.'
        type: integer
        minimum: 1
    '204':
      # No Content
      description: 'No Content Purged'
    '400':
      # Bad Request (e.g. syntactically invalid regular expression in request body)
      $ref: 'TS29571_CommonData.yaml#/components/responses/400'
    '404':
      # Not Found
      $ref: 'TS29571_CommonData.yaml#/components/responses/404'
    '413':
      # Payload Too Large
      $ref: 'TS29571_CommonData.yaml#/components/responses/413'
    '414':
      # URI Too Long
      $ref: 'TS29571_CommonData.yaml#/components/responses/414'
    '415':
      # Unsupported Media Type
      $ref: 'TS29571_CommonData.yaml#/components/responses/415'
    '500':
      # Internal Server Error
      $ref: 'TS29571_CommonData.yaml#/components/responses/500'
    '503':
      # Service Unavailable
      $ref: 'TS29571_CommonData.yaml#/components/responses/503'
    default:
      $ref: 'TS29571_CommonData.yaml#/components/responses/default'

```

```

components:
  schemas:
    IngestConfiguration:
      type: object
      description: 'A configuration for content ingest.'
      properties:
        pull:
          type: boolean
        protocol:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        baseURL:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/AbsoluteUrl'

    MIMediaEntryPoint:
      description: 'A typed entry point for downlink or uplink media streaming.'
      type: object
      required:
        - relativePath
        - contentType
      properties:
        relativePath:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/RelativeUrl'
        contentType:
          type: string
        profiles:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
          minItems: 1

    PathRewriteRule:
      type: object
      description: 'A rule to manipulate URL paths.'
      required:
        - requestPathPattern
        - mappedPath
      properties:
        requestPathPattern:
          type: string
        mappedPath:
          type: string

    CachingConfiguration:
      type: object
      description: 'A content caching configuration.'

```

```

required:
  - urlPatternFilter
properties:
  urlPatternFilter:
    type: string
  cachingDirectives:
    type: object
    required:
      - noCache
    properties:
      statusCodeFilters:
        type: array
        items:
          type: integer
      noCache:
        type: boolean
      maxAge:
        type: integer
        format: int32

DistributionConfiguration:
  type: object
  description: 'A content distribution configuration.'
  properties:
    entryPoint:
      $ref: '#/components/schemas/M1MediaEntryPoint'
    contentPreparationTemplateId:
      $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
    edgeResourcesConfigurationId:
      $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
    canonicalDomainName:
      type: string
    domainNameAlias:
      type: string
    baseURL:
      $ref: 'TS26512_CommonData.yaml#/components/schemas/AbsoluteUrl'
    pathRewriteRules:
      type: array
      items:
        $ref: '#/components/schemas/PathRewriteRule'
    cachingConfigurations:
      type: array
      items:
        $ref: '#/components/schemas/CachingConfiguration'
    geoFencing:
      type: object
      required:
        - locatorType
        - locators
      properties:
        locatorType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        locators:
          type: array
          items:
            type: string
            description: 'Format of individual locators depends on the locatorType.'
          minItems: 1
    urlSignature:
      type: object
      required:
        - urlPattern
        - tokenName
        - passphraseName
        - passphrase
        - tokenExpiryName
        - useIPAddress
      properties:
        urlPattern:
          type: string
        tokenName:
          type: string
        passphraseName:
          type: string
        passphrase:
          type: string
        tokenExpiryName:
          type: string

```

```

    useIPAddress:
      type: boolean
    ipAddressName:
      type: string
  certificateId:
    $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
  supplementaryDistributionNetworks:
    type: array
    items:
      type: object
      description: "A tuple tying a type of supplementary distribution network to its distribution mode."
      required:
        - distributionNetworkType
        - distributionMode
      properties:
        distributionNetworkType:
          $ref: '#/components/schemas/DistributionNetworkType'
        distributionMode:
          $ref: '#/components/schemas/DistributionMode'

# Schema for the resource itself
ContentHostingConfiguration:
  type: object
  description: "A representation of a Content Hosting Configuration resource."
  required:
    - name
    - ingestConfiguration
    - distributionConfigurations
  properties:
    name:
      type: string
    ingestConfiguration:
      $ref: '#/components/schemas/IngestConfiguration'
    distributionConfigurations:
      type: array
      items:
        $ref: '#/components/schemas/DistributionConfiguration'

DistributionNetworkType:
  description: "Type of distribution network."
  anyOf:
    - type: string
      enum: [NETWORK_EMBMS]
    - type: string
      description: >
        This string provides forward-compatibility with future
        extensions to the enumeration but is not used to encode
        content defined in the present version of this API.

DistributionMode:
  description: "Mode of content distribution."
  anyOf:
    - type: string
      enum: [MODE_EXCLUSIVE, MODE_HYBRID, MODE_DYNAMIC]
    - type: string
      description: >
        This string provides forward-compatibility with future
        extensions to the enumeration but is not used to encode
        content defined in the present version of this API.

```

C.3.6 M1_ConsumptionReportingProvisioning API

```

openapi: 3.0.0
info:
  title: M1_ConsumptionReportingProvisioning
  version: 2.1.0
  description: |
    5GMS AF M1 Consumption Reporting Provisioning API
    © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
tags:
  - name: M1_ConsumptionReportingProvisioning
    description: '5G Media Streaming: Provisioning (M1) APIs: Consumption Reporting Provisioning'
externalDocs:

```

```

description: 'TS 26.512 V17.7.0; 5G Media Streaming (5GMS); Protocols'
url: 'https://www.3gpp.org/ftp/Specs/archive/26_series/26.512/'
servers:
  - url: '{apiRoot}/3gpp-m1/v2'
    variables:
      apiRoot:
        default: https://example.com
        description: See 3GPP TS 29.512 clause 6.1.
paths:
  /provisioning-sessions/{provisioningSessionId}/consumption-reporting-configuration:
    parameters:
      - name: provisioningSessionId
        in: path
        required: true
        schema:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        description: 'The resource identifier of an existing Provisioning Session.'
    post:
      operationId: activateConsumptionReporting
      summary: 'Activate the consumption reporting procedure for the specified Provisioning Session by providing the Consumption Reporting Configuration'
      requestBody:
        description: 'A JSON representation of a Consumption Reporting Configuration'
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/ConsumptionReportingConfiguration'
      responses:
        '201':
          description: 'Consumption Reporting Configuration Created'
          headers:
            Location:
              description: 'URL of the newly created Consumption Reporting Configuration (same as request URL).'
              required: true
              schema:
                $ref: 'TS26512_CommonData.yaml#/components/schemas/AbsoluteUrl'
    get:
      operationId: retrieveConsumptionReportingConfiguration
      summary: 'Retrieve the Consumption Reporting Configuration of the specified Provisioning Session'
      responses:
        '200':
          description: 'Success'
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/ConsumptionReportingConfiguration'
    put:
      operationId: updateConsumptionReportingConfiguration
      summary: 'Update the Consumption Reporting Configuration for the specified Provisioning Session'
      requestBody:
        description: 'A JSON representation of a Consumption Reporting Configuration'
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/ConsumptionReportingConfiguration'
      responses:
        '204':
          description: 'Updated Consumption Reporting Configuration'
        '404':
          description: 'Not Found'
    patch:
      operationId: patchConsumptionReportingConfiguration
      summary: 'Patch the Consumption Reporting Configuration for the specified Provisioning Session'
      requestBody:
        description: 'A JSON representation of a Consumption Reporting Configuration'
        required: true
        content:
          application/merge-patch+json:
            schema:
              $ref: '#/components/schemas/ConsumptionReportingConfiguration'
          application/json-patch+json:
            schema:

```

```

    $ref: '#/components/schemas/ConsumptionReportingConfiguration'
  responses:
    '200':
      description: 'Patched Consumption Reporting Configuration'
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/ConsumptionReportingConfiguration'
    '404':
      description: 'Not Found'
  delete:
    operationId: destroyConsumptionReportingConfiguration
    summary: 'Destroy the current Consumption Reporting Configuration of the specified Provisioning Session'
    responses:
      '204':
        description: 'Destroyed Consumption Reporting Configuration'
      '404':
        description: 'Not Found'
components:
  schemas:
    ConsumptionReportingConfiguration:
      type: object
      description: "A representation of a Consumption Reporting Configuration resource."
      properties:
        reportingInterval:
          minimum: 0
          exclusiveMinimum: true
          allOf:
            - $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
        samplePercentage:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/Percentage'
        locationReporting:
          type: boolean
        accessReporting:
          type: boolean

```

C.3.7 M1_MetricsReportingProvisioning API

```

openapi: 3.0.0
info:
  title: M1_MetricsReportingProvisioning
  version: 2.2.0
  description: |
    5GMS AF M1 Metrics Reporting Provisioning API
    © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
tags:
  - name: M1_MetricsReportingProvisioning
    description: '5G Media Streaming: Provisioning (M1) APIs: Metrics Reporting Provisioning'
externalDocs:
  description: 'TS 26.512 V17.9.0; 5G Media Streaming (5GMS); Protocols'
  url: 'https://www.3gpp.org/ftp/Specs/archive/26_series/26.512/'
servers:
  - url: '{apiRoot}/3gpp-m1/v2'
    variables:
      apiRoot:
        default: https://example.com
        description: See 3GPP TS 29.512 clause 6.1.
paths:
  /provisioning-sessions/{provisioningSessionId}/metrics-reporting-configurations:
    parameters:
      - name: provisioningSessionId
        in: path
        required: true
        schema:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        description: 'The resource identifier of an existing Provisioning Session.'
    post:
      operationId: activateMetricsReporting
      summary: 'Activate the Metrics reporting procedure for the specified Provisioning Session by providing the Metrics Reporting Configuration'
      requestBody:
        description: 'A JSON representation of a Metrics Reporting Configuration'
        required: true

```



```

    content:
      application/json:
        schema:
          $ref: '#/components/schemas/MetricsReportingConfiguration'
    responses:
      '201':
        description: 'Metrics Reporting Configuration Created'
        headers:
          Location:
            description: 'URL of the newly created Metrics Reporting Configuration (same as request URL).'
            required: true
            schema:
              $ref: 'TS26512_CommonData.yaml#/components/schemas/AbsoluteUrl'
/provisioning-sessions/{provisioningSessionID}/metrics-reporting-configurations/{metricsReportingConfigurationId}:
  parameters:
    - name: provisioningSessionId
      in: path
      required: true
      schema:
        $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
      description: 'The resource identifier of an existing Provisioning Session.'
    - name: metricsReportingConfigurationId
      in: path
      required: true
      schema:
        $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
      description: 'The resource identifier of a Metrics Reporting Configuration.'
  get:
    operationId: retrieveMetricsReportingConfiguration
    summary: 'Retrieve the specified Metrics Reporting Configuration of the specified Provisioning Session'
    responses:
      '200':
        description: 'Success'
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/MetricsReportingConfiguration'
  put:
    operationId: updateMetricsReportingConfiguration
    summary: 'Update the specified Metrics Reporting Configuration for the specified Provisioning Session'
    requestBody:
      description: 'A JSON representation of a Metrics Reporting Configuration'
      required: true
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/MetricsReportingConfiguration'
    responses:
      '204':
        description: 'Updated Metrics Reporting Configuration'
      '404':
        description: 'Not Found'
  patch:
    operationId: patchMetricsReportingConfiguration
    summary: 'Patch the specified Metrics Reporting Configuration for the specified Provisioning Session'
    requestBody:
      description: 'A JSON representation of a Metrics Reporting Configuration'
      required: true
      content:
        application/merge-patch+json:
          schema:
            $ref: '#/components/schemas/MetricsReportingConfiguration'
        application/json-patch+json:
          schema:
            $ref: '#/components/schemas/MetricsReportingConfiguration'
    responses:
      '200':
        description: 'Patched Metrics Reporting Configuration'
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/MetricsReportingConfiguration'
      '404':

```

