ETSI GS ZSM 007 V2.1.1 (2023-04)

Zero-touch network and Service Management (ZSM); Terminology for concepts in ZSM

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.

Reference
RGS/ZSM-007ed211_Terminology

Keywords
management, service, terminology, vocabulary

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 Web server (https://ipr.etsi.org/).

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™** and **LTE™** 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 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 provides a glossary of terms and concepts related to Zero-touch network and Service Management (ZSM) with the goal to achieve a common language across all the ETSI ISG ZSM deliverables and to serve as terminology reference for use across the industry. Where necessary, verbose descriptions providing background for formal concise definitions will be documented.

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.

Not applicable.

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] MEF Reference Wiki.

[i.2] ETSI GR NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.3] ETSI GS ZSM 002: "Zero-touch network and Service Management (ZSM); Reference Architecture".

3 Definition of terms, symbols and definitions

3.1 Terms

0-9

Void.

A

access control: framework and procedures that authenticate and authorize a management service consumer, and trace the activities of the consumer according to SLA and other policies or regulations

artificial intelligence: algorithms that are capable of human-like traits, e.g. knowledge representation, reasoning, planning, learning, and acting, and decides on actions to be taken that maximizes the chances of achieving a target goal

authorized consumer: service consumer, inside or outside a given management domain, that is allowed to use the offered services

B

Void.

C

cross-domain data services: services that allow to share data with authorized consumers across management domains

D

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

domain service: service that is managed by a management domain

E

End-to-End Service (E2ES): CFS composed from RFSs and/or CFSs originating from one or multiple domains

E2E service management domain: management domain specialized to manage E2E services

explainable machine learning: machine learning model that can explain its decisions to humans in a comprehensible manner

external visibility: property of a ZSM service that indicates whether the scope of the service consumption spans outside the management domain

NOTE: Conventions for external visibility are defined in clause 3.4 of ETSI GS ZSM 002 [i.3].

F

fair machine learning: machine learning model that which ensure biases in the data and/or model inaccuracies do not result in unwanted preferences towards individuals or groups

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.

G

Void.

H

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

I

integration fabric: management function that plays both the roles of service consumer and service producer and which facilitates the interoperation and communication between management functions

intent-based interface: interface to phrase the consumer request(s) of what is required in a declarative form

J

Void.

K

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

L

Void.

M

machine intelligence: algorithms that leverage artificial intelligence and machine learning to enable autonomic (zero-touch) network and service management

machine learning: algorithms that can "learn" from data and improve the ability of executing a target goal, mainly based on recognizing patterns in historical and/or operational data and applying the recognized patterns to new input data

machine learning sandbox: synthetic environment that is isolated from production environment where network behaviour is represented, and machine learning algorithms can safely execute and use real and/or synthetic data

managed entity: managed resource, managed service or closed loop

NOTE: Examples of managed entities are infrastructure resources, such as Virtual Network Functions (VNFs), Physical Network Functions (PNFs), and services such as cloud services, NFV network services, CFSs, RFSs.

managed resource: resource that is managed by one or more ZSM services

managed service: service that is managed by one or more ZSM services

management domain: scope of management that federates together management services, that enables their exposure towards external service consumers and that is delineated by a business, administrative, technological or other boundary

management function: logical entity playing the roles of service consumer and/or service producer

management service: See "ZSM service".

N

Network Function (NF): functional block within a network infrastructure that has well-defined external interfaces and well-defined functional behaviour

NOTE: In practical terms, a network function is today often a network node or physical appliance (ETSI GR NFV 003 [i.2]).

Network Service (NS): composition of network function(s) and/or network service(s), defined by its functional and behavioural specification

NOTE: See https://wiki.mef.net/display/CESG/Services.

O to P

Void.

Q

QoT: metric that describes or measures the trustworthiness aspects in machine learning

NOTE 1: Trustworthiness aspects may include explainability, fairness, robustness, etc.

NOTE 2: ML QoT may apply for ML data or ML model.

R

risk: likelihood of a threat source exploiting a vulnerability and the corresponding business impact

risk analysis: process that comprehends the nature of risk and determines the level of risk

robust machine learning: machine learning model that is resilient to adversarial attacks (e.g. data poisoning, model leakage), that can handle unintentional errors (e.g. missing data, data drift), that have safeguard mechanisms (e.g. fallback to rule-based algorithms) put in place to deal with unexpected outcomes and that are reproducible

S

security assurance: processes and functionalities that evaluate and assess security of a management product

self-configuration: process by which an entity automatically configures itself, without human direct intervention

self-healing: process by which an entity perceives that it is not operating correctly and makes the necessary adjustments to restore itself to normality, without human intervention

self-monitoring: process by which an entity monitors its own behaviour

self-optimization: process by which an entity autonomously and continuously optimizes itself by adapting to the environment

self-scaling: process by which an entity is able to automatically add and/or remove resources or instances

service capability: specific part of a ZSM service

NOTE: Examples of service capabilities are defined in the sub-clauses "Provided management services" of clauses 6.3, 6.4, 6.5 and 6.6 of ETSI GS ZSM 002 [i.3].

service consumer: role of an entity consuming one or more ZSM services

service end-point: interface through which service capabilities are offered and consumed

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

service level objective: element in a service level specification that is defined in terms of parameters, and related metrics, thresholds and tolerances associated with the parameters

service level specification: specification of the minimum acceptable standard of service

service producer: role of an entity offering one or more ZSM services

T

tenant: representation of user/group of users/organization that obtained access to the shared application

threat: any potential danger that is associated with the exploitation of a vulnerability

trust model: model that describes ways in which organizations can obtain the levels of trust needed to form partnerships, collaborate with other organizations, share information, or receive information

trustworthy machine learning: machine learning model that respects applicable laws, regulations, ethical principles, values, and is robust from a technical perspective while considering its social environment

NOTE 1: The proposed EU regulation for machine learning divides machine learning systems into three categories:

i) unacceptable-risk machine learning systems;

ii) high-risk machine learning systems; and

iii) limited- and minimal-risk machine learning systems.

Based on those risk levels, the proposed EU regulation for machine learning has put forward a set of seven key requirements that machine learning systems should meet for them to be considered trustworthy:

i) human agency and oversight;

ii) technical robustness and safety;

iii) privacy and data governance;

iv) transparency;

v) diversity, non-discrimination, and fairness;

vi) accountability; and

vii) societal and environmental well-being.

The details on each of those seven requirements are presented in Annex C.

NOTE 2: Source: [i.1].

U

Void.

V

vulnerability: weakness in a system that allows a threat source to compromise its security

W to Y

Void.

Z

ZSM framework: set of services that together provide capabilities for the automatic network and service management