ISG ZSM PoC Proposal

1 PoC Project Details

1.1 PoC Project

PoC Number: *(assigned by ETSI)*	
PoC Project Name:	Security SLA assurance in 5G network slices
PoC Project Host:	Telefónica
Short Description:	This PoC aims at showcasing a security closed loop across multiple domains and sites interconnected using a security framework based on ZSM Reference Architecture (ZSM 002) and a E2E slice orchestration solution based on the principles of ZSM 003. To that end, the demo showcases the request and implementation for two network slices with specific security demands expressed as Security Service Level Agreements (SSLAs) between a 5G network slice Broker and a 5G operator. The PoC will also implement a close-loop automation to ensure the SSLAs compliance, in case of security breaches. Two different network slices will be deployed and monitored, one related to provide a secure slice connectivity between and access and a 5G Core network domains and second one for IoT related services. The solution is based on the technology developed in INSPIRE-5Gplus EU funded project [1]. This project has taken the ZSM reference architecture as the baseline to create a solution to address security demands and develop several security enablers and will demonstrate how they can be integrated to address security problems.

1.2 PoC Team Members

	Organisation name	ISG ZSM participant (yes/no)	Contact (Email)	PoC Point of Contact (*)	Role (**)	PoC Components
1	Telefonica	Yes	**Antonio Pastor** antonio.pastorperales@telefonica.com **Diego R. López** diego.r.lopez@telefonica.com	X	Network/ service provider	- Use case specification - PoC architecture - Setup Telefonica Lab - Security Agents and MANO components
2	Universidad de Murcia	No	Alejandro Molina alejandro.mzarca@um.es Antonio Skarmeta skarmeta@um.es		Other (University, test labs & integrator)	- Use case specification - Setup UMU Lab - integrator
3	Montimage	No	Edgardo Montes de Oca edgardo.montesdeoca@montimage.com		Supplier	- INSPIRE5G-plus components
4	CTTC	No	Pol Alemany pol.alemany@cttc.cat Charalampos Kalalas ckalalas@cttc.es Raul Muñoz raul.munoz@cttc.es		Other (research centers, test labs & integrator)	- Use case specification - Setup CTTC Lab - PoC integrator
5	THALES	No	Dhouha Ayed dhouha.ayed@thalesgroup.com		Supplier	- Use case specification - INSPIRE5G-plus components
6	EURESCOM	No	Uwe Herzog herzog@eurescom.eu		Other (test labs, research center)	-INSPIRE5G-plus components - Setup EURESCOM Lab
(*) Identify the PoC Point of Contact with an X. (**) The Role will be network/service provider, supplier, or other (universities, research centers, test labs, Open Source projects, integrators, etc…).						

All the PoC Team members listed above declare that the information in this proposal is conformant to their plans at this date and commit to inform ETSI timely in case of changes in the PoC Team, scope or timeline.

1.3 PoC Project Scope

1.3.1 PoC Topics

PoC Topics identified in this clause need to be taken for the PoC Topic List identified by ISG ZSM and publicly available in the ZSM WIKI. PoC Teams addressing these topics commit to submit the expected contributions in a timely manner.

PoC Topic Code	PoC Topic Description	Related WI	Expected Contribution	Target Date
3	Intent-driven Closed-Loop automation	ZSM 002, ZSM 011	– Insights from a closed-loop scenario for automation of E2E security service aligned with ZSM 002 reference	Sep 2022

			− Demonstrate an Intent based security policies engine for conflict analysis, and translation	
4	Cross-domain user-driven E2E services	ZSM 008, ZSM 014	− Implement a secure E2E cross-domain management for several domains related to 5G connectivity and verticals using ZSM 008 processes concepts − Link security and trust concepts with SLAs and E2E service management − Architecture for security aspects on ZSM 014	Nov 2022

1.3.2 Other topics in scope

List here any additional topic for which the PoC plans to provide input/feedback to the ISG ZSM.

