**3GPP TSG-SA5 Meeting #155 *S5-243264d1***

Jeju, South Korea, 27 - 31 May 2024 Revision of S5-242836

**Source: Ericsson España S.A., Huawei**

**Title: pCR TR 28.879 Add and correct references**

**Document for: Approval**

**Agenda Item: 6.19.21**

# 1 Decision/action requested

***The group is asked to discuss and approve the proposal.***

# 2 References

[1] 3GPP TR 28.879, " Study on OAM for service management and exposure to external consumers".

# 3 Rationale

Among the study objectives in [1], WT-1 is focused on communication services and the relationship with network provisioning solutions such as network slicing, from concept and modelling viewpoints. The actual sub-objectives defined within WT-1 are detailed below:

“

* ***WT-1.1*** *Identify generic requirements for exposure of SA5 management services to external consumers, irrespective of the vertical industry.*
* ***WT-1.2*** *Identify 1) potential mechanisms to discover management service producers and their respective capabilities while leveraging as much as possible the existing solutions and extending where necessary. Compare existing solutions (e.g., CAPIF, EGMF, MnS Registry and/or MSAC) that could be leveraged. 2) procedures for exposure of management services based on CAPIF, EGMF, MnS Registry, MSAC or a combination thereof. Some of the identified gaps for use of CAPIF in SA5 are listed in S5-236381 clause 4.1.2.*
* ***WT-1.3*** *Identify potential requirements that would be provided to the access control (MSAC) work item.*
* ***WT-1.4*** *Study whether and how SA5 defined exposure mechanisms fit within the GSMA Open Gateway framework. This framework includes OPG, CAMARA and TM Forum*

”.

In SA5#154, TDoc S5-242008 was agreed. However, when implemented in the latest version of TR 28.879 [1], it can be noticed that this TDoc had:

* wrong pointers (to references listed in the bibliography) and missing references.
* Wrong references to stage 3 SS.

This pCR aims to fix this. It is related to WT-1.4.

# 4 Detailed proposal

It is proposed to make the following changes in the latest version of TR 28.879 [1].

|  |
| --- |
| **1st Change** |

# 2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 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: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2"

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

[7] 3GPP [TS 23.434](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3587): "Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows".

[8] 3GPP [TS 23.255](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3843): "Application layer support for Vehicle-to-Everything (V2X) services; Functional architecture and information flows".

[9] 3GPP [TS 23.286](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3562): "Application layer support for Uncrewed Aerial Systems (UAS) services; Functional architecture and information flows".

[10] 3GPP [TS 23.545](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3948): "Application layer support for Factories of the Future (FF) ".

[11] 3GPP [TS 23.542](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4156): "Application layer support for Personal IoT Networks".

[12] 3GPP [TS 23.554](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3818): "Application architecture for MSGin5G Service; Stage 2".

[13] 3GPP [TS 29.222](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3450): "Common API Framework for 3GPP Northbound APIs; stage 3".

[14] 3GPP [TS 33.122](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3420): "Security aspects of Common API Framework (CAPIF) for 3GPP Northbound APIs".

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

[16] "GSMA Operator Platform Group – Requirements and Architecture", version 5.0, July 2023 [[link](https://www.gsma.com/futurenetworks/wp-content/uploads/2023/07/OPG.02-v5.0-Operator-Platform-Requirements-and-Architecture.pdf)]

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

[18] 3GPP [TS 28.531](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3274): "Management and orchestration; Provisioning"

[19] 3GPP [TS 23.435](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4092): "Procedures for Network Slice Capability Exposure for Application Layer Enablement Service"

[a] 3GPP [TS 23.558](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3723): "Architecture for enabling Edge Applications"

[b] 3GPP [TS 28.550](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3411): "Management and orchestration; Performance assurance"

[c] 3GPP [TS 28.111](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4178): "Management and orchestration; Fault Management (FM)"

[d] 3GPP [TS 28.105](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3970): "Management and orchestration; Artificial Intelligence / Machine Learning (AI/ML) management"

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

[f] 3GPP [TS 28.541](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3400): "Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and 3"

[g] 3GPP [TS 28.312](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3554): "Management and orchestration; Intent driven management services for mobile networks"

[h] 3GPP [TS 28.538](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3910): "Management and orchestration; Edge Computing Management"

