ETSI GR ZSM 019 V1.1.1 (2026-01)

GROUP REPORT

Zero-touch network and Service Management (ZSM);
ZSM Framework for NaaS

Reference
DGR/ZSM-019_GRonNaas

Keywords
abstracted network information, automation

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

Contents

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.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Zero-touch network and Service Management (ZSM).

Modal verbs terminology

In the present document "**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.

Executive summary

The present document examines the ZSM framework in the context of Network-as-a-Service (NaaS), wherein demands for customer-facing services delivered by ZSM-managed network resources, and related ZSM framework consumer demands for ZSM framework management services, may originate with entities that are operated by or on behalf of different organizations, while ZSM management domains may themselves be operated by or on behalf of different organizations. Information, authority, permissions, data privacy or security requirements, etc. may align with or be determined or constrained by such organizational differences; implications of this on the ZSM framework and its components and services are considered. Further, the ZSM framework may leverage abstraction in the operation of management services. However, not all interactions between a ZSM framework and ZSM framework consumers, or among ZSM management domains, will or can be equally abstracted. "Variable abstraction management" thus needs to be accommodated functionally by the ZSM framework. Finally, ZSM management domains and management services may be sources, and/or consumers, of information related to resource use or scarcity, patterns of resource use on behalf of different consuming entities, etc. Such information, how it might be used, and how it might be provided or usefully consumed by ZSM management domains and management services, are considered.

Introduction

ETSI ISG ZSM defines an architecture and a set of services that together provide capabilities for automatic network and service management. Collectively, this architecture and set of services is referred to as the ZSM framework [i.1]. ETSI ISG ZSM has not so far considered, in detail, interactions between the ZSM framework and ZSM framework consumers. This is somewhat natural in the sense that the focus of ISG ZSM lies within the ZSM framework. However, the ZSM framework exists to provide services to ZSM framework consumers. It is therefore logical to consider the ZSM framework in inter-operation with ZSM framework consumers. Consider, for example, a context wherein many different entities - that differ from one another organizationally, legally and/or administratively - are consuming services from a given ZSM framework instance. This particular context arises in the Network-as-a-Service (NaaS) environment, as that term is broadly used. It might require, or benefit from, generating, handling or using information differently among consuming entities, for functional, data privacy or other reasons. This fact might influence consideration of detailed functional requirements on certain ZSM data services.

The present document focuses on several aspects of this context-based examination of the ZSM framework:

- As one aspect: as suggested above, demands for customer-facing services delivered by ZSM-managed network resources, and related ZSM framework consumer demands for ZSM framework management services, may originate with entities that are operated by or on behalf of different organizations. Further, ZSM management domains may themselves be operated by or on behalf of different organizations. Information, authority, permissions, data privacy or security requirements, etc. may align with or be determined or constrained by such organizational differences. How should the ZSM framework be equipped to deal with this? This aspect is the subject of clause 5.

- As a second aspect: the ZSM framework may leverage abstraction in the operation of management services. Abstraction reduces complexity, promotes scalability and facilitates separation of roles and concerns. Intent, as considered in ETSI GR ZSM 011 [i.2] and ETSI GS ZSM 016 [i.3], represents a highly abstracted mode of interaction between ZSM framework consumers and a ZSM framework, or among ZSM management domains. However, not all interactions between a ZSM framework and ZSM framework consumers, or among ZSM management domains, will or can be equally abstracted. For example, while network service commissioning might be based on intent and thus use highly abstracted management service interfaces, other processes - such as auditing and reporting of intent compliance - might require the ZSM framework to assemble and report much less abstracted information to ZSM framework consumers, or among ZSM management domains. "Variable abstraction management" thus needs to be accommodated functionally by the ZSM framework. This aspect is considered in clause 6.

- As a third aspect: ZSM management domains and management services may be sources, and/or consumers, of information related to resource use or scarcity, patterns of resource use on behalf of different consuming entities, etc. Such information might be relevant to revenue management operations - including market segmentation, pricing optimization, dynamic pricing and similar - by ZSM framework consumers or management domains, or entities associated with them, as well as cost optimization processes. Clause 7 considers such information, how it might be used, and how it might be provided or usefully consumed by ZSM management domains and management services.

1 Scope

The present document considers operation of the ZSM framework within a NaaS - Network-as-a-Service - context. Particular functional requirements on the ZSM framework, and its components or supporting technologies, that are identified or accentuated by this contextual examination, are described.

The present document is of relevance to IRTF NMRG and IETF NMOP and will be reported to those groups.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in the present clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI GS ZSM 007: "Zero-touch network and Service Management (ZSM); Terminology for concepts in ZSM".

[i.2] ETSI GR ZSM 011: "Zero-touch network and Service Management (ZSM); Intent-driven autonomous networks; Generic aspects".

[i.3] ETSI GS ZSM 016: "Zero-touch network and Service Management (ZSM); Intent-driven Closed Loops".