PoC Topic Code	PoC Topic Description	Related WG/WI	Expected Contribution	Target Date
A				
B				
<…>				

1.4 PoC Project Milestones

PoC Milestone	Milestone description	Target Date	Additional Info
P.S	PoC Project Start	May 2022	Presentation on ZSM #19
P.P	PoC proposal submission	May 2022	Submission for approval
P.PU	PoC Proposal Announce	June 2022*	Public Web announce in INSPIRE-5Gplus media (web, twitter, etc.), *Once it is approved
P.S	PoC user story detailed	July 2022	Defining and detailing the use case
P.M.1	Initial ZSM compatible infrastructure and components available	July 2022	Management Domains interconnections and INSPIRE-5Gplus components delivered.
P.M.2	Testing phase and executions	Aug 2022	Integration, testing and validations of expected functionalities.
P.D1	PoC public Demo	Sep 2022*	ETSI Security Week*/ OSM Ecosystem Day*/ *date is pending
P.C1	PoC Expected Contributions and lesson learnt	Oct 2022	Feedback and insight, identification, and contributions roadmap in open ZSM WI
P.R	PoC Report	Nov 2022	PoC-Project-End Feedback with final presentation.
P.E	PoC Project End	Nov 2022	

NOTE: Milestones need to be entered in chronological order.

1.5 Additional Details

Demos events and dates are indicative, and still in discussion within EU H2020 INSPIRE-5Gplus consortium.

H2020 INSPIRE-5Gplus has already committed with ZSM principles and frameworks. Several details on architecture and implementation are available in the project web portal [1].

.

2 PoC Technical Details

2.1 PoC Overview

This PoC demonstrates a security oriented closed loop as well as the instantiation of a High-Level Architecture (HLA) based on ZSM reference architecture, across multiple domains and sites interconnected through an Integration Fabric. To that end, the PoC can be summarized as the request and realization of a network slices with specific Security Service Level Agreements (SSLAs) from a 5G network slice Broker consumer and a 5G operator. The PoC demonstration will be evaluated over the novel HLA solution designed in INSPIRE-5Gplus project.

The use case story will provide a 5G service protection scenario facing different type of customers' needs over a common framework. In the use case, a common E2E management domain will interact with customer demand to deploy a specific security requirement.

A specific SSLA will be requested to assure the protection of the communication between the User Equipment (UE) access domain and a 5G service cloud domain distributed in different and separated Security Management Domains (SMDs) (e.g. through a backhaul connectivity), as well as other security requirements to avoid security issues (e.g., DDoS protection). The enforcement of this SSLA will involve different domains to deploy a 5G network slice composed by the service itself as well as the security elements (i.e., channel protection IPsec proxies and different assets monitoring) to ensure the SSLA compliance for any traffic.

Other example will be an IoT protection where another SSLA will be established with focus on securing sensor data exchange between IoT sensors in remote sites and a global IoT supervision centre - interconnected via a dedicated 5G network slice - by requesting different types of channel protection between IoT devices and the supervision centre's IoT broker, using DTLS proxies. The enforcement of this network slice SSLA will also be monitored with deployed security agents which ensure the SSLA compliance.

2.2 PoC Architecture

Include a diagram outlining how the different PoC components fit in the PoC architecture.

The PoC architecture is constructed over the general definition of the HLA designed in the INSPIRE-5Gplus project as depicted in Figure 1. This HLA is compliant with ETSI ZSM reference architecture design principles and management services and domains, including the assumption of separation of different Management Domains (called in this PoC Security Management Domains or SMDs) and an E2E Security management Domain (E2E SMD) and the support of an integration fabric per domain and cross domain. Also, the SMDs are part (and leverage functionalities) of other Management Domains services, such as NFV MANO or SDN controllers to deploy security functionalities or enablers.

