5GZORRO

Grant Agreement 871533

H2020 Call identifier: H2020-ICT-2019-2

Topic: ICT-20-2019-2020 - 5G Long Term Evolution

D2.4: Final design of the 5GZORRO Platform for Security & Trust

Dissemination Level		
☒	PU	Public
☐	PP	Restricted to other programme participants (including the Commission Services)
☐	RE	Restricted to a group specified by the consortium (including the Commission Services)
☐	CO	Confidential, only for members of the consortium (including the Commission Services)

Grant Agreement no:	Project Acronym:	Project title:
871533	**5GZORRO**	**zero-touch security and trust for ubiquitous computing and connectivity in 5G networks.**

Lead Beneficiary:	Document version:
NXW	**V1.0**

Work package:
WP2 – Use Case Definition, Requirements & Architecture

Deliverable title:
D2.4: Final design of the 5GZORRO Platform for Security & Trust

Start date of the project:	Contractual delivery date:	Actual delivery date:
01/11/2019 **(Duration 36 months)**	**31/03/2022**	**12/04/2022**

Editor(s)
G. Bernini (NXW), P. G. Giardina (NXW)

List of Contributors

Participant	Short Name	Contributor
Nextworks	NXW	G. Bernini, P.G. Giardina, J. Brenes, E. Bucchianeri, M. De Angelis
Fundaciò i2CAT	I2CAT	C. Herranz, A. Fernandez, M. S. Siddiqui, Javier Fernandez
IBM Israel Science and Technology	IBM	D. Breitgand, K. Barabash
Telefonica Investigacion y Desarrollo	TID	Diego R. López
Ubiwhere	UW	F. Martins, C. Jorge, F. Santos
Fondazione Bruno Kessler	FBK	R. Behravesh
Universidad de Murcia	UMU	J.M. Jorquera Valero, P.M. Sanchez Behaves, M. Gil Perez, G. Martinez Perez
Altice Labs	ALB	B. Santos, A. Gomes
Intracom	ICOM	D. Laskaratos, A. S. Valantasis, A. Erspamer, V. Theodorou
Atos Spain	ATOS	G. Gomez
Malta Communications Authority	MCA	A. Sciberras

List of Reviewers

Participant	Short Name	Contributor
IBM Israel Science and Technology	IBM	K. Barabash
Altice Labs	ALB	B. Santos
Fundaciò i2CAT	I2CAT	M. S. Siddiqui

DISCLAIMER OF WARRANTIES

This document has been prepared by 5GZORRO project partners as an account of work carried out within the framework of the contract no 871533.

Neither Project Coordinator, nor any signatory party of 5GZORRO Project Consortium Agreement, nor any person acting on behalf of any of them:

- makes any warranty or representation whatsoever, express or implied,
  - with respect to the use of any information, apparatus, method, process, or similar item disclosed in this document, including merchantability and fitness for a particular purpose, or
  - that such use does not infringe on or interfere with privately owned rights, including any party's intellectual property, or
- that this document is suitable to any particular user's circumstance; or
- assumes responsibility for any damages or other liability whatsoever (including any consequential damages, even if Project Coordinator or any representative of a signatory party of the 5GZORRO Project Consortium Agreement, has been advised of the possibility of such damages) resulting from your selection or use of this document or any information, apparatus, method, process, or similar item disclosed in this document.

5GZORRO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871533. The content of this deliverable does not reflect the official opinion of the European Union. Responsibility for the information and views expressed in the deliverable lies entirely with the author(s).

Table of Contents

List of Tables

List of Figures

Executive Summary

The full achievement of 5G networks and service agility and pervasiveness calls for defining the more disruptive approaches for 5G network operation, that in turn requires a pervasive integration of latest innovative technologies for resource and spectrum sharing, network orchestration, end-to-end security and trust. Following this direction, three novel design principles are emerging in the 5G industrial and research communities. First is Artificial Intelligence (AI), which can transform network management into a cognitive process through which the network can self-adapt and self-react to changing conditions with minimal manual intervention (zero-touch). Second, Distributed Ledger Technologies (DLT)/Blockchains (BC) can be adopted to implement distributed security and trust across the various parties involved in the 5G service chain. Third, Cloud Native technologies allow to achieve the necessary level of flexibility, scalability, and resilience of SDN/NFV-based services for 5G. These three technologies, coupled with the advancement of the 5G specifications at 3GPP, can ensure the needed efficient delivery of cutting-edge 5G services.

Moreover, the quest for pervasiveness of 5G network services in an affordable way for Telcos who are called to build new infrastructures with very dense footprints (e.g., in cities, in industrial districts, in high aggregation areas like shopping districts, hospitals, etc.), calls for overcoming of the bilateral Business-to-Business (B2B) models traditionally adopted by operators for sharing passive infrastructure elements and governing roaming agreements.

5GZORRO envisions a **multi-party distributed model** for building 5G Networks which can involve Telcos, spectrum owners, infrastructure owners, technology providers and Verticals, who can establish cross-domain service chains with security and trust.

This document presents the final design of the ***5GZORRO high-level architecture***, which targets the achievement and implementation of the innovative 5G networks and services vision described above. More specifically, this deliverable is intended as a self-contained document, which merges the original content of deliverables D2.2 and D2.3 (that present the initial and the updated 5GZORRO high-level architecture respectively) and further improves them to align the 5GZORRO architecture functionalities with the feedback from the platform implementation undergoing in WP3 and WP4. With this document, the goal is to have a single source of information for the 5GZORRO high-level architecture, which includes the whole set of services offered, functionalities supported, and operational workflows implemented.

In practice, in alignment with the original approach proposed and described in D2.2 and D2.3, the architecture follows a principle of service-based architecture, similar to the 5G Service-based architecture defined in 3GPP and in the ETSI Zero touch network and Service Management. Integrating SDN/NFV and Cloud native orchestration technologies with a Permissioned Distributed Ledger infrastructure, the 5GZORRO architecture offers services for:

- cross-domain network slicing,
- resource and service offering via marketplaces,
- discovery, intelligent selection and trading of resources and Services via Smart Contracts
- zero-touch network slice and service lifecycle management
- cross-stakeholder e-license management
- SLA monitoring & breach prediction
- security and trust across multiple domains.

The realization of these services is made possible through the interaction of various functions for slice orchestration, network intelligence and analytics, security and trust, management of virtualized resources, all executed for multi-domain and single domain scopes. Moreover, 5GZORRO leverages many state-of-the-art technologies and standards for virtualization, NFV, Cloud Native platforms and services, zero touch, SDN, distributed ledgers, data lakes, which have been extensively reviewed to summarise the specific positioning of the 5GZORRO innovative proposition.

The 5GZORRO architecture implements the concept of sharing operational data across the whole system in a logically centralized data reservoir (a.k.a. Data Lake), so that multiple asynchronous management components and analytics agents may act upon this shared data pool towards optimizing a target set of KPIs. The ***5GZORRO Operational Data Lake*** component serves as a logically centralized reservoir of all the operational data, channelled by management services running in stakeholder domain, and it provides APIs for adding, processing (in place) and retrieving data for analytical processes. A ***5GZORRO Permissioned Distributed Ledger*** component allows to implement Smart Contracts among the parties for 5G network services and slices, and ensures interoperability by providing data governance, multi-party trust, and accounting for data usage by different participating parties.

This document first describes the **5GZORRO concept and offered services**, which are imported as-is from deliverable D2.2 for the sake of completeness of this final design deliverable. Next, the 5GZORRO high-level architecture is presented as an update of the building blocks and core functionalities from D2.2 and D2.3. Indeed, most of the **architecture functional blocks** descriptions have been revised to reflect their final design, resulting from the feedback coming from the platform implementation and validation activities. These include details on the services they offer and expose, by identifying the envisaged functionality, its level of support (i.e., M-mandatory, O-Optional) and scope (i.e., cross-domain of intra-domain). The document also provides the final high-level design of the software platforms that group the various 5GZORRO functionalities and services according to their scope and offered features and realize the overall **5GZORRO software platform**. Similarly, the document also reviews the **operational patterns** defined in D2.2 and D2.3, aiming at providing a final set of workflows to describe how the various components in the 5GZORRO platforms interact for publishing resource offers, for trustworthy resource discovery, for smart contract setup with spectrum, edge/core resources and network slices.

1 Introduction

Despite enormous progress achieved during recent years, current 5G deployments are still far from reaching the level of maturity needed to address all the requirements from the vertical industries. A partial support to the network slicing and network monitoring, with limited possibility to establish a cross-operator end-to-end slice, and a very limited support of the ITU-T 5G vertical applications other than eMBB (e.g., URLLC and mMTC) represent a significant barrier to the achievement of full 5G potential. One main cause resides in the way the network, its actors (mainly telco operators) and the business relationships among them have been considered so far. In fact, current business relationships between Telcos, infrastructure owners and regulators are based on bilateral agreements, intended mainly for enabling roaming and sharing of passive infrastructure elements, which practically represent the only negotiated resource. Further, such kind of agreements are often negotiated offline between the involved parties and they take a long time to be defined and finally deployed in the network environment. This results into a general difficulty and lack of efficiency in establishing end-to-end services based on resources other than those in passive infrastructure, across different providers, with a subsequent limited capacity of the current 5G operators to become truly pervasive with their service offering.

This document describes the final design of the 5GZORRO high-level architecture, and aims at specifying such a framework, characterized by services and tools enabling the network stakeholders to offer, select and trade the resources, slices and services from different providers and to establish business relationships exploiting automatic and secure procedures.

It is worth to highlight that this document merges the content of deliverables D2.2 [2] and D2.3 [3], which provided the initial and updated design of the 5GZORRO architecture respectively, and integrates it with additional details and feedbacks from the software implementation and experimental validation activities carried out in the project. In practice, this document is intended to be the final outcome of the 5GZORRO architecture design work, and therefore includes all those updates to the architecture functional blocks, provided services, high-level software platforms design, operational patterns that are finally supported by the 5GZORRO architecture. In practice, this means that only part of this document includes new text and content, while some specific parts are imported as-is from D2.2 and D2.3 for the sake of completeness of this deliverable.

In particular, most of the new material is included in section 5 for the description of the final capabilities and services provided by the various functional blocks in the 5GZORRO high-level architecture. In addition, the 5GZORRO software platform design in section 6 also provides updated content, mostly in terms of specification of the main reference points among the various components and platforms, with the aim of having a clear picture of which interactions occur through which interface. Finally, section 7 is also updated to provide a final description of the 5GZORRO platform operational patterns, in support of scenarios such as marketplace onboarding operations, smart contract lifecycle management, slice orchestration, e-licensing management and control, SLA monitoring and breach prediction, and intelligent slice optimization.

1.1 Document outline

This document is structured as follows:

- Section 2 describes the concepts and the innovations 5GZORRO aims to introduce and the technologies enabling these solutions. This section is imported as-is from deliverable D2.2 and is included for the sake of completeness of this document.
- Section 3 details the services offered by the 5GZORRO architecture supporting the benefits mentioned above. This section is imported as-is from deliverable D2.2 and is included for the sake of completeness of this document.
- Section 4 describes the reference architectures, technologies, and standards on top of which the 5GZORRO concept is built. This section is imported as-is from deliverable D2.2 and is included for the

sake of completeness of this document. The extensive review of the state-of-the-art can be found in Appendix I of D2.2, structured in four main areas: Intelligent zero-touch management, Cross-domain resource & service trading, Security & Trust and Technology enablers.

- Section 5 presents the 5GZORRO architecture design principles, and provides the 5GZORRO high-level architecture description, together with a detailed specification of provided services and offered capabilities for each of the functional blocks. This section combines and updates the content of D2.2 and D2.3, bringing it up to date with the final design of the 5GZORRO high-level architecture.
- Section 6 establishes the 5GZORRO platform software design principles and provides the final software architecture design by grouping the functional blocks in different inter-working software platforms. This section is mostly imported from D2.2, and updates it with new material related to the identification of main reference points and interactions among the platform components.
- Section 7 illustrates how the 5GZORRO functional elements interact in the most relevant operation patterns that cover the main services and capabilities offered by the 5GZORRO platform. This section is also a merge of D2.2 and D2.3 contents, with relevant updates in some operational patterns to reflect the final workflows and interactions supported in 5GZORRO.
- Section 8 concludes the document providing a table where the project KPIs are mapped to the sections of this document in which the handling of the specific KPI is covered.
- Section 9 and Section 10 provide references and abbreviations, respectively

2 5GZORRO Concept

5GZORRO incorporates solutions based on three novel concepts:

i) Data-driven and AI-based solutions which can enable automatic and autonomous network operations following AIOps paradigm;
ii) Distributed Ledger Technologies (DLT) which enable trust and security in multi-party end-to-end service/slice implementation
iii) Cloud-Native technologies which once integrated into SDN/NFV environments can increase the level of flexibility required by advanced 5G based services (e.g., scalability, resilience).

The combination of these three concepts is the basis for realization of the three main 5GZORRO innovations, briefly summarized in the following.

Zero-touch/Automated Resource discovery using DLT/Blockchains. The automatic (zero-touch) resource discovery is based on the extensive use of AIOps and DLT solutions. The main goal is, from the one hand, to allow different stakeholders to publish their own resource/service offerings and, from the other hand, to enable the business logic to automatically discover the most suitable set of resources while minimizing the human intervention. For the resource/service trading, 5GZORRO offers a set of modules that build a proper Marketplace Application (described in Section 6.5), where the business agent can discover and classify the available resources and services. Each resource/service offering published into the Marketplace, is stored into the blockchain and becomes immutable, facilitating the process of discovery and classification and making it secure from a business point of view. The discovery and classification process can be hence completely automatized (zero-touch), directly affecting the way the various parties establish business relationships: offerings are clear, immutable and need no human interaction and/or offline negotiations. Further, the concept of Marketplace enlarges the set of network resources and extends it to abstractions like services and slices, opening the door to a new generation of network stakeholders beyond classical Telcos.

Intelligent 3rd party resource selection, request and access/usage. Once resources have been made available on the DLT-based resource catalogue and automatically discovered and classified, an automatic AI-based process can select the most suitable ones, request them from the owners and, after the business transaction has been fixed into the DLT, finally use them. The decision process is driven by analysing the historical information stored into the operational Data Lake, like costs and KPIs. Static rules can be set manually by the potential resource consumer that can act as a pre-filter, reducing the set of resources the AI-based agents can use for selection. The transactions are stored in the form of Smart Contracts, legally binding, automatically generated by the Platform when resources/services are requested for deployment, that also happen automatically. This last aspect involves also the lifecycle management of the resources/services, not only the deployment phase, but also of the configuration and the optimization of the service based on the resource selected whose conditions are fixed into the smart contract. In particular, the Intelligent 3rd Party resource selection heavily applies the zero-touch management paradigm that guarantees that different resources/services offered by different providers (administrative domains) can be seamlessly composed (service creation/service stitching) across the different domains. AI-based mechanisms apply the correct configuration of the services/resources while guaranteeing that the Service Level Agreement is properly applied in all of the parts of the service chain belonging to all the different domains. Special SLA monitoring mechanisms are implemented to react in case of SLA breaching. The application of the zero-touch paradigm dramatically reduces the time of resource/service negotiation between the involved parties: everything happens in an automatic way, from the selection of the resources, to the deployment of the services, passing through all the business and legal aspects.

Trust establishment among multiple parties. In view of enabling the automatic establishment of business relationships, 5GZORRO offers a mechanism that guarantees the trust and the security among the parties involved, with end-to-end security for the deployed services. Each stakeholder that wants to deploy a slice/service needs to be sure that all the resources/services provided by the 5GZORRO framework are secure and provided by trusted sources. The level of security and trust of each party is established in the smart contracts between the parties.

In Figure 2-1 it is depicted how different business parties can take advantage of the 5GZORRO framework innovations to offer different resources and to establish multi-party end-to-end services.

Figure 2-1: zero-touch/Automated Resource discovery (1), Intelligent 3rd party resource selection, request and access/usage (2) and Trust establishment among multiple parties (3) in 5GZORRO.

As first step (see spot 1 in Figure 2-1), Operators use 5GZORRO DLT-Based marketplace to publish and to check for new resources (*zero-touch/Automated Resource discovery using DLT/BC*). In order to build a cross-operator service, the framework intelligence automatically selects proper resources (see spot 2 - *Intelligent 3rd party resource selection*) whose usage and chaining is automatically formalized through the mechanism of the Smart Contracts (see spot 3 - *Trust establishment among multiple parties*).

A more detailed discussion can be found in D2.1 [1] where all of the 3 innovation concepts are planned and validated in representative use cases.

3 5GZORRO Services

The core 5GZORRO services are introduced in this section detailing principles and core concepts for

- cross-domain network slicing,
- resource and service offering via marketplaces,
- discovery, intelligent selection and trading of resources and Services via Smart Contracts,
- zero-touch network slice and service lifecycle management,
- cross-stakeholder e-license management,
- SLA monitoring & breach prediction,
- security and trust across multiple domains.

3.1 Cross-domain network slicing

3.1.1 Concept of multi domain slice and relevant scenarios

In the 5G vision, a high degree of reutilization of the infrastructure resources in order to overcome the elevated costs of investment and operation of the computing, transport, and radio resources. In a similar manner, it is envisioned that end-to-end services will traverse multiple geographical areas and will have varying demands in terms of edge resources, which are by definition scarce and hence it is unlikely that one single network operator will have enough resources to satisfy all the demand. Therefore, 5G network services and management platforms shall support mechanisms to enable flexible and on-demand resource sharing across multiple administrative domains and across different segments of the network.

The 5GZORRO architecture specifically aims to offer a set of interfaces to enable the transparent deployment of services relying on resources belonging to different network operators, infrastructure providers, etc. For this we leverage on the network slicing concept introduced in 5G, where a Network Slice (NS) represents the complete logical network, offering specific services over a computing, network and storage infrastructure. A Network Slice Instance (NSI) in this context is the realization of a network slice targeting the specific service constraints. Figure 3-1 illustrates the 3GPP [4] concept on how NSIs can be used to support the end-to-end communication services and how NSIs are further divided into network slice subnet instances (NSSIs), which are shareable logical (sub)networks providing a specific functionality and the corresponding resources.

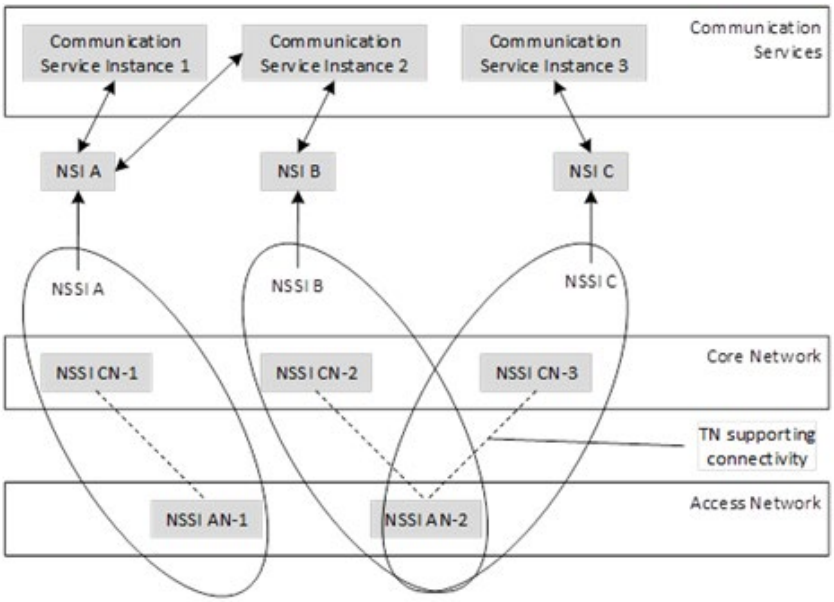

Figure 3-1: 3GPP concept of Network Slice Instance (source 3GPP) [4].

Figure 3-2 illustrates how an NS concept is mapped to the multi domain environment of 5GZORRO using a resource-oriented view of the most representative service deployment scenarios of the project.

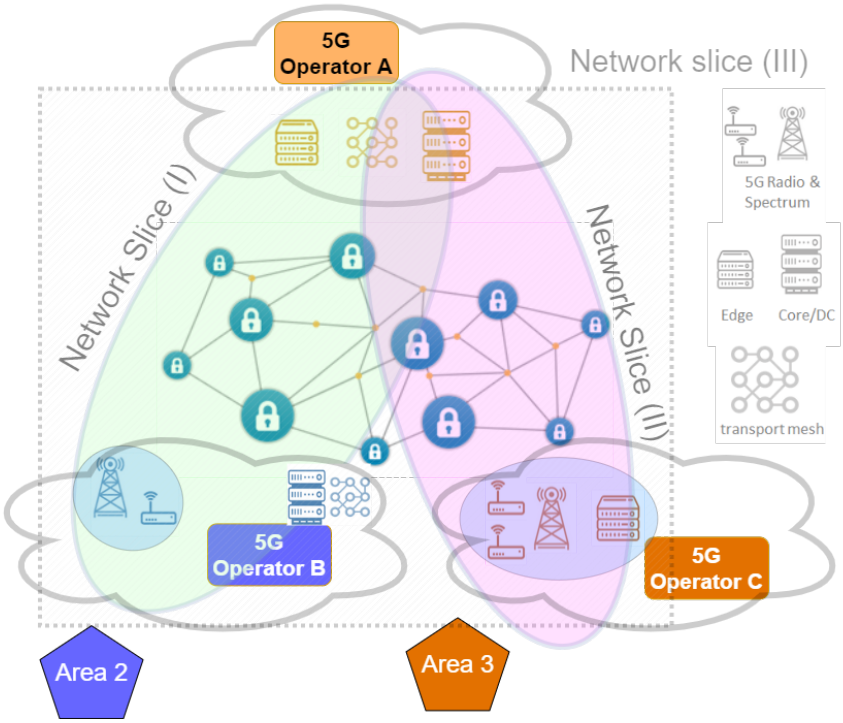

Figure 3-2: 5GZORRO Network slicing scenarios.

The three scenarios depicted in the picture are:

- '*Multi domain RAN*': as represented in Network Slice (I) the service is deployed using slice relying on core, edge and RAN resources from operator 'A' and RAN and spectrum resources from operator 'B', probably due to the coverage constraints of the service. Since operator 'A' does not have the means to offer the service in 'Area 2', the RAN and spectrum resources shall be acquired using the 5GZORRO Marketplace. It is important to highlight that the RAN and spectrum resources could even be provided by different parties;
- '*Multi domain RAN and edge*': as in the previous case the core functionalities and resources are provided by operator 'A', but in this case the edge, RAN and spectrum resources are provided by operator 'C'. This is the typical scenario of industrial facilities, where it is foreseeable private deployments of 5G RAN and edge infrastructure will appear in the near future to accommodate latency sensitive service on the edge;
- '*Dynamic edge and RAN allocation*': in this scenario, the network slice is dynamically scaled to accommodate new RAN, edge and spectrum resources due to a change in the service constraints. In this scenario, the slice can start as in Network Slice (I) and be scaled dynamically to embrace the resources used in Network Slice (II) (as represented in Network Slice (III)). This scenario represents the case where the terminals, using latency sensitive services, are expected to move across different areas.

From perspective of the logical functionality, the network slices will leverage also other types of 3rd party resources available on the market (i.e., VNFs)

It is clear that in all the scenarios, the requirements and constraints for the different segments (e.g., Cloud/Edge, RAN, Transport, etc) could be different. Similarly, the different sections will offer different kinds of information that the ML/AI algorithms could use to derive the orchestration decisions. In the following subsections we detail the specifics of each segment.

3.1.2 Generic Network Slice template & abstract parameters

A Generic Network Slice Template (GST) defined by GSMA in [5] is a set of attributes that can characterise a type of network slice/service. A GST where attributes are filled with desired values of a Network Slice is called Network Slice Template (NEST). The NEST is used for instantiating the Network Slice
Instance (NSI) and one or more NSIs can be created from the same NEST. The Table 3-1 describes a subset of relevant attributes of GST.

Table 3-1: Relevant attributes of a Generic Network Slice Template (GST).

NAME	DESCRIPTION
Area of service	Specifies the area where the terminals can access a particular network slice
Delay tolerance	Describes service delivery flexibility, if supported
Downlink throughput per network slice (guaranteed)	Describes the guaranteed data rate supported by the network slice in downlink
Downlink throughput per network slice (maximum)	Defines the maximum data rate supported by the network slice for all UEs together in downlink
Downlink throughput per UE (maximum)	Describes the maximum data rate supported by the network slice per UE in downlink, it could be used to offer different contract qualities
Isolation level	Describes different types of isolation
Maximum supported packet size	Describes the maximum packet size supported by the network slice and may be important for URLLC (Ultra-Reliable Low Latency Communication) and MIoT (Massive IoT), or to indicate a supported maximum transmission unit (MTU)
Radio spectrum	Defines the radio spectrum supported by the network slice. This is important information, as some terminals might be restricted in terms of frequencies to be used
Slice quality of service parameters	Defines all the QoS relevant parameters supported by the network slice. For some of these parameters 3GPP has already defined standard values in [6]
Supported device velocity	Defines the maximum speed supported by the network slice
UE density	Describes the maximum number of connected and/or accessible devices per unit area (per km2) supported by the network slice
Uplink throughput per network slice (guaranteed)	Describes the guaranteed data rate supported by the network slice in uplink (and not per user)
Uplink throughput per network slice (maximum)	Describes the maximum data rate supported by the network slice in uplink (and not per user)
Uplink throughput per UE (maximum)	The maximum data rate supported by the network slice per UE in uplink, it could be used to offer different contract qualities

According to 3GPP TS 28.541 [7], a Network Slice has a Slice/Service Type (SST) field to describe the expected network behaviour. There are three standardised values for SST described in Table 3-2. Each SST is defined by a set of additional parameters with standard values, listed in [7].

Table 3-2: Standardised SST (Slice/Service Type) values.

NAME	SST value	Description
eMBB	1	Slice suitable for the handling of 5G enhanced Mobile Broadband.
URLLC	2	Slice suitable for the handling of ultra- reliable low latency communications.
MIoT	3	Slice suitable for the handling of massive IoT.

The characteristics in network slice described by 3GPP using SST has reference in GSMA GST. Standardised SST values refer to Network Slice characteristics defined by GST attributes populated with standardised values.

3.1.3 Principles of mapping of network slices in RAN

At the time of instantiating a network slice, a set of computational and infrastructure resources are allocated in order to provide the agreed end-to-end service requirements. When the network slice involves a wireless or cellular network deployment, spectrum and radio infrastructure resources must also be allocated, thus creating a 'RAN slice'.

Typically, the end-to-end service does not define the radio access requirements and, consequently, there is a need to translate the service requirements to RAN resources. This translation logic is implemented at the RAN Controller in the 5GZORRO architecture. The RAN Controller takes some of the end-to-end service requirements of a network slice as input to create a 'RAN slice.' The input parameters include delay tolerance, maximum (guaranteed) throughput, UE density or number of simultaneous connections, type of service, available spectrum, and the area of service. With this information, the RAN Controller will deploy the necessary RAN resources in the geographical area of application of the service. The RAN resources devoted to the resulting 'RAN slice' is composed of a set of Access Points (AP) or cellular base stations and, for each of them, its radio access technology (e.g., Wi-Fi, LTE, 5G NR), a set of operation bands or channels, central operation frequencies, and operation bandwidths.

On top of this, the 'RAN slice' also determines the amount of total spectrum resources of each access point or cell allocated to a service. In particular, the global scheduler implementation in the 5GZORRO RAN Controller enforces that each slice obtains the necessary amount of spectrum resources to meet the service requirements. The RAN Controller enables the possibility to isolate slices, meaning that idle spectrum resources are not shared among slices. Once the global scheduler allocates spectrum resource to each slice, users within a slice are served following any of the wide-spread scheduling algorithms in the Wi-Fi APs or cellular base stations. The RAN slicing configuration is flexible so it can accommodate the addition or removal of slices or modify the amount of spectrum resources allocated to an active RAN slice.

The RAN Controller in the 5GZORRO may push to or collect data from the data lake in order to generate statistics, which can be used by a ML/AI model to determine the optimal radio configuration for a given type of service. For instance, the intelligence in the RAN Controller would favour the creation of a RAN slice with 5G resources for a service with a stringent low latency requirement with a given bandwidth based on the service requirements and statistics in the data lake.