[i.4] ETSI GS ZSM 002: "Zero-touch network and Service Management (ZSM); Reference Architecture".

[i.5] IETF Internet Draft: NASR Use Case and Requirements, version 03 updated 2025-04-23, draft-liu-nasr-requirements.

[i.6] IETF Internet Draft: Zero-Trust Sovereign AI: Verifiable Geofencing & Residency Proofs for Cybersecure Workloads, version 03 updated 2025-10-19, draft-lkspa-wimse-verifiable-geo-fence-03/.

[i.7] IETF Internet Draft: Applicability of Abstraction and Control of Traffic Engineered Networks (ACTN) to IETF Network Slicing, version 10 updated 2024-08-29, draft-ietf-teas-applicability-actn-slicing.

[i.8] IETF Internet Draft: SIMAP: Concept, Requirements, and Use Cases, version 07 updated 2025-11-17, draft-ietf-nmop-simap-concept.

[i.9] ETSI GR ZSM 015: "Zero-touch network and Service Management (ZSM); Network Digital Twin".

[i.10] ETSI GS ZSM 018: "Zero-touch network and Service Management (ZSM); Network Digital Twin for enhanced zero-touch network and service management".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

economic information management: generation and consumption, by ZSM framework entities, of information relevant to revenue management and cost optimization processes, by or on behalf of organizations associated with ZSM framework consumers and components

identity management: management, within the ZSM framework, of requirements created by the diversity of organizations associated with ZSM framework consumers and components in a NaaS environment

variable abstraction management: ability of an E2E SMD or MD to tailor abstractions - views of information - as required for various purposes and interactions with diverse components and entities, through controlled pruning or addition and refactoring of information

3.2 Symbols

Void.

3.3 Abbreviations

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

BSS Business Support System
E2E SMD E2E Service Management Domain

NOTE: As defined in ETSI GS ZSM 002 [i.4].

MD Management Domain

NOTE: As defined in ETSI GS ZSM 002 [i.4].

NaaS Network-as-a-Service

4 Description of NaaS

Network as a Service - NaaS - is a term that has been used for some time by industry organizations, in marketing materials and press reports, and to describe some operator products. In different contexts and at different times it has taken on various detailed meanings. In general, however, the term has implied three categories of characteristics: these are described below. All are relevant to a view of NaaS for purposes of the present document. As suggested in the Introduction, that purpose is to create an overall context for use of the ZSM framework that will, ideally, illuminate most or all detailed requirements or constraints on the ZSM framework.

Potential complexity of network service composition: A network service may comprise connectivity only, or both connectivity and non-connectivity components (e.g. firewalls). Connectivity services may be of arbitrary topological complexity, including e.g. point-to-point and multipoint-to-multipoint, and may be based on any network layer technology or combination of layer technologies. Connectivity service components may be individually customized with respect to performance targets or constraints such as bandwidth, latency and availability.

Dynamic network service composition: Network services, network service components and their characteristics may be dynamically created, modified and deleted.

Fragmentation of network service demand sources: Demands for various network services may originate from multiple sources in parallel, and may pass through multiple stages of collection and management in entities (e.g. BSSs) that may be under different ownership and/or administrative responsibility. For example, some network services may originate with retail demands, from enterprises or consumers, provided to a NaaS operator.

Demands aggregated by that NaaS operator may be presented, in parallel with demands from other sources, to a further operator, which assembles and manages all demands for presentation to one or more ZSM frameworks that manage the resources used for network service delivery. See Figure 1: as automation is of interest, network demand sources and aggregators are represented as entities which interoperate using management services provided by the ZSM framework, or similar mechanisms operating among systems lying outside the ZSM framework. Again, every entity may be owned and/or operated by a different administrative entity, including the E2E and management domains within a ZSM framework. Permutations of network service demand sources, in respect of a given ZSM framework instance, may evolve over time.

