Zero-touch network and Service Management (ZSM); Requirements based on documented scenarios

Disclaimer

The present document has been produced and approved by the Zero touch network and Service Management (ZSM) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG. It does not necessarily represent the views of the entire ETSI membership.
Contents

Intellectual Property Rights.................................................................................................................7
Foreword..................................................................................................................................................7
Modal verbs terminology.........................................................................................................................7
1 Scope ..................................................................................................................................................8
2 References .........................................................................................................................................8
  2.1 Normative references ....................................................................................................................8
  2.2 Informative references ..................................................................................................................8
3 Definition of terms, symbols and abbreviations .................................................................................9
  3.1 Terms...............................................................................................................................................9
  3.2 Symbols..........................................................................................................................................9
  3.3 Abbreviations ...............................................................................................................................9
4 Introduction .........................................................................................................................................11
5 List of requirements............................................................................................................................13
  5.1 Introduction ..................................................................................................................................13
  5.2 Requirements ...............................................................................................................................13
6 Scenarios ............................................................................................................................................28
  6.1 Introduction ..................................................................................................................................28
  6.2 E2E network and service management .......................................................................................28
    6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration ....28
      6.2.1.1 Network slice lifecycle management ..............................................................................28
        6.2.1.1.1 Description ...............................................................................................................28
        6.2.1.1.2 Rationale and challenges .............................................................................................28
        6.2.1.1.3 ZSM scenario details ..................................................................................................28
        6.2.1.1.4 Related requirements for ZSM ....................................................................................29
        6.2.1.2 Network slice isolation management .............................................................................30
          6.2.1.2.1 Description ...............................................................................................................30
          6.2.1.2.2 Rationale and challenges .............................................................................................30
          6.2.1.2.3 ZSM scenario details ..................................................................................................30
          6.2.1.2.4 Related requirements for ZSM ....................................................................................31
        6.2.1.3 Network slice monitoring ...............................................................................................31
          6.2.1.3.1 Description ...............................................................................................................31
          6.2.1.3.2 Rationale and challenges .............................................................................................31
          6.2.1.3.3 ZSM scenario details ..................................................................................................31
          6.2.1.3.4 Related requirements for ZSM ....................................................................................32
      6.2.1.4 E2E network slicing provisioning in support of 5G services ..............................................32
        6.2.1.4.1 Description ...............................................................................................................32
        6.2.1.4.2 Rationale and challenges .............................................................................................32
        6.2.1.4.3 ZSM scenario details ..................................................................................................32
        6.2.1.4.4 Related requirements for ZSM ....................................................................................33
      6.2.1.5 Performance monitoring of E2E network slicing and service in support of 5G network and service .........................................................................................................................34
        6.2.1.5.1 Description ...............................................................................................................34
        6.2.1.5.2 Rationale and challenges .............................................................................................34
        6.2.1.5.3 ZSM scenario details ..................................................................................................34
        6.2.1.5.4 Related requirements for ZSM framework ...................................................................34
      6.2.2 E2E automation of 5G network slice management and orchestration in support of 5G services (network slice as a service) .........................................................................................34
        6.2.2.1 Exposure to support management and orchestration of NSaaS ....................................34
          6.2.2.1.1 Description ...............................................................................................................34
          6.2.2.1.2 Rationale and challenges .............................................................................................35
          6.2.2.1.3 ZSM scenario details ..................................................................................................35
          6.2.2.1.4 Related requirements for ZSM ....................................................................................35
        6.2.2.2 E2E 5G network slicing management and orchestration in support of 5G services .......35
          6.2.2.2.1 Description ...............................................................................................................35
          6.2.2.2.2 Rationale and challenges .............................................................................................35
          6.2.2.2.3 ZSM scenario details ..................................................................................................35
          6.2.2.2.4 Related requirements for ZSM ....................................................................................35

