The Standards People

ETSI Zero touch network and Service Management (ZSM)

Enabling agile service delivery and new business opportunities

Presented by: **Klaus Martiny**
ETSI ISG ZSM Chair

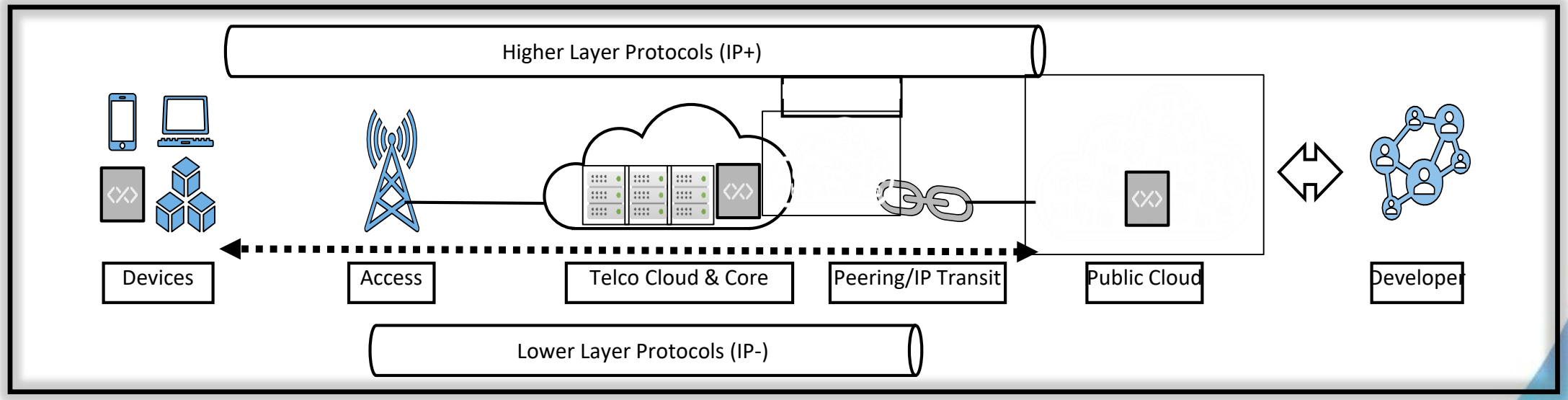
For: **Analyst Summit 21.05.2020**

19.05.2020

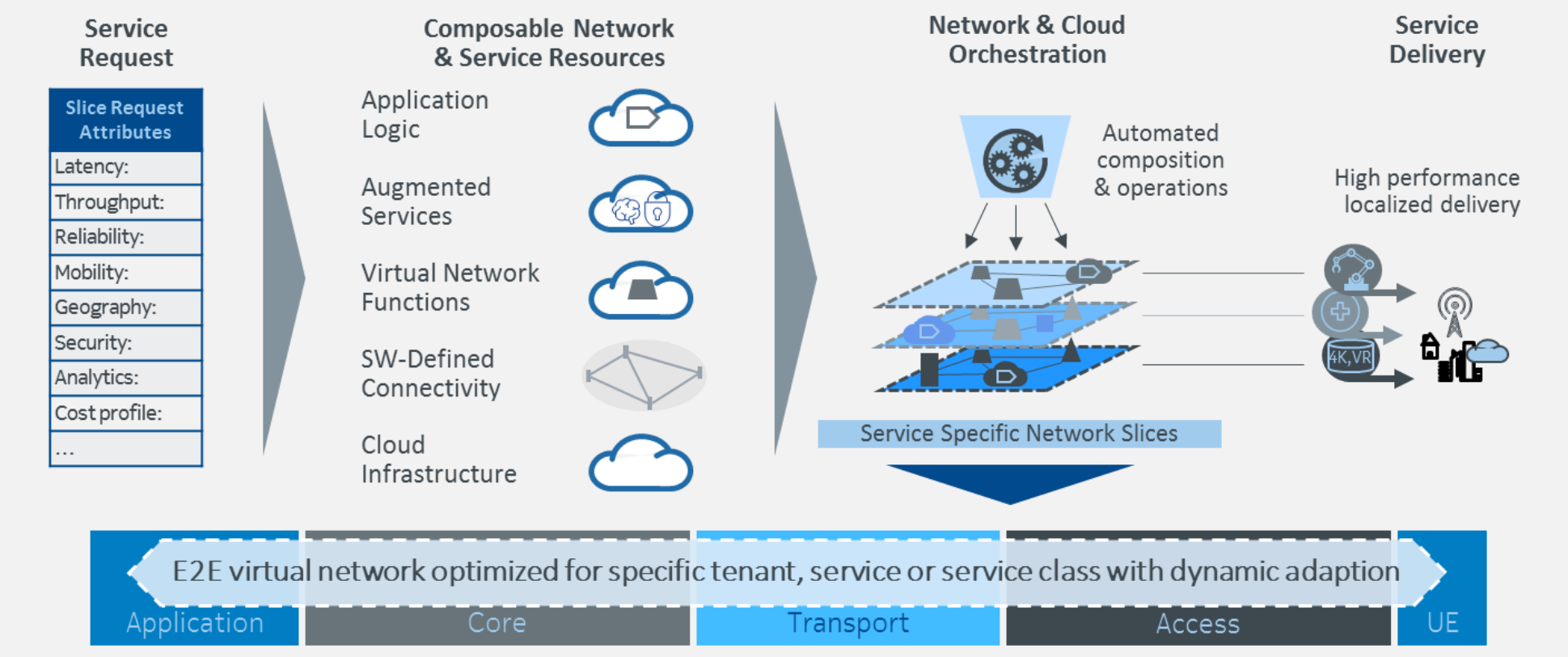
Zero-touch network and service management
Trends and market drivers

- Rapid business digitization and automation of all major industries, supporting a similar level of business agility and flexibility
- Increase in overall complexity created by the transformation of the networks into programmable, software-driven and service-based architecture
- New business models and value creation opportunities enabled by technology breakthroughs such as Network Slicing, imposing unprecedented operational agility and higher cooperation across network domains

Network Complextity



Network Slicing - the foundation for future value create How do we want to manage this?



- ★ > 10,000s slices
- ★ > 100,000s Network Functions
- ★ Hybrid
- ★ Versions
- ★ Heterogenous
- ★ Multi-domain
- ★ Wafting at edges

Source: Nokia

The disruptive deployment of 5G triggers the need for a radical change in the way networks and services are managed and orchestrated; full end-to-end automation of network and service management becomes an urgent necessity.

Commercial Impact

- Automation is key to enable Telcos, Operator to increase the capability to manage Services and the Network
- More the only Network & Service Management
  - Service deployment
  - Service introduction
  - Network Monitoring
  - Fault management
  - etc.
- End to End

Current state of the industry

Currently there are multiple inconsistent management frameworks in the industry, many silos, a lack of alignment and a lack of interoperability.

It is essential to move to an environment that leverages synergies and achieves alignment through convergence on a single end-to-end network and service management architecture.

ETSI ISG ZSM
Formed in December 2017; first meeting in January 2018

14 founding members

Key objective

Enable future operational processes and tasks to be executed automatically, end-to-end

Goal

Accelerate the definition of the end-to-end service management architecture, spanning both legacy and virtualized network infrastructures

Formed under the auspices of the ETSI ISG

Industry convergence

Facilitate collaboration with the relevant open-source projects, standardization bodies and fora

Interoperability

Provide a common foundation to enable a diverse ecosystem of open source groups to produce interoperable solutions

The ISG ZSM continues growing in a steady and healthy pace

69 members; 19 operators

Working principles

- Existing specifications and solutions (both ETSI and external ones) will be analysed and where appropriate leveraged to avoid duplication and maximize synergies.
- Input from implementations and Proof of Concepts (PoCs) will be used to validate the draft specifications.
- All deliverables are openly published.