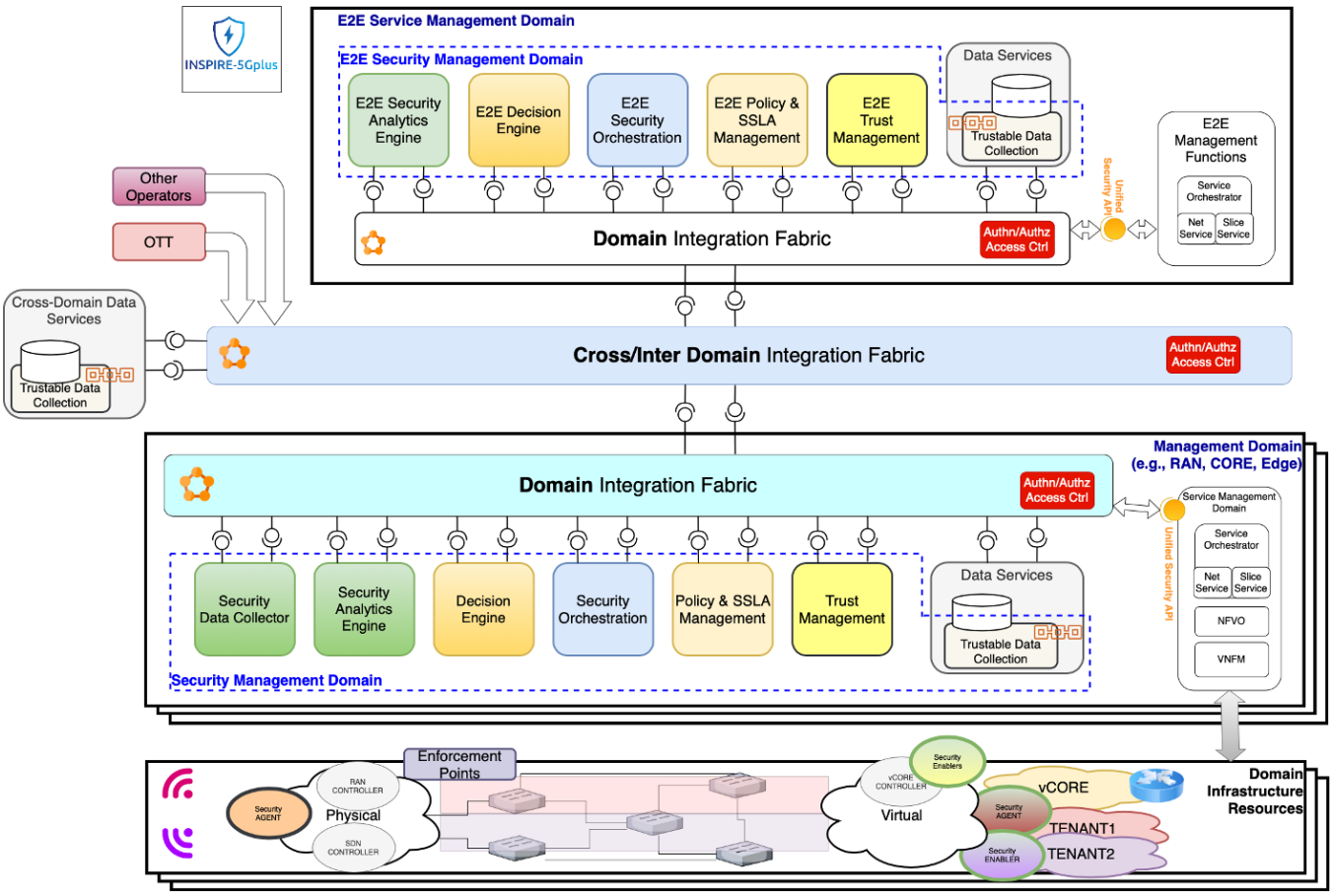

Figure 1: PoC architecture

The PoC architecture is split into different SMDs to support the separation of security management concerns (e.g., for the Radio Access Network RAN, Edge or Core Network). Each SMD is responsible for intelligent security automation of resources and services within its scope. The E2E SMD is a special SMD that manages security of E2E services (e.g., network slice) that span multiple domains. The E2E SMD coordinates between domains using orchestration. The decoupling of the E2E security management domain from the other domains allows to escape from monolithic systems, reducing the overall system's complexity, and enabling the independent evolution of security management at both domain and cross-domain levels.

Each SMD, including the E2E SMD, comprises a set of functional modules, including:

- **Security Data Collector (SDC)**, which aims to gather all the data coming from the security enablers at the domain level, needed by the security management functions (e.g., Security Analytics Engine).
- **Security Analytics Engine (SAE)**, which derives insights and predictions on a domain's security conditions based on data collected in that specific domain or even from other domains. In the context of INSPIRE-5Gplus, the SAE provides Anomaly Detection and Root Cause Analysis (RCA) services.
- **Decision Engine (DE)**, which oversees the different actions emitted by the security assets and the SAE to select the best decisions which can be applied for securing a running targeted service.
- **Security Orchestration (SO)**, which oversees the different security enablers to enforce the security requirements specified by the adopted security policies. The SO drives the security management by interacting, through the integration fabric, with different SDN controllers, NFV MANO and security management services.
- **Policy and SSLA Management (PSM)**, which transforms the abstract Protection Level and Security Level requirements and constraints expressed by consumers as intents and providers into specific parameters that indicate, to the SO, the security services to configure, deploy and manage.