```

        description: 'Not Found'
      delete:
        operationId: destroyMetricsReportingConfiguration
        summary: 'Destroy the specified Metrics Reporting Configuration of the specified Provisionin
g Session'
        responses:
          '204':
            description: 'Destroyed Metrics Reporting Configuration'
          '404':
            description: 'Not Found'
    components:
      schemas:
        MetricsReportingConfiguration:
          type: object
          description: "A representation of a Metrics Reporting Configuration resource."
          required:
            - metricsReportingConfigurationId
            - samplingPeriod
          properties:
            metricsReportingConfigurationId:
              $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
            sliceScope:
              type: array
              items:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
              minItems: 1
            scheme:
              $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
            dataNetworkName:
              $ref: 'TS29571_CommonData.yaml#/components/schemas/Dnn'
            reportingInterval:
              minimum: 0
              exclusiveMinimum: true
              allOf:
                - $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
            samplePercentage:
              $ref: 'TS26512_CommonData.yaml#/components/schemas/Percentage'
            urlFilters:
              type: array
              items:
                type: string
              minItems: 1
            samplingPeriod:
              minimum: 0
              exclusiveMinimum: true
              allOf:
                - $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
            metrics:
              type: array
              items:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
              minItems: 1

```

C.3.8 M1_PolicyTemplatesProvisioning API

```

openapi: 3.0.0
info:
  title: M1_PolicyTemplatesProvisioning
  version: 2.2.1
  description: |
    5GMS AF M1 Policy Templates Provisioning API
    © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
tags:
  - name: M1_PolicyTemplatesProvisioning
    description: '5G Media Streaming: Provisioning (M1) APIs: Policy Templates Provisioning'
externalDocs:
  description: 'TS 26.512 V17.7.0; 5G Media Streaming (5GMS); Protocols'
  url: 'https://www.3gpp.org/ftp/Specs/archive/26_series/26.512/'
servers:
  - url: '{apiRoot}/3gpp-m1/v2'
    variables:
      apiRoot:
        default: https://example.com
        description: See 3GPP TS 29.512 clause 6.1.

```

```

paths:
  /provisioning-sessions/{provisioningSessionId}/policy-templates:
    parameters:
      - name: provisioningSessionId
        in: path
        required: true
        schema:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        description: 'The resource identifier of an existing Provisioning Session.'
    post:
      operationId: createPolicyTemplate
      summary: 'Create (and optionally upload) a new Policy Template'
      requestBody:
        description: 'A JSON representation of a Policy Template'
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/PolicyTemplate'
      responses:
        '201':
          description: 'Policy Template Created'
          headers:
            Location:
              description: 'URL of the newly created Policy Template resource.'
              required: true
              schema:
                $ref: 'TS26512_CommonData.yaml#/components/schemas/AbsoluteUrl'

  /provisioning-sessions/{provisioningSessionId}/policy-templates/{policyTemplateId}:
    parameters:
      - name: provisioningSessionId
        in: path
        required: true
        schema:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        description: 'A unique identifier of the Provisioning Session.'
      - name: policyTemplateId
        in: path
        required: true
        schema:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        description: 'A resource identifier of a Policy Template.'
    get:
      operationId: retrievePolicyTemplate
      summary: 'Retrieve a representation of an existing Policy Template in the specified Provisioning Session'
      responses:
        '200':
          description: 'Success'
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/PolicyTemplate'
        '404':
          description: 'Not Found'
    put:
      operationId: updatePolicyTemplate
      summary: 'Update a Policy Template for the specified Provisioning Session'
      requestBody:
        description: 'A JSON representation of a Policy Template'
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/PolicyTemplate'
      responses:
        '204':
          description: 'Updated Policy Template'
        '404':
          description: 'Not Found'
    patch:
      operationId: patchPolicyTemplate
      summary: 'Patch the Policy Template for the specified Provisioning Session'
      requestBody:
        description: 'A JSON representation of a Policy Template'
        required: true
        content:

```

```

    application/merge-patch+json:
      schema:
        $ref: '#/components/schemas/PolicyTemplate'
    application/json-patch+json:
      schema:
        $ref: '#/components/schemas/PolicyTemplate'
  responses:
    '200':
      description: 'Patched Content Hosting Configuration'
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/PolicyTemplate'
    '404':
      description: 'Not Found'
  delete:
    operationId: destroyPolicyTemplate
    responses:
      '204':
        description: 'Destroyed Policy Template'
      '404':
        description: 'Not Found'
components:
  schemas:
    PolicyTemplate:
      type: object
      description: "A representation of a Policy Template resource."
      required:
        - policyTemplateId
        - state
        - stateReason
        - externalReference
      properties:
        policyTemplateId:
          readOnly: true
          allOf:
            - $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        state:
          readOnly: true
          anyOf:
            - type: string
              enum: [PENDING, INVALID, READY, SUSPENDED]
            - type: string
              description: >
                This string provides forward-compatibility with future
                extensions to the enumeration but is not used to encode
                content defined in the present version of this API.
        stateReason:
          readOnly: true
          allOf:
            - $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
        externalReference:
          type: string
        qoSSpecification:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/M1QoSSpecification'
        applicationSessionContext:
          type: object
          properties:
            sliceInfo:
              $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
            dnn:
              $ref: 'TS29571_CommonData.yaml#/components/schemas/Dnn'
        chargingSpecification:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ChargingSpecification'

```

C.3.9 M1_EdgeResourcesProvisioning API

```

openapi: 3.0.0
info:
  title: M1_EdgeResourcesProvisioning
  version: 2.1.2
  description: |
    5GMS AF M1 Edge Resources Provisioning API
    © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.

```

```

tags:
  - name: M1_EdgeResourcesProvisioning
    description: '5G Media Streaming: Provisioning (M1) APIs: Edge Resources Provisioning'
externalDocs:
  description: 'TS 26.512 V17.6.0; 5G Media Streaming (5GMS); Protocols'
  url: 'https://www.3gpp.org/ftp/Specs/archive/26_series/26.512/'
servers:
  - url: '{apiRoot}/3gpp-m1/v2'
    variables:
      apiRoot:
        default: https://example.com
        description: See 3GPP TS 29.512 clause 7.10.
paths:
  /provisioning-sessions/{provisioningSessionId}/edge-resources-configurations:
    parameters:
      - name: provisioningSessionId
        in: path
        required: true
        schema:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        description: 'The resource identifier of an existing Provisioning Session.'
    post:
      operationId: createEdgeResourcesConfiguration
      summary: 'Create an Edge Resources Configuration within the scope of the specified Provisioning Session'
      requestBody:
        description: 'A JSON representation of an Edge Resources Configuration'
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/EdgeResourcesConfiguration'
      responses:
        '201':
          description: 'Edge Resources Configuration Created'
          headers:
            Location:
              description: 'URL of the newly created Edge Resources Configuration.'
              required: true
              schema:
                $ref: 'TS26512_CommonData.yaml#/components/schemas/AbsoluteUrl'
  /provisioning-sessions/{provisioningSessionId}/edge-resources-configurations/{edgeResourcesConfigurationId}:
    parameters:
      - name: provisioningSessionId
        in: path
        required: true
        schema:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        description: 'The resource identifier of an existing Provisioning Session.'
      - name: edgeResourcesConfigurationId
        in: path
        required: true
        schema:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        description: 'The resource identifier of an existing Edge Resources Configuration.'
    get:
      operationId: retrieveEdgeResourcesConfiguration
      summary: 'Retrieve the Edge Resources Configuration of the specified Provisioning Session'
      responses:
        '200':
          description: 'Success'
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/EdgeResourcesConfiguration'
    put:
      operationId: updateEdgeResourcesConfiguration
      summary: 'Update an Edge Resources Configuration for the specified Provisioning Session'
      requestBody:
        description: 'A JSON representation of an Edge Resources Configuration'
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/EdgeResourcesConfiguration'
      responses:
        '204':

```

```

      description: 'Updated Edge Resources Configuration'
    '404':
      description: 'Not Found'
  patch:
    operationId: patchEdgeResourcesConfiguration
    summary: 'Patch the Edge Resources Configuration for the specified Provisioning Session'
    requestBody:
      description: 'A JSON representation of a Edge Resources Configuration'
      required: true
      content:
        application/merge-patch+json:
          schema:
            $ref: '#/components/schemas/EdgeResourcesConfiguration'
        application/json-patch+json:
          schema:
            $ref: '#/components/schemas/EdgeResourcesConfiguration'
    responses:
      '200':
        description: 'Patched Edge Resources Configuration'
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/EdgeResourcesConfiguration'
      '404':
        description: 'Not Found'
  delete:
    operationId: destroyEdgeResourcesConfiguration
    responses:
      '204':
        description: 'Destroyed Edge Resources Configuration'
      '404':
        description: 'Not Found'

components:
  schemas:
    EdgeResourcesConfiguration:
      type: object
      description: 'A representation of an Edge Resources Configuration resource.'
      required:
        - edgeResourcesConfigurationId
        - edgeManagementMode
        - easRequirements
      properties:
        edgeResourcesConfigurationId:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        edgeManagementMode:
          $ref: '#/components/schemas/EdgeManagementMode'
        eligibilityCriteria:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/EdgeProcessingEligibilityCriteria'
        easRequirements:
          $ref: '#/components/schemas/EASRequirements'
        easRelocationRequirements:
          $ref: '#/components/schemas/M1EASRelocationRequirements'

    M1EASRelocationRequirements:
      type: object
      description: 'Relocation requirements of an EAS.'
      required:
        - tolerance
      properties:
        tolerance:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/EASRelocationTolerance'
        maxInterruptionDuration:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/UIntegerRm'
        maxResponseTimeDifference:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/UIntegerRm'

    EASRequirements:
      type: object
      description: 'Requirements of an EAS.'
      properties:
        easProviderIds:
          type: array
          items:
            type: string
          minItems: 1
        easId:
          type: string

```

```

easType:
  type: string
easFeatures:
  type: array
  items:
    type: string
  minItems: 1
serviceKpi:
  $ref: 'TS29558_Eees_EASRegistration.yaml#/components/schemas/EASServiceKPI'
serviceArea:
  $ref: 'TS29558_Eecs_EESRegistration.yaml#/components/schemas/GeographicalServiceArea'
serviceAvailabilitySchedule:
  type: array
  items:
    $ref: 'TS29122_CpProvisioning.yaml#/components/schemas/ScheduledCommunicationTime'
  minItems: 1
serviceContinuityScenarios:
  type: array
  items:
    $ref: 'TS29558_Eecs_EESRegistration.yaml#/components/schemas/ACRScenario'
  minItems: 1
serviceContinuitySupport:
  type: array
  items:
    $ref: 'TS29558_Eecs_EESRegistration.yaml#/components/schemas/ACRScenario'
  minItems: 1

