|  |  |
| --- | --- |
| 3GPP TR 28.879 V19.1.0 (2025-03) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Management and orchestration;  Study on OAM for service management and  exposure to external consumers  (Release 19) | |
|  | |
|  | 3GPP-logo_web |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2025, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

Introduction 6

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 8

3.1 Terms 8

3.2 Symbols 8

3.3 Abbreviations 8

4 Concepts and Background 9

4.1 Exposure of management services 9

4.1.1 Overview 9

4.1.2 Background of existing SA5 solutions related to exposure 10

4.1.3 Background on existing telco exposure initiatives 10

4.1.3.1 3GPP exposure framework 10

4.1.3.2 GSMA Open Gateway 13

4.1.4 Examples of external MnS consumers 14

5 Use Cases 15

5.1 Exposure of management services 15

5.1.0 Exposure of management services through the CAPIF framework 15

5.1.0.1 Description 15

5.1.0.2 Potential requirements 16

5.1.1 Use case #1: API provider domain registration into CAPIF 17

5.1.1.1 Description 17

5.1.1.2 Potential requirements 17

5.1.1.3 Potential solutions 17

5.1.1.3.0 Potential solution #1: MSED is the API provider domain for management services 17

5.1.1.3.1 Potential solution #2: Map MSED information into APIProviderEnrolmentDetails 18

5.1.1.4 Evaluation of potential solutions 19

5.1.1.4.0 Evaluation of potential solution #1: MSED is the API provider domain for management services 19

The potential solution proposes to use MSED as the API provider domain for management services. The potential solution enables the fulfilment of the use case requirement PREQ-FS\_MExpo-Reg-015.1.1.4.1 Evaluation of potential solution #2: Capturing MSED registration information with APIProviderEnrolmentDetails 19

5.1.2 Use case #2: Publishing of management services to the CCF 20

5.1.2.1 Description 20

5.1.2.2 Potential requirements 20

5.1.2.3 Potential solutions 20

5.1.2.3.1 Potential solution #1: Mapping of management service information into service API information 20

5.1.2.3.2 Potential solution #2: Mapping MnS API URI to Service API URI. 23

5.1.2.3.3 Potential solution #3: MSED providing the APF functionality 24

5.1.2.4 Evaluation of potential solutions 24

5.1.2.4.1 Evaluation of potential solution #1 24

5.1.2.4.2 Evaluation of potential solution #2 24

5.1.2.4.3 Evaluation of potential solution #3 24

5.1.3 Use case #3: Configuring discovery policy information for an external MnS consumer 25

5.1.3.1 Description 25

5.1.3.2 Potential requirements 25

5.1.3.3 Potential solutions 25

5.1.3.4 Evaluation of potential solutions 25

5.1.4 Use case #4: Authorization of the external MnS consumer to access the management service API 26

5.1.4.1 Description 26

5.1.4.2 Potential requirements 26

5.1.4.3 Potential solutions 26

5.1.4.3.1 Potential solution #1: Using Identity class to define the authorization information of an external MnS consumer 26

5.1.4.3.2 Potential solution #2: Identity class made available to the CCF 27

5.1.4.4 Evaluation of potential solutions 30

5.1.4.4.1 Evaluation of potential solution #1 30

5.1.4.4.2 Evaluation of potential solution #2 30

5.1.5 Use case #5: Logging the management service API invocations to the CCF 31

5.1.5.1 Description 31

5.1.5.2 Potential requirements 31

5.1.5.3 Potential solutions 31

5.1.5.3.1 Potential solution #1: Creation and logging of the management service API invocations 31

5.1.5.4 Evaluation of potential solutions 33

6 Conclusions and recommendations 33

6.1 Conclusions 33

6.1.0 General 33

6.1.1 Use case #1: API provider domain registration into CAPIF 33

6.1.2 Use case #2: Publishing of management services to the CCF 34

6.1.3 Use case #3: Configuring discovery policy information for an external MnS consumer 34

6.1.4 Use case #4: Authorization of the external MnS consumer to access the management service API 34

6.1.5 Use case #5: Logging the management service API 34

6.2 Recommendations 34

Annex A: 3GPP management capabilities 36

Annex B: Change history 38

# Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

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

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

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

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

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

**should** indicates a recommendation to do something

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

**may** indicates permission to do something

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

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

**can** indicates that something is possible

**cannot** indicates that something is impossible

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

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

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

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

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

In addition:

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

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

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

# Introduction

The present document is to study exposure of management services to external consumers.

# 1 Scope

The present document identifies potential use cases and requirements for a generic approach for exposure of management services to external consumers. It documents and evaluates potential solutions and provides recommendations for the normative work.

# 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 28.533: "Management and orchestration; Architecture Framework".

[3] 3GPP TS 28.622: "Telecommunication management; Generic Network Resource Model (NRM) Integration Reference Point (IRP); Information Service (IS)".

[4] 3GPP TS 28.537: "Management and orchestration; Management capabilities".

[5] 3GPP TS 23.222: "Common API Framework for 3GPP Northbound APIs".

[6] SP-231669: "LS on collaboration and alignment of 3GPP defined application enablers with GSMA Open Gateway".

[7] 3GPP TS 23.434: "Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows".

[8] 3GPP TS 23.255: "Application layer support for Uncrewed Aerial System (UAS); Functional architecture and information flows".

[9] 3GPP TS 23.286: "Application layer support for Vehicle-to-Everything (V2X) services; Functional architecture and information flows".

[10] 3GPP TS 23.545: "Application layer support for Factories of the Future (FF)".

[11] 3GPP TS 23.542: "Application layer support for Personal IoT Networks".

[12] 3GPP TS 23.554: "Application architecture for MSGin5G Service; Stage 2".

[13] 3GPP TS 29.222: "Common API Framework for 3GPP Northbound APIs".

[14] 3GPP TS 33.122: "Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs".

[15] "[The Ecosystem for Open Gateway NaaS API Development](https://www.gsma.com/solutions-and-impact/gsma-open-gateway/wp-content/uploads/2023/05/The-Ecosystem-for-Open-Gateway-NaaS-API-development.pdf)", white paper, June 2023.

[16] [GSMA Official Document OPG.02](https://www.gsma.com/solutions-and-impact/technologies/networks/wp-content/uploads/2023/07/OPG.02-v5.0-Operator-Platform-Requirements-and-Architecture.pdf): "Operator Platform Group:- Requirements and Architecture", version 5.0, 26 July 2023.

[17] 3GPP TS 28.532: "Management and orchestration; Generic management services".

[18] 3GPP TS 28.531: "Management and orchestration; Provisioning".

[19] 3GPP TS 23.435: "Procedures for Network Slice Capability Exposure for Application Layer Enablement Service".

[20] 3GPP TS 23.558: "Architecture for enabling Edge Applications".

[21] 3GPP TS 28.550: "Management and orchestration; Performance assurance".

[22] 3GPP TS 28.111: "Fault Management".

[23] 3GPP TS 28.105: "Management and orchestration; Artificial Intelligence/Machine Learning (AI/ML) management".

[24] 3GPP TS 28.104: "Management and orchestration; Management Data Analytics (MDA)".

[25] 3GPP TS 28.541: "Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and 3".

[26] 3GPP TS 28.312: "Management and orchestration; Intent driven management services for mobile networks".

[27] 3GPP TS 28.538: "Management and orchestration; Edge Computing Management".

[28] 3GPP TS 28.536: "Management and orchestration; Management services for communication service assurance; Stage 2 and stage 3".

[29] 3GPP TS 28.319: "Management and orchestration; Access Control for Management services".

[30] 3GPP TS 32.158: "Management and orchestration; Design rules for REpresentational State Transfer (REST) Solution Sets (SS)".

[31] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

[32] IETF RFC 7519: "JSON Web Token (JWT)".

[33] 3GPP TS 28.552: "Management and orchestration; 5G performance measurements".

# 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].

**MnS consumer:** Defined in 3GPP TS 28.533 [2].

**MnS producer:** Defined in 3GPP TS 28.533 [2].

## 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].

5GC 5G Core

AAA Authentication, Authorization and Accounting

AEF API Exposing Function

AMF API Management Function

APF API Publishing Function

CAPIF Common API Framework

CCF CAPIF Core Function

CSP Communication Service Provider

EAS Edge Application Server

ECS Edge Configuration Server

EDN Edge Data Network

EEC Edge Enabler Client

EES Edge Enabler Server

FF Factories of the Future

GSMA GSM Association

MnS Management Service

NOTE: See 3GPP TS 28.533 [2].

NaaS Network as a Service

NEF Network Exposure Function

NOP Network Operator

NSACF Network Slice Access Control Function

NSCE Network Slice Capability Enablement

NWDAF Network Data Analytics Function

OAM Operation, Administration and Maintenance

OPAG Operator Platform API Group

OPG Operator Platform Group

SEAL Service Enabler Abstraction Layer

UAS Uncrewed Aerial Systems

V2X Vehicle-to-Everything

VAE Vertical App Enabler

WAS Whole Agreement Services

WG Working Group

# 4 Concepts and Background

## 4.1 Exposure of management services

### 4.1.1 Overview

The present document studies a generic approach to expose management services to external MnS consumers. An external MnS consumer is a MnS consumer that discovers and consumes management services using the CAPIF. Common API Framework (CAPIF) is a framework comprising common API aspects (e.g., publishing, discovery, access control) that are required to support service APIs. Service APIs are produced by the API provider domain, and consumed by API invokers.

A management service (MnS) is identified by different component types, i.e. MnS component type A (management operations or notifications), MnS component type B (managed objects), and MnS component type C (performance and fault information) (as defined in clause 4.2 of 3GPP TS 28.533 [2]). Accordingly, in order for the external MnS consumer to consume management services, the access rights have to be configured for the external MnS consumer. These access rights determine which MnS resources (i.e. component type B and component type C) can be accessed. In addition, the access rights also determine what operations (i.e. MnS component A) can or cannot be performed on the MnS resources. For example, considering Figure 4.1.1-1, the MnS A producer produces MnS A that is directly consumed by the internal MnS consumer and the external MnS consumers 1 and 2 respectively. Depending on the different access rights assigned to the external MnS consumers 1 and 2, it's possible that:

- The internal MnS Consumer and external MnS Consumer 1 and 2 can access the same or different managed objects under the management scope of MnS A producer.

- The operations (i.e. CRUD) or notifications that internal MnS Consumer and external MnS Consumer 1 and 2 can perform on the accessed managed objects are the same or different.

- The internal MnS Consumer and external MnS Consumer 1 and 2 can or cannot access the same or different performance and fault information associated with the accessible managed objects of MnS A.



Figure 4.1.1-1: Example of Exposing Management Services concept

To provide a MnS to be consumed, it first needs to be published into CAPIF. After it is published, the MnS will be available to be discovered by the external MnS consumers. Following discovery, authentication and authorization mechanisms need to be applied to ensure that the external MnS consumers only have access to the allowed MnS component type A, B, or C for the MnS.

### 4.1.2 Background of existing SA5 solutions related to exposure

This study will focus on how the 3GPP management system should be enhanced to expose MnSs to external MnS consumers using the CAPIF framework.

A MnS can be available (i.e. instantiated) and hence discoverable by an MnS consumer using 3GPP management system mechanisms as defined in the following specifications:

- An available MnS is described by the MnsInfo IOC (see clause 4.3.42 of 3GPP TS 28.622 [3]).

