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

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.

NOTE 3: Security relevant data is for example credentials for access control, keys for building secure communication channels, certificates of interaction parties, etc.

[Sec-Cla-07] The ZSM framework reference architecture shall support capabilities to ensure the data security the closed loops deal with management data.

NOTE 4: Management data is for example configuration and performance data related to the closed-loops.

NOTE 5: Data security includes data integrity, confidentiality and availability of the data.

[Sec-Cla-08] The ZSM framework reference architecture shall support capabilities to identify vulnerabilities of closed loop's components.

[Sec-Cla-09] The ZSM framework reference architecture shall support capabilities to provide recommendations for mitigation of security risks caused by vulnerabilities of closed loop's components.

[Sec-Cla-10] The ZSM framework reference architecture shall support capabilities to ensure integrity and confidentiality of a closed loop notification.

[Sec-Cla-11] The ZSM framework reference architecture shall support capabilities to automatically detect and identify deceit or spoofing attacks regarding an intent in a declarative form which is used as input for closed loops supported by ZSM framework.

4.2.2 AI/ML model robustness and security requirement

This clause defines requirements to support robustness and security of AI/ML model in ZSM framework during its lifecycle.

[SAI-01] The ZSM framework reference architecture shall support capability to analyse and predict security threats and risks on a deployed AI model.

[SAI-02] The ZSM framework reference architecture shall support capability to evaluate security and robustness of a deployed AI model against adversary attacks.

NOTE 1: The AI model can be deployed, for example, in a controlled testing environments (e.g. sandboxes) for evaluation.

[SAI-03] The ZSM framework reference architecture shall support capability to recommend or trigger security risk mitigation measures for a deployed AI model.

NOTE 2: The result of security and robustness evaluation result defined in SAI-02 can be used as one of input for security risk analyse defined in SAI-01. The security risk analysis result defined in SAI-01 is used as a justification to recommend or trigger security risk mitigation measures defined in SAI-03.

5 Specification of management services relevant to security

5.1 Trust management service

5.1.1 Overview

One major challenge for ZSM framework consists in monitoring the trust of different management services and their managed resources. The reason is the complex nature of the infrastructure (and related applications) supporting the execution of these resources and services; indeed, it features heterogeneity (the infrastructure spans multiple network and technology domains) and multi-party (the infrastructure spans multiple administrative domains).

Also, complex multi-operator environment can result in competition between providers who offer different (albeit similar) levels of guarantees and trust. Support trust management in each management domain and in a E2E vision will allow transparency and automation in provision and operations over ZSM framework.

Trust models depend on the motivation by a management domain to place or not trust on other based on their capabilities demonstrating Trustworthiness. The Trustworthiness capabilities can be obtained by measuring the capacity of their systems to preserve the security of the information during its whole lifecycle and anomaly detection and closed-loop mitigation against any attacks.

The objective for a trust management service is:

- Collect different metrics from management domain services related to trust, such as security metrics, audit logs, trustworthiness, risk values, etc.
- Evaluate trust for a management domain based on the trustworthiness measures of their services and including their infrastructure resources managed. This evaluation process is dynamic over the time.
- Provide a level of trust for specific services within a given management domain, or across management domains.

5.1.2 Provided management services

5.1.2.1 Trustworthiness evidence collection service

This service allows collecting data relevant in security and availability area that impacts to the trustworthiness and reputation of the systems or services managed in the domain. Data can be collected directly from the domain security specific resources, including physical security functions (e.g. anti-DDoS appliance, intrusion detection systems, firewalls, security probes) and/or or virtualized security functions (e.g. anti-virus, WAF, access control solutions). Additionally, relevant events from the domain management services related to the service enablers' health, privacy, isolation, geolocation, etc., will be incorporated from the domain log collection service. This service will collect, extract relevant to trust data, aggregate and transform the data collected to help in the trust evaluation service. Additionally, this service can collect Trustworthiness evidence from different capabilities from the Trustworthiness metric generation service.

Table 5.1.2.1-1: Service definition

Service name		Trustworthiness evidence collection service.
External visibility		Optional.
Service capabilities		
	Configure trustworthiness metrics (M)	Configure new source of trustworthiness metrics. It can be a new type of metric or a new entity with and associated metric.
	Provide trustworthiness metrics (M)	Provide query capacity by subscription, streaming telemetry, batch process, on demand, the different metrics or trust related attributes.
	Provide trustworthiness metrics list (O)	Provide notifications with the type of metrics supported and stored.