3.1.4 Principles of mapping of Network slices in edge/core

The inclusion of edge/core infrastructure resources in network slices is a fundamental aspect in the creation of logical networks on top of common physical 5G infrastructures. Since a network slice instance is by nature purpose-built, business requirements related to edge/core resources need to be mapped into slice ingredients. In particular, compute, storage and/or hardware-based (e.g., GPU, TEE) capabilities as well as affinity rules, based for instance on geographical location or trust, are potential inputs to be taken into account for the setup of network slices. Moreover, core properties of network slicing such as guaranteed performance, isolation and reliability must be also ensured.

For network slices containing edge resources, a first level of slice mapping decisions could regard the selection of the appropriate Edge Point of Presence (PoP) on which to instantiate each slice subnet. Decision criteria could regard hard constrains, such as geographical coverage, end-users' location, infrastructure resources availability; as well as non-functional requirements about latency, throughput; and even reputation-based criteria.

In order to meet requested criteria and accommodate virtualized edge/core resources as part of network slices, translation rules need to be implemented as part of the slice provisioning and adaptation mechanisms. To do so, a common approach is to rely on a pure imperative scheme by specifically stating what edge/core resource chunks a slice needs to include. The use of monitoring data analytics coupled with ML/AI techniques

can be exploited to perform a more intelligent slice provisioning by stating what a slice needs to support and/or how a slice needs to perform. Likewise, by leveraging smart prediction mechanisms, potential problems can be anticipated and proactive actions can be taken accordingly to avoid reliability or performance degradation during the slice operation. In the scope of 5GZORRO, the combination of both schemes is foreseen, which allows not only to achieve a higher degree of customization and elasticity during the entire slice lifecycle but also to optimize the use of shared infrastructure resources.

3.2 Offer and resource catalogues

One of the key services offered by the 5GZORRO architecture is the marketplace service which enables the trading of resources. This will allow resource providers (i.e., infrastructure providers, network operators, NS providers, VNF providers, etc) to publish the resources they aim to trade along with the particular business and pricing conditions associated with the offer. Resource consumers (i.e., vertical companies), on the other hand, shall be able to query the market to acquire the resources needed by the service they aim to instantiate or modify.
In 5GZORRO, the approach used in [8] is used, where a resource market is mainly supported by three different catalogues: (i) the resource catalogue; (ii) the service catalogue (iii) the offer catalogue. The resource catalogue holds the inventory of the 5GZORRO available resources (VNF/CNF packages, NSDs, RAN elements, Spectrum resources).

In general terms, a resource entry shall contain: the type of resource, a reference to the specific resource definition, relationships with 3rd parties (i.e., owner, provider, etc) and a set of specification characteristics and configurable parameters. Due to the decentralized nature of 5GZORRO, the reference to the specific resource definitions, and all the catalogue entries shall contain a decentralized identifier (DID), as detailed in Section 3.7.1.

Resources are usually associated with service entries that detail how a resource can be consumed, instantiated or deployed. These service entries contain therefore: the set of resources associated, relationships with other service specifications, a set of service characteristics and agreements established for the service. In order to be available for use by other parties, services and resources need to be mapped into product offers. In broad terms, product offers contain a reference to the related services and resources, the pricing options and the agreements established for the offer. In 5GZORRO, the offers shall be also supported by smart contracts which ensure the cohesion and security across the multiple domains. 5GZORRO also relies on the DLT and smart contract capabilities to perform all the currency procedures. The 5GZORRO architecture is therefore agnostic to the specifics of the money transfers and billing mechanisms.

Service providers will be able to specify new services based on the services and resources available as product offers. When a new service is to be instantiated, the 5GZORRO Marketplace user will need to acquire the related resources, referring to the product offers available. The following sub-sections detail the specific offer and resource specification considerations for the most important assets within the project, and the high-level workflow to publish a new a resource offer.

For each type of offer specified in the following subsections, the resource provider – being it spectrum resource provider or edge/cloud infrastructure provider or RAN provider, etc) should create an offer containing:

- *Agreements*: the agreement between the parties, e.g., to exploit the licensed spectrum (auction), a pricing agreement between the resource provider and the resource consumer, etc. For example, the license/unlicensed spectrum bands, the set of base stations and their location, an agreement on using certain backhaul connections, an agreement on leasing baseband capacity for the antennas, an agreement on the percentage of resource to guarantee, etc.
- *Pricing models*: These models rely on input parameters (such as the SLA, the number of spectrum resources, etc), and determine the price using the 5GZORRO currency.
- *Business terms*: These are the terms for which the offer is valid. For example, the region of applicability, the specific frequency resources, the prohibition of reselling the spectrum, an

agreement not to exceed a determined transmission power, region of applicability, leasing time, expected total uptime, etc.

3.2.1 Spectrum offers

A Spectrum Resource Provider (SRP) in the 5GZORRO Marketplace can freely share their spare spectrum resources. Then, spectrum resource consumers can acquire the resources available in the Catalogue.

Before placing a spectrum offer in 5GZORRO, the SRP must get the recognition from the National Regulator as the legitimate owner of the claimed spectrum. Then, the Regulator will issue a spectoken for the SRP, which will be included in the spectrum offer. The owner of the spectoken is recognised in the 5GZORRO architecture as the sole operator of the frequency range defined in the spectoken.

In order to publish spectrum offers in the 5GZORRO Marketplace, the SRP will provide the spectrum details and the spectoken generated by the National Regulator. Both the offer and the spectoken refer to the same range of frequencies and geographical area.

3.2.2 RAN elements (active & passive) offers

Mobile Network Operators (MNO) and RAN infrastructure providers may share their RAN assets with resource consumers within the 5GZORRO architecture. To this aim, the RAN infrastructure providers put RAN infrastructure offers in the 5GZORRO Marketplace. The RAN resource consumers can acquire RAN elements by selecting the most appropriate offers in the 5GZORRO Catalogue.

3.2.3 Edge/Core Cloud resources (IaaS, PaaS) offers

Edge/core cloud infrastructure providers may offer their cloud or edge computing assets, such as CPU/GPU servers, storage, and networking, to resource consumers connected to the 5GZORRO Marketplace. To this aim, the edge/cloud infrastructure providers publish the edge/core cloud resource offers in the 5GZORRO Marketplace. The edge/core cloud resource consumer can browse the 5GZORRO catalogue and choose the most suitable offer for deploying their services.

3.2.4 VNF/CNF offers

Software vendors will be able to trade their VNFs/CNFs using the 5GZORRO Marketplace. Other software vendors will be able to use the VNF/CNFs in the Marketplace as part of their service, while end-users will be able to acquire the required VNF/CNF licenses based on the offers available.

In order to publish a VNF/CNF in the 5GZORRO Marketplace, Software Vendors will provide an identifier pointing to the VNF package or the CNF image. A resource entry will be created to register this asset containing: identifier, package/image format software version, package signature, configuration parameters, etc. A service entry will be created to detail how this VNF/CNF can be instantiated, identifying supported platforms, access points, etc.

3.2.4.1 Management of descriptors across multiple-domains

VNF vendors may offer their software products in the 5GZORRO marketplace, allowing other providers to compose services or slices with software products from diverse vendors, trading them in the marketplace. Resources and services will be published in the marketplace with a decentralized identifier (DID) associated, in order to unequivocally and globally identify the asset; this approach is discussed further in Section 3.3.1 .

The resource offer is composed by the business and legal offer definition, reflected in the smart contract and published in the DLT, but also by data content like descriptors, VIM endpoints, or VM/container images.

Sizeable binary data such as resource offer technical specifications will not be stored on the DLT as it may have scaling implications depending on the DLT implementation. Instead, this data will be stored 'off-chain' in traditional storage mechanisms e.g., database, a common optimisation technique used in conjunction with distributed ledgers. A minimal set of data attributes, including the DID of the offer and a cryptographic hash of the offer contents will be committed to the DLT. This will ensure that the amount of data stored on the ledger remains relatively small, and services are able to locate full offer meta-data from off-chain sources. Taking this approach will ensure that the DLT remains performant and the hash of the offer contents will

support non-repudiation of the offer contents itself; this will need to be updated each time an offer is updated in order to remain in sync.

Once the resource agreement is completed, the purchaser 5GZORRO platform will request the metadata associated to the offer through the universal resolution system. The resolution system will translate the DID to resolve the offer's metadata and its location in the whole ecosystem, making this data available for the resource/service roll out or modification.

3.2.5 Network Slice and Network Service Offers

Network Service (NS) providers will offer their Services through the 5GZORRO platform. Services themselves are defined by a composition of several embedded resources, potentially originated from multiple providers, that are required for their instantiation and execution, such as spectrum, software (one or multiple VNFs/CNFs), and hardware specifications.

To be able to publish a NS in the 5GZORRO Marketplace, the provider operator builds the service definition comprising the necessary resources resulting in the creation of a new smart contract that includes the service offered, the terms of service and pricing. After publishing of the document, the system verifies all aspects that pertain the validity of the service and, if all is correct, a smart contract is published in the 5GZORRO Marketplace rendering the Service available at the marketplace for consumption.

Network Slice providers will also be able to offer "slices" using the 5GZORRO platform. Network slices are composed by a set of resources, such as spectrum, computing and network resources. Although not enforced, Network Slice offers should be created alongside Network Service offers to accommodate their deployment. In other words, a Network Slice Instantiation (NSI) is typically devoted to accommodate a particular Network Service instantiation. Furthermore, given that the Network Service resources, as well as its requirements, are specified, the creation and publishing of a Network Slice Offer in 5GZORRO Marketplace is a relatively straightforward procedure.

3.3 Discovery, intelligent selection and trading (5GZORRO Marketplace)

3.3.1 Resource and Service discovery

The 5GZORRO system will serve as a decentralized marketplace whereby participants can freely trade resources and services without the need for a trusted intermediary. Each participant will host a distributed application (DApp) that interfaces with their domain's DLT node, forming a peer-to-peer (P2P) network consortium.

Providers will register resources and services via the marketplace using a standardised data format or schema in order to form a catalogue of items available to consumers. These resources and services can be seen as tokenised digital assets stored on the DLT, forming an immutable record of ownership and availability on the ledger that is tracked and updated over time in accordance with an associated Smart Contract that governs any state change; e.g., metadata update, or when leased to a particular consumer. By way of optimisation, metadata associated with an asset will be stored off-chain with just essential properties and a cryptographic hash of the resource definition being recorded on the ledger.

Resources & services will be universally identifiable and discoverable thanks to the employment of DIDs and Verifiable Claims. A DID can identify any subject such as a person, organisation, or thing. DLT is a key enabler for DIDs, which removes the need for a centralized registry or authority and empowers the controller of the DID to prove control over it without permission from a third party. The process of registering a resource or service will involve generating a DID and associated Verifiable Credential that describes associated cryptographic material, verification methods and service endpoints, allowing the owner (controller) to prove control over the resource and present any associated claims, and third parties to discover endpoints. This DID will be referenced in the tokenised state stored on the DLT and catalogue associated with the resource or service meaning that any participant can utilise the DID to query associated metadata.

When advertising a resource or a service, a provider will also associate legal prose with its definition. Prose will be generated from templates that are subject to a governance process, defining the legal framework and SLAs for the resource; Smart Contracts, derived from approved legal prose templates will facilitate the autonomous validation of actions made against the digital asset and management of the contract lifecycle in-line with the terms defined within.

The advertisement of resources or services by providers will be realised via automated mechanisms that will involve interfacing with their domain's management and/or orchestration entities. NFV MANO frameworks (e.g., OSM), edge orchestration platforms (such as Kubernetes lightweight distributions) or plain resource management entities will interwork with 5GZORRO platform in order to announce, register and update offers about available resources and services to the marketplace.

3.3.2 Intelligent 3rd party resource selection

The 5GZORRO architecture aims to facilitate multi-party collaboration in dynamic 5G environments where Operators and Service Providers often need to employ 3rd party resources to satisfy a contract. In 5GZORRO, there are several stages in the process of obtaining access to 3rd party resources.

As described above in Section 3.3.1, resource providers make their resources available for share by advertising them in 5GZORRO marketplace. The Cross-domain Monitoring and Analytics component keeps track of the resources available for sharing continuously over time, collecting the information that Smart Resource Discovery component can rely upon. Resource Consumers then use Smart Resource Discovery component to obtain the list of resources available and suitable to satisfy their need and to decide what 3rd party resources are the most appropriate to use. Upon making the choice, resource consumer initiates Smart Contract creation as described below in Section 3.3.3. When the agreement is sealed, 5GZORRO marketplace is updated about the new stratus of resources and offers catalogues.

For making decisions about what resources are the most appropriate to use in each particular case, Smart Resource Discovery component can rely on different data sources and algorithms: static considerations, e.g., performance and QoS characteristics, cost, historical or business preference for connecting to a certain provider, etc.; and dynamic considerations, e.g., current and predicted load and performance of relevant systems, components and services, topological network proximity of available resources to satisfy latency constraints, etc. While static considerations can be provided by the resource consumer as part of resource lookup request, dynamic considerations can only be computed using data collected at runtime. To achieve the latter, Smart Resource Discovery component will use streamed and historical data of 5GZORRO Operational Data-lake and Machine Learning algorithms to create, train, and validate models for each specific resource usage case. For example, network topology awareness can be infused into Smart Resource Discovery component by correlating the reported service QoS with monitored network characteristics such as technology, provider, proximity, hop-to-hop latency, etc., over historical data across many similar past resource usage contracts.

Of course, it must be noted that making data-based decisions in production business environments requires that all the data taken into consideration is trustworthy at all stages – at collection, transmission, transformations, computation, etc., putting strict security requirements on 5GZORRO AIOps platform. This ties in with architectural decisions already made by 5GZORRO team: incorporate Smart Contracts, DLT, and Trusted Execution Environments (TEEs) to ensure multi-party trust to ensure the data is verifiably authentic, traceable to its source, and not tampered with while in transfer or in processing.

3.3.3 Resource and Service trading via Smart Contracts

Creating a commercial trading agreement between provider and consumer autonomously will be facilitated through smart contracts. Smart contracts ensure that an agreement and any associated actions on that agreement are processed in accordance with the agreed terms by validating any transition of ledger state. What this means is that on entering into an agreement, whereby each party agrees terms and signs the transaction, from that point on there is a commercial agreement between the two legally identifiable entities backed by a legally enforceable contract (Ricardian Contract [9]).

Smart Contract templates will be developed to capture both the broader general terms of an agreement, and operational terms relating to a Service Level Objective (SLO), with specialized templates to serve the needs of each resource type to be traded as necessary. These templates will consist of parametrised legal prose to be utilised by stakeholders, crucially encapsulating real-world legally ratified contracts. Smart contract templates will give rise to legally enforceable smart contracts, but also the compelling improvement over existing working practices by standardising contract terms across all stakeholders.

Resource and service business meta-data will comprise concrete instantiations of these templates, producing a hierarchy of terms that outline the legal terms of the agreement, SLAs and their associated SLOs.

These agreements will be deployed and managed by a component that manages the lifecycle events of the contract. Smart Contracts will mirror that of the real-world contract and encapsulate logic to automate the calculation of SLA compliance. On deployment of the contract to the ledger, the autonomous set-up of monitoring and configuration of aggregation algorithms will be initiated by the Smart Contract Lifecycle Manager. During the course of the contract's lifetime, metrics can be posted to the smart contract by the monitoring aggregation service and at frequencies as agreed in the contract. Should a breach occur, the Smart Contract will enact any subsequent events, which might simply be to record the breach until such time that a threshold is reached or trigger the termination of the contract.

Smart contracts are ultimately providing autonomous near real-time execution of contract lifecycle stages, from creation, monitoring & SLA enforcement through to settlement, disbursement and finally termination.

3.4 Zero-touch lifecycle management for network slices and network services

This sub-section describes how 5GZORRO will deal with the zero-touch concept for life-cycle management of the Network Slices and/or Network Service, especially when cross-operator aspects of it are addressed.

3.4.1 Cross-Domain Network Slice Lifecycle Management

Achieving zero-touch Network Slice life-cycle management is in itself particularly challenging, even when just within the domain of a single operator. But in 5GZORRO we believe we can handle this challenge if we adopt some tools and processes, as described next.

The context for the following text is:

> *we want a Network Slice to be instantiated and managed (i.e., expanded, re-configured, etc.), cross domain (e.g., expand only its radio part, or its edge computing, only 5G connectivity, etc.) and even cross-operator.*

As illustrated in Figure 3-2, multiple types of resources of a slice (core, edge, RAN & spectrum) might be subject to these lifecycle operations, with the added complexity that these resources could either belong or be managed by more than one operator. In this scenario, specific interactions between the owners/managers of those resources must take place.

5GZORRO uses a DID/DLT mechanism to uniquely identify these different resources, even when they are described in a distributed manner (see sub-section 3.2, above). These descriptors are extended with the interconnection data mentioned above, thus allowing for a far more extensive scope of a Slice Descriptor, e.g., to include RAN, spectrum and other relevant resource components of the concrete slicing implementation.
Please note that those service provider-specific credentials should cover the whole Network Slice lifecycle. If a service provider does not have the capability to expose certain parts of the Network Slice lifecycle, this must be known right at the Network Slice definition phase, since it limits further actions on subsequent phases.

3.4.1.1 Network Slice instantiation

With a clear and complete Network Slice Descriptor, its instantiation should be fairly simple: it implies negotiating with every Network Service provider that provides each of the Network Services that are part of the slice, the instantiation of that service and its connection to the other services.

3.4.1.2 Network Slice expansion/reduction

Expanding/reducing a slice can mean different things, some of them simultaneously within a single use case, which we address below:

- Expanding/reducing the capability of each one of the Network Services comprising the slice: in this scenario, more/less instances of the same Network Service might be added/reduced, depending on more or less complex licensing schemas (see below, the sub-section about licensing), and inter-connected/disconnected. This can be seen as a scaling-out scenario of the Network Services. An alternative to this practice would be to maintain the number of (interconnected) Network Services but scale-out (expand) or scale-in (reduce) each one of those instances. This latest option might be preferable in scenarios where the establishment of the new connections between new Network Services instances and/or deletion of existing connections are considered more expensive than simply expanding/reducing the capacity of the existing network services;
- Migrating the currently deployed Network Service instances and their interconnections to more performant/with more available resources node(s) (or less performant/cheaper nodes): the externally perceived performance of the Network Slice would be different, even though the only characterization that would change would be the nodes where it is currently running;
- Expanding/reducing the capacity of the existing Network Service instances: this is the simplest scenario of all, being applicable only in some very specific scenarios (usually related to a pattern of heavy data transportation/transformation), where the bottleneck is the interconnections between the multiple Network Service instances.

The main trade-off in the autoscaling strategies exists between provisioning cost and Quality of Experience (QoE) perceived by the users, which resonates with under-provisioning and over-provisioning resources. While increasing the resources assigned to VNF instances guarantees a certain level of QoE, it leads to higher OPEX for the MNOs. Therefore, an autoscaling mechanism must be aware of its economic costs to reduce the total expenditure while maintaining an acceptable QoE as agreed in the service SLA. Currently, industry, academia, and open-source communities (e.g., open network automation platforms) are focused on developing centralized learning algorithms for intelligent end-to-end management and orchestration of network services. However, centralized learning requires aggregating operational data from various data sources (e.g., mobile edge nodes) belonging to single or multiple domains for insightful analytics. Nonetheless, such data aggregation mechanisms incur practical challenges, such as regulatory restrictions on sharing sensitive data (e.g., EU general data protection regulation), high bandwidth resources required to transfer the raw data to a central server, and the increased risk associated with a single point of failure. Particularly, in a multi-domain ecosystem, assuring isolation among domains is crucial because of the security concerns related to one domain possessing access to another domain's data. Moreover, data aggregation mechanisms described in ETSI ZSM/ETSI ENI SDO's are for non-sensitive data, which might not be useful for designing smart ML algorithms for network management [10]

3.4.1.3 Network Slice instance migration

Depending on the concrete implementation(s), Network Slice instance migration might translate directly into the migration of the corresponding Network Service instances and interconnections between those instances. The obvious use case of a Network Slice migration is the one related with performance: for example, if the use case implies keeping a low latency in the end-to-end service, migrating some of the service instances comprising the slice instance might achieve the required objective.

This feature is one of the most dependent on an accurate run-time measurement, collection and analysis of data, in order for the whole set of involved service providers to be able to provide this capability on time.

The ideal scenario here is to have at least some prediction capabilities for the need of this migration, so that such a complex operation can be triggered on time to fulfil the desired expectation.
Network Slice migration strongly depends on more basic features, such as instantiation (see above) and instance tear down (see next sub-section).

3.4.1.4 Network Slice instance tear down

Tearing down a Network Slice instance should be available only when any of its comprising service instances do not have any connection to any user. It should start by requesting any interconnection between these instances to be teared down, followed by tearing down each Network Service.

3.4.1.5 Network Slice deletion

Network Slice deletion capability should be available only if the specific Network Slice does not have an instance currently running. Again, all the necessary credentials must be in place in order for this feature to be executed, given that it will, in the general case, affect business rules on the involved partners.

3.4.2 Cross-Domain Network Service Lifecycle Management

A network slice can be considered as the composition of a set of slice components, connected according to a slice topology, and managed end-to-end, integrating the different participant domains by means of the necessary trust fabric (credentials, policies…) to coordinate its lifecycle across them.

The ETSI NFV [11] analysis of the support of network slices in software-based virtualized infrastructures maps the concept of the component of network slices, known in 3GPP as *network slice subnets* [12], onto the NFV concept of a network service. A network service constitutes the orchestration and management unit for a given NFV domain, and includes the description of the network functions of any nature, either physical (PNF) or virtual (VNF), the necessary connections among them (through the so-called Forwarding Graphs) and its attachment points to allow network service users to access it.

The management and orchestration domain delimiting service provisioning are not pre-defined, and relies on the different structuring a given network provider, or set of providers, can decide, according to technology, architecture and/or business considerations. In a 5G network environment, a natural division could belong to the different network segments: RAN, transport, edge, core and cloud, though other division are possible. It is important to remark that service management and orchestration (MANO) takes place under the control of a single MANO stack, coordinated by a single *orchestrator*, and supporting a single interface for service lifecycle and assurance management, as defined by ETSI NFV SOL005 [13]. The integration of the cooperating management domains is foreseen by the loosely coupled Service-Based Architecture defined by the ETSI ISG ZSM architecture [14], through the components of the slice descriptor depicted in the previous section.

The SOL005 interface supports the following lifecycle management operations:

- Related to network service descriptors
  - *Create NSD info*
  - *Upload NSD archive*
  - *Fetch NSD archive*
  - *Update NSD info*
  - *Delete NSD*
  - *Query NSD info*
  - *Read NSD*
  - *Fetch NSD archive manifest*
  - *Create PNFD info*
  - *Upload PNFD archive*
  - *Fetch PNFD archive*
  - *Update PNFD info*
  - *Delete PNFD*
  - *Query PNFD info*
  - *Read PNFD*
  - *Fetch PNFD archive manifest*
- Related to network service management
  - *Create network service identifier*
  - *Instantiate network service*
  - *Scale network service*
  - *Update network service*
  - *Query network service*
  - *Terminate network service*
  - *Delete network service identifier*
  - *Heal network service*
- Related to network service performance management
  - *Create monitoring job*
  - *Query monitoring job*
  - *Delete monitoring job*
- Related to operational and monitoring data
  - *Get operation status*

- *Subscribe*
- *Query subscription information*
- *Notify*
- *Terminate subscription*
- *Create monitoring threshold*
- *Query monitoring threshold*
- *Delete monitoring threshold*

The interface also enables to invoke error handling procedures (Retry, Rollback, Continue, Cancel, Fail) on the operation occurrences, and API version information retrieval.

3.4.2.1 Cross-Domain Data-Driven Network Service

At the core of the 5GZORRO proposal are the distributed data mechanisms (data lakes, DLTs and off-chain data stores) used to support data-driven management of infrastructures and user-facing services. These data mechanisms become essential for many of the management operations described above, in particular:

- Service descriptors will be found by querying the different offers available at the off-chain data stores, as part of the operational data lake(s) or elsewhere, and trust scoring assigned by records held by the DLT(s). The same applies for the individual components of the service descriptors (VNFs and PNFs, and embedded services).
- Service instantiation and scaling will rely on resource offerings selected through a similar combination of queries and trust evaluations.
- Update and healing procedures of services and their components will follow an approach like the described above for their location and trust evaluation.
- Monitoring procedures of any nature will use as main destination the appropriate data lake(s).
- Subscription mechanism will include data lake importer interfaces as their main targets.
- All operation requests, results and error handling mechanisms will be recorded through the appropriate data lake(s) and DLT(s) to enable compensation schemas through tokenization and support further auditing and trust evaluation.

3.5 Cross-stakeholder e-license management

Software vendors need to materialize the revenues on their development investments and intellectual property rights associated with them, applying licensing costs to their products according to their business plans using an automated implementation, like the cloud licensing models developed by Amazon [15] or Google [16].

However, Virtual Functions (including VNFs and CNFs) are software functions that can be instantiated and replicated very quickly thanks to the NFV technology in a multi-domain ecosystem. Their agility increases the challenge of the license control and management.

5GZORRO offers a cross stakeholder e-License management service to provide operators and software vendors the mechanisms to trustworthy control the usage of the vendors' software products based on the metric that better fits the agreement, involving the operators and service providers. Vendors will onboard their products specifying in the smart contract of the offer the license conditions, negotiation goal, constraints and associated metric for its monitoring. The design of the service is focused on the control of the licenses at VF level. However, its implementation contemplates the possibility of controlling the licenses of a Network Service or Network Slice even if they are composed by VFs from different providers. The approach taken also allows the management of the licensing regardless of the location or the domain in which the VF is running. Different business models have been evaluated and configured in cooperation with the marketplace catalogue by means of selecting the appropriate product specification characteristics in a Product Offering Price:

- *Flat*: Contract of the VF Vendor for a part or the complete set of features of the VFs without considering time or usage of the service.

- *Pay-as-you-Grow*: In this model, the price varies depending on the increase or decrease of the customer business. Thus, the final cost will be calculated based on one or several conditions of usage of the VFs, like number of instances of VFs or the number active users in a certain moment.
- *Subscription*: Operator contracts the right to use the VF for a certain period of time.

The e-License management service is designed on the metric-based control of the proprietary VFs in the different domains, which may be obtained directly as an application metric or by itself through the MANO layer or the infrastructure. In this way, every action produced in each domain for a controlled VF will be tracked and evaluated for the licensing fulfilment. The key concept that guarantees the trust in the e-licensing framework is provided by the nature of the DLT, i.e., all stakeholders are involved in the agreement and in the consensus of the usage of every VF as it is detailed in Section 5.3.14.

3.6 SLA monitoring & breach prediction

A *Service Level Agreement (SLA*) is an element of a formal, negotiated commercial contract between two Organizations, i.e., one with a Service Provider (SP) role and one a Service Consumer (Customer) Role [17]. It documents the common understanding of all aspects of the Product (what a service provider offers) and the role and responsibilities of both Organizations from product ordering to termination. SLAs can include many aspects of a Product, such as performance objectives, customer care procedures, billing arrangements, service provisioning requirements, etc. The specification of the Service Level Commitments on the SP side is the primary purpose of an SLA. They include 1) the *Service Level indicators (SLIs),* which are the parameters (or metrics) chosen to be measured in a monitoring system, 2) the Thresholds, which are quantitative values to be reached by metrics and 3) a description of measuring, reporting and violation handling processes. Examples of SLI parameters are availability, reliability, throughput, bandwidth, response time, etc. Furthermore, the SLI parameters and the related thresholds express the *Service Level Objectives (SLOs*). Specifically, SLOs are the objectives that must be achieved, i.e., the target value or range of values for a service level. A typical example of SLO structure is: *lower bound ≤ SLI ≤ upper bound.*

SLA Monitoring is the process of comparing the measured SLA parameters (the SLIs) against the thresholds defined in the SLOs of an SLA. The SLIs can be periodically obtained from a monitoring subsystem and are examined against the guarantees given in the SLA. In case of violation a management system could be notified in order to take the appropriate actions.

3.6.1 SLA Monitoring service

The SLA Monitoring service collects, and analyses monitoring data to detect violations in SLAs. After each new contractual agreement, it starts to collect and analyse monitoring data from the monitoring data aggregator service of 5GZORRO. Furthermore, it keeps a record of the SLAs of all the active contracts to periodically consume resource metrics from the monitoring data provider.

SLA monitoring examines SLIs such as availability or response time by retrieving monitored data representing the overall service levels. SLA Monitoring analyses the monitored data and compares the metrics with the thresholds in SLAs to detect SLA violations. The service provider can be notified about SLA violations, which are subsequently propagated to the smart contract for the purposes of re-calculating SLA status. There may be momentary violations, violations of some duration, and violations that appear to be permanent. Contracts may specify the duration that an SLA violation must have in order to be considered as an SLA breach. Each SLA violation can be characterized by its type, the start time and the level of violation.

