ETSI GR ZSM 010 V1.1.1 (2021-07)

Zero-touch network and Service Management (ZSM); General 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
DGR/ZSM-010_SecStudy

Keywords
countermeasures, security, threat analysis

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

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Security consideration is critical to commercially deploy ZSM framework based solutions. The present document covers security threat and risk analytics on ZSM framework based on assets of ZSM framework and attack mechanism defined in Common Attack Pattern Enumeration and Classification (CAPEC) project of MITRE (see [i.4]).

Several key security issues are identified according to risk analysis result, and solutions were proposed to mitigate the risks, which include:

- Trust issue of cross domain service management and build relationship between multiple management domains.
- Potential security risk caused by vulnerability of management function and security assurance of ZSM management function.
- Security isolation and security requirement fulfilment in multi-tenancy environment of ZSM Framework.

- Access control for management service provided by multiple domain service producers of ZSM framework.
- Leverage existing security specifications to identify security risk of AI/ML model and protect AI/ML models in ZSM framework.

1 Scope

The present document studies the security aspects of the ZSM use cases, framework and solutions, identifies potential security threats and mitigation considerations to be covered in ZSM standardization activities. It aims to outline a list of security controls (aka security countermeasures) in order to raise awareness of security aspects that could be considered in ZSM specifications. The present document will explore the relationship between security controls and technology-specific solutions.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

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

NOTE: While any hyperlinks included in 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] ISO/IEC 27005:2011: "Information technology - Security techniques - Information security risk management".

[i.2] NIST Special Publication 800-30 (Revision 1): "Guide for Conducting Risk Assessments".

[i.3] Recommendation ITU-T X.805 (10/2003): "Security architecture for systems providing end-to-end communications".

[i.4] MITRE Common Attack Pattern Enumeration and Classification (CAPEC) project.

NOTE: Available at https://capec.mitre.org/.

[i.5] MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) project.

NOTE: Available at https://attack.mitre.org/.

[i.6] General Data Protection Regulation (EU GDPR) definitions.

NOTE: Available at https://gdpr-info.eu/art-4-gdpr/.

[i.7] GSMA Network Equipment Security Assurance Scheme (NESAS).

NOTE: Available at https://www.gsma.com/security/network-equipment-security-assurance-scheme/.

[i.8] ETSI TR 133 916 (V15.1.0): "Universal Mobile Telecommunications System (UMTS); LTE; Security Assurance Methodology (SCAS) for 3GPP network products (3GPP TR 33.916 version 15.1.0 Release 15)".

[i.9] Adversarial ML Threat Matrix.

NOTE: Available at https://github.com/mitre/advmlthreatmatrix/blob/master/pages/adversarial-ml-threat-matrix.md#structure-of-adversarial-ml-threat-matrix.

[i.10] ETSI GR SAI 004 (V1.1.1): "Securing Artificial Intelligence (SAI); Problem Statement".

[i.11] ETSI GR SAI 005 (V1.1.1): "Securing Artificial Intelligence (SAI); Mitigation Strategy Report".

[i.12] ISO/IEC TR 24028:2020: "Information technology - Artificial intelligence - Overview of trustworthiness in artificial intelligence".

[i.13] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[i.14] ISO/IEC 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

[i.15] ETSI GS ZSM 002: "Zero-touch network and Service Management (ZSM); Reference Architecture".

[i.16] ETSI GS ZSM 007: "Zero-touch network and Service Management (ZSM); Terminology for concepts in ZSM".

[i.17] NIST 800-39: "Managing Information Security Risk".

NOTE: Available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.

[i.18] ETSI GS ZSM 001: "Zero-touch network and Service Management (ZSM); Requirements based on documented scenarios".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

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

control or countermeasure: technique that puts into place to mitigate (reduce) the potential risk

information system: management functions and management services used in the present document

qualitative risk analysis: risk analysis technique that uses a scale of qualifying attributes to describe the magnitude of potential consequences (e.g. Low, Medium and High) and the likelihood that those consequences will occur

NOTE: An advantage of qualitative analysis is its ease of understanding by all relevant personnel while a disadvantage is the dependence on subjective choice of the scale.

quantitative risk analysis: risk analysis technique that uses a scale with numerical values (rather than the descriptive scales used in qualitative risk analysis) for both consequences and likelihood, using data from a variety of sources

NOTE: The quality of the analysis depends on the accuracy and completeness of the numerical values and the validity of the models used.

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

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

security baseline: set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system

NOTE: Source: [i.2].

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

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

3.2 Symbols

Void.

3.3 Abbreviations

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

AAA	Authentication, Authorization and Account/Audit
AI	Artificial Intelligence
ANAS	Authentication Administration Service
API	Application Programming Interface
APT	Advanced Persistent Threat
ARAS	Authorization Administration Service
ATT	Adversarial Tactic and Technique
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge
BSS	Business Support System
CAPEC	Common Attack Pattern Enumeration and Classification
CDANA	Cross-Domain Authentication Administration/decision
CDANAS	Cross-Domain Authentication Administration Service
CDARA	Cross-Domain Authorization Administration/decision
CDARAS	Cross-Domain Authorization Administration Service
CDIF	Cross-Domain Integration Fabric
CI/CD	Continuous Integration/Delivery
CN	Core Network
CVE	Common Vulnerabilities and Exposures
DAC	Discretionary Access Control
DANA	Domain Authentication Administration/decision
DANAS	Domain Authentication Administration Service
DARA	Domain Authorization Administration/decision
DARAS	Domain Authorization Administration Service
DIF	Domain Integration Fabric
DoS	Denial of Service
DSS	Data Security Standard
EU	European Union
FM	Fault Management
GDPR	General Data Protection Regulation
GPU	Graphic Processing Unit
GSMA	Global System for Mobile communications Association
IAM	Identity and Access Management
IP	Intellectual Property
ISO	International Organization for Standardization
ISV	Independent Software Vendor
IT	Information Technologies
KPI	Key Performance Indicator
LS	Liaison Statement
MAC	Mandatory Access Control
MFA	Multi-Factor Authentication
ML	Machine Learning
NESAS	Network Equipment Security Assurance Scheme
NFV	Network Function Virtualisation
NGFW	Next Generation Firewall
OSINT	Open Source Intelligence
OWASP	Open Web Application Security Project
PCI	Payment Card Industry

PKI	Public Key Infrastructure
PM	Performance Management
RAN	Radio Access Network
SAI	Securing Artificial Intelligence
SAP	Service Access Point
SCAS	Security Assurance Specifications
SDO	Standard Development Organization
SECAM	Security Assurance Methodology
SLA	Service Level Agreement
SLS	Service Level Specification
SSO	Single Sign On
TLS	Transport Layer Security
TM	Trace Management
TRA	Threat and Risk Analysis
TTPs	Tactics, Techniques and Procedures
UEBA	User and Entity Behavior Analytics
VM	Virtual Machine

4 Threat and risk assessment/analysis

4.1 Methodology of threat and risk analysis

4.1.1 General approach of ZSM threat and risk analysis

The present document refers NIST 800-30 [i.2], ISO/IEC 27005 [i.1] and Recommendation ITU-T X.805 [i.3] for security Threat and Risk Analysis (TRA) of ZSM framework and solutions. Qualitative or Semi-Quantitative Assets/Impact-oriented were proposed in the present document and the following aspects would be covered during TRA:

- Define scope of TRA for ZSM. The present document analyses the risk of ZSM framework, use cases, requirements and solutions in E2E service point of view and use top-down approach to assess impacted assets.
- Identify and categorize ZSM assets. The assets include management/managed service, management function, management/managed data, managed resource, etc.
- Identify threats that are relevant to the assets. Threat natural, human or machine origin, accidental or deliberate, internal or external. Threats include destruction, corruption or modification of service or function, theft, removal or loss of data, violation of regulation, etc.
- Identify vulnerabilities and threat surfaces that could be exploited by threat agent. Vulnerabilities includes out of date or mis-designed or mis-configured architecture, software, hardware, etc., as well as deficient management process, policies, etc.
- Identify the existing controls and their effect on the vulnerabilities and threats identified. In the first stage of the present document, no existing security control is considered. The present document can be iteratively updated based on new controls adopted.

NOTE: Vulnerabilities, threats and controls can be changed continuously, and identification of vulnerabilities, threats and controls could be interleaved. E.g. Security controls could reduce threat surface caused by vulnerabilities, therefore the vulnerabilities would not be exploited by threat.

- Determine the likelihood that the identified threat would incur security incident and damage the asset. It can be e.g. very likely, likely, possible, not likely, etc.
- Determine the adverse impacts on the assets from the exploitation of vulnerabilities by threat, and consequence of the provider and consumer of the assets. It can be e.g. Disastrous, Damaging, Harmful, Annoying, etc.
- Determine information security risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation.

4.1.2 ZSM threat and risk analysis framework

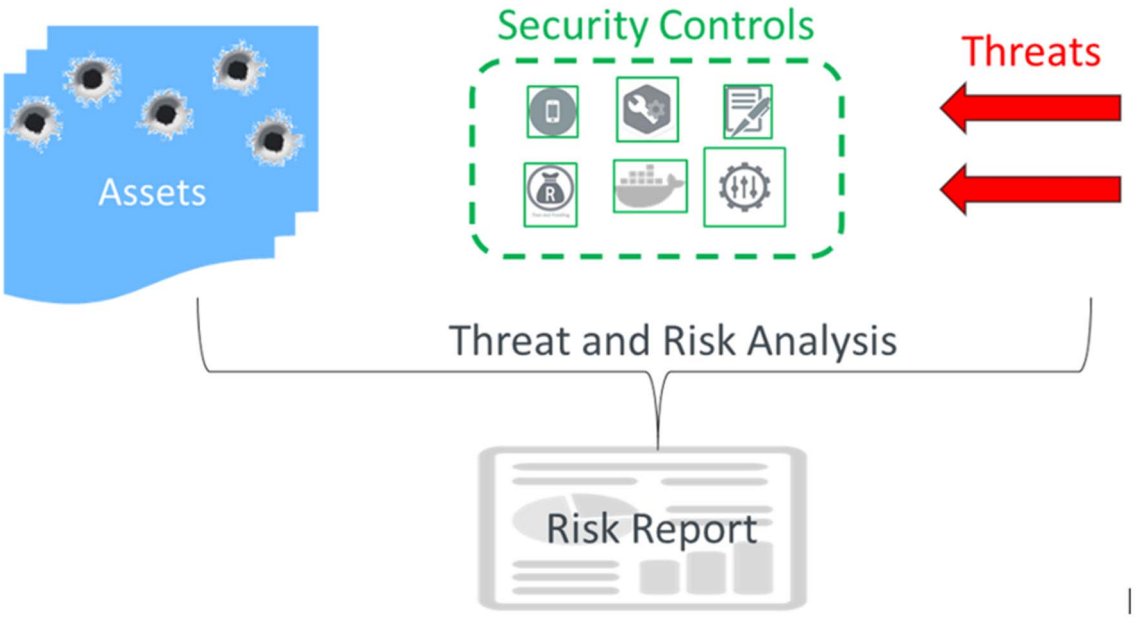

Figure 4.1.2-1: ZSM threat and risk analysis framework

4.1.3 Risk score and priority

There are various methods to calculate risk scale with either qualitative or quantitative scale, or mixture of both. For example, a quantitative risk scale is defined according to quantitative asset value and qualitative threat vulnerability levels. In some other example, a quantitative or qualitative risk scale is defined based on qualitative likelihood of an incident scenario and qualitative estimated business impact against the impact. In yet another example, a quantitative risk scale is calculated with quantitative consequences (asset value) and quantitative likelihood of threat occurrence (taking account of vulnerability aspects).

Considering difficulty to evaluate asset value independently, the present document proposes that the quantitative or qualitative risk scale is calculated based on qualitative likelihood of an incident and Business Impact caused by the incident. Refer to table E.1 b) of ISO/IEC 27005:2011(E) [i.1].

The likelihood of an incident scenario is given by a threat exploiting a vulnerability with a certain likelihood. It depends on the attractiveness of the asset and its susceptibility of the vulnerability to exploitation, as well as the ease of conversion exploiting the vulnerability of the asset into reward and the technical capabilities of the threat agent.

The business impact caused by the incident scenario can be a violation of legal and regulatory obligations, financial loss, disruption of activities, loss of services, incompliance of organizational policies, loss of reputations, unsatisfaction of contract or agreement with a customer, etc.

The table maps likelihood incident scenario against the business impact to quantitative risk score. The resulting risk is measured on a scale of 0 to 8 that can be evaluated against risk acceptance criteria. This risk scale could also be mapped to a simple qualitative risk rating, for example:

- Low risk: 0-2
- Medium Risk: 3-5
- High Risk: 6-8

4.1.4 Typical threat categories considered in ZSM

4.1.4.0 Description

Threats may be deliberate or accidental which may result in, for example, leak of information, damage of services or loss of properties, etc. The business or reputation can also be impacted because of threat of regulation incompliance. The present document lists typical threats may be relevant to ETSI ZSM framework and solutions.

4.1.4.1 Deliberate threat

This table lists potential deliberate threats on ZSM. It is expressed as Adversarial Tactic and Technique (ATT). Adversarial Tactic for ZSM is catalogued in table 4.1.4.1-1. Adversarial Technique could be various on different assets, it will be described in threat analysis for concrete assets.

Table 4.1.4.1-1: List of potential Deliberate threat on ZSM

Threat Cat Id	Adversarial Tactic	Description	Threat Source
D1	Engage in deceptive interactions	Attack patterns within this category focus on malicious interactions with a target in an attempt to deceive the target and convince the target that it is interacting with some other principal and as such take actions based on the level of trust that exists between the target and the other principal. These types of attacks assume that some piece of content or functionality is associated with an identity and that the content/functionality is trusted by the target because of this association. Often identified by the term "spoofing", these types of attacks rely on the falsification of the content and/or identity in such a way that the target will incorrectly trust the legitimacy of the content. For example, an attacker may modify a financial transaction between two parties so that the participants remain unchanged but the amount of the transaction is increased. If the recipient cannot detect the change, they may incorrectly assume the modified message originated with the original sender. Attacks of these type may involve an adversary crafting the content from scratch or capturing and modifying legitimate content.	Individual • Outsider • Insider Organization • Competitor Nation-State
D2	Abuse Existing Functionality	An adversary uses or manipulates one or more functions of an application in order to achieve a malicious objective not originally intended by the application, or to deplete a resource to the point that the target's functionality is affected. This is a broad class of attacks wherein the adversary is able to alter the intended result or purpose of the functionality and thereby affect application behavior or information integrity. Outcomes can range from information exposure, vandalism, degrading or denial of service, as well as execution of arbitrary code on the target machine.	Individual • Outsider • Insider Organization • Competitor Nation-State
D3	Manipulate Data Structures	Attack patterns in this category manipulate and exploit characteristics of system data structures in order to violate the intended usage and protections of these structures. This is done in such a way that yields either improper access to the associated system data or violations of the security properties of the system itself due to vulnerabilities in how the system processes and manages the data structures. Often, vulnerabilities and therefore exploitability of these data structures exist due to ambiguity and assumption in their design and prescribed handling.	Individual • Outsider • Insider • Trusted Insider • Privileged Insider Organization • Competitor • Supplier • Partner • Customer Nation-State

Threat Cat Id	Adversarial Tactic	Description	Threat Source
D4	Manipulate System Resources	Attack patterns within this category focus on the adversary's ability to manipulate one or more resources in order to achieve a desired outcome. This is a broad class of attacks wherein the attacker is able to change some aspect of a resource's state or availability and thereby affect system behavior or information integrity. Examples of resources include files, applications, libraries, infrastructure, and configuration information. Outcomes can range from vandalism and reduction in service to the execution of arbitrary code on the target machine.	Individual • Outsider • Insider • Trusted Insider • Privileged Insider Organization • Competitor • Supplier • Partner • Customer Nation-State
D6	Employ Probabilistic Techniques	An attacker utilizes probabilistic techniques to explore and overcome security properties of the target that are based on an assumption of strength due to the extremely low mathematical probability that an attacker would be able to identify and exploit the very rare specific conditions under which those security properties do not hold.	Individual • Outsider • Insider Organization • Competitor Nation-State
D7	Collect and Analyse Information	Attack patterns within this category focus on the gathering, collection, and theft of information by an adversary. The adversary may collect this information through a variety of methods including active querying as well as passive observation. By exploiting weaknesses in the design or configuration of the target and its communications, an adversary is able to get the target to reveal more information than intended. Information retrieved may aid the adversary in making inferences about potential weaknesses, vulnerabilities, or techniques that assist the adversary's objectives. This information may include details regarding the configuration or capabilities of the target, clues as to the timing or nature of activities, or otherwise sensitive information. Often this sort of attack is undertaken in preparation for some other type of attack, although the collection of information by itself may in some cases be the end goal of the adversary.	Individual • Outsider • Insider • Trusted Insider • Privileged Insider Organization • Competitor • Supplier • Partner • Customer Nation-State
D8	Subvert Access Control	An attacker actively targets exploitation of weaknesses, limitations and assumptions in the mechanisms a target utilizes to manage identity and authentication as well as manage access to its resources or authorize functionality. Such exploitation can lead to the complete subversion of any trust the target system may have in the identity of any entity with which it interacts, or the complete subversion of any control the target has over its data or functionality. Weaknesses targeted by subversion of authorization controls are often due to three primary factors: 1) a fundamental dependence on authentication mechanisms being effective; 2) a lack of effective control over the separation of privilege between various entities; and 3) assumptions and over confidence in the strength or rigor of the implemented authorization mechanisms.	Individual • Outsider • Insider Organization • Competitor • Supplier • Partner • Customer Nation-State
NOTE: This table mainly refers to MITRE Common Attack Pattern Enumeration and Classification (CAPEC) for ZSM specific attack patterns.			

