ETSI GS ZSM 014 V1.1.1 (2024-03)

GROUP SPECIFICATION

Zero-touch network and Service Management (ZSM); ZSM security aspects

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

DGS/ZSM-014_SecAspects

Keywords

automation, closed control loop, network,
security, service

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

Important notice

The present document can be downloaded from:
https://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

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 defines the security reference architecture for the Zero-touch network and Service Management (ZSM) framework based on a set of security capabilities.

The present document specifies a set of security capabilities as management services, complementing the existing management services defined in ETSI GS ZSM 002 [1], which including adaptive trust relationship between management domains, dynamic access control and exposure of ZSM service, robustness of AI/ML model, automatic security governance of management service producer.

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 012: "Zero-touch network and Service Management (ZSM); Enablers for Artificial Intelligence-based Network and Service Automation".

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] NIST 800-39: "Managing Information Security Risk".

[i.2] Information Technology Laboratory of NIST Computer Security Resource Center: "Trust Relationship".

[i.3] ETSI GR ZSM 010: "Zero-touch network and Service Management (ZSM); General Security Aspects".

[i.4] GSMA Network Equipment Security Assurance Scheme (NESAS).

[i.5] ETSI TR 133 916 (V15.1.0): "Universal Mobile Telecommunications System (UMTS); LTE; Security Assurance Methodology (SCAS) for 3GPP network products (Release 15)".

[i.6] draft-ietf-scitt-architecture-04: "An Architecture for Trustworthy and Transparent Digital Supply Chains".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

security profile/descriptor: list of characteristics of a management service producer which influences security risk surfaces of the management service producer

NOTE: The profile includes, for example, hardware and software technology and architecture information, functionalities, external and internal interfaces/APIs, etc., of the management service producer.

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

3.2 Symbols

Void.

3.3 Abbreviations

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

AAA	Authentication, Authorization & Auditing
AI	Artificial Intelligence
BSS	Business Supporting System
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DLP	Data Leak Prevention
DoS	Denial of Service
E2E	End to End
E2ES	End-to-End Service
HW	HardWare
IDS	Intrusion Detection System
IT	Information Technology
ML	Machine Learning
MnF	Management Function
MnS	Management Service
QoT	Quality of Trustworthiness
SDO	Standard Developing Organisation
SLA	Service-Level Agreement
SSO	Single Sign On
TLS	Transport Layer Security
WAF	Web Application Firewall

4 Security requirements

4.1 General security requirements

4.1.1 Trust relationship requirement

This clause defines requirements to support adaptive trust relationship between management domains of ZSM framework, as well as trust of third party by ZSM framework if necessary.

NOTE: In ZSM context, trust relationship represents the trust established among ZSM management domains (refer to [i.2]). It is governed by criteria for secure interaction, behaviour, and outcomes relative to the protection of management services/functions of the management domains, or by policies that how does management function in differing management domains honour each other's authorizations (refer to [i.3]).

[trust-01] The ZSM framework reference architecture shall support capability to evaluate trustworthiness of ZSM entities within or across management domain(s).

[trust-02] The ZSM framework reference architecture shall support capability to decide trust model and trust relationship between two ZSM entities within or across management domains based on trustworthiness of the ZSM entities.

[trust-03] The ZSM framework reference architecture shall support capability to re-evaluate the trustworthiness of a ZSM entity to reflect any change on the ZSM entity in the ZSM framework.

[trust-04] The ZSM framework reference architecture shall support capability to re-build the trust model for a ZSM entity and re-establish trust relationship between the changed ZSM entity and other ZSM entities to reflect any change on the ZSM entity in the ZSM framework.

[trust-05] The ZSM framework reference architecture shall support capability to apply corresponding security controls on ZSM entities based on trust relationship between the ZSM entities.

4.1.2 Access control requirement

This clause defines requirements to support access control on ZSM services.

[AC-01] The ZSM framework reference architecture shall support dynamic identity management (e.g. create, read, update and delete identity) of various type of MnS consumer and producer.

NOTE 1: MnS consumer can be ZSM framework consumer, MnF, domain integration fabric, digital portal acting on behalf of system administrator, etc., MnS producer can be MnF.

[AC-02] The ZSM framework reference architecture shall support dynamic authentication policy management (e.g. create, read, update and delete policies) for each MnS consumer and producer.

NOTE 2: The authentication policies may include authentication factor (e.g. single factor, multi-factors, etc.), authentication mode (e.g. local authentication, domain authentication, common authentication, SSO, etc.), authentication protocol (e.g. TLS, SAML2.0, OpenID, basic user/password, Kerberos, etc.), and other context adaptive information (e.g. different anthemion factor may be applied to different location and time the consumer authenticates to the ZSM framework).

[AC-03] The ZSM framework reference architecture shall support capability to generate consolidated authentication policy based on MnS consumer and producer(s) of multiple management domains.

[AC-04] The ZSM framework reference architecture shall support capability to authenticate MnS consumer and producer based on authentication policy.

NOTE 3: MnS consumer authentication (e.g. validate identity and credentials of MnS consumer, and optionally return token/assertion to the consumer) is proceeded on integration fabric. MnS producer authentication (e.g. validate identity and credentials of MnS producer) is performed by the MnS consumer intends to access MnSs provided by the MnS producer.

[AC-05] The ZSM framework reference architecture shall support dynamic authorization/access control policy management (e.g. create, read, update, delete, etc.) for each group/role of MnS consumers based on clearance of the group/role and classification of MnSs to be accessed.