- **Trust Management (TM)**, which provides various services for the trust related functions, such as trust reputation calculation, component certification, and Ordered Proof of Transit (oPoT).
- **Security Agent (SA),** a security asset or enabler for monitoring and managing security at a local point in network, with traffic capture and security packet processors. The SAs communicate with the INSPIRE-5Gplus management plane to provide security data to the analysis and management functions from the traffic control and data plane (e.g., an active or passive probe).

The various security management services provided by these modules are exposed within the same domain but also cross-domain, to the authorized consumers, through an integration fabric. Data Services allow the different security services to persist data that can be shared in one or more domains.

The functional modules operate in an intelligent closed-loop way to enable AI-driven software defined security (SD-SEC) orchestration and management in compliance with the expected SSLA and regulatory requirements. By adopting service-based and SD-SEC models, it allows to build up sustainable security measures that can adapt to dynamic changes in threats landscape and security requirements in next-generation mobile networks.

2.2.1 Close-loop approach

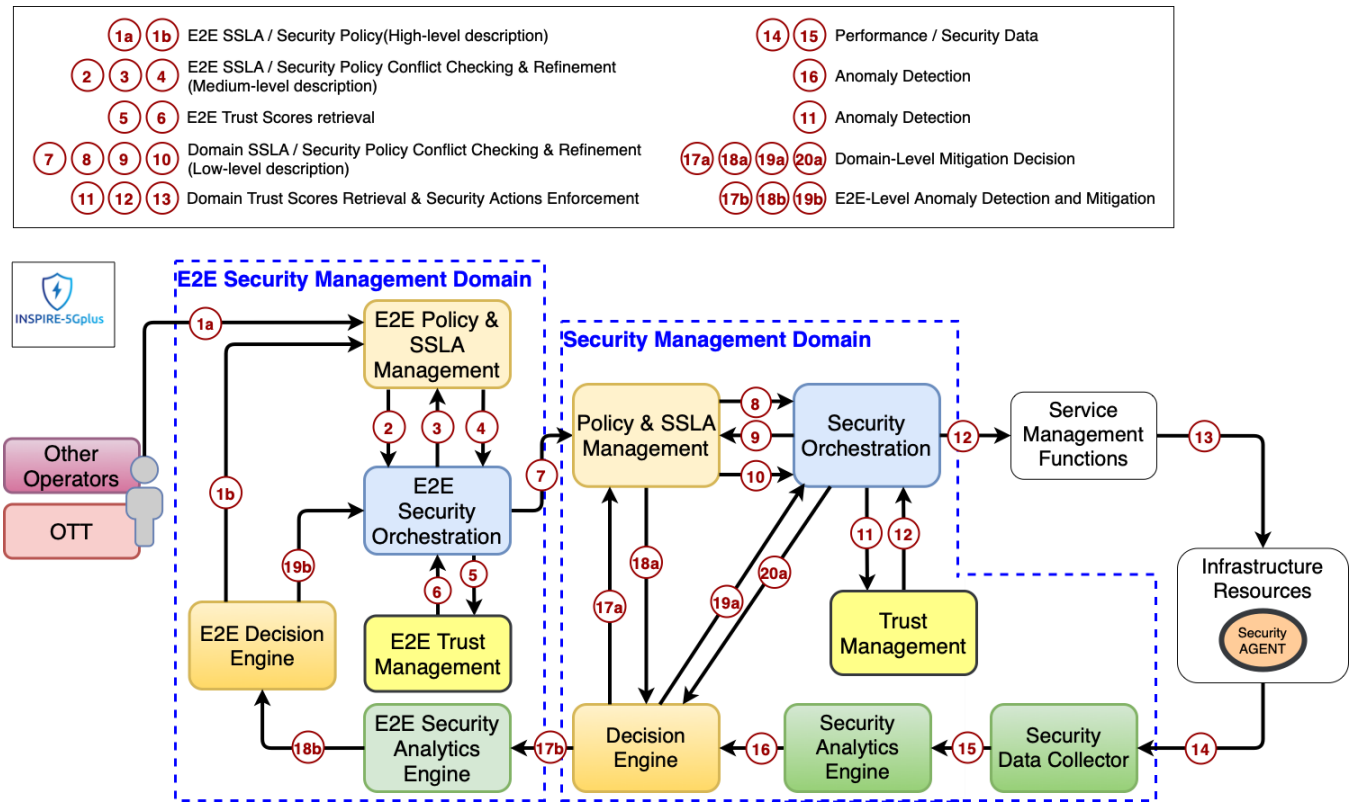

Figure 2: Closed-loop solution workflow

A particular security management Closed-Loop is proposed in this PoC from the generic approach is represented in Figure 2. Two starting points exists for the whole process at the E2E SMD level (1a,1b), both implying the provision of an E2E SSLA coming from an external customer (e.g., OTT) or internally as an AI based decision. Once the SSLA arrives to E2E SSLA Manager expressed as an intent, a refinement process (2-4) is performed producing an orchestration High-Level Security Policy Language (HSPL) which in turn is refined in several orchestration Medium-Level Security Policy Language (MSPL), at least one per involved SMD. This HSPL to MSPL refinement takes profit of trustworthiness scores and taking advantage of the historical behavior of the system among others (5,6).