This service could operate in a Trusted Execution Environment (Section 5.3.9) to enforce trusted analysis on monitoring data and to assure, combined with DLT mechanisms, the trusted level required among Service Consumer and Service Provider for the analysis of monitoring data.

3.6.2 SLA Breach Prediction service

The SLA Breach Prediction service goes one step further from SLA monitoring as instead of detecting SLA violations in real-time, it can predict them before their actual occurrence. For this reason, it collects and analyses monitoring data from the monitoring data aggregator service of 5GZORRO using AI techniques in order to predict possible breaches in SLAs and detect anomalies. Anomaly Detection refers to the problem of finding instances or patterns in data that deviate from normal behaviour. It is important because anomalies often indicate useful, critical, and actionable information (for example problems in the provisioning of a resource or an intrusion which exhausts a resource).

SLA Breach Prediction is a novel service and hence not well established for 5G architectures. Hence, in the following part we provide an introduction for the service in existing service-based architectures [18]. In such architectures, machine learning models are used for the prediction and are subsequently fitted to sufficient historical data. These data can be:

1) *Facts,* representing data which is already known at prediction time.
2) *Unknowns,* which are the opposites of facts, in that they represent data which is entirely unknown at prediction time.
3) *Estimates,* which lie in the middle between facts and unknowns, in that they represent data, which is not yet available, but can be estimated. An example of such data are the Quality of Service (QoS) data, since techniques as QoS monitoring can be used to get insights on the response time of a service before it is actually invoked.

The gathered data can be used for training and testing of the prediction model accuracy as well as can be evaluated with real-time data.

SLA Breach Prediction approaches are used for maintaining SLAs between service providers and consumers, such as the work presented in [19]. Specifically, in this work the authors propose a profile-based model for the prediction of SLA violations from the provider's perspective. Each consumer has a different profile and the prediction helps service providers in making decisions about whether to form SLAs as well as in avoiding SLA violations. The prediction model generates an alarm to the service provider that a violation is likely as well as generates a recommendation for remedial action. This gives the provider the opportunity to arrange appropriate resources to avoid the violation. Further methods to predict violations are linked to Bayes models for predicting the mean load over a long-term time interval [20]. Additionally, this method can be used for predicting the mean load in consecutive future time intervals by identifying novel predictive features of host load that capture the expectation, predictability, trends and patterns of host load. The combination with Bayes logic allows a service provider to estimate the probability of whether SLA violation will occur.

SLA breach prediction can be also used to provide resilience in a service-based architecture. Specifically, resilience is linked not only to operational violations, but also to cyber-security-oriented violations. Such violations occur as a result of malicious activities that are initiated by adversaries and are located at different service levels as the network, application or even the operating system level. To perform such activities, adversaries need to first gain access to a service by identifying and exploiting its vulnerabilities (Section 3.7.2). This allows them to either cause direct damage to the service or even leverage connections to other services or domains to magnify the attack's impact. The malicious activities that are triggered by adversaries can be detected using rule-based or knowledge-based techniques. Rule-based techniques are very effective in detecting known cyber-attacks based on a list of existing signatures. However, they require a frequent update of their signatures as well as cannot cope with sophisticated or zero-day attacks. Hence, knowledge-based techniques are also employed in order to learn the normal behaviour of each service and create a profile of nominal operation. Such profile can be created using statistical or AI techniques. Both rule and knowledge-based techniques lead to the detection of anomalies that can either be: 1) accurate SLA violation predictions or 2) false positives and false negatives. For the first point the predicted incident actually occurs and such SLA violation is categorized as a true positive. For the second point a false positive indicates that a predicted incident does not occur and a false negative that a real incident that has occurred was not predicted.

During the early stages of development in the project, several experiments were conducted to discover a suitable model for real-time predictions as discussed above. Long-short Term Memory (LSTM) [21] recurrent networks and the ARIMA (AutoRegressive Integrated Moving Average) [22] family of models have proven to be efficient in predicting future values based on time series. In those experiments, the subjects of SLAs are computing resources, whose values vary as time progresses. Therefore, the models were tested against a series of **bandwidth** values captured from a live Intracom Telecom CDN server. Note that the metrics were captured a minute apart from each other for a total of approximately 8500 minutes, 60% of which were used for model training. Evaluation of the model involved the input of sequences of consecutive bandwidth values that the model was unfamiliar with (i.e., not used for training) with the goal of predicting the next value in each sequence. Results showed that LSTM, applied with several different configurations, had overall better performance than ARIMA, with an accuracy close to 99% at times.

Finally, the SLA Breach Prediction service could also operate in a Trusted Execution Environment (Section 5.3.9) to enforce trusted prediction of SLA violations on monitoring data.

3.7 Security and trust across multiple domains

The massive increase in device quantity and the increase in activities and connections available on devices that interact in a 5G network together lead to an increase in potential risks and threats that both end-users and service providers may suffer.
In this sense, it is necessary to define new distributed models to develop efficient connectivity in 5G networks, through which a group of entities (whether small or large) can establish cross-domain/operator service chains, with trust and security.

3.7.1 Identities and trust across multiple domains

Distributed trust models can allow network connections to be established between domains reliably, avoiding possible connections that could endanger user data integrity or compromise the security of service providers and end-users.

Key to the realisation of trust across domains is the use of decentralized identity management (DIdM), which is based on DIDs.

DIDs are a novel type of identifiers proposed by W3C [23] that allows associating any subjects such as stakeholders, resources, services, organizations, entities, and so on, with a digital identity. DIDs are global identifiers which enable verifiable and decentralized digital identity, allowing to uniquely identify any subject, e.g., a person, organization, abstract entities, etc. To achieve this purpose, DIDs are associated with cryptographic material, such as public keys, and service endpoints, making each DID globally unique, resolvable with high availability, and cryptographically verifiable.

The usage of DIDs provides to an application of self-administered identity management, enabling further self-managed capabilities such as authentication, authorization, role management, and identity information exchange between two identity domains.

Related to the identity management, it should be pointed out the primordial role of Verifiable Credentials. A Verifiable Credential (VC) [24] is a tamper-evident and privacy-preserving credential (set of claims) that can be demonstrated through a cryptographic process. Verifiable Credentials can represent the same information that physical credentials represent in real life such as driving licenses, passports, health insurance card, and so on. Therefore, Verifiable Credentials represent statements made by an issuer in a tamper-evident and privacy-preserving manner.

Another imperative aspect to ensure trust across domains is the determination and establishment of end-to-end trustworthy chains among multi-stakeholders which are mostly covered by trust models. Trust is an essential pillar in multi-party business scenarios as the lack of it may entail improper partner selection as well as arising unexpected security incidents. In this vein, trust models cater for the required functionalities to automatically enable stakeholders to take the most reliable option. To tackle the above-mentioned objective,

AI and ML have conventionally been used not only to automate the trust assessment process but also to determine the relevance, weight and correlation between defined attributes. Hence, well-known methods such as Bayesian networks, Markov model and Fuzzy Logic are some of the most profitable ones [25]. When it comes to Bayesian networks, they allow through Bayesian inference to compute the probability from which trust values are finally represented without a high complexity. Despite the fact that Bayesian networks should address certain uncertainty and randomness issues, recent researches have taken them into account and reached a 0.9516 [26] and 1.0 [27] accuracy in dynamic and distributed deployment scenarios. In the case of the Markov model, it is an analytic method, and in consequence, it guarantees speed and precision when producing results. Markov model analysis implies great care during the model building phase because the model accuracy is all-important in obtaining valid results, therefore, implicit assumptions should be avoided. Nevertheless, Markov models are generally valuable approaches that allow for consuming event streams and forecasting feasible changes in business relationships, at the same time that they ensure profitable accuracy rate, 0.8 in [28], and detect traditional trust attacks, 92% and 89% detection rates against on-off and bad-mouthing attacks [29]. Last but not least, Fuzzy Logic is a straightforward and justifiable system whose fuzzy rationale is commonly employed for business purposes. Besides, it also promotes the control of purchaser items. As principal drawbacks, the fuzzy rationale is not constantly exact and the verification and approval of a fuzzy information-based framework involve broad testing. Yet, Fuzzy Logic continues nowadays being utilised in multiple scenarios where parties are continually interacting with the system and both newcomers and selfish users appear at any given moment, guaranteeing high scores such as 95% [29] and 90% [31] accuracy.

3.7.2 Detection and countermeasures for security vulnerabilities

The massive number of new devices connected in 5G networks entails the emergence of new security challenges, which in turn leads to a bigger attack surface. 5G systems deployment is expected to bring numerous security risks, threats, and challenges in a multitude of scenarios such as network virtualization, the rise of new communication protocols and their compatibility with existing, or even critical communication infrastructure.

Security is an essential characteristic that is usually interconnected to other characteristics, and therefore should not be addressed properly on its own without considering other factors. A possible example is the correlation between security and trust. By definition, both characteristics complement each other, that is, a trust establishment between two providers will be guaranteed if services and protocols deployed in both entities are secure, and a communication will be safe if the involved entities are trustworthy (non-malicious) and do not attempt to alter information flow.

To tackle all efforts towards a risk-free 5G multi-stakeholder scenario, a risk analysis service is required. 5GZORRO architecture includes actions related to risk detection, assessment, and treatment via a risk management methodology, which is part of one of the services that make up the end-to-end trust and security model in distributed multi-stakeholder scenarios. In particular, the actions related to risk management are inspired by the ISO/ICE 27005 standard, but it should be noted that none of the entities that make up 5GZORRO's ecosystem possess and/or such a certificate. In this sense, 5GZORRO intends to use only some steps of this standard, since they are considered a universal approach to risk management. Among the actions to be followed are the definition of assets to be included in the process and collection of all necessary information to gather the relevant risks (also known as context establishment), and the risk identification, risk analysis, and risk evaluation (risk assessment). Besides the detection of software vulnerabilities and compromises, risk analysis service provides a set of countermeasures for any of these detected vulnerabilities and its implications on the network services (risk treatment).

4 Reference architectures & technologies

Specifications from many Standard Development Organizations fall into the scope of the 5GZORRO architecture. Similarly, several technologies and tools are used as core enablers of the 5GZORRO architecture. Indeed, the 5GZORRO architecture has been designed considering various specifications and technologies in order to leverage on the most of them and realize a multi-operator zero-touch service management.

For sake of readability and because of the large set of relevant references, the following tables provide a summary overview of the 5GZORRO core focus aspects with respect to

- reference standards and architectures in state of the art, split across three major area: *Intelligent zero-touch Management*, *Cross-domain resource & service trading*, and *Security and Trust* (see Table 4-1)
- reference technology enablers (see Table 4-2).

As the reference standards and technology enablers in scope for the 5GZORRO architecture are not changed since the preparation of D2.2 [2] and D2.3 [3], and assuming that most of the general overview information on applicable SDOs and technologies might be already known to the reader, full details for the cited references are provided in the Appendix I of D2.2 Appendix I [2].

Table 4-1: 5GZORRO focus aspects from reference architectures in different areas

Area	Standard Development Organisation	5GZORRO Focus Aspects	Overview details
Intelligent zero-touch Management	• **ETSI ZSM**	• Zero-touch and domain-oriented management • Service-based architecture	[14][32][47]
	• **ETSI NFV MANO**	• Network Slice (incl. GSMA and 3GPP reference templates) • Network Slice Network Service, VNF lifecycle management	[48][49]
	• **ETSI ENI**	• AI/ML based policy management, orchestration decisions and suggestions	[50]
Cross-domain resource & service trading	• **TMForum Telecom infrastructure marketplace**	• Infrastructure sharing & trading principles and trials • Spectrum sharing and licensed spectrum trading • Marketplace-Orchestration platforms interoperability	[51][52][53]
	• **ITU-T**	• Permissioned DLT reference architecture	[54]
	• **ETSI PDL**	• Permissioned DLT reference architecture	[55]
	• **MEF LSO SONATA**	• Offering information models and management • Multi operator connectivity services	[56][57][58][59]
	• **CBAN**	• Permissioned DLT reference architecture	[60][61][62][63]

		• Offering information models and management • DLT-based Applications and Marketplace	
Security and Trust	• **ITU-T Y.3054** • **ETSI TR 10368** • **ISO/IEC TR 23186**	• Trust modelling and computation techniques • Marketplace-Orchestration platforms interoperability	[64][65][66]

Table 4-2: 5GZORRO focus aspects from technology enablers

Technology	Enabling solutions	5GZORRO Focusing Aspects	Overview details
Distributed Ledgers & Smart Contracts	• **R3 CORDA**	5GZORRO employ DLT and Smart Contracts technologies for realization of a Marketplace with contract negotiation and provisioning of resources & services and SLA enforcement.	[67]
Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs)	• **Hyperledger Indy** • **Hyperledger Aries**	5GZORRO use DIDs and VCs to enable a multi-stakeholder decentralized identity management solution. Also, DIDs will be employed to identify the resources offered in the 5GZORRO marketplace, and VIM/NFVI.	[68][69]
Data Lakes	• **OpenDataHub** • **CNCF OpenTelemetry**	5GZORRO use and enhance data lake technologies to aggregate and store relevant monitoring data from different stakeholders, and to perform analytics to predict SLA breaches.	[70][71]
Artificial Intelligence solutions for Network Management	• **Feed Forward Neural Networks (FFNN)** • **Long Short-Term Memory networks (LSTM)** • **Convolutional Neural Networks (CNN)**	5GZORRO employ different machine learning and deep learning algorithms for VNF auto-scaling, Network Slice resource auto-scaling, SLA breach prediction and smart resource Discovery	[72][21]
Trusted Execution Environments	• **HW TEE** • **SW TEE** • **Mixed HW/SW TEE**	5GZORRO use TEE to protect the data that are stored locally in each DLT node and to isolate the VIM or NFVI components allowing to protect the sensitive data of applications and services that are running on them.	[73][74][75]
Cloud-native technologies for 5G	• **Kubernetes** • **ISTIO** • **NSM**	5GZORRO use a container engine in order to realize an environment where CNF and VNF can coexists and an orchestrator (Kubernetes) to manage these containers. ISTIO and NSM will be used to provide communication	[38][76][77]

	between services, possibly instantiated through VNF or CNF.

5 5GZORRO High-level Reference Architecture

5.1 Design principles

A set of common best practices in design of automated systems implementing zero-touch service orchestration have been analysed and adopted to design the 5GZORRO architecture. In general terms, the 5GZORRO architecture is inspired by the following design principles:

- **Service based architecture**, as in 3GPP and ETSI ZSM.
- Allow separation of **responsibilities & scopes per domain/inter-domain.**
- **Modular and scalable architecture** which offers self-contained services, which can be independently deployed and scaled.
- **Extensible architecture** which allows adding new services, capabilities and service end-points in a pluggable manner, without requiring changes to existing designs, implementations and interactions.
- **Model-driven architecture with open interfaces,** which uses information models to capture the attributes and supported operations of the managed objects. The information models and interfaces are independent from implementation and are modelled in YAML and Open API specification to facilitate portability and reusability.
- Adopt **communication mechanisms** capable to implement both publish-subscribe patterns and direct invocations among functions for: a) Network Slice lifecycle management; b) Service and resource discovery/management; c) Network analytics; d) Security & trust.
- **Distributed architecture with instances in all domains** of the involved 5GZORRO parties.
- Includes a **distributed trusted data layer** for SLA enforcement, resource discovery and smart contracts management implemented through **Permissioned Distributed Ledger Technologies.**
- Includes an **Operational Data Lake** capable to collect telemetry data from various domains and services and to implement AI-driven insights on service, resource and infrastructure operations.

5.2 Architecture overview and core building blocks

The 5GZORRO High Level reference architecture is depicted in Figure 5-1. It is comprised by four major logical sub-systems grouping different types of functionalities according to previously defined service-centric architectural model principles. Figure 5-1 shows both single-domain and multi-domain interaction among the various sub-systems. In particular, each coloured box in a sub-system identifies a different provider, thus functional sub-systems belonging to the same provider interact each other through the domain communication fabric, while those belonging to different providers interact through the multi-domain communication fabric. A logically centralized Data Lake enables data store and exchange for cross-domain analytics and AIOps functionalities. Those providers that own infrastructure resources also have a 5G Virtualization Platform box depicted in the figure (could be a subset of the whole set of providers considered). It should be noted that such logical grouping aims at identifying the various 5GZORRO functionalities, while defining functional blocks belonging to the same logical sub-system. However, this does not provide a software design view of the architecture, which indeed is defined in section 6.

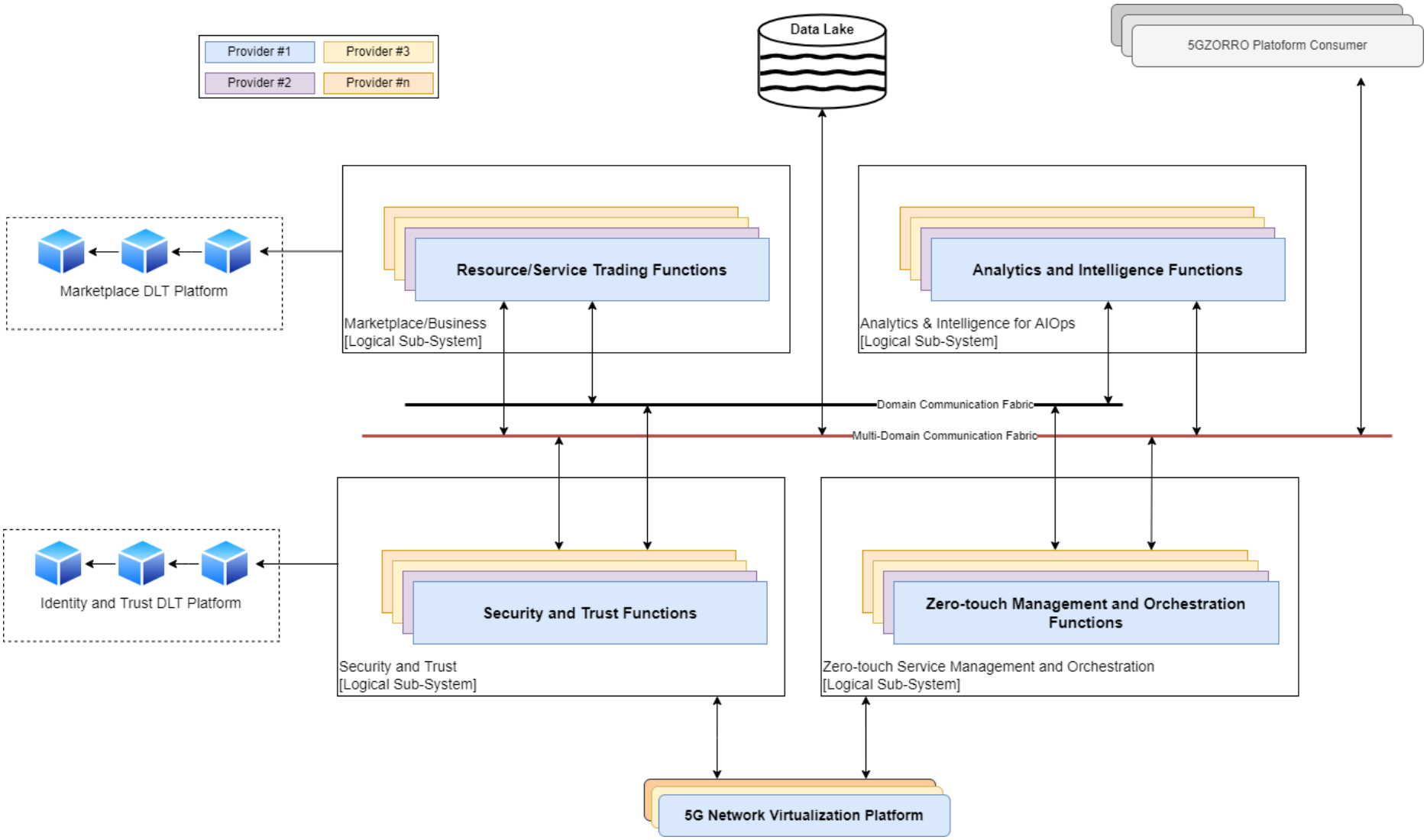

Figure 5-1: 5GZORRO High Level reference architecture

The **Zero Touch Management and Orchestration** sub-system (see Figure 5-2) provides the required functionalities to control 5G Managed Infrastructure Resources including Radio Spectrum resources, Transport Networking resources and Computing resources (at data centers and at edge computing nodes) as well as existing legacy resource controllers from previous 5G deployments. It applies ETSI zero-touch network and service management architectural patterns to enable zero-touch automated management of 5G networks including the end-to-end management of the life-cycle of network slices and associated services, which are integrated with automated capabilities for e-Licensing management. An abstract functional element (Abstract Resource Management and Control) is responsible to manage and control any type of 5G resource. Then, the management and control of each type of 5G resource extends from this new Abstract Functional Block. Virtual, radio and spectrum resources, have been identified as 5GZORRO resource types managed and controlled by functional elements extending from the Abstract Resource Management and Control functional block. The Spectrum Resource Management addresses Spectoken related requirements coming from Use Case 2

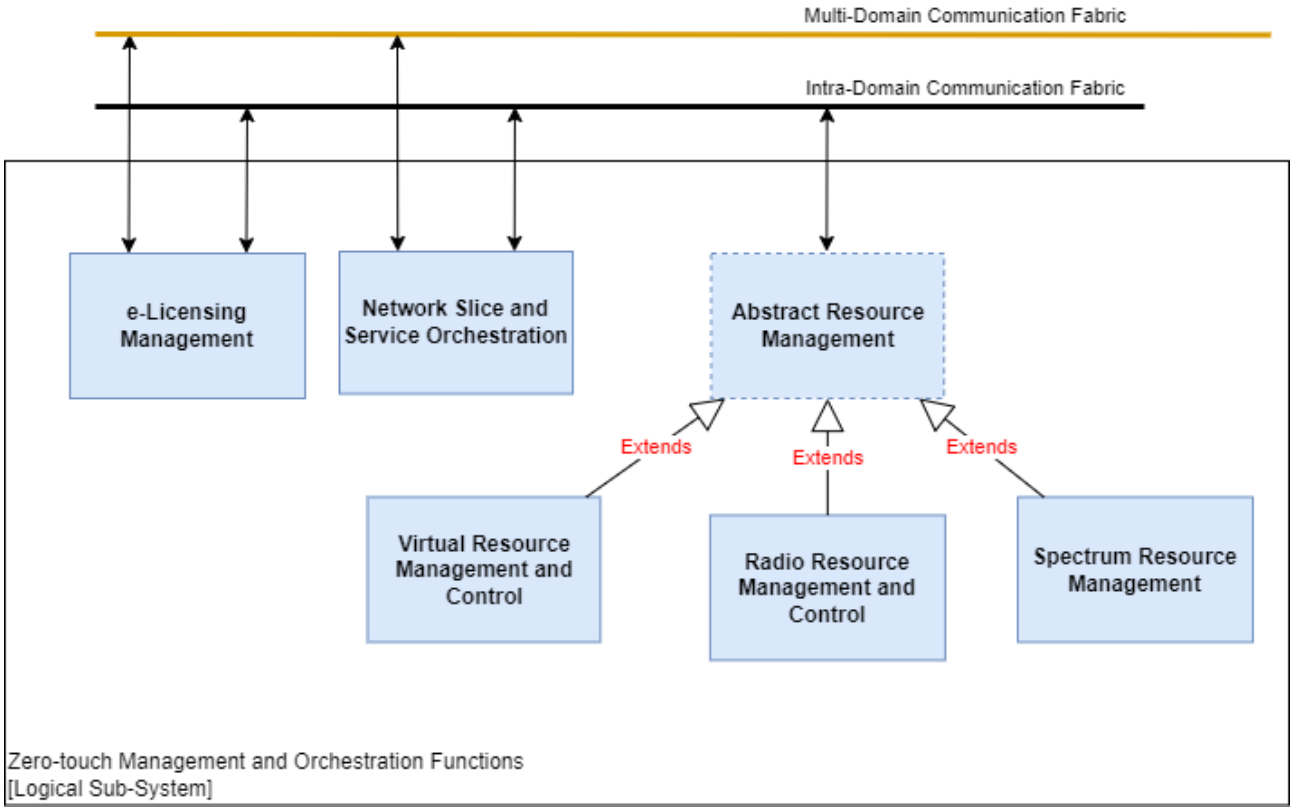

Figure 5-2: Functional Elements populating the Zero Touch and Orchestration sub-system

The **Security and Trust** sub-system (see Figure 5-3) provides a generic framework to administrate the trust and security evaluation of internal entities and resources, and the ones from other stakeholders. It entails complicated and modular tasks owing to the number of fronts to be enveloped (see Figure 5-3). In this vein, the Security and Trust sub-system guarantees security not only at intra-domain level through detection and mitigation of possible attacks or threats in the stakeholder's network, but also at inter-domain level where it secures the communication between multiple domains as well as exchanged information. Furthermore, it aims to ensure an end-to-end trustworthiness establishment among different stakeholders based on previous experiences and recommendations. Hence, the trust management makes possible to determine the stakeholder trust scores, as well as enable the generation of a trust chain among involved entities. Another major feature of the Security and Trust sub-system is the choice of ensuring secure computation of critical tasks, guaranteeing security, reliability, and privacy-preserving, thus managing trusted execution environments. Finally, the Security and Trust sub-system is also the management of the global (cross-domain) identifiers (e.g., stakeholder identifiers and the 5GZORRO resource identifiers) in accordance with the self-sovereign identity principles by leveraging on a dedicated Identity and Trust DLT platform. It supports the

creation, verification, and revocation of certificates as well as authentication and authorisation of identities across 5GZORRO domains.

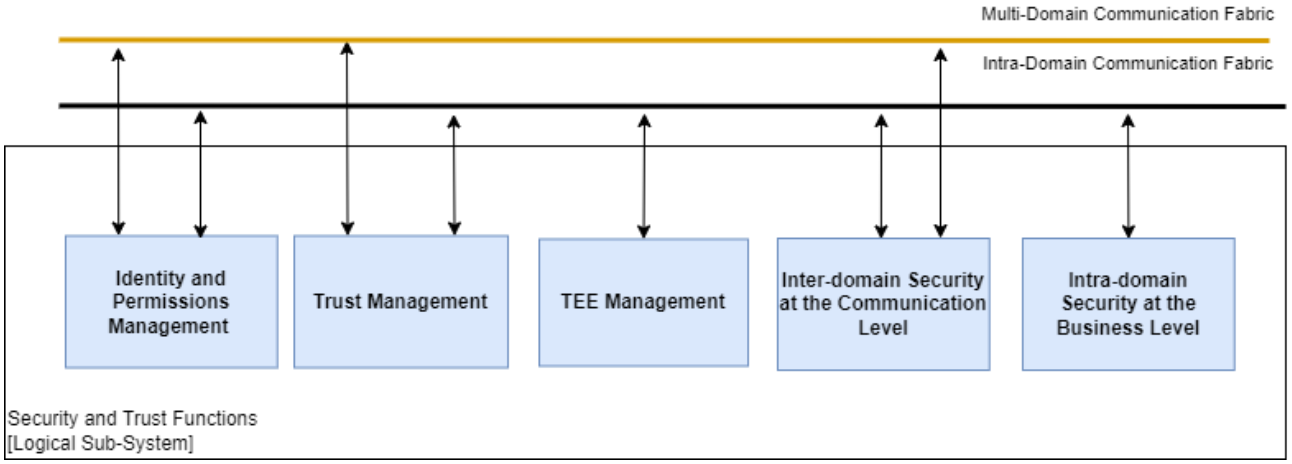

Figure 5-3: Functional Elements populating the Security and Trust sub-system

The **Marketplace and Business sub-system** (see Figure 5-4) enables the trading of 5G resources (including Radio Spectrum resources) across different domains by using Smart Contracts on the dedicated Marketplace DLT platform. The Marketplace is ruled by a decentralized Governance Model where Governance Administrators (i.e., 5GZORRO stakeholders with permissions to vote) can take decentralized decisions such as accept/reject network participation, issue/revoke membership rights, and resolve disputes. Major Marketplace features are: decentralized catalogues for 5G Resource offers and 5G Service offers, decentralized repository for legal prose statements to be used in smart contracts and the life-cycle management of smart contracts for offers and agreements between providers and consumers.