4.1.4.2 Accidental threat

It is used for grouping threats that can accidentally damage information assets.

Table 4.1.4.2-1: List of potential accidental threats on ZSM

Threat Id	Threat Name	Threat Description
A1	Spill sensitive information	Authorized user erroneously contaminates a device, information system, or network by placing on it or sending to it information of a classification/sensitivity which it has not been authorized to handle. The information is exposed to access by unauthorized individuals, and as a result, the device, system, or network is unavailable while the spill is investigated and mitigated.
A2	Mishandling of critical and/or sensitive information by authorized users	Authorized privileged user inadvertently exposes critical/sensitive information.
A3	Incorrect privilege settings	Authorized privileged user or administrator erroneously assigns a user exceptional privileges or sets privilege requirements on a resource too low.
A4	Mis-configuration	Administrator erroneously configure a system, e.g. enable a vulnerable port, disable security function, etc.
A5	Communications contention	Degraded communications performance due to contention.
A6	Introduction of vulnerabilities into software products	Due to inherent weaknesses in programming languages and software development environments, errors and vulnerabilities are introduced into commonly used software products.
A7	Disk error	Corrupted storage due to a disk error.
A8	Pervasive disk error	Multiple disk errors due to aging of a set of devices all acquired at the same time, from the same supplier.
A9	Natural disaster	Loss of data or damage of service caused by the regional disaster.
A10	Infrastructure Failure/Outage	Loss of data or damage of service caused by outage of infrastructure.
A11	Infrastructure Incapability	Degraded security assurance because unexpected limitation of infrastructure.

4.1.4.3 Regulation noncompliance threat

It is used for grouping threats caused by violation of regulatory laws.

Table 4.1.4.3-1: List of potential threats of regulatory incompliance

Threat Id	Threat Name	Regulation Type	Regulation Requirement
R1	Privacy	Regional/Industry Regulation	Privacy of user
R2	Data Exfiltration	Regional Regulation	Boarder control of data
R3	Service Exfiltration	Regional Regulation	Service in specific area
R4	Leak sensitive information	Industry Regulation	Confidentiality of data
R5	IP or license compromising	Regional Regulation	License of Cryptographic or other algorithm

4.1.5 Threat analysis and assessment template

4.1.5.0 Description

There are several threat models defined in security industry, some models categorize threats based on impaction caused by the incident (e.g. description, corruption, disclosure, interruption, etc., defined in ITU-T), some models group threats according to domain of targets (e.g. software, hardware, communication, etc. defined in CAPEC project of MITRE), or attack mechanism (e.g. Deceptive Interaction, Abuse functionality, Manipulate resource, etc. defined in CAPEC project of MITRE), and some models classify threats for different phases of Advanced Persistent Threat (APT) (e.g. Initial Access, persistent, lateral movement and exfiltration, etc., defined in ATT&CK project of MITRE (see [i.5])).

The present document proposes ZSM threat analysis and assessment based on assets of ZSM framework and classifies threats according to attack mechanism defined in CAPEC project of MITRE.

Following pattern will be adopted as template of threat and risk report.

4.1.5.1 Asset description

This clause describes the functionality and value of the asset in general, the construction of the asset (e.g. software, hardware, etc.), the potential owner and supply chain of the asset, external and internal interface of the asset, technologies used in the asset, and potential lifecycle of the asset and possible deployment area of the asset, etc.

Furthermore, this clause identifies vulnerabilities of the asset which may be exploited by a threat agent.

4.1.5.2 Threat analysis and assessment Report

Table 4.1.5.2-1: Threat Analysis and assessment report template

Threat Id (note 3)	Threat Cat Id (note 2)	Adversarial Technique (note 1)	Threat Description	Consequence of Incident	Business Impact Level	Likelihood of Incident Scenario	Risk Score	Potential countermeasure

NOTE 1: This field is only applicable for Deliberate threat.
NOTE 2: The Threat Cat Id is same to Threat Id for non-adversarial threat.
NOTE 3: The threat Id started with "D" represents Deliberate threat, the threat Id started with "A" represents Accidental threat, the threat Id started with "O" represents Other types of threat.
NOTE 4: The Business Impact Level is determined according to severity and range of adverse effect caused by threat event.

Very high: The threat event could be expected to have catastrophic adverse effect on the framework or the framework provider's business, e.g. it incurs cease of business or huge financial loss of the framework provider.

High: The threat event could be expected to have a severe adverse effect on the framework or the framework provider's business. E.g. It causes severe degradation or loss of mission capability of framework to an extent and duration that the framework is not able to perform one or more of its primary functions. Financial or reputation loss of the framework provider is significant but still manageable.

Medium: The threat event could be expected to have a serious adverse effect on the framework or the framework provider's business. E.g. It causes a significant degradation in mission capability to an extent and duration that the framework is able to perform its primary functions, but the effectiveness of the functions is significantly reduced. Financial or reputation loss of the framework provider is manageable.

Low: The threat event could be expected to have a limited adverse effect on the framework or the framework provider's business. E.g. It causes a degradation in mission capability to an extent and duration that the framework is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced. Few business impacts on the framework provider.

Very Low: The threat event could be expected to have a negligible adverse effect on the framework.

NOTE: Impact levels and risk scores proposed in this table are based on best practice in general perspective. The values can change according to different scenarios, deployment environments, organization policies and regional regulations, etc. The organizations could re-prioritize the risks including the impact levels and adopt relevant countermeasures accordingly.

4.2 Threat and risk analysis on ZSM framework

4.2.1 Targets of assessment

The present document analyses the risk of ZSM framework in E2E service point of view and focuses on assets listed in table 4.2.1-1.

Table 4.2.1-1: List of assets to be assessed

Asset Name	Asset Description
E2E Service management domain	Refer to clause 3.1 of ETSI GS ZSM 007 [i.16]
E2E Service management function	Management function (refer to clause 3.1 of ETSI GS ZSM 007 [i.16]) in E2E Service management domain
E2E Service management service	Management service (refer to clause 3.1 of ETSI GS ZSM 007 [i.16]) in E2E Service management domain.
Cross-Domain data service	Refer to clause 3.1 of ETSI GS ZSM 007 [i.16]
Integration fabric	Refer to clause 3.1 of ETSI GS ZSM 007 [i.16]
Collected data	Refer to note 2 of clause 5.3.2 of ETSI GS ZSM 002 [i.15]

4.2.2 Threat and risk report

4.2.2.1 E2E Service management domain

4.2.2.1.1 Asset description

E2E Service management domain represents a management scope that federates together management services, and enables their exposure towards external E2E services consumers.

The E2E Service management domain is comprised of management functions which are producers of E2E management services and can be consumers of other domain management services.

E2E Service management domain (which is generally provided by a mobile network operator) is exposed to vertical domains such as enterprise, finance, governments, web-scale, etc. to provide capabilities to the vertical consumer to build and manage E2E services. On the other hand, The E2E service management domain interacts with other industry domains, e.g. transport provider, cloud provider, etc., to reserve, book and deploy resources for the E2E services. The trust levels required by different domains are various, and the trust levels of the same domain in different context can also be different. In addition, cloud-native management functions and service-based architecture are adopted by ZSM to facilitate fast deployment and update of services to satisfy the diversity requirements from various vertical customers. The trust context and relationship between management functions of the same domain or different domains could be changed dynamically along with the change of the management domain itself, its consumer or its producer. The security posture or threat surface of the E2E Service management domain can be changed constantly accordingly. E.g. if one producer of the E2E service management domain is compromised by security attack concerning the 5GC domain, the security of the E2E service management domain can be influenced and therefore appropriate actions should be taken to further ensure security. Another example is that if an E2E service management domain supports a financial consumer from now, the security level of the E2E management domain should be increased to comply with Payment Card Industry Data Security Standard (PCI DSS). Further, the border of the E2E service management domain becomes blurred by using new technologies, and the visibility of the risk become fuzzy because of multi-domains and multi-layers.

E2E Service management data is Management data (refer to clause 6.4.1 of ETSI GS ZSM 002 [i.15]) in E2E Service management domain which including e.g. PM, FM, TM data used for SLA assurance, IAM data for access control, tenant information, etc. The confidentiality of sensitive data (e.g. IAM related data, tenant information), integrity and availability of data (e.g. Performance Management, Fault Management, Trace Management data, configuration files, orchestration policies, logs, service models, etc.) for SLA fulfilment and assurance should be protected. The privacy of individuals should be protected when the ZSM framework deal with personal data. E.g. the data collected, proceeded and distributed by the ZSM framework (as data controller or processor) should not be used to identify a person or behaviour of a person without consent of the data subject.

NOTE: Refer to General Data Protection Regulation (EU GDPR) [i.6] for definition of data subject and 'consent' of the data subject.

4.2.2.1.2 Threat analysis and assessment report

Table 4.2.2.1.2-1

Threat Id	Threat Cat Id	Adversarial Technique	Threat Description	Consequence of Incident	Impact Level	Likelihood of Incident	Risk Score	Potential countermeasure
D1.1	D1	Spoofing	An adversary deceives an application or user with Content Spoofing, Identity Spoofing, Resource location Spoofing, etc., especially when there is change on previously trusted parties	MnS producer of E2E service management domain was deceived to expose sensitive resource or capability to unauthorized party, request a resource from an unintended location or execute malicious request, etc., then damage the management and managed entities in the domain	High	High	6	Build adaptive trust model, adopt UEBA to prevent potential APT, employ robust authentication processes (E.g. multi-factor authentication)
D2.3	D2	Functionality bypass	An adversary attacks a service by bypassing some or all functionality intended to protect it. Often, a system user will think that protection is in place, but the functionality behind those protections has been disabled	The confidentiality, integrity, availability of the E2E service management service is compromised to lose of service or leak of information	High	High	6	Built in compliance check and enforcement
D3.2	D3	Shared Data Manipulation	An adversary exploits a data structure shared between multiple applications or an application pool to affect application behavior	This can result in invalid trust assumptions, corruption or stolen of additional data through the normal operations of the other users of the shared data, or even cause a crash or compromise of the sharing applications	High	High	6	Apply software vulnerability validation. Data classify, label and isolation
D4.6	D4	Exploit multi-tenancy in a cloudified environment	Adversary, with processes running in an organizationally-used cloudified environment, takes advantage of multi-tenancy to observe behavior of organizational processes, acquire organizational information, or interfere with the timely or correct functioning of organizational processes	Loss of sensitive information of an organization, loss of reputation of the framework provider	Very High	Very High	8	Resource isolation for different tenants during deployment and runtime, strong access control for interaction between tenants, monitor and detect abnormal behaviours, encrypt sensitive information
D4.7	D4	Exploit insecure or incomplete data deletion in multi-tenant environment	Adversary obtains unauthorized information due to insecure or incomplete data deletion in a multi-tenant environment (e.g. in a cloud computing environment)	Loss of sensitive information of an organization, loss of reputation of the framework provider	Medium	Medium	4	Resource isolation for different tenants across multi-layers during deployment and runtime, clean-up information when terminate a service for a tenant

Threat Id	Threat Cat Id	Adversarial Technique	Threat Description	Consequence of Incident	Impact Level	Likelihood of Incident	Risk Score	Potential countermeasure
D4.8	D4	Violate isolation in multi-tenant environment	Adversary circumvents or defeats isolation mechanisms in a multi-tenant environment (e.g. in a cloud computing environment) to observe, corrupt, or deny service to hosted services and information/data	Loss of sensitive information of an organization, loss of service for legitimate organization, loss of reputation of the framework provider	Very High	Very High	8	Resource isolation for different tenants during deployment and runtime, strong access control for interaction between tenants, monitor and detect abnormal behaviours
D7.1	D7	Illegal Interception	An adversary monitors data streams to or from the service or service owner for information gathering purposes	Leak of sensitive information	Medium	High	5	Data encryption and access control
D9.1	D9	Tamper management data	An adversary (internal user with required privilege or external attack with privilege escalation after initial access) tamper management data (e.g. event, measurement, KPI, configuration file, log, etc.) to change the behaviour or reaction of the system	Cause disrupt or loss of service, and prevent efficient reaction in case of exception in incident	Very High	Very High	8	Data integrity protection and strict access control
D9.2	D9	Tamper security log	An adversary (internal user with required privilege or external attack with privilege escalation after initial access) tamper security log or other trace information to hide anomaly behaviour	The attack cannot be detected and traced, and the forensic evidence cannot be provided in case of compromising and financial/business loss	Medium	Medium	4	Data classification and labelling, integrity protection and strict access control
A1			Authorized user or client erroneously contaminates a device, information system, or network by placing on it or sending to it information of a classification/sensitivity which it has not been authorized to handle	The information is exposed to access by unauthorized individuals, and as a result, the device, system, or network is unavailable while the spill is investigated and mitigated	High	High	6	Data classification, labelling, isolation and tracking, anomaly detection and alerting
A2			Authorized privileged user or client inadvertently exposes critical/sensitive information	Leak of critical/sensitive information	High	Medium	5	Data classification, labelling, isolation and tracking and anomaly detection and alerting
A3			Authorized privileged user or administrator or client erroneously assigns a user exceptional privileges or sets privilege requirements on a resource too low	Leak of critical/sensitive information to unauthorized users	High	Medium	5	Compliance check and enforcement, and Resource isolation
A7			Corrupted storage due to a disk error	Loss of critical data and interruption of service	Very High	Low	5	Backup and Restore

Threat Id	Threat Cat Id	Adversarial Technique	Threat Description	Consequence of Incident	Impact Level	Likelihood of Incident	Risk Score	Potential countermeasure
A8			Multiple disk errors due to aging of a set of devices all acquired at the same time, from the same supplier	Loss of critical data and interruption of service	Very High	Very Low	4	Backup and Restore
E1			Loss of data or damage of service caused by the regional disaster	Disruption of service	Very High	Low	5	Cross region Backup and restore capability
E2			Loss of data or damage of service caused by outage of infrastructure	Disruption of service	Very High	Low	5	Backup and restore capability
R1			Invasion of privacy	Being fined because of disclosure of user's privacy	Very High	Very High	8	Privacy protection aligned with regional/industry regulations
R2			Violate boarder control of data	Leak national secret	Very High	Medium	6	Security zone and Data leak protection
R3			Violate boarder control of the service	Cease of service because of violating regional law	Very High	low	5	Security zone and policy enforcement
R4			Confidentiality of data	Leak sensitive information of business	Very High	High	5	Data leak protection. Data classification, labelling and isolation

4.2.2.2 E2E Service management service

4.2.2.2.1 Asset description

E2E Service management service is a set of offered management capabilities in the E2E Service management domain. The service is exposed to the consumers (e.g. verticals, third parties, etc.) from various domains and regions through human or machine interfaces.

E2E Service management services include E2E service orchestration services, E2E service intelligence services, E2E service analytics services, E2E service data collection and supporting services such as E2E policy management services.

As consumer facing services, all open web application security risks could be applied on the E2E Service MnSs. Access control is another main concern for E2E Service MnS to make sure the MnS itself and its managed entities are defended from unauthorized reading and writing. In addition, security SLA/SLS assurance for E2E service is critical for the business and reputation of the E2E Service MnS producer, and the authenticity of the domain MnSs to support E2E service management and orchestration should be always validated.