The solution selected needs to be enforced on the different SMDs (7), which in turn are responsible of the infrastructure. The Orchestration MSPLs are refined onto Domain MSPLs (8-10) while taking care of possible dependencies as well as conflicts

between them. Similar to the trustworthiness score-based solution prioritization done at E2E level, at this level not only the possible solutions are evaluated but also the infrastructure on which they are going to be deployed (11-12). As a result of this process the precise interactions with the infrastructure elements (12) are obtained and the system's behavior is altered (13).

The system's behavior is constantly monitored (14), to look for security flaws. In the PoC some attacks and security events will be generated to trigger events to be reported to the SAE (15). When an anomaly is detected, the DE at the SMD level is informed (16).

AI techniques are employed to generate a mitigation in MSPL form again inspected for conflicts with the already enforced policies (17a,18a). Finally (19a,20a) the SMD loop is closed by providing the SO with the new policy that is altering system behavior again.

Alternatively, or by explicit decision, E2E SAE is informed(17b) of the anomaly and the countermeasure decided, if any. This action will help in closed-loop coordination. The E2E SAE will inform the E2E DE (18b) that again may decide to provide a countermeasure but probably affecting neighboring SMDs via the E2E SO (19b) therefore closing the E2E loop.

2.2.2 Components and ZSM relationship

For the PoC implementation not all the components defined in the INSPIRE-5Gplus architecture would be used in all SMDs and in the E2E SMD, but only those involved in each of the use stories. Also, the PoC will involve at least one E2E SMD and 2 SMD for each of the use stories to demonstrate the cross-domain functionality. Figure 3 provides a reference of the key components involved in the PoC.

