The Standards People

ETSI ZSM and Autonomous Networks

Presented by: **ETSI ISG ZSM Officials**   For: **OCG Ad-hoc meeting AN#1**

November 11, 2020

Our mission – technical perspective

As documented in the ZSM ToR:

"…The "Industry Specification Group Zero touch network and Service Management" (ISG ZSM) is working on the definition of a new, future-proof, horizontal and vertical end-to-end operable framework and solutions to enable agile, efficient and qualitative management and automation of emerging and future networks and services…The goal is to have all operational processes and tasks (e.g., delivery, deployment, configuration, assurance, and optimization) executed automatically, ideally with 100% automation…."

Our working principles

As documented in the ZSM ToR:

"…The ISG intends to analyse existing specifications and solutions (both ETSI and external ones) and where appropriate leverage them to avoid duplication and maximize synergies…

…The ISG will work to strengthen the collaboration… in order to promote the adoption of and alignment with the ZSM architecture and solutions to ensure automated end-to-end network and service management can be achieved…"

# Our role – collaboration with relevant SDOs, open-source projects and Fora perspective

As documented in the ZSM ToR:

"…The ISG ZSM aims to act as a central point for end-to-end network and service automation and facilitate the coordination and cooperation between relevant standardization bodies and open source projects. The unique value of ISG ZSM will be in providing guidance to the implementation of management interfaces as well as coordinating and giving directions to achieve automated end-to-end network and service management solutions and architecture."

Coordination between key (ETSI and external) standardization groups and open-source projects is KEY; in accordance with its mission, ZSM has a central role in facilitating the coordination and providing guidance.

ZSM (horizontal & vertical end-to-end) framework (ZSM 002)
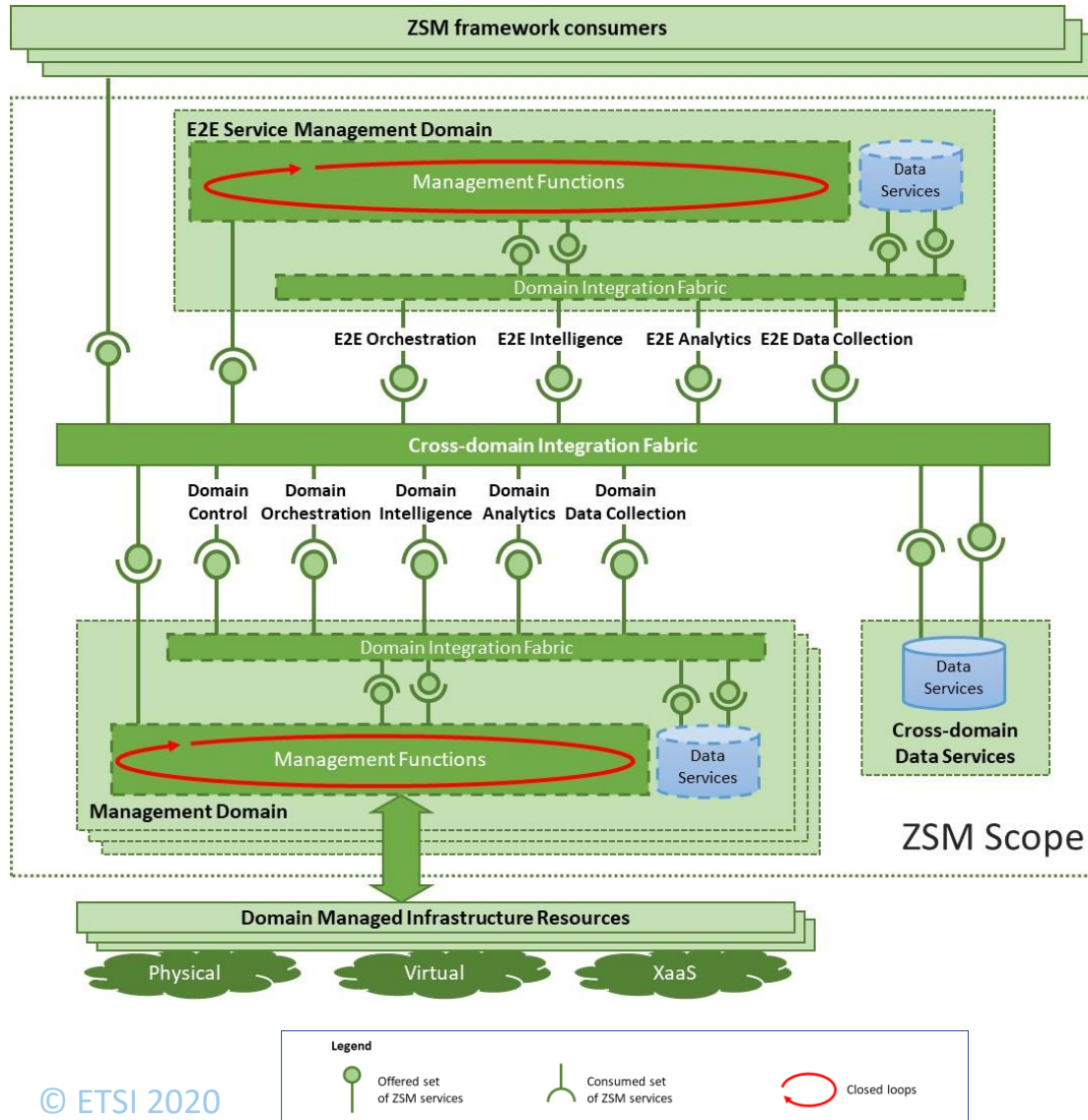
Designed for closed-loop automation and optimized for data-driven machine learning and artificial intelligence algorithms