4.2.2.2.2 Threat analysis and assessment report

Table 4.2.2.2.2-1

Threat Id	Threat Cat Id	Adversarial Technique	Threat Description	Consequence of Incident	Impact Level	Likelihood of Incident	Risk Score	Potential countermeasure
D1.1	D1	Spoofing	An adversary deceives an application or user with Content Spoofing, Identity Spoofing, Resource location Spoofing, etc., especially when there is change on previously trusted parties	MnS of E2E service management service was deceived to expose sensitive resource or capability to unauthorized party or consume service or data from fraudulent producer that could damage both E2E service management service producer and consumer	High	High	6	Build adaptive trust model, adopt UEBA to prevent potential APT, employ robust authentication processes (e.g. multi-factor authentication)
D2.1	D2	Excessive Allocation	An adversary tampers the service request which causes the target to allocate excessive resources to servicing the attackers' request	Reduce the resources available for legitimate services and degrading or denying services	High	High	6	Integrity protection and validation of the service request, and employ robust access control could be helpful
D2.3	D2	Functionality bypass	An adversary attacks a service by bypassing some or all functionality intended to protect it. Often, a system user will think that protection is in place, but the functionality behind those protections has been disabled	The confidentiality, integrity, availability of the E2E service management service is compromised to lose of service or leak of information	High	High	6	Compliance check and enforcement
D2.4	D2	API Manipulation	An adversary manipulates the use or processing of an Application Programming Interface (API) resulting in an adverse impact upon the security of the system implementing the API	Unauthorized access, data disclosure data, loss or manipulation, account takeover, resource and function manipulation, privilege escalation, etc.	Medium	High	5	Best practice suggested by Open Web Application Security Project (OWASP) and OWASP API should be adopted
D2.5	D2	Flooding	An adversary consumes the resources of a target by rapidly engaging in a large number of interactions with the target	Prevents legitimate users from accessing the service and can cause the target to crash or DoS	High	Medium	5	Employ robust access control and flow control, deploying NGFW could be helpful
D2.6	D2	Resource Leak Exposure	An adversary utilizes a resource leak on the target to deplete the quantity of the resource available to service legitimate requests	Resource depletion through leak until the target is reset, therefore reduce the resources available for legitimate services and degrading or denying services	High	High	6	Apply software vulnerability validation
D2.7	D2	Communication Channel Manipulation	An adversary manipulates a setting or parameter on communications channel in order to compromise its security	This can result in information exposure, insertion/removal of information from the communications stream, and/or potentially system compromise	Medium	Medium	4	Correctly configure the security service, and capable to integrate with existing AAA system

Threat Id	Threat Cat Id	Adversarial Technique	Threat Description	Consequence of Incident	Impact Level	Likelihood of Incident	Risk Score	Potential countermeasure
D2.8	D2	Sustained Client Engagement	An adversary attempts to deny legitimate users access to a resource by continually repeatedly performs actions or abuse algorithmic flaws such that a given resource is tied up and not available to a legitimate user	Legitimate users are limited or completely denied access to the resource	High	Medium	6	Apply software vulnerability validation. Provide proxy services to filter malicious traffic
D2.9	D2	Protocol Manipulation	An adversary subverts a communications protocol to perform an attack	This type of attack can allow an adversary to impersonate others, discover sensitive information, control the outcome of a session, or perform other attacks	Medium	Medium	4	Apply protocol vulnerability validation. Capable to update the security control in real-time according to new threat intelligence
D6.2	D6	Brute Force	The attacker attempts to gain access to this asset by using trial-and-error to exhaustively explore all the possible secret values in the hope of finding the secret (or a value that is functionally equivalent) that will unlock the asset	Allow the attacker to logging into the system, steal information and manipulate the system	High	Medium	6	Strong credential and algorithm, MFA, etc.
D7.1	D7	Illegal Interception	An adversary monitors data streams to or from the service or service owner for information gathering purposes	Leak of sensitive information	Medium	High	5	Data encryption and access control
D8.1	D8	Exploitation of Trusted Credentials	Attacks on session IDs and resource IDs take advantage of the fact that some software accepts user input without verifying its authenticity	The result is that spoofing and impersonation is possible leading to an attacker's ability to break authentication, authorization, and audit controls on the system	Medium	High	5	Best practice suggested by Open Web Application Security Project (OWASP) should be adopted
D8.2	D8	Man-in-the-Middle	The attacker sits between the two components to intercept and alter the message from one component to another	The potential for Man-in-the-Middle attacks yields an implicit lack of trust in communication or identify between two components	Medium	Medium	4	Apply PKI, encrypt the communication channel, strong mutual authentication
D8.3	D8	Authenticati on Abuse or bypass	An attacker obtains unauthorized access to an application, service or device either through knowledge of the inherent weaknesses of an authentication mechanism, or by exploiting a flaw in the authentication scheme's implementation	Steal information and manipulate the system	High	Medium	5	Apply software vulnerability validation, strong authentication
D8.4	D8	Privilege Abuse	An adversary is able to exploit features of the target that should be reserved for privileged users or administrators but are exposed to use by lower or non-privileged accounts	Access to sensitive information and functionality assigned to high trusted user	High	High	6	Strong access control mechanism and policies, enforce configuration compliance

Threat Id	Threat Cat Id	Adversarial Technique	Threat Description	Consequence of Incident	Impact Level	Likelihood of Incident	Risk Score	Potential countermeasure
A3			Authorized privileged user or administrator erroneously assigns a user exceptional privileges or sets privilege requirements on a resource too low	Leak of critical/sensitive information to unauthorized users	High	High	6	Compliance check and enforcement, and Resource isolation
A4			Administrator erroneously configure a system, e.g. enable a vulnerable port, disable security function, etc.	Attacked by other service in the framework or by external entity	Medium	Medium	5	Compliance check and enforcement, and Resource isolation
E3			Degraded security assurance because unexpected limitation of framework	Security SLA compromised	Medium	Very High	6	Security function availability
R1			Invasion of privacy	Being fined because of disclosure of user's privacy	High	High	6	Privacy protection aligned with regional/industry regulations
R3			Violate boarder control of the service	Cease of service because of violating regional law	Very High	Low	5	Security zone and policy enforcement

4.2.2.2.2.1 Special threats on E2E service data collection

Table 4.2.2.2.2.1-1

Threat Id	Threat Cat Id	Adversarial Technique	Threat Description	Consequence of Incident	Impact Level	Likelihood of Incident	Risk Score	Potential countermeasure
D3.2	D3	Shared Data Manipulation	An adversary exploits a data structure shared between multiple applications or an application pool to affect application behavior	This can result in invalid trust assumptions, corruption or stolen of additional data through the normal operations of the other users of the shared data, or even cause a crash or compromise of the sharing applications	High	Medium	5	Apply software vulnerability validation. Data classify, label and isolation
D9.3	D9	Tamper collected data	An adversary (internal user with required privilege or external attack with privilege escalation after initial access) tamper collected data	Cause misbehaviour of the framework especially on the impacted services	High	High	5	Data integrity protection and strict access control
D9.4	D9	Tamper data during transmission	Man-in-the-middle attack was adopted to alter the data from one component to another	Cause misbehaviour of the framework especially on the impacted services	High	Medium	5	Strong mutual authentication, integrity protect during data transfer
D9.5	D9	Fake data or service resource	Malicious logic inserted in the supply chain (e.g. implant malicious software) to deceive the consumer to use flatulent data or services	Cause misbehaviour of the framework especially on the impacted services	High	High	6	Build adaptive trust model, employ robust authentication processes
A7			Corrupted storage due to a disk error	Loss of critical data and interruption of service	Very High	Low	5	Backup and Restore
A8			Multiple disk errors due to aging of a set of devices all acquired at the same time, from the same supplier	Loss of critical data and interruption of service	Very High	Very Low	4	Backup and Restore
E1			Loss of data or damage of service caused by the regional disaster	Disruption of service	Very High	Very Low	4	Cross region Backup and restore capability
E2			Loss of data or damage of service caused by outage of infrastructure	Disruption of service	Very High	Very Low	4	Backup and restore capability
R2			Violate boarder control of data	Leak national secret	Very High	Medium	6	Security zone and Data leak protection
R4			Confidentiality of data	Leak sensitive information of business	High	Medium	5	Data leak protection. Data classification, labelling and isolation

4.2.2.2.2.2 Special threats on E2E service analytics

Table 4.2.2.2.2.2-1

Threat Id	Threat Cat Id	Adversarial Technique	Threat Description	Consequence of Incident	Impact Level	Likelihood of Incident	Risk Score	Potential countermeasure
D7.4	D7	Evocation	An adversary actively probes the target in a manner that is designed to solicit information by exploring the target via ordinary interactions for the purpose of gathering intelligence about the target, or by sending data that is syntactically invalid or non-standard in an attempt to produce a response that contains the desired data	The adversary is able to obtain information from the target that aids the attacker in making inferences about its security, configuration, or potential vulnerabilities	High	High	6	Data classification and access control, apply UEBA
D9.5	D9	Fake data or service resource	Malicious logic inserted in the supply chain (e.g. implant malicious software) to deceive the consumer to use flatulent data or services	Impact analytics result and hide system anomaly and mislead system reaction	High	High	6	Build adaptive trust model, employ robust authentication processes
R2			Violate boarder control of data	Leak national secret	Very High	Medium	6	Security zone and Data leak protection
R4			Confidentiality of data	Leak sensitive information of business	High	Medium	5	Data leak protection. Data classification, labelling and isolation

4.2.2.2.2.3 Special threats on E2E service intelligence

Table 4.2.2.2.2.3-1

Threat Id	Threat Cat Id	Adversarial Technique	Threat Description	Consequence of Incident	Impact Level	Likelihood of Incident	Risk Score	Potential countermeasure
D7.4	D7	Evocation	An adversary actively probes the target in a manner that is designed to solicit information by exploring the target via ordinary interactions for the purpose of gathering intelligence about the target, or by sending data that is syntactically invalid or non-standard in an attempt to produce a response that contains the desired data	The adversary is able to obtain information from the target that aids the attacker in making inferences about its security, configuration, or potential vulnerabilities	High	High	6	Data classification and access control, apply UEBA
D9.5	D9	Fake data or service resource	Malicious logic inserted in the supply chain (e.g. implant malicious software) to deceive the consumer to use flatulent data or services	Impact ML result and AI decision	High	High	6	Build adaptive trust model, employ robust authentication processes

Threat Id	Threat Cat Id	Adversarial Technique	Threat Description	Consequence of Incident	Impact Level	Likelihood of Incident	Risk Score	Potential countermeasure
D9.6	D9	Tamper AI Module	An attacker undermines the integrity of a product, software, or technology at some stage of the distribution channel	The integrity of the software was undermined, and the software gets to an insecure state	High	High	6	Validate the authenticity of the code source and integrity of the code during deployment/update, etc.
D9.7	D9	Steal Intelligence Property of AI module	An adversary discovers the structure, function, and composition of an object, resource, or system by using a variety of analysis techniques to effectively determine how the analysed entity was constructed or operates	Loose competitiveness and potential business as leak of IP of the module provider	Medium	Medium	4	Employ code obfuscation, encryption and access control on the target module
D9.8	D9	Utilize ML/AI for attack	Simulate human behaviour (e.g. fake captcha) to circumvents security measures	The adversary deceives authentication system and compromise the system after logged in	High	Medium	5	Employ strong Authentication, UEBA detection
A6			Due to inherent weaknesses in design and development, errors and vulnerabilities are introduced into AI Module	The vulnerabilities were exploited by the adversary to compromise the function and associated systems	High	Medium	5	Apply vulnerability validation during deployment, upgrade, and runtime, etc.
R5			License of Cryptographic or other algorithms	Being fined because of tort or violating exporting law	High	Low	4	Security zone and policy enforcement
O1			Dynamics of the AI module	The AI module can be instantiated, terminated, updated and scaled dynamically and automatically, the security control could be compromised because of the change	Medium	Very High	6	Employ adaptive security orchestration and monitoring

4.2.2.2.2.4 Special threats on E2E service orchestration

Table 4.2.2.2.2.4-1

Threat Id	Threat Cat Id	Adversarial Technique	Threat Description	Consequence of Incident	Impact Level	Likelihood of Incident	Risk Score	Potential countermeasure
D9.5	D9	Fake data or service resource	Malicious logic inserted in the supply chain (e.g. implant malicious software) to deceive the consumer to use flatulent data or services	Impact capability provided to the E2E service and loss of reputation of E2E service orchestration provider	Medium	High	5	Build adaptive trust model, employ robust authentication processes
D9.6	D9	Tamper catalogue	An attacker changes service profile/descriptor in catalogue	The integrity of the catalogue was compromised that cause incapability/wrong-capability of associated E2E service	Medium	High	5	Validate the authenticity and integrity of the service profile/descripted during service deployment/update, etc. Employ strong access control
D9.9	D9	Tamper inventory	An attacker undermines the integrity of inventory during runtime	The state of E2E service and related resources could be reported incorrectly, and cause unexpected result of capacity and feasibility check	Medium	Medium	4	Employ strong access control
D9.10	D9	Mis-operation	Deliberately or accidentally update, terminate or scale E2E service inexpertly by unauthorized user or program module	The E2E service is interrupted or disrupted, loss reputation and money of both E2E service orchestration consumer and producer	Medium	High	5	Strong permission management and access control
O2			Dynamics of the E2E service	The E2E Service can be instantiated, terminated, updated and scaled dynamically and automatically, the security control could be compromised because of the change	Medium	Very High	6	Employ adaptive security orchestration and monitoring

4.2.2.2.2.5 Special threats on E2E policy management service

Table 4.2.2.2.2.5-1

Threat Id	Threat Cat Id	Adversarial Technique	Threat Description	Consequence of Incident	Impact Level	Likelihood of Incident	Risk Score	Potential countermeasure
D9.11	D9	Tamper Policies	An attacker undermines the integrity of policy at some stage of policy lifecycle	The integrity of the policy was compromised that cause instability of E2E service and service producer, especially when policy confliction is triggered	High	High	6	Validate the authenticity and integrity of policies. Employ strong access control
D9.12	D9	Mis-operation	Deliberately or accidentally create, update or delete policies incorrectly by unauthorized user or program module	The reliability and stability of the framework could be damaged and impact both E2E service and service producer	High	High	6	Validate the authenticity and integrity of policies. Strong permission management and access control

4.2.2.3 E2E Service management function

4.2.2.3.1 Asset description

E2E Service management function is a logical entity playing the roles of service consumer and/or service producer in E2E Service management domain. The MnF can be contaminated during its lifecycle including design, implementation, building, distribution, deployment, updating, runtime and termination. The vulnerabilities of the MnF could be exploited by the adversary to compromise the MnF itself, then attack its neighbour, and its producer and consumers as well.

In addition, the intellectual property of software to construct Management Function can be misused if the software is not well protected, especially in a sharing environment.

Furthermore, dynamic MnF lifecycle introduced new challenge for security control of the MnF during its lifecycle.

4.2.2.3.2 Threat analysis and assessment report

NOTE: The threats D2.2, D3.1, D4.1 to D4.5, D6.1, D7.2, D8.5 are specific to E2E management function. Other threats are common threats which are applicable to E2E service management function and other assets, e.g. E2E service Management Domain (refer to clause 4.2.2.1) and/or E2E service Management Service (refer to clause 4.2.2.2).

Table 4.2.2.3.2-1

Threat Id	Threat Cat Id	Adversarial Technique	Threat Description	Consequence of Incident	Impact Level	Likelihood of Incident	Risk Score	Potential countermeasure
D1.1	D1	Spoofing	An adversary deceives an application or user with Content Spoofing, Identity Spoofing, Resource location Spoofing, etc., especially when there is change on previously trusted parties	MnS provided by E2E service management function was deceived to expose sensitive resource or capability to unauthorized party or consume service or data from fraudulent producer that could damage both E2E service management service producer and consumer	High	High	6	Build adaptive trust model, adopt UEBA to prevent potential APT, employ robust authentication processes (e.g. multi-factor authentication)
D2.1	D2	Excessive Allocation	An adversary tampers the service request which causes the target to allocate excessive resources to servicing the attackers' request	Reduce the resources available for legitimate services and degrading or denying services	High	High	6	Integrity protection and validation of the service request, and employ robust access control could be helpful
D2.2	D2	Functionality Misuse	The vulnerability of management function was exploited by adversary to achieve a negative technical impact	Security downgrade and leak of information	High	High	6	Apply software vulnerability validation
D2.3	D2	Functionality bypass	An adversary attacks a service by bypassing some or all functionality intended to protect it. Often, a system user will think that protection is in place, but the functionality behind those protections has been disabled	The confidentiality, integrity, availability of the E2E service management function is compromised to lose of service or leak of information	High	High	6	Compliance check and enforcement
D2.5	D2	Flooding	An adversary consumes the resources of a target by rapidly engaging in a large number of interactions with the target	Prevents legitimate users from accessing the service and can cause the target to crash or DoS	High	Medium	5	Employ robust access control and flow control, deploying NGFW could be helpful
D2.6	D2	Resource Leak Exposure	An adversary utilizes a resource leak on the target to deplete the quantity of the resource available to service legitimate requests	Resource depletion through leak until the target is reset, therefore reduce the resources available for legitimate services and degrading or denying services	High	High	6	Apply software vulnerability validation
D3.1	D3	Buffer Manipulation	An adversary manipulates an application's interaction with a buffer in an attempt to read or modify data they should not have access to	reading or overwriting of other unintended program memory.	Medium	High	5	Apply software vulnerability validation

Threat Id	Threat Cat Id	Adversarial Technique	Threat Description	Consequence of Incident	Impact Level	Likelihood of Incident	Risk Score	Potential countermeasure
D3.2	D3	Shared Data Manipulation	An adversary exploits a data structure shared between multiple applications or an application pool to affect application behavior	This can result in invalid trust assumptions, corruption or stolen of additional data through the normal operations of the other users of the shared data, or even cause a crash or compromise of the sharing applications	High	High	6	Apply software vulnerability validation. Data classify, label and isolation
D4.1	D4	Configuration/Environment Manipulation	An attacker manipulates files or settings external to a target application which affect the behavior of that application	The function could be corruption or mis-operation	Medium	High	5	Integrity protection and validation of external files the service depends on
D4.2	D4	Software Integrity Attack	An attacker initiates a series of events designed to cause a user, program, server, e.g. trigger to download/upgrade malicious code	The integrity of the software was undermined, and the software gets to an insecure state	Medium	High	5	Validate the authenticity of the code source and integrity of the code
D4.3	D4	Modification During Manufacture	An attacker modifies a technology, product, or component during a stage in its manufacture for the purpose of carrying out an attack against some entity involved in the supply chain lifecycle	The integrity of the software was undermined, and the software gets to an insecure state	High	High	6	Validate the authenticity of the code source and integrity of the code during deployment/update, etc.
D4.4	D4	Manipulation During Distribution	An attacker undermines the integrity of a product, software, or technology at some stage of the distribution channel	The integrity of the software was undermined, and the software gets to an insecure state	High	High	6	Validate the authenticity of the code source and integrity of the code during deployment/update, etc.
D4.5	D4	Contaminate Resource	An adversary contaminates organizational information systems (including devices and networks) by causing them to handle information of a classification/sensitivity for which they have not been authorized	The function was engaged as zombie of botnet to attack other network entities. It will be unavailable while the compromise is investigated and mitigated	High	High	6	Validate the authenticity of the code source and integrity of the code during deployment/update. Monitor and detect the anomaly of the function and network during runtime
D6.1	D6	Fuzzing	The adversary leverages fuzzing to try to identify weaknesses in the system by feeding randomly constructed input to the system and looking for an indication that a failure in response to that input has occurred	The adversary leverages the weakness identified through fuzzing to compromise the function	Medium	High	5	Support fuzzing/penetration test on the function

Threat Id	Threat Cat Id	Adversarial Technique	Threat Description	Consequence of Incident	Impact Level	Likelihood of Incident	Risk Score	Potential countermeasure
D6.2	D6	Brute Force	The attacker attempts to gain access to this asset by using trial-and-error to exhaustively explore all the possible secret values in the hope of finding the secret (or a value that is functionally equivalent) that will unlock the asset	Allow the attacker to logging into the system, steal information and manipulate the system	High	Medium	6	Strong credential and algorithm, MFA, etc.
D7.2		Reverse Engineering	An adversary discovers the structure, function, and composition of an object, resource, or system by using a variety of analysis techniques to effectively determine how the analysed entity was constructed or operates	Steal Intelligent Property, plan attack on the target based on the logic of the software	Medium	Medium	4	Employ code obfuscation in development and store, strong encryption and access control in storage
D8.5	D8	Privilege escalation	An adversary exploits a weakness enabling them to elevate their privilege and perform an action that they are not supposed to be authorized to perform	Manipulate the function and likely prepare for persistent and lateral movement of APT	Medium	High		Apply software vulnerability validation during test, deployment and runtime, filter for malicious messages, continuous monitoring
A6			Due to inherent weaknesses in design and development, errors and vulnerabilities are introduced into management function	The vulnerabilities were exploited by the adversary to compromise the function and associated systems	High	Medium	5	Apply vulnerability validation during deployment, upgrade, and runtime, etc.
R5			License of Cryptographic or other algorithms	Being fined because of tort or violating exporting law	High	Low	4	Security zone and policy enforcement
O1			Dynamics of the management function	The management function can be instantiated, terminated, updated and scaled dynamically and automatically, the security control could be compromised because of the change	Medium	Very High	6	Employ adaptive security orchestration and monitoring

5 Key security issues/risks and security control/countermeasures

5.1 Trust relationship between management domains

5.1.1 Issue description

According to security threat and risk analysis in clauses 4.2.2.1 and 4.2.2.2 (e.g. D1.1, D9.5), the openness and dynamics of ZSM framework introduced new challenges to build trust relationships between diverse management domains of ZSM framework.