EdgeManagementMode:
  description: 'The management mode of an EAS.'
  anyOf:
    - type: string
      enum: [EM_AF_DRIVEN, EM_APP_DRIVEN]
    - type: string
      description: >
        This string provides forward-compatibility with future
        extensions to the enumeration but is not used to encode
        content defined in the present version of this API.

```

C.3.10 M1_EventDataProcessingProvisioning API

```

openapi: 3.0.0
info:
  title: M1_EventDataProcessingProvisioning
  version: 2.0.1
  description: |
    5GMS AF M1 Event Data Processing Provisioning API
    © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
tags:
  - name: M1_EventDataProcessingProvisioning
    description: '5G Media Streaming: Provisioning (M1) APIs: Event Data Processing Provisioning'
externalDocs:
  description: 'TS 26.512 V17.4.0; 5G Media Streaming (5GMS); Protocols'
  url: 'https://www.3gpp.org/ftp/Specs/archive/26_series/26.512/'
servers:
  - url: '{apiRoot}/3gpp-m1/v2'
    variables:
      apiRoot:
        default: https://example.com
        description: See 3GPP TS 29.512 clause 6.1.
paths:
  /provisioning-sessions/{provisioningSessionId}/event-data-processing-configurations:
    parameters:
      - name: provisioningSessionId
        in: path
        required: true
        schema:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        description: 'The resource identifier of an existing Provisioning Session.'
    post:
      operationId: createEventDataProcessingConfiguration
      summary: 'Supply an Event Data Processing Configuration for the specified Provisioning Session'
      requestBody:
        description: 'A JSON representation of a Event Data Processing Configuration'

```

```

    required: true
    content:
      application/json:
        schema:
          $ref: '#/components/schemas/EventDataProcessingConfiguration'
  responses:
    '201':
      description: 'Event Data Processing Configuration Created'
      headers:
        Location:
          description: 'URL of the newly created Event Data Processing Configuration (same as
request URL).'
          required: true
          schema:
            $ref: 'TS26512_CommonData.yaml#/components/schemas/AbsoluteUrl'
/provisioning-sessions/{provisioningSessionId}/event-data-processing-
configurations/{eventDataProcessingConfigurationId}:
  parameters:
    - name: provisioningSessionId
      in: path
      required: true
      schema:
        $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
      description: 'The resource identifier of an existing Provisioning Session.'
    - name: eventDataProcessingConfigurationId
      in: path
      required: true
      schema:
        $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
      description: 'The resource identifier of an Event Data Processing Configuration.'
  get:
    operationId: retrieveEventDataProcessingConfiguration
    summary: 'Retrieve the specified Event Data Processing Configuration of the specified
Provisioning Session'
    responses:
      '200':
        description: 'Success'
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/EventDataProcessingConfiguration'
  put:
    operationId: updateEventDataProcessingConfiguration
    summary: 'Update the specified Event Data Processing Configuration for the specified
Provisioning Session'
    requestBody:
      description: 'A JSON representation of a Event Data Processing Configuration'
      required: true
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/EventDataProcessingConfiguration'
    responses:
      '204':
        description: 'Updated Event Data Processing Configuration'
      '404':
        description: 'Not Found'
  patch:
    operationId: patchEventDataProcessingConfiguration
    summary: 'Patch the specified Event Data Processing Configuration for the specified
Provisioning Session'
    requestBody:
      description: 'A JSON representation of a Event Data Processing Configuration'
      required: true
      content:
        application/merge-patch+json:
          schema:
            $ref: '#/components/schemas/EventDataProcessingConfiguration'
        application/json-patch+json:
          schema:
            $ref: '#/components/schemas/EventDataProcessingConfiguration'
    responses:
      '200':
        description: 'Patched Event Data Processing Configuration'
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/EventDataProcessingConfiguration'

```



```

      '404':
        description: 'Not Found'
    delete:
      operationId: destroyEventDataProcessingConfiguration
      summary: 'Destroy the specified Event Data Processing Configuration of the specified Provisioning Session'
      responses:
        '204':
          description: 'Destroyed Event Data Processing Configuration'
        '404':
          description: 'Not Found'
  components:
    schemas:
      EventDataProcessingConfiguration:
        description: 'A representation of an Event Data Processing Configuration resource.'
        type: object
        required:
          - eventDataProcessingConfigurationId
          - eventId
          - dataAccessProfiles
        properties:
          eventDataProcessingConfigurationId:
            $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
          eventId:
            $ref: 'TS29517_Naf_EventExposure.yaml#/components/schemas/AfEvent'
          authorizationUrl:
            $ref: 'TS26512_CommonData.yaml#/components/schemas/Url'
          dataAccessProfiles:
            type: array
            items:
              $ref: 'TS26532_Ndcaf_DataReportingProvisioning.yaml#/components/schemas/DataAccessProfile'

```

C.4 OpenAPI representation of the M5 APIs

C.4.1 M5_ServiceAccessInformation API

```

openapi: 3.0.0
info:
  title: M5_ServiceAccessInformation
  version: 2.5.0
  description: |
    5GMS AF M5 Service Access Information API
    © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
tags:
  - name: M5_ServiceAccessInformation
    description: '5G Media Streaming: Media Session Handling (M5) APIs: Service Access Information'
externalDocs:
  description: 'TS 26.512 V17.9.0; 5G Media Streaming (5GMS); Protocols'
  url: 'https://www.3gpp.org/ftp/Specs/archive/26_series/26.512/'
servers:
  - url: '{apiRoot}/3gpp-m5/v2'
    variables:
      apiRoot:
        default: https://example.com
        description: See 3GPP TS 29.512 clause 6.1.
paths:
  /service-access-information/{provisioningSessionId}:
    parameters:
      - name: provisioningSessionId
        description: 'The resource identifier of an existing Provisioning Session.'
        in: path
        required: true
        schema:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
    get:
      operationId: retrieveServiceAccessInformation
      summary: 'Retrieve the Service Access Information resource'
      responses:
        '200':

```

```

        description: 'Success'
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/ServiceAccessInformationResource'
        '404':
          description: 'Not Found'
components:
  schemas:
    M5MediaEntryPoint:
      description: "A typed entry point for downlink or uplink media streaming."
      type: object
      required:
        - locator
        - contentType
      properties:
        locator:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/AbsoluteUrl'
        contentType:
          type: string
      profiles:
        type: array
        items:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        minItems: 1

    ServerAddresses:
      description: "A set of application endpoint addresses."
      type: array
      items:
        $ref: 'TS26512_CommonData.yaml#/components/schemas/AbsoluteUrl'
      minItems: 1

    ServiceAccessInformationResource:
      description: "A representation of a Service Access Information resource."
      type: object
      required:
        - provisioningSessionId
        - provisioningSessionType
      properties:
        provisioningSessionId:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        provisioningSessionType:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ProvisioningSessionType'
      streamingAccess:
        type: object
        properties:
          entryPoints:
            type: array
            items:
              $ref: '#/components/schemas/M5MediaEntryPoint'
          eMBMSServiceAnnouncementLocator:
            $ref: 'TS26512_CommonData.yaml#/components/schemas/AbsoluteUrl'
      clientConsumptionReportingConfiguration:
        type: object
        required:
          - serverAddresses
          - locationReporting
          - accessReporting
          - samplePercentage
        properties:
          reportingInterval:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
          serverAddresses:
            $ref: '#/components/schemas/ServerAddresses'
          locationReporting:
            type: boolean
          accessReporting:
            type: boolean
          samplePercentage:
            $ref: 'TS26512_CommonData.yaml#/components/schemas/Percentage'
      dynamicPolicyInvocationConfiguration:
        type: object
        required:
          - serverAddresses
          - policyTemplateBindings
          - sdfMethods
        properties:

```

```

serverAddresses:
  $ref: '#/components/schemas/ServerAddresses'
policyTemplateBindings:
  type: array
  minItems: 1
  items:
    type: object
    required:
      - externalReference
      - policyTemplateId
    properties:
      externalReference:
        type: string
      policyTemplateId:
        $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
sdfMethods:
  type: array
  items:
    $ref: 'TS26512_CommonData.yaml#/components/schemas/SdfMethod'
  minItems: 0
clientMetricsReportingConfigurations:
  type: array
  minItems: 1
  items:
    type: object
    required:
      - metricsReportingConfigurationId
      - serverAddresses
      - scheme
      - samplePercentage
      - urlFilters
      - samplingPeriod
      - metrics
    properties:
      metricsReportingConfigurationId:
        $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
      serverAddresses:
        $ref: '#/components/schemas/ServerAddresses'
      sliceScope:
        type: array
        items:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
        minItems: 1
      scheme:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
      dataNetworkName:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Dnn'
      reportingInterval:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
      samplePercentage:
        $ref: 'TS26512_CommonData.yaml#/components/schemas/Percentage'
      urlFilters:
        type: array
        items:
          type: string
          minItems: 0
      samplingPeriod:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
      metrics:
        type: array
        items:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
networkAssistanceConfiguration:
  type: object
  required:
    - serverAddresses
  properties:
    serverAddresses:
      $ref: '#/components/schemas/ServerAddresses'
clientEdgeResourcesConfiguration:
  type: object
  required:
    - easDiscoveryTemplate
  properties:
    eligibilityCriteria:
      $ref:
'TS26512_CommonData.yaml#/components/schemas/EdgeProcessingEligibilityCriteria'
    easDiscoveryTemplate:

```

```

    $ref: '#/components/schemas/EASDiscoveryTemplate'
  easRelocationRequirements:
    $ref: '#/components/schemas/M5EASRelocationRequirements'

M5EASRelocationRequirements:
  description: 'Relocation requirements of an EAS.'
  type: object
  required:
    - tolerance
  properties:
    tolerance:
      $ref: 'TS26512_CommonData.yaml#/components/schemas/EASRelocationTolerance'
    maxInterruptionDuration:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/UIntegerRm'

EASDiscoveryTemplate:
  description: 'A template for discovering an EAS instance .'
  type: object
  properties:
    easId:
      type: string
    easType:
      type: string
    easProviderIds:
      type: array
      items:
        type: string
      minItems: 1
    serviceFeatures:
      type: array
      items:
        type: string
      minItems: 1

```

C.4.2 M5_ConsumptionReporting API

```

openapi: 3.0.0
info:
  title: M5_ConsumptionReporting
  version: 2.2.0
  description: |
    5GMS AF M5 Consumption Reporting API
    © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
tags:
  - name: M5_ConsumptionReporting
    description: '5G Media Streaming: Media Session Handling (M5) APIs: Consumption Reporting'
externalDocs:
  description: 'TS 26.512 V17.7.0; 5G Media Streaming (5GMS); Protocols'
  url: 'https://www.3gpp.org/ftp/Specs/archive/26_series/26.512/'
servers:
  - url: '{apiRoot}/3gpp-m5/v2'
    variables:
      apiRoot:
        default: https://example.com
        description: See 3GPP TS 29.512 clause 6.1.
paths:
  /consumption-reporting/{provisioningSessionId}:
    parameters:
      - name: provisioningSessionId
        in: path
        required: true
        schema:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        description: 'See 3GPP TS 26.512 clause 11.3.2.'
    post:
      operationId: submitConsumptionReport
      summary: 'Submit a Consumption Report'
      requestBody:
        description: 'A Consumption Report'
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/ConsumptionReport'

```

