ISG ZSM PoC Report

1 PoC Project Details

1.1 PoC Project

PoC Number: (assigned by ETSI)	
PoC Project Name:	Automated platform expansion, service provisioning, and proactive service-level agreement (SLA) preservation across multi-site and multi-stakeholder environments.
PoC Project Hosts:	UoP, Telefonica S.A.
Short Description:	This PoC assumes that an open orchestration platform already manages a certain domain in the city of Athens. Upon request, the PoC begins with the demonstration of (i) the expansion of the orchestration platform towards a new private domain in a zero-trust fashion and with high-degree of automation, (ii) the automated provisioning of compute, network, and end user services across the new and the existing domains, and (iii) policy-based access control towards service component coupled with a proactive preservation of a multi-domain SLA in a truly zero-touch manner. This PoC addresses the following ZSM PoC topics: (i) the Automation in Multi-Stakeholder Ecosystems (Topic 2 here, WIs ZSM-001 and ZSM-003) (ii) the Cross-domain user-driven E2E services (Topic 4 here, WI ZSM-008).

1.2 PoC Team Members

	Organisation name	ISG ZSM participant (yes/no)	Contact (Email)	PoC Point of Contact (*)	Role (**)	PoC Components
1	UBITECH Ltd.	No	Georgios P. Katsikas gkatsikas@ubitech.eu		Network/service provider	- Use case definitions - Testbed provider
2	p-NET	No	Christos Tranoris ctranoris@p-net.gr		Network/service provider	- Use case definitions - Testbed provider
3	Telefónica Innovación Digital	Yes	Diego R. López diego.r.lopez@telefonica.com		Network/service provider	- Testbed provider - NDT environment provider
4	UPM	No	Alberto Mozo a.mozo@upm.es		University/ supplier	- AI Model repository provider
5	NOVA	No	Ioannis Markopoulos Ioannis.Markopoulos@novaict.gr		Network/service provider	- Secure integration fabric service provider - Integrator
6	University of Patras	Yes	Kostis Trantzas ktrantzas@ece.upatras.gr	X	University/ supplier	- End-user service provider - Integrator
7	CTTC	Yes	Lluis Gifre lluis.gifre@cttc.es		Research center/supplier	- Transport network controller provider - Network security controller provider
8	LMI	No	Joseph McNamara joseph.mcnamara@ericsson.com		Integrator	- Automation service for SLA adaptation
9	WINGS	Yes	Dimitrios Triantafyllou dtriantafillou@wings-ict-solutions.eu		Integrator	- Automation service for SLA adaptation
10	K3Y	No	Evangelos Syrmos esyrmos@k3y.bg		Integrator	- Automation service for SLA monitoring and forecasting

(*) 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 report 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
ACROSS Automation PoC - Scenario #1 (see Section 2.2.2)	East-west platform expansion to a new private edge domain	ZSM-001, ZSM-003, ZSM-008	Propose a solution to automate the east-west expansion of an orchestration platform to a new private domain in a secure and trusted manner. The solution includes the provisioning of a dedicated domain orchestrator instance in the new domain that will be interconnected with a multi-domain orchestrator via a secure integration fabric.	By 30/11/2025
ACROSS Automation PoC - Scenario #2 (see Section 2.2.3)	Zero-touch multi-domain end-to-end service provisioning	ZSM-001, ZSM-003, ZSM-008	Propose a solution to automate the provisioning of an end-to-end 5G-based service across the central management domain and the new private edge domain. This solution will entail the automated provisioning of (i) compute (Kubernetes-as-a-Service) and mobile network (5G-as-a-Service) resources, (ii) the end-user service on top of the allocated resources, and (iii) end-to-end telemetry for compute, 5G, and end user services.	By 30/11/2025
ACROSS Automation PoC - Scenario #3 (see Section 2.2.4)	Zero-touch service access control and proactive SLA preservation	ZSM-001, ZSM-003, ZSM-008	Propose a solution for creating an SLA for the deployed service and ensuring that this SLA is proactively preserved using Analytics forecasting for potential SLA violations and a closed loop Automation that proactively adapts the end user service to preserve the SLA.	By 30/11/2025

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
-	-	-	-	-

1.4 PoC Project Milestones

PoC Milestone	Milestone description	Target Date	Additional Info
P.ST	PoC project start	July 01, 2025	-
P.SM	PoC proposal submission	July 18, 2025	-
P.PR	PoC presentation	September 09-10, 2025	ETSI ZSM #32 plenary meeting (online presentation)
P.P.A	PoC public announcement	At a convenient date set by ETSI ZSM	-
P.U.S	PoC user story detailed	October 2025	-
P.T.P	PoC test plan	October 2025	-
P.D	PoC demo	November 14, 2025	Webinar
P.R	PoC report	December 01, 2025	-

NOTE: Milestones need to be entered in chronological order.

1.5 Additional Details

Horizon Europe ACROSS project [1] web portal details information about project's scope and multiple references to design, implementation, validation, and open-source contributions.

2 PoC Technical Details

2.1 PoC Overview

This PoC aims at demonstrating the automated expansion of an orchestration platform to a new private domain, where the domain stakeholder is offered means to (i) provision end-to-end 5G-based services in a fully automated manner and (ii) proactively preserve the service's SLA using smart SLA forecasting and service reconfiguration actions. This PoC will utilize parts of the infrastructure of the ACROSS Horizon Europe project [1].

2.1.1 Infrastructure

This PoC leverages infrastructure from the ACROSS project; ACROSS is a Horizon Europe RIA project that envisions ambitious – yet tangible – breakthroughs in zero-touch service and network management. To realize this vision, ACROSS establishes a hierarchical orchestration platform based on 4 main pillars:

1. A logically centralized (cloud managed) Multi-domain Orchestration (MDO) platform that resides in an end-to-end service management domain.
2. A dedicated domain orchestration (DO) platform instance in every managed domain (DO is distributed)
3. A Network Planning domain where Digital Twins and realistic Data Generation mechanisms are employed to facilitate the training of smart AI/Analytics-based models for network management.
4. An open and programmable Zero-Trust Connectivity (ZTC) Fabric which ensures secure integration of all the managed domains with the end-to-end service management and the network planning domains.

ACROSS provides the above capabilities through a testbed that is currently active in the south part of Europe across Greece and Spain as shown in Figure 1. The domains of this testbed and their main components are explained in the rest of this section.

Note that additional services may be part of each testbed, depending on the needs of a certain use case; Section 2.2 showcases a more detailed view of this testbed will all the components that participate in the proposed PoC.