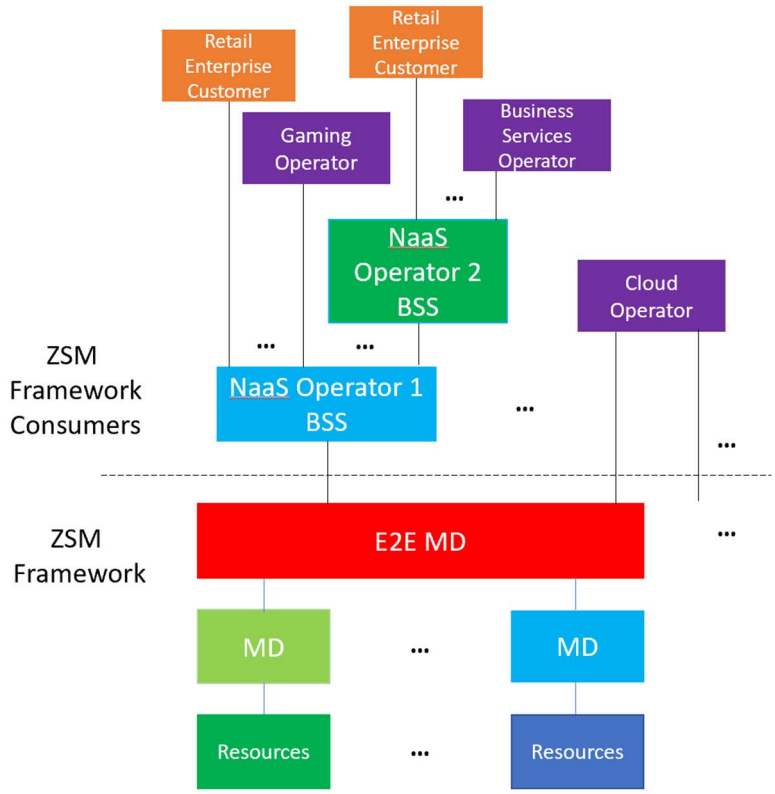

Figure 1: Retail and wholesale network service demand generating entities may interact directly with one or more ZSM frameworks, directly or via one or more NaaS operator entities (e.g. BSSs)

5 Identity management

5.1 Background

As described in clause 4, demands for network services delivered by ZSM-managed network resources, and related ZSM framework consumer demands for ZSM framework management services, may originate with entities that are operated by or on behalf of different organizations. Further, ZSM management domains may themselves be operated by or on behalf of different organizations.

The present clause considers the implications on ZSM management services of organizational diversity among ZSM framework consumers and components.

Organizations may require assured privacy and security of:

a) information which they consider proprietary and sensitive; and

b) command and control of services delivered by, or use of resources belonging to, ZSM frameworks or components of them.

Such assurance requires, first and fundamentally, that ZSM framework components should be able to associate management services, data and managed resources with particular entities or organizations either lying outside the ZSM framework or associated with E2E MDs, MDs or managed resources. Identification of associated entities or organizations provides a basis for managing related restrictions on use of management services, data and managed resources, as well as for differential application of permissions management, authentication, encryption or other security measures. Identifiers, denoting entities or organizations, should be associated with management services, data and managed resources. To maximize anonymity, such identifiers should be generic: for the most part, within the ZSM framework, it is necessary only to distinguish entity or organizational associations one from another, not to fully identify entities or organizations as such.

Identification of associated entities or organizations may also be required for reasons not directly related to privacy or security. Two such reasons, and the use of identity management mechanisms, are considered in clauses 6 and 7.

Specific impacts of these requirements on ZSM components are considered in detail in clause 5.2.

5.2 Supporting framework capabilities and services

The ZSM architecture is based on management services, each of which has a producer and one or more consumers. Functional associations of management services construct virtual entities called management functions (see ETSI GS ZSM 002 [i.4] Appendix C for a representation of management services-management functions relationships). Management functions are often hosted by or associated with specific MDs or E2E SMDs (i.e. the producers - especially - of the implicated management services are hosted by or otherwise associated with a particular MD or E2E MD), while any management services that span inter-MD/E2E SMD boundaries (via the cross-domain integration fabric) represent "inputs" or - perhaps more predominantly - "outputs" of the management function. This is neither required nor rigorous: a management function may in and of itself span MDs/E2E SMDs, by making liberal use of management services that transit the cross-domain integration fabric. Nonetheless, the notions of domain-oriented management functional partitioning and domain hierarchy are intrinsic to the ZSM architecture. As a rule, each interaction between a given MD and another MD or E2E SMD, or between a ZSM framework consumer and an E2E SMD, crosses a boundary that reflects a separation of intrinsic roles, responsibilities, scope of resource control and visibility, visibility of data and information, etc. In the NaaS context - as described in clause 5.1 - it often also represents crossing organizational, administrative and/or ownership boundaries. In and around inter-domain boundaries - here construing the term "domain" broadly to mean all of ZSM framework consumers, E2E SMDs and MDs - is therefore a logical place to concentrate identity management actions and mechanisms within the ZSM framework. Following this, the following identity management principles and measures are proposed:

1) Management service producers hosted by or associated with an E2E SMD should create and manage identifiers (per clause 5.1) that reflect differing identities of extra- (ZSM) framework consumers of those management services. These identifiers subsequently may be associated with particular instances of management service operations or lifecycles, data, managed resources, etc. - see 5) below.

2) Management service producers hosted by or associated with an MD should create and manage identifiers (per clause 5.1) that reflect differing identities of MD- or E2E SMD-hosted or associated consumers of those services. These identifiers subsequently may be associated with particular instances of management service operations or lifecycles, data, managed resources, etc., - see 5) below.

3) Management service producers, or the E2E SMDs or MDs that host them or are associated with them, should maintain any applicable correlations between identifiers received and identifiers generated.

4) As discussed in clause 5.1, identifiers may be generic: they need not in and of themselves reflect any specifics or details of entities they represent; rather, they need serve only to distinguish one such entity from another.