5.1.2.2 Trustworthiness attestation service

Ensuring an overall level of trustworthiness requires a dynamic and intelligent system able to adapt to the diversity of its subsystems and their trust relationships. This service allows enforcing extensible trustworthiness specific metrics valid for any system and network. Initial metrics considered are the ones related to remote attestation procedures.

Table 5.1.2.2-1: Service definition

Service name		Trustworthiness attestation service.
External visibility		Optional.
Service capabilities		
	Request remote attestation service (O)	Trigger on demand the execution of a remote attestation against the list of IT resources or network connectivity associated to a specific management service in a domain.
	Provide remote attestation report (O)	Report with the results of the last remote attestation.

NOTE: Additional capabilities beyond attestation can be included in future, e.g. data privacy.

5.1.2.3 Trustworthiness evaluation service

Different metrics provided by the trustworthiness evidence collection service are combined to calculate the level of trustworthiness or reputation. For example, some metrics will be related to availability (i.e. the provider's monitoring system works, or the provider has no lack of resources to deploy specific service), the isolation (i.e. data in transit do not leave a geographic area or cross over specific device), or the security (i.e. time to mitigate a DoS). Different evaluation models can be supported to generate specific Level of Trust metric.

Table 5.1.2.3-1: Service definition

Service name		Trustworthiness evaluation service.
External visibility		Optional.
Service capabilities		
	Request Trustworthiness evaluation method (O)	Trigger trust evaluation process method to be used.
	Provide level of trust for specific managed service in a Domain(O)	Trust report with metrics used, evaluation method used and results for a specific management service.
	Provide level of trust for a specific Domain(O)	Trust report with metrics used, evaluation method used and results from a specific domain.

5.1.2.4 Trustworthiness adaptation service

Reflective and Adaptive trust model is proposed as a possible way to build mutual trust between entities inside a management domain or inter different domains of ZSM framework, before the entities interact with each other, to protect management services/functions of the management domains.

The service provides capabilities to dynamically build/rebuild trust model and trust relationship towards a management domain/function/service based on trustworthiness evaluation result of the management service consumer and producer.

NOTE 1: Reflective and Adaptive trust model is a model which is dynamically built based on trustworthiness of the interacting entities, e.g. the trust relationship and trust model between two entities are built based on threat and risk analysis of the entities and security countermeasures applied on the entities. The trust model can be rebuilt according to re-evaluated trustworthiness of the entities.

NOTE 2: The trust model between two entities (e.g. MnS consumer and producer) is initially built based on trustworthiness evaluation of the entities, and rebuilt based on the change and re-evaluated trustworthiness of the entities.

Table 5.1.2.4-1: Service definition

Service name		Trustworthiness adaptation service.
External visibility		Optional.
Service capabilities		
	Request trust model (O)	Trigger to (re)build trust model between two ZSM entities within or across management domains based on evaluated trustworthiness of the ZSM entities (see note 1).
	Provide trust model (O)	Respond the trust model between the two ZSM entities.
	Request trust relationship (O)	Trigger to (re)establish trust relationship between two ZSM entities within or across management domains based on trust model of the ZSM entities (see note 2).
	Provide trust relationship (O)	Respond the trust relationship between the two ZSM entities.
NOTE 1: The trust model could be for example, validated trust, direct historical trust, mediated trust, mandated trust, and hybrid trust, or direct delegated trust, collaborative trust, transitive trust and reputational trust, etc., see [i.1]. NOTE 2: The trust relationship reflects authorizations of two ZSM entities based on their trust model, which is governed by criteria or security policies to protect management services/functions of the management domains. For example, remote attestation is required for a zero trust management service/domain, while certificate validation is sufficient for a MnS with reputational trust. Another example, monitoring behaviour of management service consumer with different security rules based on various trust levels of the consumers.		

5.1.3 Cross-domain Trustworthiness services

Cross-domain trustworthiness services can be used by internal ZSM consumer and external consumer of ZSM framework.

Any ZSM deployment shall contain management functions that provide in a cross-domain fashion management services as defined in table 5.1.3-1, indicating for each service whether its support by the cross-domain integration fabric is OPTIONAL or MANDATORY.