For E2E network slicing management as a use case (refer to Figure 4.1-1 of ETSI GS ZSM 002 [i.15]), the trust relationship between E2E Service Management Domain and CN Management Domain can be different than trust relationship between E2E Service Management Domain and RAN Management Domain, because the security capability and assurance of CN and RAN Management Domains are different. In addition, the trust relationship between E2E Service Management Domain and RAN Management Domain can be changed time by time as the change of Management Functions (MnFs) in either domain (e.g. operational status change, package upgrade to support new features, scale to other region, etc.), the change of its service consumers (e.g. new consumer comes from a new industry domain, such as webscale) and the change of its service producers (e.g. compromising of a CN Management Function, etc.).

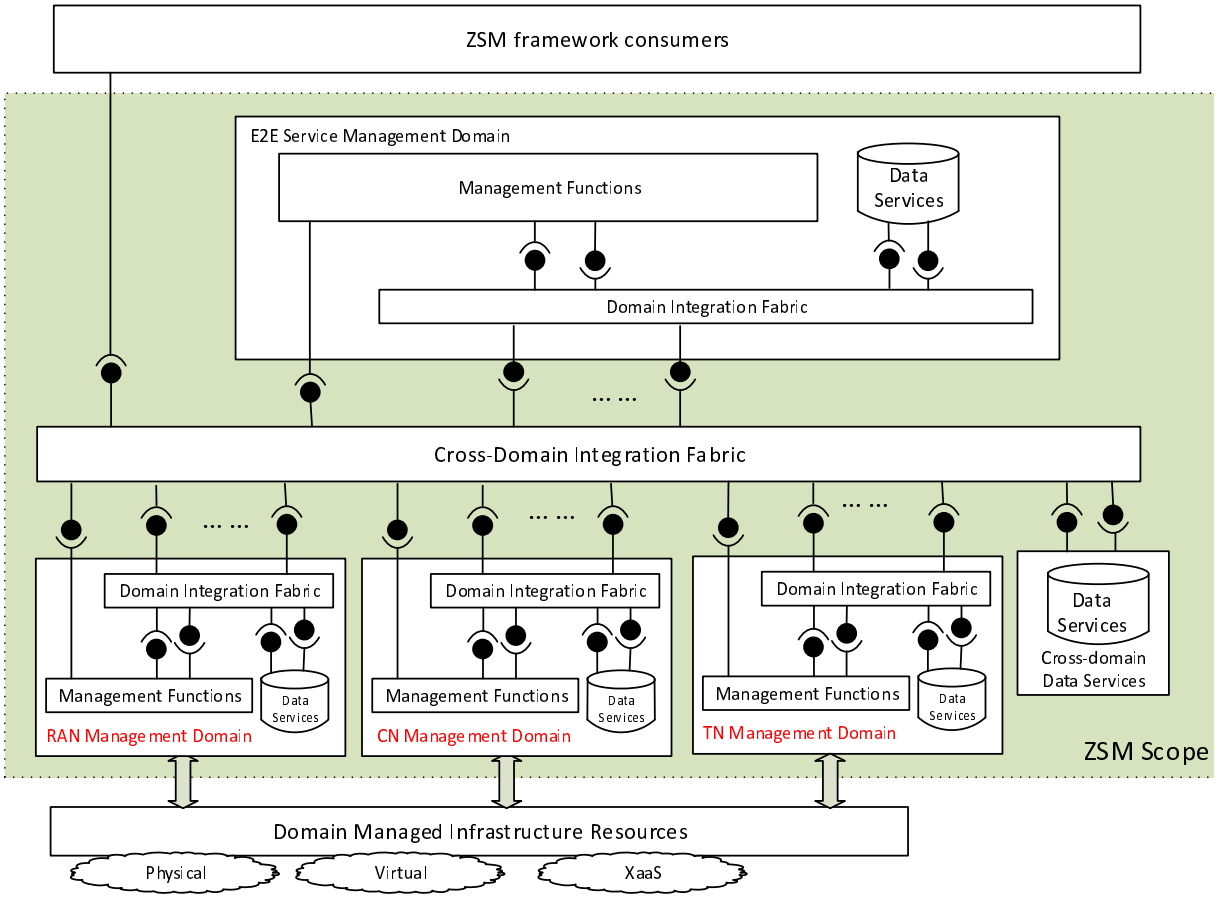

Figure 5.1.1-1: ZSM architecture deployment example for network slicing management (extracted from ETSI GS ZSM 002 [i.15])

Traditionally, there are several trust models defined to establish trust relationship between different entities and allow one entity to obtain the levels of trust needed to form partnerships, collaborate with other organizations, share information, or receive information/services. The typical trust models were defined in NIST 800-39 [i.17] including validated trust, direct historical trust, mediated trust, mandated trust, and hybrid trust. Furthermore, ETSI NFV decomposed transitive trust to several more granular models such as direct delegated trust, collaborative trust, transitive trust and reputational trust. Those trust models can be applied to various entities to build different levels of trust, but statically. The existing trust model, either single trust model or combination of multiple trust models, cannot be used independently and statically to adapt diversity and dynamics of ZSM framework.

5.1.2 Proposed solutions/countermeasures

5.1.2.1 High Level description of the proposed solution

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 ensure confidentially, integrity, availability and regulation compliance of each management domain.

Both service consumer and producer in each management domain need to evaluate the trustworthiness of the other entity based on threat and risk analysis of the entity and security countermeasures applied on the entity. Then decide the trust relationship and trust model need to be established between the consumer and producer. Afterwards, the consumer and producer can authenticate each other, defines access control rules for the opposite entity, build secure channel with each other, and record behaviors of the opposite entity, etc., according to the trust model.

5.1.2.2 Procedures of the proposed solution

5.1.2.2.1 Concepts used in the procedures

- Composition of Trust: Information generated according to analytics on Chain of Risk, Trust Profile, Trust Assurance and other context data of an entity.
- Chain of Risk: Information generated based on Trust Profile, Trust Assurance and other context data of chain of service consumers and chain of service producers of the entity.
- Chain of Service Consumer: A list of Service Consumers of an entity including direct consumers of the entity and consumers of its consumers. A Service Consumer can be Management Function, Network Function, Tenant, Operator, or any software or human entity.
- Chain of Service Producer: A list of Service Producers of an entity including direct producer of the entity and producers of its producers. A Service Producer can be Management Function, Network Function, Operator, or any software or human entity.
- Trust profile: It defines security characters (e.g. security threat and risk, applied countermeasure, security polices, regulations, etc.) and security capability (e.g. available security functions, etc.) of an entity. The Trust Profile can be changed according to upgrade, scaling of the entity, or adding/deleting/updating of services provided by the entity, adding/removing/changing of consumers or producers of the entity, security status and threat surface changing of the entity itself or its consumers or producers, the policy or regulation change on the entity, etc.
- Trust assurance: It defines capability and level of Security enforcement, verification, monitoring and compliance of an entity. Trust assurance can be dynamically changed based on change of the entity or change of its Trust profile, etc.

NOTE 1: ZSM entity in this context is a representation of a management service producer or consumer in the ZSM framework.

NOTE 2: A source ZSM entity needs to get trust assurance of a target entity before the source ZSM entity accesses MnSs provided by the target ZSM entity. In one case, the source ZSM entity retrieves information of trust assurance of the target ZSM entity from a Common Trust Entity before initial trust is established between the source and target ZSM entities. In another case, the source ZSM entity retrieves information of trust assurance of the target ZSM entity from the target ZSM entity directly if initial trust has been established between source and target ZSM entities.

NOTE 3: Common Trust Entity takes role of Root of Trust in ZSM framework. It provides trust evaluation and other trust related information of ZSM entities to build initial trust between ZSM entities.

5.1.2.2.2 Establish trust relationship between E2E service management domain and another domain

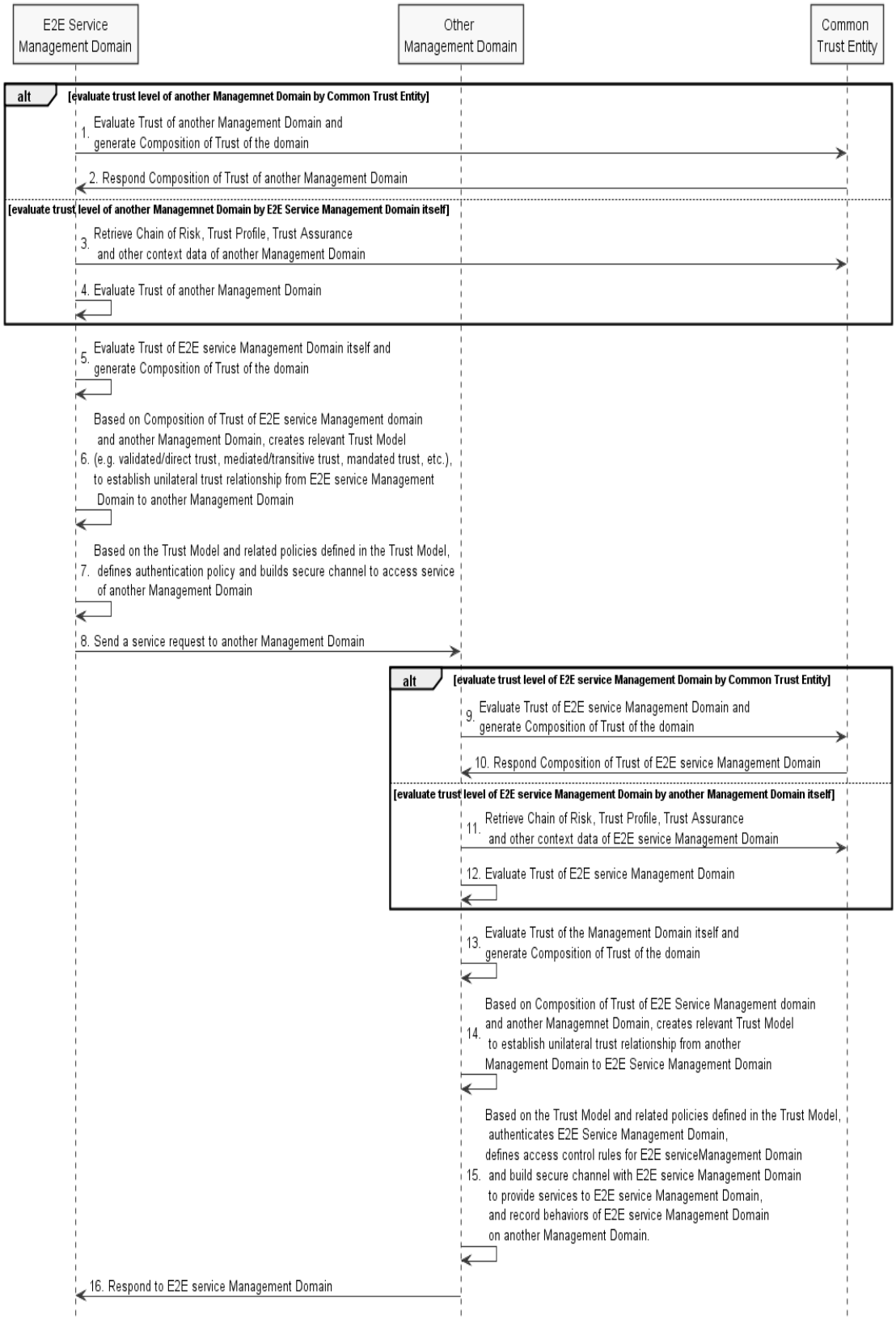

Figure 5.1.2.2.2-1: Establish trust relationship between management domains

5.1.2.2.3 Update trust relationship between E2E service management domain and another domain

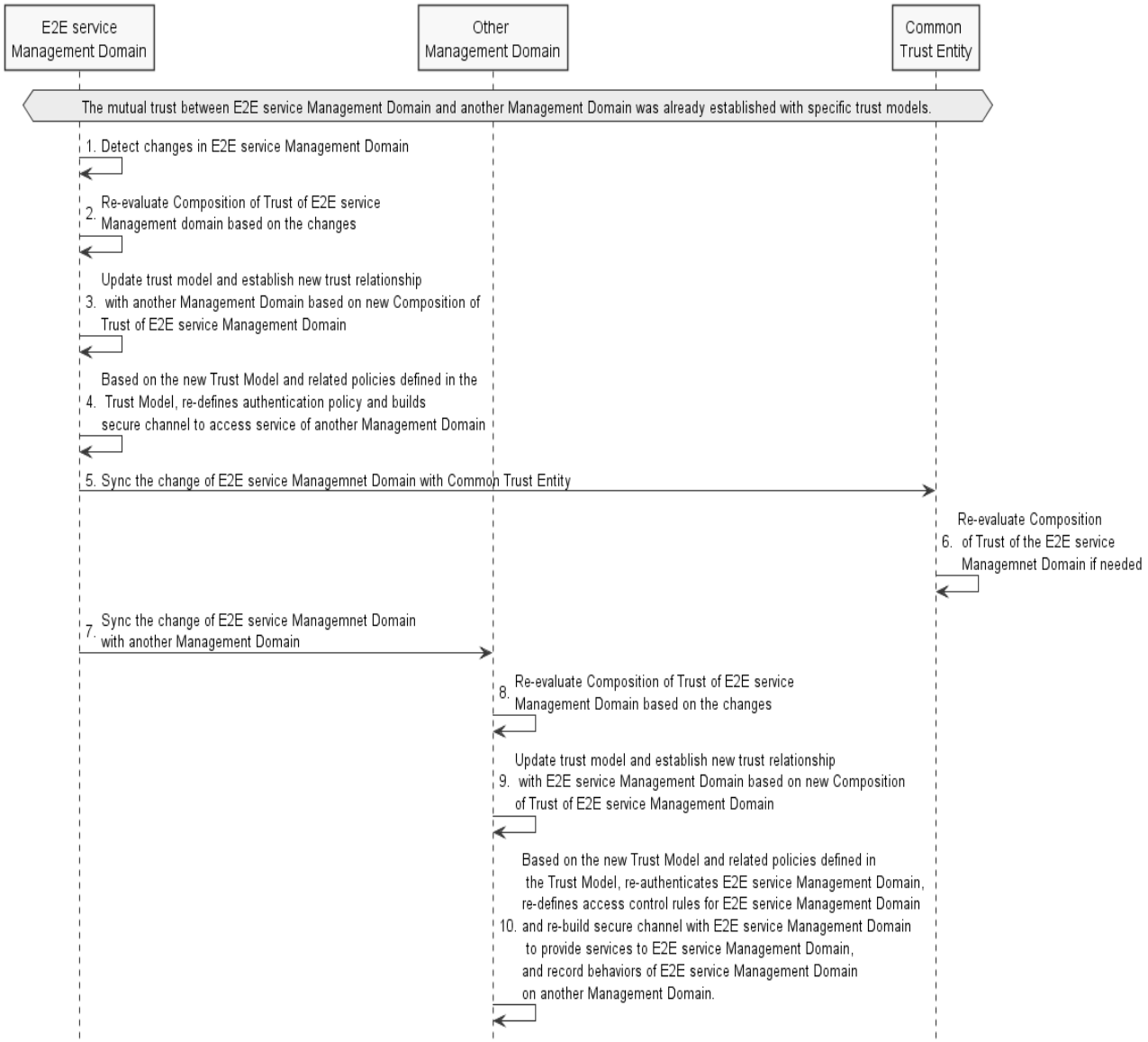

Figure 5.1.2.2.3-1: Update trust relationship between management domains

NOTE: The change of a Management Domain includes at least:

Change of the Management Domain itself, e.g.:

- Management Function in the domain upgrades, e.g. to introduce new feature, new service, or use new technology, new software or hardware, etc.
- Management Function or data in the domain is scaled or moved, especially to new geo-location.
- Security state of Management Function or data in the domain is changed, e.g. the function or data was compromised or damaged, etc.