5) Mechanisms should be defined that serve operationally to associate identifiers with particular instances of management service operations or lifecycles, data, managed resources, etc. Such mechanisms could include tokens, session or flow labels, etc. These mechanisms should be operable between ZSM framework consumers and E2E SMDs, such that the former may provide to the latter a basis for identity-based classification of interface interactions.

6) A class of identity policy management services should be created, that can host and provide information related to identity-related policies. Such policies might be used by domains and management services to govern identity-based access to specific data or information, use of control or orchestration services, etc.

It is noted for emphasis that "identities" - for purposes of the present document - refers to organizational identities that correlate differentially to management services and/or data or information produced or consumed by them.

This is distinct from, and incremental to, processes defined elsewhere in ZSM for the registration of, and subscription for use of, management services themselves. The latter processes extend directly to management functions composed of management services.

The present document therefore does not deal with identification of management functions such as agents, closed loops or digital twins as such: only, potentially, with correlation of such management functions to organizational identities.

6 Variable abstraction management

6.1 Background

While it has not been explicitly drawn out within ETSI ISG ZSM documents to date, it is clear that E2E SMDs and MDs should be able to manage the fact that varying degrees of abstraction will feature in interactions among themselves and with framework consumers. This is easily appreciated by considering the following case. Consider an E2E SMD which interacts with a ZSM framework consumer on an intent basis, per ETSI GR ZSM 011 [i.2] and ETSI GS ZSM 016 [i.3]. Network services to be used by the ZSM consumer are negotiated and reported on a highly abstracted basis, using constructs that reflect the defining characteristics of the services, but contain no information about the managed resources that may be used in delivering the services. Now consider that, among the negotiated characteristics of a network service, there may appear constraints such as that all physical network paths and equipment should lie within a particular geographical region, or should lie outside of some particular geographical region. This is sometimes referred to as geofencing. The ZSM consumer might want to see audit reports proving compliance with geofencing constraints. In that case, the E2E SMD might have to generate reports for the consumer that illustrate the geographical locations of network resources. Consider now that the E2E SMD might itself interact with one or more subordinate MDs on an intent basis. In such cases, the E2E SMD would have to call on these MDs to provide contributions to the audit reports, as the E2E SMD might have no direct knowledge about the managed resources being employed by these MDs. Although technologies are being developed that would support alternative (or complementary) approaches to geofencing management and verification, see [i.5] and [i.6], geofencing-related constraints are obvious content for inclusion within network service-defining intents, implying that ZSM frameworks should be able to handle their enforcement and, by extension, related compliance auditing.

This case demonstrates that different levels of abstraction might be required or appropriate, with respect to various management services and operations, between or among the same ZSM consumers and producers.

Another important case is related to network slicing. Hard- or soft-partitioning of network resources allocated for use in the fulfilment of network services for different consumers might be facilitated by the use of abstraction. For example, the consumer might require a certain set of resources (e.g. nodes, links, ports); the MD allocates a subset of its available nodes, links and ports, providing the consumer visibility and/or control of only those resources, representing them as a virtual network comprised of virtual resources.

This is precisely the approach followed by the IETF TEAS (Traffic Engineering and Signalling) Working Group, through its body of work under the framework ACTN (Abstraction and Control of Transport Networks) e.g. [i.7]. This in turn has generated some discussion in the IETF NMOP (Network Management Operations) Working Group, in the context of the work on SIMAP (Service & Infrastructure Map). SIMAP seeks to provide a root infrastructure and services model, and a basis for assembly and reconciliation of other models (e.g. inventory, telemetry) e.g. [i.8]. Such an assembly of models and information might provide the "status snapshot" used by (for example) NDTs, per e.g. ETSI GR ZSM 015 [i.9] and ETSI GS ZSM 018 [i.10]. But how are models representing different levels of abstraction to be reconciled? By definition, models that represent lesser abstraction contain information that models representing greater abstraction do not. More generally, for what purposes should such models be reconciled, and what precisely would needs-driven reconciliation mean?

These are the kinds of issues that are considered in the present clause and mapped to ramifications on ZSM functional and managed services requirements.

The relevance of variable abstraction management to NaaS is clear. Different abstractions are used by and presented to consumers of management services in respect of different operations and according to their different identities, in a controlled and managed fashion.

6.2 Supporting framework capabilities and services

The use of abstraction has a definitive purpose: to manage - to limit, to optimize, to "corral" - complexity. Abstraction manages complexity through controlled omission or pruning of information that is extraneous - that is, not needed for operational purposes - from the point of view of the consumer to, or with whom, the abstraction is presented or used.

This becomes particularly important as network and service scale increase, as the range of network and equipment types and domains rises, etc. Differences in information needed to support management of different operations on different domains derive in part from differences in operations management responsibilities among ZSM components. There is therefore both a natural tendency and a logical reason for ZSM architectures to "abstract up" - that is, for interactions between E2E SMDs and ZSM framework consumers, and between E2E SMDs and MDs, to make use of abstraction. It is also important to see abstractions as actively and differentially managed by MDs and E2E SMDs: differing abstractions - for different purposes - might be presented to or used with different management services, or - importantly - with management service operations corresponding to different entity identities, in the sense of clause 5.