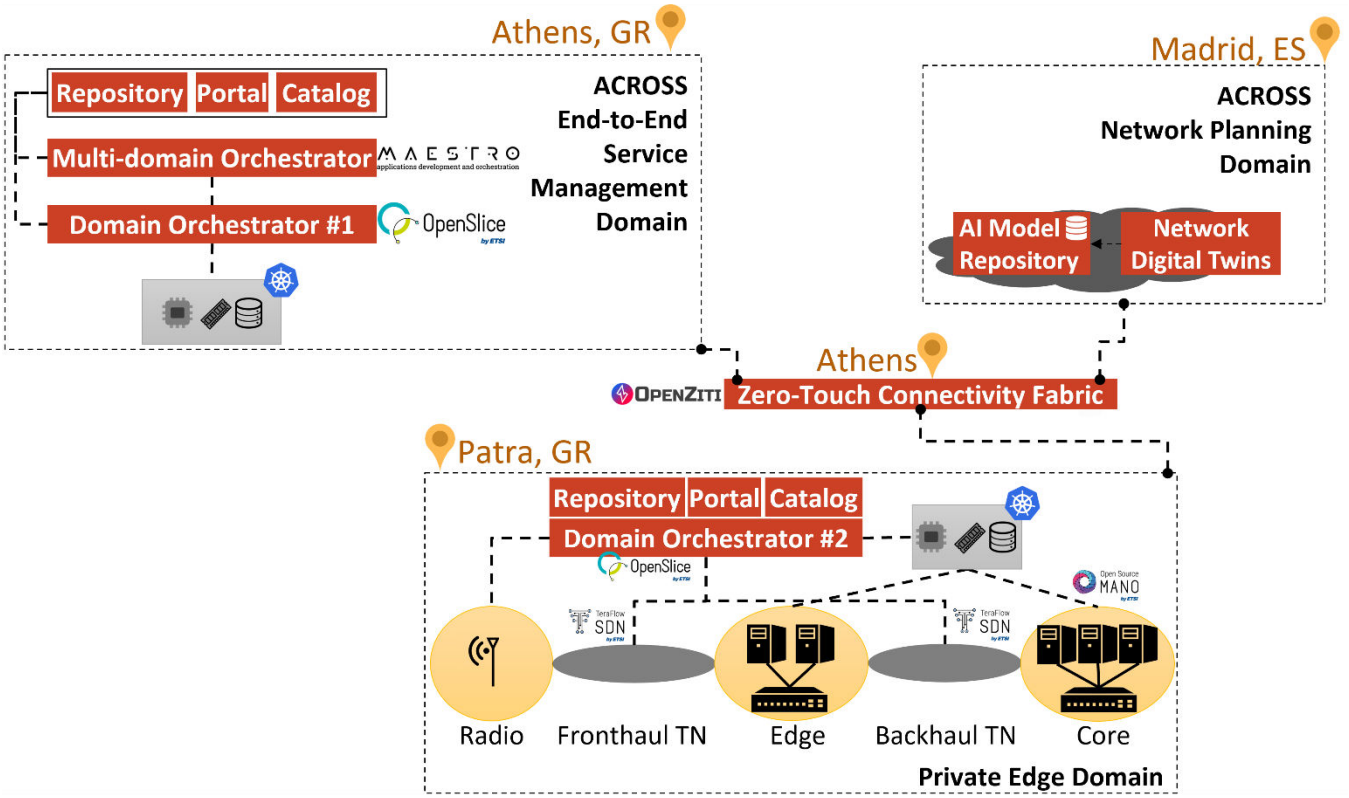

Figure 1: ACROSS infrastructure sites leveraged by this PoC.

End-to-end Service Management Domain (Athens, Greece)

This domain serves as a central point of management, where ACROSS employs an instance of the MDO as well as an instance of the DO (i.e., Domain Orchestrator #1 in Figure 1) for managing local compute resources as shown in the top left part in Figure 1. UBITECH's Maestro [7] service orchestration platform acts as the MDO and ETSI OpenSlice [8] acts as the Domain Orchestrator #1.

Network Planning Domain (Madrid, Spain)

This domain offers Telefonica's Network Digital Twin (NDT) environment for serving as a pre-production facility where telco operators can test their services under realistic conditions and traffic patterns. Part of the NDT's capabilities is (i) the training of AI/Analytics-based models using either artificial or real network data, (ii) the validation of these models, and (iii) the persistence of these models into a model repository that is exposed to other domains via a secure integration fabric (i.e., the Zero-Touch Connectivity Fabric). This domain is in line with the concept of the Network Digital Twins as defined in the ETSI GS ZSM 018 document [6].

Private Edge Domain (Patra, Greece)

This domain serves as a realistic environment for employing vertical applications from different sectors, such as smart cities, energy management, Industry 4.0, etc. These services leverage the large-scale Patras 5G testbed that spans across the UoP campus, the Patras city centre, and other locations in the region of Patra. This testbed offers distributed points-of-presence of compute and mobile network resources that can be dynamically interconnected and orchestrated by a local DO (i.e., OpenSlice acting as Domain Orchestrator #2) instance. Underneath OpenSlice, additional ETSI SGD platforms are employed to manage 5G cNFs (ETSI OSM [9]) and transport network services (ETSI TFS [10]).

Zero-Trust Connectivity (ZTC) Fabric (Athens, Greece)

This domain is the glue among all the other domains as it provides a secure and programmable fabric for establishing on-demand tunnels between services that reside in geo-distributed private domains. This is done via OpenZiti [11], an open-source platform that acts as the foundation for the ACROSS ZTC fabric. This platform is in line with the concept of the Integration Fabric as defined in the ETSI GS ZSM 002 architecture document [2].

2.1.2 Objective

This PoC will leverage the ACROSS infrastructure to showcase a comprehensive zero-touch orchestration use case deployed across multiple administrative domains with minimal manual configuration. The demonstration will capture the entire service lifecycle—from the initial expansion of the infrastructure, through automated onboarding of required services, to dynamic end user service provisioning over on-demand compute and network resources—coupled with end-to-end SLA-driven service management. Specifically, the use case assumes:

- A Multi-domain Orchestrator, a Domain Orchestrator (i.e., Domain Orchestrator #1 in Figure 1), and the Zero-Touch Connectivity Fabric initially operate within Domain A. The MDO triggers the establishment of a secure, orchestrated link towards a newly introduced Domain B via the ZTC Fabric, enabling inter-domain connectivity.
- Following the successful establishment of secure connectivity towards Domain B, MDO orders the instantiation of a second Domain Orchestrator (DO#2) instance within Domain B. This new orchestration instance assumes control over local infrastructure and resource controllers, managing them autonomously and exposing them in an "as-a-Service" manner.
- Once Domain B is fully onboarded, the user service is prepared, and its deployment is requested via the orchestration platform. The MDO initiates the service order by instructing DO#2 to provision the necessary compute, network, and telemetry resources tailored to the service requirements. Upon successful provisioning, the MDO proceeds to deploy the user application atop the newly instantiated infrastructure and launches the telemetry collection and visualization workflow.
- During the service runtime, the PoC supports dynamic enforcement of security policies governing access to service components. Simultaneously, it enables the definition of an SLA, followed by continuous SLA monitoring and predictive analytics to detect deviations in advance. The latter forms the basis for a self-sustaining, closed-loop control mechanism that preserves SLA compliance autonomously, without human intervention.