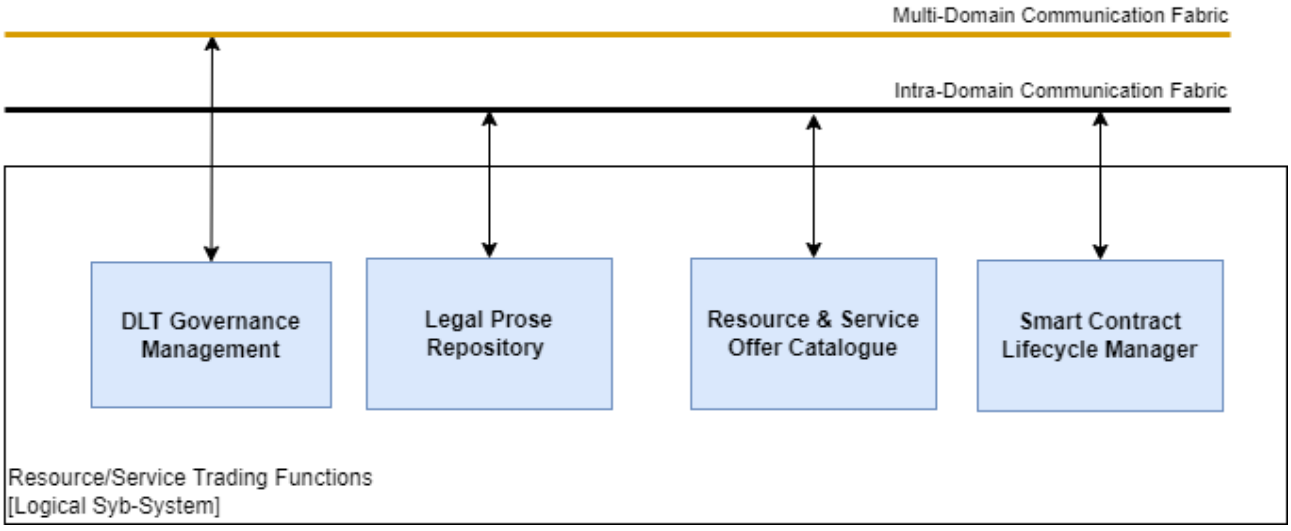

Figure 5-4: Functional Elements populating the Marketplace and Business sub-system

The **Analytics & Intelligence for AIOps** (see Figure 5-5) sub-system leverages data lake and AI technologies to provide data persistence, data sharing and data analytics platform for 5GZORRO framework, within and across domains. It enables collecting the operational data through Monitoring Data Aggregation block and using the collected data for the data-driven automation of complex operational procedures, through pluggable use-case specific blocks realising custom data processing and analytics functions. Examples of such functions are presented in Figure 5-5: Intelligent Network Slice Management and Optimization, Smart Resource and Service Discovery, and Intelligent SLA monitoring and breach prediction.

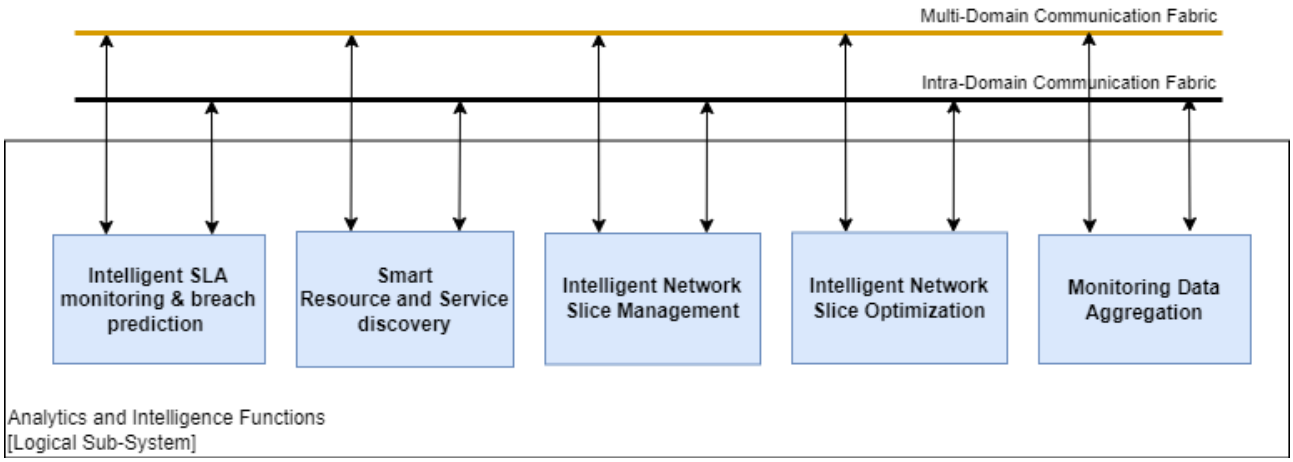

Figure 5-5: Functional Elements populating Analytics & Intelligence for AIOps sub-system

The **Communication Fabric** provides all required functionalities to support the communication and interoperation across 5GZORRO framework in a loosely coupled way, within or across domains. The registration, discovery, and invocation of 5GZORRO services, data transfer, are major functionalities provided by the Communication Fabric. Depending on the communication needs and each Domain policies, different types of communication patterns should be supported including: Synchronous communications; Asynchronous (pub/sub) communications; Point-to-point communications; Brokered communications.

Different instances of Communication Fabrics may be deployed in 5GZORRO:

- *Intra-Domain (or Domain) Communication Fabric*, where registered services are available within a single administrative 5GZORRO domain
- *Cross-Domain Communication Fabric*, where registered services are available across all administrative 5GZORRO domains.

5.3 Specification of the 5GZORRO functional blocks

This section describes the 5GZORRO Functional Entities deriving from the functional breakdown of the entire reference architecture. Not all these entities are exposed to 5GZORRO users: in fact, some of them remain internal and support the execution of zero-touch or security actions.

5.3.1 DLT Governance Management

5.3.1.1 Overview

The marketplace is subject to a DLT-based governance model. This ensures that decisions such as admission, revocation of membership, and dispute resolutions are managed in accordance with a uniform agreeable governance model; acceptance of these terms would be mandated as part of registration along with Know Your Client (KYC) & Anti-Money Laundering (AML) checks.

5.3.1.2 Provided Services

To support this, a Governance service provides the necessary API to enact all governance actions. It is subject to Role Based Access Control (RBAC) in order to ensure that only members of the Governance Admin role are able to - for instance – propose Governance decisions. Marketplace Stakeholders should be notified of any governance decisions, as well as any intermediary steps, e.g., received, approved, and rejected.

Table 5-1: Definition of Governance Service (cross-domain level)

Service name: ***Governance Service***		Type: ***Cross-domain***
Capabilities	**Support (O|M)**	**Description**
Apply for membership	**M**	Facility for a new stakeholder to apply for Marketplace membership including the claims that are being requested and specification of how to be notified of marketplace events e.g., governance decision
Check membership status	**M**	Allow a platform user to check the membership status of a particular Stakeholder, for example a stakeholder can check the status of their application.
List members	**M**	Obtain a list of active Marketplace members to allow a governance administrator to review onboarded members, their info, approved roles & assets, etc
Revoke membership	**M**	Revoke a stakeholder's Marketplace membership to enable a stakeholder to 'leave' the Marketplace. This corresponds to an extreme undesirable scenario, where the governance decision could be against the will of the member being revoked
Propose governance decision	**M**	Propose a decision based on the information provided by the interested party, after reviewing according to the governance model
Get a proposed governance decision	**M**	Retrieve the details pertaining to a particular proposed governance action
Notes		
none		

5.3.2 Resource & Service Offer Catalogue

5.3.2.1 Overview

The Resource & Service Offer Catalogue is the place where shared resources (e.g., network, infrastructure and spectrum assets) and services to be used for exchange are stored. Likewise, the Resource & Service Offer Catalogue stores the available offers to be advertised across the 5GZORRO platform. Following the TMF nomenclature, resource, and service technical specifications are created at domain level and eventually used to compose product offers. In turn, product offers, which also contain business-related attributes (e.g., price offer terms, etc.), are made available for trading by publishing such offers via the Marketplace DLT platform and can be purchased by means of product orders.

5.3.2.2 Provided Services

The Resource & Service Offer Catalogue provides to 5GZORRO users the possibility to add resource or service offers to the 5GZORRO Catalogue, list the active resource and service offers, query, modify or remove a resource or service offer, and make an order for a specific resource or service offer. The catalogue management service is also responsible for maintaining the Resource & Service Offer Catalogue up to date. Resource and Service catalogues offer interfaces for querying Marketplace offers. Requesters are able to make 'simple' criteria requests that query the catalogue's off-chain storage for available resources or services meeting a basic set of requirements. The requester is then able to apply any domain-specific intelligence they wish to further filter results with.

Table 5-2 defines the Resource & Service Offer Catalogue services.

Table 5-2: Definition of Resource & Service Offer Catalogue service

Service name: **Resource & Service Offer Catalogue**		Type: ***Per-domain***
Capabilities	**Support (O|M)**	**Description**
Onboard Assets (Resources or Services)	**M**	Update list of resources or services that Operator declares to be available for external users.
Manage offer lifecycle	**M**	The Resource & Service Offer Catalogue is able to perform the typical management operations including creation, modification, query and removal of resource and service offers.
Provide offer information	**M**	The Resource & Service Offer Catalogue can be requested to provide information on a general or a particular set of offers in the Catalogue, including filtered look-up queries.
Purchase an offer	**M**	The Resource & Service Offer Catalogue also has the mechanisms to enable transaction on the resources and services offered in the 5GZORRO architecture.
Notes		
none		

5.3.3 Legal Prose Repository

5.3.3.1 Overview

The Legal Prose Repository is a shared repository of parameterised legal statement templates that can subsequently be associated with a given resource or service by providers. These statements could be optionally subject to a governance process such that admin network members will need to approve any new or updated statements since their definition will relate directly to verification logic in equivalent Smart Contracts. Legal prose instances consist of both human readable and machine-readable portions, the former being referenced by smart contracts should a need to refer to it arise e.g., to mediate a dispute.

Legal prose reflects SLAs and their associated SLOs and SLIs, feeding into active agreements and associated monitoring during the agreement's lifecycle.

5.3.3.2 Provided Services

Services include the ability to create, modify and archive legal prose templates, as well as additional governance operations to manage their versioning and publication.

Table 5-3: Definition of Legal Prose service (cross-domain level)

Service name: **Legal Prose Repository**		Type: ***Cross-domain***
Capabilities	**Support (O|M)**	**Description**
Get Legal Statement Templates	**M**	Retrieve a set of legal statement templates that can subsequently be used to define terms for a given Resource or Service Offer
Create Legal Statement Template	**M**	Provide the ability to create a new template that corresponds with a particular Smart Contract
Update Legal Statement Template	**M**	Provide the ability to update an existing template
Remove Legal Statement Template	**M**	Provide the ability to remove a template from active use

Approve Legal Statement Template	**O**	Facilitate a review/governance process that ensures a template has been legally ratified but also that it meets the requirements of the associated Smart Contract
Notes		
none		

5.3.4 Smart Resource and Service discovery

5.3.4.1 Overview

The Smart Resource and Service Discovery functional block allows the discovery and selection of available offers from the 5GZORRO Marketplace through the declaration of customer intents. Motivated by ETSI ZSM means of automation [32] principles, this module leverages ML/AI techniques to allow the discovery of product offers that best satisfy the consumer needs.

5.3.4.2 Provided Services

Offers discovery is facilitated by a Smart Resource and Service Discovery service. In addition to basic query capabilities (via lookup filters), implemented at the Resource and Service Offering Catalogue (Section 5.3.2), this functional block allows to intelligently define relationships in the offers present in the marketplace and to translate high-level discovery intents, in order to better attend to the users' requests. This discovered capability is exposed via intent-based API to other 5GZORRO functional blocks, such as the Intelligent Service and Slice Management. Specifically, the Intelligent Service and Slice Management can invoke the Smart Resource and Service Discovery with given user intent to retrieve the offers that match the intent.

Table 5-4: Definition of Resource and Service Catalogue service (domain level)

Service name: **Smart Resource and Service Discovery**		Type: ***per-domain***
Capabilities	**Support (O|M)**	**Description**
Generate (offers) Clusters	**M**	Provide a mechanism for grouping together resources and services of a certain class are. To do so, a clustering model is trained offline to learn the similarities from the resources and services properties in order to obtain relevant clusters of offers. To ensure that the considered training remains accurate over time, this procedure can be repeated periodically.
Classify (resource or service) Offers	**M**	Provide a classification mechanism based on supervised learning that takes the resulting clustered offers as labelled dataset for training. Such prediction model is then able to for determining, at run time, for every incoming offer which of the computed clusters it belongs to. In a similar way as above, this submodule can be retrained upon any update to the offer's clusters.
Discover (resource or service) Offers	**M**	Provide a mechanism for receiving offers retrieval requests in the form of intents, defined in this context as high-level resource and service requirements. In particular, this component is able to translate the received intention into specific clusters, in order to retrieve the set of marketplace offers that best satisfy the user request.
Notes		
none		

5.3.5 Intelligent Slice and Service Management

5.3.5.1 Overview

If an Operator requires resources beyond what is available, it may be able to obtain resources from some other Operator(s) using the 5GZorro marketplace. The rationale for this can be extending the Operator's footprint to cover a larger service area or scaling out its communication services to mitigate imminent or present SLA breaches. The Intelligent Slice and Service Management (ISSM) is a cross-domain functionality. It comprises a collection of local Workflow Management (WFM) engines and a central Workflow Engine that helps synchronizing and stitching local per-domain workflows. The overall functionality is termed ISSM-WFM.

Each ISSM workflow starts in a specific Operator domain triggered either by an operator or by automated functionality such as Intelligent SLA Breach Prediction or Intelligent SLA Monitor, which communicate a high-level intent that requires realization. This high-level intent is being used by ISSM-WFM to discover resources relevant to creating a new cross-domain communication service. For example, these can be resources of a specific kind, within a specific geography, within a certain price range and capacity capabilities, or offered by a specific party. The resources are being discovered through querying the Smart Resource Discovery function. Next, ISSM-WFM interfaces with the Intelligent Network Slice and Service Optimization function; and once the optimized resources are selected, ISSM-WFM procures them on the marketplace and triggers local workflows for technical orchestration in a specific domain.

5.3.5.2 Provided Services

The main service of ISSM-WFM is end-toe end fully distributed business level orchestration of all technical flows in the 5GZorro platform. ISSM-WFM uses a concept of a workflow. New workflows can be added at will by the 5GZorro developer persona. This way, functionality of ISSM-WFM can be grown continuously and sustainably. The typical tasks that ISSM-WFM helps with in any workflow is orchestrating discovery of the resources on the marketplace, optimization of resource selection, resource procurement, initiation of life cycle management for slices and services, mitigation actions orchestration in response to Intelligent SLA Breach Prediction and Intelligent SLA Monitoring services.

Table 5-5: Definition of Intelligent Network Slice and Service Orchestration service (cross-domain level)

Service name: **Intelligent Network Slice and Service Orchestration**		Type: ***Cross-domain***
Capabilities	**Support (O|M)**	**Description**
Discover 3rd party resource initiation	**M**	Through Smart Resource and Service discovery function element, discover all 3rd party resources offered in the 5GZORRO architecture.
Select 3rd party resource initiation	**M**	Through Intelligent 3rd party resource selection functional element, select the best available 3rd party resource w.r.t cost and QoS among all the discovered resources.
Resource agreement setup initiation	**M**	Through Smart Contracts Lifecycle Management functional element, setup the proposed resource agreement via smart contract.
Proactive multi-domain network slice lifecycle initiation	**M**	Proactively notify Network Slice and Service Orchestration functional element to initiate multi-domain network slice extension to satisfy the network slice SLA.
Notes		
none		

5.3.6 Smart Contracts Lifecycle Management

5.3.6.1 Overview

The Smart Contract Lifecycle Management is responsible for both the lifecycle management of entities published to the Marketplace DLT as well as the management of Resource/Service provider Agreements and SLAs that can be utilised by other functionalities when composing product offers. Agreement & SLA management facilitates the definition of re-usable agreements/SLAs for a particular class of resource or service, and not an instantiated SLA relating to a specific commercial agreement. It is the terms that subsequently get agreed and deployed to the DLT that represent the instantiation of these terms.

5.3.6.2 Provided Services

Management of contracts throughout their lifecycle, from agreement negotiation and instantiation through to termination are managed by an SLA & Licensing Manager service. The SLA & Licensing manager mediates interactions with stakeholders such as coming to an off-chain agreement of terms or viewing active agreement i.e., its primary role is based around viewing and updating contract state. The Smart Contract Lifecycle manager service on the, other hand, works closely with the SLA & Licensing manager but provides services specific to the lifecycle of an agreement and associated events triggered by contracts.

Table 5-6: Definition of SLA & Licensing Manager service (cross-domain level)

Service name: **SLA & Licensing Manager**		Type: ***Cross-domain***
Capabilities	**Support (O|M)**	**Description**
Offer Agreement Proposal	**M**	Facility to create an agreement proposal for a given set of Resource or Service Offers. Each resource/service's availability status would be checked and confirmed to the requester.
Offer Agreement Creation	**M**	Facility to take an Offer agreement, and 'deploy' the necessary smart contracts to realise the agreement on the DLT. On successfully establishing the agreement this event will be published to prompt a cross-domain monitoring & analytics component to configure a data aggregator to provide the measurements at intervals agreed in the contract (see 5.3.15)
Terminate an agreement	**M**	Facility for a stakeholder to terminate an active agreement. As per creation, termination of an agreement should teardown the necessary configured monitoring by publishing the event for a cross-domain monitoring & analytics component to process (See 5.3.15)
Get agreement	**M**	Facility for stakeholders to retrieve the details of one of their agreements
Get agreements	**M**	Facility for stakeholders to retrieve a filtered list of one or more of their agreements
Update offer agreement	**M**	Facility for a stakeholder to update an active offer agreement e.g., make a pricing adjustment. When an agreement is updated, the update will be published to prompt a cross-domain monitoring & analytics component to re-configure monitoring aggregation to align with the updated contract terms (see 5.3.15)
Record monitoring measurements	**M**	A contract defines a monitoring aggregation service that has been agreed to be the sole provider of SLA related metrics. At intervals defined in the contract, measurements will be

		submitted to the SLA & Licensing Manager (see section 5.3.15) which will subsequently locate the associated smart contract and notify the smart contract should a breach have been occurred. The smart contract will trigger any subsequent actions as determined by the terms of the agreement. In addition to the measurement, a hash of the monitoring data and the period for which that account should be supplied in the request to the SLA & Licensing Manager in order for it to be stored on the ledger to achieve non-repudiation of the submitted raw logs.
Submit licensing action	**M**	Licensing-related actions need to be recorded and validated by Smart Contracts. For example, recording a scaling operation to add an additional VNF instance would need to verify that this action is in-line with the agreed licensing terms. The response would indicate whether the action is valid/invalid based on the terms; see section 5.3.14.
Notes		
'Record monitoring measurement' and 'Submit Licensing Action' may provide interfaces or simply rely on messaging protocols. It depends upon how communications between the Cross-domain SLA Monitoring & Analytics and eLicensing manager respectively interact with the marketplace. In both these cases, they could be functional elements that subscribe to measurements/actions.		

Table 5-7: Definition of Smart Contract Lifecycle Manager service (cross-domain level)

Service name: **Smart contract lifecycle manager**		Type: ***Cross-domain***
Capabilities	**Support (O|M)**	**Description**
Compose and deploy smart contact	**M**	Take an agreed set of terms and deploy the necessary contracts to the DLT
Subscribe to and manage lifecycle events	**M**	Subscribe to contract events such as SLA threshold warning, SLA breach, termination etc.
Notes		
none		

5.3.7 Identity Management and Permissions Management

5.3.7.1 Overview

The goal of Identity Management and Permissions Management is to supply the mechanisms required for generating unique identifiers in 5GZORRO ecosystem, recognising communicating endpoints, identifying and authenticating entities, services, and organizations, and authorising consumer requests to access a preserved services and resources.

In its present form, Identity Management is able to identify providers, consumers, services, resources, organizations, etc., using Decentralized Identifiers (DIDs) associated with Verifiable Credentials. Through these Verifiable Credentials, it is possible to authenticate the issuance by a certain Issuer. In the case of Permissions Management, this allows setting up a secure layer that regulates the access to resources, services, and delimited areas using a set of policies and rules. By means of policies and rules, each domain can determine the amount of information exposed, the duration for which that information is shared, what kind of information is shared, limiting resource capabilities, and so on. Therefore, each domain must define its policies and rules based on its criteria such as improving security, usability, availability, and cost-efficiency.

In the end, Permissions Management attempts to prevent unauthorised access to services, resources, and data, making access control enforcement as granular as possible.

5.3.7.2 Provided Services

The main services provided by Identity and Permissions Management mechanisms are: an appropriate mechanism to identity entities, services, resources, consumers, providers, and organizations, which allows decentralisation of the system without forgetting the security principles; a reliable authentication using Decentralized Identifiers (DIDs), DID Communication Protocols, and Verifiable Credentials; and finally, a granular control access mechanism that standardises authorised access to data, resources, and services.

Table 5-8: Definition of identity and permissions management service (domain level)

Service name: **Per-domain Identity and Permissions Management**		Type: ***Per-domain***
Capabilities	**Support (O|M)**	**Description**
Request Stakeholder Identity	**M**	It allows an interested party to request a new stakeholder credential, specifying its role on the marketplace, assets that it partakes in, organization info, etc., in the 5GZORRO ecosystem.
Check Operation in Progress	**M**	It returns the current status of a requested stakeholder credential.
Check Operation	**M**	It gives back the current status of a finished stakeholder registry operation.
Create Identity Proof	**M**	Generates a Proof object based on the issued stakeholder Verifiable Credential
Create Operator Keys	**M**	Generates a pair of keys to enable cross-domain End-2-End Security operations.
Create DID	**M**	It is used to append a unique Decentralized Identifier to SLAs, Product Offers, etc.
Check DIDs	**M**	It enables the stakeholder to check which DIDs has issued.
Request License	**M**	It allows a registered stakeholder to request a new stakeholder license, specifying its services in the 5GZORRO ecosystem.
Check Licenses	**M**	It returns the information of all stakeholder licenses that are requested, accepted or rejected.
Notes		
none		

Table 5-9: Definition of identity and permissions management service (cross-domain level)

Service name: **Cross-domain Identity and Permissions Management**		Type: ***Cross-domain***
Capabilities	**Support (O|M)**	**Description**
Resolve Stakeholder Identity	**M**	Capability provided to an Administrator to resolve a requested stakeholder credential.
Revoke Stakeholder Identity	**M**	Administrator functionality that disables a decentralised identifier (DID) stakeholder credential from the 5GZORRO system.
Authenticate Identity	**M**	It verifies the Proof of Ownership of a stakeholder's membership by an issuance-capable Agent.
Verify Operator Keys	**M**	It allows the key pairing of a certain Operator to be validated by any other of the existing Domain Operators.

Resolve Stakeholder License	**M**	Capability of a Regulator to resolve a requested stakeholder license.
Notes		
none		

5.3.8 Trust Management Framework

5.3.8.1 Overview

The Trust Management functional block aims to provide the capabilities and operations required to administrate the trust and reputation evaluation of internal entities and resources, and the ones of other stakeholders.

A key capability for 5GZORRO architecture is to evaluate the trustworthiness of the infrastructure and activities of other stakeholders in order to decide with which stakeholder commercial relationships will be established based on its reputation, for example buying processing capabilities to a 3rd party in order to enhance the service performance.

Figure 5-6 shows a diagram of the architecture model of the Trust Management functional block, which is divided into four phases. The first phase is about the collection of trust statements from a set of trust sources. As we can see on the left side of Figure 5-6, there are three principal interfaces that may be employed by the Trust Management Framework to gather trust information: The Data Lake platform, the resource & service catalogue, and the smart resource & service discovery. After gathering trust information, this first module is also able to infer statements through direct trust (trust history) and indirect trust (recommendations).

The second phase consists of evaluating the trust level of an entity based on direct and indirect trust previously acquired. In this vein, the trust assessment module plays a pivotal role. On the one hand, this module contemplates a decentralized trust model named PeerTrust which considers statistical measures to forecast trust scores. In the current design, the Trust Management Framework leverages the PeerTrust model as the main technique to compute a trust score between two stakeholders, and in consequence, establish a trustworthy business relationship. On another hand, this module should withstand conventional trust model attacks such as bad-mouthing attack (dishonest recommendations) and Sybil attack (multiple identities, associated with the same entity, increasing/decreasing reputation).

Then, the third phase oversees storing trust information (direct trust, indirect trust, results, interactions, etc.,) since trust is considered as a long-term process, and in consequence, it is paramount to keep track over time. Regarding trust results and evidence storage, the Trust Management Framework introduces two main storage sources based on the type of information. In the first place, this framework contemplates the Data Lake platform as a feasible storage source of trust information that could be shared with other 5GZORRO stakeholders. Nonetheless, Data Lake platform should not record sensitive information or intra- and inter-domain policies and rules that the Trust Management Framework may utilise to make decisions. In those cases, a stakeholder can store its information in a dedicated and private trust score database.

Finally, the fourth phase brings an essential characteristic of trust models, dynamicity, and context-dependence. Trust is understood as a concept that changes over time, and consequently, it is required to identify and set a collection of triggers that enable to bring the trust establishment up to date. In this regard, security threats from the security analysis service, SLA violations from the SLA breach predictor, and changes in relationships are contemplated as events and triggers that allow continuously updating trust scores, at the same time they boost a zero-touch approach.

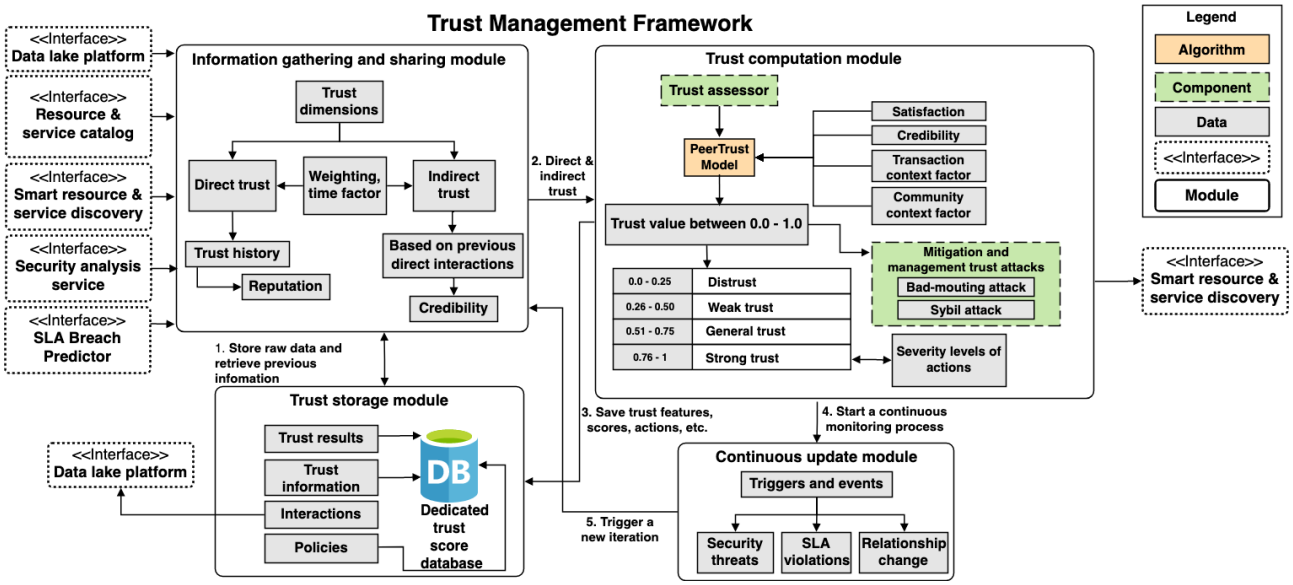

Figure 5-6: Trust Management Framework architecture model.

5.3.8.2 Provided Services

The Trust Management services and interfaces are described separately, differentiating between intra- (see Table 5-10) and inter-domain (see Table 5-11) services. 5GZORRO follows a Zero Trust approach for the management of the resources, this is, there is no differentiation or security guarantee based on the resource location, this is, if the resource is inside or outside the stakeholder private network.

Besides, note that the Trust Management services can, and should, be deployed and utilised in parallel, combining their capabilities to ensure a correct functioning of the rest of the elements of the architecture.