Note that abstraction may be used in respect of data and information generally: e.g. inventory, network and service topology, telemetry, etc.

The implications of the preceding observations might be summarized as follows:

i) Abstractions are managed differentially with respect to different management services and entity identities.

ii) In general, "lower" components in the ZSM framework - i.e. MDs vs. E2E SMDs, and E2E SMDs vs. ZSM framework consumers - may make operational use of, and have access to, information that "higher" (or "adjacent" - one MD vs. another MD) components may not. This derives from the "abstraction up" tendency, and that abstraction means the controlled pruning of information. (Note that, of course, higher ZSM components also have access to information that lower components do not. However, as a rule, such information is strictly irrelevant to, or in some cases perhaps is more firmly withheld from, lower components and their operational responsibilities. It is not a matter of complexity management).

iii) Point ii) above implies that higher ZSM components may sometimes need to augment their normally operationally relevant and accessible information, with information available to lower ZSM components. See, e.g. the geo-fencing compliance audit use case described in clause 5.1. This may need to be done through or across multiple domains. (Note that it is assumed that such information is requested and shared on a transactional basis, rather than simply exposing corresponding data or information services fully to the higher or adjacent ZSM or external components).

These functional aspects reveal two identifiable requirements for abstraction management:

1) Abstraction is an action - controlled pruning of information - that is managed and executed by MDs and E2E SMDs.

2) Abstraction management requires the use of the identity management mechanisms described in clause 5.2.

When requests for information per iii) above are made, it is necessary that there be some basis for specifying the nature of the information to be provided. It may be useful to define information types or classes for this purpose: e.g. real and virtual equipment types & lists, locations, topologies, status, performance, etc. Generative AI tools might also be able to interpret information requests across domain boundaries.

7 Economic information management

7.1 Background

As discussed in the Introduction, ZSM management domains and management services may be sources of information related to resource use on behalf of different consuming entities or organizations, resource availability or scarcity, and patterns of demand presentation to ZSM frameworks or their components. Such information might be used in resource allocation management by ZSM framework components. It may also be used in revenue management operations - including market segmentation, pricing optimization, dynamic pricing and similar - by ZSM framework consumers or entities associated with them.

The present clause considers such information, how it might be used, and how it might be provided by ZSM management domains and management services. This is referred to, in the present document, as economic information management.

A first category of information to consider concerns resource use and scarcity.

Outside of the limited circumstances considered in clause 6 (e.g. use-of-resource audits), ZSM framework consumers are presumed not to know or control the allocation of network resources used in fulfilment of network services on their behalf. This is strictly true in the case of intent-based interactions between ZSM framework consumers and ZSM frameworks, see ETSI GR ZSM 011 [i.2] and ETSI GS ZSM 016 [i.3], but - given the availability of resource orchestration and control management services, closed loops and the fundamental automation objective of ZSM - it is also presumably, if not necessarily strictly, true generally. Consumers thus have no intrinsic means of regulating their use of network resources, nor any intrinsic reason to attempt to do so.

However, the use of a larger quantity of resources by a network service increases the operational (e.g. power consumption) and amortized capital cost of the resources associated with delivering that network service. ZSM frameworks should therefore allocate resources among consumers in some rational way.

Allocation can be based on programmatic rationing: this would require ZSM frameworks to include, or have access to, quotas limiting resource allocation by consumer that presumably would be administered by owners or operators of the resources, or of associated ZSM frameworks or framework components.

Generally, however, in the NaaS framework described in clause 4, resource allocation among consumers may be expected to be managed economically, through network service pricing. Services requiring more resources would be charged higher prices than services requiring fewer resources. This can be done in a range of ways, from use of static or semi-static (i.e. periodically re-set) pricing schema, to use of fully individualized and even dynamic pricing.

Data regarding current and historical aggregate and consumer-specific use of resources or resource classes, as well as related statistics (e.g. average, maximum, minimum, variance, etc.) can be used in support of pricing schemes and algorithms: this data should be generated by ZSM framework components.

Also useful is information related to resource scarcity, which can be derived from aggregate use-of-resource information by complementing it with total available resource information. To be useful, such information typically would be parsed by resource type, class or characteristics (e.g. link latency). Scarce resources might be priced higher than plentiful resources.

Consumers of use-of-resource and resource scarcity information, and of management services making such information available, may lie both within and outside of ZSM frameworks. Note that, as a rule, these consumers do not require detailed identification or description of resource types or classes. As with consumer identification, only generic identification labelling of resource types or classes is generally needed.