2.2 PoC Architecture and Story

This section gradually introduces the PoC architecture and high-level storytelling, following 4 distinct scenarios as follows:

(i) **Scenario #0 (PoC setup):** the initial state of the testbed before the launch of the PoC.
(ii) **Scenario #1 (PoC begins):** Launch of the PoC with the expansion of the orchestration platform to a new domain (i.e., Domain B in the city of Patras).
(iii) **Scenario #2:** Telemetry-aware end-to-end service provisioning across domains A and B.
(iv) **Scenario #3 (PoC ends):** Real-time service security and proactive SLA preservation across domains A and B.

After the end of Scenario #3, the testbed reaches its final state. A figure highlights this state, also defined as the PoC architecture. The rest of this section describes each scenario in greater detail.

2.2.1 Scenario #0 - Testbed state before the PoC

Figure 2 visualizes the state of the testbeds before launching the PoC. During this stage the orchestration platform operates on two domains, namely domains A and C.

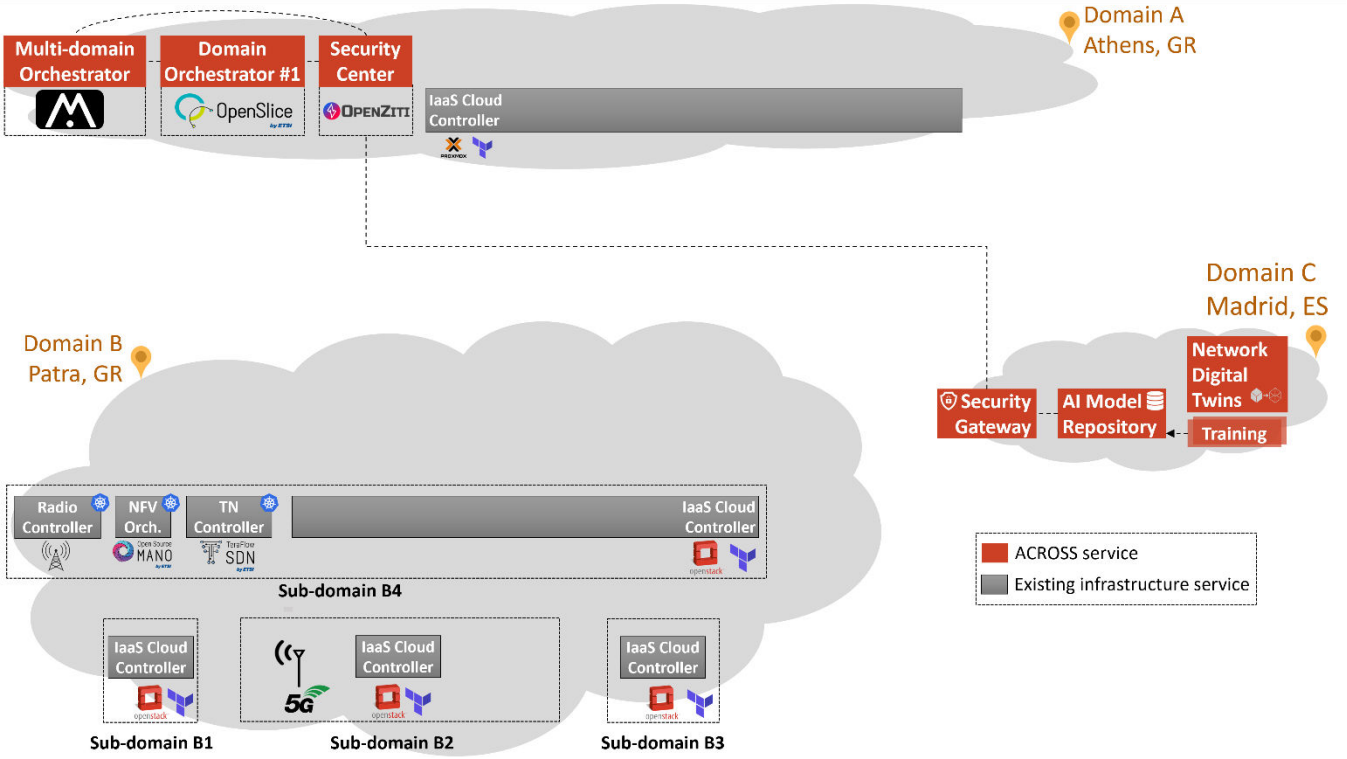

Figure 2: Scenario #0 - Initial state of testbeds before the PoC.

Domain A

Domain A acts as a central management domain of the ACROSS Platform. It is in Athens (Greece) with the following components in place:

- an instance of the Multi-domain Orchestrator (see Figure 2).
- an instance of the Domain Orchestrator (i.e., Domain Orchestrator #1 in Figure 2).
- an instance of the Zero-Touch Connectivity Fabric (i.e., Security Center in Figure 2).
- Infrastructure-as-a-Service (IaaS) cloud services based on ProxMox [13] and Terraform [15] to host additional platform and end-user services of the proposed PoC at later stages (see Scenario #2 and Scenario #3).

Domain C

Domain C is used as a Network Planning domain. This domain is in Madrid (Spain) and offers the following services:

- an instance of the ZTC Gateway (Security Gateway in Figure 2) connected to the ZTC Fabric (Security Center) in Athens. This allows secure connectivity of this domain with the rest of the platform.
- an instance of an NDT used for offline training AI/Analytics services (Network Digital Twins Training in Figure 2). This is used by a telco operator to train smart services under realistic conditions and expose these services in a production environment for real-time inference.
- an instance of the AI model repository (see Figure 2) for storing the AI/Analytics models produced by the NDTs. This repository offers an API for remote AI/Analytics inference services to fetch the models.

Domain B

Domain B is in Patra (Greece). At this initial scenario of the PoC, this domain is not orchestrated by the platform. The owner of this edge domain uses some local infrastructure services (across sub-domains B1, B2, and B3 in Figure 2) to manage the compute and network resources of this domain, as follows:

- an instance of a mobile radio controller for managing Tx/Rx characteristics of 5G base stations (sub-domain B4).
- an instance of an NFV Orchestrator – based on ETSI OSM [9] – for managing the core Network Functions of the 5G Core (sub-domain B4).
- an instance of a programmable Transport Network controller – based on ETSI TFS [10] – for managing transport connectivity services within the domain (sub-domain B4).
- four instances of IaaS cloud services based on OpenStack [14] and Terraform [15], each one in a different sub-domain (i.e., B1, B2, B3, and B4 in Figure 2). These cloud sites are planned to host some dynamic platform and end-user services of the proposed PoC at later stages (see Scenario #1-Scenario #3).