[i] 3GPP [TS 28.536](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3701): "Management and orchestration; Management services for communication service assurance; Stage 2 and 3"

|  |
| --- |
| **2nd Change** |

### 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.

A screenshot of a computer

Description automatically generated

Figure 4.1.3.1-1: 3GPP exposure framework (Figure extracted from [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. Common API Framework (CAPIF) is defined to manage access to all 3GPP APIs, in a consistent and uniform way with regards to publication, discovery and access control, among other functionalities. 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 TS 23.558 [a]:  - 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).  Note that the Edge Computing Layer only consumes network capability set from the 3GPP system (see Figure 4.1.3.1-1) |
| 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 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 TS 23.255 [8].  - drone applications known as uncrewed aerial systems (UAS), see TS 23.286 [9]  - Industry 4.0/OT applications, also referred to as factories of the future (FF), see TS 23.545 [10]  - Personal IoT networks, see TS 23.542 [11]  - Message communication in massive IoT, also referred to as MSGIn5G, see TS 23.554 [12]. |
| Common API Framework (CAPIF) | Started in Release 15, CAPIF services are listed in TS 23.222 [5] and specified in TS 29.222 [13] with security aspects being addressed in 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. |

#### 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 must make available for 3rd parties, to ensure global reach and scale. These must-be 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).

A screenshot of a computer

Description automatically generated

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.

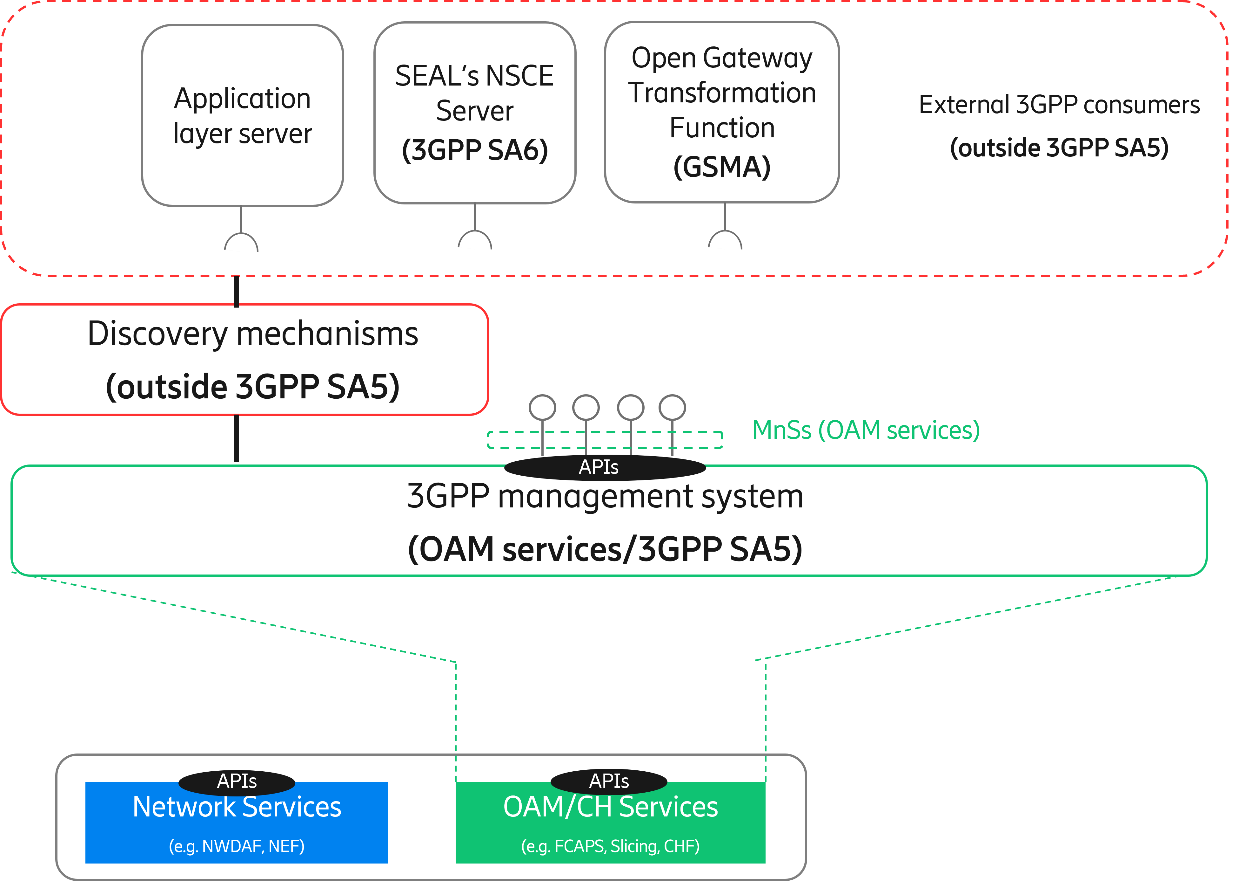


Figure 4.1.4-1: Examples of external MnS consumers.