- The available MnSs in the 3GPP management system can be found in the MnSRegistry IOC (see clause 4.3.41 of 3GPP TS 28.622 [3]).

- The use case procedures for discovery are described in clause 5 of 3GPP TS 28.537 [4].

The access control framework is defined in 3GPP TS 28.319 [29]:

- The concept and solution for access control are described in clause 4 and clause 7 of 3GPP TS 28.319 [29].

### 4.1.3 Background on existing telco exposure initiatives

#### 4.1.3.1 3GPP exposure framework

3GPP standard exposure technologies hide the complexity of 5G and offer 3rd party applications a simple, secure, use-case-oriented configuration interface to the 5G system. The exposure interfaces will be quite valuable to a multitude of industrial use cases (i.e. non-telco use cases, with requirements beyond secure and reliable connectivity), allowing industry verticals to make use of the key features and performance that 5G has to offer in a simple and straightforward manner.

The development of solutions for exposure in 3GPP is led by SA6 WG. Figure 4.1.3.1-1 pictures the latest status of the 3GPP exposure framework. As seen, the framework consists of a set of Application Enablement Services ("Edge", "SEAL", "Vertical App Enabler") that pursue one mission: to provide means to 3rd parties to rapidly develop and deploy new vertical-oriented applications ("Application Layer") over 3GPP system ("Network and OAM/CH"). To that end, Application Enablement services offer industry-tailored APIs ("Northbound Interface - service APIs") that build on 3GPP system APIs ("Southbound Interface - network APIs"). All these APIs are documented in 3GPP Technical Specifications and made available under the 3GPP GitLab repository.



Figure 4.1.3.1-1: 3GPP exposure framework  
(Source: SP-231669 [6])

SA6 WG realized soon that managing all these APIs, especially in an environment where 3rd parties are developing applications, will also require a management layer that enforces the strong security policies defined by SA3 WG (e.g. Mutual TLS Authentication). This is where CAPIF comes to the picture. The operator can use CAPIF as an entry point for the Application Layer to gain access to 3GPP APIs, including not only the APIs offered by Application Enablement services (SA6), but also the APIs offered by the 3GPP system (SA2 and SA5).

Table 4.1.3.1-1 provides a more detailed description of all the components mentioned above.

Table 4.1.3.1-1: Components of the 3GPP exposure framework

|  |  |
| --- | --- |
| Component | Description |
| 3GPP system | Also referred to "5G Network Services" in Figure 4.1.3.1-1, it includes:  - Network Services: groups all the capabilities related to 3GPP SA2. These are made available through Core network functions, e.g. Network Exposure Function (NEF).  - OAM/CH services: groups all the capabilities related to 3GPP SA5. These capabilities are offered through MnSs by producers. |
| Edge Services | It includes services for hosting edge computing applications, while consolidating edge computing standardization in 3GPP. These services provide various capabilities such as rich discovery of the Edge Application Servers (EAS), service continuity between multiple Edge Data Networks (EDN), interworking with the core network, and APIs for EASs to integrate with the edge hosting environments. The main components building out this layer are specified in 3GPP TS 23.558 [20]:  - Edge Enabler Server (EES), primarily responsible for enabling discovery of EASs.  - Edge Enabler Client (EEC), providing support functions, such as EAS discovery to the application clients in the device.  - Edge Configuration Server (ECS), providing configurations to the EEC to connect with targeted EAS(s).  See note. |
| Service Enabler Abstraction Layer (SEAL) | It provides a set of core services that are common to industry verticals. The motivation is largely to avoid redefining the individual services for each vertical industry, thereby lowering the deployment costs for operators, and significantly reducing the barrier of adoption and the time-to-market for integrating new verticals to the 3GPP ecosystem. SEAL services are specified in 3GPP TS 23.434 [7], and include location management, group management, configuration management, identity management, key management, network resource management, data delivery, notification management, Network Slice Capability Enablement (NSCE) and application data analytics enablement. |
| Vertical App Enabler (VAE) | It provides vertical-specific service enablers. In contrast to the SEAL, VAE targets service specific vertical applications. As of today, the verticals service enablers are defined for:  - Automotive applications referred to as Vehicle-to-anything (V2X) communications, see 3GPP TS 23.255 [8].  - Drone applications known as Uncrewed Aerial Systems (UAS), see 3GPP TS 23.286 [9].  - Industry 4.0/OT applications, also referred to as Factories of the Future (FF), see 3GPP TS 23.545 [10]  - Personal IoT networks, see 3GPP TS 23.542 [11].  - Message communication in massive IoT, also referred to as MSGIn5G, see 3GPP TS 23.554 [12]. |
| Common API Framework (CAPIF) | Started in Release 15, CAPIF services are listed in 3GPP TS 23.222 [5] and specified in 3GPP TS 29.222 [13] with security aspects being addressed in 3GPP TS 33.122 [14]. It provides a unified Northbound API framework across network/application functions, to facilitate a harmonized approach for API exposure within 3GPP. This framework builds upon three main components:  - API invokers: they represent consumers of 3GPP APIs.  - CAPIF Core Function (CCF): responsible for managing onboarding of API invokers, and access control (authentication, authorization) when trying to gain access to 3GPP APIs.  - API provider domain: collection of functions (discovery, registration, publishing, auditability) required to allow authorized API invokers to consume 3GPP APIs. They implement agents that allow API producers to make APIs available through CAPIF. |
| Application Layer | This layer represents the 3rd party applications that want to gain access (discover and consume) 3GPP APIs, to develop and deploy new vertical services. |
| NOTE: The Edge Computing Layer only consumes network capability set from the 3GPP system (see Figure 4.1.3.1-1) | |

#### 4.1.3.2 GSMA Open Gateway

The development of telco capability exposure (also coined "Network as a Service" (NaaS)) requires a collaborative workspace that bring together incumbent telco standard bodies with IT/cloud communities, industry associations and open-source projects. An effective collaboration among organizations needs to be based on a clear demarcation on their scope of work, avoiding their participating organizations running overlapping activities or duplicate efforts; otherwise, NaaS may risk ending up with a fragmented ecosystem. To that end, the GSM Association (GSMA) launched Open Gateway in MWC Barcelona 23. GSMA Open Gateway mission is twofold:

i) to provide a governance framework for NaaS, covering technical and business aspects;

ii) to get operator commitment to launch universal NaaS API services in 2023.

Open Gateway initiative recognizes that NaaS the concept builds on the work developed by three organizations - see Table 4.1.3.2-1. The role of the different organizations and their relationship is graphically shown in Figure 4.1.3.2‑1.

Table 4.1.3.2-1: Organizations participating in GSMA Open Gateway initiative

|  |  |
| --- | --- |
| Organization | Description of Activity |
| Linux Foundation's CAMARA | it represents the "exposure" doctrine, i.e. how capabilities are exposed for external consumption through 3rd party facing APIs. CAMARA defines these APIs and is responsible for their hosting and release management. 3rd party facing APIs are dev-friendly (semantics tailored to service and business needs of 3rd parties) and open (following Apache2.0 license). |
| GSMA | it represents:  i) the "technical" doctrine, by specifying how 3rd party facing APIs are to be supported by underlying telco capabilities; and  ii) the "business" doctrine, with the definition of agreement templates for federation between the operator networks and for relationship with 3rd parties, ensuring a consistent yet fair commercial framework for exposing services.  GSMA conducts the technical workstream through OPG/OPAG (Operator Platform Group / Operator Platform API Group) and the business workstream through WAS (Wholesale Agreement Services) group. |
| TM Forum | It represents the "operational" doctrine, i.e. how 3rd party facing APIs are to be operated and managed, to make a commercial product out of them. Aspects such as 3rd party onboarding, application registration, access control and billing aspects are in scope. |

On the one hand, scope of "GSMA" is restricted to the telco domain. GSMA prescribes the capabilities that all operators can make available for 3rd parties, to ensure global reach and scale. These capabilities are referred to as Open Gateway services. The GSMA is also responsible for:

i) the prioritization and roadmap management of Open Gateway services, according to market needs and commercial readiness of underlying technologies; and

ii) architecting the platform that individual operators will use to realize, federate, and expose Open Gateway services.

On the other hand, the focus of "CAMARA" and "TM Forum is on the dev-friendly APIs that allows programmatic access to Open Gateway services. As seen in the bottom of Figure 4.1.3.2-1, these APIs can be clustered into three groups:

- service APIs;

- service management APIs; and

- operate APIs.

For further information on these APIs, see [15].

Each Communication Service Provider (CSP) exposes APIs through the Open Gateway Transformation Function (Figure 4.1.3.2‑1). Deployed as an internal component of GSMA Operator Platform [16] the Open Gateway Transformation Function is tasked with defining and enforcing the mapping between the dev-friendly APIs (towards 3rd party applications) and network APIs (towards 3GPP system). The mapping logic is not standardized, though GSMA provide non-prescriptive guidelines on a per API basis. For the interaction with OAM systems, the white paper in [15] notes that transformation function may interact with TM Forum (Open API portfolio) and 3GPP SA5 (management services).



Figure 4.1.3.2-1: GSMA Open Gateway ecosystem

### 4.1.4 Examples of external MnS consumers

Figure 4.1.4-1 provides examples of functional entities that can become external MnS consumers. Table 4.1.4-1 elaborates on the rationale.



Figure 4.1.4-1: Examples of external MnS consumers

Table 4.1.4-1: Examples of external MnS consumers

|  |  |
| --- | --- |
| Functional Entity | Justification |
| Application Layer Server | Any 3rd party application that gains access (discover and consume) to MnSs using the CAPIF framework is an external MnS consumer. The logic of this application is on the 3rd party and outside standardization. |
| SEAL's NSCE server | Network Slice Capability Enablement (NSCE) is a SEAL service that provides add-on slicing capabilities to vertical customers' applications. NSCE has a server and multiple clients (installed on vertical customer's devices). NSCE server consumes slicing capabilities related to OAM (i.e. MnSs) and 5G network services (i.e. NEF APIs, NWDAF APIs, NSACF APIs), and process them (aggregation, abstraction, filtering, etc.) in order to build vertical-oriented slicing functionality to applications.  The set of operations/notifications related to OAM that are eligible for consumption by NSCE server are specified in 3GPP TS 28.531 [18], and conceptually grouped under the NSCE-OAM interface in 3GPP TS 23.435 [19]. To gain access to these capabilities, NSCE server can use a discovery mechanism defined outside SA5. In this regard, the NSCE server becomes an external (network slice / network slice subnet) MnS consumer. |
| Open Gateway Transformation Function | Open Gateway services (defined by GSMA) are offered through dev-friendly APIs (specified and maintained by CAMARA and TM Forum). Some services provisioning and monitoring actions on 5G managed resources, including network slicing. In such a case, the invocation of these dev‑friendly APIs needs to be mapped into one or more calls to MnSs. The Open Gateway Transformation Function is in charge of this mapping and MnS invocation. To that end, the Open Gateway Transformation needs to be able to discover MnS. In this regard, one can realize that the Open Gateway Transformation Function complies with the external MnS consumer when it gains access to MnSs using the CAPIF framework. |

It is worth noting that the functional entities represented as examples of external MnS consumers in Table 4.1.4-1:

- Provides a non-exhaustive list; the only aim is to provide clarity on how external MnS consumer concept fits with the background of telco exposure initiatives reported in the background.