ZSM frameworks and framework components are also capable of assembling information related to demand presentation by consumers of network services. As discussed in ETSI GR ZSM 011 [i.2] and ETSI GS ZSM 016 [i.3], consumers may present demands that, following what amounts to negotiation with ZSM frameworks, end up either abandoned or altered before fulfilment. Network service pricing might be a component of such "negotiations" and potentially a key determinant of their outcomes. Both aggregate and consumer-specific data and statistics concerning such negotiations may be useful in at least two ways:

a) It can help owners and administrators of resource domains, and/or related ZSM frameworks or framework components, to assess "latent" network service demand beyond their current capacity to fulfil, or to fulfil cost-effectively, and what new resources would be required to effectively fulfil and "monetize" such latent demand.

b) It can help entities, either outside or inside a ZSM framework, to understand price sensitivities of demand, both in aggregate and with respect to specific network service consumers, and with respect to specific network service characteristics. This information is key to revenue management methods ranging from market segmentation to individualized and dynamic pricing.

Clause 5 described mechanisms by which consumers of management services, managed resources and network services provided by ZSM frameworks may be differentially identified by ZSM framework components and management services. Such identification is obviously a necessary component of consumer-specific use-of-resource data as well as of consumer-specific price sensitivity of demand data.

Specific impacts of these various requirements on ZSM components are considered in detail in clause 7.2.

7.2 Supporting framework capabilities and services

The discussion of clause 7.1 points directly at several essential capability and service requirements, in connection with economic information management:

1) Economic information management requires the use of the identity management mechanisms described in clause 5.2.

2) It may be required or desirable to create new ZSM framework data services, corresponding to economically relevant information categories, and the assembly and controlled sharing or availability of such information by ZSM domains. Such control is facilitated by the use of identity management mechanisms per 1).

3) It may be required or desirable to create new data types, corresponding to economically relevant information categories, to facilitate the transactional exchange of such information among domains, in analogy with requirement iii) of clause 6.2. This may be particularly useful in support of intent-based inter-domain interactions, including interactions between ZSM framework consumers and E2E SMDs.

Summarizing aspects of clause 7.1: particular types of economically relevant information, to be synthesized by ZSM management domains and made available via data services or inter-domain transactions, include:

i) Data related to **use of resources:** this can comprise real-time, historical, and statistical information; it may be assembled and presented in aggregate and identity-specific (in the sense of clause 5) forms; and it may be parsed according to resource types, classes or characteristics (e.g. link latency);

ii) Data related to **resource scarcity:** this is a comparison of resources allocated or in use, to total resources available: it is a fractional measure. Resource scarcity data can comprise real-time, historical, and statistical information; it may be assembled and presented in aggregate and identity-specific (in the sense of clause 5) forms; and, it may be parsed according to resource types, classes or characteristics (e.g. link latency);

iii) Data related to **demand presentation** by consumers of network services: this might comprise historical and statistical information derived from presented demands for network services and the results of any (e.g. intent-style) negotiations, with ZSM frameworks or domains, for delivery or modification of such services. Both aggregate and identity-specific (in the sense of clause 5) forms of such data may be assembled and presented. What resource or service types, classes or characteristics are initially requested; at what times and frequencies they are requested; which resources or service characteristics are provided or indicated as unavailable; and pricing points which are accepted or refused during negotiations - again, by whom, at what times and frequencies, etc. - in respect of particular resource or service types, classes or characteristics - may all be relevant aspects of demand presentation information.

8 Summary and recommendations

The discussions contained in clauses 5 through 7 make clear that identity management, in the sense described in clause 5.1, is the primary and fundamental requirement to support ZSM framework operations in a NaaS context. Such contexts come with fragmentation of network service demand sources, as described in clause 4, which generates a need to correlate these sources with management services and the operations management services may support, and the data they may generate or use.

Clause 5.2 identifies six specific operational aspects of identity management that may need to be supported by ZSM framework entities - management domains and services - in NaaS (and potentially other) contexts.

Clause 6 describes the origins of requirements to support variable abstraction management in the NaaS context. It is partly the desire to manage complexity, driven by large numbers of network services and by separations of responsibility among domains - especially but not necessarily uniquely between ZSM frameworks and their consumers - that drive the use of abstraction. The commercial context is also important: ZSM frameworks belong to one or more organizational entities that sell network services to multiple consumers. This drives separations of roles and responsibilities - beginning with, but not limited to, buying and using a network service versus providing and selling it. But it also drives the complexities and dynamics of network composition discussed in clause 4 that benefit strongly from complexity management through abstraction. The commercial context also makes the economically relevant information, discussed in clause 7, important to manage in the NaaS context.

Clauses 6 and 7 indicate that the identity management capabilities described in clause 6 are required to support variable abstraction management and economic information management. Those clauses also describe other potential requirements related to each case. Some such potential further requirements relate to new types or classes of data or information services or transactional information sharing. The responsibility of management domains to execute pruning and information assembly functions, in support of variable abstraction management, also creates a functional requirement.

Annex A:
Application description

The present annex attaches some example specifics to the generic NaaS organizational-architectural diagram, Figure 1 (in clause 4), and then traces the various aspects dealt with in clauses 5 through 7, while illustrating their utility.

The organizational specifics that define this illustrative example are shown in Figure A.1.