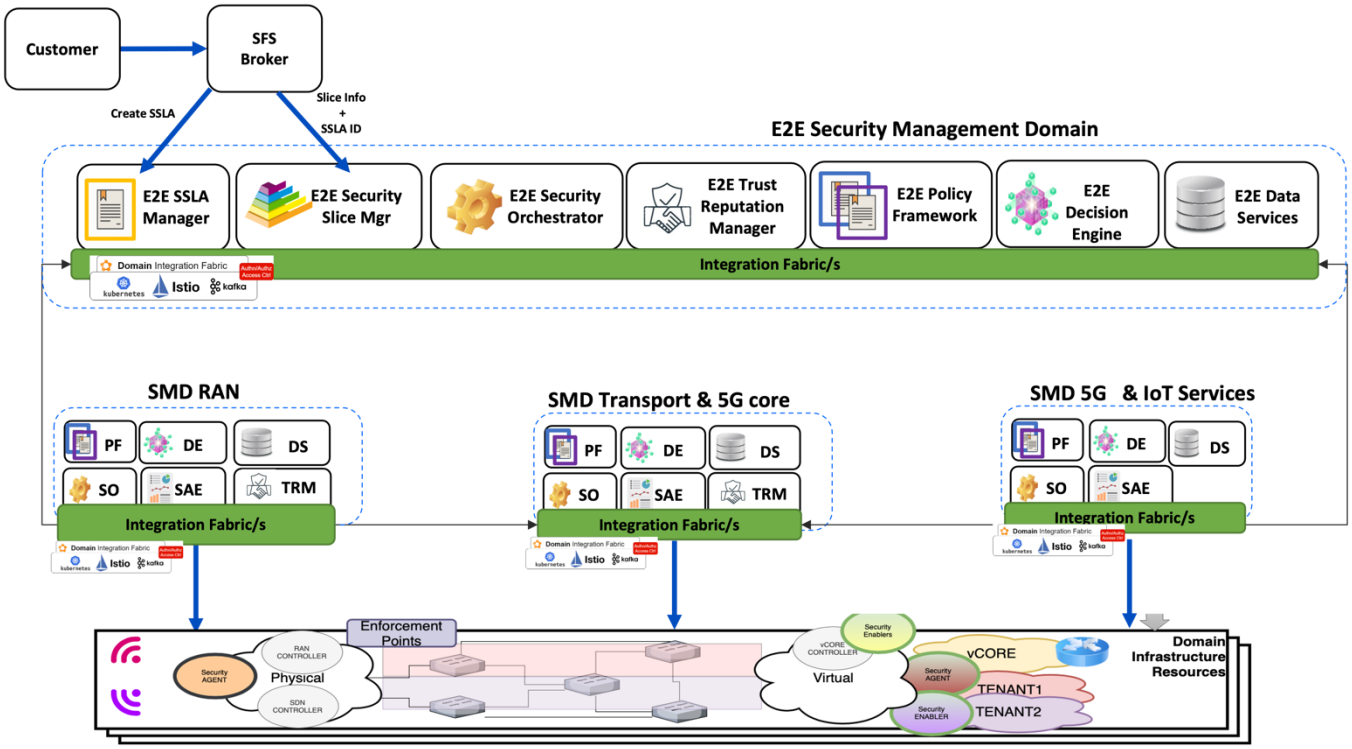

Figure 3: Closed-loop solution workflow

In this PoC, there are several Management Domains belonging to the same operator, but each one is independent from the point of view of the management and security following the assumption that in Telco management processes and operations, each domain can be independently operated for specialized teams (radio access domain, transport domain, 5G core domain, and different 5G or IoT services), but always below a common E2E coordination and security provisioning.

In Table 1 is provided a mapping between components from INSPIRE-5gPlus in the proposed PoC and the ZSM 002 framework.

Table 1. PoC common components and their alignment with ZSM services

ZSM architecture sub-system	INSPIRE-5Gplus component	Provided ZSM services
ZSM framework consumer	**SFS Broker**: performs the brokering operation to select the optimal slice provider (operator) for requested SSLA	• N/A
ZSM E2E Service MD	**E2E Slice Manager:** generate a 5G Security Slice Orchestration policy from the SSLA and the 5G network slice requirements	• E2E Orchestration • E2E Data services
	E2E Security Orchestrator: orchestrate and distribute orchestration policies from the E2E domain to the different SMD	• E2E orchestration • E2E Data services
	E2E Decision Engine: Generate reactive security E2E policies (e.g., replicate security policies to another MD)	• E2E Domain intelligence
	E2E Policy Framework: validate and refine policies	• Supporting services (policy mgmt)
ZSM individual MD's	**Security Orchestrator**: Generate orchestration plan and interact with MD orchestration	• Domain orchestration
	Policy Framework: Translate HSLP to MSPL and use Trust metrics	• Domain orchestration • Domain control • Domain data services
	Decision Engine: Generate reactive security policies (e.g., redeploy a VNF, configure drop rule, etc.)	• Domain intelligence
	Security Analytics Engine: Process data from collector and detect attacks and anomalies in the network slices based on AI	• Domain intelligence
	Security Data collector: Collect security related data from infrastructure or from the Security Agents	• Domain data collection
	Security Agents: Different security assets to provide data, aggregate info generates security alerts	• Domain data collection • Domain data analytics • Domain intelligence
	Trust Reputation Manager: Collect trust level metrics and generate reputation values	• Domain intelligence
	MANO stack: NFVO (Open Source MANO) + VIM (Openstack + k8s) + SDN controller (I2NSF)	• Domain orchestration • Domain control • Domain data services
Cross-domain integration fabric	**INSPIRE-5Gplus Integration Fabric**	• Management service Discovery • Management communication

2.3 Additional information

[1] H2020 project INSPIRE-5Gplus [Online]. Available: https://www.inspire-5gplus.eu/