```

responses:
  '204':
    description: 'Consumption Report Accepted'
  '400':
    description: 'Bad Request'
  '415':
    description: 'Unsupported Media Type'
components:
  schemas:
    ConsumptionReport:
      description: "A representation of a Consumption Report."
      type: object
      required:
        - mediaPlayerEntry
        - reportingClientId
        - consumptionReportingUnits
      properties:
        mediaPlayerEntry:
          type: string
        reportingClientId:
          type: string
        consumptionReportingUnits:
          type: array
          items:
            $ref: '#/components/schemas/ConsumptionReportingUnit'
    ConsumptionReportingUnit:
      description: "A Consumption Reporting Unit."
      type: object
      required:
        - mediaConsumed
        - startTime
        - duration
      properties:
        mediaConsumed:
          type: string
        clientEndpointAddress:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/EndpointAddress'
        serverEndpointAddress:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/EndpointAddress'
        startTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
        duration:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
        locations:
          type: array
          items:
            $ref: 'TS26512_CommonData.yaml#/components/schemas/TypedLocation'
      minItems: 1

```

C.4.3 M5_MetricsReporting API

```

openapi: 3.0.0
info:
  title: M5_MetricsReporting
  version: 2.0.0
  description: |
    5GMS AF M5 Metrics Reporting API
    © 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
tags:
  - name: M5_ConsumptionReporting
    description: '5G Media Streaming: Media Session Handling (M5) APIs: Metrics Reporting'
externalDocs:
  description: 'TS 26.512 V17.2.0; 5G Media Streaming (5GMS); Protocols'
  url: 'https://www.3gpp.org/ftp/Specs/archive/26_series/26.512/'
servers:
  - url: '{apiRoot}/3gpp-m5/v2'
    variables:
      apiRoot:
        default: https://example.com
        description: See 3GPP TS 29.512 clause 6.1.
paths:
  /metrics-reporting/{provisioningSessionId}/{metricsReportingConfigurationId}:
    parameters:
      - name: provisioningSessionId

```

```

    in: path
    required: true
    schema:
      $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
    description: 'The resource identifier of an existing Provisioning Session.'
  - name: metricsReportingConfigurationId
    in: path
    required: true
    schema:
      $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
    description: 'The resource identifier of a Metrics Configuration in the specified Provisioning Session.'
  post:
    operationId: submitMetricsReport
    summary: 'Submit a Metrics Report'
    requestBody:
      description: 'A Metrics Report'
      required: true
      content:
        application/3gpdash-qoe-report+xml:
          schema:
            type: string
            format: xml
        application/*:
          schema:
            type: string
    responses:
      '204':
        description: 'Metrics Report Accepted'
      '400':
        description: 'Bad Request'
      '415':
        description: 'Unsupported Media Type'

```

C.4.4 M5_DynamicPolicies API

```

openapi: 3.0.0
info:
  title: M5_DynamicPolicies
  version: 2.0.2
  description: |
    5GMS AF M5 Dynamic Policy API
    © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
tags:
  - name: M5_DynamicPolicies
    description: '5G Media Streaming: Media Session Handling (M5) APIs: Dynamic Policies'
externalDocs:
  description: 'TS 26.512 V17.6.0; 5G Media Streaming (5GMS); Protocols'
  url: 'https://www.3gpp.org/ftp/Specs/archive/26_series/26.512/'
servers:
  - url: '{apiRoot}/3gpp-m5/v2'
    variables:
      apiRoot:
        default: https://example.com
        description: See 3GPP TS 29.512 clause 6.1.
paths:
  /dynamic-policies:
    post:
      operationId: createDynamicPolicy
      summary: 'Create (and optionally upload) a new Dynamic Policy resource'
      requestBody:
        description: 'An optional JSON representation of a Dynamic Policy resource'
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/DynamicPolicy'
      responses:
        '201':
          description: 'Created Dynamic Policy Resource'
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/DynamicPolicy'
      headers:

```

```

    Location:
      description: 'The URL of the newly created Dynamic Policy resource'
      required: true
      schema:
        $ref: 'TS26512_CommonData.yaml#/components/schemas/AbsoluteUrl'
  '400':
    description: 'Bad Request'
  '401':
    description: 'Unauthorized'
/dynamic-policies/{dynamicPolicyId}:
  parameters:
    - name: dynamicPolicyId
      description: 'The resource identifier of a Dynamic Policy resource'
      in: path
      required: true
      schema:
        $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
  get:
    operationId: retrieveDynamicPolicy
    summary: 'Retrieve an existing Dynamic Policy resource'
    responses:
      '200':
        description: 'Success'
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/DynamicPolicy'
      '400':
        description: 'Bad Request'
      '401':
        description: 'Unauthorized'
      '404':
        description: 'Not Found'
  put:
    operationId: updateDynamicPolicy
    summary: 'Update an existing Dynamic Policy resource'
    requestBody:
      description: 'A replacement JSON representation of a Dynamic Policy resource'
      required: true
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/DynamicPolicy'
    responses:
      '400':
        description: 'Bad Request'
      '401':
        description: 'Unauthorized'
      '404':
        description: 'Not found'
  patch:
    operationId: patchDynamicPolicy
    summary: 'Patch an existing Dynamic Policy resource'
    requestBody:
      description: 'A JSON patch to a Dynamic Policy resource'
      required: true
      content:
        application/merge-patch+json:
          schema:
            $ref: '#/components/schemas/DynamicPolicy'
        application/json-patch+json:
          schema:
            $ref: '#/components/schemas/DynamicPolicy'
    responses:
      '200':
        description: 'Patched Dynamic Policy'
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/DynamicPolicy'
      '204':
        description: 'Patched Dynamic Policy'
      '400':
        description: 'Bad Request'
      '401':
        description: 'Unauthorized'
      '404':

```

```

        description: 'Not found'
delete:
  operationId: destroyDynamicPolicy
  summary: 'Destroy an existing Dynamic Policy resource'
  responses:
    '204':
      description: 'Destroyed Dynamic Policy'
    '400':
      description: 'Bad Request'
    '401':
      description: 'Unauthorized'
    '404':
      description: 'Not Found'
components:
  schemas:
    DynamicPolicy:
      description: "A representation of a Dynamic Policy resource."
      type: object
      required:
        - dynamicPolicyId
        - policyTemplateId
        - serviceDataFlowDescriptions
        - provisioningSessionId
      properties:
        dynamicPolicyId:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        policyTemplateId:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        serviceDataFlowDescriptions:
          type: array
          items:
            $ref: 'TS26512_CommonData.yaml#/components/schemas/ServiceDataFlowDescription'
        mediaType:
          $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/MediaType'
        provisioningSessionId:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
        qosSpecification:
          $ref: 'TS26512_CommonData.yaml#/components/schemas/M5QoSSpecification'
        enforcementMethod:
          type: string
        enforcementBitRate:
          type: integer

```

C.4.5 M5_NetworkAssistance API

```

openapi: 3.0.0
info:
  title: M5_NetworkAssistance
  version: 2.1.0
  description: |
    5GMS AF M5 Network Assistance API
    © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
tags:
  - name: M5_NetworkAssistance
    description: '5G Media Streaming: Media Session Handling (M5) APIs: Network Assistance'
externalDocs:
  description: 'TS 26.512 V17.6.0; 5G Media Streaming (5GMS); Protocols'
  url: 'https://www.3gpp.org/ftp/Specs/archive/26_series/26.512/'
servers:
  - url: '{apiRoot}/3gpp-m5/v2'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in subclause 4.4.1 of 3GPP TS 29.501.
paths:
  /network-assistance/:
    post:
      operationId: createNetworkAssistanceSession
      summary: 'Create a new Network Assistance Session.'
      requestBody:
        description: 'The initial parameters for the Network Assistance Session resource'
        content:
          application/json:
            schema:

```



```

    $ref: '#/components/schemas/NetworkAssistanceSession'
  responses:
    '201':
      description: 'Created Network Assistance Session'
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/NetworkAssistanceSession'
      headers:
        Location:
          description: 'The URL of the newly created Network Assistance Session resource'
          required: true
          schema:
            $ref: 'TS26512_CommonData.yaml#/components/schemas/AbsoluteUrl'
    '400':
      description: 'Bad Request'
    '401':
      description: 'Unauthorized'

/network-assistance/{naSessionId}:
  parameters:
    - name: naSessionId
      description: 'The resource identifier of an existing Network Assistance Session resource'
      in: path
      required: true
      schema:
        $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
  get:
    operationId: retrieveNetworkAssistanceSession
    summary: 'Retrieve an existing Network Assistance Session resource'
    responses:
      '200':
        description: 'A JSON representation of a Network Assistance Session resource'
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/NetworkAssistanceSession'
      '400':
        description: 'Bad Request'
      '401':
        description: 'Unauthorized'
      '404':
        description: 'Not Found'
  put:
    operationId: updateNetworkAssistanceSession
    summary: 'Update an existing Network Assistance Session resource'
    requestBody:
      description: 'A replacement JSON representation of a Network Assistance Session resource'
      required: true
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/NetworkAssistanceSession'
    responses:
      '400':
        description: 'Bad Request'
      '401':
        description: 'Unauthorized'
      '404':
        description: 'Not found'
  patch:
    operationId: patchNetworkAssistanceSession
    summary: 'Patch an existing Network Assistance Session resource'
    requestBody:
      description: 'A JSON patch to a Network Assistance Session resource'
      required: true
      content:
        application/merge-patch+json:
          schema:
            $ref: '#/components/schemas/NetworkAssistanceSession'
        application/json-patch+json:
          schema:
            $ref: '#/components/schemas/NetworkAssistanceSession'
    responses:
      '200':
        description: 'Patched Network Assistance Session'
        content:
          application/json:

```

```

        schema:
          $ref: '#/components/schemas/NetworkAssistanceSession'
      '204':
        description: 'Patched Network Assistance Session'
      '400':
        description: 'Bad Request'
      '401':
        description: 'Unauthorized'
      '404':
        description: 'Not Found'
  delete:
    operationId: destroyNetworkAssistanceSession
    summary: 'Destroy an existing Network Assistance Session resource'
    responses:
      '204':
        description: 'Destroyed Network Assistance Session'
      '400':
        description: 'Bad Request'
      '401':
        description: 'Unauthorized'
      '404':
        description: 'Not Found'

/network-assistance/{naSessionId}/recommendation:
  get:
    operationId: requestBitRateRecommendation
    summary: 'Obtain a bit rate recommendation for the next recommendation window'
    parameters:
      - name: naSessionId
        description: 'The resource identifier of an existing Network Assistance Session resource'

        in: path
        required: true
        schema:
          type: string
    responses:
      '200':
        description: 'Success'
        content:
          application/json:
            schema:
              $ref: 'TS26512_CommonData.yaml#/components/schemas/M5QoSSpecification'
      '400':
        description: 'Bad Request'
      '401':
        description: 'Unauthorized'
      '404':
        description: 'Not Found'