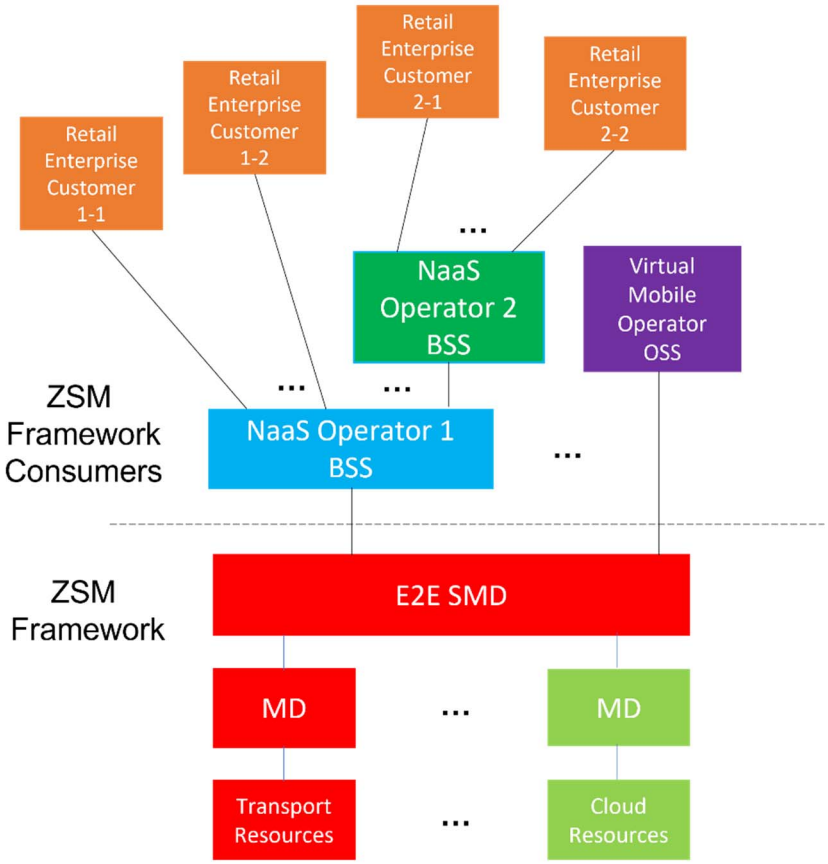

Figure A.1: The ZSM framework consumer and ZSM framework entities and their relative organizational affiliations, as used in the illustrative example of the present annex

The ZSM framework itself consists of an E2E SMD and transport and other resource domains and their associated management domains, which - other than cloud resources - are under the administrative purview of a single operator organization (red boxes). The cloud resources and their associated management domain are under the administrative purview of a separate operator organization (light green boxes). Interactions between the E2E SMD and the MDs are presumed to be intent-based, with - it is further presumed - pricing as a service definition component (and thus a partial basis for intent negotiation). The two operators are in a commercial relationship with one another.

The consumer realm comprises two direct and four indirect ZSM framework consumers, all mapping to different organizational - different business - entities. The direct consumers are network service customers of the E2E SMD operator and are in a commercial relationship with them, while the indirect consumers are network service customers of the direct consumers. The direct consumers aggregate network service demands from the indirect consumers and intermediate their management interactions with the network. The interactions between the direct consumers and the E2E SMD are intent-based, as are the interactions between the indirect consumers and their respective direct consumers: these interactions all cross commercial relationship (i.e. buyer-seller) boundaries. The customers of both NaaS operators are enterprises consuming complex and dynamic network services, with pricing a component of the intent-based interactions. Given this, the NaaS operator systems are effectively BSSs, rather than OSSs, as they assume responsibility for commercial interactions but do not participate, in any real way, in the management of network operations. In the case of the Virtual Mobile Operator (VMO), pricing is assumed not to constitute an element of the intent-based interactions with the E2E SMD, such that the VMO system should be labelled a sort of OSS, but an extremely lightweight one indeed: it only manages the life cycles of network services and plays no role in their operational management. In this case it is presumed that a separate billing system manages the commercial aspects of the relationship, for example on a fixed price or fixed price per use basis.

Identity management: Given the preceding description, it is clear that each of the entities lying within the ZSM framework consumer realm in Figure A.1, should be treated as representing an independent organization for identity management using the methods and mechanisms described in clause 5.2. In the case of the VMO OSS, there is one identity involved.

NOTE: The possibility of multiple network service slices that map to different slice consumer identities is excluded in this example.

In the case of NaaS Operator 1 BSS, there are multiple identities to be managed: NaaS Operator 1 BSS itself, NaaS Operator 2 BSS and Retail Enterprise Customers 1-1 and 1-2 as first-order flow-through identities, and Retail Enterprise Customers 2-1 and 2-2 as second-order flow-through identities. Flow-through identities are constructed by the respective ZSM framework consumer domains using correlations, per item 3) of clause 5.2. The red and green components of the ZSM framework in Figure A.1 represent different organizations and are also mapped to different identities for management per clause 5.2. The mechanisms supporting flow-through identity handling described in item 3) of clause 5.2 operate in this case as well.