`

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 a discovery mechanism defined outside SA5 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 TS 28.531 [18], and conceptually grouped under the NSCE-OAM interface in 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 a discovery mechanism defined outside SA5. |

It is worth noting that the functional entities represented as examples of external MnS consumers:

- 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”, when the discovery mechanism these entities use to gain access to MnSs is the mechanism provided by CAPIF.

|  |
| --- |
| **3rd Change** |

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 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 (TS 28.532 [17]) + PM control NRM fragment (TS 28.622 [3]) | X | X |
| CRUD operation (TS 28.532 [17]) + ManagementDataCollection NRM fragment (TS 28.622 [3]) | X | X |
| Measurement job control (TS 28.550 [b]) | X |  |
| Performance data report | CRUD operations (TS 28.532 [17]) + PM control NRM fragment (TS 28.622 [3]) | X | X |
| File data reporting service (TS 28.532 [17]) | X |  |
| Streaming data reporting service (TS 28.532 [17]) | X |  |
| Performance data monitoring | CRUD operations (TS 28.552) + Threshold monitoring control NRM fragment (TS 28.622 [3]) | X | X |
| Trace/MDT data collection control | CRUD operations (TS 28.532 [17]) + Trace control NRM fragment (TS 28.622 [3]) | X | X |
| CRUD operation + ManagementDataCollection NRM fragment (TS 28.622 [3]) | X | X |
| Trace/MDT data report | File data reporting service (TS 28.532 [17]) | X |  |
| CRUD operations (TS 28.532 [17]) + File retrieval NRM fragment (TS 28.622 [3]) | X | X |
| Streaming data reporting service (TS 28.532 [17]) |  |  |
| Fault data control | CRUD operations (TS 28.532 [17]) + FM control NRM fragment (TS 28.111 [c]) | X | X |
| Fault supervision data control service (TS 28.532 [17]) |  |  |
| Fault data report | CRUD operations (TS 28.532 [17]) + FM control NRM fragment (TS 28.111 [c]) | X | X |
| Fault supervision data report service (TS 28.532 [17]) |  |  |
| QoE control | CRUD operations (TS 28.532 [17]) + QMC control NRM fragment (TS 28.532 [17]) | X | X |
| Service registry and discovery | CRUD operations (TS 28.532 [17]) + MnS Registry NRM fragment (TS 28.622 [3]) | X | X |
| Subscription | CRUD operations (TS 28.532 [17]) + Notification subscription control NRM fragment (TS 28.622 [3]) | X | X |
| AI/ML management | CRUD operations (TS 28.532 [17]) + ML Training NRM fragment (TS 28.105 [d]) | X |  |
| Management Data Analytics | CRUD operations (TS 28.532 [17]) + MDA request & report NRM fragment (TS 28.104 [e]) | X |  |
| NR Provisioning | CRUD operations (TS 28.532 [17]) + NR NRM fragment (TS 28.541 [f]) | X | X |
| 5GC Provisioning | CRUD operations (TS 28.532 [17]) + 5GC NRM fragment (TS 28.541 [f]) | X | X |
| Network Slice Provisioning | CRUD operations (TS 28.532 [17]) + Network slice NRM fragment (TS 28.541 [f]) | X | X |
| Network slicing provisioning service (TS 28.531 [18]) | X |  |
| SON Policy | CRUD operations (TS 28.532 [17]) + NRM fragments for DANR/ DES/ DRACH/ DMRO/ DPCI/ CES / CPCI/ DLBO / CCO management (TS 28.541 [f]) | X | X |
| Intent Driven Management | CRUD operations (TS 28.532 [17]) + Intent NRM fragment (TS 28.312 [g]) | X |  |
| Edge Computing Provisioning | CRUD operations (TS 28.532 [17]) + Edge NRM fragment (TS 28.538 [h]) | X |  |
| Communication Service Assurance | CRUD operations (TS 28.532 [17]) + Assurance NRM fragment (TS 28.536 [i]) | X |  |

|  |
| --- |
| **End of Changes** |