ETSI TS 128 533 V19.3.0 (2025-10)

TECHNICAL SPECIFICATION

5G;
Management and orchestration;
Architecture framework
(3GPP TS 28.533 version 19.3.0 Release 19)

Reference
RTS/TSGS-0528533vj30

Keywords
5G

ETSI

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

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

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

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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

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

The cross reference between 3GPP and ETSI identities can be found at 3GPP to ETSI numbering cross-referencing.

Modal verbs terminology

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

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

Contents

Intellectual Property Rights 2
Legal Notice 2
Modal verbs terminology 2
Foreword 5
Introduction 5
1 Scope 6
2 References 6
3 Definitions and abbreviations 9
3.1 Definitions 9
3.2 Abbreviations 10
4 Service Based Management Architecture (SBMA) 10
4.1 Management Services (MnS) 10
4.2 MnS components 11
4.2.1 Introduction 11
4.2.2 MnS component type A 11
4.2.3 Management information 11
4.2.3.1 MnS component type B 11
4.2.3.2 MnS component type C 11
4.2.4 MnS producer profile 11
4.3 Combination of MnS components 11
4.4 Management capability exposure governance 12
4.5 Management Function (MnF) concept 13
4.6 Management data analytics capability 15
4.7 Management service discovery 16
4.7.1 Introduction 16
4.7.2 Void 16
4.7.3 MnS discovery service 16
4.8 Management capability support in multiple tenant environment 16
4.9 Access control capability 16
4.9.1 Authentication service 16
4.9.2 Authorization service 17
5 Architecture reference model 18
5.1 General concepts 18
5.1.1 Management service producers, consumers and exposure 18
5.1.2 Interactions between management service producer and management service consumer 19
5.2 Management interactions with NFV MANO 22
5.3 Management service deployment based on ZSM framework 22
5.4 Management interactions with NWDAF 23
5.5 Using Management Services to support multiple players interoperability 23
6 Void 25
Annex A (informative): Example of deployment model with utilization of management services 26
A.1 Utilization of Management services in network and subnet layers 26
A.2 Utilization of management services in network function management 26
A.3 Utilization of management services by Exposure Governance Management Function (EGMF) 27
A.4 Utilization of interface to NFV-MANO by the producer of management services 28
A.5 Management Data Analytics Service (MDAS) 29
A.6 Utilization of management services in functional management architecture 30

A.7 Utilization of management data analytics services 31
A.8 An example of deployment scenario for network and network slice 31
A.9 Deployment examples of ONAP platform consuming 3GPP MnS(s) 33
A.9.1 Integration with ONAP DCAE collection framework utilizing 3GPP MnS(s) 33
A.9.2 Integration with ONAP controller utilizing 3GPP MnS(s) 33
A.10 Management domain provided management services mapped with ZSM 34
A.11 Illustrative architecture reference model for management and orchestration 35
A.12 Summary and capabilities of the architecture reference model for management and orchestration 37
A.12.1 ML Training Function (MLTRF) 37
A.12.2 ML Testing Function (MLTEF) 37
A12.3 ML Emulation Function (MLEMF) 38
A.12.4 Management Data Analytics Function (MDAF) 38
A.12.5 Intent Handling Function (IHF) 38
A.12.6 UE Data Handling Function (UDHF) 39
A.12.7 Performance Management Function (PMF) 39
A.12.8 Fault Management Function (FMF) 40
A.12.9 Data Management Function (DMF) 40
A.12.10 Provisioning Function (PRF) 41
A.12.11 Network Digital Twin Function (NDTF) 41
A.12.12 Closed Control Loop Function (CCLF) 41
Annex B (normative): Solutions for management of 5G network and network slicing 43
Annex C (informative): Example of mapping Management Services (MnS) to pre-Rel-15 management framework 44
Annex D (normative): Access control workflow 45
D.1 Explicit authentication and authorization 45
D.2 Implicit authentication and authorization 47
Annex E (informative): 5G specifications overview 49
Annex F (informative): Overview of management capabilities and corresponding solution sets in SBMA 52
Annex G (informative): Change history 55
History 58

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

Introduction

The management of the 3GPP network is provided by management services. The service based architecture and interfaces support various management services of vastly different requirements on network configuration, network performance, and network fault supervision. The 3GPP network management architecture evolves supporting operators' design and management of their service oriented networks.

1 Scope

The present document defines the network management and orchestration architecture SBMA for 3GPP networks including network slicing. The use cases and requirements are specified in TS 28.530 [3].
SBMA applies to 5G.

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] Void

[3] 3GPP TS 28.530: "Management and orchestration of networks and network slicing; Concepts, use cases and requirements".

[4] 3GPP TS 28.541: "Management and orchestration of 5G networks; Network Resource Model (NRM); Stage 2 and stage 3".

[5] 3GPP TS 28.552: "Management and orchestration of 5G networks; Performance measurements".

[6] 3GPP TS 28.554: "Management and orchestration of 5G networks; 5G End to end Key Performance Indicators (KPI)".

[7] 3GPP TS 32.425: "Telecommunication management; Performance Management (PM); Performance measurements Evolved Universal Terrestrial Radio Access Network (E-UTRAN)".

[8] 3GPP TS 28.531: "Management and orchestration of 5G networks; Provisioning".

[9] 3GPP TS 28.532: "Management and orchestration; Generic management services".

[10] 3GPP TS 28.500: "Telecommunication management; Management concept, architecture and requirements for mobile networks that include virtualized network functions"

[11] 3GPP TS 28.510: "Telecommunication management; Configuration Management (CM) for mobile networks that include virtualized network functions; Requirements".

[12] 3GPP TS 28.511: "Telecommunication management; Configuration Management (CM) for mobile networks that include virtualized network functions; Procedures".

[13] 3GPP TS 28.512: "Telecommunication management; Configuration Management (CM) for mobile networks that include virtualized network functions; Stage 2".

[14] 3GPP TS 28.513: "Telecommunication management; Configuration Management (CM) for mobile networks that include virtualized network functions; Stage 3".

[15] 3GPP TS 28.515: "Telecommunication management; Fault Management (FM) for mobile networks that include virtualized network functions; Requirements".

[16] 3GPP TS 28.516: "Telecommunication management; Fault Management (FM) for mobile networks that include virtualized network functions; Procedures".

[17] 3GPP TS 28.517: "Telecommunication management; Fault Management (FM) for mobile networks that include virtualized network functions; Stage 2".

[18] 3GPP TS 28.518: "Telecommunication management; Fault Management (FM) for mobile networks that include virtualized network functions; Stage 3".

[19] 3GPP TS 28.520: "Telecommunication management; Performance Management (PM) for mobile networks that include virtualized network functions; Requirements".

[20] 3GPP TS 28.521: "Telecommunication management; Performance Management (PM) for mobile networks that include virtualized network functions; Procedures".

[21] 3GPP TS 28.522: "Telecommunication management; Performance Management (PM) for mobile networks that include virtualized network functions; Stage 2".

[22] 3GPP TS 28.523: "Telecommunication management; Performance Management (PM) for mobile networks that include virtualized network functions; Stage 3".

[23] 3GPP TS 28.525: "Telecommunication management; Life Cycle Management (LCM) for mobile networks that include virtualized network functions; Requirements".

[24] 3GPP TS 28.526: "Telecommunication management; Life Cycle Management (LCM) for mobile networks that include virtualized network functions; Procedures".

[25] 3GPP TS 28.527: "Telecommunication management; Life Cycle Management (LCM) for mobile networks that include virtualized network functions; Stage 2".

[26] 3GPP TS 28.528: "Telecommunication management; Life Cycle Management (LCM) for mobile networks that include virtualized network functions; Stage 3".

[27] ETSI GS NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV V1.3.1 (2018-01)".

[28] Void.

[29] ETSI GS ZSM 002: "Zero-touch Network and Service Management (ZSM); Reference Architecture V.1.1.1 (2019-08)".

[30] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[31] 3GPP TS 23.501: "System Architecture for the 5G system".

[32] 3GPP TS 28.622: "Telecommunication management; Generic Network Resource Model (NRM) Integration Reference Point (IRP); Information Service (IS)".

[33] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[34] IETF RFC 4253: "The Secure Shell (SSH) Transport Layer Protocol".

[35] 3GPP TS 28.100: "Management and orchestration; Levels of autonomous network".

[36] 3GPP TS 28.533: "Management and orchestration; Architecture framework".

[37] 3GPP TS 28.535: "Management services for communication service assurance; Requirements".

[38] 3GPP TS 28.536: "Management services for communication service assurance; Stage 2 and stage 3".

[39] 3GPP TS 28.537: "Management and orchestration; Management capabilities".

[40] 3GPP TS 28.538: "Management and orchestration; Edge Computing Management".

[41] 3GPP TS 28.540: "Management and orchestration; 5G Network Resource Model (NRM); Stage 1".

[42] 3GPP TS 28.550: "Management and orchestration; Performance assurance".

[43] 3GPP TS 32.421: "Telecommunication management; Subscriber and equipment trace; Trace concepts and requirements".

[44] 3GPP TS 32.422: "Telecommunication management; Subscriber and equipment trace; Trace control and configuration management".

[45] 3GPP TS 32.423: "Telecommunication management; Subscriber and equipment trace; Trace data definition and management".

[46] 3GPP TS 28.312: "Management and orchestration; Intent driven management services for mobile networks".

[47] 3GPP TS 28.557: "Management and orchestration; Management of Non-Public Networks (NPN); Stage 1 and stage 2".

[48] 3GPP TS 28.404: "Telecommunication management; Quality of Experience (QoE) measurement collection; Concepts, use cases and requirements".

[49] 3GPP TS 28.405: "Telecommunication management; Quality of Experience (QoE) measurement collection; Control and configuration".

[50] 3GPP TS 28.406: "Telecommunication management; Quality of Experience (QoE) measurement collection; Information definition and transport".

[51] 3GPP TS 28.631: "Telecommunication management; Inventory Management (IM) Network Resource Model (NRM) Integration Reference Point (IRP); Requirements".

[52] 3GPP TS 28.632: "Telecommunication management; Inventory Management (IM) Network Resource Model (NRM) Integration Reference Point (IRP); Information Service (IS)".

[53] 3GPP TS 28.633: "Telecommunication management; Inventory Management (IM) Network Resource Model (NRM) Integration Reference Point (IRP); Solution Set (SS) definitions".

[54] 3GPP TS 28.623: "Telecommunication management; Generic Network Resource Model (NRM) Integration Reference Point (IRP); Solution Set (SS) definitions".

[55] 3GPP TS 32.130: "Telecommunication management; Network sharing; Concepts and requirements".

[56] 3GPP TS 28.310: "Management and orchestration; Energy efficiency of 5G".

[57] 3GPP TS 28.104: "Management and orchestration; Management Data Analytics (MDA)".

[58] 3GPP TS 28.313: "Management and orchestration; Self-Organizing Networks (SON) for 5G networks".

[59] 3GPP TS 28.314: "Management and orchestration; Plug and Connect; Concepts and requirements".

[60] 3GPP TS 28.315: "Management and orchestration; Plug and Connect; Procedure flows".

[61] 3GPP TS 28.316: "Management and orchestration; Plug and Connect; Data formats".

[62] 3GPP TS 28.555: "Management and orchestration; Network policy management for 5G mobile networks; Stage 1".

[63] 3GPP TS 28.556: "Management and orchestration; Network policy management for 5G mobile networks; Stage 2 and stage 3".

[64] ETSI GS NFV-IFA 008 (V4.3.1): "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Ve-Vnfm reference point - Interface and Information Model Specification".

[65] ETSI GS NFV-IFA 013 (V4.3.1): "Network Function Virtualisation (NFV) Release 4; Management and Orchestration; Os-Ma-nfvo reference point - Interface and Information Model Specification".

[66] 3GPP TS 28.105: "Management and orchestration; Artificial Intelligence / Machine Learning (AI/ML) management".

[67] 3GPP TS 28.317: "Management and orchestration;Self-configuration of Radio Access Network Entities (RAN NEs)".

[68] 3GPP TS 28.111: "Management and orchestration; Fault management (FM)".

[69] 3GPP TS 28.318: "Management and Orchestration; Network and services operations for energy utilities".

[70] 3GPP TS 28.319: "Management and orchestration; Access Control for Management services".

[71] 3GPP TS 26.247: "Transparent end-to-end Packet-switched Streaming Service (PSS); Progressive Download and Dynamic Adaptive Streaming over HTTP (3GP-DASH)"

[72] 3GPP TS 28.558: "Management and Orchestration UE level measurements for 5G system"

[73] 3GPP TS 28.561: "Management and orchestration; Management aspects of Network Digital Twins"

[74] 3GPP TS 28.567: "Management and orchestration; Management aspects of closed control loops"

[75] 3GPP 29.501: "5G System; Principles and Guidelines for Services Definition"

[76] 3GPP TS 23.222: "Common API Framework for 3GPP Northbound APIs; Stage 2"

[77] 3GPP TS 28.579: "Management and orchestration; Management services exposure to external consumers through CAPIF"

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions 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] or NFV-MANO [27].

Exposure governance management function: Management Function entity with the role of management service exposure governance.

Management Service (MnS): set of offered management capabilities.

External MnS consumer: MnS consumer outside the PLMN trust domain.

Internal MnS consumer: MnS consumer within the PLMN trust domain.

NOTE: the concept of PLMN trust domain is defined in TS 23.222 [76].

Management Function (MnF): logical entity playing the roles of Management Service consumer and/or Management Service producer.

Network Function (NF): defined in TS 23.501[31].

NOTE: In 3GPP NRM, the Network Functions are modeled using the ManagedFunction IOC and its sub-classes (e.g. AMFFunction).

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1], TS 28.530 [3], in NFV-MANO [27] 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].

CM	Configuration Management
LCM	Lifecycle Management
MDAS	Management Data Analytics Service
MnF	Management Function
MnS	Management Service
NF	Network Function
NFV-MANO	Network Functions Virtualisation Management and Orchestration
PM	Performance Management
SBMA	Service Based Management Architecture

4 Service Based Management Architecture (SBMA)

4.1 Management Services (MnS)

The fundamental building block of the Service Based Management Architecture (SBMA) is the Management Service (MnS). An MnS is a set of offered capabilities for management and orchestration of network and services. The entity producing an MnS is called MnS producer. The entity consuming an MnS is called MnS consumer.

An MnS producer offers its MnS via a standardized service interface composed of individually specified MnS components. This service interface is represented in Figure 4.1.1. The MnS offering is depicted with a circle symbol attached by a solid line to the MnS producer. The MnS consumption is depicted with a socket symbol attached by a solid line to the MnS consumer.

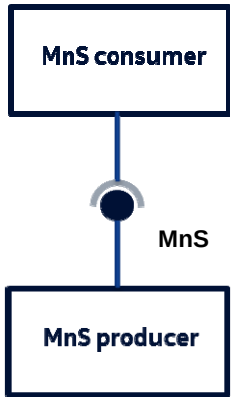


Figure 4.1.1: MnS producer and MnS consumer

4.2 MnS components

4.2.1 Introduction

An MnS is specified using different independent components. A concrete MnS is composed of at least two of these components. Three different component types are defined, called MnS component type A, MnS component type B and MnS component type C. These components are defined in the following clauses 4.2.2 and 4.2.3.

4.2.2 MnS component type A

The MnS component type A is a group of management operations and/or notifications that is agnostic with regard to the entities managed. The operations and notifications as such are hence not involving any information related to the managed network. These operations and notifications are called generic or network agnostic.

For example, operations for creating, reading, updating and deleting managed object instances, where the managed object instance to be manipulated is specified only in the signature of the operation, are generic.

4.2.3 Management information

4.2.3.1 MnS component type B

MnS component type B refers to management information represented by information models representing the managed entities. A MnS component type B is also called Network Resource Model (NRM).

MnS component type B examples are:

1) Network resource models as defined in TS 28.622 [32].

2) Network resource models as defined in TS 28.541 [4].

4.2.3.2 MnS component type C

MnS component type C is performance information of the managed entity and fault information of the managed entity.

The following are examples of Management service component type C:

1. Alarm information as defined in TS 28.111 [68].

2. Performance data as defined in TS 28.552 [5], TS 28.554 [6] and TS 32.425 [7].

4.2.4 MnS producer profile

A MnS producer is described by a set of meta data called MnS producer profile. The profile holds information about the supported MnS components and their version numbers. This may include also information about support of optional features. For example, a read operation on a complete subtree of managed object instances may support applying filters on the scoped set of objects as optional feature. In this case the MnS profile should include the information if filtering is supported.

In the context of SBMA, the MnS version can be used to identify the operations (component A) available for an MnS consumer to communicate with a specific version of an MnS producer.

An MnS version number shall consist of at least 3 fields following a MAJOR.MINOR.PATCH pattern as defined in TS 29.501 [75], clause 4.3.1.1.

4.3 Combination of MnS components

An MnS is composed by an MnS component type A and

- an MnS component type B, or

- an MnS component type B and an MnS component type C.

The instances of management services carry information about specified management service components in the metadata attributes. Figure 4.3.1.illustrates examples of management service instances with various management service components of type A, type B and type C:

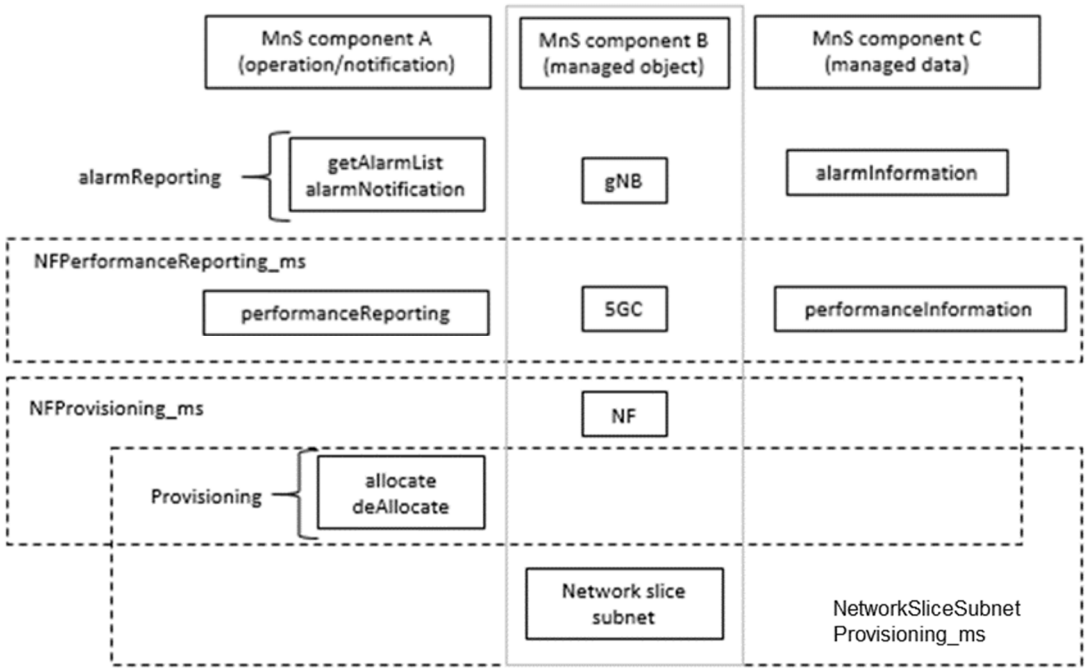


Figure 4.3.1: Examples of Management Service instances and their corresponding MnS component type A, B and C

One instance of a MnS may comprise MnS components of different versions.