- Are all optional; the decision to deploy these functional entities or not is up to operator discretion.

- Perform the role of "API invokers" (see definition in clause 2 of TS 23.222 [2]).

# 5 Use Cases

## 5.1 Exposure of management services

### 5.1.0 Exposure of management services through the CAPIF framework

#### 5.1.0.1 Description

To expose management services through the CAPIF framework, the 3GPP management system should define the functional entity to provide the API provider domain functions (i.e., API Exposing Function (AEF), API management function (AMF), API publishing function (APF)) as defined by the CAPIF framework in clause 6.3 of TS 23.222[5].

For the present document, the functional entity is called the management services exposure domain (MSED). The MSED can consume CCF APIs (i.e., CAPIF-3, CAPIF-4 and CAPIF-5 interfaces) and allow API invokers to access management services through service APIs (using CAPIF-2/2e interface).



Figure 5.1.0-1: MSED providing the API provider domain functions as defined by the CAPIF framework.

The MSED provides the CAPIF API provider domain functions, and the following can apply for this functional entity:

- The MSED is a non-binding name. The final name will be discussed on normative phase.

- The following aspects can apply for the MSED:

- The MSED requires providing CAPIF interfaces, which are not defined in the 3GPP management system.

- The MSED publishes the management service APIs for discovery through the CAPIF core function (CCF) and exposes the management services for invocation by external MnS consumers through the AEF of the MSED.

- The possible deployment options of the MSED will be documented at the normative phase.

- Whether the MSED needs to provide the required mappings between SA5 and SA6 data types will be discussed in normative phase.

#### 5.1.0.2 Potential requirements

**PREQ-FS\_MExpo-MSED-01:** The 3GPP management system should support the capability to provide the API provider domain functions defined for CAPIF.

### 5.1.1 Use case #1: API provider domain registration into CAPIF

#### 5.1.1.1 Description

For a management service to be made available for external consumption through CAPIF, it is needed that the 3GPP management system defines an API provider domain for management services. This API provider domain includes the functionality to ensure that selected management services can be exposed through CAPIF for external consumption.

In the CAPIF, the scope of registration is limited to the API provider domain functions that are relevant for the CCF, which include the API Exposing Function (AEF), the API Publishing Function (APF) and the API Management Function (AMF). In CAPIF, the registration is the procedure whereby these functions become recognized users of the CCF. This procedure is described in clause 8.28 of 3GPP TS 23.222 [5], with stage 3 solution set detailed in clause 8.9 of 3GPP TS 29.222 [13].

To register (de-register and/or update the registration information of) an API provider domain on the CCF, the AMF of this API provider domain communicates with the CCF over CAPIF-5 interface. This means that:

- This API provider domain should have an AMF.

- The AMF of this API provider domain should be an authorized user of CCF.

- The AMF security information for CCF to validate the registration request is provisioned by the CAPIF administrator.

#### 5.1.1.2 Potential requirements

**PREQ-FS\_MExpo-Reg-01:** The 3GPP management system shall provide the capability to define an API provider domain for management services.

**PREQ-FS\_MExpo-Reg-02:** The 3GPP management system shall provide the capability to register the API provider domain for management services to the CCF.

**PREQ-FS\_MExpo-Reg-03:** The 3GPP management system shall provide the capability to deregister the API provider domain for management services from the CCF.

**PREQ-FS\_MExpo-Reg-04:** The 3GPP management system shall provide the capability to update the registration details of the API provider domain for management services at the CCF.

#### 5.1.1.3 Potential solutions

##### 5.1.1.3.0 Potential solution #1: MSED is the API provider domain for management services

This potential solution proposes to use MSED as the API provider domain for management services. To register the MSED to the CCF, it is needed that MSED supports the following API provider domain functionality:

- AEF. If supported, this means that the MSED will need to support:

- CAPIF-2/2e interface, so that the API invokers acting as external MnS consumers can access service APIs, when required. The functionality supported on this reference point is defined in clauses 6.4.4 and 6.4.5 of TS 23.222[5] and the API operations that will be implemented on this interface are defined in clause 9.1 of TS 29.222 [13]).

- CAPIF-3 interface, so that the AEF functionality of the MSED can communicate with CCF to exercise access and policy related control for service API invocations initiated by the API invoker. The functionality supported on this reference point is defined in clause 6.4.6 of TS 23.222[5] and the API operations that will be implemented on this interface are defined in clauses 8.3, 8.5, 8.7 and 8.6 of TS 29.222 [13]).

- APF. If supported, this means that the MSED will need to support the CAPIF-4 interface, so that it can communicate with CCF to publish (and manage the published) MnS information. The functionality supported on this reference point is defined in clause 6.4.7 of TS 23.222[5] and the API operations that will be implemented on this interface are defined in clause 8.2 of TS 29.222 [13].

- AMF. If supported, this means that MSED will need to support the CAPIF-5 interface. The functionality supported on this reference point is defined in clause 6.4.8 of TS 23.222[5] and the API operations that will be implemented on this interface are defined in clauses 8.3 and 8.9 of TS 29.222 [13].

To register the MSED as the API provider domain for management services, the AMF functionality of the MSED communicates the MSED details (including supported API provider domain functions) to the CCF using the CAPIF\_API\_Provider\_Management\_API as described in clause 5.1.1.3.1 of the present document.

##### 5.1.1.3.1 Potential solution #2: Map MSED information into APIProviderEnrolmentDetails

5.1.1.3.1.1 Introduction

This solution assumes that the MSED is the API provider domain that needs to get registered onto the CCF.

In CAPIF, the registration procedure is executed with the CAPIF\_API\_Provider\_Management API (see 3GPP clause 8.3 of TS 29.222 [13]), initiated by the AMF functionality of the MSED over the CAPIF-5 interface. The AMF functionality of the MSED sends a HTTP POST message to the CCF with a request body containing the following dataType: "APIProviderEnrolmentDetails" (see 3GPP TS 29.222 [13], clause 8.9.4.2.2).

The solution proposes the MSED information with the "APIProviderEnrolmentDetails" and reuse the CAPIF\_API\_Provider\_Management API to register, de-register and update registration information related to the MSED.

5.1.1.3.1.2 Description

How the MSED information relevant for registration can be captured with "APIProviderEnrolmentDetails" is described in tables 5.1.1.3.1.2-1, 5.1.1.3.1.2-2 and 5.1.1.3.1.2-3.

Table 5.1.1.3.1.2-1 lists the attributes of type APIProviderEnrolmentDetails (see clause 8.9.4.2.2 of TS 29.222 [13]) and how the MSED information can be mapped. See table 8.9.4.2.2-1 of TS 29.222 [13] for the data type, presence indicator, cardinality, description and applicability information for the attributes of type APIProviderEnrolmentDetails.

Table 5.1.1.3.1.2-1: Representing MSED registration information with  
APIProviderEnrolmentDetails attributes

| Attribute name | Attribute additional information | Mapping to MnSInfo IOC attributes/Comments |
| --- | --- | --- |
| apiProvDomId | The data type of this attribute is defined as "string" and presence qualifier is defined as "O" (see table 8.9.4.2.2-1 of TS 29.222 [13]). | Assigned by the CCF to the AMF functionality of the MSED during registration of the MSED as the API provider domain. |
| regSec | The data type of this attribute is defined as "string" and presence qualifier is defined as "M" (see table 8.9.4.2.2-1 of TS 29.222 [13]). | It can be used to store the security credentials of the MSED. |
| apiProvFuncs | The data type of this attribute is defined as "array(APIProviderFunctionDetails)" and presence qualifier is defined as "O" (see table 8.9.4.2.2-1 of TS 29.222 [13]). | See Table 5.1.1.3.1.2-2. |
| apiProvDomInfo | The data type of this attribute is defined as "string" and presence qualifier is defined as "O" (see table 8.9.4.2.2-1 of TS 29.222 [13]). |  |
| suppFeat | The data type of this attribute is defined as "SupportedFeatures" and presence qualifier is defined as "C" (see table 8.9.4.2.2-1 of TS 29.222 [13]). | Only applicable when API provider is SCEF/NEF, and thus not applicable when API provider is MSED. |
| failReason | The data type of this attribute is defined as "string" and presence qualifier is defined as "C" (see table 8.9.4.2.2-1 of TS 29.222 [13]). |  |
| apiProvName | The data type of this attribute is defined as "string" and presence qualifier is defined as "O" (see table 8.9.4.2.2-1 of TS 29.222 [13]). | RNAA. |

Table 5.1.1.3.1.2-2 lists the attributes of type APIProviderFunctionDetails (see clause 8.9.4.2.3 of TS 29.222 [13]) and how the MSED information can be mapped. See table 8.9.4.2.3-1 of TS 29.222 [13] for the data type, presence indicator, cardinality, description and applicability information for the attributes of type APIProviderFunctionDetails.

Table 5.1.1.3.1.2-2: Representing MSED registration information with  
APIProviderFunctionDetails attributes

| Attribute name | Attribute additional information | Mapping to MnSInfo IOC attributes/Comments |
| --- | --- | --- |
| apiProvFuncId | The data type of this attribute is defined as "string" and presence qualifier is defined as "C" (see table 8.9.4.2.3-1 of TS 29.222 [13]). | The API provider function id assigned to each function composing the MSED (i.e., AEF, APF or the AMF) by the CCF as part of the MSED registration request response. |
| regInfo | The data type of this attribute is defined as "RegistrationInformation" and presence qualifier is defined as "M" (see table 8.9.4.2.3-1 of TS 29.222 [13]). | See Table 5.1.1.3.1.2-3. |
| apiProvFuncRole | The data type of this attribute is defined as "ApiProviderFuncRole" and presence qualifier is defined as "M" (see table 8.9.4.2.3-1 of TS 29.222 [13]). | This data type serves to specify, for the MSED to be registered, which CAPIF API provider domain function(s) will be supported. |
| apiProvFuncInfo | See clause 8.9.4.3.3 of TS 29.222 [13] for the enumeration values and description of type ApiProviderFuncRole. |  |

Table 5.1.1.3.1.2-3 lists the attributes of type RegistrationInformation (see clause 8.9.4.2.4 of TS 29.222 [13]) and how the MSED information can be mapped. See table 8.9.4.2.4-1 of TS 29.222 [13] for the data type, presence indicator, cardinality, description and applicability information for the attributes of type RegistrationInformation.

Table 5.1.1.3.1.2-3: Representing MSED registration information with  
RegistrationInformation attributes

|  |  |  |
| --- | --- | --- |
| Attribute name | Attribute additional information | Mapping to MnSInfo IOC attributes/Comments |
| apiProvPubKey | The data type of this attribute is defined as "string" and presence qualifier is defined as "M" (see table 8.9.4.2.4-1 of TS 29.222 [13]). | It can be used to store the public key of the MSED. |
| apiProvCert | The data type of this attribute is defined as "string" and presence qualifier is defined as "O" (see table 8.9.4.2.4-1 of TS 29.222 [13]). | It can be used to store the client certificate of the MSED, if existing. |

#### 5.1.1.4 Evaluation of potential solutions

##### 5.1.1.4.0 Evaluation of potential solution #1: MSED is the API provider domain for management services

The potential solution proposes to use MSED as the API provider domain for management services. The potential solution enables the fulfilment of the use case requirement PREQ-FS\_MExpo-Reg-01.