/network-assistance/{naSessionId}/boost-request:
  post:
    operationId: requestDeliveryBoost
    summary: 'Request a delivery boost'
    parameters:
      - name: naSessionId
        description: 'The resource identifier of an existing Network Assistance Session resource'

        in: path
        required: true
        schema:
          type: string
    responses:
      '200':
        description: 'Delivery Boost Request Processed'
        content:
          application/json:
            schema:
              $ref: 'TS26512_CommonData.yaml#/components/schemas/OperationSuccessResponse'
      '400':
        description: 'Bad Request'
      '401':
        description: 'Unauthorized'
      '404':
        description: 'Not Found'

components:
  schemas:
    NetworkAssistanceSession:
      description: 'A representation of a Network Assistance Session resource.'
      type: object

```

```

required:
  - naSessionId
  - provisioningSessionId
  - serviceDataFlowDescriptions
properties:
  naSessionId:
    $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
  provisioningSessionId:
    $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
  serviceDataFlowDescriptions:
    type: array
    items:
      $ref: 'TS26512_CommonData.yaml#/components/schemas/ServiceDataFlowDescription'
    minItems: 1
  mediaType:
    $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/MediaType'
  policyTemplateId:
    $ref: 'TS26512_CommonData.yaml#/components/schemas/ResourceId'
  requestedQoS:
    $ref: 'TS26512_CommonData.yaml#/components/schemas/M5QoSSpecification'
  recommendedQoS:
    $ref: 'TS26512_CommonData.yaml#/components/schemas/M5QoSSpecification'
  notificationURL:
    $ref: 'TS26512_CommonData.yaml#/components/schemas/AbsoluteUrl'

```

C.5 OpenAPI representation of data reporting records

C.5.1 R4 data reporting records

For the purpose of referencing entities defined in this clause, it shall be assumed that the OpenAPI definitions below are contained in a physical file named "TS26512_R4_DataReporting.yaml".

```

openapi: 3.0.0
info:
  title: 5GMS Data Reporting data types
  version: 1.0.1
  description: |
    5GMS Data Reporting data types
    © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
tags:
  - name: 5GMS Data Reporting data types
    description: '5G Media Streaming: Data Reporting data types'
externalDocs:
  description: 'TS 26.512 V17.4.0; 5G Media Streaming (5GMS); Protocols'
  url: 'https://www.3gpp.org/ftp/Specs/archive/26_series/26.512/'
paths: {}
components:
  schemas:
    MediaStreamingAccessRecord:
      allOf:
        - $ref: 'TS26532_Ndcaf_DataReporting.yaml#/components/schemas/BaseRecord'
        - type: object
          required:
            - mediaStreamHandlerEndpointAddress
            - applicationServerEndpointAddress
            - requestMessage
            - responseMessage
            - processingLatency
          properties:
            mediaStreamHandlerEndpointAddress:
              $ref: 'TS26512_CommonData.yaml#/components/schemas/EndpointAddress'
            applicationServerEndpointAddress:
              $ref: 'TS26512_CommonData.yaml#/components/schemas/EndpointAddress'
            sessionIdentifier:
              type: string
            requestMessage:
              type: object

```