Change of context of the Management Domain, e.g.:

- Add/delete consumer/producer of the domain, e.g. add consumer of specific industry domain.
- The security context of its consumers or producers was changed, e.g. security policy changes of its consumer.

- The threat surface related to the domain is changed, e.g. there is new vulnerability exposed, or new attack mode disclosed, etc.
- Security Policies or regulations related to the domain are changed.

5.1.2.3 Potential requirements on trust related capability

- The ZSM framework could provide knowledge based Common Trust Evaluation Service to evaluate trustworthy of ZSM entities in any management domains based on Chain of Risk, Trust Profile and Trust Assurance of the entity.
- The ZSM framework could provide knowledge based Domain Trust Evaluation Service to evaluate trustworthy of ZSM entities within the management domain based on Chain of Risk, Trust Profile and Trust Assurance of the entity.
- The ZSM framework could provide knowledge based Common Trust Model Adaptation Service to decide trust relationship and trust model between two ZSM entities in different management domains based on Composition of Trust from Trust Evaluation Service.
- The ZSM framework could provide knowledge based Domain Trust Model Adaptation Service to decide trust relationship and trust model between two ZSM entities within or across management domains based on Composition of Trust from Trust Evaluation Service.
- The ZSM framework could provide capability to re-evaluate the trustworthy of the entity to reflect any change on a ZSM entity in the ZSM framework.
- The ZSM framework could provide capability to re-build the Trust Model for the entity and re-establish Trust Relationship between the changed ZSM entity and other ZSM entities to reflect any change on an ZSM entity in the ZSM framework.

5.2 Security Assurance of E2E Management Function

5.2.1 Issue description

According to security threat and risk analysis in clause 4.2.2.3 (for E2E Service management function), the Management Functions deployed in ZSM framework can be compromised during its lifecycle. The vulnerabilities of the Management Function (MnF) could be exploited by the adversary to compromise the MnF itself, then attack other MnFs, finally endanger the whole ZSM framework and/or ZSM consumers. Also, integrity of the Management Function could be undermined by malicious party that cause MnF move to an insecure state.

5.2.2 GSMA Methodology

In addition, GSMA Network Equipment Security Assurance Scheme (NESAS) defines security requirements and an assessment framework for secure product development and product lifecycle processes, as well as using 3GPP defined security processes and test cases for the security evaluation of network equipment.

3GPP defines the complete Security Assurance Methodology (SECAM) evaluation process (refer to clause 4.5 and Figure 4.5-1 from ETSI TR 133 916 [i.8]) and roles (refer to clause 4.6.1 and Figure 4.6.2.2-1 from ETSI TR 133 916 [i.8]) to provide the expected security assurance for the Network Equipment.

SECAM defined Security assurance process

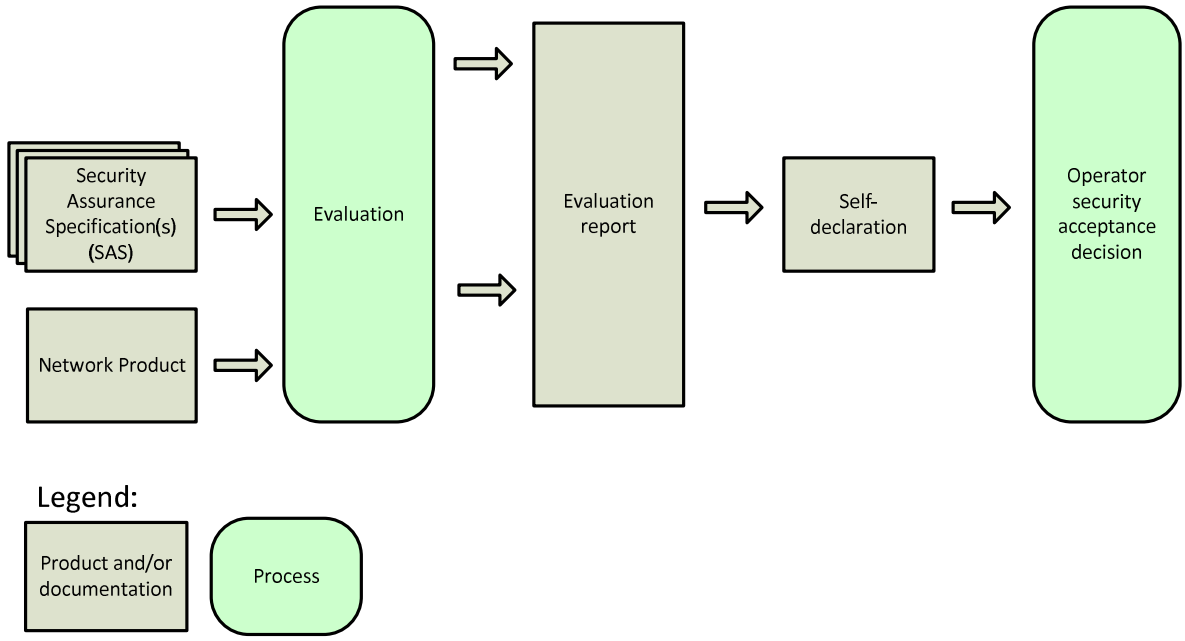

Figure 5.2.2-1: SECAM defined Security assurance process (extracted from ETSI TR 133 916 [i.8])

SECAM Roles Overview

- **Vendor** produces the network product.
- **Test laboratory** is a Test Laboratory (accredited third-party test laboratory or accredited vendor test laboratory) that evaluates the network product, evaluates evidence of compliance to the vendor development and product lifecycle requirements, and produces an evaluation report.
- **Operator** makes the decision regarding accepting assurance of security properties of the product for that vendor.
- **3GPP** is responsible for producing Security Assurance Specifications (SCAS).
- **SECAM Accreditation Body** is responsible for accreditation tasks as applicable. This role is assumed by **GSMA**.

Examples of instantiation of roles in SECAM

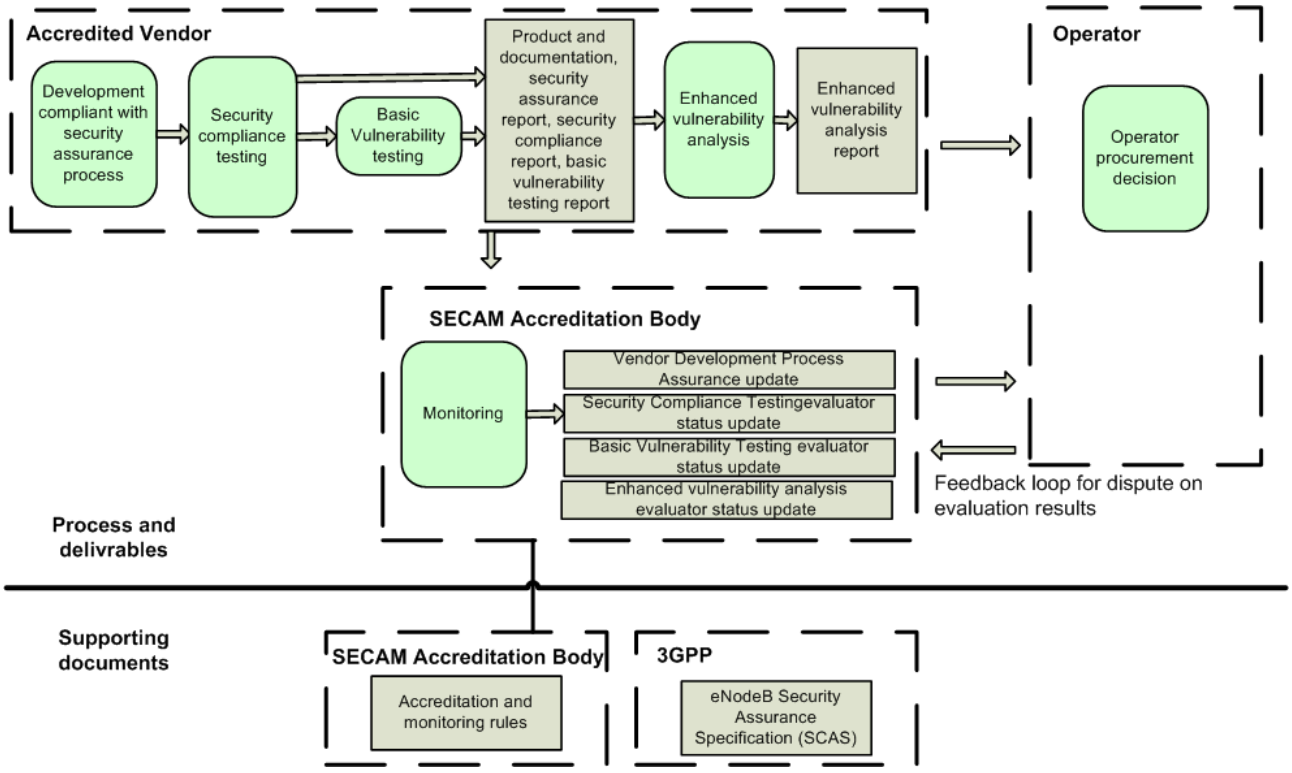

Figure 5.2.2-2: Complete self-evaluation of a 3GPP network product (e.g. eNodeB B from vendor Y) (extracted from ETSI TR 133 916 [i.8])

The present document will refer to 3GPP and GSMA to propose security assurance methodologies to ensure the security of the network products, management functions and management services deployed in ZSM framework.

5.2.3 Proposed solutions/countermeasures

5.2.3.1 High Level description of the proposed solution

ZSM framework allows the framework owner to automatically deliver new capabilities/management services provided by MnF. Security assurance process automation should be considered to avoid security threats introduced by MnF.

NOTE: Refer to clause 4.2.2.3 for potential security threats and risks of MnFs.

5.2.3.2 Procedures of the proposed solution

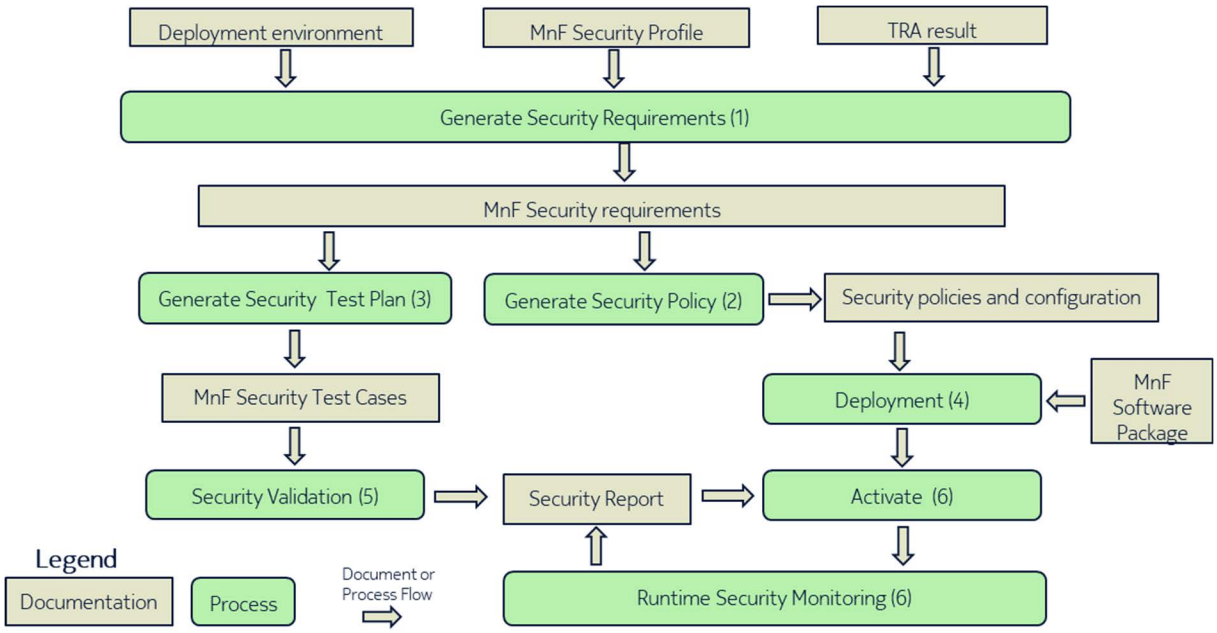

Figure 5.2.3.2-1: Security assurance process for MnF of ZSM framework

Processes:

1. Generate security requirements based on MnF security profiles (includes MnF's hardware and software technology and architecture information, functionalities, external and internal interfaces/APIs, etc.), security Threat and Risk Analysis (TRA) result (which is deduced from threat and risk analysis of the MnF in the present document (refer to clause 4.2.2), deployment environment (e.g. in which region area or country the MnF deployed, is deployed as physical box or VM or container, etc.).

2. Generate security policies based on security requirements, which could derive management functions to support security features (call it as security functions), as well as configuration parameters of the MnF and security functions, etc.

3. Generate security test plans and test cases based on security requirements, and import the test cases to the recommended tools (e.g. dynamic security tests, interactive security tests, penetration tests, etc.).

4. Deploy the MnF and security functions and configure the MnF and security functions according to security policies.

5. Configure the test tools and execute security validation for the MnF, and generate security test report.

6. Activate the MnF if security validation is passed according to test report.

7. Continuously monitoring security state (e.g. compliance checking based on security policy baseline(s), user and entity behavior detection, etc.) of the MnF in runtime, and generate security report.

5.2.3.3 Potential requirements on management function security assurance capabilities

- The ZSM framework could provide a capability to generate a security baseline for a management function deployed in the ZSM framework according to the security profile of the MnF, deployment region and mode, applied industry, organization policy of the framework owner.

NOTE 1: Security control in a security baseline for a management function could be for example the management function should be hardened with disabling unused ports and services.

- The ZSM framework could provide a capability to evaluate the security level(s) and state of a management function based on the security baseline.

NOTE 2: Security level or security assurance level is defined in ISO Common Criteria (see ISO/IEC 15408-2 [i.13], ISO/IEC 15408-1 [i.14]) or 3GPP SECAM (which used by GSMA NESAS (see ETSI TR 133 916 [i.7])) to evaluate confidence in the security of IT products and systems, or effort in terms of scope, depth and rigor applied on security assurance.

- The ZSM framework could provide a capability to support security compliance tests for a management function.

NOTE 3: Security compliance includes e.g. comply with security baseline, security standards, security regulations, security guidelines, security organization policies, etc.

- The ZSM framework could provide a capability to support vulnerability tests for a management function.
- The ZSM framework could provide a capability to validate the authenticity of the code source and the integrity of a software package of a management function.
- The ZSM framework could provide a capability to monitor and detect the anomaly and incompliance with security baseline of the management function during runtime.
- The ZSM framework could provide a capability to report the anomaly and the incompliance with security baseline.
- The ZSM framework could provide a capability to trigger the remediation on the compromised management function.

NOTE 4: E.g. trigger to run a security playbook based on security assessment result generated by AI//ML model or human input.

- The ZSM framework could provide a capability to quarantine the compromised management function.

NOTE 5: Quarantine here means segment the management function in separated execution environment, e.g. run the function in a sandbox.

5.3 Multi-tenancy of ZSM Framework

5.3.1 Issue description

Multi-tenancy refers to an architecture in which a single instance of software runs on a server and serves multiple tenants. Systems designed in such manner are often called shared. A tenant is a group of users who share a common access with specific privileges to the software instance. Gartner also defined *"The tenants (application instances) can be representations of organizations that obtained access to the multitenant application (this is the scenario of an ISV offering services of an application to multiple customer organizations)"*.

As shown in Figure 6.2-1 of ETSI GS ZSM 002 [i.15], management services (MnSs) of ZSM framework are shared by multiple ZSM framework consumers. A tenant of ZSM framework can be a group of consumers share MnSs offered by common MnFs of ZSM framework.

According to security threat and risk analysis in clause 4.2.2.1 (e.g. D4.6 - D4.8), exploiting multi-tenancy of ZSM framework and vulnerability in the multi-tenancy environment, as well as circumventing/defeating isolation mechanism in the multi-tenancy environment could cause loss of sensitive information or E2E service deployed in ZSM framework and loss of reputation of the framework provider/owner. The business impact is very high. In addition, there will be a large set of different customer types, each demanding specific capability or management services from ZSM framework. Security aspect of multi-tenancy is essential to ZSM framework to deliver corresponding capabilities to its customers, and protect the resources of the customers in the framework.

5.3.2 Proposed solutions/countermeasures

5.3.2.1 High Level description of the proposed solution

Manage tenant information in each management domain of ZSM framework. Tenant information includes, e.g. tenant Id, tenant specific policies (e.g. security policy, isolation policy, resource access policies, etc.). The policies can be defined by the tenant or ZSM management service provider based on the agreement with tenant. Tenant information also includes links to resources assigned to the tenant.

The management domain of ZSM offers corresponding capability to a tenant according to the policies defined/assigned to the tenant. In addition, the management domain should isolate resources of a tenant from other tenants based on the policies.