6.2.2.2.1 Description ........................................................................................................... 35
6.2.2.2.2 Rationale and challenges ...................................................................................... 36
6.2.2.2.3 ZSM scenario details ........................................................................................ 36
6.2.2.2.4 Related requirements for ZSM ............................................................................. 36
6.2.3 Automation of E2E network and service management ........................................... 36
6.2.3.1 Zero-touch full automation of 5G network and service management ..................... 36
6.2.3.1.1 Description .......................................................................................................... 36
6.2.3.1.2 Rationale and challenges ..................................................................................... 37
6.2.3.1.3 ZSM scenario details ........................................................................................ 37
6.2.3.1.4 Related requirements for ZSM ............................................................................. 38
6.2.3.2 Automated network bandwidth management ........................................................ 38
6.2.3.2.1 Description .......................................................................................................... 38
6.2.3.2.2 Rationale and challenges ..................................................................................... 38
6.2.3.2.3 ZSM scenario details ........................................................................................ 39
6.2.3.2.4 Related requirements for ZSM ............................................................................. 39
6.2.3.3 ZSM automated healing ........................................................................................ 39
6.2.3.3.1 Description .......................................................................................................... 39
6.2.3.3.2 Rationale and challenges ..................................................................................... 40
6.2.3.3.3 ZSM scenario details ........................................................................................ 40
6.2.3.3.4 Related requirements for ZSM ............................................................................. 40
6.2.3.4 Automatic E2E network and service topology management ................................. 40
6.2.3.4.1 Description .......................................................................................................... 40
6.2.3.4.2 Rationale and challenges ..................................................................................... 40
6.2.3.4.3 ZSM scenario details ........................................................................................ 41
6.2.3.4.4 Related requirements for ZSM ............................................................................. 41
6.2.3.5 Zero-touch E2E 5G network and service management as well as orchestration including edge computing ................................................................. 42
6.2.3.5.1 Description .......................................................................................................... 42
6.2.3.5.2 Rationale and challenges ..................................................................................... 42
6.2.3.5.3 ZSM scenario details ........................................................................................ 42
6.2.3.5.4 Related requirements for ZSM ............................................................................. 43
6.2.3.6 Automatic software deployment ........................................................................... 43
6.2.3.6.1 Description .......................................................................................................... 43
6.2.3.6.2 Rationale and challenges ..................................................................................... 43
6.2.3.6.3 ZSM scenario details ........................................................................................ 44
6.2.3.6.4 Related requirements for ZSM ............................................................................. 44
6.2.3.7 Automatic software upgrade ............................................................................... 45
6.2.3.7.1 Description .......................................................................................................... 45
6.2.3.7.2 Rationale and challenges ..................................................................................... 45
6.2.3.7.3 ZSM scenario details ........................................................................................ 45
6.2.3.7.4 Related requirements for ZSM ............................................................................. 45
6.2.3.8 Automation using policies .................................................................................... 46
6.2.3.8.1 Description .......................................................................................................... 46
6.2.3.8.2 Rationale and challenges ..................................................................................... 46
6.2.3.8.3 ZSM scenario details ........................................................................................ 46