Table 5.1.3-1: Support of services offered by the cross-domain

Service name	Clause	Support
Management services trustworthiness evidence collection services	5.1.2.1	OPTIONAL
Management services Trustworthiness evaluation service	5.1.2.2	OPTIONAL
Management services Trustworthiness adaptation service	5.1.2.3	OPTIONAL
Management services Trustworthiness attestation service	5.1.2.4	OPTIONAL

5.1.4 Domain Trustworthiness services

A management domain including the E2E service management domain may contain management functions that provide management services as defined in table 5.1.4-1, indicating for each service whether its visibility outside the domain is OPTIONAL or MANDATORY. Services not externally visible need not be supported.

Table 5.1.4-1: Support and external visibility of services offered by the domain

Service name	Clause	External visibility
Management services trustworthiness evidence collection services	5.1.2.1	OPTIONAL
Management services Trustworthiness evaluation service	5.1.2.2	OPTIONAL
Management services Trustworthiness adaptation service	5.1.2.3	OPTIONAL
Management services Trustworthiness attestation service	5.1.2.4	OPTIONAL

5.2 Access Control

5.2.1 Overview

Access control in ZSM framework is capabilities 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.

Access control services include:

- authentication services support dynamic identity management, identity group management, authentication policy management and authentication decision and enforcement;
- authorization services support dynamic access control policy management, permission generating and granting, and authorization decision;
- audit services support security log collection and audit report generation.

The access control services can be cross-domain or domain services. Cross-domain access control services, e.g. cross-domain authentication, authorization and audit services, could be optionally provided by cross-domain integration fabric. Domain access control services, e.g. domain authentication and authorization services, could be optionally provided by domain integration fabric or other management service producers.

5.2.2 Provided management services

5.2.2.1 Management services authentication administration service

Table 5.2.2.1-1: Service definition

Service name		Management services authentication administration service.
Service capabilities		
	Manage identity (M)	Manage (create, read, update and delete) identity of management service consumer or producer, and manage notification subscription for management service consumer.
	Provide identity change notification (O)	Notify subscribed consumer when security state and/or security context of the identity is changed.
	Manage identity group (M)	Manage (create, read, update and delete) group of management service consumer according to specific properties of the consumers, e.g. consumer of same tenant, in same management domain, same type of management functions, etc., and manage notification subscription for management service consumer.
	Provide group change notification (O)	Notify subscribed consumer when state of the group is changed.
	Manage authentication policy (M)	Manage (create, read, update and delete) authentication policies, enable generating consolidated authentication policies based on management service consumer and producer(s) of multiple management domains, and manage notification subscription for management service consumer.
	Provide authentication policy change notification (O)	Notify subscribed consumer, e.g. authentication enforcement point, when authentication policies of a related group are changed.
NOTE: The identify is used to identify MnS consumer or producer before authentication. MnS consumer and producer can be played by MnF of ZSM framework. MnS consumer can also be external consumer of ZSM framework, e.g. it can be digital store fronts, web portals, BSS components, etc.		

5.2.2.2 Management services authentication enforcement service

Table 5.2.2.2-1: Service definition

Service name		Management services authentication enforcement service.
Service capabilities		
	Enforce authentication (M)	Authenticate a management service consumer or producer through verifying its identity and credential based on authentication policy, and establish authentication session if needed, optionally generate and provide authentication assertion in the authentication response.

5.2.2.3 Management services authorization administration service

Table 5.2.2.3-1: service definition

Service name		Management services authorization administration service.
Service capabilities		
	Manage role (O)	Manage (create, read, update and delete) role of management service consumers or group of management service consumers according to type of the consumers, and manage notification subscription for management service consumer.
	Provide role change notification (O)	Notify subscribed consumer when state of the role is changed.
	Manage authorization policy (M)	Manage (create, read, update and delete) authorization policies for a group or role on management services, enable generating contextual policies based on clearance of the group/role and classification of management services, and manage notification subscription for management service consumer.
	Provide authorization policy change notification (M)	Notify subscribed consumer, e.g. authorization administration or enforcement point, when authorization policies of a related group/role are changed (see note 2).
NOTE 1: Authorization administration service can be reused for exposure configuration service (see clause 6.3.2.5 of ETSI GS ZSM 002 [1]) for access control of an external ZSM consumer in specific deployment. NOTE 2: The MnS consumer can be external consumer of ZSM framework, internal consumer of same or different management domain(s), also the MnS consumer may be acting on behalf of system administrator, or daily maintainer, or developer. Role is used to represent the aforementioned different type of consumers, then different privileges can be assigned to different roles. E.g. the role represents external consumer has privilege to access MnSs exposed by E2E service management domain, the role represents system administrator of ZSM framework has full privileges for ZSM services, the role represents developer has privilege to only access log collection services, etc.		