2.2.2 Scenario #1 – East-west platform expansion to a new private edge domain

This scenario triggers the launch of the proposed PoC. The owner of Domain B (Patras testbed) is registered to the orchestration platform as a new stakeholder with role "Infrastructure owner". The owner of Domain B expresses interest to the MDO administrator to bring Domain B under the realm of the orchestration platform, explaining that Domain B is a private domain (i.e., its local infrastructure services are not publicly accessible). The MDO admin authenticates against the MDO portal and initiates the process of expanding the MDO to a new private domain. This process starts with (i) the MDO requesting an identity for the Domain B owner from the Security Center and (ii) the Security Center generating and returning a secure authentication token for the Domain B owner. This is sent back to the MDO via an encrypted channel and MDO associates this token with the Domain B owner user. When domain B infrastructure owner logs in to Maestro, he/she can find a download button for this security token under the platform view, along with instructions on how to initiate a Security Gateway process in Domain B, using this authentication token. Once the Domain B owner launches the Security Gateway in a designated machine in Domain B (see Figure 3), a secure link is established between Domain A (the Security Center) and Domain B, where the Security Gateway acts as a proxy. At this point in time, no private infrastructure services are yet exposed outside of Domain B as this process requires further actions (approved by Domain B owner). This is important to highlight because the proposed Integration Fabric poses zero security and trust compromises upon the installation of the Security Gateway in a new private domain.

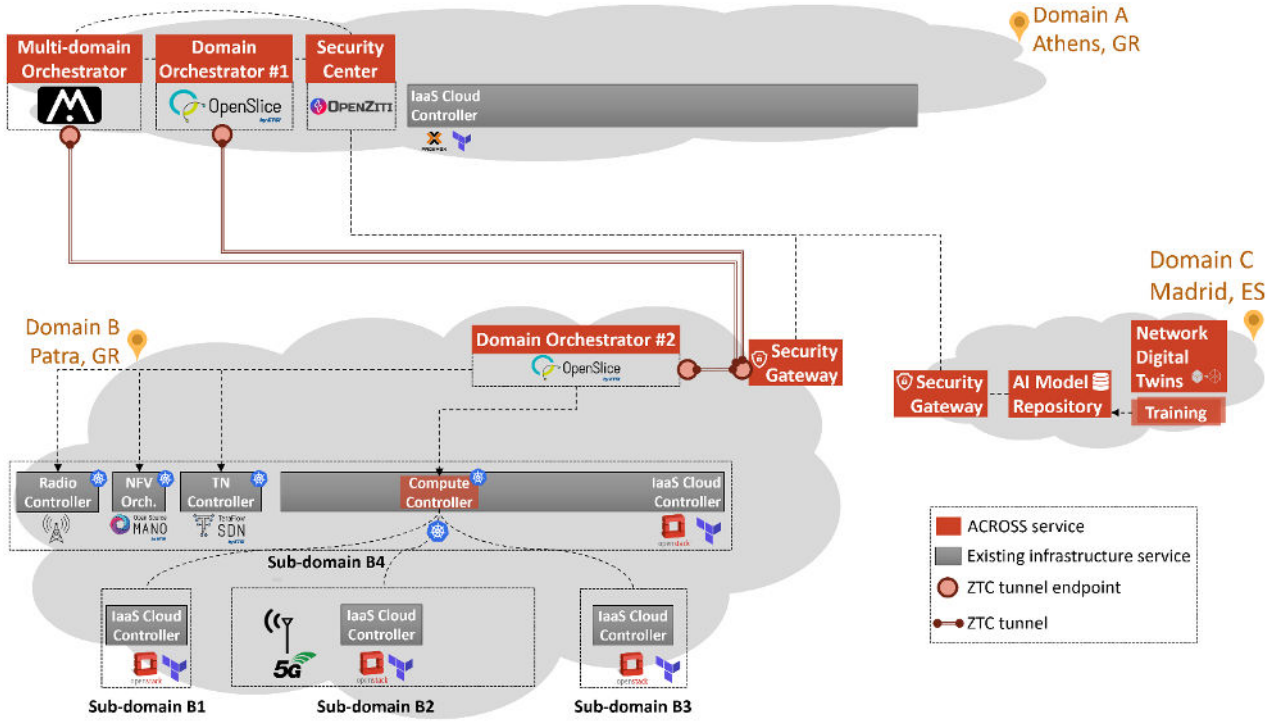

Figure 3: Scenario #1 – East-west platform expansion to a new private edge domain.

The MDO in now able to see Domain B as a new candidate domain for orchestration. To do so, the MDO needs to initiate the process of provisioning a new instance of a DO within this new domain. To facilitate this process, the infrastructure owner uses the MDO portal to register an existing Kubernetes cluster in Domain B onto the MDO. This cluster will be used to host the new instance of the DO (i.e., DO#2) in Domain B. When this cluster is made available to the MDO, the latter is able to order the instantiation of the DO in Domain B. When the DO #2 instance is successfully provisioned in Domain B (see Figure 3), the underlying infrastructure resources (i.e., all infrastructure controllers) in sub-domain B4 are automatically discovered as custom Kubernetes resources using the DO's compute controller service (also shown as a new service in Figure 3) and added to the DO #2 service catalog.

Scenario #1 result: The orchestration platform has successfully established a secure encrypted link between the central management domain (i.e., Domain A) and a new private edge domain (i.e., Domain B) and a new DO instance installed in Domain B dynamically exposes resources-as-a-service (Kubernetes and 5G) towards the MDO. Domain B is now ready for real-time orchestration. The amount of automation embodied in this scenario is substantial, as the platform undertakes a lot of hidden steps to instruct secure east-west expansion to a new domain. The steps that require human intervention are mostly kept manual for not compromising privacy and security requirements of the Domain B owner.

Scenario #1 video: The demonstration of Scenario #1 can be found in X.

2.2.3 Scenario #2 – Zero-Touch multi-domain end-to-end service provisioning

In this scenario, Domain B is already under the orchestration platform's realm (as a result of Scenario #1) and DO#2 is available for exposing domain B resources-as-a-service to the MDO. Scenario #2 begins with the MDO attempting to peer with DO #2; during the peering process, the MDO dynamically onboards compute and network services from the DO #2 service catalog into its own service catalog. Specifically, DO #2 advertises a "Kubernetes-as-a-Service" service specification for acting as a compute platform service and a "5G-as-a-Service" service specification for acting as a network platform service. Both services are now onboarded into the MDO catalog, thus the MDO can offer these services to accommodate end-user services on top.