Landscape (ZSM 004)

Scope: a landscape report for Zero-Touch Network and Service Management (ZSM), introducing information about activities in other bodies (such as Standards Developing Organizations, Open Source Communities, and Industry Associations) that are relevant to the work in ISG ZSM.

Already established Collaboration links:

Standardization organizations:

- ETSI NFV
- 3GPP SA 5
- GSMA
- a.o.

Open Source Projects:

- ONAP
- OSM
- a.o.

ZSM work program

Work item number	Title	Rapporteur	Status
ZSM 001	Requirements based on documented scenarios (specification)	Michael Klotz (DT)	Published
ZSM 002	Reference Architecture (specification)	Uwe Rauschenbach (Nokia)	Published
ZSM 003	End-to-end management and orchestration of network slicing (specification)	Zou Lan (Huawei)	In-progress
ZSM 004	ZSM landscape (report)	Wu Jinhua (ZTE)	Published
ZSM 005	Means for automation (report)	Andreas Krichel (HPE)	Approved
ZSM 006	Proof of Concept framework (specification)	Klaus Martiny (DT)	Published
ZSM 007	Terminology (specification)	Magnus Buhrgard (Ericsson)	Published
ZSM 008	End-to-end cross-domain service orchestration and automation (specification)	Uwe Rauschenbach (Nokia)	In-progress
ZSM 009-1	Closed-loop automation: enablers (specification)	Pedro Henrique (Ericsson)	In-progress
ZSM 009-2	Closed-loop automation: solutions (specification)	Ishan Vaishnavi (Huawei)	In-progress
ZSM 009-3	Closed-loop automation: advanced topics (report)	Laurent Ciavaglia (Nokia)	In-progress
ZSM 010	General security aspects (report)	Jing Ping (Nokia)	In-progress

ZSM Scenarios and Key Requirements (ZSM 001)

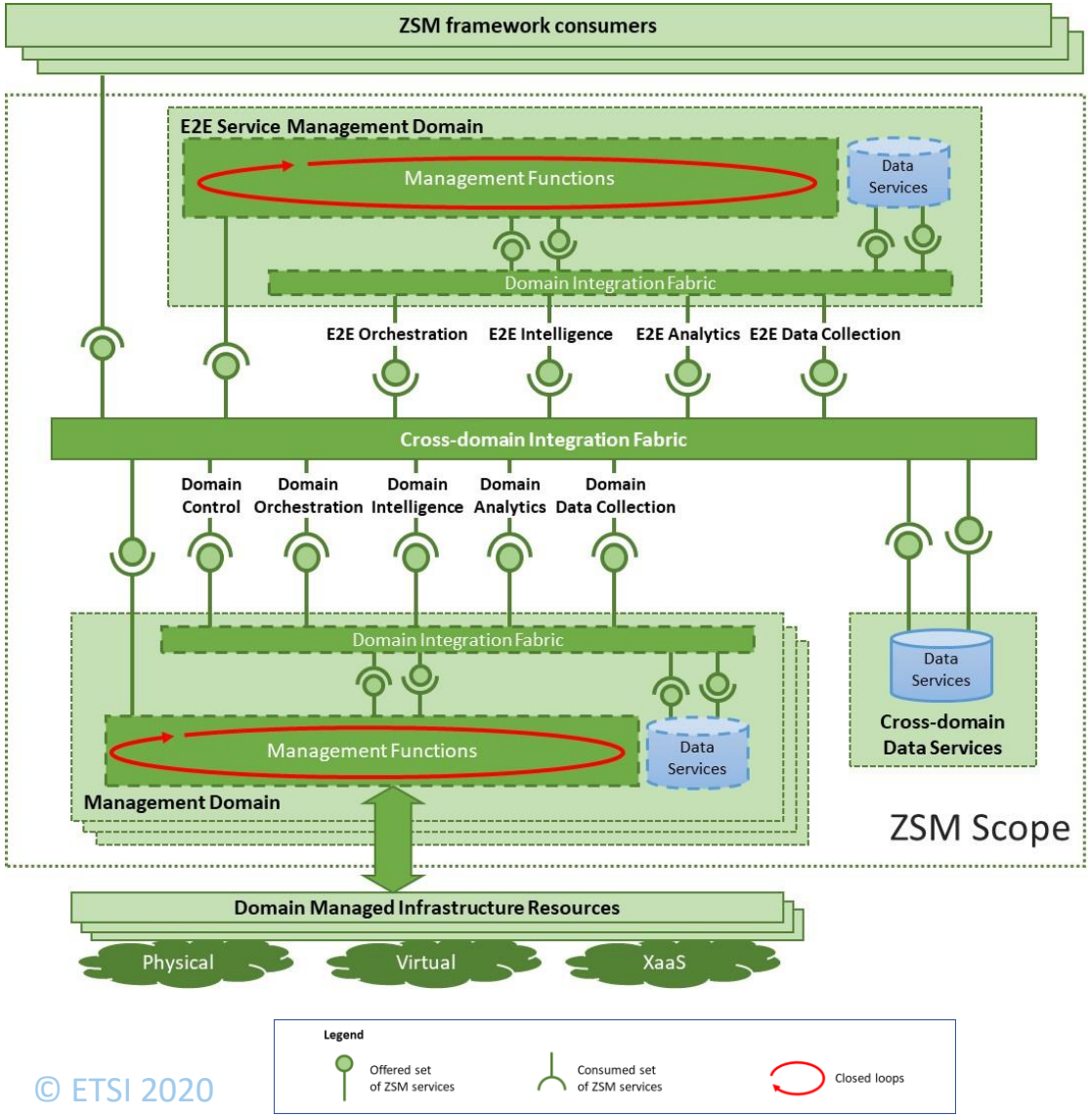
- 39 scenarios are used to identify business-oriented and automation-related challenges faced by operators and vertical industries.