Table 5-10: Definition of trust management service (per-domain level)

Service name: **Per-domain Trust Management**	Type: ***Per-domain***
Capabilities	**Support (O|M)**	**Description**
Start Data Collection	**M**	It is responsible for handling the cold start of the Trust Management Framework
Stop Trust Relationship	**M**	It disables the process of collecting trust information about a stakeholder as well as a relationship with it.
Request Trust Scores	**M**	It sends a list of offers to the Trust Management Framework received by the Smart Resource and Service Discovery.
Gather Information	**M**	It activates the process of collecting trust information about a stakeholder from data sources.
Compute Trust Level	**M**	This method calculates trust level of the stakeholder to some internal resource using the previously acquired parameters.
Store Trust Level	**M**	This capability enables to records the previously calculated trust level and the utilized information in the available storage sources.
Update Trust Level	**M**	This capability enables to update a trust score of an ongoing relationship, based time-driven and event-driven mechanisms.
Notify Final Selection	**M**	This method is employed by the ISSM-WFM to notify the Trust Management Framework the final resource or service/slice selected and on which the Gather Information service will be launched internally.

Notes
none

Table 5-11: Definition of trust management service (cross-domain level)

Service name: **Cross-domain Trust Management**		Type: **Cross-domain**
Capabilities	**Support (O|M)**	**Description**
Query Trust Level	**M**	This capability enables to request the current trust level of a particular resource.
Notes		
none		

5.3.9 Trusted Execution Environment Management

5.3.9.1 Overview

Trusted Execution Environment (TEE) is an isolated processing environment in which services, tasks, and applications can be securely executed irrespective of the rest of the system. Hence, this technology can withstand usual software attacks and physical attacks such as access-based and contention-based cache attacks. Regarding their functionality, the TEEs are mainly made of hardware-based solutions which guarantee a secure memory area, software-based solutions which protect the kernel and operating system via robust cryptographic methods, and integrated hardware-software solutions. Therefore, TEE solutions ensure both secure isolation and remote code and data integrity attestation.

Since trust is an essential capability for 5GZORRO ecosystem, TEEs enable the code and data loaded within these isolated environments to be protected with respect to integrity and confidentiality.

As previously described in D2.2 and D2.3, 5GZORRO has adopted a hardware-based TEE approach, specifically Intel's SGX (Software Guard Extension). This technology is basically a set of security related instruction codes, at the CPU level, that can define private regions of memory (enclaves). The contents of those enclaves are protected, and unable to be read or saved by processes outside the region, enabling the protection of code and data from disclosure or modification.

The SCONE framework was selected to enable the TEE capabilities. SCONE abstracts the interface within Intel SGX and allows the secure and trusted instantiation of container-based services in a TEE environment. More specifically, it provides the ability to transform a base container image into a confidential container image, working with some base software requirements like docker and a Kubernetes service. SCONE also exposes a set of APIs which can be used by the Trusted Execution Environment Management service, as reported in D4.1.

It has also been determined SCONE's ability to work in an OpenStack and Kubernetes environment. Figure 5-7 depicts a particular scenario: the OpenStack instance is running under a partner's domain and the TEE-powered NFVI is in a public cloud, providing the provider's ability to deliver underlying (bare-metal) SGX support.

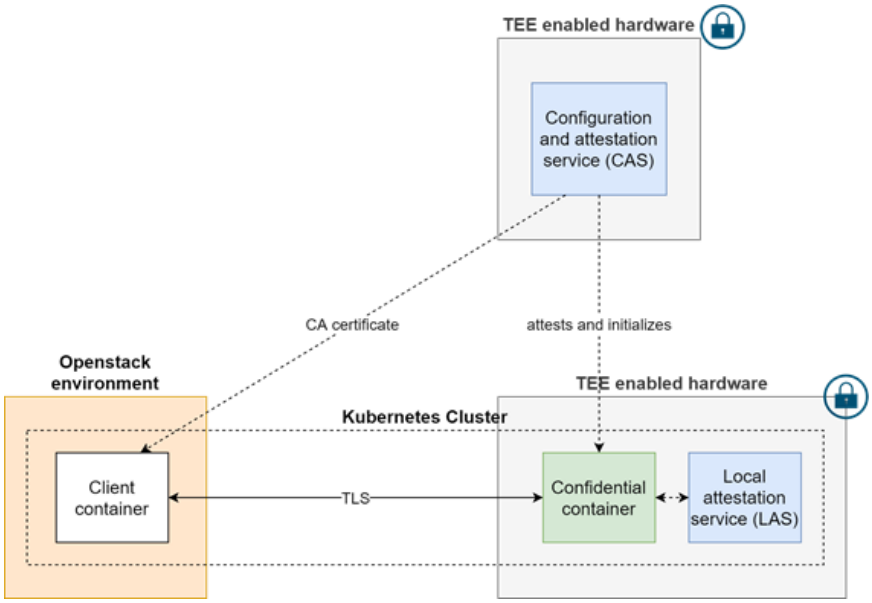

Figure 5-7: TEE cluster in an OpenStack and Kubernetes environment.

With respect to the functional view of the architecture, SCONE enhances 5GZORRO's ability to run 5GZORRO core components in a TEE environment. The CAS component, made available by SCONE during development, is also a new module that shall encompass the set of 5GZORRO core services.

5.3.9.2 Provided Services

It is envisioned that the TEE Management service provides the required functionalities to integrate TEEs in the execution of some 5GZORRO components, enhancing the security and trust of the software executed under those components.

Given the premise that raw monitoring data exists on the data lake, from a trusted source, and that it is verifiable (signed and hashed), there remains an assortment of other platform functions that aggregate, process or produce alerts over that data. Potentially ran by the service providers themselves. We can leverage TEEs here to give a high assurance to all stakeholders about the integrity of the execution of those functions. In that sense, when it comes to running core 5GZorro elements in a TEE, SLA Monitoring and Monitoring Data Aggregation (MDA) have been primarily selected, to assure the aggregation/processing/computation integrity of SLA monitoring data and to guarantee that the detection of SLA violations occurs in a safe environment.

We can run the MDA aggregator and SLA monitoring components under TEE as depicted in the following picture:

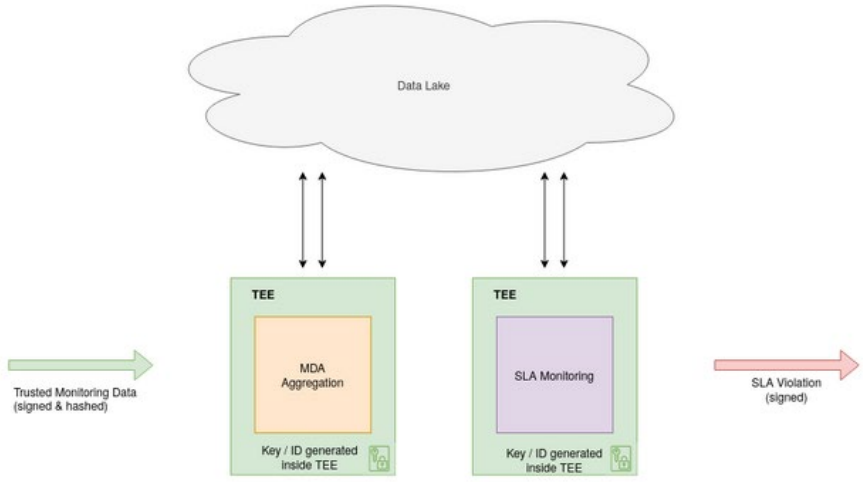

Figure 5-8: MDA and SLA Monitoring running under a TEE.

However, to execute this flow, a platform CAS service (made available by SCONE) is required, and also a service component to manage it (TEE Management service/TEE Manager). To attest that the components are being executed untampered on a TEE we need a source of truth for the expected measurement of the enclave. The TEE Management service has the capability to attests components running under a TEE by checking if the measurement corresponds to an expected value.

The following table depicts the principal TEE intra-domain services.

Table 5-12: Definition of Trusted Execution Environment Management service (domain level)

Service name: **TEE Capabilities Management**		Type: ***Per-domain***
Capabilities	**Support (O|M)**	**Description**
Get TEE components	**O**	Retrieves list of object components instantiated on a TEE and their attestation information.
*Get TEEs**	**O**	This capability enables to acquire the current TEEs available in which code and service execution can be carried out.
*Create TEE connection**	**O**	This capability initializes and configures the connection with the available or selected TEE.
*Execute command in TEE**	**O**	This capability allows to execute commands in the TEE once a connection has been established.
*Delete TEE connection**	**O**	This capability deletes the connection with the TEE, deleting all the data left in the environment.
Notes		
*These functionalities are provided by SCONE set of APIs and may not be directly exposed by the TEE Management service.		

5.3.10 Intra-domain Security at the Business Level

5.3.10.1 Overview

This functional block emerges from the subdivision performed over the previous Trust & Security Management originally included in the D2.2 initial architecture. It aims to provide the security services in charge of performing network diagnostics, to detect possible network vulnerabilities, attacks or threats for

Network Services inside each domain. Besides, the use of this module can enhance the trust relationship between stakeholders, increasing it as there is a proven measure of internal security.

This functional block applies security analysis mechanisms for the collection and monitoring of network service metrics, in order to efficiently analyse the network traffic and detect possible network vulnerabilities or malicious behaviour. These diagnostics could be stored as aggregated reporting/statistics, in order to be further provided to TMF component.

In this sense, this functional block is designed to protect the 5GZORRO platform modules, resources, and services, as well as network infrastructure of the 5GZORRO platform consumers, such as mobile core infrastructure with MANO or mobile edge.

5.3.10.2 Provided Services

The services provided by the inter-domain security module are described in Table 5-13.

Table 5-13: Definition of Intra-domain Security service (per-domain level)

Service name: **Intra-domain security**		Type: ***Per-domain***
Capabilities	**Support (O|M)**	**Description**
Set network traffic mirroring	**M**	This capability sets the live mirroring of network traffic of different network services to an active monitoring interface through a virtual TAP VNF.
Set network traffic monitoring interface	**M**	This capability sets the monitoring interface for the collection and monitoring of incoming network traffic.
Start network analysis of the collected data	**M**	This capability allows to perform real-time security network analysis of the collected data in order to obtain diagnostics and store statistics.
Stop network analysis of the collected data	**M**	This capability disables the performance of real-time network analysis.
Notes		
none		

5.3.11 Inter-domain Security at the Communication Level

5.3.11.1 Overview

This functional block emerges from the subdivision performed over the previous Trust & Security Management originally included in the D2.2 initial architecture. It aims to provide the capabilities for generating secure point-to-point and on-demand connections between entities located in different domains.

Then, this functional block integrates Virtual Private Network (VPN) technologies with the Identity and Permissions Management (Id&P) and the Network Service Mesh Manager (NSMM) functionalities to offer automated VPN-as-a-Service functionalities. These services are designed both from a server and client perspective, allowing automated interactions and connection setup. Besides, they can be also deployed as a gateway-to-gateway service, decoupling the network configuration from VNFs and other delegated resources.

The design of this module follows a lightweight approach, ensuring privacy, security, and trust properties but without sacrificing performance. First and foremost, the Id&P Management service, under the demand of the NSMM, generates a unique decentralized identifier (DID) and a key pair, which will be forwarded to the proper gateway, in order to configure it as a server or client. Subsequently, each gateway is bound to authenticate the public key and the associated DID of the other end of the connection. Hence, the gateways will contact the proper Id&P Agent to check whether the public key is correctly linked to the shared DID. Lastly, the VPN instances will carry out the network configuration as well as set up the on-demand tunnel, which will be leveraged for the NSMMs so as to swap traffic across domains.

5.3.11.2 Provided Services

The services provided by the inter-domain security module allows users to create and remove secure point-to-point connections, verify gateway identity and guarantee privacy and security across domains. For supporting these capabilities, it needs to expose the services in Table 5-14 and Table 5-15.

Table 5-14: Definition of Inter-domain Security service (per-domain level)

Service name: **Inter-domain security establishment**		Type: ***Per-domain***
Capabilities	**Support (O|M)**	**Description**
Launch VPN	**M**	This capability retrieves the key pair and the DID in order to configure a VPN as a server and generates server configuration.
Connect VPN	**M**	This capability enables to launch a secure communication between two stakeholders through a tunnel.
Add Client	**M**	This capability enables to add new clients to the server.
Disconnect VPN	**M**	This capability enables to finish a previous connection.
Remove Client	**M**	This capability deletes old clients on the server.
Notes		
none		

Table 5-15: Definition of Inter-domain Security service (cross-domain level)

Service name: **Inter-domain security establishment**		Type: ***Cross-domain***
Capabilities	**Support (O|M)**	**Description**
Get Server Configuration	**M**	This capability enables to know, from client side, the necessary configuration to later establish a connection through a VPN.
Notes		
none		

5.3.12 Communication Fabrics

5.3.12.1 Overview

The communication fabric provides a set of services that make possible the integration and interoperation of the 5GZORRO services, facilitating the flexibility to allow closed loops automation across domains. The communication fabric allows cross-domain access to the 5GZORRO services' exposure and communication, using management data transport (streaming data to subscribers), management service exposure (service publication, discovery, consumption) and management service control (e.g., authorization, access control).

The cross-domain communication fabric facilitates the reachability of cross-domain services and the access of cross-domain endpoints. This also includes services for the communication between 5GZORRO services, which facilitates the provisioning of metadata to authorized consumers who require them.

5.3.12.2 Provided Services

The provided services by the Communication Fabric component are directly inherited from the ETSI ZSM reference architecture and comprises this set of mandatory capabilities:

- **Service registration**: Manage (create, read, update, delete, list) registrations of 5GZORRO services.

- **Service discovery**: Manage the requests for registered services, providing access to their capabilities and notifications about potential changes in the location or availability of the services.
- **Communication** service: Enables communication between two or more services using a set of communication channels.

5.3.13 Network Slice and Service Orchestration

5.3.13.1 Overview

The Network Slice and Service Orchestration is responsible for the deployment of network slice instances, together with the orchestration of network services composing such network slices, in order to provide the associated communication services. This functional block provides a service that can be offered and consumed at the two different levels considered in 5GZORRO, the intra and the cross-domain. This latter is considered optional since the cross-domain orchestration decisions can also be taken at the level of network slice optimization (See Section 5.3.17) and enforced towards different instances of per-domain network slice and service orchestration functional elements.

5.3.13.2 Provided Services

The Network Slice and Service Orchestration service allows users to create and maintain network slice instances via traditional LCM operations. By using this service, users can establish a logical network that uses infrastructure resources contained inside a single domain or that expands across multiple administrative domains. This function is also responsible for the instantiation, run-time operation and orchestration of services that rely on the abstracted view of the underlying infrastructure that slices provide.

Taking into account the diverse nature of stakeholders targeted in 5GZORRO, in the cross-domain scope two scenarios are contemplated: i) slice setup with 3rd party resources and ii) slice setup with 3rd party orchestrated services. The former refers to the case in which a slice creation/extension is done using leased resources (including VNF resources) but the orchestration is only handled by the purchaser domain; while the latter targets the composition of cross-domain slices by concatenating services offered by different domains, each one with its own orchestration deployment.

More details about the service capabilities at domain and cross-domain levels are outlined in Table 5-16 and Table 5-17, respectively.

Table 5-16: Definition of network slice and service orchestration service (domain level)

Service name: **Per-domain Network Slice and Service Orchestration**		Type: ***Per-domain***
Capabilities	**Support (O|M)**	**Description**
Manage slice lifecycle	**M**	Manage the lifecycle of slices that are deployed within the domain. The slice composition in terms of resource technologies is determined by the infrastructure of the considered domain. This capability supports traditional LCM operations (i.e., creation, modification and removal).
Manage services lifecycle	**M**	Manage the lifecycle of network services that are deployed over a given slice within the domain. This capability supports service-specific LCM operations, including instantiation, configuration, scaling and removal.
Provide slice(s) information	**M**	Provide on-demand information regarding slice description (including hosted NFs) and operational status for one or several slices.
Provide notifications about slice changes	**O**	Keep updated information in the data lake about lifecycle changes of slices (including changes on hosted NFs).
Notes		
none		

Table 5-17: Definition of network slice and service orchestration service (cross-domain level - Optional)

Service name: **Per-domain Network Slice and Service Orchestration**		Type: ***Cross-domain***
Capabilities	**Support (O|M)**	**Description**
Manage slice lifecycle	**M**	Manage the lifecycle of slices that span across multiple administrative domains by including infrastructure resources from 3rd party domains. This capability supports the same operations as its per-domain counterpart.
Manage services lifecycle	**M**	Manage the lifecycle of services that are deployed over infrastructure resources from 3rd party domains (in a cross-domain slice). This capability supports the same operations as its per-domain counterpart.
Coordinate slice setup with 3rd party orchestrated services	**M**	Interact with other network slice and service orchestration services to setup cross-domain slices containing resources and services orchestrated by 3rd party domains.
Provide slice(s) information	**M**	Provide on-demand information regarding slice description (including hosted NFs) and operational status for one or several slices.
Provide notifications about slice changes	**O**	Keep updated information in the data lake about lifecycle changes of slices (including changes on hosted NFs).
Notes		
none		

5.3.14 e-Licensing Management

5.3.14.1 Overview

5GZORRO offers a cross stakeholder e-License management in the form of an microservice-based agent (eLMA) fully integrated in the orchestration mechanism of the 5GZORRO Platform. Its scope and main characteristic have been introduced in Section 3.5.

The e-License management service is designed for the metric-based control of the proprietary Virtual Functions (VFs) in the different domains. The licensing agreements signed in the smart contracts that grants the use of the VF are translated in the licensing manager to pieces of software to observe the actions that are produced in the tracked VFs that are called watchers. Therefore, every action produced in each domain for every license-controlled VF is tracked and evaluated for the licensing fulfilment.

The e-Licensing Manager Agent makes use of a synchronization interface between analogous instances in different administrative domains instead of having part of the control logic centralized. This new functionality still allows the horizontal growth of new domains that want to use the 5GZORRO system to offer or consume services while reduces the complexity of the initial configuration and simplifies the data management too since no domain-specific data ever exits the domain where it was obtained from.

5.3.14.2 Provided Services

In order to make possible this metric control, the eLMA should request the agreement for each VF to evaluate the potential licensing terms associated and generate the licensing watchers lied to these licensing terms. Once the watcher tied to a VF is activated due to an instantiation, scale, termination, etc. The eLMA should be capable to launch the action record request in the DLT. Watchers provide validation in two stages:

- At instantiation time they check that the attached Product Offering DID exists in marketplace of the administrative domain where the VF is going to be deployed. Every involved Resource and Service Specifications as well as associated Product Offering Prices are fetched from the marketplace, which are used in combination with information obtained directly from the infrastructure manager (MANO

or k8s) to ensure that the instantiation and the agreement are aligned. Licensing expiration checks are performed and lastly, checks against the licensing constraints are evaluated based on the instantiation information and provided records from neighbouring e-Licensing Managers.

- For those cases in which the instantiation is permitted, watchers remain actively keeping track of the status and licensing metrics of the VFs. Additionally, it continues to check for expiration and constraints breaches of the license for the full lifecycle of the instance.

In order to support these capabilities, it needs to expose the services in Table 5-18 and Table 5-19.

Table 5-18: Definition of e-Licensing Management service (domain level)

Service name: **e-Licensing Management**		Type: ***Per-domain***
Capabilities	**Support (O|M)**	**Description**
Licensing control trigger	**M**	Capability of the technical orchestrator (NSSO or ISSM-MEC) to notify the e-Licensing Manager that licensing control needs to be checked in a specific software resource which is about to be deployed.
Read resource agreements	**M**	Retrieve the licensing terms for the service from the Marketplace
Read application metrics	**M**	Licensing terms may rely on application metrics which are provided in the data lake through the MDA.
Licensing watchers LCM	**M**	Create, remove, update the licensing watchers to observe the VF licensing events in the virtualized infrastructure
Read VF status	**M**	Watchers need to check the status and information of VFs to ensure that there is not a breach on the licensing terms.
Trigger action record	**M**	Create the action record request in the DLT.
Notes		
none		

Table 5-19: Definition of e-Licensing Management service (cross-domain level)

Service name: **e-Licensing Management**		Type: ***Cross-domain***
Capabilities	**Support (O|M)**	**Description**
Licensing control synchronization	**M**	Capability to communicate with analogous instances of e-Licensing Management Service in a different administrative domain to ensure that the licensing constraints are verified in an aggregated way.
Action notification	**M**	Manage ACK/ERROR notifications of the licencing actions recording to the stakeholders.
Notes		
none		

5.3.15 Monitoring Data Aggregation

5.3.15.1 Overview

The 5GZORRO framework provides configurable SLA monitoring as described in Section 5.3.16. The metric collection, aggregation and reporting of the aggregated metrics is performed by the Monitoring Data Aggregation (MDA) functional block. The MDA is a new 5GZORRO functional block that has emerged when it was decided to have all related SLA monitoring intelligence functionalities in a single functional block by merging "Service & Resource Monitoring" into "Intelligent SLA breach predictor". In this way, it is possible to

have the right functional workflow, where MDA aggregates monitoring data prior to send it to the Data Lake while the Intelligence SLA monitoring breach Prediction functionalities (Section 5.3.16) gets data from the Data Lake.

5.3.15.2 Provided Services

The main service provided by Monitoring Data Aggregation is the management of data monitoring configurations, sent by the Network Slice and Service Orchestration. For this, the MDA implements mechanisms to manage queues and to aggregate the read data. This data, which can also be sent as real-time direct readings, is then sent to the Data Lake.

The Table 5-20 displays the available endpoints to management of data monitoring configurations:

Table 5-20: Definition of Management of Data Monitoring Configurations

Service name: **Management of Data Monitoring Configurations**		Type: ***Cross-domain***
Capabilities	**Support (O|M)**	**Description**
Create monitoring specification	**M**	Creates a monitoring specification with dynamic configuration variables. This operation queues the metrics to read and triggers all MDA mechanisms to aggregate and send the read data to the Data Lake.
Enable monitoring specification	**M**	Enable a certain monitoring specification associated with a certain ID. This option is available for disabled and incomplete monitoring specifications.
Disable monitoring specification	**M**	Disable a monitoring specification associated with a given ID. This operation keeps the monitoring specification available for reactivation for as long as the user intends.
Modify monitoring configuration	**M**	Modify a monitoring data fetching configuration, i.e., Data Lake topic, metrics to be queried, etc., associated with a given ID.
Check monitoring configuration	**M**	Retrieve one of the registered monitoring specifications.
Check all monitoring configurations	**M**	Retrieve all the currently registered monitoring specifications.
Discard monitoring configurations	**M**	Permanently remove an existing monitoring configuration in the system.
Notes		
none		

5.3.16 Intelligent SLA monitoring & breach prediction

5.3.16.1 Overview

This functional entity consists of two main services:

1. *SLA Monitoring* service which collects, and analyses aggregated monitoring data, detect violations in SLAs. The Marketplace (Section 5.3.1) can be notified about SLA violations and the appropriate smart contract is subsequently notified for re-calculating SLA status. This service is provided by the Smart Contracts Lifecycle Management functional block (Section 5.3.6) and works closely with the DLT and Smart Contracts to realise trustworthy SLA governance.
2. *Intelligent SLA Breach Prediction* (ISBP) service which collects, and analyses aggregated monitoring data using AI techniques, in order to predict possible breaches in SLAs and detect anomalies. The

Intelligent Network Slice and Service Orchestration functional block (Section 5.3.17) could use this information, in order to proactively allocate additional resources before the SLA violation to effectively prevent it. This service operates off-chain in the Data Lake.

Both services subscribe to receive aggregated monitoring data from other 5GZORRO functional entities, such as the Monitoring Data Aggregation (Section 5.3.15). Then, the SLA Monitoring uses this data to detect SLA violations and inform the related smart contracts, while the SLA Breach Prediction uses historical and current aggregated monitoring data to predict SLA violations. Other 5GZORRO functional blocks, such as the Intelligent Network Slice and Service optimization (Section 5.3.17), can subscribe to the SLA Breach Prediction service for specific SLAs/Contracts, in order to receive SLA breach predictions and anomaly detection indicators.

5.3.16.2 Provided Services

The 5GZORRO SLA Monitoring starts operating as soon as contractual agreement is signed in the marketplace. The Monitoring Data Aggregator module is configured to collect resource monitoring data as described in Section 5.3.15. These data are then submitted to a Kafka streaming service, exposed by the DataLake module (see Section 5.3.21). SLA Monitoring service waits for new SLA events in the Datalake and then subscribes to the Datalake streaming service in order to receive the respective monitoring data. SLAs of all the active contracts are kept internally. SLA Monitoring analyses the monitoring data and compares the metrics (SLIs) such as availability or response time, with the thresholds in SLAs, in order to detect SLA violations. Other components can subscribe to the SLA Monitoring output topic in the Datalake to receive notifications about the SLA Violations and such notifications are subsequently propagated to the smart contract for the purposes of re-calculating SLA status. The types of considered violations are described in Section 5.3.6. Table 5-21 lists the SLA monitoring services, which are also part of the functionalities of the Smart Contracts Lifecycle Management.

Table 5-21: Definition of SLA Monitoring service (domain level)

Service name: **SLA Monitoring**		Type: ***Per-domain***
Capabilities	**Support (O|M)**	**Description**
Start SLA Monitoring process	**M**	On the arrival of SLA events, the service subscribes to the products in the Datalake which in turn provides the service with the monitoring data. This signals the start of the monitorization of a specific SLA which from that point onwards receive and analyse the monitoring data to detect violations.
Update SLA Monitoring process	**O**	This capability is used when there is a need to change the characteristics of an SLA Monitoring Process. It can be used when the contracts SLAs have been changed and when there is a need to add/remove SLAs or modify Start/End Times.
Terminate SLA Monitoring process	**O**	This capability is used to stop receiving and analysing resources monitoring data for specific contract SLAs.
Return active SLA Monitoring Processes	**O**	This capability is used to create a list of active SLAs Monitoring Processes.
Publish Notifications for SLA Violations	**M**	This capability is used to send to the subscribed modules SLA violations as they are occurring. The violations include the SLOs that are violated, when these violations occurred and to what extent the SLOs are violated.
Notes		
none		

The SLA Breach Prediction is similar to the SLA Monitoring service in that it consumes monitoring data provided by MDA and use this data for predicting possible SLA violation. It keeps the current status of all active SLAs and predicts whether the resource metrics violate the SLA parameter values as well as the exact time that this happens. The predictions include:

- SLA metrics (resources) that could be violated,
- Estimation of the time that these violations could occur,
- value that the resource will likely reach.

Table 5-22 provides an overview of the SLA breach prediction services.

Table 5-22: Definition of SLA Breach Prediction service (cross-domain level)

Service name: **SLA Breach Prediction**		Type: ***Cross-domain***
Capabilities	**Support (O|M)**	**Description**
Start SLA Breach Prediction	**O**	The service starts to receive and analyse resources monitoring data from the *Monitoring Data Aggregator* service for specific contract SLAs using AI techniques in order to predict possible breaches in SLAs and detect anomalies. SLA Breach Prediction process could be started by the marketplace after a new contractual agreement or by the *Intelligent Network Slice and Service Orchestration* service in order to estimate the future needs for resources.
Update SLA Breach Prediction	**O**	This capability is used when there is a need to change the characteristics of an SLA Breach Prediction Process. It can be used when the contracts SLAs have been changed and when there is a need to add/remove SLAs or modify Start/End Times.
Terminate SLA Breach Prediction	**O**	This capability is used to stop receiving and analysing resources monitoring data for specific contract SLAs.
Return active SLA Breach Predictions	**O**	This capability is used to create a list of active SLA Breach Predictions, their descriptions, their breach predictions and their subscribers.
Publish Notifications for SLA Breach Predictions	**M**	This capability is used to send to the subscribed modules predictions for SLA violations. The predictions include the SLOs that will be violated, when these violations will occur, to what extent the SLs will be violated and the level of certainty for SLAs violations.
Notes		
none		

5.3.17 Intelligent Network Slice and Service optimization

5.3.17.1 Overview

Intelligent Network Slice and Service optimization (ISSM-O) functionality is responsible for embedding a logical 5G slice topology and – broader – a topology of a communication service into the physical substrate of the 5G network. ISSM-O receives information about the high-level intent of a communication service and transforms it with topology information, annotated with latency and bandwidth for each pair of VNFs communicating in this service. Next, it uses the information about the available resources discovered via Smart Resource Discovery and which are passed to it by ISSM-WFM, to find a feasible embedding of the logical network, i.e., communication service forwarding graph, into these available network resources. An embedding is feasible when all bandwidth and latency constraints are satisfied. The optimization also

searches for the minimum cost maximum trust solution. Intelligent Network Slice and Service Optimization is a cross-domain functionality. A local instance of optimization function executes in every Operator domain. The resulting embedding, complete with the resource allocation plan, is used by ISSM-WFM to orchestrate the actual technical instantiation and implementation of the communication service.