NOTE 4: The authorization/access control policies are business logic dependent, which describes right subject has the right access to the right resource/object at the right time for the right reasons, generally it may include, e.g.:

- Who: subject (user/entity or group or role) accessing management services.

- What: object (MnS or group of MnSs) and operations on the object.
- When: timeframe to access specific MnS.
- Where: region/location to access specific MnS.
- Why: reason to access specific MnS.

All access should be denied unless explicitly allowed in the policies.

NOTE 5: Clearance of the group/role of MnS consumers could be e.g. SLA, industry, region of the group of MnS consumers, and mission of the role of MnS consumers. Classification of MnS could be e.g. security level, applied industry, region and security status of the MnS.

NOTE 6: Integration fabric, analytics and intelligence management services may be involved for dynamic authentication and authorization policy management.

[AC-06] The ZSM framework reference architecture shall support capability to generate and grant permissions to an authenticated MnS consumer based on access control policies of group/role of the MnS consumer in multiple domains and security context of the MnS consumer.

NOTE 7: Security context of the MnS consumer could be e.g. time, location, security status of the MnS consumer, and reason of accessing.

[AC-07] The ZSM framework reference architecture shall support authorization enforcement through validate the permissions grant to a MnS consumer.

NOTE 8: authorization enforcement may be performed by MnS producer or integration fabric.

[AC-08] The ZSM framework reference architecture shall support capability to collect security logs in data service for recording every registration, login and access request and result.

[AC-09] The ZSM framework reference architecture shall support capability to generate security/audit report for specific domain, cross-domain, specific service, specific tenant, specific consumer, etc., based on security logs collected from domain/cross domain log service.

4.1.3 Security assurance requirement

This clause defines requirements to support security assurance process automation to align with ZSM Management Service (MnS) producer deployment and operation automation. Refer to GSMA NESAS [i.4] and ETSI TR 133 916 [i.5] for security assurance process.

NOTE 1: The target of protection in this requirement is Management Function (MnF)/MnS producer. The security capability to ensure the security of MnF/MnS producer will be exposed as security related management services.

[SA-01] The ZSM framework reference architecture shall support capability to validate the authenticity and the integrity of a software package of a management service producer.

[SA-02] The ZSM framework reference architecture shall support capability to validate a digital signature of a software package of a management service producer to ensure the software is provided by a trusted supplier without tampering.

NOTE 2: Capability to support Digital Supply Chains Integrity, Transparency, and Trust, e.g. support transparent service defined in SCITT [i.6] for software artefacts registration and validation, is not considered in the present document.

[SA-03] The ZSM framework reference architecture shall support capability to generate a security baseline for a management service producer.

NOTE 3: Definition of security baseline and recommendation on how to generate it refer to ETSI GR ZSM 010 [i.3].

NOTE 4: Security control in a security baseline for a management service producer could be for example the management service producer could be hardened with disabling unused ports and services.

[SA-04] The ZSM framework reference architecture shall support capability to provision security policies for a management service producer.

[SA-05] The ZSM framework reference architecture shall support capability of security tests in order to test management service producer.

NOTE 5: Security test could be for example vulnerability test according to Common Vulnerability and Exposures (CVE) (to check if there's known vulnerability in the software of the management service producer), etc.

[SA-06] The ZSM framework reference architecture shall support capability of security compliance validation in order to validate management service producer.

NOTE 6: Security compliance validation is based on security baseline of the management service producer to check if the security configuration for the management service producer is aligned with security policies.

[SA-07] The ZSM framework reference architecture shall support capability to monitor behaviour of the management service producer to detect any anomalies of the management service producer.

[SA-08] The ZSM framework reference architecture shall support capability to report the anomaly of management service producer including the incompliance of a management service producer against the security baseline of the management service producer.

[SA-09] The ZSM framework reference architecture shall support capability to trigger remediation on the compromised management service producer.

NOTE 7: Remediation on the compromised management service producer could be for example, reconfigure security policies for the management service producer, apply security patch on the software of the management service producer, upgrade the software of the management service producer, quarantine the compromised management service producer, etc.

NOTE 8: Requirements SA-01 to SA-04 are mainly required in software deployment and update phase, requirements SA-07 to SA-09 are mainly required in runtime phase, requirement SA-04 and SA-05 may be required in both phases.

4.2 Solution specific security requirements

4.2.1 Closed-loop automation security requirements

This clause defines closed-loop automation related security requirements.

[Sec-Cla-01] The ZSM framework reference architecture shall support capabilities to automatically detect and identify security incidents of closed loop supported by ZSM framework.

[Sec-Cla-02] The ZSM framework reference architecture shall support capabilities to notify security incidents of closed loop supported by ZSM framework to authorized consumers of these closed-loops.

[Sec-Cla-03] The ZSM framework reference architecture shall support capabilities to automatically react to security incidents of closed loop supported by ZSM framework.

NOTE 1: A reaction could be for example to execute a mitigation plan.

[Sec-Cla-04] The ZSM framework reference architecture shall support capabilities to automatically react to security incidents between related closed loops supported by ZSM framework.

NOTE 2: For example, an incident could be an attack against the closed loop supported by ZSM framework and/or performance degradation(s) of the closed loop supported by ZSM framework. and/or between the related closed loops supported by ZSM framework.

[Sec-Cla-05] The ZSM framework reference architecture shall support capabilities to ensure privacy of the data when the closed loops deal with personal data.

[Sec-Cla-06] The ZSM framework reference architecture shall support capabilities to ensure the data security when the closed loops deal with security relevant data.