##### 5.1.1.4.1 Evaluation of potential solution #2: Capturing MSED registration information with APIProviderEnrolmentDetails

To manage the registration of the MSED to the CCF using CAPIF\_API\_Provider\_Management API, it is needed to populate the "APIProviderEnrolmentDetails" datatype with the registration information of the MSED. Detailed in clause 5.1.1.3.1.2, the mapping solution is summarized below:

- The security credentials of the MSED can be mapped to "APIProviderEnrolmentDetails /regSec".

- The different API provider domain functions provided by the MSED can be mapped to "APIProviderEnrolmentDetails /apiProvFuncs".

- The public key of the MSED can be mapped to "APIProviderEnrolmentDetails/ apiProvFuncs/regInfo/apiProvPubKey".

The solution satisfies the use case requirements PREQ-FS\_MExpo-Reg-02, PREQ-FS\_MExpo-Reg-03 and PREQ‑FS\_MExpo-Reg-04.

### 5.1.2 Use case #2: Publishing of management services to the CCF

#### 5.1.2.1 Description

Upon registration of the MSED into the CCF (see clause 5.1.1), then the MSED can be enabled to decide, on a per MnS basis, what information related to this MnS will be made available for external consumption. This decision is subjected to operator internal policies; for example, the operator might not want that all resources which can be accessed through this MnS are visible to CAPIF, but only a subset of them.

Once this decision is made, then the management service information needs to be published into CCF, so that it can later be used by the external MnS consumers to discover and subsequently invoke the MnS. To publish information into CCF, the Publish\_Service\_API (see clause 5.3.2.2 of TS 29.222 [13]) needs to be invoked over CAPIF-4 interface. To make it happen, the following should occur:

- First, the management service information is mapped into "ServiceAPIDescription" data type (see clause 8.2.4.2.2 in 3GPP TS 29.222 [13]), which represents the information passed over Publish\_Service\_API. The attributes of the "ServiceAPIDescription" data type describes the information of a service API. The need for this mapping is due to the fact that the CAPIF framework publishes service APIs (and not management services). It is worth noting that an operator can decide to publish one MnS as one or more service APIs.

- Secondly, the service API information resulting from the above mapping gets published into the CCF. The APF sends this information to the CCF when invoking Publish\_Service\_API (see clause 5.3.2.2 of TS 29.222 [13]) over CAPIF-4 interface.

#### 5.1.2.2 Potential requirements

**PREQ-FS\_MExpo-Pub-01:** The 3GPP management system shall have the capability to map management service information into service API information.

**PREQ-FS\_MExpo-Pub-02:** The 3GPP management system shall have the capability provide the APF functionality.

#### 5.1.2.3 Potential solutions

##### 5.1.2.3.1 Potential solution #1: Mapping of management service information into service API information

5.1.2.3.1.1 Introduction

To publish a service API to the CCF, the APF uses the Publish\_Service\_API. Specifically, the APF sends a HTTP POST message to the CCF, including information of the service API for publishing. This service API information is represented with ServiceAPIDescription data type.

To publish a management service to the CCF, there is a need to map management service information into service API information. This potential solution describes how this mapping can be done, capturing it in Table 5.1.2.3.1.2-1. This solution assumes that the MSED provides the APF functionality.

5.1.2.3.1.2 Description

Table 5.1.2.3.1.2-1 lists the attributes contained in the ServiceAPIDescription data type, and clarifies which attributes can be mapped from management service information. See table 8.2.4.2.2-1 of TS 29.222 [13] for the data type, presence indicator, cardinality, description and applicability information for the attributes of ServiceAPIDescription.

Table 5.1.2.3.1.2-1: Mapping of management service information into ServiceAPIDescription data type attributes

| Attribute name | Attribute additional information | Equivalent MnSInfo IOC attribute/comments |
| --- | --- | --- |
| apiName | The data type of this attribute is defined as "string" and presence qualifier is defined as "M" (see table 8.2.4.2.2-1 of TS 29.222 [13]). | Corresponds to the following IOC attribute: mnsType |
| apiId | The data type of this attribute is defined as "string" and presence qualifier is defined as "O" (see table 8.2.4.2.2-1 of TS 29.222 [13]). |  |
| aefProfiles | The data type of this attribute is defined as " array(AefProfile)" and presence qualifier is defined as "C" (see table 8.2.4.2.2-1 of TS 29.222 [13]). | See Table 5.1.2.3.1.2-2 |
| description | The data type of this attribute is defined as "string" and presence qualifier is defined as "O" (see table 8.2.4.2.2-1 of TS 29.222 [13]). |  |
| supportedFeatures | The data type of this attribute is defined as "SupportedFeatures" and presence qualifier is defined as "O" (see table 8.2.4.2.2-1 of TS 29.222 [13]). | Not applicable in the context of SA5 MnS. |
| shareableInfo | The data type of this attribute is defined as "ShareableInformation" and presence qualifier is defined as "O" (see table 8.2.4.2.2-1 of TS 29.222 [13]). | Not applicable in the context of SA5 MnS. |
| serviceAPICategory | The data type of this attribute is defined as "string" and presence qualifier is defined as "C" (see table 8.2.4.2.2-1 of TS 29.222 [13]). |  |
| ccfId | The data type of this attribute is defined as "string" and presence qualifier is defined as "C" (see table 8.2.4.2.2-1 of TS 29.222 [13]). | Not applicable in the context of SA5 MnS. |
| apiSuppFeats | The data type of this attribute is defined as "SupportedFeatures" and presence qualifier is defined as "O" (see table 8.2.4.2.2-1 of TS 29.222 [13]). | Not applicable in the context of SA5 MnS. |
| pubApiPath | The data type of this attribute is defined as "PublishedApiPath" and presence qualifier is defined as "C" (see table 8.2.4.2.2-1 of TS 29.222 [13]). | Not applicable in the context of SA5 MnS. |

Table 5.1.2.3.1.2-2 lists the attributes contained in the AefProfile data type (see clause 8.2.4.2.4 of TS 29.222 [13]) and clarifies which ones can be mapped from management service information. See table 8.2.4.2.4-1 of TS 29.222 [13] for the data type, presence indicator, cardinality, description and applicability information for attributes of AefProfile.

Table 5.1.2.3.1.2-2: Mapping of management service information into AefProfile data type attributes

|  |  |  |
| --- | --- | --- |
| Attribute name | Attribute additional information | Equivalent MnSInfo IOC attribute/comments |
| aefId | The data type of this attribute is defined as "string" and presence qualifier is defined as "M" (see table 8.2.4.2.4-1 of TS 29.222 [13]). | Corresponds to the AEF identifier provided by the CCF upon MSED registration (see clause 5.1.1). |
| versions | The data type of this attribute is defined as "array(Version)" and presence qualifier is defined as "M" (see table 8.2.4.2.4-1 of TS 29.222 [13]). | See Table 5.1.2.3.1.2-3. |
| protocol | The data type of this attribute is defined as "Protocol" and presence qualifier is defined as "O" (see table 8.2.4.2.4-1 of TS 29.222 [13]). | Only "HTTP\_1\_1" and "HTTP\_1\_2" are applicable in the context of SA5 MnS. |
| dataFormat | The data type of this attribute is defined as "DataFormat" and presence qualifier is defined as "O" (see table 8.2.4.2.4-1 of TS 29.222 [13]). | Only "JSON" value is applicable in the context of SA5 MnS. |
| securityMethods | The data type of this attribute is defined as "array(SecurityMethod)" and presence qualifier is defined as "O" (see table 8.2.4.2.4-1 of TS 29.222 [13]). | Only "OAUTH" value (i.e. TLS with OAuth token) is applicable in the context of SA5 MnS. |
| domainName | The data type of this attribute is defined as "string" and presence qualifier is defined as "O" (see table 8.2.4.2.4-1 of TS 29.222 [13]). |  |
| interfaceDescriptions | The data type of this attribute is defined as "array(InterfaceDescription)" and presence qualifier is defined as "O" (see table 8.2.4.2.4-1 of TS 29.222 [13]). | See Table 5.1.2.3.1.2-5. |
| aefLocation | The data type of this attribute is defined as "AefLocation" and presence qualifier is defined as "O" (see table 8.2.4.2.4-1 of TS 29.222 [13]). |  |

Table 5.1.2.3.1.2-3 lists the attributes of Version data type (see clause 8.2.4.2.5 of TS 29.222 [13]), and clarifies which attributes can be mapped from management service information. See table 8.2.4.2.5-1 of TS 29.222 [13] for the data type, presence indicator, cardinality, description and applicability information for attributes of Version.

Table 5.1.2.3.1.2-3: Mapping of management service information into Version datatype attributes

|  |  |  |
| --- | --- | --- |
| Attribute name | Attribute additional information | Equivalent MnSInfo IOC attribute/comments |
| apiVersion | The data type of this attribute is defined as "string" and presence qualifier is defined as "M" (see table 8.2.4.2.5-1 of TS 29.222 [13]). | Corresponds to the following MnSInfo IOC attribute: mnsVersion |
| expiry | The data type of this attribute is defined as "DateTime" and presence qualifier is defined as "O" (see table 8.2.4.2.5-1 of TS 29.222 [13]). | Not applicable in the context of SA5 MnS. |
| resources | The data type of this attribute is defined as "array(Resource)" and presence qualifier is defined as "O" (see table 8.2.4.2.5-1 of TS 29.222 [13]). | See Table 5.1.2.3.1.2-4.  Each Resource corresponds to an MOI accessed through this MnS. |
| custOperations | The data type of this attribute is defined as "array(CustomOperation)" and presence qualifier is defined as "O" (see table 8.2.4.2.5-1 of TS 29.222 [13]). |  |

Table 5.1.2.3.1.2-4 lists the attributes of Resource data type (see clause 8.2.4.2.6 of TS 29.222 [13]), and clarifies which attributes can be mapped from management service information. See table 8.2.4.2.6-1 of TS 29.222 [13] for the data type, presence indicator, cardinality, description and applicability information for attributes of type Resource.