6.2.3.8.4 Related requirements for ZSM ............................................................................. 47
6.2.3.9 Closed loop automation ....................................................................................... 48
6.2.3.9.1 Description .......................................................................................................... 48
6.2.3.9.2 Rationale and challenges ..................................................................................... 48
6.2.3.9.3 ZSM scenario details ........................................................................................ 48
6.2.3.9.4 Related requirements for ZSM ............................................................................. 49
6.2.3.10 Full automation of VNF provisioning ................................................................. 49
6.2.3.10.1 Description ........................................................................................................ 49
6.2.3.10.2 Rationale and challenges ................................................................................... 49
6.2.3.10.3 ZSM scenario details ........................................................................................ 49
6.2.3.10.4 Related requirements for ZSM .......................................................................... 50
6.2.3.11 Automated detection of services offered by management domains .................... 50
6.2.3.11.1 Description ........................................................................................................ 50
6.2.3.11.2 Rationale and challenges ................................................................................... 50
6.2.3.11.3 ZSM scenario details ........................................................................................ 50
6.2.3.11.4 Related requirements for ZSM .......................................................................... 50
6.2.3.12 Service management by 3GPP management system and ETSI NFV MANO .... 51
6.2.3.12.1 Description ........................................................................................................ 51
6.2.3.12.2 Rationale and challenges ................................................................................... 51
6.2.3.12.3 ZSM scenario details ........................................................................................ 51
6.2.3.12.4 Related requirements for ZSM .......................................................................... 51
<table>
<thead>
<tr>
<th>Section</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4.10.4</td>
<td>Related requirements for ZSM</td>
</tr>
<tr>
<td>6.5</td>
<td>Collaborative/federated service management</td>
</tr>
<tr>
<td>6.5.1</td>
<td>Communication services hosted across multiple operators</td>
</tr>
<tr>
<td>6.5.1.1</td>
<td>Description</td>
</tr>
<tr>
<td>6.5.1.2</td>
<td>Rationale and challenges</td>
</tr>
<tr>
<td>6.5.1.3</td>
<td>ZSM scenario details</td>
</tr>
<tr>
<td>6.5.1.4</td>
<td>Related requirements for ZSM</td>
</tr>
<tr>
<td>6.5.2</td>
<td>Private communication services hosted by an operator</td>
</tr>
<tr>
<td>6.5.2.1</td>
<td>Description</td>
</tr>
<tr>
<td>6.5.2.2</td>
<td>Rationale and challenges</td>
</tr>
<tr>
<td>6.5.2.3</td>
<td>ZSM scenario details</td>
</tr>
<tr>
<td>6.5.2.4</td>
<td>Related requirements for ZSM</td>
</tr>
<tr>
<td>6.5.3</td>
<td>Automation in multi-stakeholder ecosystems</td>
</tr>
<tr>
<td>6.5.3.1</td>
<td>Description</td>
</tr>
<tr>
<td>6.5.3.2</td>
<td>Rationale and challenges</td>
</tr>
<tr>
<td>6.5.3.3</td>
<td>ZSM scenario details</td>
</tr>
<tr>
<td>6.5.3.4</td>
<td>Related requirements for ZSM</td>
</tr>
<tr>
<td>6.6</td>
<td>Security</td>
</tr>
<tr>
<td>6.6.1</td>
<td>Troubleshooting of encrypted traffic in ZSM framework</td>
</tr>
<tr>
<td>6.6.1.1</td>
<td>Description</td>
</tr>
<tr>
<td>6.6.1.2</td>
<td>Rationale and challenges</td>
</tr>
<tr>
<td>6.6.1.3</td>
<td>ZSM scenario details</td>
</tr>
<tr>
<td>6.6.1.4</td>
<td>Related requirements for ZSM</td>
</tr>
<tr>
<td>6.6.2</td>
<td>Testing</td>
</tr>
<tr>
<td>6.6.2.1</td>
<td>Automated system test in production network</td>
</tr>
<tr>
<td>6.6.2.2</td>
<td>Description</td>
</tr>
<tr>
<td>6.6.2.3</td>
<td>Rationale and challenges</td>
</tr>
<tr>
<td>6.6.2.4</td>
<td>ZSM scenario details</td>
</tr>
<tr>
<td>6.6.2.5</td>
<td>Related requirements for ZSM</td>
</tr>
<tr>
<td>6.6.3</td>
<td>Automated test capabilities concerning ZSM</td>
</tr>
<tr>
<td>6.6.3.1</td>
<td>Description</td>
</tr>
<tr>
<td>6.6.3.2</td>
<td>Rationale and challenges</td>
</tr>
<tr>
<td>6.6.3.3</td>
<td>ZSM scenario details</td>
</tr>
<tr>
<td>6.6.3.4</td>
<td>Related requirements for ZSM</td>
</tr>
<tr>
<td>6.6.4</td>
<td>Tracing</td>
</tr>
<tr>
<td>6.6.4.1</td>
<td>Automated tracing capabilities</td>
</tr>
<tr>
<td>6.6.4.2</td>
<td>Description</td>
</tr>
<tr>
<td>6.6.4.3</td>
<td>Rationale and challenges</td>
</tr>
<tr>
<td>6.6.4.4</td>
<td>ZSM scenario details</td>
</tr>
<tr>
<td>6.6.4.5</td>
<td>Related requirements for ZSM</td>
</tr>
<tr>
<td>6.6.5</td>
<td>Integration/interoperation</td>
</tr>
<tr>
<td>6.6.5.1</td>
<td>ZSM framework as entity in an ecosystem</td>
</tr>
<tr>
<td>6.6.5.2</td>
<td>Description</td>
</tr>
<tr>
<td>6.6.5.3</td>
<td>Rationale and challenges</td>
</tr>
<tr>
<td>6.6.5.4</td>
<td>ZSM scenario details</td>
</tr>
<tr>
<td>6.6.5.5</td>
<td>Related requirements for ZSM</td>
</tr>
</tbody>
</table>