4.4 Management capability exposure governance

As precondition for Management Service exposure governance offer, producer of management capability exposure governance should have access to:

An association between information about specified management service components and instances of management services.

NOTE: The detail creation of an association is left for implementation and out of scope of 3GPP standardization.

Management capability exposure governance provides exposure governance on basic elements of management function service based interface:

1) Management service component type A
2) Management service component type B
3) Management service component type C

As described in Figure 4.4.1 left hand part, when there is a Management Service A exposure without exposure governance, Management Service A Consumer (e.g. 3rd party) can access all management capability offered by Management Service A Producer.

As described in Figure 4.4.1 right hand part, when Management Service A is exposed with applied exposure governance it becomes Management Service A'. Management Service A' Consumer can access Management Service A' after following steps:

- Management Service A, exposed by Management Service A Producer, is consumed by Management Service A Consumer;

- Management Service B, exposed by Management Service B Producer, is consumed by Management Service B Consumer (e.g. operator) who is authorized to access offered management capabilities exposure governance(s);

- Management Service B Consumer (e.g. operator) request a specified exposure governance on Management Service A;

- Management Service A' Producer produces Management Service A' based on applied exposure governance on consumed Management Service A.

NOTE: The Management Service A Consumer, the Management Service A' Producer and Management Service B Producer can be represented as a single Management Function e.g. a single MnF).

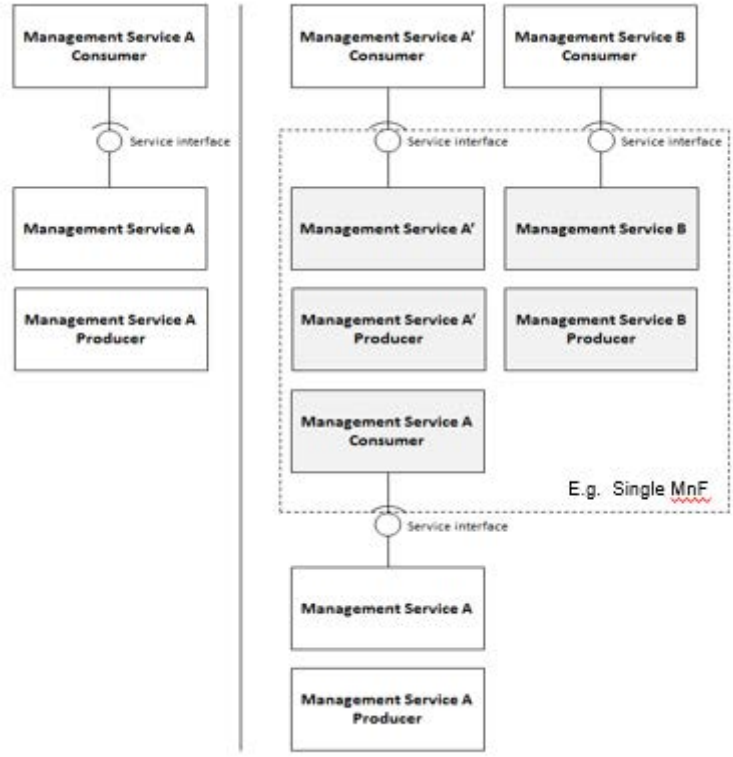


Figure 4.4.1: Management capability exposure governance applied on exposed Management Service A

4.5 Management Function (MnF) concept

A Management Function (MnF) is a logical entity playing the roles of MnS consumer and/or MnS producer.

A Management Service produced by MnF may have multiple consumers. The MnF may consume multiple Management Services from one or multiple Management Service producers. An example of a MnF playing both roles (Management Service producer and consumer) illustrated in the figure 4.5.1 below.

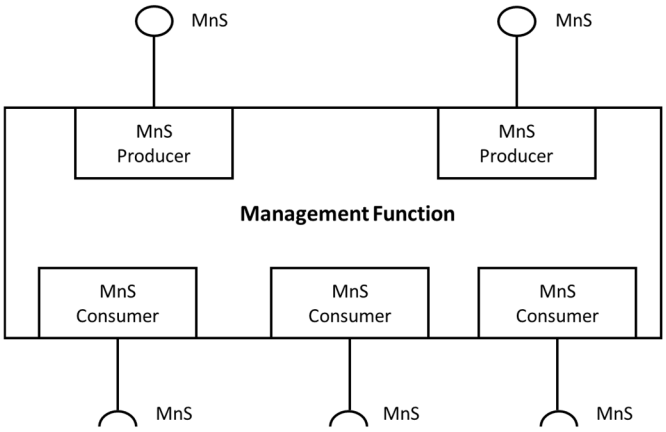


Figure 4.5.1: Example of Management Function and Management Services

A Management Function can be deployed as a separate entity or embedded in Network Function to provide MnS(s). Following figure 4.5.2 shows an example (on the left) in which a MnF deployed as a separate entity to provide MnS(s) and another example (on the right) in which a MnF is embedded in a Network Function to provide MnS(s):

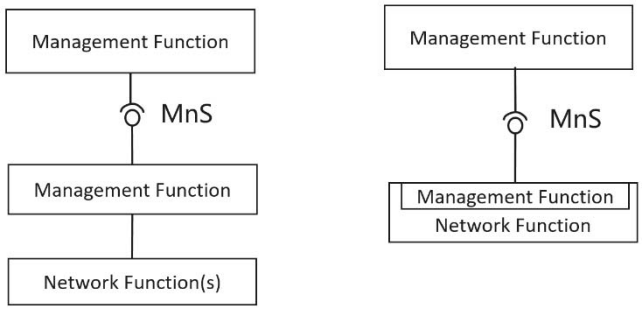


Figure 4.5.2 Examples of MnS deployment scenario

Management Functions may interact by consuming Management Services produced by other Management Functions. The figure 4.5.3 below illustrates multiple scenarios:

- MnF1 produces Management Service MnS-a;
- MnF2 consumes Management Service MnS-a produced by MnF1 and produces Management Services MnS-b and MnS-c;
- MnF3 produces Management Service MnS-c;
- MnF4 consumes Management Service MnS-b produced by the MnF2;
- MnF5 consumes Management Services MnS-c produced by the MnF2 and MnF3, and in turn produces the same Management Service MnS-c. The behaviour of MnF5 may be seen as aggregation of Management Services MnS-c.

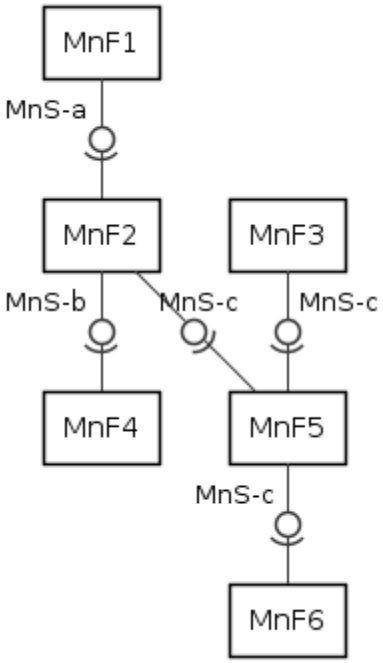


Figure 4.5.3: An example of interactions between Management Functions

NOTE: The specification of a MnF is out of scope of the present document.

4.6 Management data analytics capability

Mobile networks have the capability to support a wide variety of services and requirements. This, along with increasing flexibility of the network may present management and operational challenges and complexities. The management system can therefore benefit from management data analytics services for improving networks performance and efficiency to accommodate and support the diversity of services and requirements. The management data analytics utilize the network management data collected from the network (including e.g. service, slicing and/or network functions related data) and make the corresponding analytics based on the collected information. The information provided by PM analytics can be used to optimize network performance, and the information provided by FM analytics can be used to predict and prevent failures of the network. MDAF can be deployed at different levels, for example, at a domain level (e.g. RAN, CN, network slice subnet) and/or in a centralized manner (e.g. at a PLMN level).

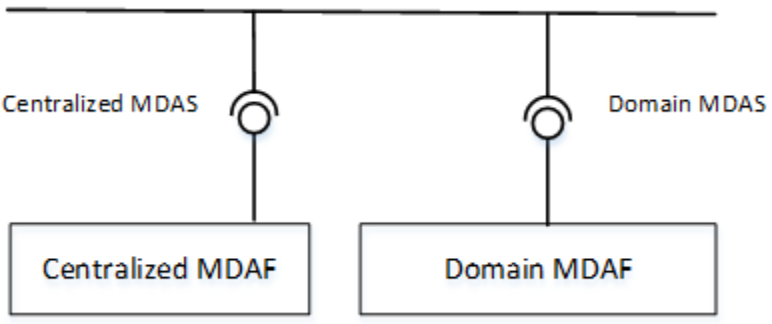


Figure: 4.6.1: Service based architecture for management data analytics

4.7 Management service discovery

4.7.1 Introduction

The MnS consumer in an operator's management system need to discover the availability of MnS instances provided by other MnS producer(s). In order to enable the MnS instances to be discovered by MnS consumer, the MnS needs to be discoverable to the operator's management system when the MnS instance become operative.

4.7.2 Void

4.7.3 MnS discovery service

The MnS discovery service enables MnS consumer to discover management capabilities of MnS producer(s).

4.8 Management capability support in multiple tenant environment

In a 3GPP management system, a tenant represents a group of MnS consumers associated with the management capabilities they are allowed to access and consume. The 3GPP management system provides multi-tenancy support, by associating different tenants with different sets of management capabilities. Every tenant may be authorized to access and consume those MnSs that the operator makes available to this tenant based on SLA.

4.9 Access control capability

4.9.1 Authentication service

Authentication service producer provides identity management capabilities to provision MnS consumer/producer, group of MnS consumers/producers and authentication policies for the identities.

Authentication service producer provides capabilities for authentication of MnS consumer explicitly or implicitly.

NOTE 1: Explicit authentication: MnS consumer interacts directly with authentication service producer to acquire authentication assertion to interact with MnS producer or authorization service producer.

NOTE 2: Implicit authentication: MnS consumer interacts indirectly with authentication via MnS producer, to establish a secure session.

NOTE 3: Certificate issued by trusted CA is used by MnS consumer/producer to authenticate the authentication service producer. E.g. a MnS consumer access the authentication service through Transport Layer Security (TLS) (see [33]), then the MnS consumer/producer could authenticate the producer through validating the signature signed with certificate of the producer issued by the trusted CA.

NOTE 4: Generally, certificate issued by trusted CA is used by MnS consumer to authenticate a MnS producer. E.g. when a MnS consumer accesses the MnS through TLS (see [33]) or SSH (see [34]), the MnS consumer could authenticate the MnS producer through validating the signature signed with certificate of the producer issued by the trusted CA.

Authentication Service producer can be deployed at different levels, for example, at a domain level (e.g. in RAN, CN, domain) and/or in a centralized manner (e.g. at a PLMN level).

NOTE 5: If the MnS consumer and the MnS producer to be accessed are inside the same domain, Authentication Service producer may be deployed at domain level to support authenticating the MnS consumer explicitly or implicitly. If the MnS consumer and the MnS producer to be accessed are in the different domain, Authentication Service producer is deployed in a centralized manner to support authenticating the MnS consumer explicitly or implicitly.

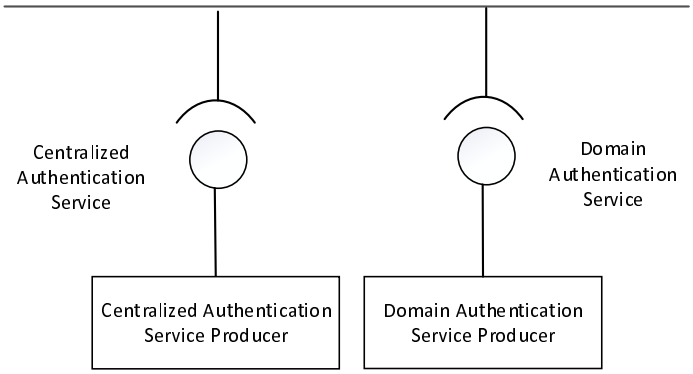


Figure 4.9.1-1: Authentication capability on service based architecture

4.9.2 Authorization service

Authorization service producer provides management capabilities to provision access permissions on MnSs for a MnS consumer or a group of MnS consumers.

Authorization service producer provides capabilities to grant permissions to a MnS consumer explicitly or implicitly.

NOTE 1: Explicit authorization : MnS consumer interacts with authorization service producer, to acquire access token to interact with MnS Producer. MnS Producer enforces access control by verifying the access token. A token may include a list of permissions with conditions and a digital signature signed by the authorization service producer.

NOTE 2: Implicit authorization : MnS Producer enforces access control using local policies which might be preconfigured locally or synchronized from centralized authorization service producer for the current authentication context.

Authorization Service producer can be deployed at different levels, for example, at a domain level (e.g. in RAN, CN, domain) and/or in a centralized manner (e.g. at a PLMN level). The Centralized Authorization Service producer can be named as Cross Domain Authorization Service producer.

NOTE 3: Authorization Service producer may be deployed at domain level to support access control between MnS consumer and producer inside the same domain. Specifically, an domain Authorization Service producer may be deployed together with management service producer. Authorization Service producer is deployed in a centralized manner to especially to support access control between MnS consumer and producer from different domains.

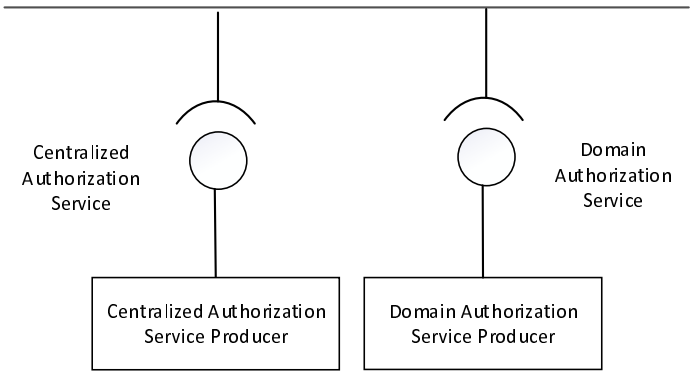


Figure 4.9.2-1 Authorization capability on service based architecture

5 Architecture reference model

5.1 General concepts

5.1.1 Management service producers, consumers and exposure

The management services for a mobile network with or without network slicing may be produced by any entity. For example, it can be a Network Functions (NF), or network management functions. The entity may provide (produce) such management services as, for example, the performance management services, configuration management services and fault supervision services.

The management services can be consumed by another entity, which may in turn produce (expose) the service to other entities. Figure 5.1.1-1 shows an example of the management service X which is initially produced by the entity A which is an NF , then consumed by another entity B which is a network management function. Then entity B in turn exposes it to the entity C.

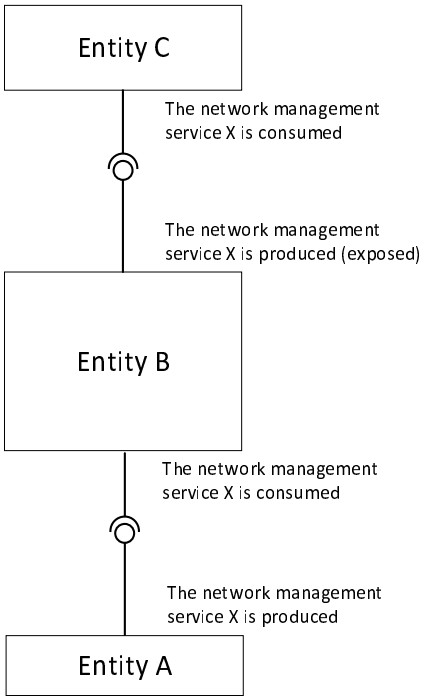


Figure 5.1.1-1. Example of producers and consumers of the management service

Figure 5.1.1-2 shows another example of the management service X which is produced by the entity A which is a NF, then entity B processes the information and produce management service Y and exposes it to the entity C.

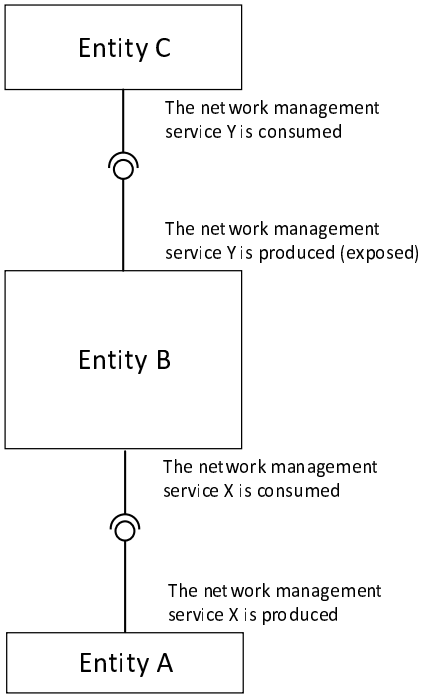


Figure 5.1.1-2. Example of producers and consumers of management services

5.1.2 Interactions between management service producer and management service consumer

The interactions between the management service producer and management service consumer follows one of the three following paradigms:

- "Request-response": A management service producer is requested by a management service consumer to invoke an operation, which either performs an action or provides information or both. The management service producer provides response based on the request by management service consumer.