Table 5.1.2.3.1.2-4: Mapping of management service information into Resource data type attributes

|  |  |  |
| --- | --- | --- |
| Attribute name | Attribute additional information | Equivalent MnSInfo IOC attribute/comments |
| resourceName | The data type of this attribute is defined as "string" and presence qualifier is defined as "M" (see table 8.2.4.2.6-1 of TS 29.222 [13]). | IOC name of the MOI.  In the URI structure of the MnS API (see clause 5.1.2.3.2), this attribute corresponds to the variable parameter {className}. |
| commType | The data type of this attribute is defined as "CommunicationType" and presence qualifier is defined as "M" (see table 8.2.4.2.6-1 of TS 29.222 [13]). | Only "REQUEST\_RESPONSE" value is applicable for SA5 MnS of type Provisioning. |
| uri | The data type of this attribute is defined as "string" and presence qualifier is defined as "M" (see table 8.2.4.2.6-1 of TS 29.222 [13]). | In the URI structure of the MnS API (see clause 5.1.2.3.2), this attribute corresponds to: {URI-LDN-first-part}/{className} = {id}. |
| custOpName | The data type of this attribute is defined as "string" and presence qualifier is defined as "O" (see table 8.2.4.2.6-1 of TS 29.222 [13]). |  |
| custOperations | The data type of this attribute is defined as "array(CustomOperation)" and presence qualifier is defined as "O" (see table 8.2.4.2.6-1 of TS 29.222 [13]). |  |
| operations | The data type of this attribute is defined as "array(Operation)" and presence qualifier is defined as "C" (see table 8.2.4.2.6-1 of TS 29.222 [13]). | In the URI structure of the MnS API (see clause 5.1.2.3.2), this attribute specifies the HTTP methods under {URI-LDN-first-part}/{className} = {id}. |
| description | The data type of this attribute is defined as "string" and presence qualifier is defined as "O" (see table 8.2.4.2.6-1 of TS 29.222 [13]). |  |

Table 5.1.2.3.1.2-5 lists the attributes of InterfaceDescription data type (see clause 8.2.4.2.3 of TS 29.222 [13]), and clarifies which attributes can be mapped from management service information. See table 8.2.4.2.3-1 of TS 29.222 [13] for the data type, presence indicator, cardinality, description and applicability information for attributes of InterfaceDescription.

Table 5.1.2.3.1.2-5: Mapping of management service information into InterfaceDescription datatype attributes

|  |  |  |
| --- | --- | --- |
| Attribute name | Attribute additional information | Equivalent MnSInfo IOC attribute/comments |
| ipv4Addr | The data type of this attribute is defined as "Ipv4Addr" and presence qualifier is defined as "C" (see table 8.2.4.2.3-1 of TS 29.222 [13]). | Not applicable in the context of SA5 MnS |
| ipv6Addr | The data type of this attribute is defined as "Ipv6Addr" and presence qualifier is defined as "C" (see table 8.2.4.2.3-1 of TS 29.222 [13]). | Not applicable in the context of SA5 MnS |
| fqdn | The data type of this attribute is defined as "Fqdn" and presence qualifier is defined as "C" (see table 8.2.4.2.3-1 of TS 29.222 [13]). | In the URI structure of the MnS API (see clause 5.1.2.3.2), this attribute corresponds to the following: {URI-DN-prefix}.  The FQDN can be constructed from the DN prefix as detailed in clause 4.2.3, 3GPP TS 32.158 [30]. |
| port | The data type of this attribute is defined as "Port" and presence qualifier is defined as "O" (see table 8.2.4.2.3-1 of TS 29.222 [13]). |  |
| apiPrefix | The data type of this attribute is defined as "string" and presence qualifier is defined as "O" (see table 8.2.4.2.3-1 of TS 29.222 [13]). | In the URI structure of the MnS API (see clause 5.1.2.3.2), this attribute corresponds to the following:: "/" + {root} |
| securityMethods | The data type of this attribute is defined as "array(SecurityMethod)" and presence qualifier is defined as "O" (see table 8.2.4.2.3-1 of TS 29.222 [13]). | Only "OAUTH" value (i.e. TLS with OAuth token) is applicable in the context of SA5 MnS. |

With this mapping, it is possible to publish management service information into the CCF.

##### 5.1.2.3.2 Potential solution #2: Mapping MnS API URI to Service API URI.

5.1.2.3.2.1 Introduction

When publishing on the CCF, MnS APIs need to be mapped to service APIs, so that the latter can be accessed by external MnS consumers. This potential solution compares the URI structure of a MnS API and a service API, to help understand how this mapping looks like.

5.1.2.3.2.2 Description

The table below compares the URI structure for Service API and MnS API.

Table 5.1.2.3.2.2-1: URI structure for Service API and MnS API

| Service API | MnS API (see 3GPP TS 32.158) |
| --- | --- |
| URI: = <apiRoot>/<apiName>/<apiVersion>/<APISpecificSuffixes>  See NOTE 1 | URI: = {MnSRoot}/{MnSName}/{MnSVersion}/{URI-LDN-first-part}/{className} = {id}  See NOTE 2 |
| NOTE 1: <apiRoot>:= https://<authority>/<API-prefix>, with <API-prefix> being optional.  NOTE 2: {MnSRoot} = https://{URI-to-DN-prefix}/{root}, with {root} being optional. | |

It is needed that the URI structure for MnS APIs follow the same format as defined for service APIs. This means:

- {MnSRoot} corresponds to the <apiRoot>. The {apiRoot} variable of the URI structure for the service API can be constructed by the API invoker based on the "interfaceDescriptions" attribute of the AefProfile data type (Table 5.1.2.3.1.2-2). For further information, see clause 5.2.2.2.2 in 3GPP TS 29.222 [13].

- {URI-to-DN-prefix} corresponds to the <authority> (host and optional TCP port). The host name is constructed from the DN prefix as detailed in clause 4.2.3, 3GPP TS 32.158 [30].

- {root} corresponds to <API-prefix>.

- {MnSName} corresponds to <apiName>. For example, when <MnSName> := ProvMnS, then the apiName in the service API URI shall be ProvMnS.

- {MnSVersion} corresponds to <apiVersion>.

- {URI-LDN-first-part}/{className} = {id} corresponds to <apiSpecificSuffixes>.

##### 5.1.2.3.3 Potential solution #3: MSED providing the APF functionality

5.1.2.3.3.1 Introduction

This potential solution that the APF functionality is provided by MSED.

5.1.2.3.3.2 Description

The MSED described in clause 5.1.0 is within 3GPP management system. The scope of MSED is to provide API provider domain functions in the context of CAPIF.

API provider domain functions include APF. Based on this, the MSED can provide the APF functionality.

#### 5.1.2.4 Evaluation of potential solutions

##### 5.1.2.4.1 Evaluation of potential solution #1

The potential solution #1 shows that it is feasible to map management service API information into service API information. Therefore, it fulfils PREQ-FS\_MExpo-Pub-01.

For the cases where the operator decides to publish a MnS as two (or more) service APIs, the mapping proposed in potential solution #1 needs to be done with this in mind, mapping management service information into two (or more) ServiceAPIDescription data type.

The ServiceAPIDescription data type provides valuable information for an external MnS consumer. For example, for discovery purposes, the following attributes are relevant:

- "resources" (see Table 5.1.2.3.1.2-4). This attribute provides information on the scope of a service API, i.e. constituent service API resources. This solution requires that the external MnS consumer understand the NRM tree.

- "ServiceAPICategory" (see Table 5.1.2.3.1.1-1). This attribute provides additional information for a specific API. It complements "resource" attribute.

NOTE: The usage of "ServiceAPICategory" is currently limited to CAPIF-6/6e interface. In the event the usage of this attribute is extended to other CAPIF interfaces, then this attribute could be used to accommodate future optional MnSInfo IOC attributes.

##### 5.1.2.4.2 Evaluation of potential solution #2

The potential solution #2 shows that the URI structure of MnS APIs can be mapped into the URI structure of service APIs. Therefore, it fulfils PREQ-FS\_MExpo-Pub-01.

The potential solution identifies that {MnSVersion} in MnS corresponds to <apiVersion> in service API. However, it is worth noting that <apiVersion> represents only the major release, e.g. "v1", while the <MnSVersion> follows "v<major>.<minor>.<patch>" format, e.g. "v15.0.1". Reconciling the API version mapping between {MnSVersion} and <apiVersion> can be done by the network operator, and it is not subject to standardization;

##### 5.1.2.4.3 Evaluation of potential solution #3

The potential solution #3 shows that the MSED provides the APF functionality. The MSED is defined within the 3GPP management system. Therefore, potential solution #3 fulfils PREQ-FS\_MExpo-Pub-02.

### 5.1.3 Use case #3: Configuring discovery policy information for an external MnS consumer

#### 5.1.3.1 Description

One or more API invokers may want access to published service APIs. For an API invoker to become a recognized user of the CAPIF, there are two stages:

- API invoker enrolment. In this first stage, a subscription for this API invoker is created, based on service agreement between the CAPIF provider and the API invoker (see clause 5.1 of TS 23.222 [5]). This subscription defines the list of published service APIs that the API invoker can discover and access later, together with SLA related to API invocations (e.g., quota, throttling). This subscription allows generating an onboarding credential for the API invoker is created. This credential is sent together with CCF details (address, root CA certificate) to the API invoker. As noted in clause 6.1 of TS 33.122 [14], these artefacts will be required by API invoker to initiate the onboarding stage.

- API invoker onboarding. In this second stage, the API invoker onboards itself at the CCF. To that end, the API invoker sends an onboarding request to the CCF (see clause 8.1 of TS 23.222 [5]) over CAPIF-1e interface. This request is sent using CAPIF\_API\_Invoker\_Onboarding\_API (see clause 5.5.2.2 of TS 29.222 [13]), with input information represented with APIInvokerEnrolmentDetails data type (see clause 8.4.2.2.3.1 in TS 29.222 [13]). Successful onboarding results in CCF provisioning API invoker profile (which includes identity for the API invoker and information required for the CCF to authenticate and authorize API invoker on subsequent CAPIF-1e interactions) and creating the list of service APIs that the CCF authorizes the API invoker to access (based on the subscription created during the API invoker enrolment).

Upon completion of these two stages, the API invoker is a recognized CAPIF user and can proceed with the discovery. For discovery, the API invoker sends a request to the CCF (see clause 8.7 of TS 23.222 [5]) using CAPIF\_Discover\_Service\_API (see clause 8.8 of TS 29.222 [13]). This request includes the API invoker identifier and query information.

As noted in clause 8.7.3 of TS 23.222 [5], the discovery procedure requires the fulfilment of two pre-conditions. On the one hand, that the API invoker is onboarded and has received an API invoker identity; this is needed for the CCF to authenticate the API invoker on CAPIF-1e interface. On the other hand, that the CCF is configured with a discovery policy information; this is needed for CCF to perform filtering on service APIs information which matches the discovery criteria. For further information on discovery policy information, see clause 8.7.3 of TS 23.222 [5].

It is also worth noting that the discovery is performed at Service API level. The atomic information used both by API invoker (when including the query information in the discovery request) and the CCF (when applying the discovery policy information) is service API, not service API resource. Because of this, and because discovery only implies interaction over CAPIF-1e interface, there is no impact on 3GPP management system for the discovery use case.

#### 5.1.3.2 Potential requirements

There are no requirements impacting 3GPP management system for this use case.

#### 5.1.3.3 Potential solutions

There are no solutions available for this use case.

#### 5.1.3.4 Evaluation of potential solutions

There are no solution evaluations available for this use case.

### 5.1.4 Use case #4: Authorization of the external MnS consumer to access the management service API

#### 5.1.4.1 Description

Upon completion of discovery, the API invoker is now ready to consume service APIs. To gain access to one or more service APIs, the API invoker needs to get authorized using CAPIF built-in OAuth2.0 framework. As noted in clause 6.5.2.3 of TS 33.122 [14], the authorization use case is a two-stage process, as follows:

- Stage #1: Authorization request (over CAPIF-1e interface). In this stage, the API invoker requests the CCF for authorization to access one or more service APIs. The CCF issues this authorization to the API invoker in the form of an JWT access token. This access token contains the API invoker’s permissions for requested service APIs.