Next, the Domain B owner wishes to provision an end-to-end service for one of his/her customers. This service is comprised of several components that shall be deployed across multiple domains as follows:

- Sub-domain B3 shall host a compute cluster
- The compute cluster in sub-domain B3 shall host a 5G video streaming server
- Sub-domain B1 shall host a compute cluster
- The compute cluster in sub-domain B1 shall host a 5G video streaming client
- Sub-domain B2 shall host a compute cluster
- The compute cluster in sub-domain B2 shall host the software-based network functions of an end-to-end 5G system
- Sub-domain B2 shall also host the radio elements of the same 5G system. This 5G system will connect the streaming client with the streaming server.

Domain B owner also expresses a will to expose compute, network, and user service telemetry information to the MDO (in Domain A), as this telemetry data will be useful for the MDO to preserve the SLA of this service (this will be shown in Scenario #3). For this reason, another telemetry data federation service is employed between Domain A and B as highlighted in the top right corner in Figure 4. The blue boxes in Figure 4 highlight the presence of all end-user service components across sub-domains B1 and B3 as well as Domain A.

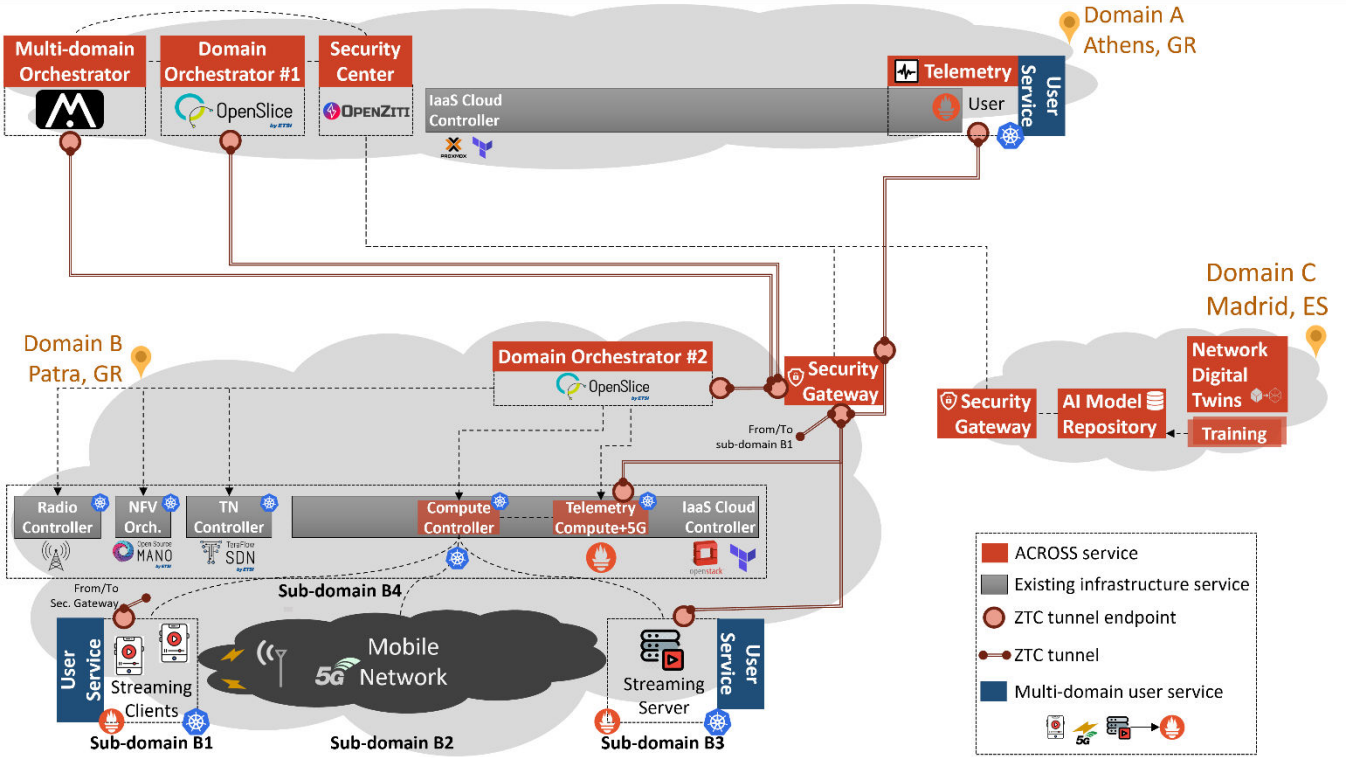

Figure 4: Scenario #2 – Zero-Touch multi-domain end-to-end service provisioning.

Before deploying these user service components, the orchestration platform requires to:

(i) design a suitable end-user service specification for this service,
(ii) onboard this service specification onto the MDO service catalog, and
(iii) bundle this service specification with the compute and network platform services fetched from DO #2 to ensure that the user service has enough resources to operate as expected.

This scenario assumes that steps (i) and (ii) are already done by the MDO administrator, as these steps are related with the design scenario of an end-user service, which is typically done offline. That said, Scenario #2 continues with a service order request to the MDO, which contains 5 service order items:

- 2x Kubernetes-as-a-Service order items for creating clusters within sub-domains B1 and B3
- 1x 5G-as-a-Service order item for provisioning an end-to-end 5G system in sub-domain B2, to act as a cellular high-speed transport between streaming clients in sub-domain B1 and the streaming server in sub-domain B3.
- 1x end-user service order item for the streaming clients service in sub-domain B1.
- 1x end-user service order item for the streaming server service in sub-domain B3.

For the successful completion of this service order, the MDO first initiates 3 additional service orders to DO #2. This is because the Kubernetes-as-a-Service and 5G-as-a-Service service order items belong to the DO #2 service catalog, thus their lifecycle needs to be managed by the Domain B orchestrator (i.e., DO #2). Only when these services are successfully deployed (i.e., the compute clusters are ready to host the user service), the MDO can proceed with the provisioning of the other 2 user services. When this is also finished, the MDO also instructs the federation of telemetry data from the Telemetry platform service in sub-domain B4 to the Telemetry platform service in Domain A as shown in Figure 4. This telemetry data in only sent via a dedicated tunnel of the secure integration fabric.