An optimization flow can be triggered either by administrator or by components, such as Intelligent SLA Breach Prediction and Intelligent SLA Monitor, which communicate the need for mitigating SLA breaches via ISSM-WFM. The latter calls ISSM-O to perform [re]-optimization: e.g., to find an optimized embedding for scaling-out the communication service.

5.3.17.2 Provided Services

The main aim of ISSM-O is to help with arbitration among multiple alternatives for embedding of logical topologies of slices and services (i.e., help selecting available resources from the marketplace) so that trade-offs between cost, performance, and trust are optimized. It many scenarios it is not sufficient to select a highest ranked resource offer as provided by the Smart Resource Discovery capability. For example, a slice might be required to support 100K PDU sessions simultaneously. However, in the marketplace, there are no resources from a single Operator to host UPFs of the required capacity. However, a few Operators' resources can be used to host place smaller UPFs, so that collectively they will support the required QoS. This type of scenarios clearly requires mathematical optimization techniques in addition to Smart Resource Discovery functionality and this is what ISSM-O offers to the platform.

Table 5-23: Definition of 5.3.17Intelligent Network Slice and Service optimization service

Service name: **SLA Breach Prediction**		Type: ***Cross-domain***
Capabilities	**Support (O|M)**	**Description**
Allocate Slice or Service	**M**	This capability provides for cost-efficient allocation of resources present at the marketplace to implement the required slice or service.
Optimize	**M**	This capability reoptimizes resource selection for the resources allocated to a service or a slice to explore benefit from the new offerings.
Configure Optimization	**M**	This capability allows to fine tune specific optimization heuristic.
Notes		
none		

5.3.18 Abstract Resource Management and Control

The Abstract Resource Management and Control (ARMC) is a new functional block introduced in the new version of the 5GZORRO functional architecture and not reported in D2.2 [33].

This new architecture considers the feedback received from deliverables D3.1 and D4.1 because of the effort in designing the software components building the 5GZORRO Platform. Specifically, the resource management capabilities currently under consideration (virtual, radio, and spectrum) are implemented by different pieces of software logically encapsulated in a single software module, the Virtual Resource Manager.

To embed this software architectural choice into the new 5GZORRO functional architecture, this new ARMC functional block is introduced. The goal is to improve the overall understanding of the functionality of the 5GZORRO platform, based on a better alignment of the functional architecture with the software architecture and to improve flexibility, leaving the door open to the possible management of new resources, whose functional blocks would be derived from the ARMC.

The ARMC offers the two following generic services:

- Management of resource description and specification, e.g., Descriptors, images, etc.

- Monitoring of the managed resources, in terms of performance, usage and fault statistics.

These services are further specialized and extended by three derived functional blocks, as described in section 5.3.18.1, 5.3.18.2 and 5.3.18.3 below and depicted in Figure 5-2.

5.3.18.1 Virtual Resource Management and Control

5.3.18.1.1 Overview

The Virtual Resource Management and Control functional block is positioned between the Network Slice and Service Orchestration functional element and the domains' NFV MANO and optionally SDN controller components.

5.3.18.1.2 Provided Services

Main services of Virtual Resource Management and Control functional element include allocation, release, upgrade of NFVI resources, maintaining a repository of NFVI hardware (compute, storage, networking) and software resources (hypervisors), managing software images, supporting VNF forwarding graphs by assigning virtual links, subnets, and ports, and collecting performance and fault monitoring data. Additionally, it also includes instantiation, scaling, updating, and termination of VNFs based on the monitored KPI data. Therefore, Virtual Resource Management and Control is also responsible for forwarding the collected monitoring data from their managed entities to the Intelligent Network Slice and Service Optimization functional element. It is important to highlight that the set of capabilities exposed by the Virtual Resource Management and Control functional block, listed in Table 5-24, is already covered by features provided by the underlying virtual infrastructure management so, the real implementation of such capabilities can be delegated to lower management and control modules, such as VIMs and/or NFVOs.

Table 5-24: Definition of Virtual Resource Management and Control service (domain level)

Service name: **Virtual Resource Management and Control**		Type: ***Per-domain***
Capabilities	**Support (O|M)**	**Description**
Manage NFVI resources and VNFs in Edge/cloud slice subnet	**M**	Manage the lifecycle of edge/cloud NFVI resources and VNFs deployed in a slice. This is done by interacting with VIM, VNFM and NFVO components of the domain.
Provide NFVI resource and VNF performance statistics	**M**	Push monitoring data about the NFVI resource usage and VNF performance/fault statistics to the 5GZORRO operational data lake.
Manage transport network slice subnet	**O**	Manage, configure, and optimize traffic flow control within the network according to the forwarding policies defined in the domains SDN controller.
Provide transport network statistics	**O**	Push monitoring data about the transport network to Private data lake within the Intelligent Network Slice and Service Optimization functional element.
Notes		
none		

5.3.18.2 Radio Resource Management & Control

5.3.18.2.1 Overview

The Radio Resource Management & Control is a per-domain functional block responsible for (i) exposing the RAN infrastructure to the stakeholder's instance of the 5GZORRO Marketplace; (ii) managing radio parameters (central frequency, bandwidth, etc.) of each RAN node; (iii) managing RAN node sub nets (RAN slice); and (iv) configuring RAN nodes to expose radio and spectrum metrics.

5.3.18.2.2 Provided Services

The Radio Resource Management & Control offers three services to other 5GZORRO functional blocks. On the one hand, it offers a service to expose and manage the transmission parameters of each radio node in the stakeholder's domain.

The Radio Resource Management & Control offers a service aiming at managing the life cycle of RAN slice sub-nets (creation, modification, removal). A RAN slice sub-net is a subset of RAN resources. The Radio Resource Management & Control logically interconnects RAN slice sub-net to a network slice and deploys a 5G service over the radio RAN slice, which includes connecting any cellular base station in the RAN slice sub-net to the 5G core associated to the service.

The Radio Resource Management & Control component also offers a RAN node statistic service, which instructs RAN nodes to expose radio and spectrum use metrics. This metrics are a combination of radio node's internal transmission parameters and channel state measurements (received power and interference levels) from clients. This last aspect is key to get a notion of the radio environment in the whole coverage area. The metrics exposed by each RAN node can be fetched by the Monitoring Data Aggregator functional block and pushed to the 5GZORRO operational data lake for data ingestion and further processing.

Diverse radio resource providers are expected to co-exist in the 5GZORRO architecture. However, each Radio Resource Management & Control is responsible to configure the radio resources (infrastructure) within its own domain. Therefore, no cross-domain Resource Management & Control is assumed. In case a service of network slices requires to be mapped to more than one RAN slice, they communicate with each domain Resource Management & Control independently.

More details about the Radio Resource Management & Control service capabilities at domain level are outlined in Table 5-25.

Table 5-25: Definition of Radio Resource Management & Control service (domain level)

Service name: **Radio Resource Management & Control**		Type: ***Per-domain***
Capabilities	**Support (O|M)**	**Description**
Manage RAN infrastructure	**M**	Exposes the RAN infrastructure that is offered in 5GZORRO Marketplace and allows configure the radio parameters of each RAN node.
Manage RAN slice sub-nets	**M**	Manage the lifecycle of RAN slice sub-nets that are deployed within the domain. The slice composition in terms of resource technologies is determined by the SLA and infrastructure availability of the considered domain. This capability supports traditional LCM operations (i.e., creation, modification, adaptation, and removal).
Provide RAN node statistics	**M**	Configures RAN nodes to expose radio and spectrum resource use metrics.
Notes		
none		

5.3.18.3 Spectrum Resource Management & Control

5.3.18.3.1 Overview

The Spectrum Resource Management & Control functional block is responsible for the introduction of licensed spectrum assets inside 5GZORRO. Licensed spectrum is a special case among all the network resources in consideration for trading within the platform because it is the only regulated resource, subject to multiple policies and control. For this reason, the licensed spectrum resource provider, typically an MNO, must declare the spectrum assets it offers for trading within the 5GZORRO platform, and these assets need to be in alignment with a real spectrum license issued by regulators.

5.3.18.3.2 Provided Services

The scope of the Spectrum Resource Management & Control has been reduced from what was declared in D2.3 [3]. This entity is now envisioned to serve stakeholders which are in possession of a spectrum license, typically MNOs. Specifically, the Spectrum Resource Management & Control offers a service to register spectrum assets, which is the first step to onboard spectrum resources that can later be used in product offers. This service is consumed by the 5GZORRO Portal, whereby the licensed spectrum resource provider declares spectrum asset by providing its technical details, naming downlink and uplink frequency ranges, duplex mode, radio technology, operation band, and geographical area.

After receiving request for creation of a spectrum asset in the Portal, the Spectrum Resource Management & Control validates the technical information in the request by means of comparisons against spectrum certificates (digitalised versions of spectrum licenses stored in 5GZORRO's Identity Management and Permissions Manager). If the technical information of a spectrum asset matches a valid spectrum certificate, the creation request is accepted, and a spectrum resource is stored in the Spectrum Resource Management & Control. After this moment, the spectrum resource is included in the list of available network resources that the stakeholder can use to create product offers.

It is worth mentioning that the Spectrum Resource Management & Control does not offer a spectrum resource monitoring service. Nevertheless, spectrum metrics are collected from clients that are connected to base stations using spectrum resources. For this reason, the Resource Management & Control functionality block exposes both radio and channel state (spectrum) metrics in the RAN node statistics service.

Table 5-26: Definition of Spectrum Resource Management & Control service (domain level)

Service name: **Spectrum Resource Management & Control**		Type: ***Per-domain***
Capabilities	**Support (O|M)**	**Description**
Provide spectrum asset details	**M**	The licensed spectrum resource provider declares a spectrum asset and provides its technical details (frequency ranges, technology, band, and area of application). The spectrum asset is validated against currently active spectrum certificates in 5GZORRO and stored as a spectrum resource that can be included in product offers.
Notes		
none		

5.3.19 Marketplace DLT platform

5.3.19.1 Overview

A key focus of 5GZORRO is to ensure that the Marketplace remains DLT agnostic by encapsulating a series of abstract interfaces described previously e.g., Smart Contract Lifecycle Management, Catalogue etc. DLT 'Drivers' are developed for Corda to demonstrate the full capabilities of the 5GZORRO marketplace.

The Corda DLT platform facilitates the building of distributed applications (CorDapps) to extend the capabilities of the ledger, including the specification of inter-node flows, data types and smart contracts to verify transactions.

5.3.19.2 Provided Services

R3 Corda provides the following key services for realising the DLT network and building distributed applications atop [36].

Table 5-27: Definition of Corda services (cross-domain level)

Service name: **Corda**		Type: **Cross-*domain***
Capabilities	**Support (O|M)**	**Description**
States	**M**	States are classes that encapsulate on-ledger facts. Over time, states are marked as consumed/historic as generated outputs from transactions are consumed as inputs to subsequent transactions. Each DLT node has a vault where it stores all states relevant to itself.
Contracts	**M**	A transaction is contractually valid if all its input and output states are acceptable according to the contract. Contracts are deterministic classes that encapsulate logic that perform verification over a proposed update to the ledger.
Flows	**M**	Flows are a means of programmatically defining multi-step, multi-party processes for agreeing a ledger update; flow steps can be paused/check-pointed and resumed. Communication between nodes is point-to-point and only occurs in the context of flows. Corda also provides built in flows for common tasks such as finalising a transaction with the notary.
Service Hub	**M**	An API accessible from Flows that provides an interface to node functions such as: • Network map cache – node information within the network • Identity service – for Identity resolution • State/transaction access • Contract upgrade services
Transactions	**M**	A transaction in Corda is a proposal to update the ledger. A transaction will be committed to the ledger if it doesn't contain double spends, is contractually valid and is signed by the required parties. Verification of transaction input and output states is performed by Smart Contracts and final checks for double spends, transaction timestamps and - optionally - transaction validation are performed by a notary pool, a cluster of nodes that provide the point of transaction finality in the system.
Identity	**M**	Provides services for resolving and exchanging both well-known and confidential identities to facilitate the data/transaction privacy needs of the application.
RPC Operations	**M**	A node's owner interacts with their node solely via Remove Procedure Calls (RPC) and does not have access to the afore-mentioned Service Hub. Key operations available are: • Vault querying • List and execute available flows on the node • Get node info • Get information about other network participants
Vault Querying	**M**	A node's Vault stores all the states pertinent to it. It has been built from the ground up to support proven query frameworks. There are various mechanisms for querying the vault, but a VaultService provides a flexible mechanism for querying the vault and satisfies most use cases.
Persistence	**M**	Transaction state stored in the Vault is indexed for the purposes of executing queries. However, Corda also offers the ability to expose some or all of a contact state to an Object Relational Mapper (ORM) to be persisted in a relational database. This gives rise to the potential for relational joins and hierarchical data structures.
Contract Constraints	**M**	Contract constraints serve to control and agree upon platform upgrades, whilst mitigating any attack vector that could be exploited by a bad actor.
Testing	**M**	A range of tooling is provided within the Corda ecosystem such that networks can be mocked and easily interrogated which makes contract & flow development and testing significantly easier.

Notes
none

5.3.20 Identity and Trust DLT platform

The Identity and Trust DLT platform is the key enabler of the Identity & Permissions Manager, that provides trusted interactions across domains by leveraging W3C DIDs and associated Verifiable Credentials. According to these W3C standards, the Identity and Trust DLT platform provides verifiable data registry functionalities including the mediation of the creation and verification of identifiers, keys, and other relevant data, such as verifiable credential schemas, credential registries, issued wallet keys, and so on. The Identity & Permissions Verifiers ensure with certainty that the 5GZORRO Governance Board have attested something by checking digital signatures against the Identity and Trust DLT Platform.

5.3.20.1 Provided Services

The main services provided by the Identity and Trust DLT platform rely essentially on: entity registration, through the usage of seeds (wallet identifiers of a blockchain agent), management of transactions performed by the registered agents (for DID credential issuances), and also enable the status monitoring of the DLT Network nodes.

Table 5-28: Definition of identity and trust DLT platform service (cross-domain level)

Service name: **Cross-domain Identity and Permissions Management**		Type: ***Cross-domain***
Capabilities	**Support (O|M)**	**Description**
Register Agent Identity	**M**	Enables the registration of a governance blockchain Agent in the DLT network through its unique Agent seed
Check issuance transactions	**M**	Allows the logging of the DID credentials that were issued at certain times
Check DLT nodes	**M**	Displays the status and relevant information regarding the nodes that comprise the governance DLT network
Notes		
none		

5.3.21 Data Lake Platform

5.3.21.1 Overview

The Data Lake Platform functional block consists of the distributed data store and of the cloud-native workflow engine designed for the creation of custom data processing pipelines. This data architecture enables collocating the computation with the data to save data transfer costs and to improve performance and time required for AI model training and inference and also decouples the data providers from the data consumers in the system as much as possible.

Data Lake pipelines consist of a series of steps, where the first step is typically triggered by an external event, the last step typically triggers an external event or operation, while other steps are performed, serially or in parallel, in a predefined order. Out of the box, 5GZORRO implements several required data processing steps (ingest and store raw operational data; receive data from Monitoring Data Aggregator; perform analytics to predict violation of SLA; perform actions upon detection of SLA issues) and pipelines to support 5GZORRO use cases such SLA breach prediction, SLA monitoring, trustworthy slice optimization, etc. In addition to out-of-the-box steps and pipeline, it is possible to create and install additional steps and construct new pipelines out of them.

5.3.21.2 Provided Services

Data Lake Platform services allow 5GZORRO stakeholders to enjoy the supported analytical pipelines, by managing stakeholder's operational data and his configured data pipelines as summarized in Table 5-29. For example, the Operator Lifecycle service is initiated upon stakeholder registration with the 5GZORRO platform

(see Section 7.1 for the onboarding flow). When initiated, Operator Lifecycle service allocates capacity for the stakeholder's data operations, including place in the data store, private data communication channels, data governance and sharing policies, and the required data pipelines.

Table 5-29: Definition of Data Lake Platform service (cross-domain level)

Service name: **Data Lake Platform**		Type: ***Cross-domain***
Capabilities	**Support (O|M)**	**Description**
Operator Lifecycle	**M**	Manages lifecycle of 5GZORRO stakeholder across Day 0, Day 1, and Day 2 data operations – storage, communication channels, pipelines, policies, etc.
Pipeline Lifecycle	**M**	Manages lifecycle of data pipelines across Day 0, Day 1, and Day 2 of a pipeline.
Ingestion of Data	**M**	Ingests the operational data into the Data Lake and sets up the metadata in the catalogue
Searchable Metadata	**M**	Allows to search for previously ingested data
Data Lifecycle	**M**	Manages data lifecycle from its ingestion to decommission
Notes		
none		

5.3.22 5G Network Virtualization Platform

5.3.22.1 Overview

The 5G Network Virtualization Platform is responsible for abstracting and managing the underlying virtualized infrastructure and encompasses several infrastructure controllers, employed in 5GZORRO in collaboration with Virtual Resource Management and Control and Radio Resource Management & Control blocks, without any design or development by the consortium beyond the platform integration.

The 5G Network Virtualization platform offers a set of tools that are particularly useful for slice sharing among several operator's infrastructure, activating and isolating resources on demand. These tools are required to ensure the computing and storage of the requested resources and services in different domains, that could be potentially purchased in the 5GZORRO marketplace creating also the transport network.

The infrastructure controllers employed are:

- The NFV-MANO: This block is responsible for the inter-domain NFV Management and Orchestration that requires the synergy of several functional blocks and collaborating through specified reference points. The NFVO has two main functions, the NS Orchestration (NSO) and the Resource Orchestration (RO), which implement the lifecycle management of the Network Functions that compose the Network Slice Subnet Instances and the orchestration of the NFVI resources across multiple domain VIMs respectively.
- The Virtual infrastructure Manager (VIM) is responsible for controlling and managing the NFVI resources within a single domain, leveraging on hypervisors for the control of the computation/storage resources respectively.
- SDN controllers, that provides the networking between the instantiated resources that composes the shared slices and services.

6 5GZORRO Platform design

In this section, it is described how the principles discussed in Section 5.1 have been applied to provide the overall software design of the 5GZORRO platform.

6.1 Platform design principles and architectural patterns

The base idea is to design the platform as a set of modules encompassing one or more of the Functional Elements exposed in Section 5.3. Each module, and its own functionality exposed, represents a 5GZORRO Platform Service and is characterized by the following properties:

- **Loosely coupled**, i.e., is implemented minimizing dependencies between services
- **Highly maintainable and testable**
- **Independently deployable** (as much as possible) from other services and **scalable** if needed
- **Configurable at runtime**

Two main architectural patterns consider service as a key concept: *Service Oriented Architecture* (SOA) and *Microservice Architecture* (MSA). Both patterns present pros and cons and, although from a certain point of view they could be overlapped, they are characterized by several important differences.

In the SOA, the platform is structured as a collection of few services. Each service implements a complete (and even complex) functionality and all the services communicate by means of an Enterprise Service Bus (ESB), which enables discovery, connectivity and routing between services.

In a similar way, in the MSA, the platform is structured as collection of services, but each service, called "micro-service", implements one simple functionality and exposes an interface towards the final users or other services. Hence, differently from SOA, the microservices are typically in the order of hundreds. Complex tasks are implemented making microservices communicate directly with each other though well-defined interfaces using lightweight communication mechanisms, such as REST API, without the need of a central bus. In addition, in MSA, each service should maintain its own database with its data.

A third way is represented by the *Service-Based Architecture* (SBA). To the best of our knowledge, a formal definition of such an architectural pattern does not exist and it is often difficult to highlight the differences with the other service-based patterns. In [44], SBA is described as a middle ground between SOA and MSA. Nevertheless, SBA has been chosen by 3GPP as architectural pattern for the design of the 5G System Architecture [45] and by ETSI for the definition of the ZSM Architecture.

In particular, we consider ETSI ZSM as the main reference architecture for the design of the 5GZORRO platform as it is closer to the scope of the platform itself. It offers a guideline for the implementation of a zero-touch platform and, with respect to 3GPP 5G System Architecture, ETSI ZSM does not define any specific technology or protocol to be used, so becoming more suitable as “architectural template” for the aims of 5GZORRO.

6.2 Software Architecture Overview

From a software components perspective, the functional entities introduced in Section 5.3 are implemented in 5GZORRO as four distinct software platforms (see Figure 6-1).

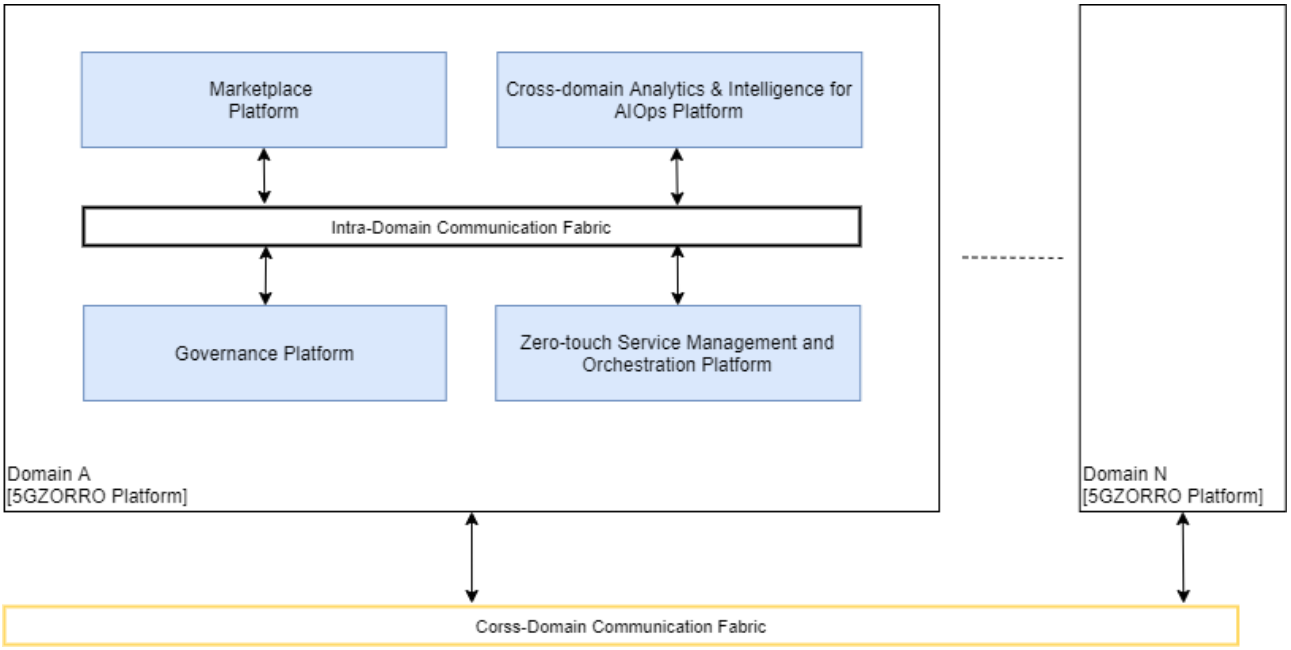

Figure 6-1: 5GZORRO Software Platform overview

The **zero-touch Service Management and Orchestration Platform** is mainly responsible to control 5G Resources including Radio Spectrum resources, Transport Networking resources and Computing resources (at data centers and at edge computing nodes) as well as existing legacy resource controllers from previous 5G deployments. 5G Resources offered in the 5GZORRO Marketplace are managed through a Resources Manager interface (including Resource offer status management and Monitoring Data Exposure) while the Network Slice and Service Orchestrator manages the life-cycle of slices and associated services at domain level and across different domains. The zero-touch Service Management and Orchestration Platform leverages data lake features (data transformation, analytics and real-time actions) to achieve the automation of some resource management procedures including a proactive scaling mechanism to increase or decrease the infrastructure capacity by using external resources published in the marketplace by Resource Providers. The zero-touch Service Management and Orchestration Platform features a Trust and Security framework to enable trustworthy usage of external resources.

The **Marketplace Platform** leverages DLT technologies including Smart Contracts technologies to enable the trade of 5G resources managed by the zero-touch Service Management and Orchestration. I.e., the 5GZORRO Marketplace is accomplished by a mesh of distributed Marketplace Platforms each one anchored to one Marketplace DLT node, and it is envisaged that each Communication Service Provider (CSP) has at least one Marketplace Platform instance deployed. The Marketplace Platform features an end-user front-end, a decentralized catalogue for 5G Resource offers and 5G Service offers, as well as the life-cycle management of smart contracts for offers and agreements between providers and consumers, as described in Section 6.5.

The **Cross-Domain Analytics & Intelligence for AIOps platform** mainly comprises the cross-domain Functionalities from the Analytics & Intelligence for AIOps logical layer, described in Section 5.2, i.e., it leverages distributed data lake and AI technologies to provide data persistence, data sharing and data analytics across domains. It includes functionalities like the ingestion and transformation of monitoring data as well as workflows created for automation of complex resource management procedures across-domain. The prediction of SLA breaches and the discovery of the most appropriated resources available in the marketplace are two examples of such resource management procedures automation. Permissions to publish resource data and to read aggregated shared data or cross-domain analytics are managed by the Governance Platform.

The **Governance Platform** is operated by stakeholders with permissions to take decisions according to the Marketplace Governance Model i.e., stakeholders playing the Governance Administrators business role, as

defined in D2.1. The Governance Platform also features the decentralized management of global (cross-domain) identifiers (stakeholder identifiers and 5GZORRO resource identifiers) according to Self-sovereign Identity principles and by leveraging DLT technologies. It supports the creation, verification and revocation of certificates as well as authentication and authorisation of identities across all 5GZORRO domains.

The **Intra-Domain Communication Fabric** and **Cross-Domain Communication Fabric** are the two different types of Communication Fabrics in the 5GZORRO Platform; the former allows modules to communicate with other modules inside the same domain, and the latter allows modules to communicate with modules in other domains. They implement the Communication fabrics functional block in the 5GZORRO high-level architecture, and, according to ETSI ZSM, the communication can be based on both publish/subscribe and request/response paradigms. In this sense, the 5GZORRO Platform design allows the implementation of both communication paradigms, by using the publish/subscribe, as much as possible, for the interaction between the service implemented from scratch in the platform, and the request-response paradigm for all those services which require it (e.g., NFVO).

Figure 6-2 provides a detailed overview of the 5GZORRO platform, consisting of four sub-systems, each with the set of specific modules implementing the functionalities described in Section 5. From an architectural point of view, the 5GZORRO follows an SBA-like pattern, where each module implements a service and communicates with other modules through the Communication Fabrics, thus formally avoiding any form of point-to-point dedicated interfacing. In order to realize the 5GZORRO services and the related operational workflows, explicit interactions between the different modules are supported by the platform, as described in Section 7 for the relevant cases.

More importantly, Figure 6-3 provides an overview of the various interactions among the 5GZORRO platform modules, with the aim of having a clearer view (that would not be possible to have with the pure SBA-like figure and communication fabrics buses) on the actual interfaces implemented. In particular, Table 6-1 and Table 6-2 provide the list of 5GZORRO reference points, with the identification of the involved modules, and a description of intra and inter platform communications supported.