- Stage #2: Service API invocation (over CAPIF-2e interface). In this stage, the API invoker issues a Service API invocation request to the AEF, sending the URI of the service API along with the access token received from the stage #1. The request is subjected to authorization, checking the API invoker’s service API invocation against the permissions in the access token. If authorization is successful, the requested service API can be invoked and the appropriate response is returned to the API invoker.

The 3GPP management system allows configuring authorization information (permissions) on a per MnS consumer basis, for authorization, leveraging role-based access control (RBAC). TS 28.319 [29] defines a framework for such a capability set, which is referred to as management service access control (MSAC). MSAC information is used by the MnS producer to authorize incoming MnS consumer requests.

When using CAPIF as the framework to expose MnS, the external MnS consumer plays the role of the API Invoker. Putting the above into the context, the following can be noted:

- The authorization information of an external MnS consumer is defined using MSAC.

- The defined authorization information of an external MnS consumer is put into an access token.

- An access token is issued by the CCF (sends the access token to the external MnS consumer) and interpreted by the MnS producer (reads the access token to authorize external MnS consumer’s service API invocation request).

The issue here is how to ensure CCF is able to issue access tokens that can be understood/interpreted by the MnS producer. This requires that CCF has access to external MnS consumer authorization information.

#### 5.1.4.2 Potential requirements

**PREQ-FS\_MExpo-Auth-01:** The 3GPP management system shall provide the capability to define authorization information for an external MnS consumer using MSAC.

**PREQ-FS\_MExpo-Auth-02:** The 3GPP management system shall provide the capability to make external MnS consumer’s authorization information available to the CCF, so that CCF can grant authorization for an external MnS consumer.

#### 5.1.4.3 Potential solutions

##### 5.1.4.3.1 Potential solution #1: Using Identity class to define the authorization information of an external MnS consumer

5.1.4.3.1.1 Introduction

The information model for MSAC is described in clause 7 of TS 28.319 [29]. The MSAC information model (see clause 7.3 of TS 28.319 [29]) specifies three classes: Identity, which represents an identity of a MnS consumer, and the associated roles; Role, which represents the role name and a list of permissions in a network management system; and AccessRule, which represents a permission in a network management system.

This potential solution proposes using Identity to define the authorization information of an external MnS consumer.

5.1.4.3.1.2 Description

During the API invoker enrolment stage, a subscription for the external MnS consumer is created. This subscription defines the list of published service APIs that the external MnS consumer can discover and access later, together with SLA related to API invocations (e.g., quota, throttling). This subscription has the information needed to define the authorization information for an external MnS consumer. To that end, the following occurs:

1) CAPIF administrator identifies the API provider domain(s) where enrolled service APIs belongs to; in this solution, the API provider domain is MSED.

2) CAPIF administrator requests the administrator(s) of identified API provider domain(s) to define the authorization information for an external MnS consumer, using the access control framework applicable in the domain(s); in this solution, the applicable access control framework is MSAC.

3) The administrator uses MSAC to create an Identity instance, by associating it to one or more Role instances, each listing one or more AccessRule instances. This information is stored in the authentication and authorization MnS producer (see clause 4.9 of TS 28.533 [2]).

4) The authentication and authorization MnS producer generates an onboarding credential for the external MnS consumer.

5) The authentication and authorization MnS producer associates the Identity instance created in step 3 with the onboarding credential created in step 4. This association is kept in the authentication and authorization service producer, i.e. not disclosed to CCF nor external MnS consumer.

6) The onboarding credential created in step 4 together with CCF details (address, root CA certificate) are sent to the external MnS consumer, so that it can initiate the onboarding.

##### 5.1.4.3.2 Potential solution #2: Identity class made available to the CCF

5.1.4.3.2.1 Introduction

From the 3GPP management system perspective, the Identity class represents the only MSAC information that can be made available to any access control system. On the other hand, AccessRule class attributes contains 3GPP management specific information (e.g., JEX expressions, DNs of MOIs, etc) that is not understood/interpretable by the CCF. On the other hand, the Role class includes a list of access rules based on AccessRule class, so not useful neither for CCF.

In this regard, the MSAC information that is eligible for CCF access is limited to the Identity class. This potential solution focuses on how to make an Identity instance available to the CCF, so that the CCF can use this information to grant authorization to external MnS consumers.

5.1.4.3.2.2 Description

The workflow describing the solution is depicted in Figure 5.1.4.3.2.2-1. The pre-condition requires executing the steps described in potential solution #1 (see clause 5.1.4.3.1.2), which is where the Identity instance for the API invoker is created.

A screenshot of a computer

Description automatically generated

Figure 5.1.4.3.2.2-1: Solution #2 workflow.

The steps 1-9 corresponding to the API invoker onboarding procedure.

1) To begin the onboarding procedure, the API invoker establishes a secure connection with the CCF based on TLS server-side authentication. The server certificate is CCF’s Root CA, which was sent to the API invoker after enrolment (see step 6 in clause 5.1.4.3.1.2).

2) The API invoker sends an onboard API invoker request to the CCF over the CAPIF-1/CAPIF-1e interface. This request involves providing the onboarding enrolment information using the APIInvokerEnrolmentDetails data type (see clause 8.4.4.2.2 of TS 29.222[13]). This data type includes the onboarding credential, which was sent to the API invoker after enrolment (see step 6 in clause 5.1.4.3.1.2).

3) The CCF sends an acknowledgment for receiving the onboard API invoker request to the API invoker.

4) The CCF takes the "onboarding credential" from the APIInvokerEnrolmentDetails data type, and sends it to the authentication and authorization MnS producer

5) The authentication and authorization MnS producer validates the received "onboarding credential".

6) If the "onboarding credential" is valid, the authentication and authorization MnS producer retrieves the MSAC Identity associated to the onboarding credential (see step 4 of clause 5.1.4.3.1.2). The retrieved MSAC Identity instance represents the authorization information of the API invoker.

7) The authentication and authorization MnS producer sends the associated MSAC identity for the API invoker to the CCF.

8) Upon receiving the associated MSAC identity, the CCF generates the "API invoker id" that represents a unique identifier for the API invoker in the CCF. The CCF associates the generated "API invoker id" with the received MSAC identity.

9) The CCF sends an onboard API invoker response to the API invoker with the response body represented by the APIInvokerEnrolmentDetails data type. The response includes the assigned "API invoker id"

To gain access to one or more service APIs, the API invoker needs to get authorized using CAPIF built-in OAuth2.0 framework. As described in clause 5.1.4.1, this authorization procedure is a two-stage process, i.e., Authorization request (steps 10 - 16) and Service API invocation.

10) When the API invoker wants to invoke specific service APIs, it establishes a secure connection with the CCF based on TLS mutual authentication.

11) The API invoker sends an access token request to the CCF to invoke specific service API(s), providing the "API invoker id" and optionally a list of service API(s) it wants to invoke. The request body carries the information described by the AccessTokenReq data type (see Table 5.1.4.3.2.2-1).

12) The CCF validates the request, and if valid, retrieves the MSAC Identity associated to the "API invoker id" (see step 9). This "API invoker id" is in the "client\_id" parameter of the received access token request.

13) The CCF sends access token request to the authentication and authorization MnS producer. In this request, the "client\_id" parameter in the access token request is set to the retrieved MSAC Identity.

14) The authentication and authorization MnS producer validates the request and generates an access token. This token will contain, as part of token claims, the allowed APIs (MnSes) that the API invoker is authorized to invoke.

15) The authentication and authorization MnS producer sends the generated access token to the CCF.

16) Upon receiving the access token, the CCF forwards the received access token response to the API invoker. The CCF sends a "service API authorization response", which carries the information described by the AccessTokenRsp data type (see Table 5.1.4.3.2.2-2)

Finally, the API invoker can successfully invoke the service API at the AEF as described in clause 6.5.2.3 of TS 33.122[14].

NOTE: How the CCF interacts with authentication and authorization MnS producer is up to implementation and not subject to standardization. The implementation may choose to collocate or not the CCF and the authentication and authorization MnS producer.

Table 5.1.4.3.2.2-1: Definition of AccessTokenReq data type

| Attribute name | Attribute additional information | Comments |
| --- | --- | --- |
| grant\_type | The data type of this attribute is defined as "string" and presence qualifier is defined as "M" (see table 8.5.4.2.6-1 of TS 29.222 [13]). | Set to “client\_credentials” |
| client\_id | The data type of this attribute is defined as "string" and presence qualifier is defined as "M" (see table 8.5.4.2.6-1 of TS 29.222 [13]). | Set to "apiInvokerId", which uniquely identifies the external MnS consumer (onboarded API invoker). |
| resOwnerId | The data type of this attribute is defined as "ResOwnerId" and presence qualifier is defined as "O" (see table 8.5.4.2.6-1 of TS 29.222 [13]). |  |
| client\_secret | The data type of this attribute is defined as "string" and presence qualifier is defined as "O" (see table 8.5.4.2.6-1 of TS 29.222 [13]). | If the external MnS consumer has a password, it can be included here. |
| scope | The data type of this attribute is defined as "string" and presence qualifier is defined as "O" (see table 8.5.4.2.6-1 of TS 29.222 [13]). | It represents the requested scope,  i.e. the list of service APIs per AEF that the external MnS consumer requests authorization for.  This attribute contains a space-delimitated string as follows: 3gpp#aefId1: apiName, apiName2, … apiNameX; aefId2: apiName1, apiName  apiNameY;…aefIdN:apiName1,apiName2,…apiNameZ |
| authCode | The data type of this attribute is defined as "string" and presence qualifier is defined as "C" (see table 8.5.4.2.6-1 of TS 29.222 [13]). | RNAA |
| redirect\_uri | The data type of this attribute is defined as "string" and presence qualifier is defined as "O" (see table 8.5.4.2.6-1 of TS 29.222 [13]). | RNAA |

Table 5.1.4.3.2.2-2: Definition of AccessTokenRsp data type

|  |  |  |
| --- | --- | --- |
| Attribute name | Attribute additional information | Comments |
| access\_token | The data type of this attribute is defined as "string" and presence qualifier is defined as "M" (see table 8.5.4.2.7-1 of TS 29.222 [13]). | It represents the access token issued by the CCF. |
| token\_type | The data type of this attribute is defined as "string" and presence qualifier is defined as "M" (see table 8.5.4.2.7-1 of TS 29.222 [13]). |  |
| expires\_in | The data type of this attribute is defined as "DurationSec" and presence qualifier is defined as "M" (see table 8.5.4.2.7-1 of TS 29.222 [13]). |  |
| scope | The data type of this attribute is defined as "string" and presence qualifier is defined as "O" (see table 8.5.4.2.7-1 of TS 29.222 [13]). | It represents the authorized scope. |

#### 5.1.4.4 Evaluation of potential solutions

##### 5.1.4.4.1 Evaluation of potential solution #1

This solution demonstrates how Identity class can be used to define the authorization information for an external MnS consumer. The authentication and authorization MnS producer generates an Identity instance, based on subscription created for the API invoker after service agreement with CAPIF provider. The solution #1 fulfils the requirement PREQ-FS\_MExpo-Auth-01 of the use case.

It is worth noting that this solution is applied offline during the API Invoker enrolment stage, which is a stage not subjected to standardization. Therefore, how steps 1-6 in the solution are executed is at operator’s discretion.