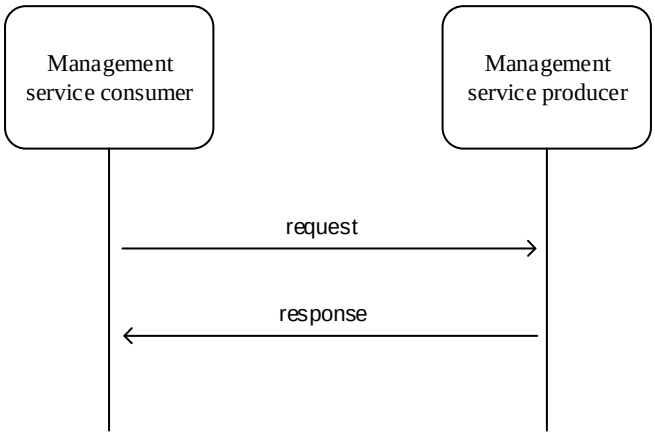


Figure 5.1.2.1: Request-response communication paradigm

- "Subscribe-notify": A management service consumer requests a management service producer to establish a subscription to receive network events via notifications, under the filter constraint specified in this operation.

  Subscriptions can be created also by other means than by using such operation.

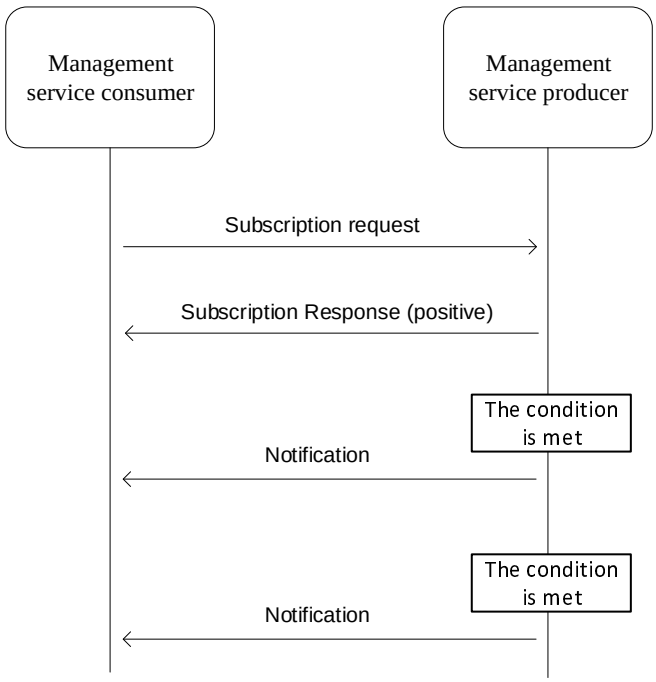


Figure 5.1.2.2: Subscribe-notify communication paradigm

NOTE: Example of a common aspect applicable to all management services is the use of notifications. For a management service to use notifications the management service consumer needs a subscription to notifications it is interested in. The management service consumer requests the creation of a subscription by sending a subscribe operation to the management service producer. To cancel a subscription the consumer sends an unsubscribe operation to the producer.

- "Connect-streaming": A management producer is provided with the address the management service consumer. The management service producer requests to establish a connection with the management service consumer for management data streaming. The management service producer sends the management data, when they are ready, by streaming to the management service consumer over the established connection.

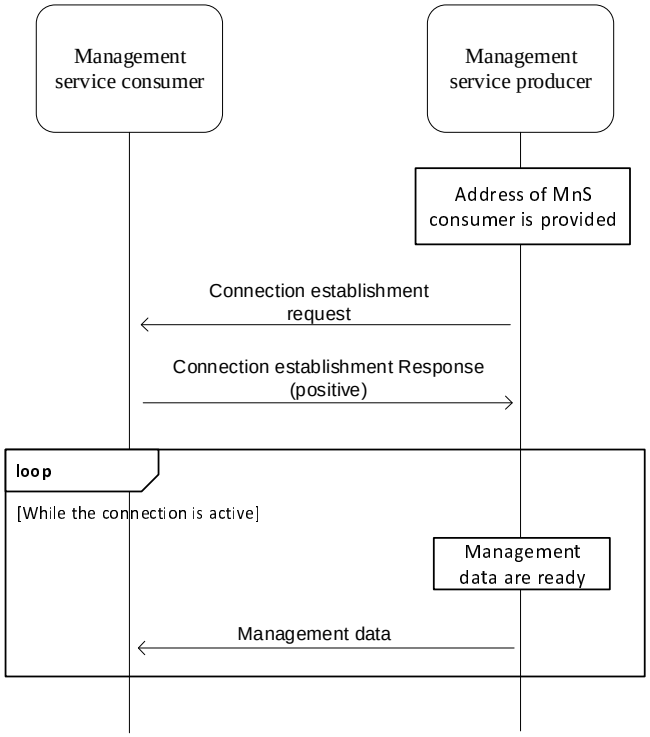


Figure 5.1.2.3: Connect-streaming communication paradigm

- "Request-response with access control" in explicit authentication and authorization mode: An authentication service producer is requested by a management service consumer for authentication, the authentication service producer authenticates the management service consumer according to information in the request, authentication policies and other information associated to the identity of the management service consumer. After being successfully authenticated, the management service consumer may send request to an authorization service producer to get access token for permissions. After getting access token from an authorization service producer, the management service consumer sends request to corresponding management service producers to access management services. The management service producer provides response to the consumer after verifying the access token. Figure 5.1.1.2-4 depicted typical Request-response communication paradigm with access control explicit authentication and authorization mode

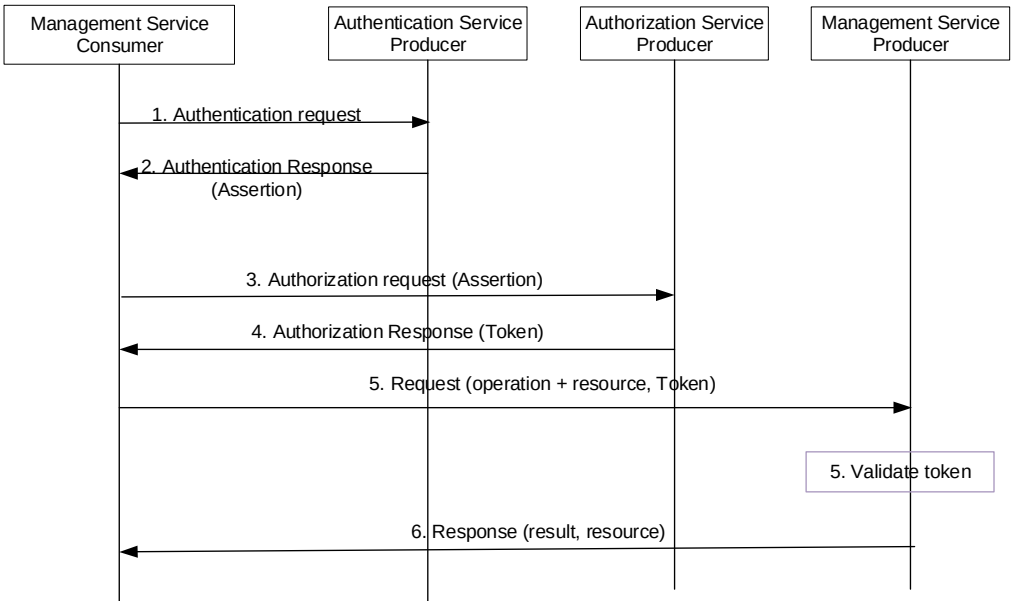


Figure 5.1.1.2-4: Request-response communication paradigm with access control (explicit authentication and authorization)

- "Request-response with access control" in implicit authentication and authorization mode: management service consumer initiates a management session towards management service producer. Management service producer accesses authentication service producer to authenticate the management service consumer according to information in the request, groups and other information associated to the identity of the management service consumer. After successfully being authenticated, the management service consumer sends request to management service producer to access management services, management service producer enforces access control using local policies applicable for the current authentication context

  NOTE: If Authentication Service Producer is unavailable, MnS Producer may opt to perform local authentication.

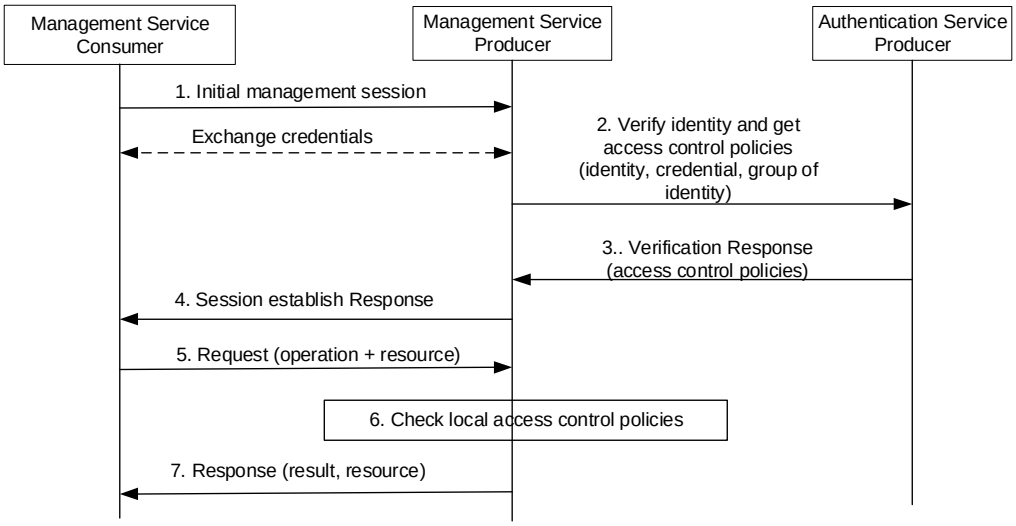


Figure 5.1.1.2-5: Request-response communication paradigm with access control (implicit authentication and authorization)

5.2 Management interactions with NFV MANO

3GPP management system shall be capable to consume NFV MANO interface (e.g. Os-Ma-nfvo, Ve-Vnfm-em and Ve-Vnfm-vnf reference points).

Producer of management services can consume management interfaces provided by NFV MANO for following purposes:

- Network service LCM.
- VNF LCM, PM, FM, CM on resources supporting VNF.

5.3 Management service deployment based on ZSM framework

ZSM framework reference architecture is described in ETSI GS ZSM 002 [29]. The ZSM framework reference architecture defines a set of architectural building blocks that collectively enable construction of more complex management services and management functions using a consistent set of composition and interoperation patterns. So it is important to show the 3GPP Management Service deployment based on ZSM Framework.Figure 5.3-1 shows an example of 3GPP Management Service deployment based on ZSM framework reference architecture. In this example:

- 3GPP Cross Management Domain (A bundle of Cross Domain MnFs) provides a set of MnS(s) for Cross Domain Network (including Network Slice) and consumes MnSs provided by the RAN Management Domain and the CN Management Domain. 3GPP Cross Management Domain can implement close loop (s) within the domain. 3GPP Cross Management Domain is a part of E2E Service Management Domain in ETSI ZSM Framework.
- RAN Management Domain (A bundle of RAN MnFs) provides a set of MnS(s) for the RAN SubNetwork and NF. RAN Management Domain can implement close loop(s) within the domain. RAN Management Domain is a Management Domain in ETSI ZSM Framework.
- CN Management Domain (A bundle of CN MnFs) provides a set of MnS(s) for the CN SubNetwork and NF. CN Management Domain can implement close loop(s) within the domain. CN Management Domain is a Management Domain in ETSI ZSM Framework.
- A 3GPP Management Framework Consumer (e.g. vertical OT system, BSS) can consume MnS(s) provided by the 3GPP Cross Management Domain, RAN Management Domain,CN Management Domain. 3GPP Management Framework Consumer is a ZSM framework consumer in ETSI ZSM Framework.

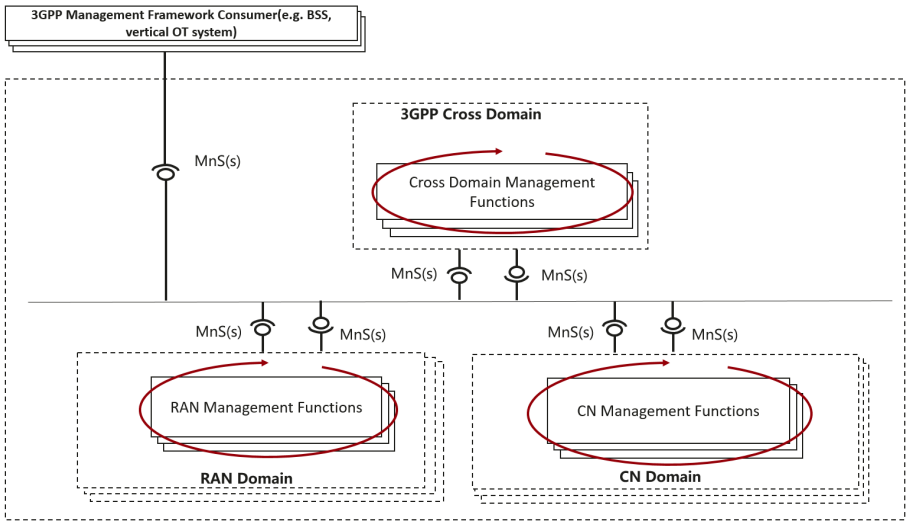


Figure 5.3-1: An example of Management Service deployment framework.

The closed control loop SLS assurance (COSLA) is an example of the closed loop in ZSM framework. COSLA can be deployed at domain level or cross domain level. A domain COSLA provides domain specific assurance, e.g. closed control loop assurance in a RAN management domain, CN management domain. A cross domain COSLA can provide a part of end-to-end SLS assurance service, e.g. to assure the service experience in 3GPP cross management domain.

5.4 Management interactions with NWDAF

3GPP management system interacts with NWDAF in a coordinated way. 3GPP management system takes the responsibility of management from the network-wide view, addresses the slow control loop with broad management scope. NWDAF is a 5GC NF as specified in TS 23.288 [30].

5.5 Using Management Services to support multiple players interoperability

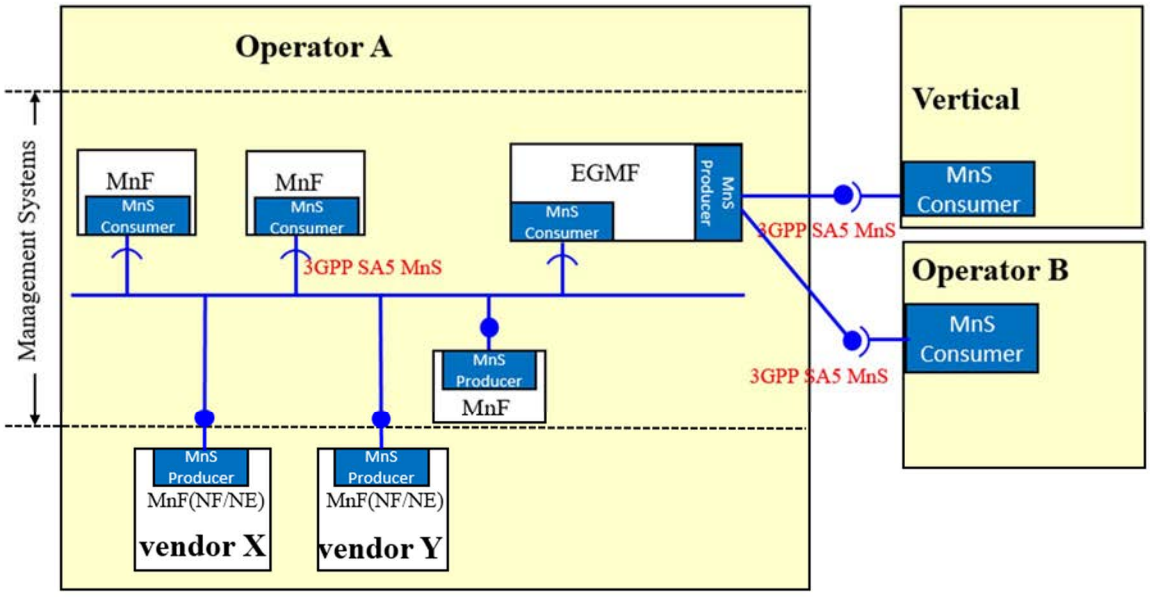


Figure 5.5-1: Example of MnS usage flexibility

Different set of management services may be used for the interoperability between different players. Figure 5.5 -1 illustrates an example showing the MnSs may be used, using the MnS flexibility. These players can be PLMM Organizations (e.g., Operator A, Operator B) and enterprise customers (e.g., Vertical). The interoperability in a multiple players scenario supported by using management services includes:

a) Interoperability within systems of a single PLMN Organisation

b) Interoperability between systems belonging to different organizations

To provide a controllable and auditable offering of capabilities to consumers belonging to different administrative domains, an exposure governance functionality is needed. This functionality policies the interactions between these consumers and corresponding MnS producers with regards to MnS discovery and access control. One potential management function performing the exposure governance functionality is EGMF.

NOTE: Assuming that the backend systems of enterprise customers are able to consume MnS semantics.

5.6 3GPP management services exposure

In the context of 3GPP management services exposure, there are different exposure scenarios depending on the type of the MnS consumer as illustrated in Figure 5.6-1.