Architectural principles:

- Modular, flexible, scalable and extensible service-based architecture

- Separation of concerns: network domain management and end-to-end cross-domain service management; resources in multiple domains can be managed separately.

- Support of model-driven, open interfaces

- Enablement of adaptive closed-loop management automation, where the automated decision-making mechanisms can be bounded by rules and policies

- Support of data services and stateless management functions

- Intent-based interfaces

- Design for resilience

- Functional abstraction

5

ZSM end-to-end cross-domain service orchestration and automation (ZSM 008)

Fulfilment and assurance processes and services:

"The work item will investigate the automation functions of managing end to end services across management domains (MDs). It will specify communication patterns and information flows used in interactions between service producer and service consumer as well as the functional requirements, interfaces and operations in support of automated cross-domain lifecycle management in the ZSM framework.

E2E service lifecycle related management processes
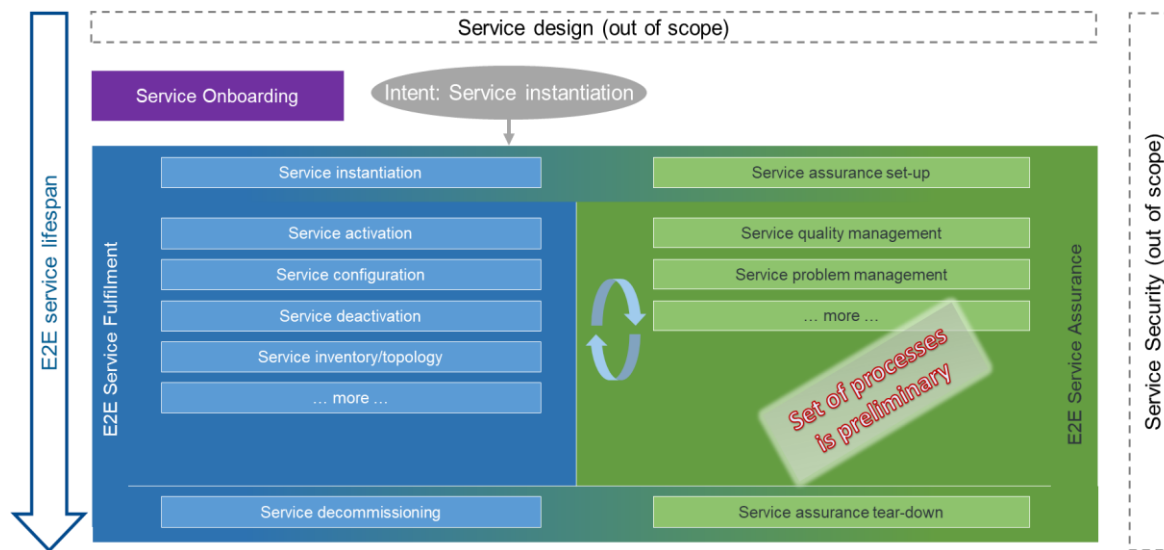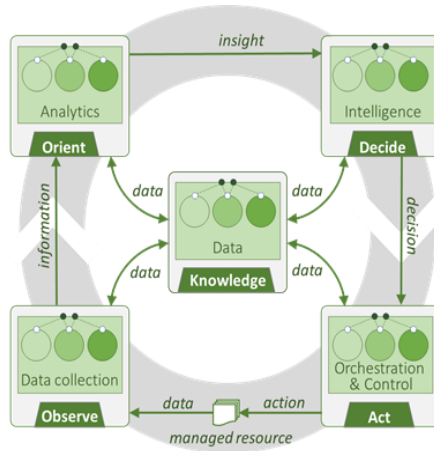