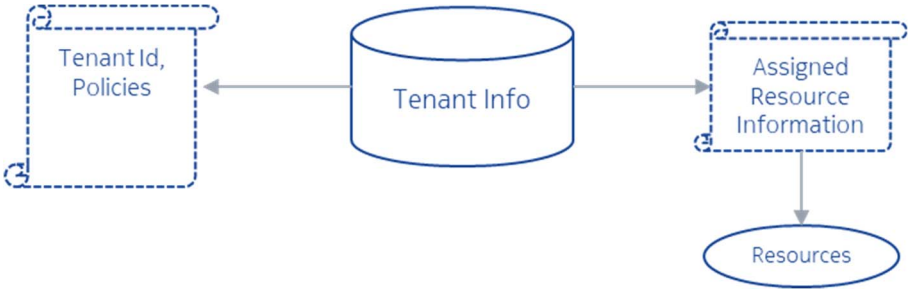

Figure 5.3.2.1-1: Tenant information in ZSM framework

5.3.2.2 Procedures of the proposed solution

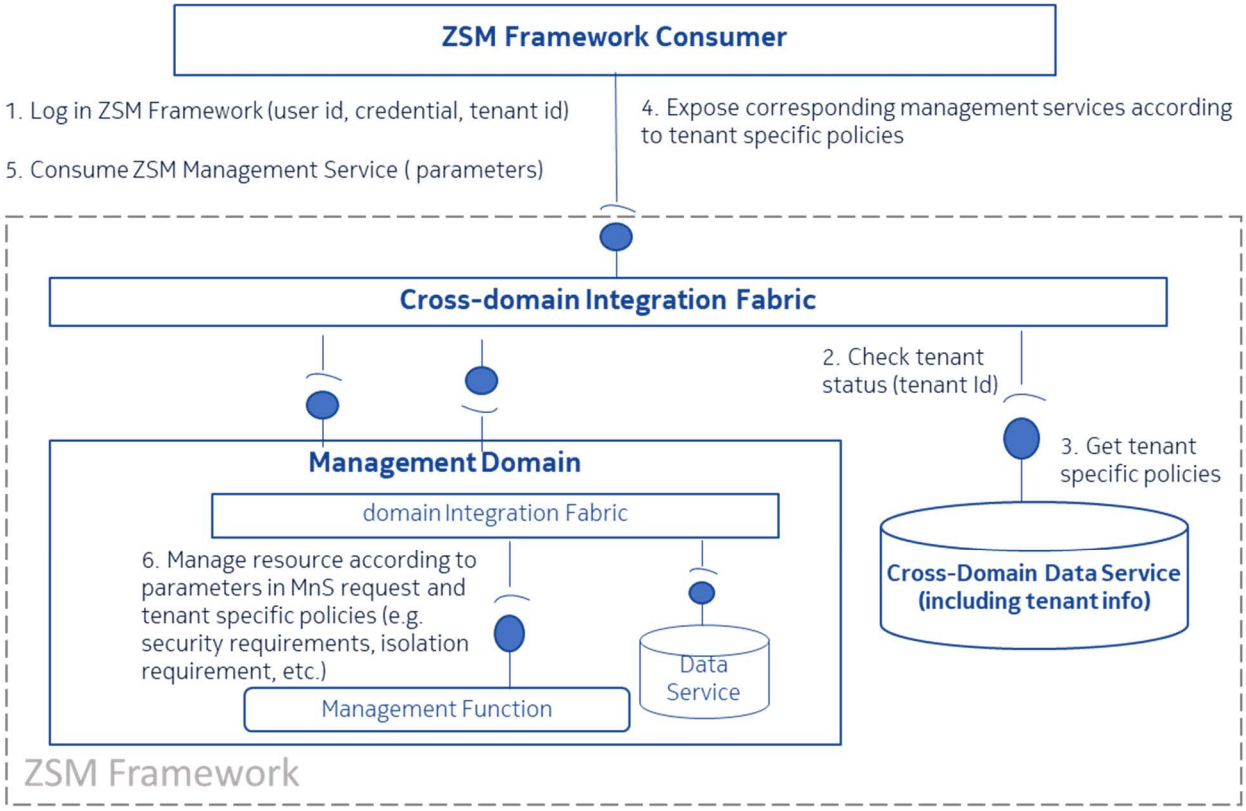

Figure 5.3.2.2-1: Multi-tenancy Scenario

Pre-condition:

- A tenant signs contract with owner of ZSM framework with negotiated SLA.
- A tenant information is created in the ZSM framework, which recorded tenant specific policies, e.g. security and isolation policies, etc., based on agreed SLS.

Steps:

1. A ZSM framework consumer, which belongs to a ZSM framework tenant, logs in the ZSM framework.
2. ZSM framework checks status of the tenant after authenticated the consumer, e.g. check if the tenant is existed and activated.
3. ZSM framework gets tenant specific policies from the tenant information created and stored in data service of the ZSM framework.
4. ZSM framework exposes corresponding management services to the consumer according to tenant specific policies.
5. The consumer sends request to ZSM framework for specific management service or resource.
6. The ZSM framework assigns/updates/deletes resources for the tenant according to the request and policies of the tenant. E.g. Isolate the resource of the tenant from others, protect the resource of the tenant with specific protection rules, etc. In addition, the ZSM framework links the resource allocated to the tenant to the tenant information created in the data service.

5.3.2.3 Potential requirement on trust related capability

- The framework could provide capability to provision tenant information.

NOTE 1: Provisioning tenant information including, e.g. create/update/delete/read tenant information.

- The framework could provide capability to protect tenant information.

NOTE 2: Protecting tenant information including, e.g. tenant id is encrypted, and tenant specific policies are tamper- resistant when stored in data service and transmitted, tenant information is only accessed by authorized users, etc.

- The framework could provide capability to expose corresponding management services to a tenant according to tenant specific polices in the tenant information.
- The framework could provide capability to assign corresponding management resources to a tenant according to tenant specific polices in the tenant information.
- The framework could provide capability to isolation management resource for a tenant according to tenant specific polices in the tenant information.
- The framework could provide capability to protect management resources of a tenant according to tenant specific polices in the tenant information.

NOTE 3: Protecting management resources including, e.g. management data (such as PM, FM data) of a tenant can only be accessed by the tenant, the management data is tamper-resistant, or anonymized based on the policies of the tenant.

NOTE 4: For the last 4 requirements, the general policies should be considered as well besides tenant specific policies.

5.4 Access Control for management service (MnS) of ZSM Framework

5.4.1 Issue description

According to security threat and risk analysis in clause 4.2.2, and especially in clause 4.2.2.2 (e.g. D2.1, D2.5, D7.1, D7.4, D8.4, D9.1, D9.3, D9.6, D9.7, D9.9, D9.10, A3, A4), an adversary could cause DoS of ZSM framework by exhausting management resources illegally, or an adversary could intercept, tamper the data, policies, etc., for other legal users (e.g. ZSM framework consumer) or management entities (e.g. management function), or a common consumer could mis-operate on management service (MnS) as high privilege administrator. Robust access control, including identification, authentication, authorization and audit, mechanism should be applied to prevent MnSs and other management resources of ZSM framework being misused by MnS consumers.

In addition, ZSM framework is built on multiple management domains. There are interactions between external entity (e.g. digital store front) and ZSM framework, between management functions (MnFs) of different MnDs, or between MnFs in the same MnD, they need to be considered differently but correlatively. Access control mechanism should be flexible to adapt the requirements and supporting technology of multiple domains.

Furthermore, the trust relationship between MnS consumer and producer could be dynamically changed along the change in each management domain. See the clause 5.1 of the present document for the trust relationship between management domains of ZSM framework. Access control mechanism should adapt the change of trust relationship between ZSM management domains, as well as between ZSM management domain(s) and external entities (e.g. ZSM framework consumers).

In ETSI GS ZSM 001 [i.18] and ETSI GS ZSM 002 [i.15], there are high level access control requirement and description in many scenarios. In addition, domain integration fabric provided capability to allow authorized consumer to configure entitlements for exposed services. However, how could the consumer (either ZSM framework consumer or MnF inside ZSM framework) be authenticated, how the access control polices be created, assigned, enforced and updated, what functionality and capability needed to support administration, decision and enforcement of authentication and authentication in consumer registration, login and service accessing phases were not specified or studied in ZSM or other network management system.

Some new services, including Cross-Domain Authentication Administration/decision Service (CDANAS), Domain Authentication Administration/decision Service (DANAS), Cross-Domain Authorization Administration/decision Service (CDARAS), Domain Authorization Administration/decision Service (DARAS) and security audit service, will be proposed in the present document to support complete access control for MnSs of ZSM framework.

Those services can be produced by cross domain/domain integration fabric, or management function in a management domain, or new cross domain management function.

5.4.2 Use cases

5.4.2.1 Access control for a ZSM framework consumer who consumes E2E service MnSs to build E2E service

Precondition:

- The consumer already registered to Cross-Domain Integration Fabric (CDIF) of ZSM framework.
- The related management function (MnF) in E2E service management domain (MnD) already registered to CDIF of ZSM framework as management service (MnS) consumer.
- All MnSs (in either E2E service or other management domains) supporting to build the E2E service are registered to CDIF or Domain Integration Fabric.

1. ZSM framework consumer logs in ZSM framework with identity and credential. CDIF, as authentication enforcement point, interacts with Cross-Domain Authentication Administration/decision Service (CDANAS) provider, to authenticate the consumer based on agreed authentication policy, as well as other security context of the identity (e.g. time, place, security status of the identity, etc.).

NOTE 1: The mechanism to manage and exchange the credential of the consumer is dependent on authentication mechanism.

2. After authentication, the CDANAS provider requests permission of the consumer from Cross-Domain Authorization Administration/decision Service (CDARAS) provider through CDIF. The identity information of the consumer should be sent to CDARAS provider.

3. The CDARAS provider assigns related access control policies to the consumer based on the classification (e.g. security level, applied industry, region, security status, etc.) of MnSs registered by multiple domains on CDIF and classification/clearance of the consumer (e.g. SLA, industry, region. etc.), as well as security context of the consumer (e.g. time, location, security status, mission/reason, etc.), and grants permission to the consumer according to the access control policies.

4. The CDARAS provider sends back the permission for the consumer to CDANAS provider.

5. The CDANAS provider generates token/assertion based on identity information and permission.

6. The CDANAS provider returns token/assertion to the ZSM framework consumer through CDIF. In addition, the CDIF exposes allowed MnSs (may include SAP, operation, resource, etc.) to the consumer.

NOTE 2: The CDIF (together with CDANAS provider and CDARAS provider) may return a single assertion/token to the consumer after successfully authentication, or return different assertion/token for different MnS producers if the consumer has capability to support that.

7. The ZSM framework consumer accesses an E2E service MnS (assume directly with address of the E2E MnS) exposed to them, the token/assertion should be included in the access request:

   a) If CDIF is exposed to the consumer, the CDIF validates the token/assertion, invoke the MnSs and forward the result to the consumer.

   b) If endpoint of MnS is exposed, the MnF of the MnS should have capability to validate the token/assertion either based on pre-configured information, or by checking with CDANAS provider.

NOTE 3: The CDIF/MnF may double check access control policies assigned to the consumer and context of the consumer with CDARAS provider before process the request.

8. After having validated the token/assertion, related MnF in the E2E service MnD maps the E2E service request to one or several requests on MnSs exposed by other management domains on CDIF.

9. The MnF of E2E service MnD logs in CDIF with its identity and credential if no authenticated session exists. The CDIF interacts with CDANAS provider to authenticate the MnF based on agreed authentication policy, as well as other security context of the MnF.

10. After authentication, the CDANAS provider requests permission of the MnF from CDARAS provider.

11. CDARAS provider assigned access control policies to the MnF and generated permission for the MnF.

12. CDARAS provider returns back permission of the MnF to CDANAS provider.

13. CDANAS provider returns token/assertion to the MnF of E2E service MnD. In addition, the CDIF exposes allowed MnSs (may include SAP, operation, resource, etc.) to the MnF.

14. The MnF of E2E service MnD accesses MnSs needed to support the service requirement of the E2E service, the token/assertion returned to the MnF should be included in the access request.

15. The related domain MnF producing MnS in the target MnD validates the token/assertion of the E2E service MnF, and processes the request. The domain MnF breakdowns the request to one or more domain MnS requests.

16. The domain MnF logs in Domain Integration Fabric (DIF) if there is no authentication session existed. The DIF interact with Domain Authentication Administration/decision Service (DANAS) provider to authenticate the domain MnF based on domain specific authentication policy, as well as other security context of the MnF. Then checks access control policies assigned to the MnF with Domain Authorization Administration/decision Service (DARAS) provider, and returns token/assertion to the domain MnF. In addition, the DIF exposes allowed MnSs (may include SAP, operation, resource, etc.) to the domain MnF.

17. The domain MnF (MnF-1) accesses another domain MnF (MnF-2) for the required MnSs with token/assertion got from the DIF. The called MnF (MnF-2) validates the token/assertion, proceeds the request and returns result to the calling MnF (MnF-1).

18. After proceeding all mapped requests with other domain MnFs, the domain MnF (MnF-1) handling request from E2E service MnD returns result to the E2E service MnF.

19. After proceeding all mapped requests with CDIF and MnFs in other MnDs, the E2E service MnF returns result to the E2E service MnS consumer.

20. CDIF records every registration, login and access request and result for the E2E service consumer, and all interactions between E2E service MnD and other MnDs in common data service.

21. DIF records every registration, login and access request and result for the MnFs of the MnD in domain data service.

5.4.2.2 Register ZSM framework consumer who may consume MnSs across multiple management domains

Precondition:

- Trust relationship between management domains of ZSM framework and Cross Domain Integration Fabric (CDIF) has been established.
- The management services will be accessed by the ZSM framework consumer are registered to cross-domain integration fabric.

1. ZSM framework consumer registers to ZSM framework, CDIF (interact with BSS or Customer care system) signs online contract with the consumer and creates record for the consumer (formal or trial tenant/customer), the negotiated SLA, may include authentication mechanism, is included in the record.

NOTE 1: As alternative, a tenant/customer might sign contract with owner of ZSM framework (e.g. Operator) in advance and the tenant/customer has been created in BSS system already, and ZSM framework administrator may register the tenant/customer to CDIF of ZSM framework on behalf of the consumer.

2. CDIF interacts with Cross-Domain Authentication/identity Administration/decision Service (CDANAS) provider to register the consumer in the access control system of ZSM framework.

3. The CDANAS provider creates primary identity for the ZSM consumer, and records the identity information, as well as preferred authentication mechanism of the consumer in common identity repository.

4. CDANAS provider returns primary identity, as well as agreed authentication mechanism to the consumer through CDIF.

NOTE 2: Authentication mechanism is decided by CDANAS provider according to its own capability, security context of the consumer and supported technology by the consumer, as well as security context of MnS producers and supported technology (e.g. type of token, assertion, etc.) by the producers which would provide services to satisfy SLA of the consumer. Through CDIF, CDANAS provider (may together with CDARAS provider) needs to go through all MnS producers and finally figure out common authentication technologies fit to potential MnS producers and also supported by the consumer.

5. With primary identity, a ZSM framework consumer could create new account and manage the access policies for the account after authentication.

NOTE 3: Discretionary Access Control (DAC) is applied in this scenario which allows ZSM framework customer to manage access policies for its own accounts in the scope of the MnSs could be accessed by the customer.

6. CDIF records every registration, login and access request and result for the ZSM framework consumer in common data service.

5.4.2.3 Register MnF as MnS consumer

Precondition:

- Mutual trust has been established between DIF, DANAS provider and DARAS provider, as well as between CDIF, CDANAS provider and CDARAS provider. In addition, MnF trusts DIF, DIF, DANAS provider and DARAS provider trusts CDIF CDANAS provider and CDARAS provider.

1. Domain Integration Fabric (DIF) of a Management Domain (MnD) registers to cross-domain integration fabric (CDIF) after the MnD being added to the ZSM framework, the request may include MnD type, MnD authentication mechanism, MnD security level, etc.

2. The CDIF calls Cross-Domain Authentication Administration Service (CDANAS) provider (including identity management) to register DIF of the MnD in the access control system of ZSM framework.

3. The CDANAS provider creates primary identity for DIF of the MnD, and records the identity information, as well as preferred authentication mechanism of the MnD in common identity repository.

NOTE 1: The CDANAS provider decides authentication policies according its own capability and security context of DIF the MnD and supported technology by the MnD.

4. CDIF returns primary identity, as well as agreed authentication mechanism to DIF of the MnD.

5. DIF of the MnD records the primary identity and authentication mechanism, and optional address of CDANAS, in domain identity repository or other domain data service.

6. With the primary identity DIF of the MnD may create account for existing MnF of the MnD in case the MnF needs to access MnS exposed on CDIF or expose its MnS on CDIF. The DIF calls CDANAS and CDARAS directly (or proxy through CDIF) to create new account and manage the access policies for the MnF together with DARAS provider.

7. After a new MnF deployed in the MnD, it registers to DIF. The DIF interacts with DANAS provider to create an identity for the MnF, together with DARAS provider, assign access control policies to the MnF for accessing domain MnSs (including DIF services) according to clearance/classification of the MnF.

   Optionally, the DIF/DANAS provider can call CDANAS and CDARAS to create account and assign access policies for the MnF together with DARAS provider, after that the MnF can register itself to CDIF, and can also access MnSs registered on CDIF and exposed to the MnF after authentication. Alternatively, the DIF could register the MnF to CDIF on behalf of the MnF.

NOTE 2: Register to domain fabric is allowed to any MnF in the MnD by default.

8. CDIF/DIF records every registration, login and access request and result for MnFs of the MnD in common/domain data service.

NOTE 3: Assume secure connection is always built in all interactions mentioned above.

NOTE 4: Based on design and security consideration of a MnD, the MnFs of the MnD could be hidden behind the DIF of the MnD. All access from/to CDIF or other domain MnFs will be proxy by DIF of the MnD. In this case, no need to create sperate account for the MnFs in CDANAS provider.

5.4.2.4 Register a new MnS

Precondition:

- DIF of the MnD registered to ZSM framework as consumer as in clause 5.4.2.3, and created account for each MnF needs to expose MnS on CDIF, and assigned basic permissions to MnF, e.g. register MnS, etc.

- MnF logged in DIF.
- DIF or MnF logged in CDIF.