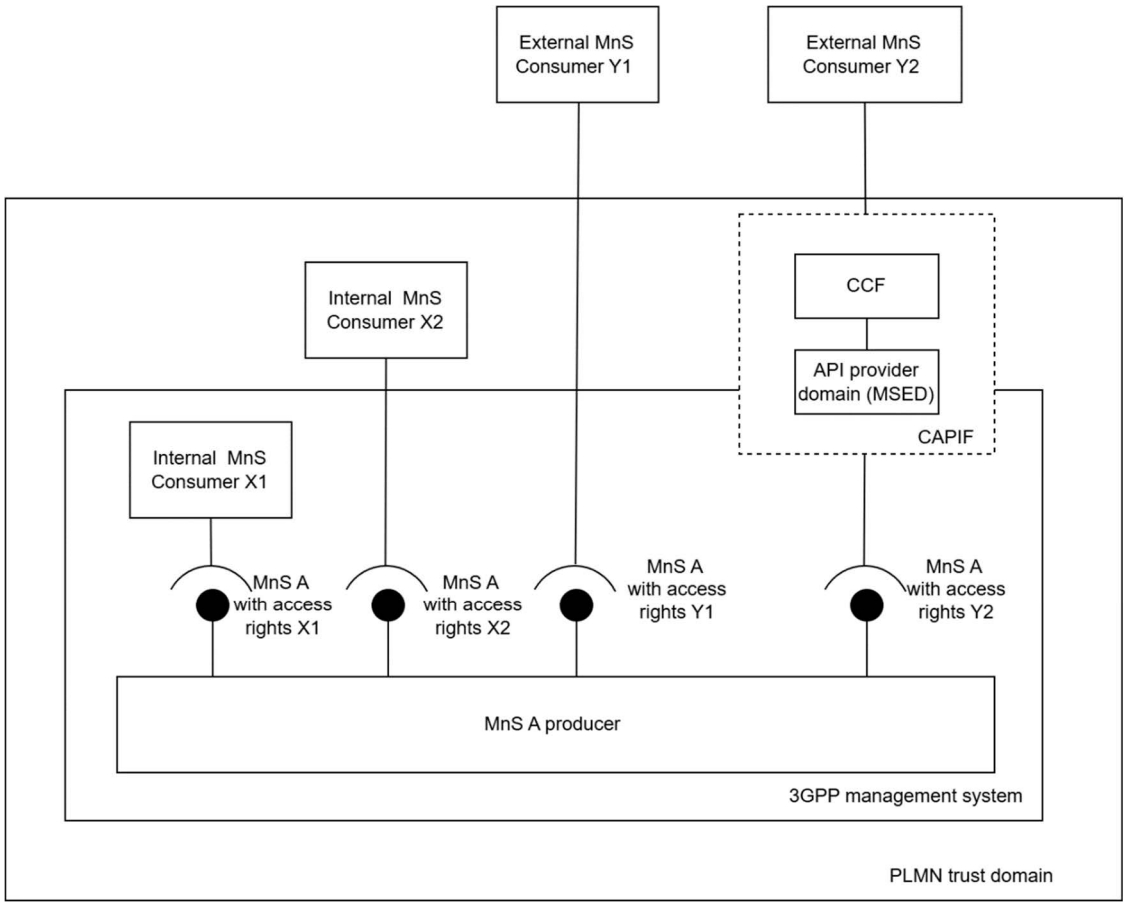


Figure 5.6-1: Management services exposure scenarios

- There are two categories of internal MnS consumers:

  a) MnS consumer within the 3GPP management system, e.g. provisioning MnS consumer, fault management MnS consumer and streaming MnS consumer. This is equivalent to internal MnS consumer X1 in Figure 5.6-1.

  b) MnS consumer outside the 3GPP management system but within the PLMN trust domain, e.g. NWDAF, operator's AFs (e.g., EAS). This is equivalent to internal MnS consumer X2 in Figure 5.6-1.

- There are two categories of external MnS consumers:

  a) MnS consumers outside the PLMN trust domain consuming management services directly from the 3GPP management system, e.g., participating operators in RAN sharing scenarios (see TS 32.130 [55]), energy utility verticals (see TS 28.318 [69]), and other verticals. This is equivalent to external MnS consumer Y1 in Figure 5.6-1.

  b) MnS consumers outside the PLMN trust domain consuming management services through exposure framework CAPIF (see TS 23.222 [76]), e.g., Energy utility verticals (see TS 28.318 [69]), and other verticals. This is equivalent to external MnS consumer Y2 in Figure 5.6-1.

The exposure of management services to the different types of MnS consumers includes two aspects: discovery of the MnSs and access control. As a precondition, the discovery of management services assumes that the management services to be exposed have been registered.

MnS discovery mechanisms for the different types of MnS consumers:

- For MnS consumers consuming management services directly from the 3GPP management system (e.g., internal MnS consumer X1, internal MnS consumer X2 and external MnS consumer Y1), the mechanisms to discover the registered management services and the corresponding management capabilities have been specified in clause 5 of TS 28.537 [39].

- For MnS consumers consuming management services through exposure framework CAPIF (e.g., external MnS consumer Y2), TS 28.579 [77] specifies how to discover the registered MnSs to this category of external MnS consumers through MnS registration, MnS publishing and MnS invocation logging capabilities.

It is up to the network operator’s discretion to determine the appropriate discovery and access control rights for the different MnS consumers when consuming a given MnS.

6 Void

Annex A (informative): Example of deployment model with utilization of management services

A.1 Utilization of Management services in network and subnet layers

To deploy a management and orchestration system for the mobile network including network slice(s), the management system can follow the network and network slice management model, subnetwork and network slice subnet management model, and network function management model. As an example, management models are shown in Figure A.1.1, management services in each management model.

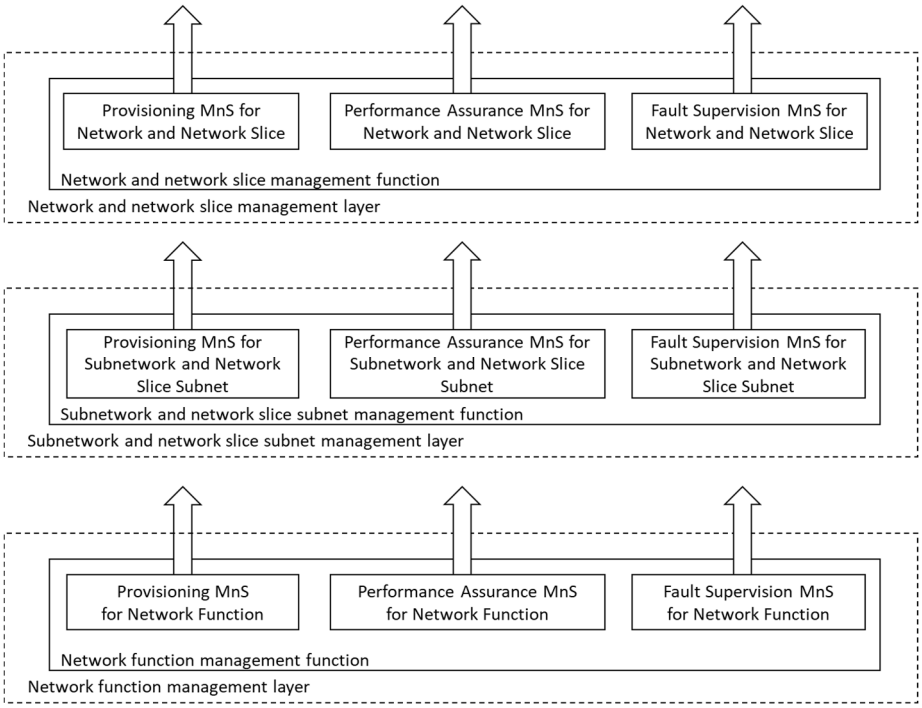


Figure A.1.1: Example management layers in layered management model

A.2 Utilization of management services in network function management

This subclause describes the network function management model in the example of management services deployment. In case that a deployment requires management service in NF management model, management services in NF management model can provide specific management capability for NFs to authorized management service consumer through service based interface.

NF management function is an execution entity to provide NF Management services in NF management model. NF Management function (NFMF) may manage more than one network functions.

NF management function for multiple managed network functions as shown in Figure A.2.1 provides:

- Management services exposure; and
- Data governance for management service exposure.

NOTE 1: One example of a management object with multiple management services is NF pooling design. Another example of a management object with this multiple NF management services is 5G Core control plane.

NOTE 2: NF management function can behave as consumer to ETSI ISG NFV MANO interfaces (e.g. Ve-Vnfm-em interface exposed by VNFM).

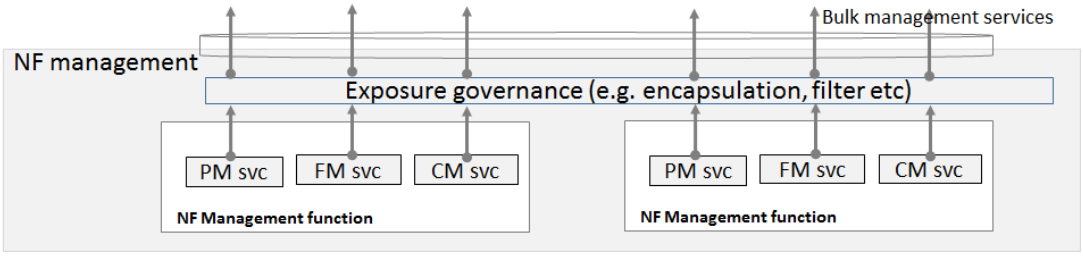


Figure A.2.1: Example NF management function layer structure

As shown in Figure A.2.1, an example of NF management function model structure is given. Exposure governance management function (EGMF) shown in Figure A.2.1 is management function in network function model with the role of management service exposure governance (i.e. abstraction, simplification, filtering, etc.). When multiple NF management services are exposed to network management, the particular group of multiple NF management services can be represented by a set of NF management services. This set of NF management services are exposed as a bulk NF management service, by NF management function. Additional management service abstraction may be needed based on NF management services because of lack of trust relationship between management service producer/consumer cannot address management services to build a global view of subnet or meaningful management purposes.

A.3 Utilization of management services by Exposure Governance Management Function (EGMF)

Exposure Governance Management Function (EGMF) offers following management capability (Figure A.3.1):

- Exposure governance

NOTE: Details of EGMF management capability exposure governance is FFS.

In Figure A.3.1, EGMF produces exposure governance management capability that operators can apply on Management Function (MnF) 1 MnS for exposing different derivation of MnF 1 MnS to:

- MnF 2 (e.g. from another Operator) and
- 3rd party (e.g. from vertical industry).

NOTE: Exposure governance can be controlled by a policy for different type of MnF 1 MnS consumers (e.g. other operator, other management system, 3rd party, other administrative domain, etc.)

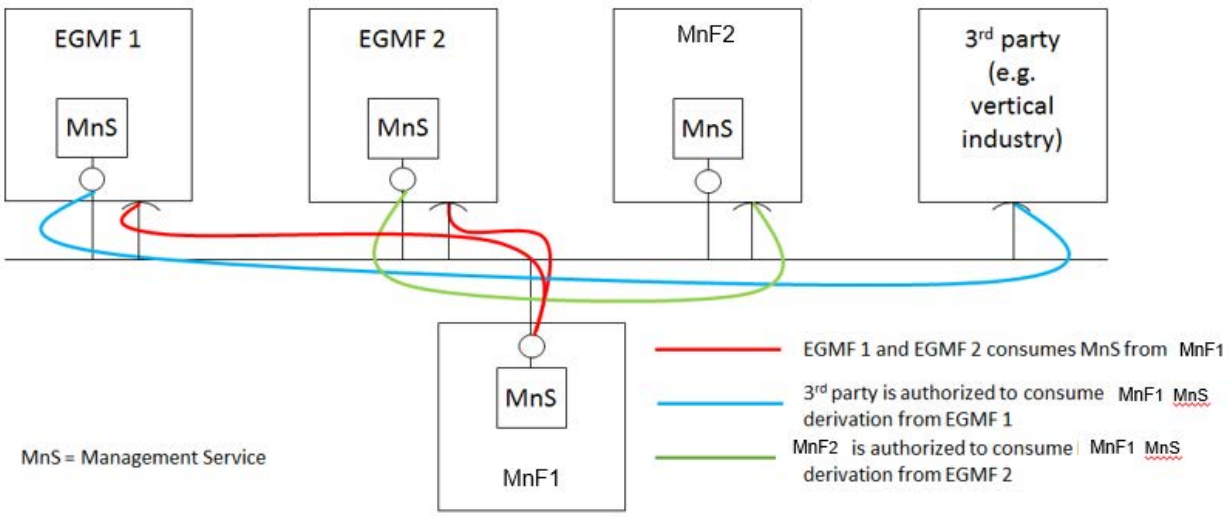


Figure A.3.1: MnF-1 Management Service (MnS) exposed through Exposure Governance Management Function 1 (EGMF 1) and through Exposure Governance Management Function 2 (EGMF 2)

A.4 Utilization of interface to NFV-MANO by the producer of management services

In this deployment scenario the producers of the network slice subnet related management services and NF related management services are also consuming the management interfaces provided by the NFV-MANO:

- -VNF PM, FM and LCM
- Network service PM, FM and LCM

These interfaces are provided via the Os-Ma-nfvo and the Ve-Vnfm-em reference points as specified in the following specifications:

- Configuration Management (CM): TS 28.510 [11], TS 28.511 [12], TS 28.512 [13], TS 28.513 [14],
- Fault Management (FM): TS 28.515 [15], TS 28.516 [16], TS 28.517 [17], TS 28.518 [18],
- Performance Management (PM): TS 28.520[19], TS 28.521 [20], TS 28.522 [21], TS 28.523 [22],
- Life Cycle Management (LCM): TS 28.525[23], TS 28.526 [24], TS 28.527 [25], TS 28.528 [26].

For details of NFV-MANO interfaces, see ETSI GS NFV-IFA008 [64] and ETSI GS NFV-IFA013[65].

In this deployment scenario:

- the entity denoted as NSSMF, is capable of consuming the VNF LCM and network service LCM related services provided by the NFV-MANO (NFVO). Same entity is also a producer of the network slice subnet related management services.
- the entity denoted as NFMF (NF Management Function), is capable of application level management of VNFs and PNFs and is a producer of the NF Provisioning service that includes Configuration Management (CM), Fault Management (FM) and Performance Management. Same entity is consumer of the NF Provisioning service produced by VNFs and PNFs.

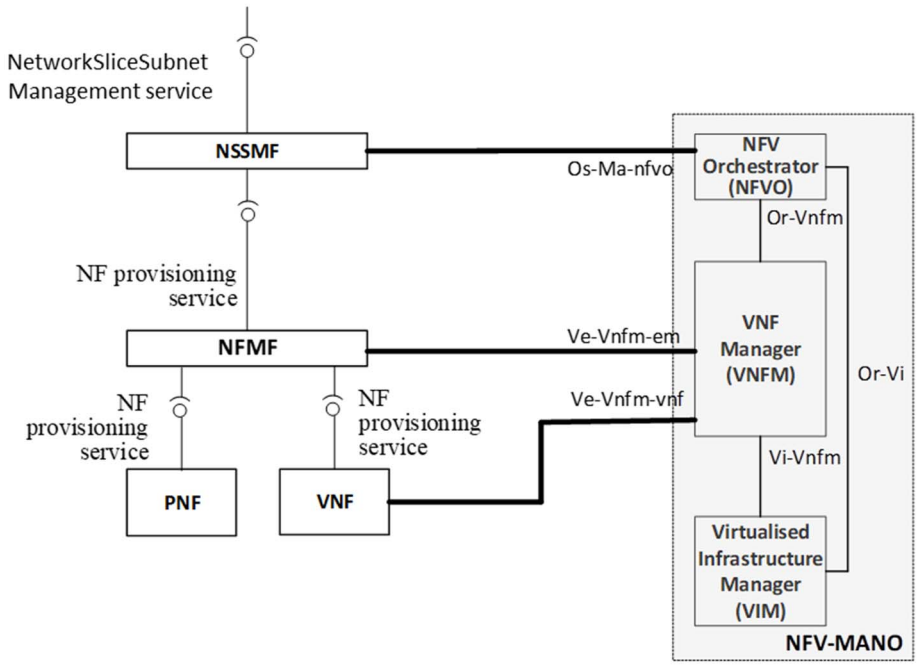


Figure A.4.1: The deployment scenario for network slice subnet management with interface to NFV-MANO

The use case Network slice subnet instance creation in the clause 5.1.2 of the TS 28.531 [8] shows example of interaction between:

- the consumer of the network slice subnet related management services (e.g. network slice subnet provisioning service) and the NSSMF as the producer of the network slice subnet related management services.
- the NSSMF and the NFMF.

and also, the interaction between:

- the NSSMF and the NFV-MANO,
- the NFMF and the NFV-MANO.

NOTE: Figure A.4.1 shows an example of a deployment scenario, not all scenarios are captured by this figure.

A.5 Management Data Analytics Service (MDAS)

A management data analytics service (MDAS) provides data analytics of different network related parameters including for example load level and/or resource utilisation. For example, the MDAS producer for NF(s) can collect the NF's load related performance data, e.g. resource usage status of the NF. The analysis of the collected data may provide forecast of resource usage information in a predefined future time. This analysis may also recommend appropriate actions e.g. scaling of resources, admission control, load balancing of traffic, etc.

A MDAS for network slice subnet(s) provides network slice subnet related data analytics. The MDAS producer for network slice subnet(s) may consume the corresponding MDAS of its constituent NF(s). The MDAS producer for network slice subnet(s) may further classify or shape the data in different useful categories and analyse them for different network slice subnet management needs (e.g. scaling, admission control of the constituent NFs etc.). If a network slice subnet is composed of multiple constituent network slice subnets, the MDAS producer for network slice subnet(s) acts as a consumer of MDAS of the constituent network slice subnets for further analysis e.g. resource usage prediction, failure prediction for a network slice subnet, etc.

A MDAS for network slice(s) provides network slice related data analytics. The MDAS producer for network slice(s) may consume the corresponding MDAS of its constituent network slice subnet(s). The MDAS producer for network slice(s) may further classify or shape the data in different useful categories according to different customer needs, e.g.

slice load, constituent network slice subnet load, communication service loads. This data can be used for further analysis e.g. resource usage prediction, failure prediction for a network slice, etc.

A.6 Utilization of management services in functional management architecture

The management services for a mobile network including network slicing may be produced by a set of functional blocks. This annex shows an example of such deployment scenario where functional blocks (such as NSMF, NSSMF, NFMF and CSMF) are producing and consuming various management services.