5.2.2.4 Management services authorization decision service

Table 5.2.2.4-1: service definition

Service name		Management services authorization decision service.
Service capabilities		
	Grant permissions (M)	Grant permissions to an authenticated management service consumer based on access control policies of group/role of the management service consumer or entitlements configured for the management service consumer, and security context of the management service consumer.
	Provide authorization decision (O)	Support authorization enforcement point to verify permissions in service access request or locally (see note).
NOTE: A management service producer (acting as authorization enforcement point) returns management service to a management service consumer after checking permissions of the consumer with an integration fabric or AAA server (acting as authorization decision point). The permissions may be included in access request or stored locally in the authorization decision point.		

5.2.2.5 Management services security log collection service

Configure managed entity and management function to provide security logs which record every operation related to authentication and authorization administration and decision, every identity registration, login, access request and result. The logs should include who access what service in which time and which location and the access result.

Log collection services defined in clause 6.5.2.2.4 of ETSI GS ZSM 002 [1] are reused to collect security log.

5.2.2.6 Management services audit service

Table 5.2.2.6-1: service definition

Service name		Management services audit service.
Service capabilities		
	Security audit (M)	Analyse and generate security audit report for cross-domain, specific domain, service, tenant, consumer, etc., based on security logs collected from domain/cross domain log service.
	Manage audit (O)	Configure audit report rule for specific domain, tenant, consumer, period, location, etc., as well as information including in the report, format of report, etc.

5.2.3 Cross-domain access control services

Cross-domain access control services can be used for access control of internal ZSM consumer and external consumer of ZSM framework. The services enable authentication and authorization of external ZSM consumer to access ZSM services, as well as authentication and authorization of internal ZSM consumer to access management services in different management domains.

Cross-domain authentication and audit services are utilized for centralized authentication and audit of intra-domain access control.

Cross-domain access control services, e.g. authentication and authorization administration service, cross-domain authentication enforcement service, cross-domain authorization decision service and audit service, can be provided by cross-domain integration fabric or dedicated service producer, such as Authentication, Authorization, Audit (AAA) server.

Authorization enforcement (validate the permissions including in the service request or check with authorization decision point, and return allowed services) is proceeded on either cross-domain integration fabric or management service producer in a management domain, including the E2E service management domain.

Any ZSM deployment shall contain management functions that provide in a cross-domain fashion management services as defined in table 5.2.3-1, indicating for each service whether its support by the cross-domain integration fabric is OPTIONAL or MANDATORY.

Table 5.2.3-1: Support of services offered by the cross-domain access control service

Service name	Clause	Support
Management services authentication administration service	5.2.2.1	MANDATORY
Management services authentication enforcement service	5.2.2.2	MANDATORY
Management services authorization administration service	5.2.2.3	MANDATORY
Management services authorization decision service	5.2.2.4	MANDATORY
Management services security log collection service	5.2.2.5	MANDATORY
Management services security audit service	5.2.2.6	MANDATORY

5.2.4 Domain access control

Domain access control services enable authentication and authorization of internal ZSM consumer to access management services in different or same management domains.

Domain access control services, e.g. authentication and authorization administration service, authentication enforcement service, authorization decision service and audit service, can be provided by domain integration fabric or management function.

Authorization enforcement (validate the permissions including in the service request or check with authorization decision point, and return allowed services) is proceeded on either domain integration fabric or management service producer.

A management domain including the E2E service management domain may contain management functions that provide management services as defined in table 5.2.4-1, indicating for each service whether its visibility outside the domain is OPTIONAL or MANDATORY. Services not externally visible need not be supported.