1. The MnS producer registers MnS to DIF, at least the Service Access Point (SAP) of the MnS needs to be provided.
2. The DIF calls DANAS to register the MnS in authentication system.
3. According to requirements of the MnS producer, the DANAS provider could create a new record for the MnS, the SAP of the MnS should be recorded; and:
   a) put the MnS into an existing group (e.g. based on service type, security level of the service, producer of the service, authentication mechanism supported by the MnS producer, etc.), and apply the group policy on the MnS; or
   b) create a new group for the MnS, and assign authentication policies to the group according to e.g. security level of the service (may impact authentication factor), technology supported by the MnS producer (may impact authentication protocol and factor) and authentication preference.
4. The DANAS provider syncs the new MnS information with DARAS provider.
5. DARAS provider may add the MnS into existing access control policies according to the classification of the MnS and classification/clearance of the subject of an access control policy.
6. If the MnS need to be exposed to cross-domain integration fabric, the MnS producer registers the MnS to CDIF, at least SAP of the MnS need to be provided.
7. The CDIF calls CDANAS to register the MnS in common authentication system.
8. According to requirements of the MnS producer, the CDANAS provider could create a new record for the MnS, the SAP of the MnS should be recorded, and put the MnS into an existing group or create a new group for the MnS, and assign authentication policies to the group.
9. The CDANAS provider syncs the new MnS information with CDARAS provider.
10. The CDARAS provider may add the MnS into existing access control policies according to the classification of the MnS and classification/clearance of the subject of an access control policy.
11. CDIF/DIF records every registration, login and access request and result for MnFs of the MnD in common/domain data service.

NOTE: Assume secure connection is always built in all interactions mentioned above.

5.4.2.5 Change of MnS consumer or producer

1) Integration fabric discovered changes of MnS producer or consumer, and syncs the changes with Authentication Administration Service (ANAS) producer or Authorization Administration Service (ARAS) producer.
2) The ANAS provider and ARAS producer updates identity repository, authentication policy and access control policies accordingly, and may terminate the ongoing access sessions of the MnSC or MnSP.
3) Analytics or intelligence function detects security status change of MnS producer or consumer and report the change to ANAS producer and ARAS producer.
4) The ANAS producer and ARAS producer could update identity status, authentication policies and access control policies according to security status change of the MnS producer or consumer, and may terminate the ongoing access sessions of the MnSC or MnSP.

5.4.2.6 Audit MnS consumer or producer

1) An authorized auditing service consumer sends request to ZSM framework to audit MnS consumer(s).

2) The audit function of ZSM framework retrieves data related to the consumer(s) from data base, analyses the data, generates a report and returns the report to the auditing service consumer.

NOTE 1: All interactions between ZSM consumer and ZSM framework components, as well as between components of ZSM framework, are secured with confidentiality and integrity protection.

NOTE 2: According to least privilege principle, the default permission of any objects and operations for a new identity is denying.

NOTE 3: Multiple cross-domain integration fabrics may be deployed to support different management domains based on performance and security requirements.

5.4.3 Potential requirement on access control capability

- The ZSM framework could provide a capability to support cross-domain authentication administration, decision and enforcement:
  - Support identify management, including identity lifecycle management of various type of MnS consumer and producer.

NOTE 1: MnS consumer can be ZSM framework consumer, MnF, DIF, system administrator, etc.; MnS producer can be MnF.

  - Support credential management, including credential lifecycle management of various type of credentials.
  - Support authentication policy management (e.g. create, delete, update, etc.) for each MnS consumer and producer.
  - Support generating consolidated authentication policy based on MnS consumer and producer(s) of multiple management domains.
  - Support authenticating MnS consumer and producer based on authentication policy.
  - Support authentication assertion/token generation for the MnS consumer after authentication.
  - Support interacting with cross-domain integration fabric for dynamic identity and authentication policy management.

NOTE 2: The authentication policies may include following information elements as examples:

    - Authentication factor: knowledge (what do I know), ownership (what do I have), personal attributes (who am I), single factor, multi-factors.
    - Authentication mode: local authentication (on MnF provided MnS), domain authentication, common authentication, SSO, etc.
    - Authentication protocol: TLS, SAML2.0, OpenID, basic user/password, Kerberos, etc.
    - Context adaptive information: e.g. in which context what anthemion factor need to be applied, etc.

- The ZSM framework could provide a capability to support domain authentication administration, decision and enforcement:
  - Support identify management, including identity lifecycle management of various type of MnS consumer and producer.

NOTE 3: MnS consumer can be MnF, DIF, system administrator, etc.; MnS producer can be MnF.

  - Support credential management, including credential lifecycle management of various type of credentials.

- Support authentication policy management (e.g. create, delete, update, etc.) for each MnS consumer and producer.
- Support generating consolidated authentication policy based on MnS consumer and producer(s) of the domain.
- Support authenticating MnS consumer and producer based on authentication policy.
- Support authentication assertion/token generation for the MnS consumer after authentication.
- Support interacting with domain integration fabric, analytics and intelligence function for dynamic identity and authentication policy management.

- The ZSM framework could provide a capability to support cross-domain authorization administration, decision and enforcement:
  - Support authorization/access control policy management (create, delete, update) for each MnS consumer.
  - Support generating access control policy based on classification/clearance and security context of MnS consumer and classification of MnSs(s) in multiple management domains.

NOTE 4: Classification/clearance of MnS consumer could be e.g. SLA, industry, region of the MnS consumer. Security context of the MnS consumer could be e.g. time, location, security status, mission/reason of the MnS consumer. Classification of MnSs could be e.g. security level, applied industry, region, security status of the MnSs.

  - Support granting permission to the MnS consumer according to the access control policies.
  - Support interacting with cross-domain integration fabric for dynamic identity and authorization policy management.
  - Support both Discretionary Access Control (DAC) or Mandatory Access Control (MAC).

NOTE 5: The authorization/access control policies are business logic dependent, which should describe 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 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.

- The ZSM framework could provide a capability to support domain authorization administration, decision and enforcement:
  - Support authorization/access control policy management (create, delete, update) for each MnS consumer.
  - Support generating access control policy based on classification/clearance and security context of MnS consumer and classification of MnSs(s) in the management domain.

NOTE 6: Classification/clearance of MnS consumer could be e.g. SLA, industry, region of the MnS consumer. Security context of the MnS consumer could be e.g. time, location, security status, mission/reason of the MnS consumer. Classification of MnSs could be e.g. security level, applied industry, region, security status of the MnSs.

  - Support granting permission to the MnS consumer according to the access control policies.
  - Support interacting with domain integration fabric, analytics and intelligence function for dynamic identity and authorization policy management.

- Support both Discretionary Access Control (DAC) or Mandatory Access Control (MAC).

- The ZSM framework could provide a capability to support security log in data service for recording every registration, login and access request and result, and generate security report for specific domain, cross-domain, specific service, specific tenant, specific consumer, based on security logs collected from domain/cross domain data service.

5.4.4 Potential enhancement on ZSM framework to support access control

Option 1: authentication/authorization administration services and audit service are provided by integration fabric

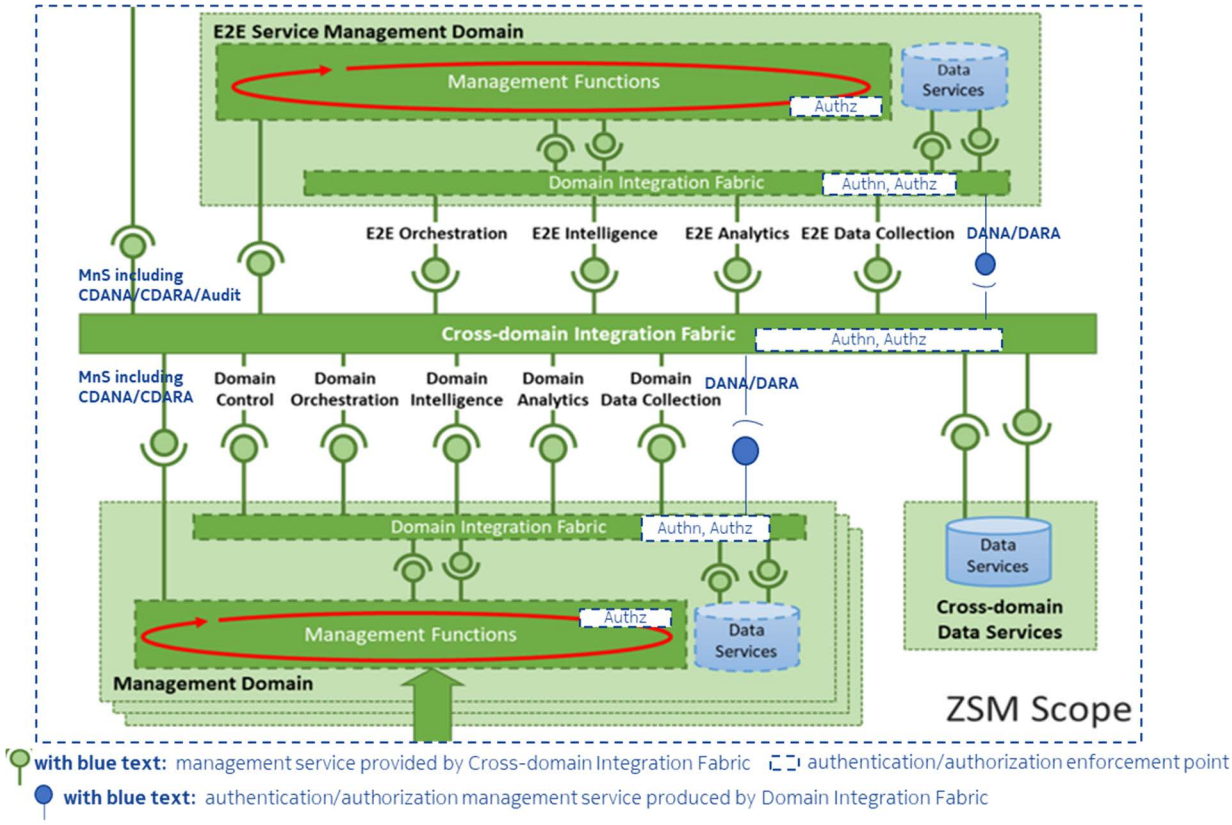

Figure 5.4.4-1

- Cross-Domain/Domain Authentication Administration (CDANA/DANA) service, Cross-Domain/Domain Authorization Administration service (CDARA/DARA) and Audit service are provided by cross-domain/domain integration fabric.

- Audit service is provided by cross-domain integration fabric.

- Authentication enforcement (validate identity and credentials, and return token/assertion) are proceeded on integration fabric.

- Authorization enforcement (validate the token and return allowed services) is proceeded on either integration fabric (in proxy case) or management function as MnS producer (in direct access case).

NOTE 1: Central authentication on integration fabric instead of each management function is proposed to improve efficiency of access control process.

Option 2: cross-domain authentication/authorization administration services and audit service are provided by dedicated AAA service producer, and domain authentication/authorization administration services are provided by domain management function

NOTE 2: The blue box in the Management Functions box is for clarification, will be removed finally.

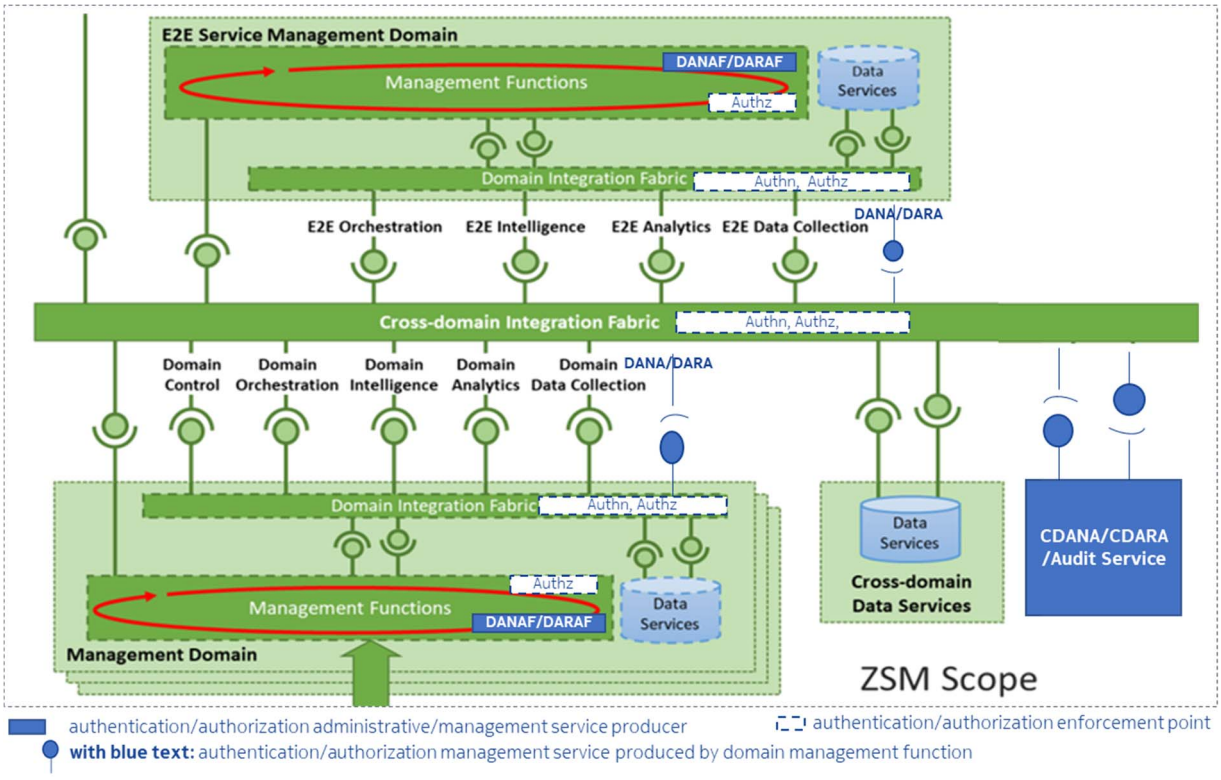

Figure 5.4.4-2

- Cross-Domain Authentication Administration (CDANA) service, cross-domain authorization administration service (CDARA) and Audit service are provided by dedicated producer like show in Figure 5.4.4-2.
- Domain Authentication Administration (DANA) service and domain authorization administration service (DARA) are provided by domain management function like show in the picture. But the box will be removed.
- Authentication enforcement (validate identity and credentials, and return token/assertion) are proceeded on integration fabric.
- Authorization enforcement (validate the token and return allowed services) is proceeded on either integration fabric (in proxy case) or management function as MnS producer (in direct access case).

5.5 Security of AI/ML-enabled services of ZSM Framework

5.5.1 Issue description

Policy and Artificial Intelligence (AI)/Machine Learning (ML) are used in the decisions and recommendations in ZSM framework. E.g. in closed-loop operation, machine learning algorithms are running to learn and recognize patterns and make predictions based on observed data.

As described in clauses 6.5.4 and 6.6.4 of ETSI GS ZSM 002 [i.15], the domain/E2E service intelligence services are responsible for driving intelligent closed-loop automation in a domain (including E2E service management domain) by supporting variable degrees of automated decision-making and human oversight with fully autonomous management being the final stage.

Decision support services enable decision making via technologies such as artificial intelligence, machine learning and knowledge management and are defined in clauses 6.5.4.2 and 6.6.4.2 of ETSI GS ZSM 002 [i.15].

From clause 6.5.3 of ETSI GS ZSM 002 [i.15], the domain analytics services provide domain-specific insights and generate domain-specific predictions based on data collected by domain data collection services and other data (e.g. data collected by other domains or provided by data services).

From clause 6.6.3 of ETSI GS ZSM 002 [i.15], the E2E service analytics services are responsible for handling E2E service impact analysis and root cause analysis and generate service-specific predictions. Also, the verification of Service Level Specifications (SLSs) and monitoring of KPIs are included in E2E service analytics.

In the last years, many companies have seen their ML systems tricked, evaded, or misled. This trend is only set to rise: According to a Gartner report 30 % of cyberattacks by 2022 will involve data poisoning, model theft, or adversarial examples. Predictably, AI/ML-enabled automation systems, such as service and network management systems based on the ZSM framework, can fail because of adversarial attacks on the ML model and data. Therefore, security threat analysis and corresponding countermeasures for AI/ML-related services/functions of the ZSM framework need to be investigated.

Many organizations of various industries study and specify security threats and related mitigation plans for AI/ML-enabled systems in general view. E.g. ISO/IEC is analysing the factors that can impact the trustworthiness of systems providing or using AI, and discussing possible approaches to mitigating AI system vulnerabilities that relate to trustworthiness (ISO/IEC TR 24028:2020 [i.12]), ETSI SAI has six studies related to AI security ontology, data supply chain security, security testing of AI, AI security problem statement (or threat analysis), AI security mitigation strategy, and the role of hardware in AI security. In addition, many traditional IT companies and academies have published research reports and solutions to address AI/ML security.

Recently, an open source project "Adversarial ML Threat Matrix" is developing to position attacks on ML systems in an Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)-style framework. The project is initiated and contributed by many AI/ML and security pioneer entities across various industries.

Basically, AI/ML security includes three main aspects:

- Using AI/ML to enhance security.
- Utilizing AI/ML systems to cause harm/malfunction.
- **Protecting AI/ML and AI/ML-enabled systems.**

This clause (clause 5.5.1) will focus on the last aspect (Protecting AI/ML and AI/ML-enabled systems) to analyse security threat and risk on AI/ML and AI/ML-enabled systems, and propose potential solutions to mitigate the risk hence protect the system.

5.5.2 Risk analysis

Many vulnerabilities are related to the use of AI/ML. These include dependency on data, opaqueness of ML models, and unpredictability. Specifically, the use of data can lead to new security threats and biased results.