Scenario #2 result: The result of this scenario is an active end-to-end 5G-enabled service across Domains B and A, where the streaming clients can stream inputs video(s) towards the streaming server via a private 5G network. In addition to this functional user service, telemetry data from the compute and 5G resources as well as the end user service is populated from in Domain B to Domain A in a secure and trusted manner (i.e., using encrypted tunnels of the ZTC fabric). The service inventory portal of both the MDO and DO #2 as well as available dashboards on the MDO and DO#2 telemetry service portals confirm

this claim. Most importantly, this composite multi-domain service provisioning scenario was triggered via a simple UI-driven interaction with the orchestration platform's portal, while the end-to-end provisioning of the underlying services was done in a truly zero-touch manner.

Scenario #2 video: The demonstration of Scenario #1 can be found in X.

2.2.4 Scenario #3 – Zero-touch service access control and proactive SLA preservation

An end-to-end service is already provisioned between Domains B and A, as a result of Scenario #2. In this Scenario, the Domain B owner expresses interest in:

(i) Scenario #3A: Defining security policies to perform real-time access control to the service components (Section 2.2.4.1).
(ii) Scenario #3B: Defining and enforcing a performance SLA for this service (Section 2.2.4.2).

2.2.4.1 Scenario #3A: On-demand service access control

Security Platform Service: An additional security controller service is pre-deployed in Domain B (see Figure 5) to ensure that access control policies defined by the Domain B owner are correctly enforced to the service. To do so, an access control service is designed and onboarded onto the DO #2. When the Domain B owner orders this service, DO #2 invokes an API call to the Security Controller's NBI to define a list of access control policies towards sub-domain B3, which in turn invokes a corresponding API call to the Transport Network Controller (based on ETSI TFS [10]) to install appropriate data plane rules for traffic filtering before the traffic gets injected into the compute cluster in sub-domain B3. This way, only the designated traffic patterns can access the resources of the Streaming server, therefore protect it from potential attacks or unnecessary requests from unauthorized/third-party clients.

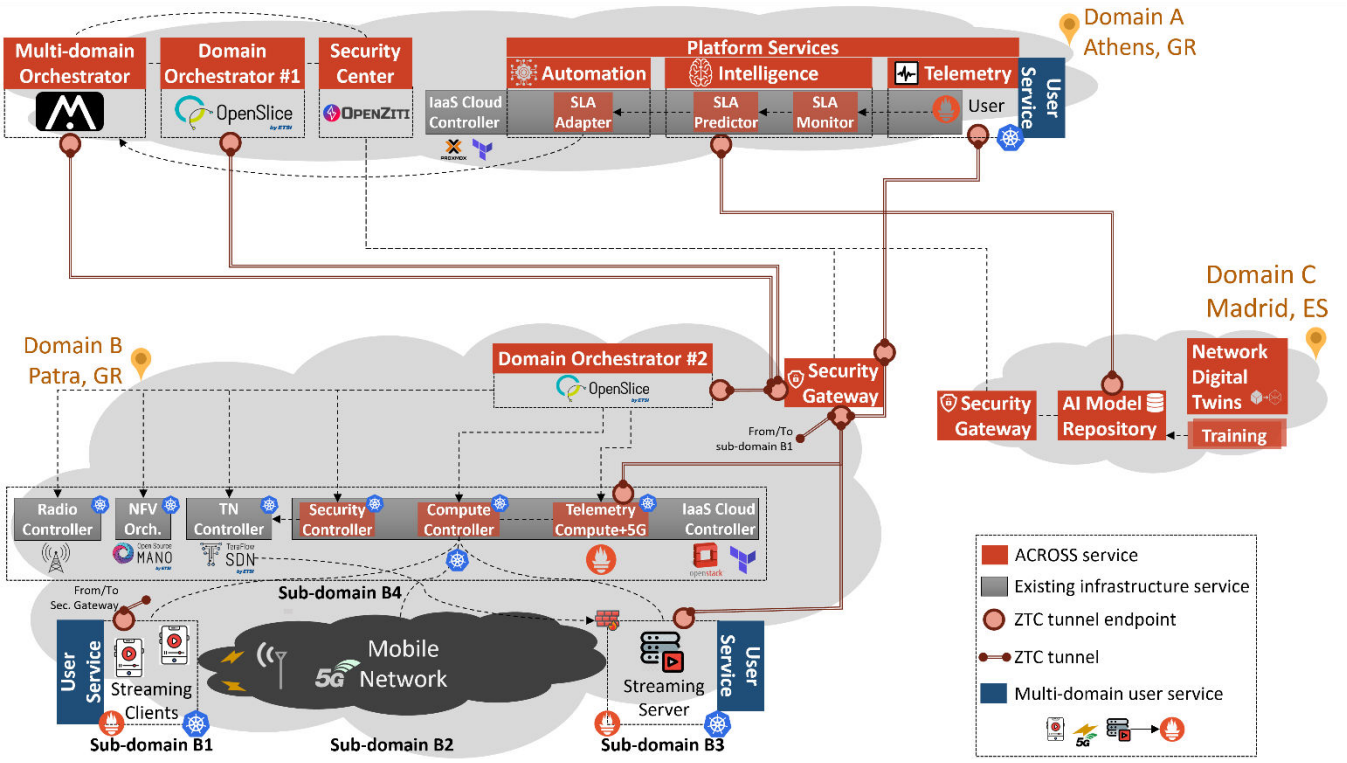

Figure 5: Scenario #3 – Zero-touch service access control and proactive SLA preservation.

2.2.4.2 Scenario #3B: Proactive SLA preservation

The performance SLA imposed by the Domain B owner demands proactive preservation of key service metrics within certain thresholds, as the owner of Domain B tolerates no violation of these thresholds whatsoever. For this reason, the operator of the orchestration platform decides to employ some additional platform services in Domain A for exploiting the gathered telemetry data to make smart, proactive decision about the user's SLA. These services are depicted in Figure 5 and briefly explained below.

Automation Platform Services: An automation platform service is employed in Domain A, titled "SLA Adapter" (see Figure 5). This service exposes a northbound API to the end user for managing SLAs in collaboration with the MDO. Specifically, the user may use this API to create an SLA around an active service that is available via the Service Inventory API of the MDO. To do so, the user uses the unique ID of the service as an input and describes three additional inputs for the proper definition of the SLA:

(i) the conformance period of the defined SLA, i.e., the time during which the SLA is valid, containing startDateTime and endDateTime.
(ii) a set of service-level objectives (SLOs) on available service metrics. Each SLO contains a unique ID and name that correspond to a service metric from the MDO Telemetry service, a conformance operator to define the condition type (e.g., <, >, =, !=), a conformance target value for the service metric (i.e., the desired minimum or maximum value of the service metric), a target threshold for the service metric (i.e., the hard boundary of the service metric to indicate an SLA violation), and a tolerance target margin (i.e., a marginal number under/above which the SLO is considered critical).
(iii) an SLO consequence defined as a set of actions to take if any SLO is violated. One consequence applies to all SLOs.
(iv) A related entity object which indicates a (list of) service ID(s) and the endpoints where the corresponding service object(s) can be retrieved from the MDO's Service Inventory API. In essence, this is the service associated with the defined SLA.