Table 5.2.4-1: Support and external visibility of services offered by the domain access control service

Service name	Clause	External visibility
Management services authentication administration service	5.2.2.1	OPTIONAL
Management services authentication enforcement service	5.2.2.2	OPTIONAL
Management services authorization administration service	5.2.2.3	MANDATORY
Management services authorization decision service	5.2.2.4	OPTIONAL
Management services security log collection service	5.2.2.5	MANDATORY
Management services security audit service	5.2.2.6	OPTIONAL

5.3 Ensure robustness of AI/ML model

5.3.1 Overview

Artificial Intelligence/Machine Learning is used in ZSM framework to provide E2E service/domain specific insights & predictions and support variable degrees of automated decision-making.

Generally, security regarding AI/ML model in ZSM would include security of data supply chain, model supply chain, model deployed in shared framework, interaction between multiple domains, trust between AI/ML service producer and consumer.

AI/ML model could be subjected to adversarial attacks such as data and model poisoning in training phase, model evasion and stealing, data extraction in inference phase. Robustness of an AI/ML model against attack could be influenced by following factors:

- Vulnerabilities of AI/ML model which could be exploited by attacker for adversarial attacks.
- Threat surface in training and deployment environment which may change probability of successful attack.
- Implemented security control.
- Ability to maintain operations during adversarial attacks.
- Ability to return to normal operations over an acceptable period of time, post-disruption, after adversarial attacks.

To ensure the robustness of the AI/ML model deployed in ZSM framework, security threat and risk analysis services should be provided to evaluate potential risks on AI/ML model, recommend the actions on the risk (e.g. report the risk, accept the risk, mitigate the risk, etc.), and trigger processes to mitigate the risk if needed.

NOTE: The new management services provided below are applicable to deployed AI model.

5.3.2 Provided management services

5.3.2.1 AI model security threat and risk analysis services

The deployed AI models can be compromised with adversarial attack or mis-operation/configuration, which may result in unavailability or disruption of the AI service. The deployed AI model security threat and risk analysis service allows evaluating and predicting the risks of loss of availability of the AI model, determining the most appropriate action to mitigate the risks.

To evaluate potential risks on the deployed AI model, the AI model security threat and risk analysis service producer needs to collect information related to known vulnerabilities of the deployed AI model, deployment environment of the AI model, successful attacks on the same type of the AI model in the similar execution environment, former analysis results, trustworthiness of the deployed AI model (e.g. Quality of Trust (QoT) configured on the AI model such as poisoning/evasion defending, refer to clause 4.6.3 of ETSI GS ZSM 012 [2]), access pattern on the AI model (e.g. frequency) and input/output samples which may reflect behaviours of the AI model and its consumers, test result of the deployed AI model, whether the model is retrained or not, security controls applied on the AI model and execution environment, etc.

Based on the collected data, the AI model security threat and risk analysis service producer predicts the probability that the identified threat would result in damaging the AI model. The AI model security threat and risk analysis service producer needs also collecting the usage pattern of the AI model, and evaluating potential business impact if the AI model is compromised in different scenarios, e.g. SLA breakdown, loss of service, leak of privacy, sensitive data or intelligent property, etc.

To recommend the action, the AI model security threat and risk analysis service producer needs to consider security objectives and baseline, as well as accepted/tolerable security risk of operator/customer, which could be input through management and orchestration system as security policies or intents. After comparing the potential risk and tolerable risk, the AI model security threat and risk analysis service producer determines either accepting or mitigating the risk. For risk mitigation, it recommends the most appropriate actions to perform on the deployed AI model such as reconfigure, retrain, upgrade, replace, pause, terminate, the AI model, or sanitize, qualify, transform, pre-process the training data and AI model input, or obfuscate the AI model output.

Table 5.3.2.1-1: Service definition

Service name		AI model security threat and risk analysis service.
External visibility		Optional.
Service capabilities		
	Request security threat and risk analysis result (O)	Trigger AI model security threat and risk analysis process to generate an analysis report.
	Provide security threat and risk result (O)	Provide a AI model security threat and risk analysis report.

5.3.2.2 AI model adversarial robustness evaluation services

The AI model security threat and risk analysis service evaluates the potential risk in production environment based on historic data. As a concrete case of AI Model Trust Evaluation services (refer to clause 4.6.3 of ETSI GS ZSM 012 [2]), the AI model adversarial robustness evaluation service provides capability to evaluate robustness of an AI model against adversarial attacks with adversary test.