```
required:
  - method
  - url
  - protocolVersion
  - size
  - bodySize
properties:
  method:
    type: string
  url:
    $ref: 'TS26512_CommonData.yaml#/components/schemas/AbsoluteUrl'
  protocolVersion:
    type: string
  range:
    type: string
  size:
    $ref: 'TS29571_CommonData.yaml#/components/schemas/UInteger'
  bodySize:
    $ref: 'TS29571_CommonData.yaml#/components/schemas/UInteger'
  contentType:
    type: string
  userAgent:
    type: string
  userIdentity:
    type: string
  referer:
    $ref: 'TS26512_CommonData.yaml#/components/schemas/AbsoluteUrl'
cacheStatus:
  $ref: 'TS26512_CommonData.yaml#/components/schemas/CacheStatus'
responseMessage:
  type: object
  required:
    - responseCode
    - size
    - bodySize
  properties:
    responseCode:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/UInteger'
    size:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/UInteger'
    bodySize:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/UInteger'
    contentType:
      type: string
processingLatency:
  $ref: 'TS29571_CommonData.yaml#/components/schemas/Float'
connectionMetrics:
  type: object
  required:
    - meanNetworkRoundTripTime
    - networkRoundTripTimeVariation
    - congestionWindowSize
  properties:
    meanNetworkRoundTripTime:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Float'
    networkRoundTripTimeVariation:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Float'
    congestionWindowSize:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/UInteger'
```

Annex D (informative): 5GMS AF API index

Table D-1: Index of Provisioning (M1) APIs

HTTP request path element hierarchy	Description	Allowed HTTP methods					Resource structure definition clause	OpenAPI definition clause
		Create	Retrieve	Update	Destroy	Non-RESTful operation		
provisioning-sessions	Provisioning Sessions collection	POST					7.2.2	C.3.1
<i>{provisioningSessionId}</i>	Provisioning Session resource		GET		DELETE			
certificates	Server Certificates collection	POST					7.3.2	C.3.2
<i>{certificateId}</i>	Server Certificate resource		GET	PUT	DELETE			
content-preparation-templates	Content Preparation Templates collection	POST					7.4.2	C.3.3
<i>{contentPreparationTemplateId}</i>	Content Preparation Template resource		GET	PUT, PATCH	DELETE			
content-protocols-discovery	Content Protocols resource		GET				7.5.2	C.3.4
content-hosting-configuration	Content Hosting Configuration resource	POST	GET	PUT, PATCH	DELETE		7.6.2	C.3.5
purge	Content Hosting cache purge operation					POST		
consumption-reporting-configuration	Consumption Reporting Configuration resource	POST	GET	PUT, PATCH	DELETE		7.7.2	C.3.6
metrics-reporting-configuration	Metrics Reporting Configuration collection	POST					7.8.2	C.3.7
<i>{metricsReportingConfigurationId}</i>	Metrics Reporting Configuration resource		GET	PUT, PATCH	DELETE			
policy-templates	Policy Templates collection	POST					7.9.2	C.3.8
<i>{policyTemplateId}</i>	Policy Template resource		GET	PUT, PATCH	DELETE			
edge-resources-configurations	Edge Resources Configurations collection	POST					7.10.2	C.3.9

<i>{edgeResourcesConfigurationId}</i>	Edge Resources Configuration resource		GET	PUT, PATCH	DELETE			
event-data-processing-configurations	Event Data Processing Configuration collection	POST					7.11.2	C.3.10
<i>{eventDataProcessingConfigurationId}</i>	Event Data Processing Configuration resource		GET	PUT, PATCH	DELETE			

Table D-2: Index of Media Session Handling (M5) APIs

HTTP request path element hierarchy	Description	Allowed HTTP methods					Resource structure definition clause	OpenAPI definition clause
		Create	Retrieve	Update	Destroy	Non-RESTful operation		
service-access-information	Service Access Information collection						11.2.2	C.4.1
<i>{provisioningSessionId}</i>	Service Access Information resource		GET					
consumption-reporting	Consumption Reporting collection						11.3.2	C.4.2
<i>{provisioningSessionId}</i>	Consumption Reporting operation					POST		
metrics-reporting	Metrics Reporting collection						11.4.2	C.4.3
<i>{provisioningSessionId}</i>	Metrics Reporting Configurations collection							
<i>{metricsReportingConfigurationId}</i>	Metrics Reporting operation					POST		
dynamic-policies	Dynamic Policies collection	POST					11.5.2	C.4.4
<i>{dynamicPolicyId}</i>	Dynamic Policy resource		GET	PUT, PATCH	DELETE			
network-assistance	Network Assistance Sessions collection	POST					11.6.2	C.4.5
<i>{naSessionId}</i>	Network Assistance Session resource		GET	PUT, PATCH	DELETE			
recommendation	Bit rate recommendation request operation					GET		
boostRequest	Delivery boost request operation					POST		

Annex E (normative): Controlled vocabularies of 5G Media Streaming UE data parameters

E.1 General

The set of parameters used to provision processing and exposure of UE data is defined for each exposed Event by a controlled vocabulary with a unique name space identifier string in the form of a URN. Each parameter is specified as a term identifier string that is unique within the scope of its parent name space.

In the context of the present document:

- The values signalled in *MetricsReportingConfiguraton.metrics* (see clause 7.8.3.1) and *ServiceAccessInformation.clientMetricsReportingConfigurations[].metrics* (see clause 11.2.3.1) shall be fully-qualified URIs formed from one of the name space identifiers specified in clause E.2 concatenated with a single hash character ('#') concatenated with the appropriate term identifier.
- The values signalled in *DataAccessProfile.parameters* (see clause 6.3.2.3 of TS 26.532 [47]) shall be fully-qualified URIs formed from the name space identifier specified in the following clauses concatenated with a single hash character ('#') concatenated with the appropriate term identifier.

E.2 Controlled vocabularies of DASH QoE metrics reporting parameters

E.2.1 Reporting parameters for 3GP-DASH metrics

The name space identifier for the controlled vocabulary of DASH QoE metrics is:

urn:3GPP:ns:PSS:DASH:QM10

The term identifiers in this controlled vocabulary shall be the set of key names defined in clause 10.2 of TS 26.247 [4], using a single forward slash character ('/') as the hierarchical separator in the resulting path specifier. In the case of metrics lists, the *Entry* object shall be omitted from the term identifier path.

EXAMPLE 1: *urn:3GPP:ns:PSS:DASH:QM10#AvgThroughput/numbytes*

To select all reportable metrics below a common branch of the metrics hierarchy the relevant terminal path element(s) are pruned from the term identifier.

EXAMPLE 2: *urn:3GPP:ns:PSS:DASH:QM10#AvgThroughput*

E.2.2 Reporting parameters for VR metrics

The name space identifier for the controlled vocabulary of VR metrics is:

urn:3gpp:metadata:2020:VR:metrics

The term identifiers in this controlled vocabulary shall be the set of key names defined in clause 9.3 of TS 26.118 [42], using a single forward slash character ('/') as the hierarchical separator in the resulting path specifier. In the case of metrics lists, the *Entry* object shall be omitted from the term identifier path.

EXAMPLE 1: *urn:3gpp:metadata:2020:VR:metrics#CompQualLatency/Latency*

To select all reportable metrics below a common branch of the metrics hierarchy the relevant terminal path element(s) are pruned from the term identifier.

EXAMPLE 2: *urn:3gpp:metadata:2020:VR:metrics#CompQualLatency*

E.3 Controlled vocabulary of 5GMS consumption reporting parameters

The name space identifier for the controlled vocabulary of 5GMS consumption reporting parameters is:

urn:3gpp:5gms:event-exposure:consumption-reporting

The term identifiers in this controlled vocabulary are specified in table E.3-1 below.

EXAMPLE: *urn:3gpp:5gms:event-exposure:consumption-reporting#locations*

Table E.3-1: Controlled vocabulary of 5GMS consumption reporting parameters

Term identifier	Description
<i>start-time</i>	The date and time of the consumption reporting unit.
<i>duration</i>	The duration of the consumption reporting unit.
<i>media-player-entry</i>	The entry pointer for the media streaming session.
<i>reporting-client-identifier</i>	Identifier for the reporting client that consumed the media.
<i>media-consumed</i>	Identifies the media consumed within the context of the media player entry.
<i>locations</i>	The UE location(s) where the media was consumed. (Only available to trusted event consumer.)

E.4 Controlled vocabulary of 5GMS Network Assistance reporting parameters

The name space identifier for the controlled vocabulary of 5GMS Network Assistance parameters is:

urn:3gpp:5gms:event-exposure:network-assistance

The term identifiers in this controlled vocabulary are specified in table E.4-1 below.

EXAMPLE: *urn:3gpp:5gms:event-exposure:network-assistance#requested-qos*

Table E.4-1: Controlled vocabulary of 5GMS Network Assistance parameters

Term identifier	Description
<i>timestamp</i>	The date and time of the Network Assistance invocation by the Media Session Handler.
<i>service-data-flow-information</i>	Identification of the media streaming application flow for which Network Assistance was requested.
<i>policy-template-identifier</i>	The policy template in force for the media streaming session.
<i>requested-qos</i>	The network Quality of Service requested by the media streamer.
<i>recommended-qos</i>	The network Quality of Service recommended by the 5GMS AF.

E.5 Controlled vocabulary of 5GMS Dynamic Policy reporting parameters

The name space identifier for the controlled vocabulary of 5GMS Dynamic Policy parameters is

urn:3gpp:5gms:event-exposure:dynamic-policy

The term identifiers in this controlled vocabulary are specified in table E.5-1 below.

EXAMPLE: `urn:3gpp:5gms:event-exposure:dynamic-policy#enforcement-bit-rate`

Table E.5-1: Controlled vocabulary of 5GMS Dynamic Policy parameters

Term identifier	Description
<i>timestamp</i>	The date and time of the dynamic policy invocation by the Media Session Handler.
<i>policy-template-identifier</i>	The policy template instantiated for the media streaming session.
<i>service-data-flow-descriptions</i>	The set of media streaming application flows managed by the Dynamic Policy.
<i>qos-specification</i>	The network Quality of Service described by the policy template currently in force.
<i>enforcement-method</i>	The Policy Enforcement Method set by the 5GMS AF.
<i>enforcement-bit-rate</i>	The bit rate currently being enforced by this Dynamic Policy.

E.6 Controlled vocabulary of 5GMS media access activity parameters

The name space identifier for the controlled vocabulary of 5GMS media access activity is:

`urn:3gpp:5gms:event-exposure:access-activity`

The term identifiers in this controlled vocabulary are specified in table E.6-1 below.

EXAMPLE: `urn:3gpp:5gms:event-exposure:access-activity#request-message/url`

Table E.6-1: Controlled vocabulary of 5GMS media access activity parameters

Term identifier	Description
<i>timestamp</i>	The date and time of the media access.
<i>media-stream-handler-endpoint-address</i>	The endpoint address of the Media Stream Handler accessing the 5GMS AS.
<i>application-server-endpoint-address</i>	The service endpoint on the 5GMS AS to which the Media Stream Handler is connected.
<i>session-identifier</i>	An opaque identifier for the HTTP session on which the Media Stream Handler request was made.
<i>request-message</i>	All term identifiers below with prefix <i>request-message</i> .
<i>request-message/method</i>	The request method.