Domain NBIs supporting the E2E service lifecycle management
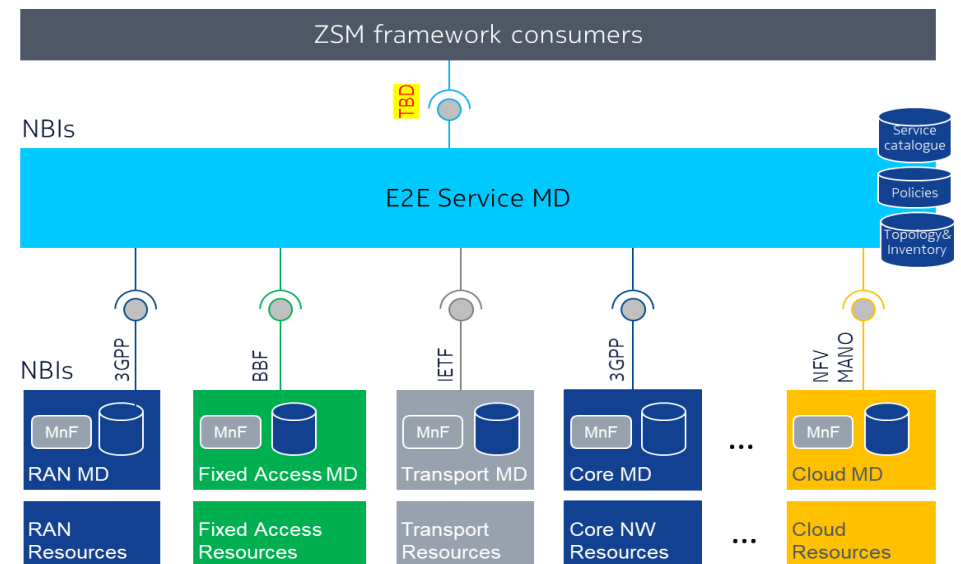
Closed-loop automation in the ZSM framework (ZSM 009 series)

Analytics
Provide insights based on collected data

Intelligence
Provide specific decisions and recommendations

Data collection
Monitor the managed entities and provide live performance and fault data

Orchestration
Automate workflows to handle lifecycle management of the managed entities