Challenges related to the lack of best practices for design, development and deployment of AI-enabled systems can introduce additional or exacerbate existing vulnerabilities and threats:

- data poisoning that results in a malfunctioning AI-enabled system;
- adversarial attacks that abuse a benign AI-enabled system;
- model stealing;
- etc.

Generally, security regarding AI/ML 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.

Following the methodology described in clause 4, aforementioned ATT&CK style Adversarial ML Threat Matrix (see [i.9]) is adopted for risk analysis of AI/ML security in ZSM framework.

As the matrix aims to address common AI/ML risk in an industry-agnostic manner, only selected threats are applicable for a ZSM system as data-centric automation framework. The following table extracts threats applicable for AI/ML used in ZSM framework.

Table 5.5.2-1: Threat and risk analysis report for AI/ML related MnS of ZSM framework

Threat Id	Adversarial Tactic	Adversarial Technique	Threat Description	Impacted ZSM MnSs
AM1.1	Reconnaissance	Acquire OSINT Information	Adversaries may leverage Open Source Intelligence (OSINT), that could identify where or how machine learning is being used in a system, and help tailor an attack to make it more effective. These sources of information include technical publications, software repositories, public data repositories.	Intelligence, Data
AM1.2		ML Model Discovery	Adversaries may attempt to identify machine learning pipelines that exist on the system and gather information about them, including the software stack used to train and deploy models, training and testing data repositories, model repositories, and software repositories containing algorithms. This information can be used to identify targets for further collection, exfiltration, or disruption, or to tailor and improve attacks.	Analytics, Intelligence, Data
AM1.3		Gathering Datasets	Adversaries may collect datasets similar to those used by a particular organization or in a specific approach. Datasets may be identified when Acquiring OSINT Information. This may allow the adversary to replicate a private model's functionality, constituting Intellectual Property Theft, or enable the adversary to carry out other attacks such as an Evasion Attack.	Analytics, Intelligence, Data
AM1.4		Model Replication	An adversary may replicate a model's functionality by training a shadow model by exploiting its API, or by leveraging pre-trained weights. In Model Replication attacks, the shadow model does not have the same fidelity as that of the victim model.	Analytics, Intelligence, integration fabric
AM1.5		Model Stealing	Machine learning models' functionality can be stolen/extracted exploiting an inference API. In model extraction attacks, the attacker is able to build a shadow model whose fidelity matches that of the victim model and hence, model stealing/extraction attacks lead to Stolen Intellectual Property.	Analytics, Intelligence, integration fabric
AM2.1	Initial Access	Pre-Trained ML Model with Backdoor	Adversaries may gain initial access to a system by compromising portions of the ML supply chain. This could include GPU hardware, data and its annotations, parts of the ML software stack, or the model itself. In some instances, the attacker will need secondary access to fully carry out an attack using compromised components of the supply chain.	Analytics, Intelligence
AM2.2		Traditional Attacks	Attacker uses well established TTPs, e.g. Exploit Public-Facing Application, Valid Accounts, External Remote Services, Trusted Relationship, etc., to attain their goal.	Analytics, Intelligence, Data
AM3.1	Execution	Execute Unsafe ML Models	An Adversary may utilize unsafe ML Models that when executed have an unintended effect. The adversary can use this technique to establish persistent access to systems. These models may be introduced via a Pre-Trained Model with Backdoor. E.g. ML Models from Compromised Sources, pickle embedding in source code, etc.	Analytics, Intelligence
AM3.2		Execution via API for MLaaS	For most Machine Learning as a Service (MLaaS), the primary interaction point is via an API. So, attackers interact with the API in three ways: To build an offline copy of the model through Model Stealing or Model Replication; or to do online attacks like Model Inversion, Online Evasion, Membership inference. Execution via API is also possible for causative attacks if the adversary can taint the training data of the model via feedback loop.	Analytics, Intelligence, integration fabric
AM3.3		Traditional Attacks	Attacker uses well established TTPs, e.g. Execution via API, Traditional Software Attacks, etc., to attain their goal.	Analytics, Intelligence, Data, integration fabric
AM4.1	Persistence	Execute unsafe ML Model Execution	An Adversary may utilize unsafe ML Models that when executed have an unintended effect. The adversary can use this technique to establish persistent access to systems. These models may be introduced via a Pre-trained Model with Backdoor. An example of this technique is to use pickle embedding to introduce malicious data payloads.	Analytics, Intelligence
AM4.2		Traditional Attacks	Attacker uses well established TTPs, e.g. Account Manipulation, Implant Container Image, etc., to attain their goal.	Analytics, Intelligence, Data

Threat Id	Adversarial Tactic	Adversarial Technique	Threat Description	Impacted ZSM MnSs
AM5.1	Evasion	Evasion Attack	Unlike poisoning attacks that needs access to training data, adversaries can fool an ML classifier by simply corrupting the query to the ML model. More broadly, the adversary can create data inputs that prevent a machine learning model from positively identifying the data sample. This technique can be used to evade an ML model to correctly classify it in the downstream task. There are Offline Evasion and Online Evasion.	Analytics, Intelligence
AM5.2		Model Poisoning	Adversaries can train machine learning models that are performant, but contain backdoors that produce inference errors when presented with input containing a trigger defined by the adversary. A model with a backdoor can be introduced by an innocent user via a pre-trained model with backdoor or can be a result of Data Poisoning. This backdoored model can be exploited at inference time with an Evasion Attack.	Analytics, Intelligence
AM5.3		Data Poisoning	Adversaries may attempt to poison datasets used by a ML system by modifying the underlying data or its labels. This allows the adversary to embed vulnerabilities in ML models trained on the data that may not be easily detectable. The embedded vulnerability can be activated at a later time by providing the model with data containing the trigger. Data Poisoning can help enable attacks such as ML Model Evasion. The Poison datasets include Tainting Data from Acquisition - Label Corruption, Tainting Data from Open Source Supply Chains, Tainting Data from Acquisition - Chaff Data, Tainting Data in Training - Label Corruption.	Analytics, Intelligence, Data
AM6.1	Exfiltration	Exfiltrate Training Data	Adversaries may exfiltrate private information related to machine learning models via their inference APIs. Additionally, adversaries can use these APIs to create copy-cat or proxy models. Membership Inference Attack and ML Model Inversion would be applied for Exfiltration.	Analytics, Intelligence, integration fabric
AM6.2		ML Model Stealing	Machine learning models' functionality can be stolen/extracted exploiting an inference API. In model extraction attacks, the attacker is able to build a shadow model whose fidelity matches that of the victim model and hence, model stealing/extraction attacks lead to Stolen Intellectual Property.	Analytics, Intelligence, integration fabric
AM6.3		Traditional Attacks	Attacker uses well established TTPs, e.g. Insecure Storage, etc., to attain their goal.	Analytics, Intelligence, Data
AM7.1	Impact	Defacement	Adversaries can create data inputs that can be used to subvert the system for fun. This can be achieved corrupting the training data via poisoning as in the case of defacement of Tay Bot, Evasion or exploiting open CVEs in ML dev packages.	Analytics, Intelligence
AM7.2		Denial of Service	Adversaries may target different Machine Learning services to conduct a DoS.	Analytics, Intelligence
AM7.3		Traditional Attacks	Attacker uses well established TTPs, e.g. Stolen Intellectual Property, Data Encrypted for Impact (e.g. ransomware), Stop System Shutdown/Reboot, etc., to attain their goal.	Analytics, Intelligence, Data

5.5.3 Potential measures

ETSI SAI is framing the security concerns arising from AI, several studies are developing in SAI including AI security problem statement and mitigation strategy. Referring to SAI studies for potential measures for the threats analysed in clause 5.5.2, the table below lists gaps that the threats have not been addressed in SAI. Further investigate in ZSM or cooperate with SAI (e.g. send LS to SAI for potential solution) to fill the gaps (either the threats/risks have not been addressed in SA1, or SA1 solution cannot fully mitigate the risks) will be performed as next step.

Table 5.5.3-1: Mapping risks of AI/ML in ZSM to risks and mitigation plans of SAI

Threat Id	Adversarial Tactic	Adversarial Technique	Map to SAI problem (ETSI GR SAI 004 (see [i.10])	Map to SAI mitigation plan (ETSI GR SAI 005 (see [i.11])
AM1.1	Reconnaissance	Acquire OSINT Information		
AM1.2		ML Model Discovery		
AM1.3		Gathering Datasets		
AM1.4		Model Replication		
AM1.5		Model Stealing	Reverse Engineering (6.4)	Mitigating Model Stealing (6.3)
AM2.1	Initial Access	Pre-Trained ML Model with Backdoor	Backdoor Attacks (6.3)	Mitigating Backdoor Attacks (5.3)
AM2.2				
AM3.1	Execution	Execute Unsafe ML Models	(Model) Poisoning (6.1), Backdoor Attacks (6.3)	Mitigating Poisoning Attacks (5.2), Mitigating Backdoor Attacks (5.3)
AM3.2		Execution via API for MLaaS	Input attack and evasion (6.2)	Mitigating Evasion Attacks (6.2)
AM3.3		Traditional Attacks		
AM4.1	Persistence	Execute unsafe ML Model Execution	(Model) Poisoning (6.1), Backdoor Attacks (6.3)	Mitigating Poisoning Attacks (5.2), Mitigating Backdoor Attacks (5.3)
AM4.2		Traditional Attacks		
AM5.1	Evasion	Evasion Attack	Input attack and evasion (6.2)	Mitigating Evasion Attacks (6.2)
AM5.2		Model Poisoning	(Model) Poisoning (6.1), Backdoor Attacks (6.3)	Mitigating Poisoning Attacks (5.2), Mitigating Backdoor Attacks (5.3)
AM5.3		Data Poisoning	(Data) Poisoning (6.1)	Mitigating Poisoning Attacks (5.2),
AM6.1	Exfiltration	Exfiltrate Training Data	Deployment and Inference (4.3.8)	Mitigating Data Extraction (6.4)
AM6.2		ML Model Stealing	Reverse Engineering (6.4)	Mitigating Model Stealing (6.3)
AM6.3		Traditional Attacks		
AM7.1	Impact	Defacement	(Data) Poisoning (6.1), Input attack and evasion (6.2)	Mitigating Poisoning Attacks (5.2),
AM7.2		Denial of Service	Poisoning (6.1), Input attack and evasion (6.2)	Mitigating Poisoning Attacks (5.2), Mitigating Evasion Attacks (6.2)
AM7.3		Traditional Attacks		

6 Conclusion

6.1 Potential security capabilities

6.1.1 Potential security capabilities of closed-loops solution

[Sec-Cla-01] Capabilities of ZSM framework to automatically detect and identify security incidents of ZSM framework closed-loops.

[Sec-Cla-02] Capabilities of ZSM framework to notify security incidents of ZSM framework closed-loops to authorized consumers of these closed-loops.

[Sec-Cla-03] Capabilities of ZSM framework to automatically react to security incidents of ZSM framework closed-loops.

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

[Sec-Cla-04] Capabilities of ZSM framework to automatically react to security incidents between related ZSM framework closed-loops.

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

[Sec-Cla-05] Capabilities of ZSM framework to authorize an authenticated ZSM framework consumer.

[Sec-Cla-06] Capabilities of ZSM framework closed-loops to ensure privacy of the data when these closed loops deal with personal data.

[Sec-Cla-07] Capabilities of ZSM framework closed-loops to ensure the data security when these 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-08] Capabilities of ZSM framework closed-loops to ensure integrity of management data when these closed loops deal with such data.

[Sec-Cla-09] Capabilities of ZSM framework closed-loops to ensure confidentiality of management data when these closed loops deal with such data.

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

[Sec-Cla-10] Capabilities of ZSM framework to trace back AI/ML based decisions of a ZSM framework to support security audits.

[Sec-Cla-11] Capabilities of ZSM framework to notify security issues and anomalies of a ZSM framework to support security monitoring.

[Sec-Cla-12] Capabilities of ZSM framework to provide security predictions based on automatic proactive security assessments.

[Sec-Cla-13] Capabilities of ZSM framework to ensure security of management functions and management services before deploying them in the ZSM framework, and to continue the monitoring of the security state of the management functions and management services after their deployment and during their runtime to react on compromising of management functions and management services on the ZSM framework.

[Sec-Cla-14] Capabilities of ZSM framework closed loops to identify vulnerabilities of closed loop's components.

[Sec-Cla-15] Capabilities of ZSM framework closed loops to provide recommendations for mitigation of security risks caused by vulnerabilities of closed loop's components.

[Sec-Cla-16] Capabilities of ZSM framework closed loops to ensure integrity and confidentiality of a closed loop notification.

[Sec-Cla-17] Capabilities of ZSM framework closed loops to enforce access control.

[Sec-Cla-18] Capabilities of ZSM framework to automatically detect and identify deceit or spoofing attacks regarding an intent in a declarative form which is used as input for ZSM framework closed-loops.

[Sec-Cla-19] Capabilities of ZSM framework to automatically mitigate security incidents.

6.2 Next steps of standardization activities for ZSM security

6.2.1 Summary of the study report

The present document did overall security threat and risk analysis for ZSM framework, listed key issues/risks of the framework based on use cases, proposed solutions to mitigate the risks, and raised potential requirements on ZSM framework to support the security capabilities.

6.2.2 Potential normative content of security aspects based on the study

Several key issues are studied in the present document and potential solutions and security capability requirements were discussed. Potential normative content based on the study are listed below:

- As E2E service automation framework, trust between multiple domains is key security issue needed to be addressed for inter-operation. As overall coordination SDO, ZSM would be a right organization to specify the capability and potential interface to support trust relationship building especially across management domains.
- User management and access control is essential to interaction or exchange information between entities of different domains based on level of trust, therefore need to be standardized as well. However, the access control solution could be specified in each domain according to technology used in the domain.
- The potential capability to support security assurance of management function could be specified to secure Continuous Integration/Delivery (CI/CD) pipeline of ZSM management service/function, and enable security assurance process automation during MnS/MnF lifecycle. 3GPP SCAS could be referred for basic methodology but automation on security process would be specifically considered in ZSM.
- To assure security of AI/ML enabled automation system provided by ZSM framework, ZSM framework would provide capability to mitigate AI/ML related security risk. Besides referring to measures proposed by ETSI SAI, ZSM may specially focus on security of data centric AI for network/service automation, especially for closed-loop automation as one of AI enabler.

All aspects mentioned above could be candidate of normative contents of security aspects for ZSM framework and solutions in next step.

6.2.3 How to handle potential requirements in study

Potential security capabilities were identified in clauses 5.1.2, 5.2.3 5.3.2, 5.4.3, 5.5.3 and 6.1.1 of the present document based on use case and analysis, best practice, industry standardization or regulations. These potential capability requirements will be revisited and evaluated during normative phase, and may be refined and merged into ETSI GS ZSM 001 [i.18] and ETSI GS ZSM 002 [i.15] or new security specification if they are identified as real security requirements, or removed if they are duplicated or invalid according to assessment.

6.2.4 Place and structure of documenting security solutions and services

A dedicated security specification is proposed to describe security solutions (studied in the present document) for ZSM framework, finally the content could be distributed to ETSI GS ZSM 002 [i.15] or other ZSM solution or governance related specifications. E.g. security requirements could be added to ETSI GS ZSM 001 [i.18], ETSI GS ZSM 002 [i.15], new capabilities or MnS of ZSM framework could be added to ETSI GS ZSM 002 [i.15], etc.

Annex A:
Change History

Date	Version	Information about changes
October 2019	0.0.1	Initial Draft: agreement on the skeleton and initial content
January 2020	0.0.2	Update according to CRs agreed in ZSM009 F2F meeting ZSM(19)000501r5, ZSM(19)000503r4, ZSM(19)000603r3, ZSM(19)000640r3
February 2020	0.0.3	Update according to CRs agreed in ZSM009 conference calls ZSM(20)000016r3, ZSM(20)000022r2
March 2020	0.0.4	Update according to CRs agreed in ZSM010 F2F meeting ZSM(20)000028r1, ZSM(20)000029r2, ZSM(20)000059r1, ZSM(19)000522r4, ZSM(19)000650r3 Move two Notes to common part of clause 4.2.2 as they are duplicated in all clauses
May 2020	0.0.5	Update according to CRs agreed in ZSM#6 online meeting and other tech calls ZSM(20)000045r2, ZSM(20)000048r2, ZSM(20)000051r2, ZSM(20)000050r2, ZSM(20)000060r7, ZSM(20)000107
June 2020	0.0.6	Update according to contribution agreed in ZSM#11 online meeting ZSM(20)000165r1
August 2020	0.0.7	Update according to contribution agreed in ZSM#11 tech calls ZSM(20)000276r1
December 2020	0.0.8	Update according to contribution agreed in ZSM#12e and ZSM#13e ZSM(20)000337r1, ZSM(20)000338r1, ZSM(20)000449r3, ZSM(20)000450r2, ZSM(20)000459r1
January 2021	0.0.9	Update according to contribution agreed in ZSM#13e ZSM(20)000460r1, ZSM(20)000505, ZSM(20)000506r1
May 2021	0.0.10	Update according to contribution agreed in ZSM#14e ZSM(21)000094r2_ZSM010_draft_cleanup_untechnical_fixing ZSM(21)000097r2_ZSM010_draft_cleanup_solve_editor_notes_in_5_1 ZSM(21)000138_ZSM010_draft_cleanup_solve_editor_notes_in_7_1 ZSM(21)000098r2_ZSM010_draft_cleanup_solve_editor_notes_in_5_2
June 2021	0.0.11	ZSM(21)000204r1_fix_editorial_issue_of_ZSM010_draft

History

Document history		
V1.1.1	July 2021	Publication