<i>request-message/url</i>	The request URL.
<i>request-message/protocol-version</i>	The HTTP protocol version, e.g. "HTTP/1.1".
<i>request-message/range</i>	The value of the <i>Range</i> request header.
<i>request-message/size</i>	The total number of bytes in the request message.
<i>request-message/body-size</i>	The number of bytes supplied by the Media Stream Handler in the HTTP request body.
<i>request-message/content-type</i>	The MIME content type of the request message, if any.
<i>request-message/user-agent</i>	A string describing the requesting Media Stream Handler from the <i>User-Agent</i> request header.
<i>request-message/user-identity</i>	A string identifying the user that made the access.
<i>request-message/referer</i>	The URL that the Media Player reports being referred from in the <i>Referer</i> request header.
<i>cache-status</i>	An indication of whether the 5GMS AS served the response object corresponding from cache.
<i>response-message</i>	All term identifiers below with prefix <i>response-message</i> .
<i>response-message/response-code</i>	The HTTP response code.
<i>response-message/size</i>	The total number of bytes in the response message.
<i>response-message/body-size</i>	The number of bytes in the HTTP response message body.
<i>response-message/content-type</i>	The MIME content type of response message.
<i>processing-latency</i>	The time, expressed in milliseconds, taken by the 5GMS AS to respond to the Media Stream Handler request.

Term identifier	Description
<i>connection-metrics</i>	All term identifiers below with prefix <i>connection-metrics</i> .
<i>connection-metrics/mean-rtt</i>	Mean network round-trip time for the HTTP session, expressed in milliseconds.
<i>connection-metrics/rtt-variation</i>	The variation in mean network round-trip time, expressed in milliseconds.
<i>connection-metrics/congestion-window-size</i>	The current size (in bytes) of the congestion window for the transport connection underlying the HTTP session.

Annex F (Informative): 5GMS AS Certificate provisioning and discovery

F.1 General

This annex describes 5GMS AS discovery by the 5GMS Client, including provisioning aspects that leverage the Domain Name System (DNS).

F.2 5GMS AS discovery and media streaming access with a Server Certificate created by the 5GMS System

Figure F.2-1 illustrates the initial provisioning needed to allow discovery of a 5GMS AS by the 5GMS Client as well as the eventual 5GMS AS discovery sequence using the Domain Name System (DNS). Specific focus here is on the provisioning and usage of TLS Certificates. The desired outcome is that the 5GMS Client is satisfied that it has established a TLS connection with an authorized 5GMS AS instance.

Here, the *Server Certificate Create* procedure (see clause 4.3.6.2) is used to request that the 5GMS AF creates the server certificate resource. In this case, the certificate's Common Name (CN) is assigned in a domain under the control of the 5GMS System operator (i.e., the 5GMS System operator is the legitimate owner of the domain name). The 5GMS System operator may use a third-party DNS service to host the domain in question.

For example, the 5GMS System operator uses the full *canonicalDomainName* value *<canonicalAsHostname>.<5GMS_Operator>.net* as the Common Name in the Server Certificate. The 5GMS AF embeds this host name in the distribution base URL it returns to the 5GMS Application Provider.

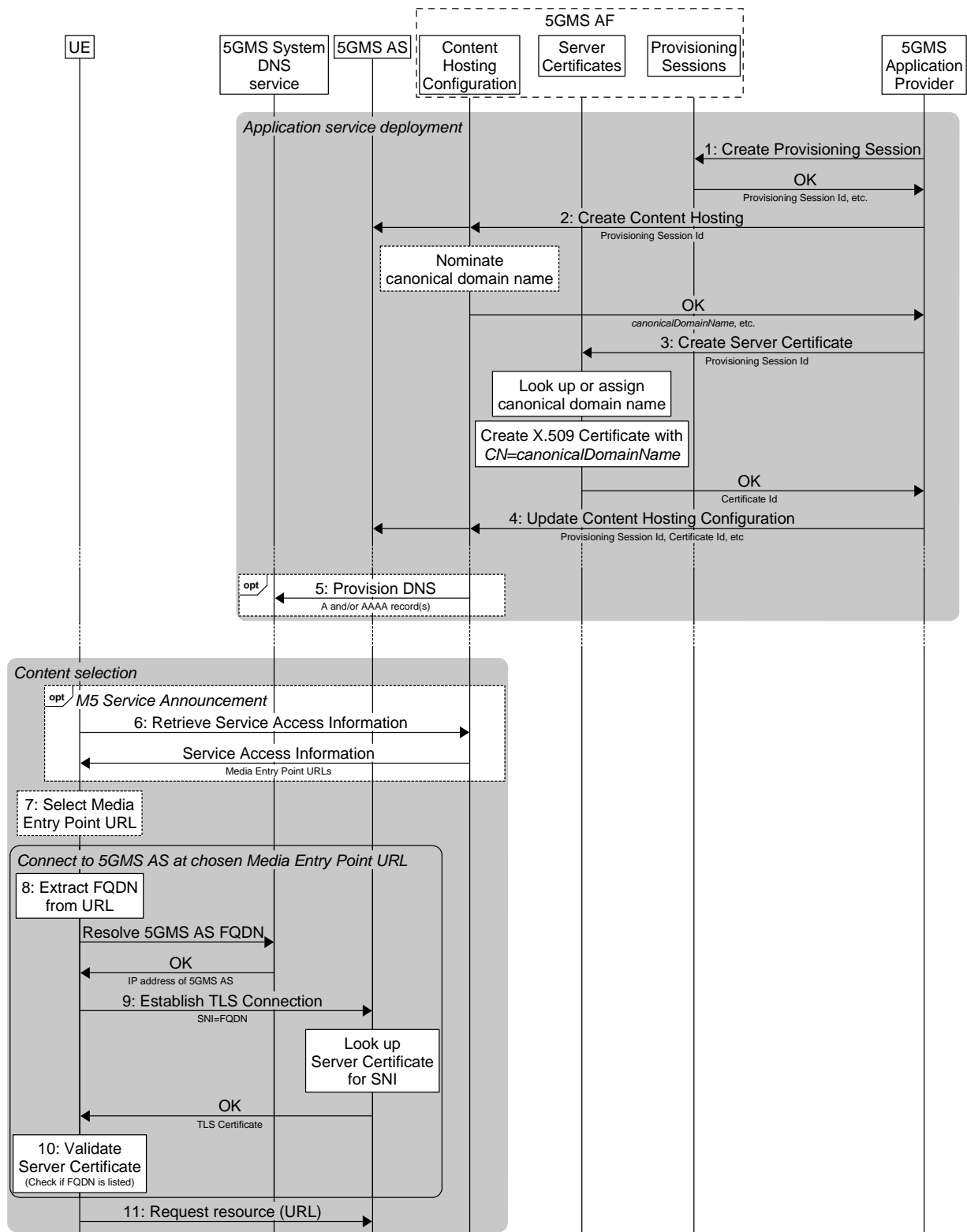
Table F.2-1: Example Content Hosting Configuration corresponding to Create Server Certificate procedure

Content Hosting Configuration property	Example value
<i>distributionConfigurations[n]</i>	
<i>canonicalDomainName</i>	<i><canonicalAsHostname>.<5GMS_Operator>.net</i>
<i>domainNameAlias</i>	Not present.
<i>baseURL</i>	<i>https://<canonicalAsHostname>.<5GMS_Operator>.net/<af-nominated-base-path></i>
<i>certificateId</i>	Pointing to Server Certificate resource with: <ul style="list-style-type: none"> - <i>CN = <canonicalAsHostname>.<5GMS_Operator>.net</i> - <i>subjectAltName[0] = <canonicalAsHostname>.<5GMS_Operator>.net</i>

The 5GMS System operator may instead use the wildcarded domain name **.<5GMS_Operator>.net* as the Common Name of the Server Certificate, in which case the 5GMS AF assigns a canonical host name *<canonicalAsHostname>* for the 5GMS AS in this domain and embeds this in the distribution base URL it returns to the 5GMS Application Provider.

In both cases, the Media Entry Point URL advertised via reference point M5 or M8 (used by the Media Player to access the content in the 5GMS AS at reference point M4) is then:

https://<canonicalAsHostname>.<5GMS_Operator>.net/<af-nominated-base-path>/<relativePath>



<https://gitlab.com/msc-generator/v8.4>

Figure F.2-1: 5GMS AS discovery using DNS using 5GMS System created server certificates

Prerequisites:

- A 5GMS-Aware Application is installed on the UE. This includes a list of API endpoint addresses for interacting with the 5GMS AF at reference point M5.

At application service deployment time:

1. The 5GMS Application Provider creates a Provisioning Session using the procedure specified in clause 4.3.2.2. The 5GMS AF provides the Provisioning Session Id in its response to the 5GMS Application Provider.
2. The 5GMS Application Provider creates a Content Hosting Configuration using the procedure specified in clause 4.3.3.2. If it has not already done so, the 5GMS AF assigns a canonical domain name for the 5GMS AS and includes this in its response to the 5GMS Application Provider (*canonicalDomainName*).
3. The 5GMS Application Provider requests that the 5GMS AF creates a Server Certificate for this Provisioning Session using the procedure specified in clause 4.3.6.2. If it has not already done so, the 5GMS AF assigns a canonical domain name for the 5GMS AS and this is used as the Common Name and the first (and only) Subject Alternative Name of the generated server certificate. The CertificateId is provided to the 5GMS Application Provider upon success.

NOTE: The order of step 2 and step 3 may be reversed, in which case step 4 is not needed and the 5GMS AS is updated as a consequence of step 2.

4. The 5GMS Application Provider updates the Content Hosting Configuration using the procedure specified in clause 4.3.3.4, adding the Certificate Identifier of the newly created Server Certificate resource (i.e., modifying the value of *distributionConfigurations[].certificateId*).

As a consequence, the 5GMS AF provisions the 5GMS AS with relevant information from the Provisioning Session, including the Server Certificate and Content Hosting Configuration.

- 5: If it has not already done so, the 5GMS AF provisions A and/or AAAA records in the DNS service mapping the canonical domain name of the 5GMS AS instance to its assigned IP address(es).

NOTE: The DNS service may be provided by a third-party service provider under the direction of the 5GMS System operator.

When content is selected in the 5GMS-Aware Application:

6. When Service Access Information retrieval at reference point M5 is used (see clause 4.7.2.3), the 5GMS Client in the UE retrieves the Service Access Information. This may include media entry point URLs within the *streamAccess.entryPoints* array. Otherwise, the 5GMS-Aware Application obtains this information via reference point M8.
7. The 5GMS Client in the UE selects one of the offered Media Entry Point URLs corresponding to the its media stream handling capabilities.
8. The 5GMS Client extracts the Fully-Qualified Domain Name (FQDN) from the chosen media entry point URL and uses the DNS service to resolve its IP address.
9. When establishing the TLS connection to the 5GMS AS at reference point M4, the Media Stream Handler in the UE cites the FQDN of the media entry point URL in the Server Name Indication (SNI) field of the TLS Client Hello message. The 5GMS AS uses the value of the SNI field to look up the corresponding Server Certificate and returns it to the Media Stream Handler in its Server Hello response. If the Server Certificate was provisioned with a wildcard Common Name, appropriate matching rules are followed by the 5GMS AS to identify the correct Server Certificate to present to the Media Stream Handler.
10. The 5GMS Client validates the Server Certificate, including whether the value of the Common Name (or one of its Subject Alternative Names) matches the FQDN of the chosen Media Entry Point URL.

When all server certificate validation steps are successfully passed, the following steps are executed:

11. The 5GMS Client requests the resource identified by the Media Entry Point over the TLS connection established with the 5GMS AS at reference point M4.

F.3 5GMS AS discovery and service access with a Server Certificate owned by the 5GMS Application Provider

Figure F.3-1 illustrates the initial provisioning needed to allow discovery of a 5GMS AS by the 5GMS Client as well as the eventual 5GMS AS discovery sequence using the Domain Name System (DNS). Specific focus here is on the provisioning and usage of TLS Certificates. The desired outcome is that the 5GMS Client is satisfied that it has established a TLS connection with an authorized 5GMS AS instance.

Here, the *Reserve Server Certificate* (see clause 4.3.6.3) and *Upload Server Certificate* (see clause 4.3.6.5) procedures are used for creating the Server Certificate resource and for subsequently providing it to the 5GMS AF. In this case, the certificate's Common Name (CN) is assigned in a domain under the control of the 5GMS Application Provider (i.e., Application Provider is the legitimate owner of the domain name). The 5GMS Application Provider may use the 5GMS System operator or any third-party DNS service to host the domain in question.

For example, the 5GMS Application Provider wishes to use the alias `<aliasHostname>.<AppProvider>.com` to access content through the 5GMS AS and it includes its chosen host name as a parameter to the *Reserve Server Certificate* operation. In response, the 5GMS AF generates a Certificate Signing Request (CSR) which it returns to the 5GMS Application Provider. The 5GMS AF assigns a canonical host name for the 5GMS AS in a domain under its control. The 5GMS AF embeds the Fully-Qualified Domain Name of the alias in the distribution base URL of the Content Hosting Configuration it returns to the 5GMS Application Provider.

Table F.3-1: Example Content Hosting Configuration corresponding to Reserve/Upload Server Certificate procedure

Content Hosting Configuration property	Example value
<i>distributionConfigurations[n]</i>	
<i>canonicalDomainName</i>	<code><canonicalAsHostname>.<5GMS_Operator>.net</code>
<i>domainNameAlias</i>	<code><aliasHostname>.<AppProvider>.com</code>
<i>baseURL</i>	<code>https://<aliasHostname>.<AppProvider>.com/<af-nominated-base-path></code>
<i>certificateId</i>	Pointing to Server Certificate resource with: <ul style="list-style-type: none"> - <i>CN</i> = <code><aliasHostname>.<AppProvider>.com</code> - <i>subjectAltName[0]</i> = <code><aliasHostname>.<AppProvider>.com</code> - <i>subjectAltName[1]</i> = ...

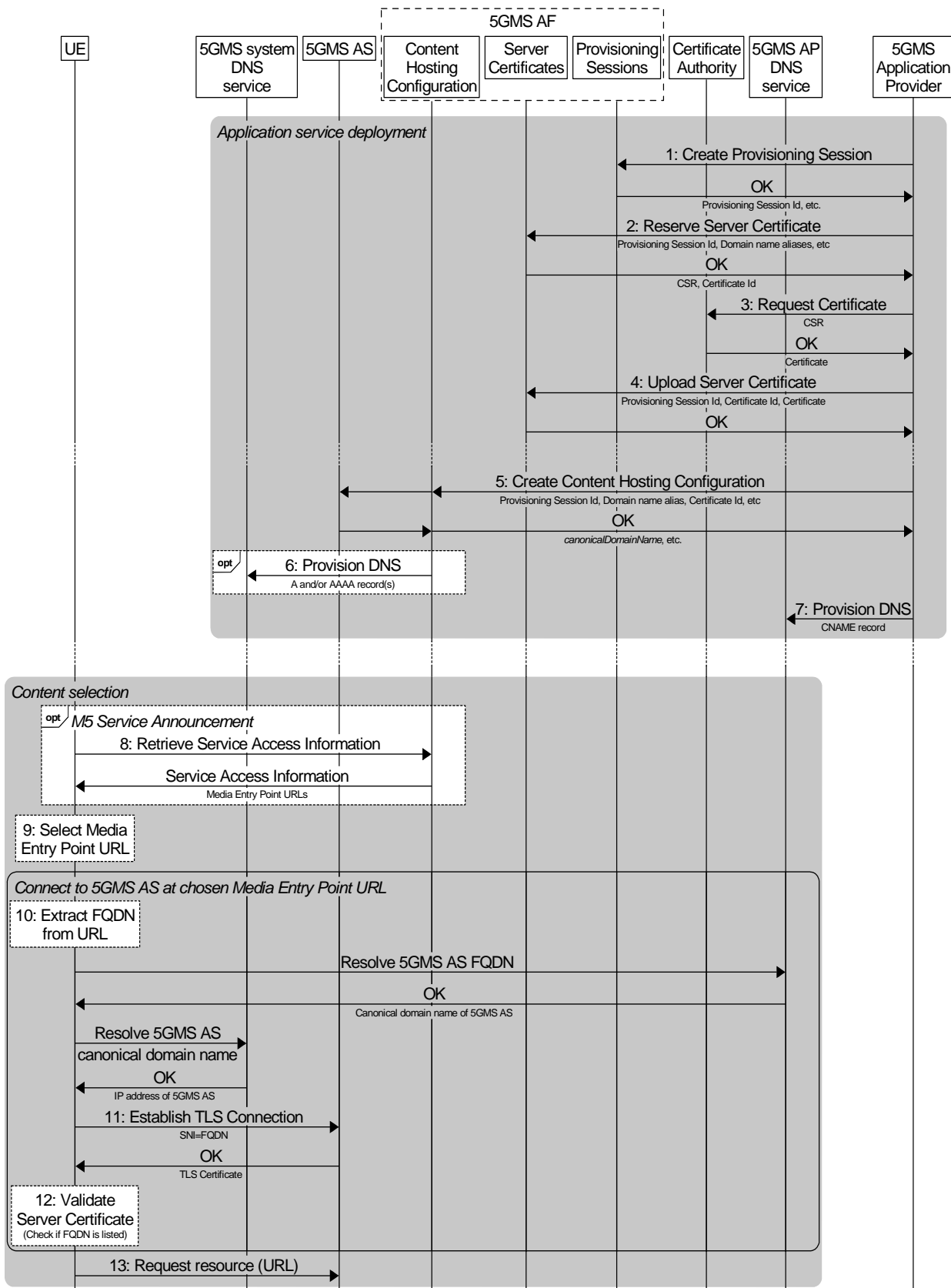
The 5GMS Application Provider additionally configures the 5GMS AF-nominated *canonicalDomainName* as a *CNAME* record for its chosen 5GMS AS domain name alias in its preferred DNS service.

Listing F.3-1: Example DNS CNAME record to support distribution configuration in table F.3-1