Closed loop

Deployment view

- ZSM provides capabilities to manage the closed-loop models and lifecycle
- Closed-loop operation can happen at the management domain level, the end-to-end service management domain level and can span across multiple management domains; multiple closed loops can run simultaneously.
- ZSM provides means of coordination/delegation/escalation between closed loops as well as the ways in which their behavior can be steered
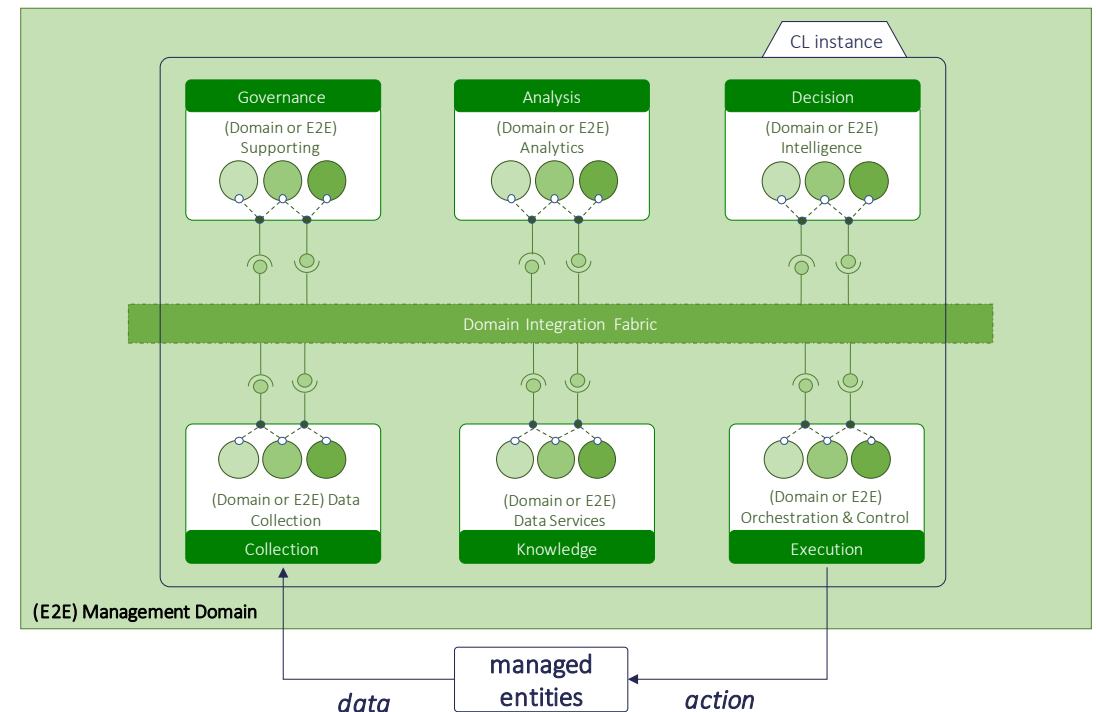
ZSM end-to-end, intent-driven closed loop automation (ZSM 009 series)
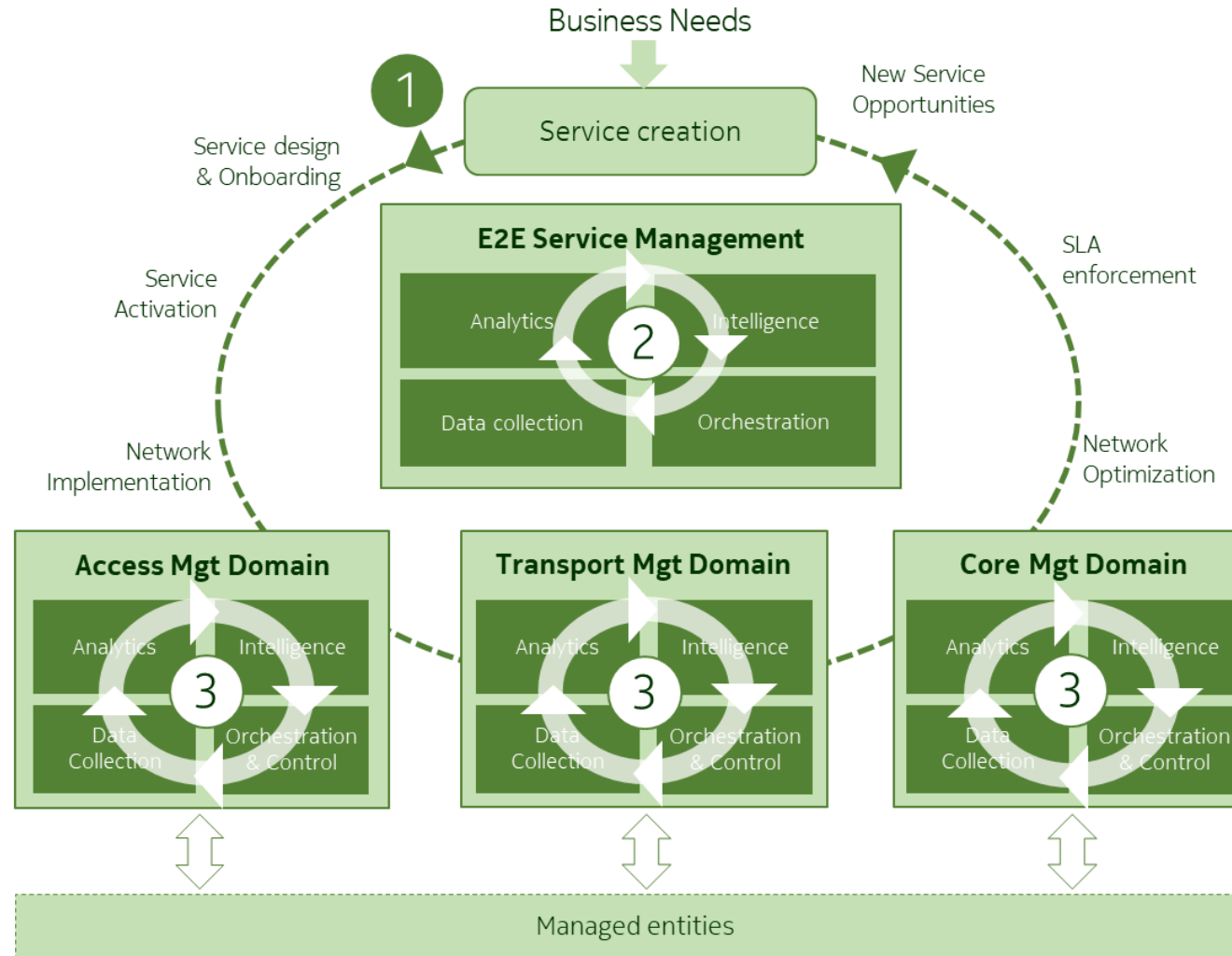
ZSM Security Aspects Study Item (ZSM 010)