Once such an SLA is defined and linked with the MDO, the Automation service verifies that the above information is correct, i.e., the service ID(s) is(are) valid in the MDO's Service Inventory API and the service metrics defined in every SLO are present in the MDO's Telemetry service. Then, the Automation Service relays the valid input SLA to the "Intelligence" platform services (described next) to actively inspect the SLOs and inform Automation when an SLO is about to be violated. Upon such an event, the Automation service invokes the right API call to the MDO to enforce the SLO consequence, thus modify the service before its SLA is violated.

Intelligence Platform Services: When a valid SLA request is received by the Automation service, this request is relayed to the Intelligence platform services. These services undertake to (i) actively monitor the SLOs (i.e., service metric values) of this SLA from the MDO's Telemetry service (input Scenario) and (ii) spawn dedicated Analytics inference jobs that forecast the value of these SLOs in relation to the above target thresholds and tolerance margins. The former step is done by the "SLA Monitor" service shown in Figure 5, while the latter step is conducted by the "SLA Predictor" service shown in Figure 5. The "SLA Predictor" service assumes that an already trained Analytics/AI model for the target SLOs is in place, which in this case is fetched from the "AI Model Repository" service in the Network Planning domain (i.e., Domain C in Figure 5). If the "SLA Predictor" does not possess a suitable Analytics/AI model for one or more SLOs, then an offline process must be started in the Network Planning domain to build and provision an NDT for training such a model as shown in Figure 5. In the context of this PoC, the training process was done prior to the PoC, thus the model is assumed to be in the "AI Model Repository" in Domain C.

Scenario #3 result: The result of this scenario is a closed-loop platform service comprised of 3 platform services in Domain A: (i) the Telemetry platform service that gathers service metrics from the service deployed in Domain B into Domain A, (ii) the Intelligence platform services that ingest this data into a smart Analytics inference model to predict potential SLA violations, and (iii) the timely invocation of the Automation service when a potential SLA violation is forecasted so as to adapt the running service in a way that its SLOs are preserved within the tolerance margins. This adaptation is done via the MDO that performs real-time service update by applying e.g., scaling (up or down) actions on compute characteristics of the Streaming server and/or the underlying cluster.

Scenario #3 videos: The demonstrations of Scenario #3A and Scenario #3B can be found in X and Y respectively.

PoC Architecture: Figure 5 demonstrates the final state of the PoC, which also comprises the PoC architecture.

2.3 Additional information

This section concludes the PoC report with some highlights, measurable outcomes, and key messages for the ETSI ZSM community (see Section 2.3.1) as well as acknowledgements to the funding sources of this work and the involved open-source communities behind these projects (see Section 2.3.2).

2.3.1 Relevance for ETSI ZSM

This section summarizes a set of key highlights as main outcomes of this PoC, classified per scenario.

Highlights

- Scenario #1 showcases the expansion of the orchestration platform in a new private domain in real-time, without the need of using traditional VPNs for accessing the private domain's resources. Instead, this PoC leverages a programmable network fabric that allows to establish encrypted tunnels on the fly, thus greatly facilitating and automating platform expansion. Moreover, the platform itself possesses means to east-west expand its components on demand, effectively demonstrating how the MDO can order a new DO instance as a service, anywhere needed. Finally, when the platform expanded to the new private domain, we showcase the dynamic discovery of resources in that domain, rendering the domain "orchestratable" in a few seconds.
- Scenario #2 demonstrates how the service catalogs of the MDO and DO can be jointly leveraged to order complex end-to-end services that involve dynamic compute and 5G network resources, end user applications, and telemetry services altogether. These services are deployed across multiple domains in a fully-automated manner, while telemetry is exposed to the central domain in a secure and trusted manner (via encrypted tunnels of the platform's secure integration fabric).
- Scenario #3 showcases two types of SLAs. First, a security SLA enforced at the level of a private edge domain via the local orchestrator and secondly a smart performance SLA enforced at a multi-domain context. The latter SLA involved also predictive mechanisms (using Analytics) that allow timely forecasting SLA violations that give enough time to the platform to enforce remedy actions before the SLA gets violated.

Measurable outcomes

In the context of this PoC, we summarize a set of key measurements that highlight technical aspects of the three scenarios.

PoC KPI description	Measured PoC KPI value	Comment
Scenario #1: MDO expansion time to domain B	45 seconds	As shown in Scenario #1 video, this time includes pauses and some additional steps to explain every move to the consumer of the video; hence it can be easily cut down to at least half of the time (~20s). Nevertheless, this time is already impressive if you consider that it can take several hours to request and establish a traditional VPN, which was bypassed by this PoC due to the use of an equivalent platform that can establish VPNs in seconds.
Scenario #1: DO expansion time	13 seconds to onboard an existing compute cluster to host the new DO 32 seconds to fill in a service order for the DO on the MDO portal 30 seconds for getting the DO service order completed (i.e., DO successfully instantiated in domain B) Total time: 75 seconds	This time can be further reduced if we automate steps 1 and 2 via gitops. We did not do that in the video to make the demo more user friendly.
Scenario #1: Degree of Automation	64%	7/11 steps of this scenario were fully-automated, while the rest were greatly facilitated by a user-friendly portal. More than 90% of Automation would be possible if we were to sacrifice security (which was not desired).
Scenario #2: Service Ordering Time for a dynamic compute fabric (Kubernetes-as-a-Service over dynamically created OpenStack VMs)	9 minutes and 4 seconds	For a Kubernetes cluster with 1 master node and 1 worker node. Includes the time to spawn new VMs as well.
Scenario #2: Service Ordering Time over a dynamic 5G fabric.	5 minutes and 14 seconds	For a full 5G system with one Amarisoft gNB configured for an indoor environment and a containerized 5GC deployment
Scenario #2: End-user service provisioning time (FIDEGAD 5G streaming server) over existing compute cluster	11 seconds	Including time for the MDO (Maestro) to (i) process the request from the TMF API, (ii) log-in to a private registry where the end user application helm package was stored, (iii) pull the service package, (iv) validate the service package, and finally (v) deploy it on the target K8s cluster
Scenario #2: End-user telemetry provisioning time	3.5 seconds 300ms	for MDO (Maestro) to federate service metrics from the K8s cluster in the Patras domain (where the service was deployed) to the central telemetry engine for the MDO (Maestro) Telemetry service to create service metric dashboards on Grafana
Scenario #2: Degree of Automation	75%	9/12 steps of this scenario were fully-automated, while the rest were greatly facilitated by a user-friendly portal. 100% of Automation would be possible if we: - statically synchronized the DO#2 catalogs onto Maestro - delegated service orders to a gitops platform (this would decrease user experience though)
Scenario #3A: Degree of Automation of Security SLA provisioning	75%	3/4 steps of this scenario were fully-automated, while the rest was greatly facilitated by a user-friendly portal. 100% of Automation would be possible using gitops, but we opted for an explicit user-triggered SLA request