```
<aliasHostname>.<AppProvider>.com. CNAME <canonicalAsHostname>.<5GMS_Operator>.net
```

The Media Entry Point URL advertised via reference point M5 or M8 (used by the Media Player to access the content `<relativePath>` at reference point M4) is then:

```
https://<aliasHostname>.<AppProvider>.com/<af-nominated-base-path>/<relativePath>
```



<https://gitlab.com/mso-generator/v8.4>

Figure F.3-1: 5GMS AS discovery using DNS using uploaded Server Certificates

Prerequisites:

- A 5GMS-Aware Application is installed on the UE. This includes a list of API endpoint addresses for interacting with the 5GMS AF at reference point M5.

At application service deployment time:

1. The 5GMS Application Provider creates a Provisioning Session using the procedure specified in clause 4.3.2.2. The 5GMS AF provides the Provisioning Session Id in its response to the 5GMS Application Provider.
2. The 5GMS Application Provider creates a CSR using the *Reserve Server Certificate* procedure of this Provisioning Session using the procedure specified in clause 4.3.6.3. The 5GMS Application Provider provides a set of 5GMS AS domain name aliases as input. The CSR and the Certificate Id are provided upon success in the response.
3. The 5GMS Application Provider uses the CSR for obtaining the Server Certificate from its preferred Certificate Authority.
4. The Application Provider uses the Upload Server Certificate procedure (see clause 4.3.6.5) to upload the received Server Certificate.
5. The 5GMS Application Provider creates the Content Hosting Configuration using the procedure specified in clause 4.3.3.2, adding the Domain Name Alias *distributionConfigurations.domainNameAlias* and CertificateId of the uploaded Server Certificate (*distributionConfigurations.certificateld*). The 5GMS AF assigns a canonical domain name (*canonicalDomainName*) and provides its with the response.

As a consequence, the 5GMS AF provisions the 5GMS AS with relevant information from the Provisioning Session, including the Server Certificate and Content Hosting Configuration.

- 6: If it has not already done so, the 5GMS AF provisions *A* and/or *AAAA* records in the 5GMS System's DNS service mapping the canonical name of the 5GMS AS instance to its assigned IP address(es).

NOTE 1: The DNS service may be provided by a third-party service provider under the direction of the 5GMS System operator.

7. The 5GMS Application Provider provisions its DNS service with the *CNAME* record mapping its chosen host name alias to the canonical name of the 5GMS AS instance.

NOTE 2: The 5GMS Application Provider may leverage the DNS of the 5GMS System.

When content is selected in the 5GMS-Aware Application:

8. When Service Access Information retrieval at reference point M5 is used (see clause 4.7.2.3), the 5GMS Client in the UE retrieves the Service Access Information. This may include media entry point URLs within the *streamAccess.entryPoints* array. Otherwise, the 5GMS-Aware Application obtains this information via reference point M8.
9. The 5GMS Client in the UE selects one of the offered Media Entry Point URLs corresponding to the its media stream handling capabilities.
10. The 5GMS Client extracts the Fully-Qualified Domain Name (FQDN) from the chosen Media Entry Point URL and uses the DNS service to resolve its IP address, first resolving the domain name alias to the canonical domain name using the 5GMS Application Provider's nominated DNS service, and then resolving the canonical domain name to the IP address(es) using the 5GMS System operator's nominated DNS service.
11. When establishing the TLS connection to the 5GMS AS at reference point M4, the Media Stream Handler in the UE cites the FQDN of the Media Entry Point URL in the Server Name Indication (SNI) field of the TLS Client Hello Message. The 5GMS AS uses the value of the SNI field to look up the corresponding Server Certificate and returns it to the Media Stream Handler in its Server Hello response.

NOTE 3: If the Server Certificate was provisioned with a wildcard Common Name, appropriate matching rules are followed by the 5GMS AS to identify the correct Server Certificate to present to the Media Stream Handler.

12. The 5GMS Client Validates the Server Certificate, including whether the value of the Common Name (or one of its Subject Alternative Names) matches the FQDN of the chosen Media Entry Point URL.

When all server certificate validation steps are successfully passed, the following steps are executed

13. The 5GMS Client requests the resource identified by the Media Entry Point over the TLS connection established with the 5GMS AS at reference point M4.

Annex G (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
25.6.2019	SA4#104	S4-190649				Initial Version	0.0.1
23.1.2020	SA4#107	S4-200077, S4-200238, S4-200239, S4-200318				Updates during SA4#107	0.3.0
07.02.2020	ConfCall	S4-AHI931, S4-AHI932				Scope, editorial improvements and online edits from Conf Call (6 th Feb 2020)	0.3.1
11.02.2020	offline					Editorial updates according to offline email discussions	0.3.2
2020-02	ConfCall	S4-AHI950				Editorial updates from Conf Call (Online, 13 th Feb 2020)	0.4.0
2020-03	-	SP-200237				Specification to TSG: 5G Media Streaming (5GMS); Protocols TS 26.512, Version 1.0.0	1.0.0
		S4-AHI953					1.0.1
2020-04	SA4#108e	S4-200513, S4-200514, S4-200633				Renaming entities in the 5GMS Provisioning API, Additional clauses to specify procedures for manipulating Ingest Protocols, Content Preparation Templates and Server Certificates, Consumption Reporting Procedure API- M1d and M5d	1.0.2
2020-05	Conf Call	S4-AHI989				New Structure	1.1.0
2020-06	SA4#109e	S4-200920, S4-200886, S4-200889, S4-200883				920: Consumption reporting in M7d interface, 886: RAN Signaling-based Network Assistance, 889: API for Service Access information acquisition, 883: APIs for Server Certificates, Content Preparation Templates and Ingest Protocols	1.2.0
2020-08	SA4#110e	S4-AHI996 S4-AHI998 S4-AHIA33				996: Completion of Content Preparation Template procedures, 998: Completion of content distribution geofencing feature, A33: Completion of Server Certificates Provisioning API	1.3.0
2020-08	SA4#110e	Cor of S4-AHI998				Correction of S4-AHI998 implementation, Editorial Correction in Clause 11.2.4	1.3.1
2020-08	SA4#110e	S4-201092, S4-201114, S4-201210, S4-201208, S4-201213, S4-201230, S4-201004, S4-201229, S4-201221, S4-201231, S4-201225, S4-201271, S4-201266, S4-201282, S4-201281				1092: Editorial Improvements, 1114: Specification structure – interfaces and APIs, 1210: Completion of Ingest Protocols API, 1208: Informative Annex on Parameter Population, 1213: Addition of General Sections, 1230: M6d APIs for 5GMS, 1004: Informative annex on Content Hosting Configuration examples, 1229: Correction of the Policy Template resource state transitions, 1221: DASH/CMAF in 5GMSd, 1231: M7d APIs, 1225: Update on consumption reporting, 1271: Update on Metrics Reporting, 1266: Updated on M5 Dynamic Policy activation API and M1 Policy Template Provisioning API, 1282: 5GMS3: AF-based Network Assistance, 1281: Provisioning Sessions API	1.4.0
2020-09	SA#89-e	SP-200666				5G Media Streaming (5GMS); Protocols (This was the presentation of Specification to TSG: 5G Media Streaming (5GMS); Protocols TS 26.512, Version 2.0.0 to bring UCC)	16.0.0

2020-12	SA#90-e	SP-200935	0004	3	F	Cumulative corrections of 5GMS3 APIs [CRs implemented: S4-201432: Cumulative corrections of 5GMS3 APIs, Ericsson S4-201305: Editorial corrections, BBC S4-201363: Additions and Modifications to M1 API on Metrics Reporting Configuration, Qualcomm S4-201622: Text on Procedures for Uplink Streaming, Qualcomm, Ericsson S4-201580: Correction of the missing SdfMethod type definition, Ericsson S4-201593: Correction of the missing CRUD operation notation, Ericsson S4-201594: Correction of the MediaPlayerEntry and ClientMetricsReportingConfiguration cardinality in the Service Access Information resource, Ericsson S4-201596: Correction of the Service Access Information subresource (URL), Ericsson S4-201597: Annex for OpenAPI Implementation, Ericsson S4-201595, Update Consumption reporting, Enensys Technology, BBC S4-201590: Bug Fixes on Metrics Reporting Functionality, Ericsson LM, Qualcomm Incorporated S4-201486: AF-based Network Assistance, Sony Europe B.V., Ericsson LM S4-201608: CR on AT Commands for RAN-based Assistance, Qualcomm Inc.]	16.1.0
2021-05	SA#91-e	SP-210039	0007	2	F	OpenAPI implementation and aggregated essential corrections	16.2.1
2021-06	SA#92-e	SP-210566	0010	1	F	ClientId for Consumption and Metrics Reporting	16.3.0
2021-06	SA#92-e	SP-210566	0011	1	F	Corrections to 5GMS stage 3 specification	16.3.0
2021-06	SA#92-e	SP-210566	0012	1	F	Correction on Dynamic Policy parameters	16.3.0
2021-09	SA#93-e	SP-210826	0013	1	F	Corrections to TS 26.512	16.4.0
2022-03	SA#95-e	SP-220055	0014	0	F	Correction to QoE metrics reporting client configuration	16.5.0
2022-03	SA#95-e	SP-220238	0019	0	F	Add support for VR QoE metrics	16.5.0
2022-03	SA#95-e						17.0.0
2022-06	SA#96	SP-220595	0020	2	B	CR on Adding Edge Support	17.1.0
2022-06	SA#96	SP-220595	0021	1	F	Fixing api-version in 5GMS RESTful APIs	17.1.0
2022-06	SA#96	SP-220598	0023	1	B	Support for Data Collection and Reporting for 5G Media Streaming	17.1.0
2022-06	SA#96	SP-220597	0024	1	B	[5MBP3] 5GMS Protocol Extensions for 5GMS via eMBMS	17.1.0
2022-07	SA#96					Editorial Corrections	17.1.1
2022-08	SA#96					Editorial Corrections	17.1.2
2022-09	SA#97-e	SP-220757	0025	1	F	[5GMS_EDGE_3] [EVEX] Rel-17 API corrections	17.2.0
2022-12	SA#98-e	SP-221043	0028	2	F	[5GMS3] Rel-17 clarifications and corrections	17.3.0
2023-03	SA#99	SP-230253	0032	1	F	[5GMS3] Rel-17 corrections	17.4.0
2023-06	SA#100	SP-230546	0033	5	F	[5GMS3, TEI17] Rel-17 corrections	17.5.0
2023-09	SA#101	SP-231053	0037	3	F	[5GMS3, TEI17] Essential maintenance	17.6.0
2023-09	SA#101	SP-230913	0053	3	F	[5GMS, TEI17] Content hosting essential correction	17.6.0
2023-09	SA#101	SP-230918	0039	5	F	[5GMS_EDGE_3] Correction of EAS Discovery	17.6.0
2023-12	SA#102	SP-231368	0054	1	F	[5GMS3, TEI17] Essential maintenance	17.7.0
2023-12	SA#102	SP-231761	0060	5	F	[5GMS3, TEI17] Correction of Server Certificate handling	17.7.0
2024-03	SA#103	SP-240051	0062	1	F	Add Slice Scope for metrics configuration and reporting in stage 3	17.8.0
2024-06	SA#104	SP-240683	0065	1	F	[EVEX] Data packaging strategies for 5GMS	17.9.0
2024-06	SA#104	SP-240574	0069	2	F	[5GMS3, TEI17] Metrics reporting corrections	17.9.0
2024-06	SA#104	SP-240681	0071	1	F	[5GMS_EDGE_3] Correction to Edge Resources	17.9.0
2024-07						Corrected implementation of CR0069	17.9.1

History

Document history		
V17.0.0	April 2022	Publication
V17.1.0	July 2022	Publication (withdrawn)
V17.1.2	August 2022	Publication
V17.2.0	October 2022	Publication
V17.3.0	January 2023	Publication
V17.4.0	April 2023	Publication
V17.5.0	July 2023	Publication
V17.6.0	October 2023	Publication
V17.7.0	January 2024	Publication
V17.8.0	April 2024	Publication
V17.9.1	August 2024	Publication