Rationale

- Threat surface is extensive in the ZSM environment because of the openness of ZSM framework and the nature of emerging technologies (e.g. AI/ML, data lake, cloud native applications)
- Compromising a ZSM system security may adversely impact the business of operator and/or vertical service provider.
- Compliancy with country/region/industry security laws and regulations is an obligation for service providers and their suppliers.

Security threat and risk analysis regarding the ZSM framework, introducing:

- A methodology for ZSM threat and risk analysis
- Threat and risk analysis report, covering aspects related to the E2E service management domain, management functions and services

Countermeasures and proposed requirements to address the high-priority security risks/issues in the ZSM framework, in relation to:

- Trust relationship between multiple management domains
- Security Assurance of management functions
- Multi-tenancy of the ZSM Framework
- Access Control for management services provided by the ZSM Framework
- Security of AI/ML-enabled services provided by ZSM Framework

Outlook

- As a continuous step of the study item, a dedicated security specification is expected to capture security requirements proposed in this report and describe security solutions for ZSM framework including AI/ML-enabled services

Epilogue

The ultimate target is to enable largely autonomous network operation driven by high-level policies; such autonomous will be capable of self-management (configuration, healing, optimization) without human intervention beyond the transmission of intents.

The ZSM framework

- is versatile and built on service-based principles offering scalability, modularity, extensibility and flexibility

- supports the transfer of autonomy from the operator to the network using intent-based interfaces

- integrates capabilities and re-usable patterns for closed-loop operation and coordination, in support to the zero-touch operational goal, driving the development of autonomic functionalities

- provides means to integrate AI-based functionalities in support to higher level of automation, leading to operational autonomy

Most importantly, ZSM provides an open framework and proposes to use it as the foundation over which to build a powerful and comprehensive autonomous network framework.

We propose that ZSM acts as the ETSI central point for coordination with key (ETSI and external) SDOs and open source projects regarding Autonomous Networks.

Thank you!

© ETSI 2020