  The scenarios are categorized into the following groups:

  - Automation of end-to-end network and service management
  - End-to-end automation of 5G network slice management
  - Analytics and Machine Learning
  - Automated Testing
  - NaaS lifecycle and exposure with slicing
  - Collaborative/Federated Service Management
  - Security
  - Integration/Interoperation

- Scenarios analysis derives architectural, functional and operational requirements

ZSM architecture framework (ZSM 002)



Designed for closed-loop automation and optimized for data-driven machine learning and artificial intelligence algorithms

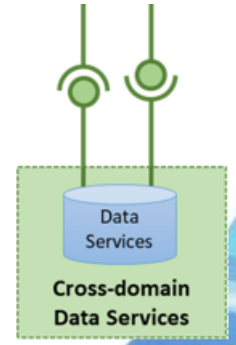
Architectural principles:

- Modular, flexible, scalable and extensible service-based architecture
- Separation of concerns: network domain management and end-to-end cross-domain service management, where each domain addresses its own sphere of expertise
- Support of model-driven, open interfaces
- Support of intent-based interfaces
- Enablement of adaptive closed-loop management automation, where the automated decision-making mechanisms can be bounded by rules and policies
- Support of stateless management functions
- Design for resilience
- Functional abstraction

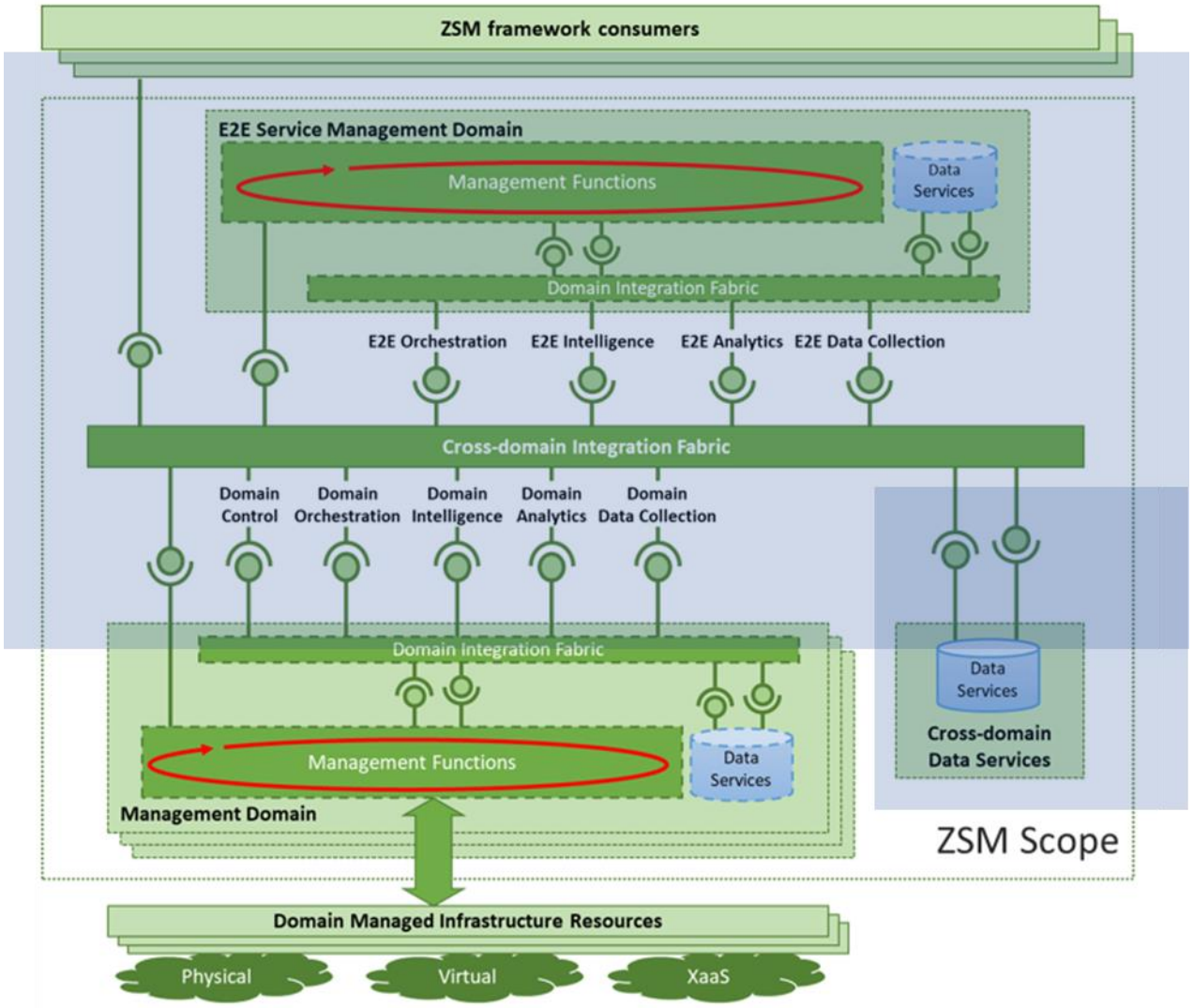
ZSM architecture framework (ZSM 002)
Data services

Efficient access to data is **key** for analytics and machine intelligence!

- Data services allow data to be stored separately from the application.
  - Data may include: performance monitoring data, assurance data, trace data, configuration data, miscellaneous log data, topology data, inventory data
- Data services support big data analysis
- Data services provide rapid access to support closed-loop automation
- Data governance is used to enforce access restrictions to data



ZSM Security Aspects Study Item (ZSM 010)



Problem Statement

- Threat surface is extensive in the ZSM environment because of the openness of ZSM framework and the nature of emerging technologies
- 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.

Scope of ZSM Security

Threat & risk analysis as well as baseline security control proposal for:

- E2E Service Management Domain
- Cross-domain Integration Fabric
- Cross-domain Data Service

Objective

- Identify security threats and propose considerations to be handled by the ZSM work
- Share best practice countermeasures related to identified security threats
- Provide recommendations and guidance for further ZSM standardization activities regarding security aspects

Essential task to do

Important for the entire Telco Industry

Thank you

Contact Details

Presenter: Klaus Martiny

Klaus.martiny@telekom.de

ETSI ZSM Support:

zsmsupport@etsi.org

Thank you!