Based on the adversary test type, e.g. data poisoning, model evasion and stealing, data extraction, the AI model adversarial robustness evaluation service deploys the target AI model in a controlled testing environments (e.g. sandboxes), simulate the adversarial attacks, and validate the robustness of the model against the attacks.

The result of evaluation will be used for security threat and risk analysis and may trigger action on the AI model, e.g. harden the model using adversarial training.

Table 5.3.2.2-1: Service definition

Service name		AI model adversarial robustness evaluation service.
External visibility		Optional.
Service capabilities		
	Request adversarial robustness evaluation result (O)	Trigger AI model adversarial robustness evaluation process to generate an evaluation report.
	Provide adversarial robustness evaluation result (O)	Provide a AI model adversarial robustness evaluation report.

5.3.2.3 AI model security risk mitigation services

The AI model security risk mitigation services allow the authorized ZSM service consumer to reconfigure the AI model to mitigate the potential security risk of AI model according to result of AI model security threat and risk analysis. E.g. the authorized entity could reconfigure robustness requirements (such as poisoning block/defence, evasion defence, extraction defence) for the AI model through AI/ML data or model trust management services defined in clause 4.6.3 of ETSI GS ZSM 012 [2]. Accordingly, following mitigation measures could be triggered, e.g.:

- model retraining for restoring or treat inference data sample separately to mitigate risks caused by backdoor attack;
- model hardening to mitigate risks caused by evasion attack;
- train the model with privacy guarantees to mitigate data risks caused by extraction attack;

- secure model (hyper-)parameters or deploy secure HW or apply encryption schemes mitigate risks caused by model stealing attack.

In addition, traditional security controls such as firewall, authentication and authorization service, host or network based Intrusion Detection System (IDS), Data Lost Prevention (DLP), Data Packet Inspection, data sanitization tool, etc., may be deployed or reconfigured to perform stronger access control, stricter traffic filter and smarter anomaly detection, and so on.

Table 5.3.2.3-1: Service definition

Service name		AI model security risk mitigation service.
External visibility		Optional.
Service capabilities		
	Request AI model security risk mitigation (O)	Trigger AI model security risk mitigation process.

5.4 Security assurance of management service producer in ZSM

5.4.1 Overview

ZSM framework allows to automatically deploy new capabilities/management services produced by Management Service (MnS) producer(s). The vulnerabilities of the MnS producer(s) deployed in ZSM framework could be exploited by the adversary to compromise the MnS producer itself, then attack other MnS producers s, finally endanger the whole ZSM framework and/or ZSM consumers. Security assurance of MnS producer should be considered to avoid security threats introduced by the MnS producer. Security process/procedures should be automated to align with automation objective of ZSM framework.

Security process of a MnS producer includes securely onboarding (e.g. to catalogue), test, deploying, provisioning, and monitoring the MnS producer.

5.4.2 Provided management services

5.4.2.1 Security assurance service in delivery phase of MnS producer

Table 5.4.2.1-1: Service definition

Service name		MnS producer delivering security services.
Service capabilities		
	Check authenticity (M)	Validate the authenticity and the integrity of a software package signed by the MnS provider for the MnS producer.
	Generate security baseline (O)	Generate a security baseline for a management service producer. Refer to ETSI GR ZSM 010 [i.3].
	Validate security (O)	Generate security test result of a MnS producer for compliance test based on security baseline of the MnS producer (see note 1) or vulnerability test according to Common Vulnerability and Exposures (CVE) (see note 2).
	Configure security policies (O)	Provision security policies for a MnS producer based on security baseline of the MnS producer.
NOTE 1: Compliance test is checking, e.g. if the security configuration is aligned with security policies defined in security baseline of MnS producer, e.g. the MnS producer is hardened, required security functions are in place with proper rules configured, etc. NOTE 2: Vulnerability test is checking if there are known vulnerabilities (e.g. reported by Common Vulnerability Scoring System (CVSS)) in the software of MnS producer.		

5.4.2.2 Security assurance service in operational phase of MnS producer

Table 5.4.2.2-1: Service definition

Service name		MnS producer operation security services.
Service capabilities		
	Configure security monitoring (M)	Configure and trigger to collect logs, security events, etc., to support security monitoring and anomaly detection on a MnS producer.
	Report security status (M)	Generate security report when detect anomaly or incompliance of a MnS producer.
	Remediate security issue (O)	Trigger remediation on the compromised MnS producer according to security report and security baseline of the MnS producer.