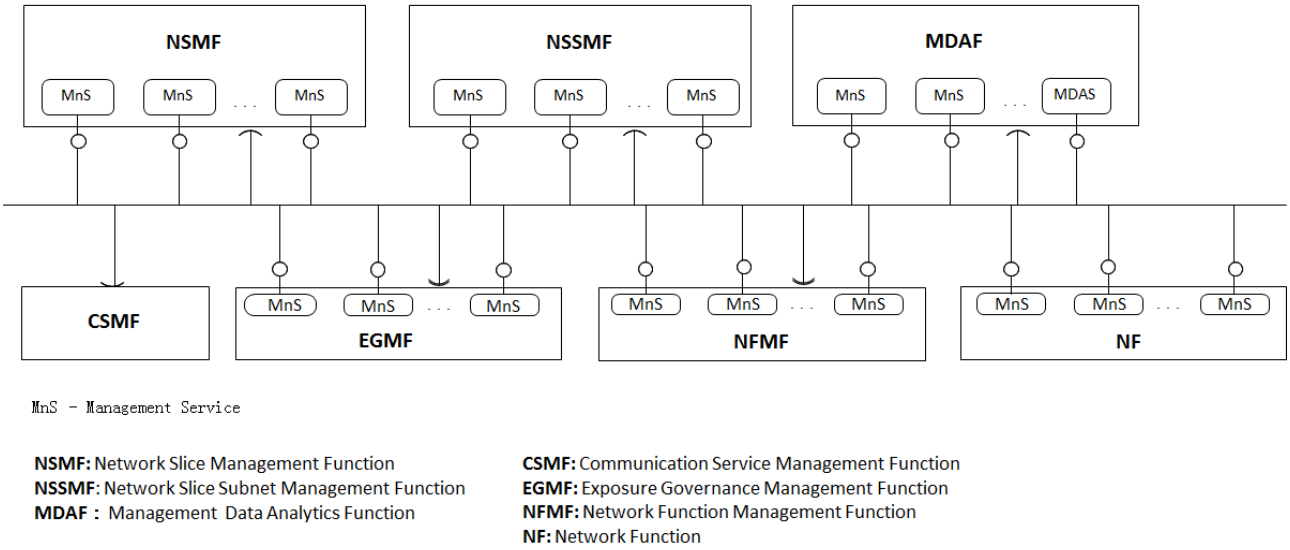


Figure A.6.1: Example of functional management architecture

In this deployment example:

- NFMF (Network Function Management Function) provides the management services for managing one or more NF(s) and may consume some management services produced by other functional blocks.
- The NF provides some management services, for example the NF performance management services, NF configuration management services and NF fault supervision services.
- NSSMF provides the management services for one or more network slice subnets and may consume some management services produced by other functional blocks.
- NSMF provides the management services for one or more network slices and may consume some management services produced by other functional blocks.
- MDAF provides the Management Data Analytics Service for one or more NF, network slice subnet and/or network slice, and may consume some management services produced by other functional blocks.
- CSMF consumes the management service(s) provided by the other functional blocks. This deployment example does not illustrate what management services the CSMF consumes.
- EGMF provides management service(s) with applied exposure governance and a management service with management capability exposure governance to one or more management service consumers and may consume some management services produced by other functional blocks.
- One functional block may consume the management service(s) provided by another functional block, depending on the management scope of the functional block(s). The scope may be expressed in the terms of Management Service Components (see clause 4.3).

A.7 Utilization of management data analytics services

A management data analytics service (MDAS) provides data analytics for the network. MDAS can be deployed at different levels, for example, at domain level (e.g. RAN, CN, network slice subnet) or in a centralized manner (e.g. in a PLMN level). A domain-level MDAS provides domain specific analytics, e.g. resource usage prediction in a CN or failure prediction in a network slice subnet, etc. A centralized MDAS can provide end-to-end or cross-domain analytics service, e.g. resource usage or failure prediction in an network slice, optimal CN node placement for ensuring lowest latency in the connected RAN, etc. Figure A.7.1 illustrates an example of deployment model of the MDAS:

- Domain MDAF produces Domain MDAS
- Domain MDAS is consumed by the Centralized MDAF and the other authorized MDAS Consumers (for example, infrastructure manager, network manager, network slice manager, network slice subnet manager, other 3rd party OSS, etc.)
- Centralized MDAF produces Centralized MDAS
- Centralized MDAS is consumed by different authorized MDAS Consumers

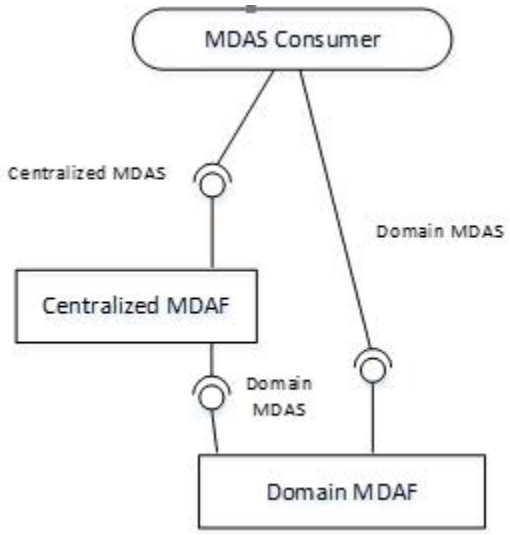


Figure A.7.1: MDAS provided at different levels

A.8 An example of deployment scenario for network and network slice

This annex shows an example of deployment scenario for management of a mobile network including network slicing.

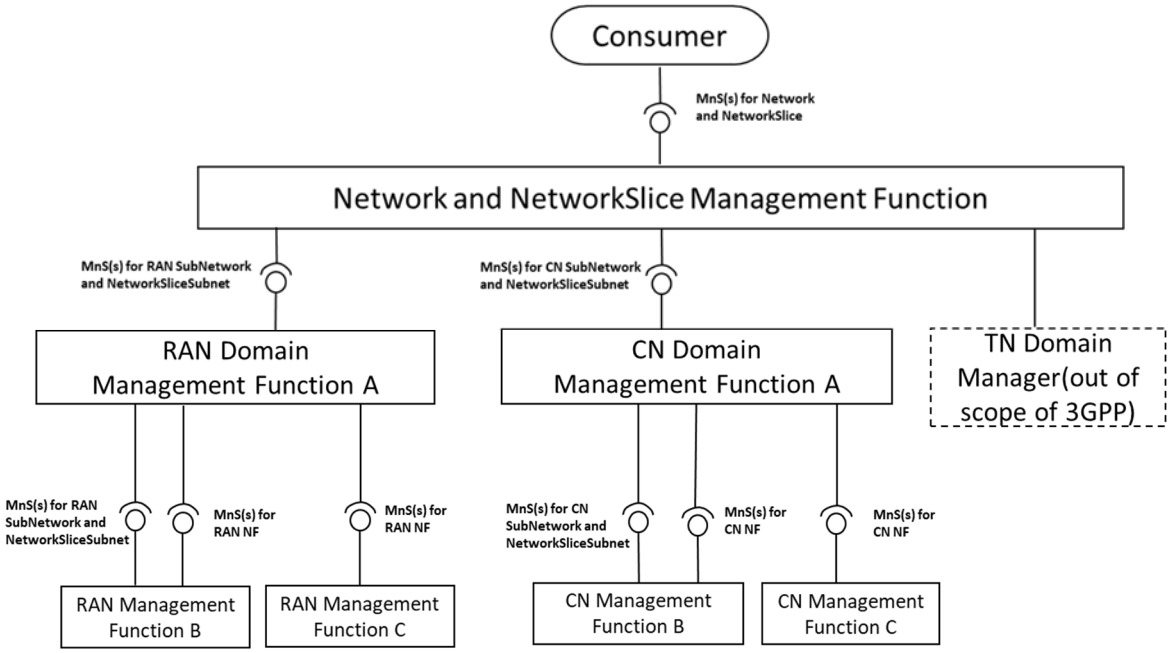


Figure A.8.1: An example of deployment scenario for management of a mobile network including network slicing

In this deployment scenario:

- Network and Network Slice Management Function provides the management services for network or network slice which includes RAN part, CN part and TN part to the Consumer. Network and NetworkSlice Management Function consumes management services for RAN SubNetwork or network slice subnet produced by RAN Management Function, management services for CN SubNetwork or NSSI produced by CN Management Function and interface produced by TN Manager.

- RAN Management Function provides the management services for a RAN SubNetwork or network slice subnet and/or management services for RAN NF(s). RAN Management Function may consume management service for RAN SubNetwork or network slice subnet and management services for RAN NF. In this scenario, the following RAN Management Function(s) are described:

  - RAN Management Function A provides the management services for RAN SubNetwork or network slice subnet to Network and Network Slice Management Function. RAN Management Function A consumes the management services for RAN network slice subnet(s) and management services for RAN NF produced by RAN Management Function B, and management services for RAN NF produced by RAN Management Function C.

  - RAN Management Function B provides the management services for RAN network slice subnet and management services for RAN NF to RAN Management Function A.

  - RAN Management Function C provides the management services for RAN NF to RAN Management Function A.

- CN Management Function provides the management services for a CN network slice subnet and/or management services for CN NF. CN Management Function may consume management service for CN network slice subnet and management services for CN NF. In this scenario, the following CN Management Function(s) are described:

  - CN Management Function A provides the management services for CN NSSI to Network and Network Slicing Management Function. CN Management Function A consumes the management services for CN NSSI and management services for CN NF produced by CN Management Function B and management services for CN NFs produced by CN Management Function C.

  - CN Management Function B provides the management services for CN NSSI and management services for CN NF to CN Management Function A.

  - CN Management Function C provides the management services for CN NF to CN Management Function A.

A.9 Deployment examples of ONAP platform consuming 3GPP MnS(s)

A.9.1 Integration with ONAP DCAE collection framework utilizing 3GPP MnS(s)

Figure A.9.1 shows an example of integration with ONAP DCAE utilizing the management services provided by 3GPP Data Report MnS Producer. In this example, the 3GPP MnS(s) Consumer which uses the ONAP DCAE Collection Framework, utilizes the management services (i.e., Performance Data File Report MnS, Performance Data Streaming MnS, Fault Supervision Data Report MnS) provided by 3GPP Management Service(s) Producer.

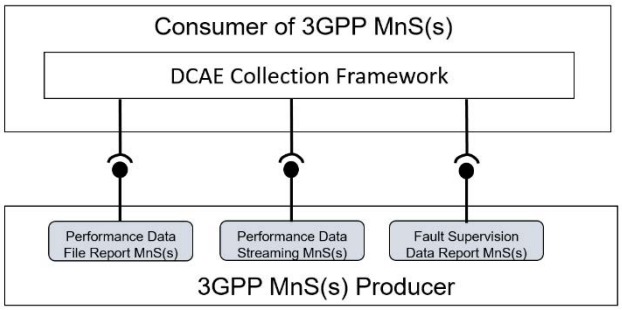


Figure A.9.1: An example of integration with ONAP DCAE Collection Framework utilizing the management services provided by 3GPP Data Report MnS(s) Producer

A.9.2 Integration with ONAP controller utilizing 3GPP MnS(s)

Figure A.9.2 shows an example of integration with ONAP Controller (e.g. APPC) utilizing provisioning management services provided by 3GPP Management Service Producer. In this example, the 3GPP MnS(s) Consumer which uses ONAP Controller may utilize the provisioning management services (e.g. configuration management related provisioning management service components) as follows provided by 3GPP Management Service Producer.

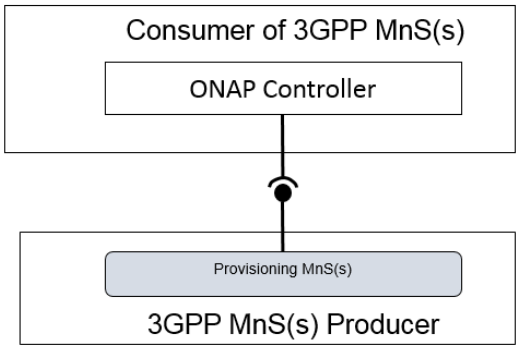


Figure A.9.2: An example of integration with ONAP Controller utilizing the management services provided by 3GPP MnS(s) Producer

A.10 Management domain provided management services mapped with ZSM

In ETSI GS ZSM 002 [29], management services provided by management domain includes the following categorization:

- Domain data collection
- Domain analytics
- Domain intelligence
- Domain orchestration
- Domain control

Figure A.10-1 shows an example of potential RAN domain management capabilities and how these different 3GPP RAN management capabilities fit into the ZSM architecture framework. These capabilities, produced by one or more management functions, are offered via corresponding MnSs through the RAN domain integration fabric:

- Domain data collection
  - RAN domain threshold monitoring control capabilities are provided by ThresholdMonitor IOC defined in TS 28.622 [32].
  - RAN domain data collection control capabilities are provided by ManagementDataCollection IOC defined in TS 28.622 [32].
- Domain analytics
  - RAN domain MDA capabilities are provided by MDAFunction IOC defined in 28.104 [57].
- Domain intelligence
  - RAN domain Intent handling capabilities are provided by IntentHandlingFunction IOC defined in TS 28.312 [46].
- Domain orchestration
- Domain control
  - RAN domain Assurance Closed Loop capabilities are provided by AssuranceClosedControlLoop IOC defined in TS 28.536 [38].
  - RAN domain Centralized SON Energy Saving capabilities are provided by CESManagementFunction IOC defined in TS 28.541 [4].
  - RAN domain Capacity and Coverage optimization capabilities are provided by CCOFunction IOC defined in TS 28.541 [4].
  - RAN domain PCI configuration capabilities are provided by CPCIConfigurationFunction IOC defined in TS 28.541 [4].
  - RAN domain PM control capabilities are provided by PerfMetricJob IOC defined in TS 28.622 [32].
  - RAN domain FM control capabilities are provided by AlarmList IOC defined in TS 28.622 [32].
  - RAN domain CM control capabilities are represented by NR NRM defined in TS 28.541 [4].

NOTE: Domain integration fabric and Cross-domain integration fabric are ZSM defined management functions (see ZSM 002 [29] for further details). These functions provide, among other capabilities, MnS discovery functionality (see further details in clause 4.7 and TS 28.622 [32]).

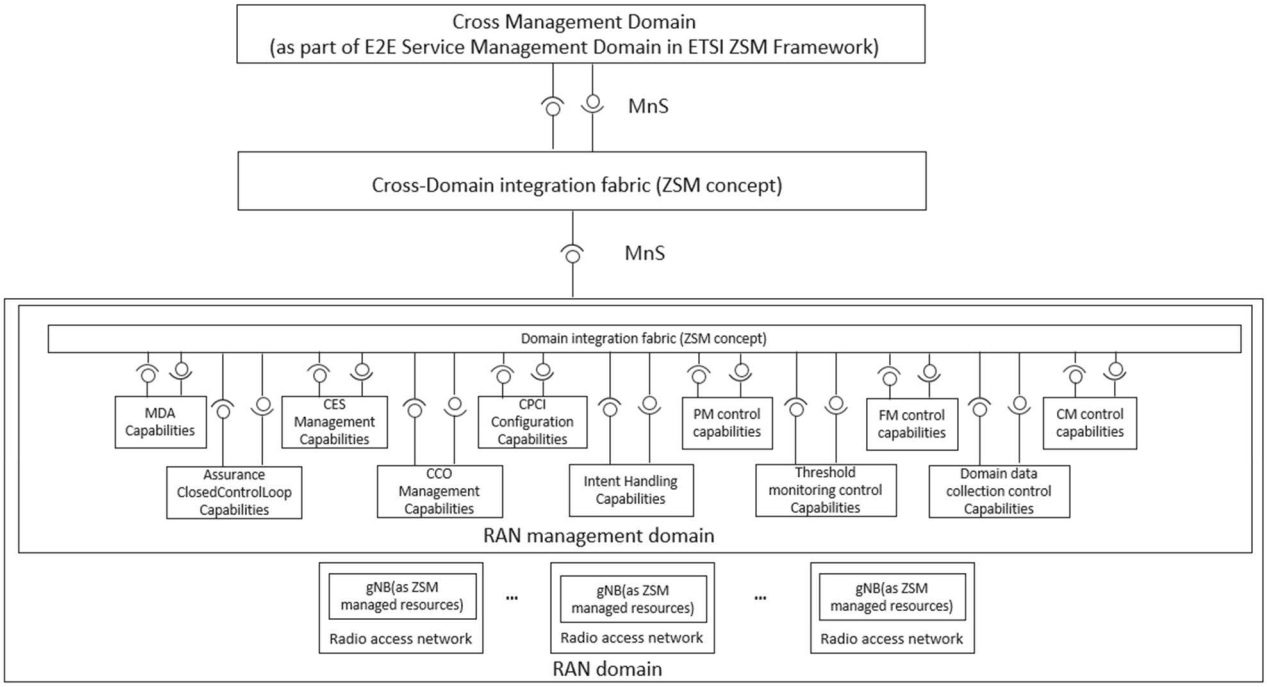


Figure A.10-1: An example of deployment scenario for RAN management functions

A.11 Illustrative architecture reference model for management and orchestration

The illustrative architecture reference model for management and orchestration in Figure A.11-a defines a set of functions in the management domain. Each function produces zero, one or more Management Services (MnSs) and/or consumes zero, one or more MnSs (see clause 4.5).

Interaction, including the production and consumption of management services, is exclusively performed via the management service interface which represents the standardised interface that interconnects functions in for the production and consumption of MnSs, enabling consistent, service-based interactions in an implementation-agnostic manner.

The Functions in the management domain are logical, implementation-agnostic entities, defined independently of any specific deployment scenario. They are characterised by their overall management responsibilities and functional scope Each function is defined by the set of MnSs it produces and/or consumes, and, where applicable, by the functional management capabilities it logically encompasses to support those MnSs, as specified in the corresponding reference specifications.