Scenario #3B: Degree of Automation of Performance SLA provisioning	86 %	6/7 steps of this scenario were fully-automated, while the rest were greatly facilitated by a user-friendly portal. 100% of Automation would be possible using gitops, but we opted for an explicit user-triggered SLA request

PoC open-source components

Component name	Open-source repository link	Partner(s)/Community(ies) behind this component
Maestro: Multi-domain service orchestrator [7]	https://maestro-mkdocs.readthedocs.io/ (Soon under ETSI OSL)	UBI
ETSI OpenSlice Operations Support System (OSS) for Network-as-a-Service [8]	https://osl.etsi.org/	ETSI OSL community. UOP, PNET, and UBI contributed to OSL throughout the ACROSS project
ETSI Open-Source MANO NFV Orchestrator [9]	https://osm.etsi.org/	ETSI OSM community. UOP undertook the integration of OSM in this PoC
ETSI TeraFlowSDN controller [10]	https://tfs.etsi.org/	ETSI TFS community. CTTC, UBI, TID contributed to TFS throughout the ACROSS project
OpenZiti Programmable platform for Zero-Trust Networking [11]	https://openziti.io/	OpenZiti community. NOVA and UBITECH undertook the integration of OpenZiti in this PoC
Open Security and Trust Orchestrator (OpenSTO) [12]	https://github.com/CTTC-PONS/OpenSTO	CTTC
Analytics training and inference service for SLA forecasting	To be released soon by the ACROSS project	K3Y
TMF-compliant Automation service for SLA preservation	To be released soon by the ACROSS project	WINGS, LMI

Key messages for ZSM

- The Security Center and Security Gateway components of the PoC are fully aligned with the concept of the ETSI ZSM Integration Fabric as per the ETSI GS ZSM 002 v1.1.1 (2019-08): "Zero-touch network and Service Management (ZSM); Reference Architecture" [2].
    - The proposed approach goes one step beyond by adding security and trust by design, leveraging the OpenZiti platform [11].
- The proposed end-to-end (compute, 5G, telemetry, end-user) service provisioning approach is fully aligned with ETSI GS ZSM 003 v1.1.1 (2021-06): "Zero-touch network and Service Management (ZSM); End-to-end management and orchestration of network slicing" [4].
- The proposed NDT environment approach is aligned with ETSI GS ZSM 018 v1.1.1 (2024-12): "Zero-touch network and Service Management (ZSM); Network Digital Twin for enhanced zero-touch network and service management" [6].

Future Work

Tighter integration between the orchestration platform and the NDT could be studied in the future. Specifically, An AI model drift detector could be: (a) linked with a real service in a domain via the Secure Integration Fabric, (b) detect data drift of existing AI models in real-time, (c) ask NDT to re-train the model with additional data, (d) rollout (hot swapping) a new version of the model in the real system for increasing its accuracy.

2.3.2 Acknowledgements

This work is jointly funded by the European Commission through (i) the HORIZON-JU-SNS-2022 **ACROSS** project [1] with Grant Agreement number 101097122 and (ii) the HORIZON-CL4-2024-DATA-01-03 **COP-PILOT** project [16] with Grant Agreement number 101189819.

Specifically, this entire PoC comprises Test Case 4 of the ACROSS project, which had originally (since the proposal time) planned to contribute this test case as a PoC to ETSI ZSM. COP-PILOT is a new CL4 Innovation Action project that leverages the ACROSS platform as a baseline to accommodate large scale trials across 4 clusters of testbeds across Europe, thus attempt to elevate the ACROSS platform's TRL to close-to-market levels. The fact that this PoC is entirely based on open-source community projects, some of which are Software Development Groups under ETSI, makes the proposed platform a suitable framework for building up a growing ecosystem, where software development communities (from EU consortia, SMEs, industries, and/or universities) contribute towards a preliminary 6G-ready orchestration platform.

3 References

The references used throughout this document are listed below:

[1]. ACROSS HEU project, Available: https://across-he.eu/
[2]. ETSI GS ZSM 002 v1.1.1 (2019-08): "Zero-touch network and Service Management (ZSM); Reference Architecture", Available: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/002/01.01.01_60/gs_ZSM002v010101p.pdf
[3]. ETSI GS ZSM 001 v1.1.1 (2019-10): "Zero-touch network and Service Management (ZSM); Requirements based on documented scenarios", Available: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/001/01.01.01_60/gs_ZSM001v010101p.pdf
[4]. ETSI GS ZSM 003 v1.1.1 (2021-06): "Zero-touch network and Service Management (ZSM); End-to-end management and orchestration of network slicing", Available: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/003/01.01.01_60/gs_ZSM003v010101p.pdf
[5]. ETSI GS ZSM 008 v1.1.1 (2022-07): "Zero-touch network and Service Management (ZSM); Cross-domain E2E service lifecycle management", Available: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/008/01.01.01_60/gs_ZSM008v010101p.pdf
[6]. ETSI GS ZSM 018 v1.1.1 (2024-12): "Zero-touch network and Service Management (ZSM); Network Digital Twin for enhanced zero-touch network and service management", Available: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/018/01.01.01_60/gs_ZSM018v010101p.pdf
[7]. Maestro end-to-end service orchestration platform, Available: https://maestro-mkdocs.readthedocs.io/
[8]. ETSI OpenSlice (OSL), Available: https://osl.etsi.org
[9]. ETSI Open-Source MANO (OSM), Available: https://osm.etsi.org
[10]. ETSI TeraFlowSDN (TFS), Available: https://tfs.etsi.org
[11]. OpenZiti, "Cloak Your Network. Secure Services not IPs", Available: https://openziti.io/
[12]. OpenSTO — Open Security & Trust Orchestrator: https://github.com/CTTC-PONS/OpenSTO
[13]. Proxmox, "Powerful open-source server solutions", Available: https://www.proxmox.com/
[14]. OpenStack, "Open-Source Cloud Computing Infrastructure", Available: https://www.openstack.org/
[15]. HashiCorp, "Terraform: Automate Infrastructure on Any Cloud", Available: https://developer.hashicorp.com/terraform
[16]. COP-PILOT EU project, Available: https://cop-pilot.eu/