##### 5.1.4.4.2 Evaluation of potential solution #2

This solution demonstrates how Identity class can be made available to CCF for an external MnS consumer, so that the CCF can use this information to grant authorization to access one or more service APIs. The authentication and authorization MnS producer sends the MSAC Identity (created during the API invoker enrolment stage) to the CCF. The CCF associates the received MSAC Identity to the "API invoker id" (created during the API invoker onboarding procedure).

The solution #2 represents a baseline solution; further elaboration on how the authentication and authorization MnS producer generates token claims will be carried out in the normative phase. This baseline solution fulfils the requirement PREQ-FS\_MExpo-Auth-02 of the use case.

### 5.1.5 Use case #5: Logging the management service API invocations to the CCF

#### 5.1.5.1 Description

When a service API is invoked by the external MnS consumers over the CAPIF-2e interface, it is crucial to monitor information related to the service API invocation. This information includes for example, details on what management service API was invoked (i.e. the service API name, which service API resource, and the operations), who invoked the API (i.e. the ID of the external MnS consumer), the result of the invocation (e.g. success, or failure) and at what time it was invoked.

Accordingly, the AEF of the API provider domain should be able to create the service API invocation log(s) (see clause 8.7 of 3GPP TS 29.222 [13]) with the desired information. Subsequently, the AEF should be able to send the invocation log(s) to the CCF via the CAPIF-3 interface. The stored logs of the service API invocations can be consumed by authorized consumers (e.g. the AMF of the API provider domain for auditing purposes and the charging functions).

#### 5.1.5.2 Potential requirements

**PREQ-FS\_MExpo-Log-01:** The 3GPP management system should support the capability to create logs based on the management service API invocations by external MnS consumers.

**PREQ-FS\_MExpo-Log-02:** The 3GPP management system should support the capability to log the management service API invocations to the CCF.

#### 5.1.5.3 Potential solutions

##### 5.1.5.3.1 Potential solution #1: Creation and logging of the management service API invocations

5.1.5.3.1.1 Introduction

The potential solution assumes that the MSED has an AEF functionality that interacts with the CCF via the CAPIF-3 interface. Accordingly, this potential solution describes how the AEF functionality of the MSED can create the management service API invocation log. Secondly, the solution describes how the AEF functionality of the MSED can send these logging data to the CCF for authorized consumers to consume (e.g. AMF and charging functions).

5.1.5.3.1.2 Description

To log the management service API invocations to the CCF, the AEF functionality of the MSED should create an invocation log (see clause 8.7 in 3GPP TS 29.222 [13]). Table 5.1.5.3.1.2-1 maps the CAPIF InvocationLog data type and the MnSInfo IOC (see clause 4.3.42 of 3GPP TS 28.622 [3]) attributes.

Table 5.1.5.3.1.2-1 lists the attributes contained in the InvocationLog data type (see clause 8.7.4.2.2 of TS 29.222 [13]) and clarifies how they are related to management service information. See table 8.7.4.2.2-1 of TS 29.222 [13] for the data type, presence indicator, cardinality, description and applicability information for the attributes of type InvocationLog.

Table 5.1.5.3.1.2-1: Relationship of CAPIF InvocationLog data type with management service information

|  |  |  |
| --- | --- | --- |
| Attribute name | Attribute additional information | Comments |
| aefId | The data type of this attribute is defined as "string" and presence qualifier is defined as "M" (see table 8.7.4.2.2-1 of TS 29.222 [13]). | Corresponds to the AEF identifier provided by the CCF upon MSED registration (see clause 5.1.1).  See “aefId” attribute in Table 5.1.2.3.1.2-2. |
| apiInvokerId | The data type of this attribute is defined as "string" and presence qualifier is defined as "M" (see table 8.7.4.2.2-1 of TS 29.222 [13]). | Provided by the external MnS consumer to the AEF functionality of the MSED when invoking the management service API |
| logs | The data type of this attribute is defined as "array(Log)" and presence qualifier is defined as "M" (see table 8.7.4.2.2-1 of TS 29.222 [13]). | See Table 5.1.5.3.1.2-2 |
| supportedFeatures | The data type of this attribute is defined as "SupportedFeatures" and presence qualifier is defined as "O" (see table 8.7.4.2.2-1 of TS 29.222 [13]). |  |

Table 5.1.5.3.1.2-2 lists the attributes of type Log (see clause 8.7.4.2.3 of TS 29.222 [13]) and how the management service information can be mapped. See table 8.7.4.2.3-1 of TS 29.222 [13] for the data type, presence indicator, cardinality, description and applicability information for the attributes of type Log.

Table 5.1.5.3.1.2-2: Mapping of CAPIF Log data type into management service information

| Attribute name | Attribute additional information | Mapping to MnSInfo IOC attributes/Comments |
| --- | --- | --- |
| apiId | The data type of this attribute is defined as "string" and presence qualifier is defined as "M" (see table 8.7.4.2.3-1 of TS 29.222 [13]). | The APF functionality of the MSED receives this attribute from the CCF after publishing the MnS information (see clause 5.1.2).  This attribute is known by the AEF functionality of the MSED. |
| apiName | The data type of this attribute is defined as "string" and presence qualifier is defined as "M" (see table 8.7.4.2.3-1 of TS 29.222 [13]). | Name of the service API that was invoked.  This attribute corresponds to the following MnSInfo IOC attribute: mnsType. |
| apiVersion | The data type of this attribute is defined as "string" and presence qualifier is defined as "M" (see table 8.7.4.2.3-1 of TS 29.222 [13]). | Version of the service API that was invoked by the API invoker. This attribute corresponds to the following MnSInfo IOC attribute: mnsVersion. |
| resourceName | The data type of this attribute is defined as "String" and presence qualifier is defined as "M" (see table 8.7.4.2.3-1 of TS 29.222 [13]). | The name of the resource that was invoked by the service API invocation request. This resource is an MOI. In the URI structure of the MnS API (see clause 5.1.2.3.2), this attribute  corresponds to the {className} parameter. |
| uri | The data type of this attribute is defined as "Uri" and presence qualifier is defined as "O" (see table 8.7.4.2.3-1 of TS 29.222 [13]). | The URI of the invoked resource by the service API invocation request  This attribute corresponds to the following URI component in the URI structure of the MnS API: {URI-LDN-first-part}/{className} = {id}. |
| protocol | The data type of this attribute is defined as "Protocol" and presence qualifier is defined as "M" (see table 8.7.4.2.3-1 of TS 29.222 [13]). | Only "HTTP\_1\_1" and "HTTP\_1\_2" are applicable in the context of 3GPP management services. |
| operation | The data type of this attribute is defined as "Operation" and presence qualifier is defined as "C" (see table 8.7.4.2.3-1 of TS 29.222 [13]). | The HTTP method that was invoked on the resource by the service API invocation request  Corresponds to one of the HTTP methods listed in the "operations" attribute in Table 5.1.2.3.1.2-4. |
| result | The data type of this attribute is defined as "string" and presence qualifier is defined as "M" (see table 8.7.4.2.3-1 of TS 29.222 [13]). | HTTP status codes. |
| invocationTime | The data type of this attribute is defined as "DateTime" and presence qualifier is defined as "O" (see table 8.7.4.2.3-1 of TS 29.222 [13]). | Date and time at which the service API invocation request is received at the AEF functionality of the MSED. |
| invocationLatency | The data type of this attribute is defined as "DurationMs" and presence qualifier is defined as "O" (see table 8.7.4.2.3-1 of TS 29.222 [13]). | The time interval between the reception of the service API invocation request and the sending of the service API invocation response at the AEF functionality of the MSED. |
| inputParameters | The data type of this attribute is defined as "ANY TYPE" and presence qualifier is defined as "O" (see table 8.7.4.2.3-1 of TS 29.222 [13]). |  |
| OutputParameters | The data type of this attribute is defined as "ANY TYPE" and presence qualifier is defined as "O" (see table 8.7.4.2.3-1 of TS 29.222 [13]). |  |
| srcInterface | The data type of this attribute is defined as "InterfaceDescription" and presence qualifier is defined as "O" (see table 8.7.4.2.3-1 of TS 29.222 [13]). |  |
| destInterface | The data type of this attribute is defined as "InterfaceDescription" and presence qualifier is defined as "O" (see table 8.7.4.2.3-1 of TS 29.222 [13]). |  |
| fwdInterface | The data type of this attribute is defined as "string" and presence qualifier is defined as "O" (see table 8.7.4.2.3-1 of TS 29.222 [13]). |  |

After creating the invocation log, the AEF functionality of the MSED can log these data to the CCF via the CAPIF-3 interface.

#### 5.1.5.4 Evaluation of potential solutions

The proposed solution satisfies the requirement PREQ-FS\_MExpo-Log-01. To fulfil the use case requirement PREQ-FS\_MExpo-Log-02, the proposed solution requires that the MSED providing the AEF functionality supports the CAPIF-3 interface and the interface operations associated to the logging capability.

# 6 Conclusions and recommendations

## 6.1 Conclusions

### 6.1.0 General

The study has focused on a generic approach to expose management services to external MnS consumers. For the present document, the chosen exposure framework is CAPIF. When management services are exposed using the CAPIF, the study has identified the need for 3GPP management system to define an API provider domain for management services. This API provider domain is referred as to MSED. As described in clause 5.1.0, the MSED provides the API provider domain functions: AEF, AMF and APF. The specification of the MSED is to be done in normative phase.

For the exposure of management services, based on the Rel-18 CAPIF specifications, the study has reported on five key use cases.

### 6.1.1 Use case #1: API provider domain registration into CAPIF

For 3GPP management system to become a recognized API provider domain, there is a need to register the MSED into CAPIF. The registration is initiated by an existing AMF functionality, which sends MSED registration information to the CCF.

The MSED registration information needs to be represented with appropriate CAPIF data type (i.e., APIProviderEnrolmentDeatils), so it can be sent over CAPIF-5 interface. The solution is described in clause 5.1.1.3.1. The solution is feasible and no gaps have been identified.

### 6.1.2 Use case #2: Publishing of management services to the CCF

For a management service to be discoverable and consumable through CAPIF, there is a need to publish this management service as one (or more) service APIs onto the CCF. The publishing is initiated by the APF (API Publishing Function) functionality of the MSED, which sends management service information to the CCF:

- The management service information need to be represented with appropriate CAPIF data type (i.e., ServiceAPIDescription), so it can be sent over CAPIF-4 interface. The solution is described in clause 5.1.2.3.1. The solution is feasible and no gaps have been identified.

- The URL components of a management service (what is offered to MnS consumer) need to match with the URL components of a service API (what is offered to external MnS consumer). The solution is described in clause 5.1.2.3.2. The solution is feasible and no gaps have been identified.

- The APF instance is provided by the registered MSED. The solution is described in clause 5.1.2.3.3. The solution is feasible and no gaps have been identified.

### 6.1.3 Use case #3: Configuring discovery policy information for an external MnS consumer

An operator may want to limit the visibility that certain API invokers have over published API information, according to the business agreements settled with the stakeholder owning the API invoker. To that end, the CCF is configured with discovery policy information on a per API invoker basis.

The discovery policy information, configured on CCF, is at the operator’s discretion. After analysis, it is concluded that this use case has no impact on 3GPP management system, so no requirements and solutions are proposed.