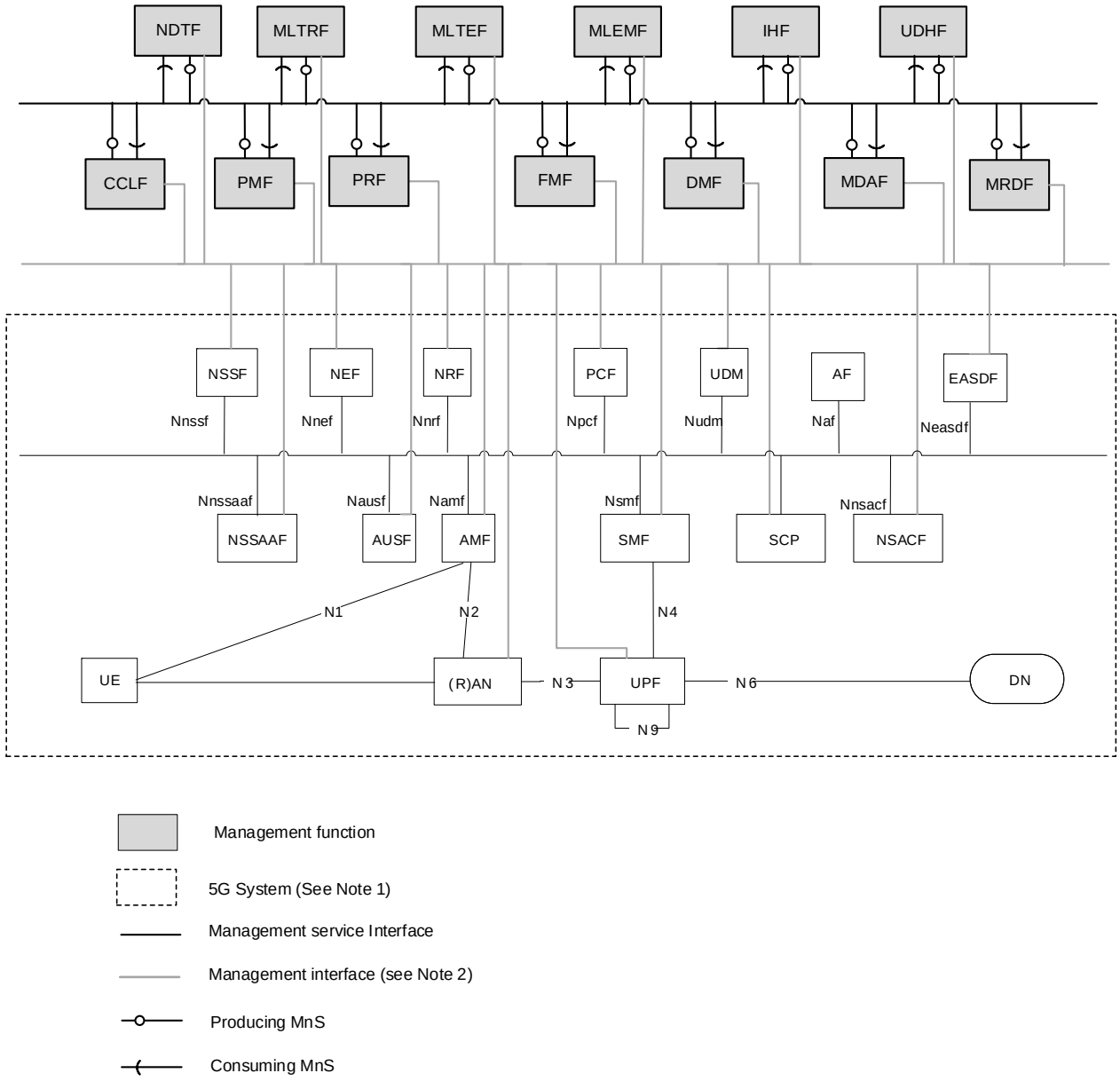


Figure A.11-a: Illustrative architecture reference model for management and orchestration.

Table A.11-b defines each function in the architecture reference model for management and orchestration along with the corresponding reference specifications that define their functionality.

Table A.11-b: Functions definition and corresponding reference specifications

Function	Reference management capability of MnS defined in Annex F	Reference specification
MDAF	Management Data Analytic	TS 28.104 [57]
MLTRF	ML model Management	TS 28.105 [66]
MLTEF	ML model Management	TS 28.105 [66]
MLEMF	ML model Management	TS 28.105 [66]
IHF	Intent Driven Management	TS 28.312 [46]
UDHF	Trace/MDT data collection control Trace/MDT data report QoE data collection control QoE data report	TS 32.422 [44], 28.405 [49], TS 28.558 [72]
PMF	Performance Metric Collection Control Performance Metric Data Report Performance Metric Threshold Monitor Control Performance Metric Threshold Notification	TS 28.552 [5]

FMF	Fault control Fault Notification	TS 28.530 [3], 28.111 [68]
DMF	File Retrieval File Download	TS 28.537 [39], TS 28.622 [32], TS 28.623 [54]).
PRF	NR Provisioning 5GC Provisioning Network Slicing Provisioning	TS 28.531 [8]
NDTF	FFS	TS 28.561 [73]
CCLF	Communication Service Assurance Control	TS 28.567 [74]
MRDF	MnS Registry and Discovery	TS 28.537 [39]

NOTE 1: For details on the 5G System reference architecture including entities/functions and interfaces, see TS 23.501, clause 4.2 [31].

NOTE 2: The management interface represents the logical abstraction for management-NFs interactions.

NOTE 3: The reference architecture does not assume or restrict the physical locality of functions in the management domain. The functions can be deployed centrally, distributed, or co-located with Network Functions (NFs) depending on operator's deployment choices (see clause 4.5).

A.12 Summary and capabilities of the architecture reference model for management and orchestration

A.12.1 ML Training Function (MLTRF)

The ML Training Function (MLTRF) provides capabilities for initial training and re-training of machine learning models. It manages the collection and preparation of training data, executes training processes, validates trained models, and may coordinate joint training of multiple ML models when required. It produces training performance reports and enables authorised consumers to configure training thresholds, select training data sources, and manage the training lifecycle.

Capabilities:

- Initial training and re-training of ML models.
- Training data collection and preparation.
- Model validation.
- Model joint training.
- Training performance reporting.
- Training threshold configuration.

(Reference: TS 28.105 [66]).

A.12.2 ML Testing Function (MLTEF)

The ML Testing Function (MLTEF) is responsible for evaluating the performance of trained ML models using independent testing datasets. It provides capabilities for selecting and applying performance indicators, comparing results against requirements, and enabling re-training if test results do not meet expectations. The function allows authorised consumers to request model testing and receive detailed test reports.

Capabilities:

- Model testing.
- Performance indicator selection and reporting.
- Model joint testing.
- Re-training triggering.
- Test report delivery.

(Reference: TS 28.105 [66]).

A12.3 ML Emulation Function (MLEMF)

The ML Emulation Function (MLEMF) provides the capability to emulate AI/ML inference processes in a controlled environment before deployment to the live network or system. It enables the evaluation of ML model inference performance under representative conditions and ensures that models meet operational performance targets without adverse effects on other network functions.

Capabilities:

- Inference emulation in test environments.
- Performance evaluation under lifelike conditions.
- Verification of non-impact on live systems.
- Inference emulation report delivery.

(Reference: TS 28.105 [66]).

A.12.4 Management Data Analytics Function (MDAF)

The Management Data Analytics Function (MDAF) enables the processing and analysis of management, service, and network data to generate actionable analytics output. It supports diverse analytics capabilities such as performance assessment, prediction, anomaly detection, and root cause analysis across network domains (RAN, CN, and cross-domain). MDAF may utilize AI/ML inference for specific analytics types and interact with various data sources including PM/KPIs, QoE, alarms, traces, configuration, and external inputs (e.g. NWDAF, LMF, AFs). It offers its output via the Management Data Analytics Service (MDAS), allowing authorised consumers to request, control, and retrieve analytics reports. MDAF also enables service assurance, mobility optimisation, fault prediction, energy saving, and cross-domain orchestration by providing analytics tailored to use case-specific data inputs.

Capabilities:

- Cross-domain analytics processing.
- AI/ML inference for analytics.
- Performance prediction and anomaly detection.
- Integration with PM/KPI, trace, QoE, and external data.
- Use case-specific analytics support (e.g., assurance, energy saving).

(Reference: TS 28.104 [57]).

A.12.5 Intent Handling Function (IHF)

The Intent Handling Function (IHF) enables high-level management of network and service behaviours by allowing authorised consumers to express desired outcomes intents without detailing how to achieve them. It translates these intents into concrete/executable actions, policies, and configurations, and manages their fulfilment using rule-based logic, closed-loop automation, or AI/ML mechanisms. IHF supports negotiation, feasibility checks, conflict resolution,

and reporting throughout the intent lifecycle. It simplifies operations by abstracting complexity and supports a wide range of use cases, including service provisioning, assurance, energy saving, and end-to-end optimisation.

IHF can interact with other functions, including Closed Control Loop Functions (CCLF), to fulfil intents that require continuous assurance or dynamic adaptation.

Capabilities:

- Intent expression and processing.
- Policy and configuration translation.
- Closed-loop and AI/ML-based fulfilment.
- Negotiation and feasibility checks.
- Conflict detection and resolution.
- Intent lifecycle reporting and monitoring.
- Use case support: assurance, energy efficiency, etc.

(Reference: TS 28.312 [46]).

A.12.6 UE Data Handling Function (UDHF)

The UE Data Handling Function (UDHF) enables detailed per-UE data collection across the 5G system. Its capabilities include mechanisms for trace, MDT, QoE, and UE-level measurements. Together, they support fine-grained performance monitoring, troubleshooting, and analytics at the individual UE level, complementing traditional aggregated performance data.

UDHF supports the collection of trace data, MDT measurements, RLF and RRC failure reports, QoE information, and 5GC UE-level measurements. Data collection can be triggered on-demand or through management-based or signalling-based activation procedures. It enables authorised consumers to configure collection policies, manage activation and deactivation, and retrieve per-UE metrics such as delay, throughput, packet loss, and QoE indicators across both RAN and 5GC domains.

Capabilities:

- Per-UE trace and measurement collection.
- RLF/RRC failure report capture.
- QoE and 5GC measurement support.
- On-demand and policy-triggered collection.
- Per-UE KPI retrieval and analysis.

(References: TS 32.422 [44], TS 28.405 [49], TS 28.558 [72]).

A.12.7 Performance Management Function (PMF)

The Performance Management Function (PMF) enables the collection, control, and reporting of performance measurements across 5G networks, including network slice instances (NSIs), network slice subnet instances (NSSIs), and network functions (NFs). PMF supports both file-based and streaming-based reporting of performance data and allows authorized consumers to create, query, and terminate measurement jobs. It includes services for threshold monitoring and KPI job control, enabling proactive performance assurance and analytics. PMF supports multi-tenant scenarios by enabling performance data collection per S-NSSAI, facilitating Network Slice as a Service (NSaaS). It interacts with various management services and data sources to provide timely and granular performance insights for assurance, optimization, and SLA compliance.

Capabilities:

- Performance measurement job control.
- File/stream-based data reporting.
- KPI threshold monitoring.
- Support for per-S-NSSAI collection.
- SLA compliance and assurance enablement.

(Reference: TS 28.552 [5]).

A.12.8 Fault Management Function (FMF)

The Fault Management Function (FMF) enables the detection, reporting, and management of faults across 5G network resources. These capabilities described in 3GPP TS 28.111 and conceptually framed in TS 28.530 enable the representation of faults, errors, and failures as alarms, facilitating timely awareness and resolution by operators or automated systems.

FMF provides mechanisms for generating, notifying, acknowledging, clearing, and correlating alarms. It supports both automatically and manually cleared alarms, alarm list reliability tracking, and alarm correlation to root causes. Alarms are modelled using a standardized structure and can be filtered, retrieved, and annotated by authorized consumers. Notifications are delivered via a service-based interface, supporting real-time and historical fault visibility.

Capabilities:

- Fault/alarm generation and clearance.
- Alarm correlation and root cause indication.
- Alarm annotation and filtering.
- Alarm acknowledgement.
- Real-time and historical alarm visibility.
- Multi-domain and multi-generation applicability.

(References: TS 28.111 [68], TS 28.530 [3]).

A.12.9 Data Management Function (DMF)

The Data Management Function (DMF) provides the management capabilities for the lifecycle of management data across network and management domains. As defined in TS 28.537, DMF facilitates the production, coordination, discovery, storage, delivery secure destruction of data at end-of-life of both 3GPP-specified and external management data, ensuring that authorized consumers can access the information they need for assurance, optimization, and automation.

Capabilities:

- Request- and subscription-based data production.
- Time-/condition-based reporting.
- Discovery of available data and metadata.
- Support for 3GPP and external data types.
- Coordination across multiple consumers.
- Storage for reuse (e.g., ML training).

(Reference: TS 28.537 [39], TS 28.622 [32], TS 28.623 [54]).

A.12.10 Provisioning Function (PRF)

The Provisioning Function (PRF) provides the capabilities required to instantiate, configure, modify, and retire managed entities within the 5G network, including network slice instances (NSIs), network slice subnet instances (NSSIs), network functions (NFs), and sub-networks. As specified in TS 28.531, PRF supports the full lifecycle of provisioning operations, from feasibility checks and resource reservation to activation and deactivation, across both physical and virtualized infrastructure.

Capabilities:

- Lifecycle management (instantiation, configuration, and termination) of NSIs, NSSIs, NFs.
- Support for feasibility checks and resource reservation.
- Activation/deactivation of managed entities including physical and virtualised network functions.
- Slice template customization (standard/private).
- Coordination with NFV MANO and transport orchestration.
- Priority-based and location-aware provisioning.
- Support for IAB-node specific configuration.

(Reference: TS 28.531 [8]).

A.12.11 Network Digital Twin Function (NDTF)

The Network Digital Twin Function (NDTF) provides management capabilities to create and operate virtual replicas of a mobile network or part of it, capturing its attributes, behaviour, and interactions to support management and orchestration. The NDTF enables simulation and/or emulation of network scenarios to evaluate configurations, predict outcomes, verify automation functions, and generate synthetic data without impacting the live network. It interacts with other t functions such as MDAF, AIML Functions, and the Intent Handling Function, and may coordinate with other NDTF instances to enhance simulation fidelity. The NDTF exposes its capabilities through the NDT Management Service (NDT MnS), allowing authorized consumers to configure, control, and retrieve simulation or emulation results.

Capabilities:

- Control and life cycle management of NDT instances including creation, configuration, execution, synchronization, and termination.
- Support for network automation by evaluating high-risk operations, failure scenarios, and issue inducement such as signalling storms and coverage problems.
- Support for verification of network scenarios, configurations, events, and automation-function configurations, providing reports on simulation or emulation outcomes.
- Support for data generation by producing synthetic network data, ML training datasets, and user experience data under simulated conditions.
- Advanced capabilities enabling collaboration between multiple NDT instances, coordinated simulations, and enhanced situational awareness through information exchange.
- Applicability across RAN, Core, and cross-domain management contexts to support both domain-specific and cross-domain use cases.

(Reference: TS 28.561 [73]).

A.12.12 Closed Control Loop Function (CCLF)

The Closed Control Loop Function (CCLF) provides management capabilities to monitor, analyze, decide, and execute control actions over managed entities, aiming to achieve defined goals autonomously. CCLF supports the dynamic composition, coordination, performance monitoring, conflict management, and escalation of closed control loops across

various network contexts. The function enables interactions with other t functions and services, leveraging historical data, triggers, and feedback mechanisms to optimize loop behaviour.

CCLF exposes its capabilities through standardized management services, allowing authorized MnS consumers to configure, control, and retrieve information related to closed control loops. It supports both open-box and closed-box CCL realizations, enabling flexible composition from discrete functions or services.

Capabilities:

- Instantiate or compose CCLs dynamically from templates or components.
- Utilize historical CCL profiles to configure and optimize new loops.
- Evaluate and monitor the performance of CCLs, including feedback on executed actions and impact assessment.
- Apply CCLs for fault management and network performance problem recovery.
- Instantiate or execute CCLs based on specified conditions.
- Detect, confirm, and resolve conflicts among goals, scopes, actions, and metrics of CCLs.
- Escalate decision-making to higher-level entities under predefined conditions.
- Coordinate CCL operations with other functions to ensure consistent actions and avoid conflicts.

(Reference: TS 28.567 [74]).

Annex B (normative): Solutions for management of 5G network and network slicing

Figure B.1 shows the two solutions for managing the mobile network including network slicing:

Solution1: Management with combination of existing interface IRP where applicable and 5G management information (Management service component type B and Management service component type C).

Solution2: Management with using the management services (Management service component type A, Management service component type B and Management service component type C).

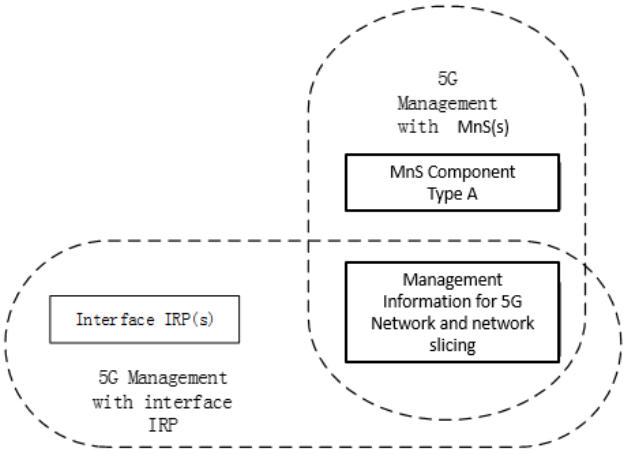


Figure B.1: Two solutions for managing a 5G network including network slicing

Annex C (informative): Example of mapping Management Services (MnS) to pre-Rel-15 management framework

Figure C.1 depicts an example of management service consumer and producer interaction shown in the context of the 3GPP pre-Rel-15 management reference model [10] where Integration Reference Point (IRP) information services are replaced by the management services. One or more management service producers are provided by a management function that applies to a network resource model representing the managed network.