5.4.3 Cross-domain security assurance services

Cross-domain security assurance services can be used by internal ZSM consumer and external consumer of ZSM framework.

Any ZSM deployment shall contain management service producers that provide in a cross-domain fashion management services as defined in table 5.4.3-1, indicating for each service whether its support by the cross-domain integration fabric is OPTIONAL or MANDATORY.

Table 5.4.3-1: Support of services offered by the cross-domain security assurance service

Service name	Clause	Support
Management services MnS producer delivering security services	5.4.2.1	OPTIONAL
Management services MnS producer operation security services	5.4.2.2	OPTIONAL

5.4.4 Domain security assurance

A management domain including the E2E service management domain may contain management functions that provide management services as defined in table 5.4.4-1, indicating for each service whether its visibility outside the domain is OPTIONAL or MANDATORY. Services not externally visible need not be supported.

Table 5.4.4-1: Support and external visibility of services offered by the domain security assurance service

Service name	Clause	External visibility
Management services MnS producer delivering security services	5.4.2.1	OPTIONAL
Management services MnS producer operation security services	5.4.2.2	OPTIONAL

6 ZSM reference architecture with security aspects

ZSM security architecture is built over ZSM framework reference architecture defined in ZSM002 (see ETSI GS ZSM 002 [1]) with additional security management services, as shown in Figure 6-1.

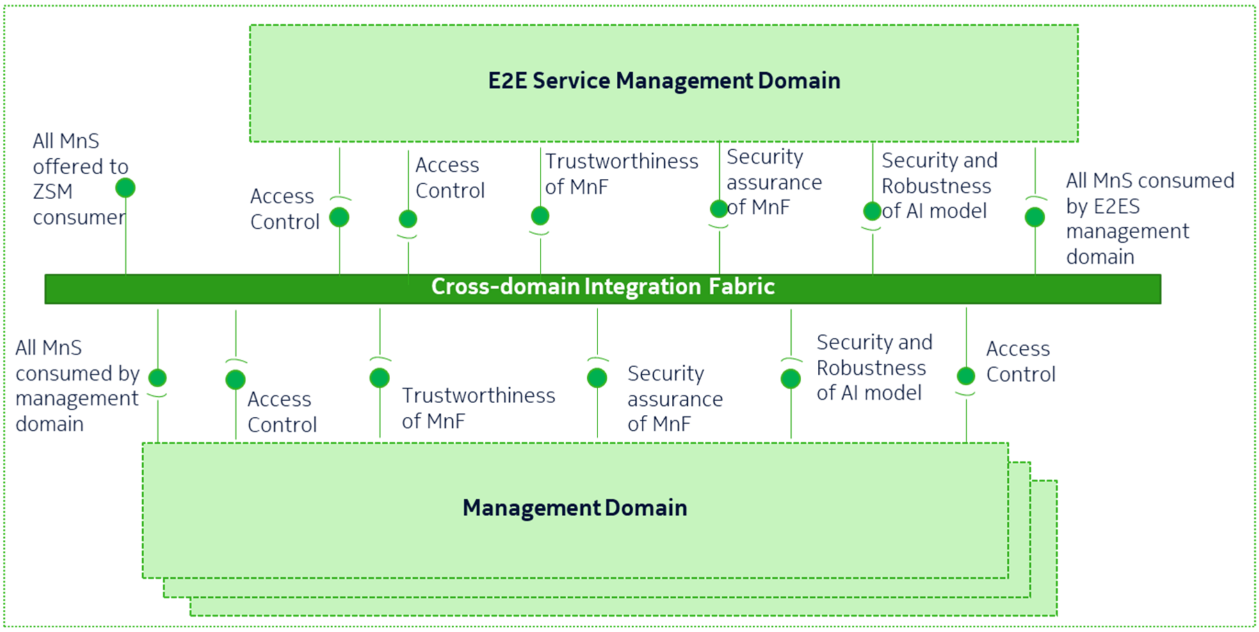
E2E Service Management Domain
All MnS offered to ZSM consumer
Access Control
Access Control
Trustworthiness of MnF
Security assurance of MnF
Security and Robustness of AI model
All MnS consumed by E2ES management domain
Cross-domain Integration Fabric
All MnS consumed by management domain
Access Control
Trustworthiness of MnF
Security assurance of MnF
Security and Robustness of AI model
Access Control
Management Domain

Figure 6-1: ZSM security reference architecture

ZSM framework reference architecture defined in ETSI GS ZSM 002 [1] includes below Management Services (MnS) depicted in Figure 6-1:

- All MnS offered to ZSM consumer.
- All MnS consumed by management domain.
- All MnS consumed by E2ES management domain.