Annex A (informative): Change History
Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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". This is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, 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.

Foreword

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

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.
1 Scope

The present document defines requirements on the zero-touch E2E (End-to-End) network and service management. Scenarios will be documented and used to derive the requirements.

The requirements will also be considered for the work on the topics Zero-touch network and Service Management (ZSM) reference architecture [1], ZSM End to end management and orchestration of network slicing [i.7], and ZSM Inter management domain lifecycle management [i.8].

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

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

The following referenced documents are necessary for the application of the present document.

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

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

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 this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GR ZSM 005: "Zero-touch network and Service Management (ZSM); Means of Automation".

[i.2] ETSI GR NFV-IFA 023: "Network Functions Virtualisation (NFV); Management and Orchestration; Report on Policy Management in MANO; Release 3".

[i.3] ETSI TS 128 530 (V15.1.0): "5G: Management and orchestration; Concepts, use cases and requirements (3GPP TS 28.530 version 15.1.0)".


[i.5] ETSI TS 138 300 (V15.6.0): "5G; NR; Overall description; Stage-2 (3GPP TS 38.300 version 15.6.0)".

[i.6] ETSI TS 123 501 (V15.5.0): "5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 version 15.5.0)".
3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GS ZSM 007 [2] and the following apply:

NOTE: If the same term is defined in both ETSI GS ZSM 007 [2] and in the present document, the definition in the present document takes precedence.

data governance: processes to define and enforce access restrictions to data, and to attach related metadata to the data

federated orchestration: orchestration performed by multiple autonomous management domains

NOTE: Autonomous domains in this context is related to independent (or self-regulating), not to be confused with the degree of automation.

hierarchical orchestration: orchestration decomposed into one or more hierarchical interactions where parts of the service are delegated to a sub-ordinate orchestrator

key performance indicator: measurement of a specific aspect of the performance of a service that can be used in a service level objective

service level agreement: part of a business agreement between a service provider and a customer, specifying the committed service quality and quantity in terms of service level specifications, and the associated consequences in case the service level objectives are not met

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS ZSM 007 [2] and the following apply:

NOTE: If the same abbreviation is defined in both ETSI GS ZSM 007 [2] and in the present document, the definition in the present document takes precedence.

3GPP 3rd Generation Partnership Project
5GC 5G Core
AI Artificial Intelligence
AMF Access and Mobility management Function
AR Augmented Reality
BBU BaseBand Unit
BSS Business Support System
CD Continuous Delivery
CEM Customer Experience Management
CFS Customer Facing Service
CI Continuous Integration
CPU Central Processing Unit
CSC Customer Service Consumer
CSP Communication Service Provider
DCN Data Centre Network
DN Data Network
Introduction

The present document describes the scenarios and requirements for zero-touch network and service management investigated by the ETSI ISG ZSM with the focus on automation as well as an E2E perspective.

These scenarios and derived requirements are used in other documents by ETSI ISG ZSM such as ETSI GS ZSM 002 [1], ETSI GS ZSM 003 [i.7] and ETSI GS ZSM 008 [i.8].

The scenarios and requirements allow the ZSM reference architecture and corresponding solutions to be aligned in scope and to be industry-relevant. The scenarios are grouped into key areas for automation and zero-touch operation respectively. They show the value of the ZSM framework reference architecture towards an E2E view and towards automated management functionalities as well as management services applicable to future-proof scenarios. Legacy environments are also considered for incremental deployment of automation and zero-touch technologies.
Analysing the scenarios and requirements from another angle allows identifying categories in slightly different dimensions such as:

- Scenarios and requirements related to use cases and which are more technology- or implementation-specific, e.g. network slicing management, edge computing, applied in 5G network, etc.
- Scenarios and requirements that can be considered as building blocks for automatic management for example concerning software management, policy management, bandwidth management, AI techniques, security management, etc.
- Scenarios and requirements that describe ways of implementing E2E automation and zero-touch management, e.g. closed loop automation, coordination between domains, integration of management services, etc.

These different viewpoints can be helpful in case the goal of the reader/stakeholder is to derive priorities among the requirements.