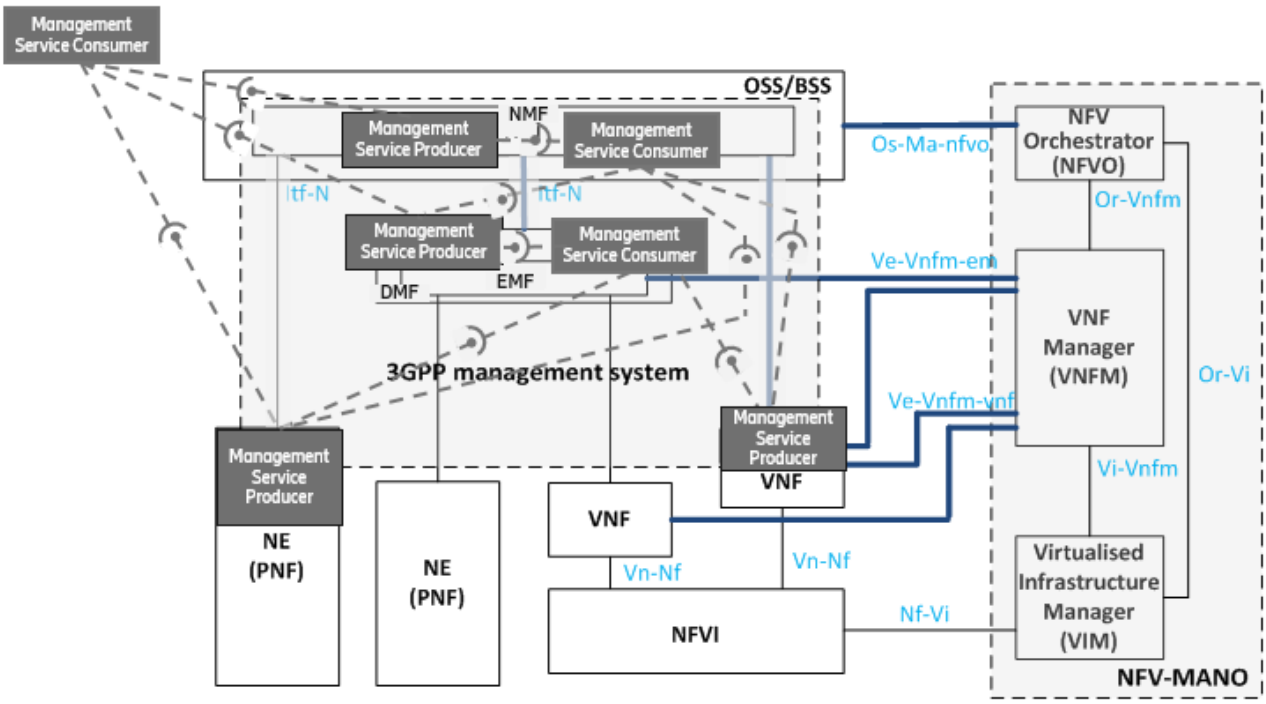
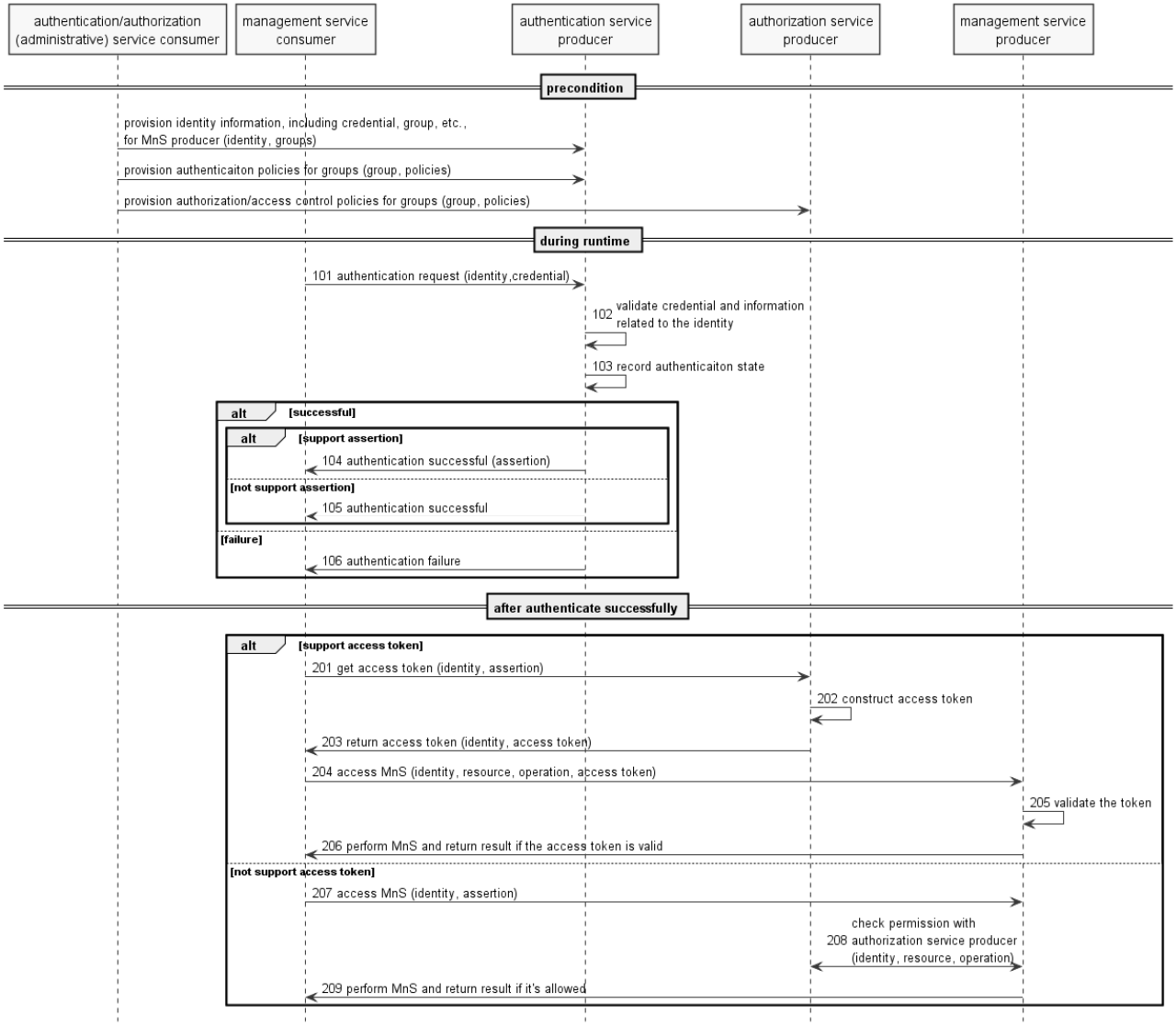


Figure C.1: Example of Management service producer and consumer interaction mapped into the pre-Rel-15 management reference model [10]

Annex D (normative): Access control workflow

D.1 Explicit authentication and authorization



NOTE 1: the authentication (administrative) service consumer could be a portal or other operator tool acting on behalf of an administrator of operator.

Precondition:

Mutual authentication between authentication (administrative) service consumer and authentication/management service producer, as well as between MnS producer and authentication service producer, has been done, according to operator's implementation.

Authentication service producer contains authentication information required to perform authentication such as identities (including credential of the identity), and/or groups, and/or authentication policies. The specific information required will depend on the implementation.

The MnS consumer successfully authenticated (or validated the authenticity of) authentication/management service producer.

Procedure:

101. When authentication request is received, authentication service producer gets the identifier and credential of the MnS consumer, along with other context information (e.g. address of the client) from the request.

NOTE 2: challenges may be exchanged between MnS consumer and authentication service producer for some authentication protocols.

102. Based on identifier in the request, authentication service producer gets identity information, e.g. status of the identity, associated group(s) of the identity, credential of the identity, etc., from data store. Then the producer authenticates the MnS consumer by validating the identity information and other context (e.g. time, location of the consumer) according to authentication policies (e.g. authentication factor, protocol, supported time, location, status of the consumer, etc.) associated to the group(s) the MnS consumer belongs to.

103. The authentication service producer updates the authentication state of the MnS consumer in the data store after authenticated the MnS consumer.

NOTE 3: If authenticate successfully and authentication assertion is supported by the protocol, the authentication service producer constructs authentication assertion and may update the assertion of the MnS consumer in the data store.

104. If authenticate successfully and authentication assertion is supported by the protocol, the authentication service producer sends successful response with an authentication assertion to the MnS consumer.

105. If authenticate successfully and authentication assertion is not supported by the protocol, the authentication service producer sends successful response without authentication assertion to the MnS consumer.

106. If fail for authentication, the authentication service producer sends failure response to the MnS consumer.

After the MnS consumer is authenticated:

If access token is supported by the MnS producer and consumer:

201. The MnS consumer gets access token from authorization service producer.

202. The authorization service producer validates the assertion and construct access token.

203. The authorization service producer returns access token to the MnS consumer.

204. The MnS consumer accesses MnS with the access token.

205. The MnS producer validates the token.

206. The MnS producer performs the operation and returns result to the MnS consumer if the token is valid.

If access token is not supported by the MnS producer and consumer:

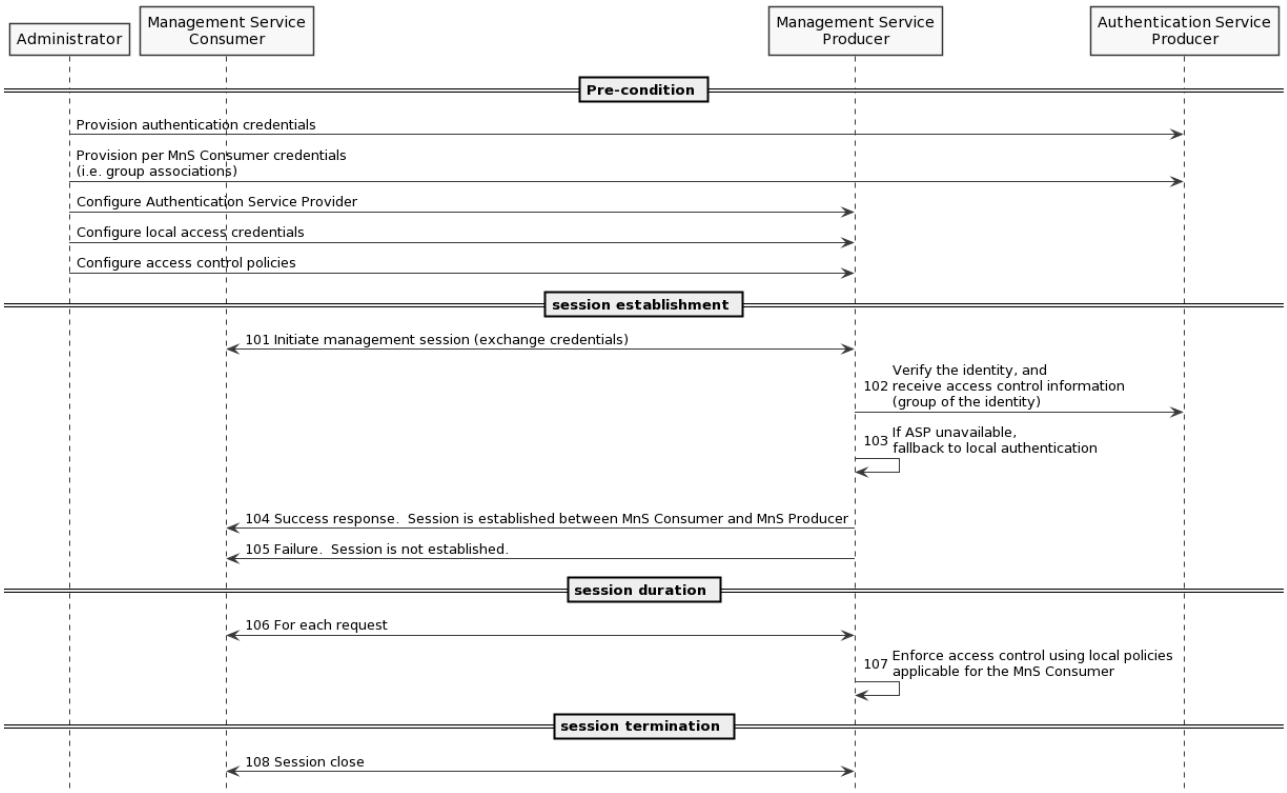
207. The MnS consumer accesses MnS from MnS producer.

208. The MnS producer validate the authentication assertion and check permission of the MnS consumer with authorization service producer.

NOTE 4: The MnS producer may authorize the MnS request of MnS consumer according to local policies.

209. The MnS producer performs the operation and returns result to the consumer if the MnS request is allowed according to permissions.

D.2 Implicit authentication and authorization



Precondition:

A centralized authentication service producer, e.g. LDAP server, is deployed in operator's network and will be used by MnS Producer to perform authentication. MnS Consumer does not interact directly with authenication service producer.

Authentication service producer contains authentication information required for MnS Producer to perform authentication such as MnS Consumer identities (including credentials) and/or groups. The specific information required will depend on the implementation.

MnS Producer has been configured to use the centralized authentication service producer.

MnS Producer optionally has support for local authentication, i.e. in event centralized authentication service is unavailable.

MnS Producer has been configured with access rules, used for local enforcement based on MnS Consumer access privileges.

Procedure:

Session Initiation:

101. MnS Consumer initiates a management session towards MnS Producer. As part of session establishment credentials are exchanged.

102. Based on credentials in the request, MnS Producer accesses Authentication Service Producer to verify the identity, and information required to perform access control including the associated group(s) of the identity.

103. If Authentication Service Producer is unavailable, MnS Producer may opt to perform local authentication.

104. If authentication is successful, MnS Producer sends success response and an authentication context is established between MnS Consumer and MnS Producer.

105. If authentication fails, MnS Producer sends failure response to MnS Consumer.

Session Duration:

106/7. For each MnS Consumer request, MnS Producer enforces access control using local policies applicable for the current authentication context.

Session Termination:

108. Upon session termination the authentication context is also terminated.

Annex E (informative): 5G specifications overview

The following figure and table show the overview information of 5G specifications which capture corresponding management features:

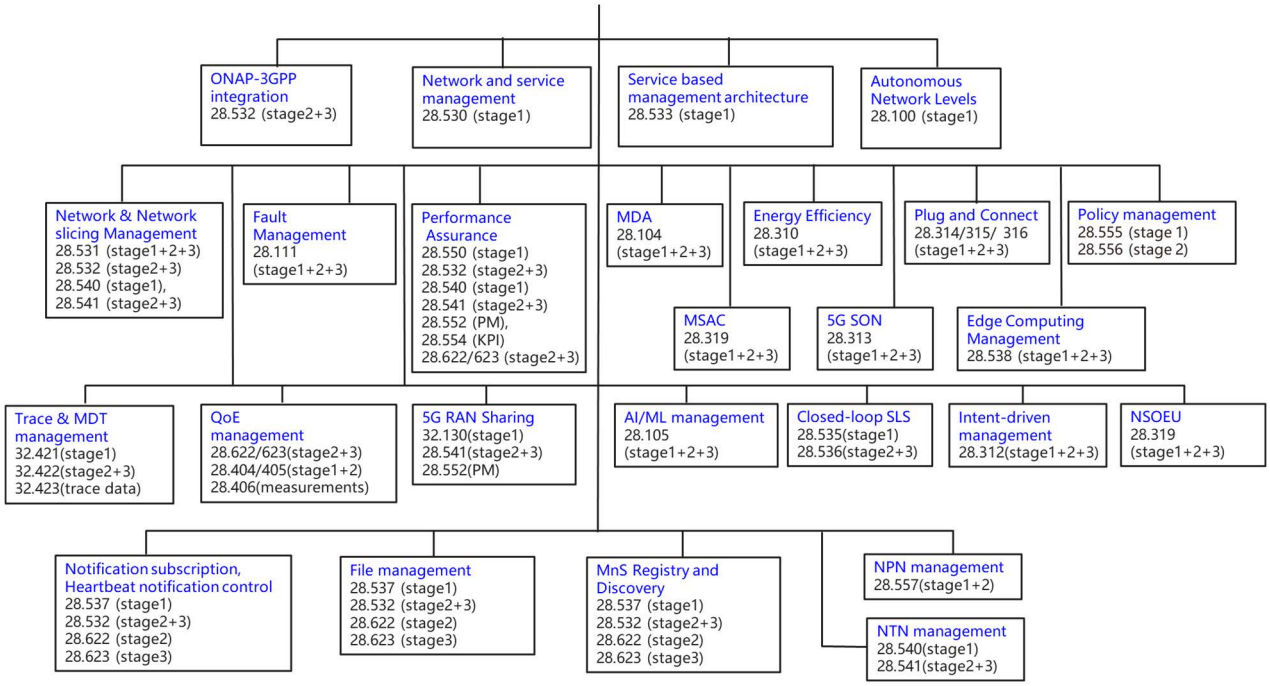


Figure E-1: Overview of 5G management specifications

The following table provides the overall 5G management features. For each listed 5G management feature, the table specifies the supporting management capabilities (see Table F-1) and the related specification information.