The additional security management services defined in current specification include:

- Trustworthiness related services produced by Management Domain or E2E Service Management Domain, which include trustworthiness evidence collection service, trustworthiness attestation service, trustworthiness evaluation service and trustworthiness adaptation service.
- MnF security assurance related services produced by Management Domain, or E2E Service Management Domain, which include security assurance service in delivery, testing and operational phases of a MnF.
- Access Control related services produced by Cross-domain Integration Fabric, or Management Domain, or E2E Service Management Domain, which include management services authentication administration and enforcement services, management services authorization administration and enforcement services, management services security log collection service and management services audit service.
- AI model robustness and security related services produced by Management Domain, or E2E Service Management Domain, which include AI model security threat and risk analysis service, AI model adversarial robustness evaluation services and AI model security risk mitigation services.

The existing management services of ZSM framework can be leveraged to produce security related management services, and the security related management services can be invoked by other ZSM service producers to implement intelligent security services to protect managed services deployed and managed in/via ZSM framework.

NOTE: For example, existing data collection services defined in ETSI GS ZSM 002 [1], AI model trust management services defined in ETSI GS ZSM 012 [2], etc., can be leveraged to produce AI model robustness and security related services defined in the present document. On the other hand, security related management services defined in the present document (such as Trustworthiness evaluation and adaptation services, Access Control services, etc.) can be invoked by Orchestration and Control services defined in ETSI GS ZSM 002 [1] to automate security controls and procedures to protect managed service, for example, network slice.

Table 6-1: Mapping between the management service and the ETSI ZSM TSs

MnS name	Status	TS number
All MnS offered to ZSM consumer	Defined	ZSM002
All MnS consumed by management domain	Defined	ZSM002
All MnS consumed by E2ES management domain	Defined	ZSM002
Trustworthiness related MnS	Defined	ZSM014
Access Control related MnS	Defined	ZSM014
Security and robustness of AI model related MnS	Defined	ZSM014
Security assurance related MnS	Defined	ZSM014

Annex A (informative): Change history

Date	Version	Information about changes
November 2021	V0.0.1	Initial Draft: agreement on the skeleton and initial content
January 2022	V0.0.2	Included contributions: ZSM(21)000402rev1 ZSM014_requirements to support adaptive trust for ZSM management domains ZSM(21)000403rev1 ZSM014 security requirement of closed-loop solution
November 2022	V0.0.3	Included contributions: ZSM(22)000038_ZSM014_requirements_for_access_control_on_ZSM_services ZSM(22)000029r2_ZSM014_management_service_to_support_access_control_on_ZSM ZSM(22)000213_ZSM014_management_service_to_support_robustness__of_AIML_model ZSM(22)000343r3_ZSM014_Add_Trust_management_service
August 2023	V0.0.4	Included contributions: ZSM(23)000023r3_ZSM014_management_service_trustworthiness_adaptation
November 2023	V0.0.5	Included contributions: ZSM(23)000024r3_ZSM014_ZSM security reference architecture ZSM(23)000217_ZSM014 scope of the GS
November 2023	V0.0.6	Included contributions: ZSM(23)000020r7_ZSM014_requirement_to_support_MnF_security_assurance ZSM(23)000021r6_ZSM014_management_service_to_support_MnF_security_assurance ZSM(23)000022r3_ZSM014_requirement_to_support_AI Robustness and Security
December 2023	V0.0.7	Editoral fixing
January 2014	V0.0.8	Included contributions: ZSM(24)000015_ZSM014_new_draft
March 2014	V0.0.9	Included contributions: ZSM(24)000039r2_ZSM014_-_Comments_to_the_remote_consensus_of_the_final_draft ZSM(24)000045_ZSM_014__Modification_proposal_for_Note_1_in_section_4_2_2__

History

Document history		
V1.1.1	March 2024	Publication