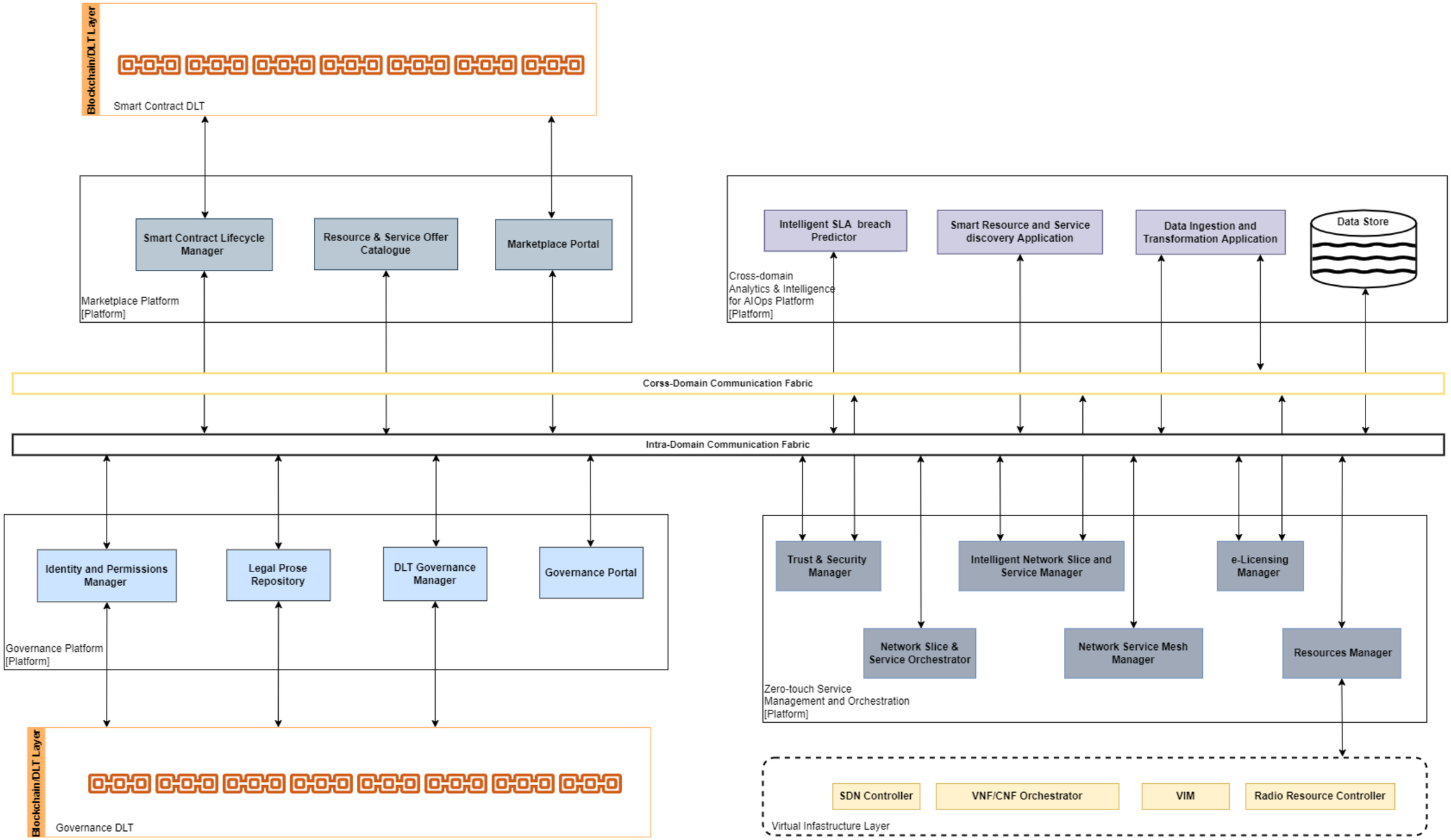

Figure 6-2: Detailed overview of the 5GZORRO Platform

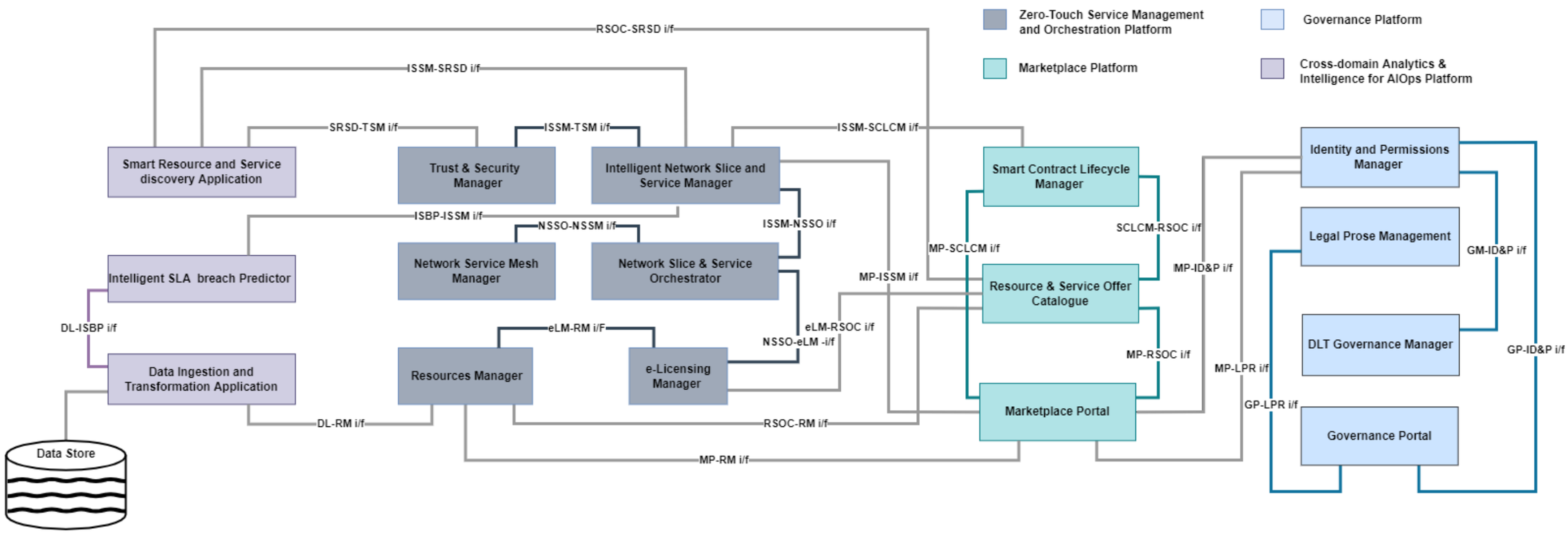

Figure 6-3: 5GZORRO Platform reference points

Table 6-1: List of 5GZORRO intra-platform reference points

Reference Point	Modules	Platforms	Description
GP-LPR	Governance Portal Legal Prose Repository	Governance	Governance portal to consume CRUD APIs of LPR
GP-ID&P	Governance Portal Identity and Permission Manager	Governance	Stakeholder credential and DID operations
GM-ID&P	Governance Manager Identity and Permission Manager	Governance	ID&P and Governance DLT operations
eLM-RM	E-Licensing Manager Resource Manager	Zero-Touch Service	e-Licensing manager to access the virtual infrastructure
NSSO-NSMM	Network Slice and Service Orchestrator Network Service Mesh Manager	Zero-Touch Service	NSSO to request VPN for multidomain secure connectivity
NSSO-eLM	Network Slice and Service Orchestrator E-Licensing Manager	Zero-Touch Service	NSSO to interact with eLM for licensing check
ISSM-NSSO	Intelligent Slice and Service Manager Network Slice and Service Orchestrator	Zero-Touch Service	Orchestration interface between ISSM and NSSO
ISSM-TSM	Intelligent Slice and Service Manager	Zero-Touch Service	Security orchestration interface

	Trust and Security Manager		
MP-SCLCM	Marketplace Portal Smart Contract Lifecycle Manager	Marketplace	Portal to access Smart Contract information
MP-RSOC	Marketplace Portal Resource and Service Offer Catalogue	Marketplace	Portal interaction with RSOC interface
SCLCM-RSOC	Smart Contract Lifecycle Manager Resource and Service Offer Catalogue	Marketplace	SCLCM to store orders on the RSOC and RSOC to pass offers to be stored in Marketplace DLT
DL-ISBP	Data Ingestion and Transformation Application Intelligent SLA Breach Predictor	Cross-Domain Analytics	ISBP to collect data stored in the DataLake to predict possible breaches

Table 6-2: List of 5GZORRO inter-platform reference points

Reference Point	Modules	Platforms	Description
DL-RM	Data Ingestion and Transformation Application Resource Manager	Cross-Domain Analytics Zero-touch	Resource Manager to push infrastructure metrics to the DataLake
ISBP-ISSM	Intelligent SLA Breach Predictor Intelligent Slice and Service Manager	Cross-Domain Analytics Zero-touch	Breach notifications and SLA activations interface
SRSD-TSM	Smart Resource and Service Discovery Trust and Security Manager	Cross-Domain Analytics Zero-touch	TSM to push reputation information to SRSD
ISSM-SRSD	Intelligent Slice and Service Manager Smart Resource and Service Discovery	Cross-Domain Analytics Zero-touch	Classified product offers collection from ISSM
RSOC-SRSD	Resource and Service Offer Catalogue Smart Resource and Service Discovery	Cross-Domain Analytics Marketplace	RSOC - SRSD interface for synchronizing about the offers
MP-RM	Marketplace Portal Resource Manager	Marketplace Zero-Touch	Resource manipulation to create offers
RSOC-RM	Resource and Service Offer Catalogue Resource Manager	Marketplace Zero-Touch	Resource information acquisition
eLM-RSOC	E-Licensing Manager Resource and Service Offer Catalogue	Marketplace Zero-Touch	Check license against the marketplace
MP-ISSM	Marketplace Portal Intelligent Slice and Service Manager	Marketplace Zero-Touch	Product Orchestration LCM
ISSM-SCLCM	Intelligent Slice and Service Manager Smart Contract Lifecycle Manager	Marketplace Zero-Touch	Smart Contract activation/deactivation
MP-ID&P	Marketplace Portal Identity and Permission Manager	Marketplace Governance	DID request for Product Offers
MP-LPR	Marketplace Portal Legal Prose Repository	Marketplace Governance	Request of Legal Templates (e.g., SLA, License, etc.) to be filled with specific values

6.3 Zero-touch Service Management and Orchestration

The Zero-Touch Service Management and Orchestration is a logical group of different software modules, all related to zero-touch service management and orchestration, and it comprises:

- The **Resource Manager** is the interface to all resource controllers in the infrastructure. It implements the Abstract Resource Management and Control functional block (see Section 5.3.18) and the following derived modules:
    - Virtual resource management and control (see Section 5.3.18.1)
    - Radio Resource Management & Control (see Section 5.3.18.2)
    - Spectrum Resource Management & Control (see Section 5.3.18.3)

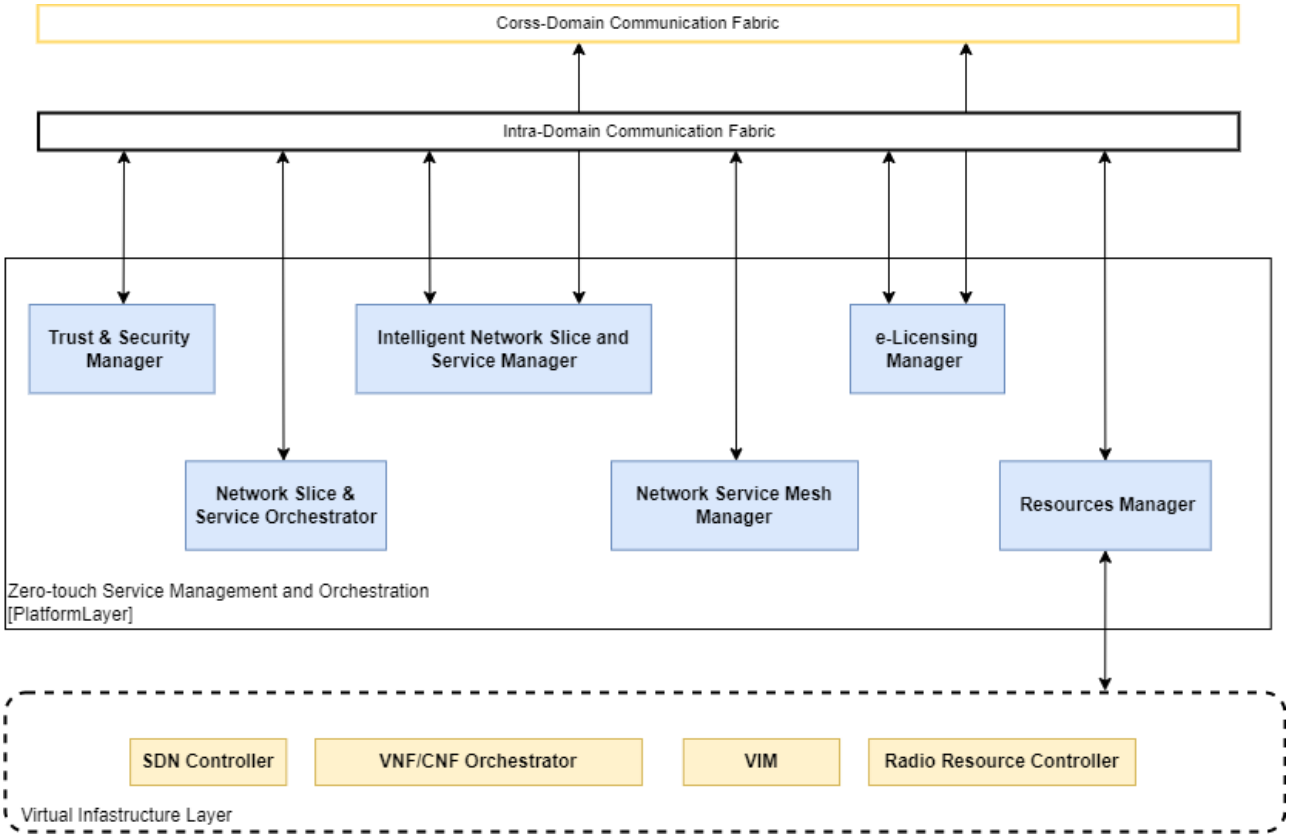

Figure 6-4: Zero-touch Service Management and Orchestration platform

- The **Network Slice and Service Orchestrator** and **Intelligent Network Slice and Service Manager** are the software modules responsible for creating and managing, in an intelligent and automated way, network slice and network service instances in the intra-domain or inter-domain environment. They implement the following functional blocks:
    - Network Slice and Service Orchestration (see Section 5.3.13)
    - Intelligent Slice and Service Management (see Section 5.3.5)
    - Intelligent Network Slice and Service optimization (see Section 5.3.17)

- The **Network Service Mesh (NSM) Manager**, is the software module that handles the service meshes and can be used for providing connectivity between different network services. It is realized as a distinct software module, implementing some functionalities of the Network Slice and Service Orchestration (see Section 5.3.13) related to service meshes, or these functionalities could be implemented in the Network Slicer module, previously described, because the management of service meshes is strictly related to the management of network slices and their network services.
- The **Trust & Security Manager** is the module responsible for evaluating the Trust and Security of a stakeholder or resources; it implements Trust and security management (see Section 5.3.8).
- The **e-licensing Manager** is the module responsible for controlling licensing terms of a service and resources published in the Marketplace and instantiated in the domain; it implements the E-licensing Management (see Section 5.3.14).

Outside the Zero-Touch Service Management and Orchestration there is the 5G virtual infrastructure, which abstracts the real 5G network elements, such as SDN Controllers, VNF/CNF Orchestrator, VIMs and radio Resource Controllers.

6.4 Governance Applications

The Governance Platform is mainly comprised by four components, as discussed below.

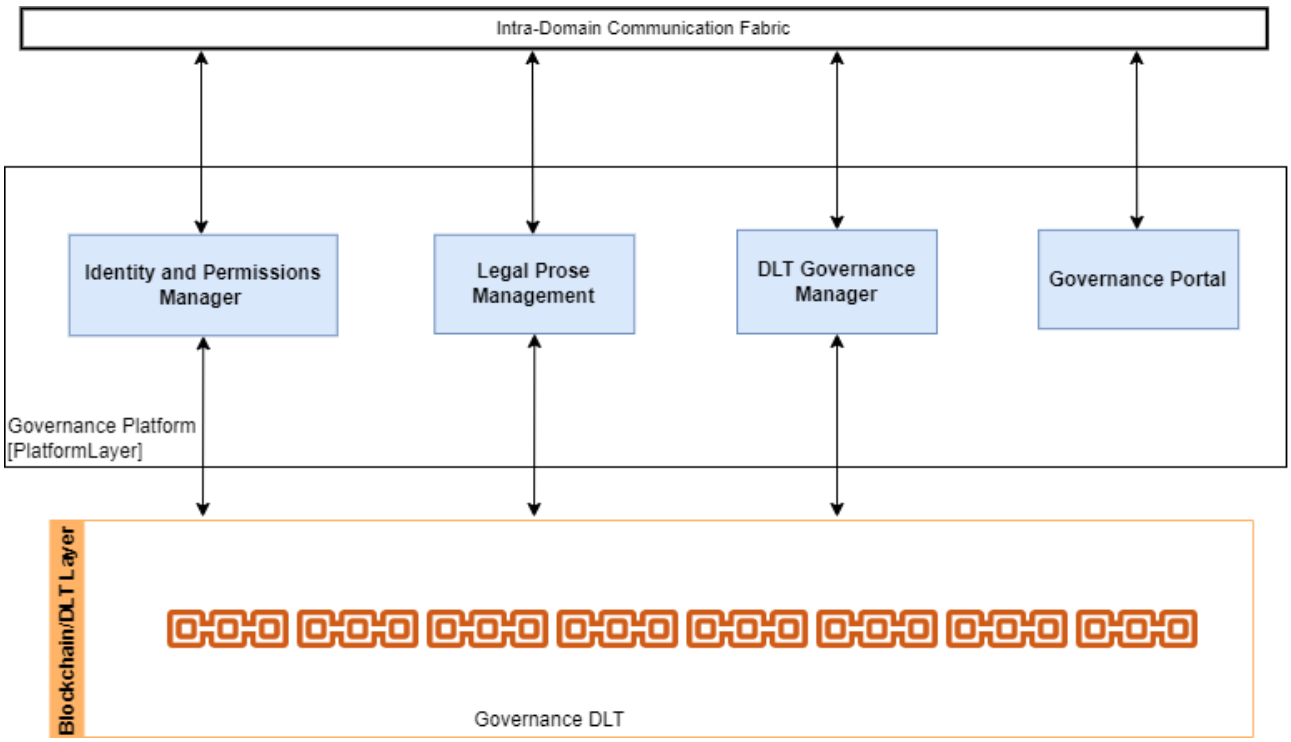

Figure 6-5: Governance Platform architecture

DLT Governance Manager: it implements the DLT Governance Management functional element as defined in Section 5.3.1, i.e., it provides functionalities to support a consortium governance model for 5GZORRO marketplace. In this way, decisions like admittance, revocation of membership and dispute resolution are managed in accordance with a mutually agreeable governance model. Any Governance decision is issued as a Verifiable Claim to be associated to some 5GZORRO Subject (Stakeholder or Business Agreement)

Legal Prose Manager: it implements the Legal Prose Repository functional element and its interfaces as defined in Section 5.3.3 i.e., it provides a shared repository of parameterised legal statement templates that can subsequently be associated with a given resource or service by providers. It is envisaged that such

parameterised legal statement templates would be Verifiable Claims data schemas that are registered in the Governance DLT.

Identity and Permissions Manager: it implements the server side functionalities for Identity Management and Permissions Management functional element and its interfaces as defined in Section 5.3.7 i.e., it provides appropriate mechanisms to identify entities, services, resources, consumers, providers, and organizations, which allows decentralisation of the system without forgetting the security principles, a reliable authentication using DIDs, and Verifiable Credentials, and finally, a granular control access mechanism that standardises authorised access to data, resources, and services. All the other 5GZORRO platforms (i.e., Marketplace, zero-touch Service Management and Orchestration and Cross Domain Analytics & Intelligence for AIOps platform) features a DID Agent component to interact with the Identity and Permissions Manager component, as DID Subjects with Verifiable Credential Holder roles i.e., it features a secure storage for the private keys and Verifiable Credentials.

Governance Portal: provides a web user interface to enable the usage of the Governance features by end-users including management of legal prose templates, tools to take governance decisions and management of Identities and Permissions.

6.5 Trustworthy Marketplace applications

The Marketplace Platform is mainly comprised by four main components, as described below.

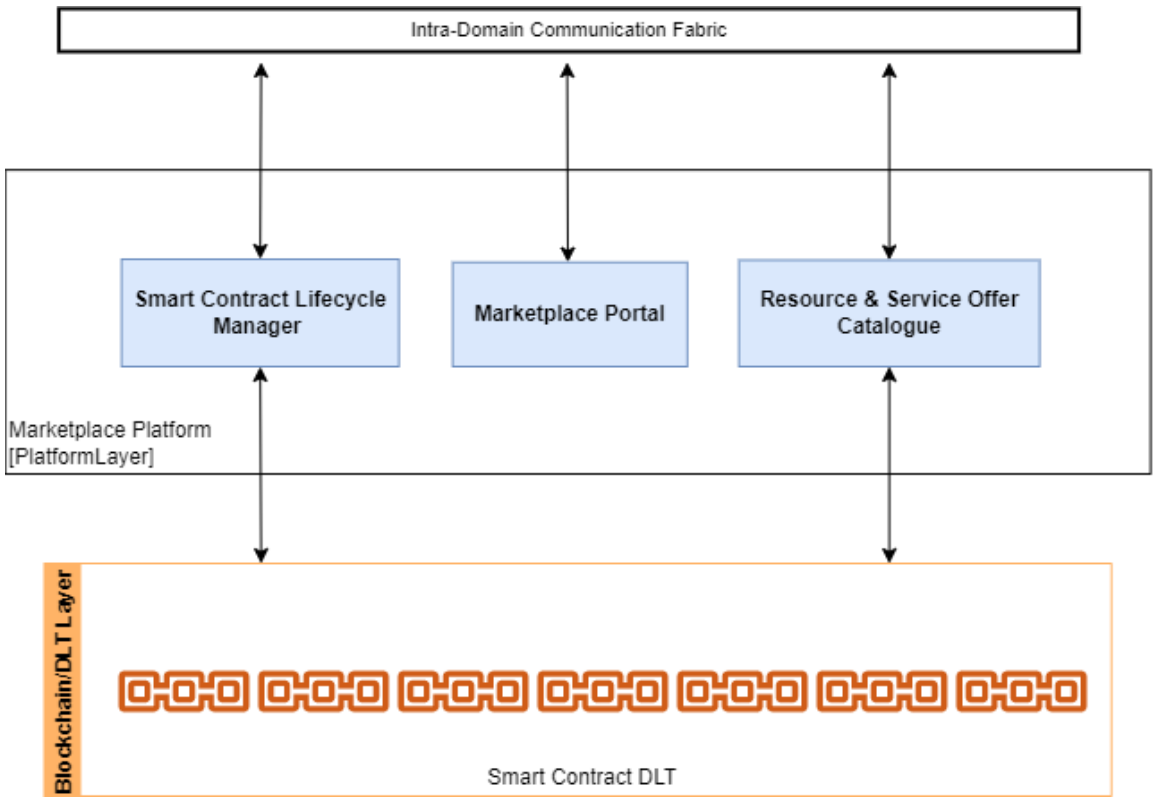

Figure 6-6: Marketplace Platform architecture

Resource & Service Offer Catalogue: it implements the Resource & Service Offer Catalogue functional element and its interfaces as defined in Section 5.3.2, i.e., it provides functionalities to publish and manage resources or services offers into 5GZORRO Marketplace, list the active resource and service offers, modify or remove a resource or service offer, and make an offer for a specific resource or service.

Smart Contract Lifecycle Manager: it implements the Smart Contract Lifecycle Manager functional element and its interfaces as defined in Section 5.3.6, i.e., it provides functionalities to manage Marketplace business

contracts (DLT Smart Contracts) throughout their lifecycle, from agreement negotiation and instantiation through to termination.

Marketplace Portal: provides a web user interface to enable the usage of the Marketplace features by end-users including the discovery of offers, management of offers and the management of business agreements.

6.6 Cross-domain Analytics & Intelligence for AIOps

The Cross-domain analytics & Intelligence for AIOps platform implements all those intelligent functionalities for AI-driven operation 5G network slices and resource and service offers and products in general. The various modules composing this platform, as show in Figure 6-7, rely on the 5GZORRO operational Data Lake to perform their analysis and output specific decisions. The operations are typically triggered by the occurrence of some event (possibly a message on a message queue) and may trigger some other event to have its output data consumed. These event and notification services run in the environment of the Data Lake, which provides the basic infrastructure to coordinate all the various operations.

Using the services of a Data Lake usually includes several coordinating steps, which can be assembled into a pipeline. The general cycle of operations is:

1. Gather data.
2. Perform some analysis on the data to obtain insights.
3. Perform some action based on the result of the analysis.

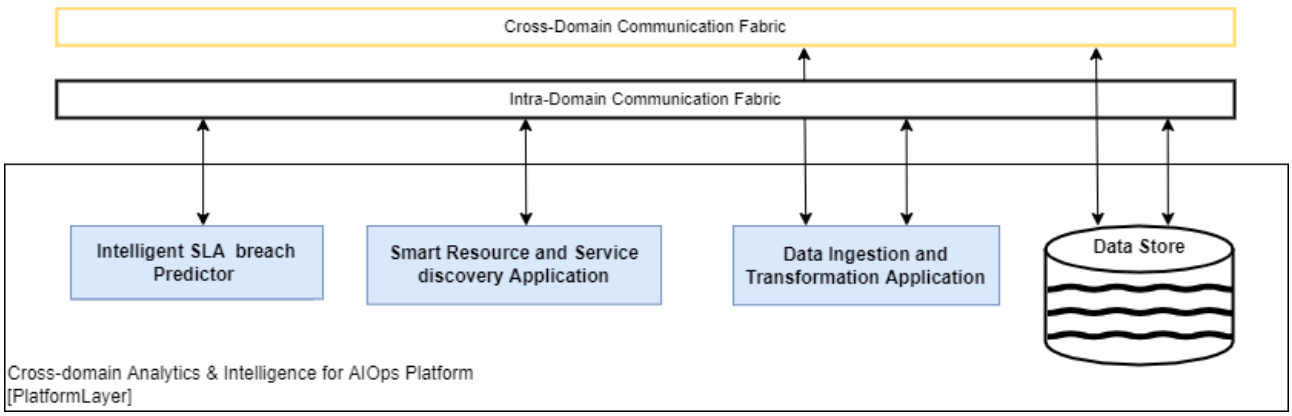

Figure 6-7: Cross-domain Analytics & Intelligence for AIOps platform

5GZORRO defined three main AIOps services, which are implemented as software modules, all of which are modelled with the same pipeline idea. These include:

- Intelligent SLA monitoring & breach predictor,
- Intelligent 3rd party resource planner,
- Data Ingestion & Transformation.

For example, for the Intelligent SLA monitoring & breach predictor, the following specific pipeline stages are applicable:

1. Provide monitoring data.
2. Aggregate the monitoring data.
3. Using the monitoring data, evaluate SLA satisfaction.
4. Perform some analytics to predict violation of SLA.
5. Raise an event for actions to be performed upon prediction of SLA violation.

However, 5GZORRO allows defining similar pipelines for additional analytics workflows.

The implementation and deployment of the stages of the pipeline must be coordinated. The output from one stage typically serves as the input for another stage. The information transferred between stages may be the actual data upon which to operate, or it may simply be a notification that the previous processing stage has completed with an indication of where to find the data in the data store.

5GZORRO uses a general framework to allow easy connectivity between services defined in a Data Lake. (See [46] for a concrete realization of a pipeline architecture for Kubernetes.)

- Register the service; specify the data that is to be used by the service (some kind of pointer to the data or other type of description of the data).
- Use messaging for communication between services.
- Each service has a channel from which it receives input and has a channel to which it sends output. The input/output might be the actual data, or it may include a pointer to the location of the relevant data to be processed.
- The output produced by a single component could be consumed by multiple consumers. For example, the output of a data aggregator service can be forwarded both to the data store as well as to a service that checks for SLA compliance.

7 Operational patterns

In this section, some relevant operations patterns for the 5GZORRO architecture are introduced, which highlight the role and service of the different Functional Entities defined in Section 5.

7.1 Resource Provider Onboarding in 5GZORRO marketplace

The Onboarding of new stakeholders in the 5GZORRO marketplace enables new Resource Providers and Service Providers to be enrolled into the 5GZORRO eco-system and begin trading resources or services with the existing 5GZORRO Marketplace members. Since D2.2, and according to input coming from technical specification and implementation performed at WP3 and WP4, there are a few major updates, notably:

- No platform certificates are required to register the stakeholder but only the services endpoints and a verification key generated when the Stakeholder DID Agent is deployed
- The usage of a DID Stakeholder Agent deployed at the Stakeholder domain performing the DID Holder Role according to the updated Identity and Permissions Management functional specification
- The usage of a DID Admin Agent deployed at the Governance Domain performing the DID Issuer Role according to the updated Identity and Permissions Management functional specification
- The way how the Governance Management interfaces with the new DID Admin Agent to approve or decline the registration request

To register in the 5GZORRO Marketplace, the candidate must deploy the 5GZORRO framework, to collect associated endpoints and assets to be traded that will be used by the consortium governance model to decide about the new member candidate. Once onboarded, the new member can begin advertising/consuming resources/services based on their assigned roles & permissions.