Table E-1 Overall 5G management features, supporting management capabilities and related specification information

5G related management feature		Supporting management capabilities	Related specifications
	Notification subscription and Heartbeat notification control	Heartbeat Control; Heartbeat Notification; Subscription Control	TS 28.537 (stage 1) [39], TS 28.532 (stage 2 and 3) [9], TS 28.622 (stage 2) [32], TS 28.623 (stage 3) [54].
	File Management	File Retrieval; File Download	TS 28.537 (stage 1) [39] (see NOTE), TS 28.532 (stage 2 and 3) [9] TS 28.622 (stage 2) [32] TS 28.623 (stage 3) [54].
	Network and service management		TS 28.530 (stage 1) [3]
	Service based management architecture		TS 28.533 (stage 1) [36]
	Autonomous Network Levels		TS 28.100 (stage 1) [35]
	Network and Network slicing management	NR Provisioning; 5GC Provisioning; Network Slicing Provisioning	TS 28.531 (stage 1, stage2 and stage3) [8] (see NOTE), TS 28.532 (stage 2 and stage 3) [9], TS 28.540 (stage 1) [41], TS 28.541 (stage 2 and stage 3) [4]

5G related management feature		Supporting management capabilities	Related specifications
	Fault Management	Fault control; Fault Notification	TS 28.111 (stage 1, stage 2 and stage 3) [68]
	Performance Assurance	Performance Metric Collection Control; Performance Metric Data Report; Performance Metric Threshold Monitor Control; Performance Metric Threshold Notification	TS 28.550 (stage 1) [42] (see NOTE), TS 28.532 (stage 2 and stage3) [9], TS 28.540 (stage 1) [41], TS 28.541 (stage 2 and stage 3) [4], TS 28.552 (PM) 5], TS 28.554 (KPI) [6] TS 28.622 (stage 2) [32], TS 28.623 (stage 3) [54]
	ONAP-3GPP integration		TS 28.532 (stage 2 and stage 3) [9]
	Trace & MDT management	Trace/MDT data collection control; Trace/MDT data report	TS 32.421 (stage 1) [43] (see NOTE), TS 32.422 (stage 2 and stage 3) [44], TS 32.423 (trace data) [45]
	QoE Management	QoE data collection control; QoE data report	TS 28.622 (stage 2) [32], TS 28.623 (stage 3) [54], TS 28.404 (stage 1) [48] (see NOTE), TS 28.405 (stage 2) [49], TS 28.406 (measurements) [50]
	Access Control for Management Services (MSAC)	MnS Access Control	TS 28.319 (stage 1, stage 2 and stage 3) [70]
	5G RAN Sharing	NR Provisioning	TS 32.130 (stage 1) [55] (see NOTE), TS 28.541 (stage 2 and stage 3) [4], TS 28.552 (PM) [5]
	Edge Computing Management	Edge Computing Provisioning	TS 28.538 (stage 1, stage 2 and stage 3) [40]
	Energy Efficiency		TS 28.310 (stage 1, stage 2 and stage 3) [56] (see NOTE), TS 28.532 (stage 2 and stage 3) [9], TS 28.552 (PM) [5], TS 28.554 (KPI) [6]
	Management Data Analytics (MDA)	Management Data Analytics	TS 28.104 (stage 1, stage 2 and stage 3) [57]
	5G SON	RANSC management SON policy	TS 28.313 (stage 1, stage 2 and stage 3) [58] (see NOTE), TS 28.317 (stage 1, stage 2 and stage 3) [67] TS 28.541 (stage 2 and stage 3) [4]
	Plug and Connect		TS 28.314 (stage 1) [59] (see NOTE), TS 28.315 (stage 2) [60], TS 28.316 (stage 3) [61]
	Policy management		TS 28.555 (stage 1) [62] (see NOTE), TS 28.556 (stage 2) [63]
	AI/ML management	ML model management	TS 28.105 (stage 1, stage 2 and stage 3) [66]
	Closed-loop SLS	Communication Service Assurance Control	TS 28.535 (stage 1) [37] (see NOTE), TS 28.536 (stage 2 and stage 3) [38]
	Intent-driven management	Intent Driven Management	TS 28.312 (stage 1, stage 2 and stage 3) [46]

5G related management feature		Supporting management capabilities	Related specifications
	MnS Registry and Discovery	MnS Registry and Discovery	TS 28.537 (stage 1) [39] (see NOTE), TS 28.532 (stage 2 and stage 3) [9] TS 28.622 (stage 2) [32], TS 28.623 (stage 3) [54]
	NPN management		TS 28.557 (stage 1 and stage 2) [47]
	NTN management	NR provisioning; 5GC provisioning	TS 28.532 (stage 2 and stage 3) TS 28.540 (stage 1) [41] (see NOTE) TS 28.541 (stage 2 and stage 3) [4]
	Network and Service Operations for Energy Utilities (NSOEU)	DSO Rapid Discovery and Threshold Monitoring	TS 28.318 (stage 1, stage 2 and stage 3) [69] (see NOTE) TS 28.554 (KPI)

NOTE: This specification is the recommended starting point for implementation of the 5G related management feature.

Annex F (informative): Overview of management capabilities and corresponding solution sets in SBMA

The model driven approach (i.e. usage of CRUD operations specified in TS 28.532 [9] and NRM fragments) can be used to support various types of management capabilities in SBMA. In addition, there are also several management capabilities which are implemented by non-CRUD operations. In the context of SBMA, Management Capability refers to the functional abilities that a management system can offer to monitor, control, and optimize network and service. These management capabilities are offered via standardized service interfaces called MnS. MnS allows these management capabilities to be consumed by internal and external consumers through well-defined APIs. Each MnS instance can combine these SBMA MnS component types A, B and C to deliver a specific management capability (see clause 4.3 combination of MnS components). Table F-1 shows an overview of management capabilities, MnS and corresponding solution sets.

Table F-1: Overview of management capabilities and corresponding solution sets

Management Feature	Management Capability	MnS definition	Solution Sets
Network and network slicing management	NR Provisioning	CRUD operations/notifications (3GPP TS 28.532 [9]) + NR NRM fragment (3GPP TS 28.541 [4])	RESTFUL
			NETCONF/YANG
	5GC Provisioning	CRUD operations/notifications (TS 28.532 [9]) + 5GC NRM fragment (3GPP TS 28.541 [4])	RESTFUL
			NETCONF/YANG
	Network Slicing Provisioning	CRUD operations/notifications (3GPP TS 28.532 [9]) + Network Slicing NRM fragment (3GPP TS 28.541 [4])	RESTFUL
			NETCONF/YANG
		Network slicing provisioning service (3GPP TS 28.531 [8])	RESTFUL
Edge Computing Management	Edge Computing Provisioning	CRUD operations/notifications (3GPP TS 28.532 [9]) + Edge NRM fragment (3GPP TS 28.538 [40])	RESTFUL
Performance Assurance	Performance Metric Collection Control	CRUD operations/notifications (3GPP TS 28.532 [9]) + PM control NRM fragment (3GPP TS 28.622 [32])	RESTFUL
			NETCONF/YANG
		CRUD operations/notifications (3GPP TS 28.532 [9]) + ManagementDataCollection control NRM fragment (3GPP TS 28.622 [32])	RESTFUL
			NETCONF/YANG
		Performance measurement job control (3GPP TS 28.550 [42])	RESTFUL
	Performance Metric Data Report	Streaming data reporting service (3GPP TS 28.532 [9]) + Performance data stream units (3GPP TS 28.550 [42])	RESTFUL+WebSocket+(GPB/ASN.1) (also used by the NETCONF/YANG solution set)
		File data reporting service (3GPP TS 28.532 [9]) + Performance data file format (3GPP TS 28.532 [9])	RESTFUL+(SFTP/FTPES /HTTPS)+XML
	Performance Metric Threshold Monitor Control	CRUD operations/notifications (3GPP TS 28.532 [9]) + Threshold monitoring control NRM fragment (3GPP TS 28.622 [32])	RESTFUL
			NETCONF/YANG
	Performance Metric Threshold Notification	notifyThresholdCrossing notification (3GPP TS 28.532 [9])	RESTFUL (also used by the NETCONF/YANG solution set)
Fault Management	Fault control	CRUD operations/notifications (3GPP TS 28.532 [9]) + FM control NRM fragment (3GPP TS 28.111 [68])	RESTFUL
			NETCONF/YANG
	Fault Notification	Fault Notifications (3GPP TS 28.111 [68])	RESTFUL (also used by NETCONF/YANG)
Trace and MDT management	Trace/MDT data collection control	CRUD operations/notifications (3GPP TS 28.532 [9]) + Trace control NRM fragment (3GPP TS 28.622 [32])	RESTFUL
			NETCONF/YANG
			RESTFUL

Management Feature	Management Capability	MnS definition	Solution Sets
		CRUD operations/notifications (3GPP TS 28.532 [9]) + ManagementDataCollection control NRM fragment (3GPP TS 28.622 [32])	NETCONF/YANG
	Trace/MDT data report	Streaming data reporting service (3GPP TS 28.532 [9]) + Trace/MDT stream date schema definition (3GPP TS 32.423 [45])	RESTFUL+WebSocket+(GPB/ASN.1) (also used by the NETCONF/YANG solution set)
		File data reporting service (3GPP TS 28.532 [9]) + Trace/MDT file date format definition (TS 32.423 [45])	RESTFUL+(SFTP/FTPES /HTTPS)+XML
QoE management	QoE data collection control	CRUD operations/notifications (3GPP TS 28.532 [9]) + QoE Measurement Collection control NRM fragment (3GPP TS 28.622 [32])	RESTFUL NETCONF/YANG
	QoE data report	File data reporting service (3GPP TS 28.532 [9]) + QoE data file format (3GPP TS 26.247 [X])	RESTFUL+XML
File Management	File Retrieval	CRUD operations/notifications (3GPP TS 28.532 [9]) + File retrieval NRM fragment (3GPP TS 28.622 [32])	RESTFUL NETCONF/YANG
	File Download	CRUD operations/notifications (3GPP TS 28.532 [9]) + File download NRM fragment (3GPP TS 28.622 [32])	RESTFUL NETCONF/YANG
Notification subscription and Heartbeat notification control	Subscription Control	CRUD operations/notifications (3GPP TS 28.532 [9]) + Notification subscription and heartbeat notification control NRM fragment (3GPP TS 28.622 [32)	RESTFUL NETCONF/YANG
	Heartbeat Control	CRUD operations/notifications (3GPP TS 28.532 [9]) + Heartbeat notification control NRM fragment (3GPP TS 28.622[32])	RESTFUL NETCONF/YANG
	Heartbeat Notification	notifyHeartbeat notification (3GPP TS 28.532 [9])	RESTFUL
MDA	Management Data Analytic	CRUD operations/notifications (3GPP TS 28.532 [9]) + NRM fragment for MDA request and MDA report (3GPP TS 28.104 [57])	RESTFUL
SON	RANSC Management	CRUD operations/notifications (3GPP TS 28.532 [9]) + RANSC NRM Fragment 3GPP TS 28.317 [67])	RESTFUL
	SON policy	CRUD operations/notifications (3GPP TS 28.532 [9]) + NRM Fragment for DANR/DES/DRACH/DMRO/DPCI/CES/CPCI/DLMO/CCO Management (3GPP TS 28.541 [4])	RESTFUL NETCONF/YANG
Closed-loop SLS	Communication Service Assurance Control	CRUD operations/notifications (3GPP TS 28.532 [9]) + Assurance management NRM fragment (3GPP TS 28.536 [38])	RESTFUL
Intent driven management	Intent Driven Management	CRUD operations/notifications (3GPP TS 28.532 [9]) + NRM fragment for intent driven management (3GPP TS 28.312 [46])	RESTFUL
AI/ML management	ML model Management	CRUD operations/notifications (3GPP TS 28.532 [9]) + NRM fragment for ML model training/testing/ inference emulation control/ ML model loading / inference (3GPP TS 28.105 [66])	RESTFUL
MnS Registry and Discovery	MnS Registry and Discovery	CRUD operations/notifications (3GPP TS 28.532 [9]) + MnS Registry NRM fragment (TS 28.622 [32])	RESTFUL NETCONF/YANG
	MgmtData Registry and Discovery	CRUD operations/notifications (3GPP TS 28.532 [9]) + MnS Registry NRM fragment (TS 28.622 [32])	RESTFUL
MSAC	MnS Access Control	CRUD operations/notifications (3GPP TS 28.532 [9]) + Information model for role based access control (3GPP TS 28.319 [70])	RESTFUL
NSOEU	DSO Rapid Recovery and Threshold Monitoring	CRUD operations/notifications (3GPP TS 28.532 [9])+ DSO Rapid Recovery NRM fragment (3GPP TS 28.318 [12]) + DSO Rapid Recovery NRM fragment(3GPP TS 28.318 [69])	RESTFUL

Management Feature	Management Capability	MnS definition	Solution Sets
External Data Management	External Data Discovery and Request	CRUD operations/notifications (3GPP TS 28.532 [9]) + External data type NRM fragment (TS 28.622 [32])	RESTFUL

Annex G (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2018-09	SA#81					Upgrade to change control version	15.0.0
2018-12	SA#82	SP-181042	0001	1	F	Add management service discovery	15.1.0
2018-12	SA#82	SP-181042	0003	1	F	Update reference to TS 28.532	15.1.0
2018-12	SA#82	SP-181042	0004	2	F	Replace MF with management function	15.1.0
2018-12	SA#82	SP-181042	0005	-	F	Implement MnS naming agreement	15.1.0
2018-12	SA#82	SP-181042	0008	1	F	Add usecase and requirements for MnS Query	15.1.0
2019-06	SA#84	SP-190372	0015	1	B	Add examples of ONAP utilizing the MnSs provided by 3GPP MnS Producer	16.0.0
2019-09	SA#85	SP-190742	0026	1	A	Add description of MnS provided by NF	16.1.0
2019-09	SA#85	SP-190750	0028	2	B	Add 3GPP Management Service deployment based on ZSM Framework	16.1.0
2019-09	SA#85	SP-190742	0031	3	A	Add management coordination with NWDAF	16.1.0
2019-12	SA#86	SP-191219	0039	2	A	Update of Management service description and diagram	16.2.0
2019-12	SA#86	SP-191171	0044	1	B	Add description for management capability support in multiple tenant environment	16.2.0
2019-12	SA#86	SP-191219	0047	2	A	Correction on example of MnS deployment scenario in clause 4.5	16.2.0
2019-12	SA#86	SP-191159	0049	-	F	Some correction on the reference in Clause 5.3	16.2.0
2019-12	SA#86	SP-191152	0051	1	B	Introduce a MnS profile	16.2.0
2019-12	SA#86	SP-191219	0053	1	A	Clarify numerous definitions	16.2.0
2020-03	SA#87E	SP-200227	0056	1	A	Add the missing paradigm of interaction between MnS producer and MnS consumer	16.3.0
2020-03	SA#87E	SP-200180	0057	1	F	Update Clause 5.3 Management service deployment based on ZSM framework	16.3.0
2020-03	SA#87E	SP-200227	0064	2	A	Update of Management service description and diagram	16.3.0
2020-06	SA#88-e	SP-200497	0068	-	B	Add clarifications to description of tenant concept	16.4.0
2020-09	SA#89e	SP-200724	0072	1	F	Add missing definition	16.5.0
2020-09	SA#89e					Adding missing definition due that were missed in CR implementation	16.5.1
2020-12	SA#90e	SP-201050	0073	1	F	Cleanup based on refined slice definition	16.6.0
2020-12	SA#90e	SP-201050	0074	-	F	Add abbreviation reference	16.6.0
2020-12	SA#90e	SP-201056	0075	1	F	Add example of closed loop SLS assurance	16.6.0
2020-12	SA#90e	SP-201088	0076	-	F	Correct inconsistent terminology	16.6.0
2021-03	SA#91e	SP-210145	0077	-	A	Fix errors in Exposure Governance descriptions	16.7.0
2021-09	SA#93e	SP-210864	0086	-	C	Remove unnecessary stage 2 details for discovery of management services	17.0.0
2021-12	SA#94e	SP-211456	0089	1	A	Correcting the Scope	17.1.0
2021-12	SA#94e	SP-211467	0090	-	C	Remove MnS Discovery use case and requirement	17.1.0
2021-12	SA#94e	SP-211468	0092	-	B	Enhance SBMA to support access control	17.1.0
2021-12	SA#94e	SP-211468	0093	-	B	Enhance request-response communication paradigm to support access contro	17.1.0
2021-12	SA#94e	SP-211454	0095	-	A	Fix editorial issues	17.1.0
2022-03	SA#95e	SP-220186	0098	1	F	Add 5G specification information	17.2.0
2023-03	SA#99	SP-230200	0102	1	A	Correct the Management Data Analytics Capability Description	17.3.0
2023-09	SA#101	SP-230940	0107	-	A	Update figure A.1.1	17.4.0
2023-09	SA#101	SP-230970	0110	-	A	Fix incorrect references	17.4.0
2023-12	SA#102	SP-231472	0120	1	B	Add example of RAN domain management capabilities mapped with ZSM	18.0.0
2023-12	SA#102	SP-231472	0121	1	B	Using Management Services to support multiple players interoperability	18.0.0
2023-12	SA#102	SP-231479	0119	1	F	Add a note sentence in clause A.4	18.0.0
2023-12	SA#102	SP-231472	0122	1	B	Overview of the usage of CRUD operations and NRM fragments in SBMA	18.0.0
2024-03	SA#103	SP-240168	0124	1	B	Rel-18 CR TS 28.533 Update Annex F Usage of CRUD operations and NRM fragments to support management capabilities in SBMA	18.1.0
2024-03	SA#104	SP-240808	0128	1	F	Rel-18 CR 28.533 Remove 28-545 reference – partially implemented due to a clash with CR0130r1	18.2.0
2024-03	SA#104	SP-240820	0129	1	F	Rel-18 CR TS 28.533 Update Annex F Usage of CRUD operations and NRM fragments to support management capabilities in SBMA	18.2.0
2024-03	SA#104	SP-240820	0130	1	F	Rel18 CR TS 28.533 Update 5G specifications overview – partially implemented due to a clash with CR0128r1	18.2.0
2024-09	SA#105	SP-241167	0139	-	A	Rel-18 CR 28.533 Correct A.5 Management Data Analytics Service (MDAS)	18.3.0
2024-09	SA#105	SP-241179	0140	-	F	Rel-18 CR TS 28.533 Address clash issues of agreed CR S5-243344 and S5-241191	18.3.0
2024-12	SA#106	SP-241650	0144	1	F	Rel-18 CR TS 28.533 Correct Annex E	18.4.0
2024-12	SA#106	SP-241650	0145	1	F	Rel-18 CR TS 28.533 Correct Annex F	18.4.0
2024-12	SA#106	SP-241640	0146		F	Rel-19 CR TS 28.533 Update the description of deployment scenario for network and network slice	19.0.0
2025-03	SA#107	SP-250160	0147	1	B	Rel-19 CR TS 28.533 Enhance SBMA definitions	19.1.0
2025-06	SA#108	SP-250553	0155	3	F	Rel-19 CR TS 28.533 Update Annex E	19.2.0

2025-06	SA#108	SP-250558	0157		D	Rel-19 CR TS 28.533 Corrections	19.2.0
2025-06	SA#108	SP-250553	0161	1	F	Rel-19 CR 28.533 Clarify combination of MnS components	19.2.0
2025-06	SA#108	SP-250553	0163	1	F	Rel-19 CR TS 28.533 Update figure in Annex E	19.2.0
2025-09	SA#109	SP-251088	0164	1	B	Rel-19 CR TS 28.533 Update Annex F to include the management capabilities related to data management	19.3.0
2025-09	SA#109	SP-251080	0165	1	C	Rel-19 CR TS 28.533 addition of Illustrative architecture reference model for management and orchestration in support of SBMA	19.3.0
2025-09	SA#109	SP-251080	0166	1	C	Rel-19 CR TS 28.533: addition of summary descriptions for functions in support of architecture reference model for management and orchestration	19.3.0
2025-09	SA#109	SP-251101	0168	1	B	Rel-19 CR 28.533 Add details for MnS component versioning	19.3.0
2025-09	SA#109	SP-251278	0169	2	B	Rel-19 CR TS 28.533 Management services exposure	19.3.0
2025-09	SA#109	SP-251080	0170	1	F	Rel-19 CR TS 28.533 Update on Annex F	19.3.0

History

Document history		
V19.3.0	October 2025	Publication