### 6.1.4 Use case #4: Authorization of the external MnS consumer to access the management service API

To get access to one or more service APIs, the external MnS consumer needs to get authorized. The consumer requests the CCF (over CAPIF-1e interface) an access token, that it can later use to invoke one or more service APIs (over CAPIF-2e interface). For this use case, the following has to occur:

- The authorization information of the external MnS consumer needs to be defined using MSAC information. The solution is described in clause 5.1.4.3.1. The solution is feasible and no gaps have been identified.

- The authorization information of the external MnS consumer needs to be made available to the CCF, so that CCF can grant authorization issuing the access token. The solution is described in clause 5.1.4.3.2. The baseline solution has been agreed, though further elaboration on how the authentication and authorization MnS producer generates token claims is required to be done during normative phase.

### 6.1.5 Use case #5: Logging the management service API

To log service API invocations, the AEF functionality of the MSED sends invocation logs to the CCF over CAPIF-3 interface. These logs can be used for auditing and charging purposes. Accordingly, it is needed to represent service API invocation logs with appropriate CAPIF data type (e.g., InvocationLog data type). The solution is described in clause 5.1.5.3.1. The solution is feasible and no gaps have been identified.

## 6.2 Recommendations

It is recommended to start normative work covering the following:

- Adding the capability for the 3GPP management system to implement the following solutions:

- solution described in clause 5.1.1.3.1, to support the following use case: "MSED registration into CAPIF use case".

- solutions described in clauses 5.1.2.3.1, 5.1.2.3.2 and 5.1.2.3.3, to support the following use case: "Publication of management services to the CCF"

- solutions described in clauses 5.1.4.3.1 and 5.1.4.3.2, to support the following use case: "Authorization of the external MnS consumer to access the management service API"

- solution described in clause 5.1.5.3.1, to support the following use case: "Logging the management service API"

- Specification of MSED. The MSED represents a new entity within 3GPP management system implementing API provider domain functions, to communicate with CCF (over CAPIF-3/4/5 interfaces) and external MnS consumers (over CAPIF-2 interface). The final name of MSED (currently non-binding) and supported capabilities need to be specified.

Annex A:  
3GPP management capabilities

SA5 WG is responsible for developing, maintaining, and evolving solutions building up the 3GPP management system. The relationship of the 3GPP management system with the state-of-the-art initiatives (clause 4.1.3) can be summarized as follows:

- Corresponds to the "OAM/CH services" box inside 3GPP system (see Figure 4.1.3.1-1).

- Is a collection of solutions, from one or more vendors, that reside within the CSP domain (see Figure 4.1.3.2‑1).

- Provides management capabilities which are realized via network APIs (see Figure 4.1.3.2-1).

The table below provides a (non-exhaustive) list of the management capabilities that can be provided by 3GPP management system. This list builds on the information available in 3GPP TS 28.533 [2], Annex F, complementing it with mechanisms that are non-CRUD based.

Table A-1: 3GPP management system capabilities

| Management Capability | Mechanisms | | Solutions | |
| --- | --- | --- | --- | --- |
| RESTFUL | NETCONF/ YANG |
| Performance data collection control | CRUD operations (3GPP TS 28.532 [17]) + PM control NRM fragment (3GPP TS 28.622 [3]) | | X | X |
| CRUD operation (3GPP TS 28.532 [17]) + ManagementDataCollection NRM fragment (3GPP TS 28.622 [3]) | | X | X |
| Measurement job control (3GPP TS 28.550 [21]) | | X |  |
| Performance data report | CRUD operations (3GPP TS 28.532 [17]) + PM control NRM fragment (3GPP TS 28.622 [3]) | | X | X |
| File data reporting service (3GPP TS 28.532 [17]) | | X |  |
| Streaming data reporting service (3GPP TS 28.532 [17]) | | X |  |
| Performance data monitoring | CRUD operations (3GPP TS 28.552 [33]) + Threshold monitoring control NRM fragment (3GPP TS 28.622 [3]) | | X | X |
| Trace/MDT data collection control | CRUD operations (3GPP TS 28.532 [17]) + Trace control NRM fragment (3GPP TS 28.622 [3]) | | X | X |
| CRUD operation + ManagementDataCollection NRM fragment (3GPP TS 28.622 [3]) | | X | X |
| Trace/MDT data report | File data reporting service (3GPP TS 28.532 [17]) | | X |  |
| CRUD operations (3GPP TS 28.532 [17]) + File retrieval NRM fragment (3GPP TS 28.622 [3]) | | X | X |
| Streaming data reporting service (3GPP TS 28.532 [17]) | |  |  |
| Fault data control | CRUD operations (3GPP TS 28.532 [17]) + FM control NRM fragment (3GPP TS 28.111 [22]) | | X | X |
| Fault supervision data control service (3GPP TS 28.532 [17]) | |  |  |
| Fault data report | CRUD operations (3GPP TS 28.532 [17]) + FM control NRM fragment (3GPP TS 28.111 [22]) | | X | X |
| Fault supervision data report service (3GPP TS 28.532 [17]) | |  |  |
| QoE control | CRUD operations (3GPP TS 28.532 [17]) + QMC control NRM fragment (3GPP TS 28.532 [17]) | | X | X |
| Service registry and discovery | CRUD operations (3GPP TS 28.532 [17]) + MnS Registry NRM fragment (3GPP TS 28.622 [3]) | | X | X |
| Subscription | CRUD operations (3GPP TS 28.532 [17]) + Notification subscription control NRM fragment (3GPP TS 28.622 [3]) | | X | X |
| AI/ML management | CRUD operations (3GPP TS 28.532 [17]) + ML Training NRM fragment (3GPP TS 28.105 [23]) | | X |  |
| Management Data Analytics | CRUD operations (3GPP TS 28.532 [17]) + MDA request & report NRM fragment (3GPP TS 28.104 [24]) | | X |  |
| NR Provisioning | CRUD operations (3GPP TS 28.532 [17]) + NR NRM fragment (3GPP TS 28.541 [25]) | | X | X |
| 5GC Provisioning | CRUD operations (3GPP TS 28.532 [17]) + 5GC NRM fragment (3GPP TS 28.541 [25]) | | X | X |
| Network Slice Provisioning | CRUD operations (3GPP TS 28.532 [17]) + Network slice NRM fragment (3GPP TS 28.541 [25]) | | X | X |
| Network slicing provisioning service (3GPP TS 28.531 [18]) | X | |  |
| SON Policy | CRUD operations (3GPP TS 28.532 [17]) + NRM fragments for DANR/DES/DRACH/DMRO/DPCI/CES/CPCI/DLBO/CCO management (3GPP TS 28.541 [25]) | | X | X |
| Intent Driven Management | CRUD operations (3GPP TS 28.532 [17]) + Intent NRM fragment (3GPP TS 28.312 [26]) | | X |  |
| Edge Computing Provisioning | CRUD operations (3GPP TS 28.532 [17]) + Edge NRM fragment (3GPP TS 28.538 [27]) | | X |  |
| Communication Service Assurance | CRUD operations (3GPP TS 28.532 [17]) + Assurance NRM fragment (3GPP TS 28.536 [28]) | | X |  |

Annex B:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-02 | - | n/a | - | - | - | Initial skeleton | 0.0.0 |
| 2024-02 | SA5#153 | S5-241089 |  |  |  | Implements S5-241060, S5-241061 | 0.1.0 |
| 2024-04 | SA5#154 | S5-242008  S5-242005  S5-242010  S5-242009  S5-242163 | pCR  pCR  pCR  pCR  pCR |  |  | Add Concepts and background for Exposure of Management Services in Clause 4  Update use case template in Clause 5  Add definition of external MnS consumer concept  Add background on existing telco exposure initiatives  Add list with the different types of external MnS consumers | 0.2.0 |
| 2024-05 | SA5#155 | S5-243264  S5-243250  S5-243252  S5-243253  S5-243256  S5-243259  S5-243262  S5-243263 | pCR  pCR  pCR  pCR  pCR  pCR  pCR  pCR |  |  | Add and correct references  Registration of MnS producer into CAPIF  Add use case for publishing management services to the CCF  Add potential solutions for publishing management services to the CCF  Configuring discovery policy for an external MnS consumer  Add use case for authorization of the external MnS consumer to access the management service API  Add use case for logging the management service API invocations  Add a new potential solution for logging the management service API invocations to the CCF | 0.3.0 |
| 2024-08 | SA5#156 | S5-244746  S5-244747  S5-244751  S5-244752  S5-244755  S5-244756  S5-244757 | pCR  pCR  pCR  pCR  pCR  pCR  pCR |  |  | pCR TR 28.879 Update concepts  pCR TR 28.879 Registration use case - update agreed content and add evaluation of solution 1  Rel-19 pCR TR 28.879 Updating the configuring discovery policy for an external MnS consumer use case  pCR TR 28.879 Discovery policy configuration - update solution 1 description and add evaluation  Rel-19 pCR TR 28.879 Add solution for authorization of the external MnS consumer to access the management service API use case  Rel-19 pCR TR 28.879 Evaluation analysis for authorization of the external MnS consumer to access the management service API use case  Rel-19 pCR TR 28.879 Evaluation analysis for Logging the management service API invocations to the CCF use case |  |
| 2024-09 | SA#105 | SP-241137 |  |  |  | Presented at SA#105 for Information | 1.0.0 |
| 2024-09 |  |  |  |  |  | After editHelp cleanup | 1.0.1 |
| 2024-10 | SA5#157 | S5-245616  S5-245617  S5-246038  S5-246283 | pCR  pCR  pCR  pCR |  |  | Rel-19 pCR TR 28.879 Update Introduction, add scope and remove clause 5.2 and 5.3  Rel-19 pCR TR 28.879 Addressing editHelp comments and Rapporteur cleanup  Rel-19 pCR TR 28.879 Clean up to clarify the roles of the MnS producer vs the MnF and differentiates between discovery info configuration and authorization  pCR TR 28.879 pCR TR 28.879 Publishing UC – updates on solution and evaluation | 1.1.0 |
| 2024-11 | SA5#158 | S5-247126  S5-247129  S5-247131  S5-247132  S5-247133  S5-247135  S5-247136  S5-247138 | pCR  pCR  pCR  pCR  pCR  pCR  pCR  pCR |  |  | pCR TR 28.879 Updates to clarify the role of CAPIF in the study  pCR TR 28.879 Update on exposure of management services through the CAPIF framework  Rel-19 pCR TR 28.879 Clean-up and enhancement of the registration UC to add MSEF as the API provider entity  pCR TR 28.879 Publishing UC - updates  pCR TR 28.879 Discovery UC - updates  pCR TR 28.879 Authorization UC - updates  Rel-19 pCR TR 28.879 Clean-up the Logging UC by adding the MSEF as the AEF entity  pCR TR 28.879 Conclusions and recommendations | 1.2.0 |
| 2024-12 | SA#106 | SP-241611 |  |  |  | Presentation to SA for Approval | 2.0.0 |
| 2024-12 | SA#106 |  |  |  |  | Upgrade to change control version | 19.0.0 |
| 2025-03 | SA#107 | SP-250149 | 0001 | 1 | F | Rel-19 CR TR 28.879 Fix inconsistencies | 19.1.0 |