With identity management mechanisms thus broadly applied, it is possible to associate management services, or particular operations, permissions and security or data governed or contained by management services, with each of different organizations corresponding to the various system entities within Figure A.1. Examples of use of these mechanisms are presented next, in respect of the abstraction management and economic information management categories considered in clauses 6 and 7. However, while these are important examples of identity management utility in the NaaS case, there may be others of interest.

Variable abstraction management: Since network service management is intent-driven throughout the system architecture instantiation represented by Figure A.1, inter-domain communications for the purposes of network service commissioning are very highly abstracted, consisting only of network service parametric requirements or targets, service performance reports expressed in the same terms, and service life cycle operations commands and responses (per ETSI GR ZSM 011 [i.2] and ETSI GS ZSM 016 [i.3]). No information concerning network resources, network or service topologies, resource status, etc. is required or included in any of this. However, by using the mechanisms described in clause 6.2 - which include, foundationally, the use of identity management mechanisms per clause 5.2 - it is possible to support transfers of information that extend beyond the contents of service intents: for example, lists of equipment types, locations and topologies involved in delivering particular services. The identity management mechanisms themselves ensure appropriate permissions and privacy of such information sharing among organizational entities. For example: NaaS Operator 1 could request and receive a network equipment and topology view, resolved according to the various network services it aggregates on behalf of its enterprise retail customers, of NaaS Operator 2, and even with respect to the enterprise retail customers of NaaS Operator 2, if permissions support that. In particular, transactional or punctual sharing mechanisms are envisaged that would not require the full consumption of native data services by higher framework domains or framework consumer domains. Note that, per clause 6.2, domains should "reach down" recursively to lower domains, as far as possible in order to assemble the information required for each case. A view of equipment locations involved in a given network service, for example, should be assembled from information perhaps available only to individual network management domains.

Economic information management: Clause 7 described economic information in three categories: data related to use of resources, data related to resource scarcity, and data related to demand presentation. In the framework architecture of Figure A.1, there are various domain intersections corresponding to commercial inter-relationships. For illustration purposes, the present annex focuses on the following such intersections: cloud MD to E2E SMD, E2E SMD to NaaS Operator 1 BSS, and NaaS Operator BSS 1 to Enterprise Retail Customers 1-1 and 1-2.

Cloud MD to E2E SMD: It is stipulated that network service interactions are intent-based and that the cloud MD (and set of resources) and E2E SMD are in a commercial relationship in which the organization corresponding to the cloud MD and resources is selling cloud-based services to the organization corresponding to the E2E SMD. In this case, all of resource use, resource scarcity and network service demand presentation (by the E2E SMD to the cloud MD) data may usefully be synthesized by the cloud MD, for use in resource planning and revenue management - whether offer customization, offer segmentation or dynamic pricing - by the cloud operator. One could conceive of cloud MD management services that would be the consumers of the three types of information and producers of planning and revenue management information. Demand presentation data could also reasonably be shared, either as an accessible data service or as punctual reports requested and delivered transactionally, with the E2E SMD, which might use it to support optimization of demand presentation scheduling or of intent parametric details.

E2E SMD to NaaS Operator 1 BSS: Since the E2E SMD and the NaaS Operator 1 BSS are in the same kind of intent-based, network service seller-buyer relationship as the cloud MD and E2E SMD, precisely similar comments to those above, may be made concerning economic information synthesis and consumption by the E2E SMD, and selective sharing with the NaaS Operator 1 BSS.

NaaS Operator 1 BSS to Enterprise Retail Customers 1-1 and 1-2: Since the E2E NaaS Operator 1 BSS and Enterprise Retail Customer 1-1 and 1-2 systems are in the same kind of intent-based, network service seller-buyer relationship as the cloud MD and E2E SMD or E2E SDM and NaaS Operator 1 BSS, precisely similar comments to those in the two prior sections, may be made concerning economic information synthesis and consumption by the NaaS Operator 1 BSS, and selective sharing with the Enterprise Retail Customer 1 and 2 systems. Note that the NaaS Operator 1 BSS "flows through" this information from the E2E SMD, which in turn assembles it based on information provided by the MDs.

Annex B:
Change history

Date	Version	Information about changes
04 2025	0.0.1	Introduction added.
06 2025	0.0.2	Clauses 4, 5.1 and 7.1 added.
11 2025	0.0.3	Clauses 5.2, 6, 7.2, 8 and Annex A added. Clause 3 content added. Editor's notes removed. Table of Contents updated. Stable draft.
12 2025	0.0.4	Technical officer feedback on version 0.0.3 incorporated. Adapted to correct template. Executive summary added. Assorted minor edits proposed. ToC updated. Proposed for adoption.

History

Version	Date	Status
V1.1.1	January 2026	Publication