The scenario categories are listed below with short descriptions concerning their contents.

**E2E network and service management**

The scenarios and requirements that are categorized into this group are related to automating the operational tasks of managing the network. The scope of the ETSI ISG ZSM covers the management of the different technological domains such as Core, RAN and Transport domains, and also includes the management of different types of resources such as VNFs, SDNs, virtual and physical resources, etc. This scenario category focuses on the automation of E2E lifecycle management of all of different types of the network resources and services, including installation, commissioning, configuration, day-2 operations, software upgrades and decommissioning. This category also includes the E2E management solutions for network slicing such as network slice cloning, isolation of network slices to ensure a sufficient level of independency between the network slice instances with tolerable interference, cross-domain network slicing management capability, etc.

**Network-as-a-Service (NaaS)**

This group focuses on the need for service capabilities exposure from all domains to enable zero touch automation, and to allow for a seamless integration of new products in the network. Network slicing is taken as an example to show what capabilities could be exposed from each domain to allow E2E automation management.

**Analytics & machine learning**

This group focuses on the scenarios that drive the need for analytics, machine learning and AI capabilities in the ZSM framework. Examples of business requirements that are categorized into this group include the capability to determine the root cause of a network anomaly, and the capability to predict network capacity exhaustion. These requirements drive further functional requirements such as collection of historical data, access to continuous up-to-date network traffic information and ML sandbox environment for self-learning. Analytics and machine learning capabilities are used in the closed-loop automation of the ZSM framework.

**Collaborative/federated service management**

This group focuses on the business requirements for management and collaboration across multiple operators' domains. An example of requirement includes the advertisement and discovery of the management services from other operators' management domains.

**Security**

Security, regulatory and privacy requirements for ZSM framework reference architecture are captured in ETSI ZSM 002 [1], and there are a few security-related requirements that are included in other groups such as NaaS and analytics & machine learning. This security group captures additional security-related features such as the handling of decrypting management traffic for troubleshooting purposes.

**Testing**

Testing group captures the business requirements for features such as automated testing of a managed resource as it is being deployed or testing of an E2E service in the production network. These automated testing features could be incorporated into the closed-loop automation of a resource or service deployment, and in support of finding the root cause of an anomaly. Additionally, requirements related to CI/CD for network services and the automated testing capabilities in connection with AI and machine learning functionalities are also included in this group.
Tracing

Tracing group includes the business requirements for automated tracing that can be triggered by events such as anomaly detection where troubleshooting and root cause analysis need to be performed. Automated tracing capabilities and execution are based on information such as rules, policies, data models, configuration data, etc.

Integration/interoperation

This group focuses on the integration and interoperation between the ZSM framework and other entities such as ZSM framework consumers e.g. user portal, other providers' domains, and human interactions.

5 List of requirements

5.1 Introduction

This clause lists the requirements which are derived from the documented scenarios in clause 6 to the corresponding scenarios are included in the table for each of the requirements. The requirements are assigned to different categories.

For further clarifications and the related detailed context of the requirements, please refer to clause 6.

Some of these requirements are further refined and broken down into multiple functional and non-functional requirements for example in ETSI GS ZSM 002 [1].

5.2 Requirements

Requirements captured from clause 6 are listed in the table 5.2-1.

Table 5.2-1: Requirements based on documented scenarios that are described in clause 6

<table>
<thead>
<tr>
<th>Req. #</th>
<th>Scenario category</th>
<th>Requirements</th>
<th>Clause of the related scenario</th>
<th>Scenario title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration</td>
<td>ZSM framework shall support the capability of cloning of network slice instance(s).</td>
<td>6.2.1.1</td>
<td>Network slice lifecycle management</td>
</tr>
<tr>
<td>2</td>
<td>6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration</td>
<td>ZSM framework shall support the capability of identifying network functions and resources by analysing the requirements for creating network slice instances.</td>
<td>6.2.1.1</td>
<td>Network slice lifecycle management</td>
</tr>
<tr>
<td>3</td>
<td>6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration</td>
<td>ZSM framework shall support the capability of analysing the status of the network resources in the commissioning phase.</td>
<td>6.2.1.1</td>
<td>Network slice lifecycle management</td>
</tr>
</tbody>
</table>