Figure 7-1 shows the exact steps of the certificate generation workflow, described below:

Steps 1 to 3: The Stakeholder deploys the DID Agent and, if successfully generated, a verification key is generated (verkey) to be used in the registration process.

Step 4-5: The Stakeholder uses the Marketplace portal to request the registration in the Marketplace by providing the verification key (verkey) previously generated on the DID Agent deployment, the roles to be performed by the stakeholder in the Marketplace plus additional information about assets to be provided or consumed in the Marketplace, as well as the different 5GZORRO services endpoints addresses available.

Steps 6 to 16: The stakeholder DID is created and stored in the wallet by the Stakeholder DID and then the Governance Board DID is resolved to retrieve the list of existing Admin Agents. One of the Admin Agents is selected and the process to register the Stakeholder credential is executed, where the Stakeholder DID Agent interacts with the selected Admin Agent. The Governance Manager handles the registration request and applies the adopted Governance Model (e.g., all Governance Board Administrators must vote) to take a decision about the new Marketplace member candidate. In case the Stakeholder registration is approved by the Governance Board, the Stakeholder Credential is issued and transferred to the Stakeholder DID Agent. Otherwise, the registration is declined, and the stakeholder is notified about this.

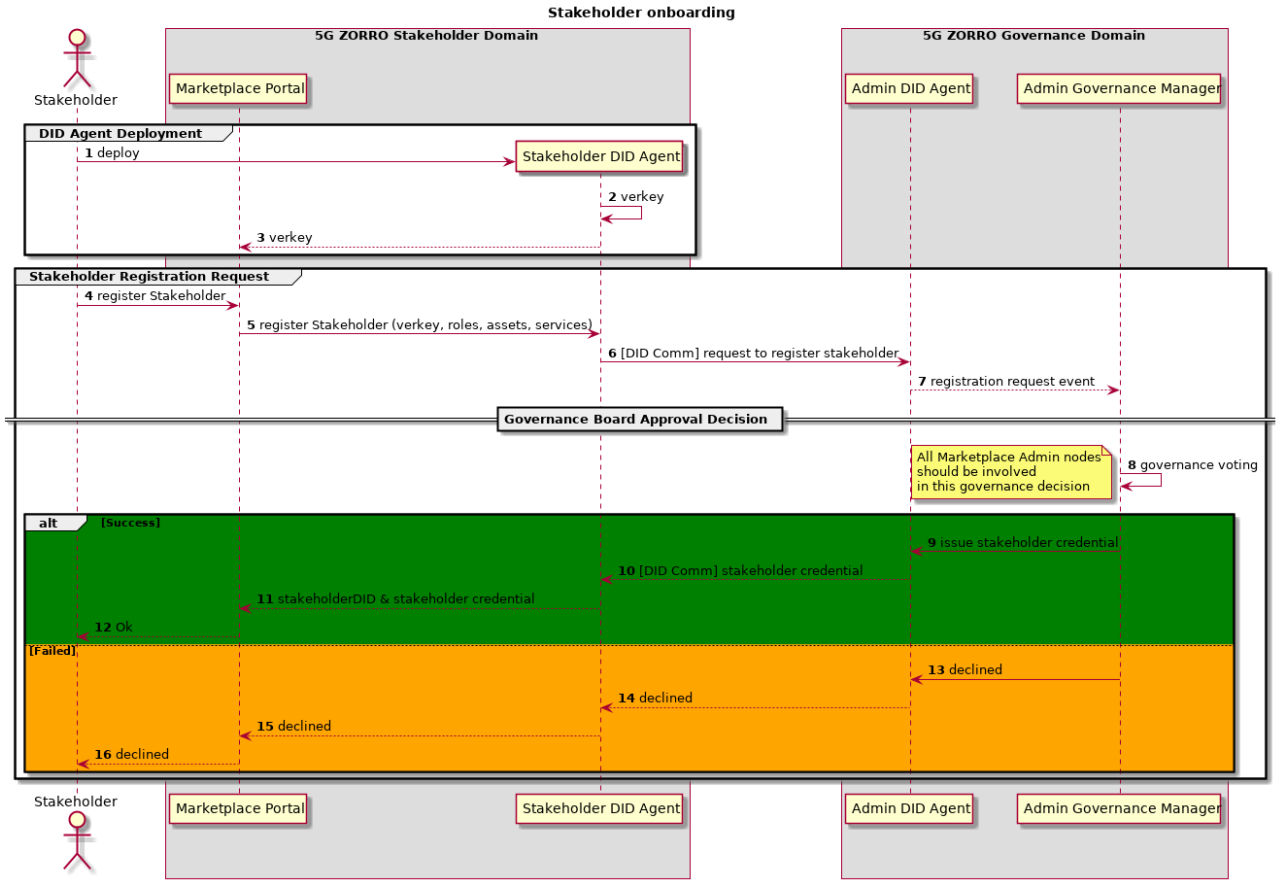

Figure 7-1: Stakeholder Onboarding in 5GZORRO marketplace

7.2 Publishing a Spectoken Resource Offer

This operational pattern describes the sequence of operations involved in the creation of a Spectoken. In the 5GZORRO vision, Spectokens are referred to as a set of spectrum resources in a licensed band. Radio transmissions over a licensed frequency band are restricted primarily to the spectrum license holder, typically a Mobile Network Operator (MNO), which won a spectrum license following a spectrum auction or contest organized by the National Regulatory Authority (NRA). The licensed spectrum owner might seek to lease underutilized spectrum either to enhance its revenue or because of obligations imposed by the NRA (increase the spectrum efficiency). The 5GZORRO architecture provides a fast, reliable, and secure spectrum trading market among the Spectrum Resource Providers (SRP) and the Spectrum Resource Consumers (SRC). Spectrum trading cannot be opaque to the NRA, who must acknowledge the radio resources to be shared.

Before the SRP publishes a spectrum offer in the 5GZORRO Marketplace, the NRA must announce the SRP's spectrum capabilities by issuing a spectrum certificate. This certificate acts as a verifiable claim in the 5GZORRO platform and determines that the SRP is the original owner of some licensed spectrum bands included in the certificate and, consequently, it can generate Spectokens and put them in the Marketplace. The use of spectrum certificates leverages the zero-touch and automation of spectrum trading by minimising the manual intervention of the NRA in the spectrum transactions within the 5GZORRO platform.

Figure 7-2 shows the exact steps of the certificate generation workflow, described below:

1. The Regulator fills the spectrum capabilities of an SRP in the 5GZORRO Portal
2. The Portal formats the spectrum capabilities in the shape of a template and sends the template to the Legal Prose Repository

3. The Legal Prose Repository provides the template DID for this particular spectrum claim
4. The Regulator's portal now sends a request to issue a spectrum claim with the template DID and the licensed model values to the Identity and Permissions Manager
5. The Identity and Permissions Manager issues the claim and sends a notification to the SRP that it has a new spectrum certificate

The SRP is now in a good position to generate Spectokens related to the spectrum certificate issued by the NR

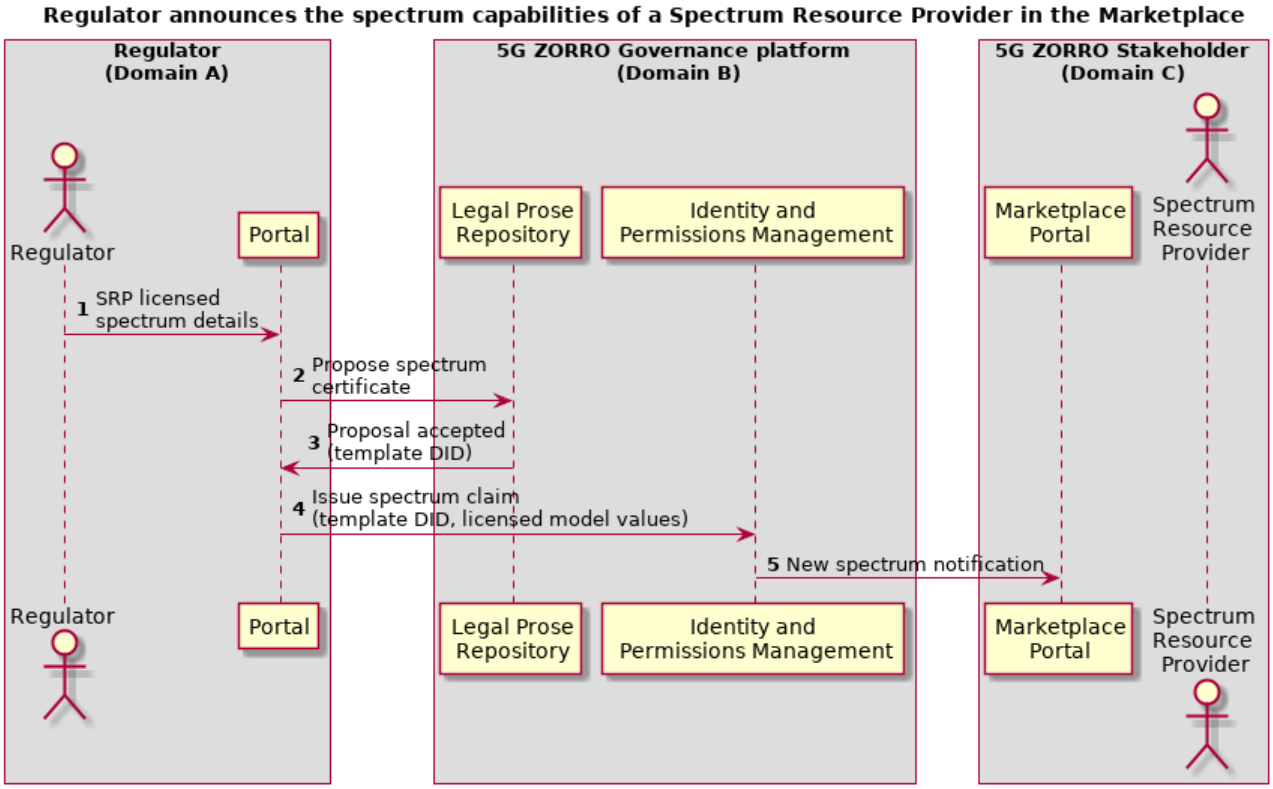

Figure 7-2: Spectrum certificate generation workflow

Figure 7-3 shows the exact steps of the Spectoken Resource Offer Publishing workflow, described below:

1. The SRP populates the Spectoken technical details (frequency range, area of application) in the Marketplace portal
2. The Marketplace portal sends a request to create a Spectoken to the SRP's Spectrum Resource Management

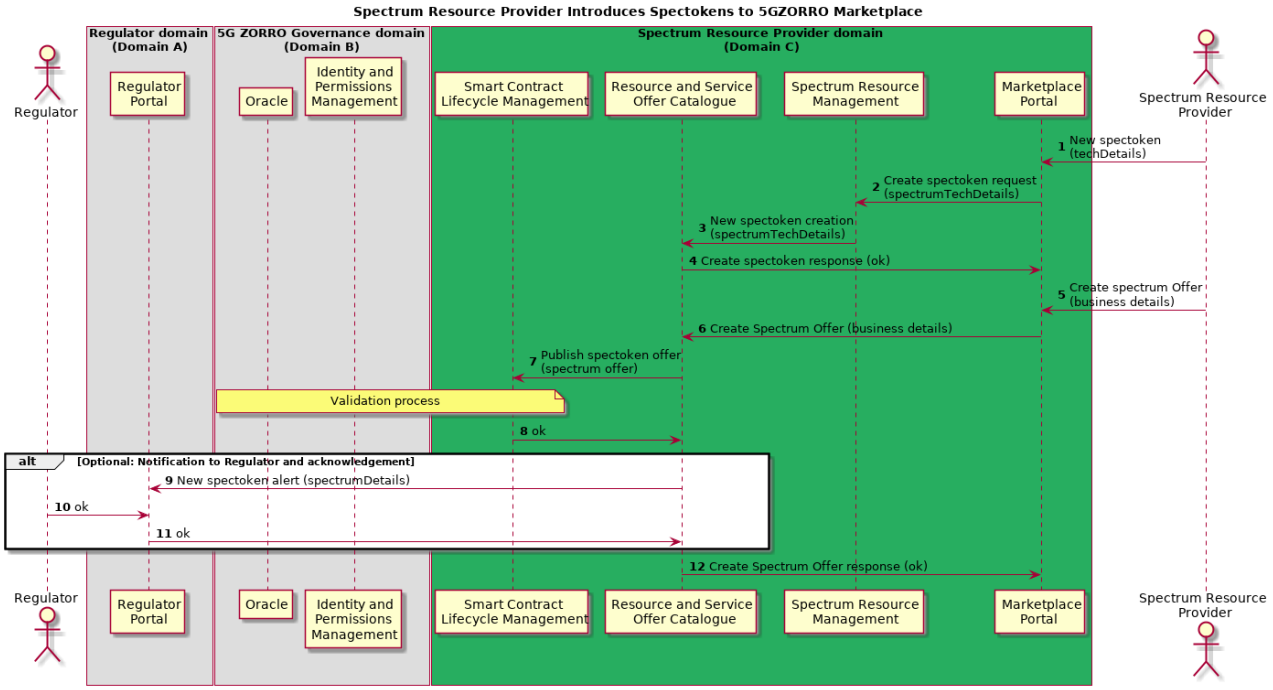

Figure 7-3: Spectoken Resource Offer Publishing workflow

3. The Spectrum Resource Manager sends a spectrum resource candidate to the Resource and Service Offer Catalogue with the spectrum technical details
4. The Resource and Service Offer Catalogue sends a response to the SRP's portal that the spectrum resource candidate has been generated
5. The SRP provides the business details of the spectrum offer in the Marketplace portal
6. The Marketplace portal sends a request to the Resource and Service Offer Catalogue to create the spectrum offer by providing the business details associated with the spectrum resource candidate
7. The Resource and Service Offer Catalogue sends a request to the Smart Contract Lifecycle Manager to publish the new Spectoken. At this stage, the Marketplace DLT in the Smart Contract Life-Cycle Manager queries the Oracle in the Governance domain to check that the Spectoken is not duplicated (it already exists in the 5GZORRO Marketplace) and that the Spectoken information is in alignment with the SRP spectrum certificate
8. If the validation process determines that the spectrum offer is valid, the Resource and Service Offer Catalogue receives a notification
9. Optionally, the Resource and Service Offer Catalogue sends a notification to the NRA that a new Spectoken has been created (notification includes both technical and business information)
10. The Regulator acknowledges the notification
11. The acknowledge is delivered from the Regulator's portal to the Resource and Service Offer Catalogue in the Marketplace
12. The Resource and Service Offer Catalogue notifies the SRP's portal that the new spectrum offer has been published

7.3 Trustworthy Resource Discovery

In 5GZORRO, the discovery of available resource and service offers is facilitated by two main functional entities, namely: a) the Resource and Service Offer Catalogue, with support for filter-based discovery; and b) the Smart Resource and Service Discovery, with support for intent-based discovery. With respect to D2.2, the workflow depicted in Figure 7-4 focuses on the operations involving the Smart Discovery service offered by the platform. This figure shows how new offers are classified at this module and made available to interested consumers for subsequent intent-based discovery requests.

The resource discovery process has been updated and the respective workflow, shown in the next Figure 7-4, completely substitutes the similar workflow described in D2.2, Section 6.3.

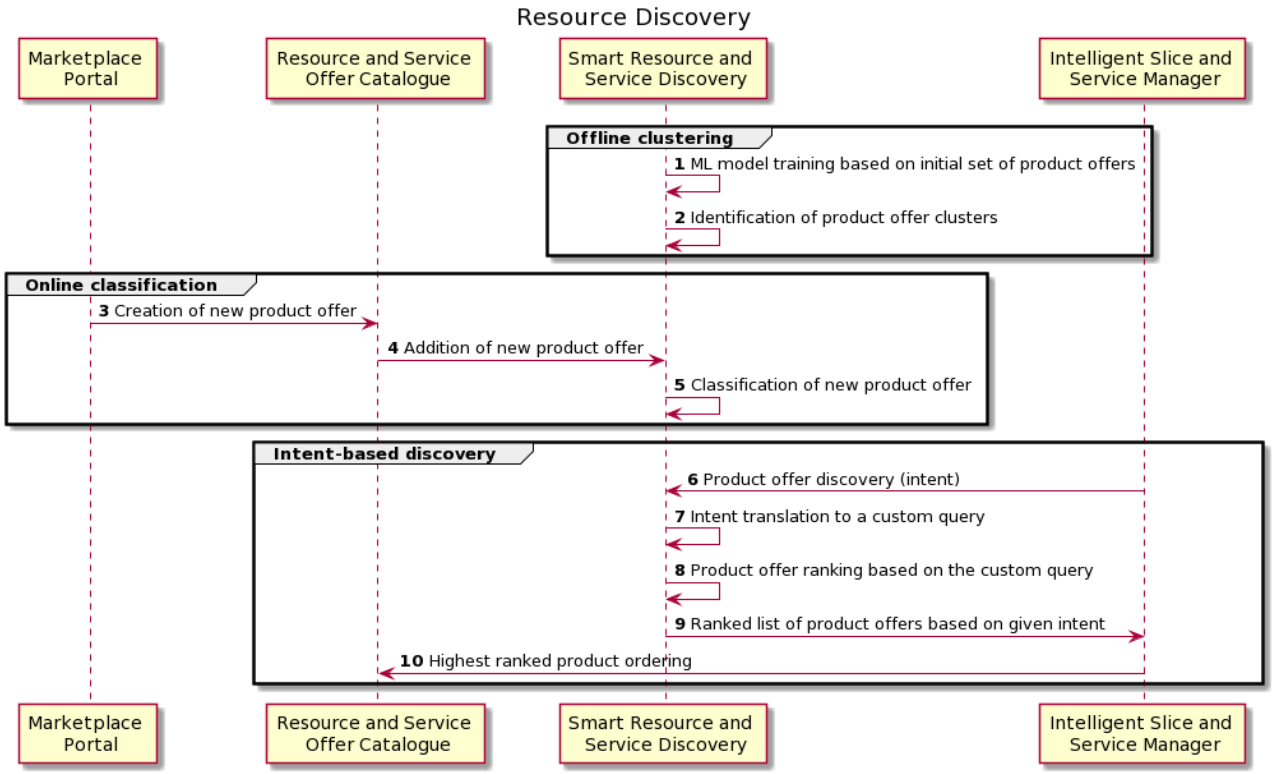

Figure 7-4: Trustworthy Resource Discovery workflow

The steps of the Trustworthy Resource Discovery workflow, are described below:

Steps 1-2: The Smart Resource and Service Discovery ML model is trained with an initial set of offers, and as a training outcome, product offer clusters are identified.

Steps 3-5: Once a new offer is added to the marketplace, the Smart Resource & Service Discovery trained ML model is used to predict the cluster to which the offer belongs.

Steps 6-10: The Intelligent Slice and Service Manager can launch an intent-based query to discover relevant product offers. As a result, the relevant offers are returned using a ranking algorithm and the Intelligent Slice and Service Manager can select the highest ranked product from the Marketplace DLT Platform.

7.4 Trustworthy Smart Contract Setup for spectrum

The workflow on trustworthy smart contract setup for spectrum defined in D2.2 has been largely modified based on discussions on spectrum-related functionalities within the 5GZORRO platform. A Spectoken is a

spectrum resource offer published by a spectrum provider in the 5GZORRO Catalogue. The spectrum provider sets not only the spectrum technical details, e.g., range of frequencies and area of application, but it also sets the business and the regulating aspects of the use of the spectrum. The consumer of the spectrum offer negotiates the smart contract with the spectrum provider and they both close the Spectoken transaction. In D2.2, this negotiation of the smart contract is done differently and involving the Regulator. In the new version of this workflow, and for the sake of transaction automation, the Regulator only takes a supervisor role of the process, and it only gets notified when a new Spectoken transaction has been carried out in the 5GZORRO platform.

At the end of a successful spectrum transaction, the spectrum consumer shall store the technical information of the acquired resource in the spectrum manager module in the Virtual Resource Manager (VRM) for two reasons: 1) to leverage the discovery of available pieces of spectrum within the consumer's domain when configuring a radio slice; and 2) to collect monitoring data from the RAN of the available spectrum resources.

According to this reasoning, the content of the trustworthy smart contract setup for spectrum in D2.2 must be replaced by the following description.

This workflow illustrates the procedure of how to get and use Spectokens. A Spectrum Resource Consumer (SRC), typically a Communication Service Provider (CSP), may have the ability to extend its radio coverage using the 5GZORRO platform. To that end, the SRC must acquire Spectokens previously provided by Spectrum Resource Providers (SRPs) and currently available at the 5GZORRO marketplace.

The other entity involved in this workflow is the Regulator, which must: firstly, approve the credentials of the CSP as SRC; and lastly, get notified about the spectrum transaction between the SRC and the SRP.

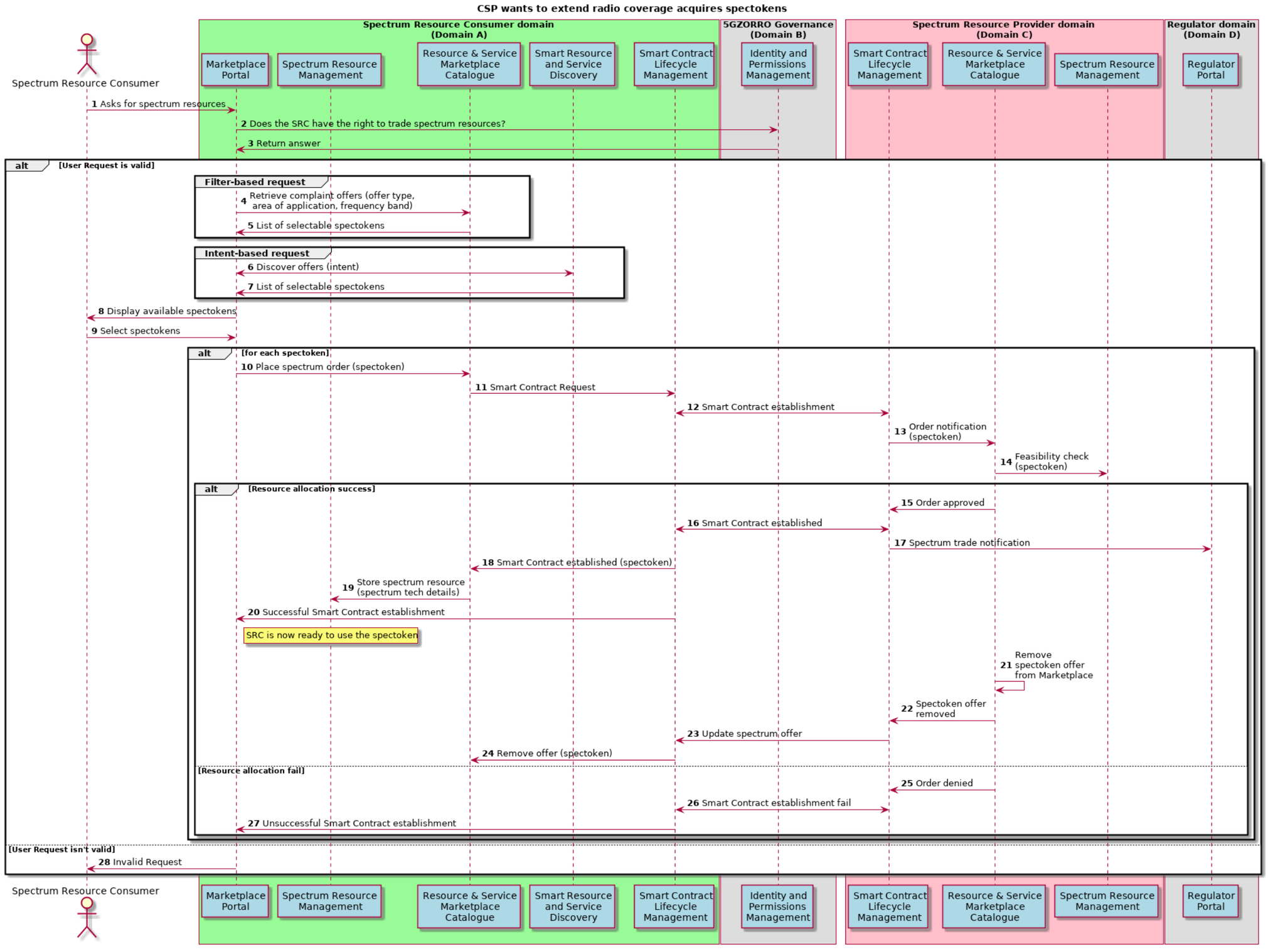

Figure 7-5: CSP who wants to extend radio coverage acquires Spectokens

Figure 7-5 depicts the main steps required in this process described as follows.

1. The Spectrum Resource Consumer (SRC) logs in the 5GZORRO Marketplace Portal and asks for Spectokens matching some criteria in the sense of geographical location, spectrum bands, etc.
2. The Marketplace Portal asks the Identity and Permissions Manager to confirm that the SRC has credentials to participate in spectrum transactions in the Marketplace.
3. The Identity and Permissions Manager replies the Marketplace Portal. If the SRC is not authorised to purchase Spectokens, jump to step 27.
4. The Marketplace Portal sends a Spectoken request to the Resource & Service Marketplace Catalogue with the Spectoken characteristics.
5. The Resource & Service Marketplace Catalogue filters the available Spectokens and sends the results to the Marketplace Portal.
6. If the SRC provided an intent instead of the Spectoken characteristics, the Marketplace Portal communicates with the Smart Resource and Discovery service.
7. The Smart Resource and Discovery service sends the Spectokens found in the Marketplace.
8. The Portal shows the Spectokens matching the SRC criteria.
9. The SRC selects some Spectokens in the Marketplace Portal.
10. For each selected Spectoken, the Marketplace Portal places the spectrum offer in the Resource & Service Marketplace Catalogue.
11. The Resource & Service Marketplace Catalogue sends a Smart Contract Request to the Smart Contract Lifecycle Manager in the SRC domain.
12. The Smart Contract Lifecycle Manager in the SRC domain establishes a Smart Contract for the Spectoken with the Smart Contract Lifecycle Manager in the SRP domain.
13. The Smart Contract Lifecycle Manager in the SRP domain notifies a Spectoken order to the Resource & Service Marketplace Catalogue in its domain.
14. The Resource & Service Marketplace Catalogue in the SRP domain asks its Spectrum Resource Management if the Spectoken is still valid. If this validation or the Smart Contract Request fails, jump to step 25.
15. The Resource & Service Marketplace Catalogue notifies the Smart Contract Lifecycle Manager that the Spectoken order is approved.
16. The Smart Contract Lifecycle Manager in the SRP notifies its counterpart in the SRC domain that the Smart Contract has been established.
17. The Smart Contract Lifecycle Manager in the SRP sends a notification to the Regulator that a spectrum transaction has occurred.
18. The Smart Contract Lifecycle Manager in the SRC notifies the Resource & Service Marketplace Catalogue in its domain that the Smart Contract of the Spectoken has been established.
19. The Resource & Service Marketplace Catalogue sends the Spectoken technical details to the Radio Spectrum Resource Management of the SRC and stores the information.
20. The Smart Contract Lifecycle Manager in the SRC notifies the SRC via Portal that the Smart Contract has been established. Now the spectrum is ready to be used by the SRC.
21. The Resource & Service Marketplace Catalogue in the SRP domain removes the Spectoken offer from the Marketplace.

22. The Resource & Service Marketplace Catalogue in the SRP domain notifies the Smart Contract Lifecycle Manager in the SRP domain that the Spectoken offer has been removed from the Marketplace.
23. The Smart Contract Lifecycle Manager in the SRP sends a Spectoken update to its counterpart in the SRC domain notifying that the Spectoken is not available.
24. The Smart Contract Lifecycle Manager in the SRC domain sends a request to the Resource & Service Marketplace Catalogue in its domain to remove the Spectoken.
25. The Resource & Service Marketplace Catalogue notifies the Smart Contract Lifecycle Manager that the Spectoken order is denied.
26. The Smart Contract Lifecycle Manager in the SRP communicates with its counterpart in the SRC domain that the Smart Contract establishment for the current Spectoken failed.
27. The Smart Contract Lifecycle Manager notifies the SRC that the Smart Contract establishment for the current Spectoken failed.
28. The SRP is notified that it is not authorised to participate in the spectrum trading in the 5GZORRO platform.

7.5 Trustworthy Smart Contract Setup for edge computing

The operational flow diagram illustrated in Figure 7-6 describes the processes involved in the automatic, trustworthy resource agreement setup, focusing on the leasing of edge computing resources. In this figure, the Resource Consumer has already selected one or more resource offers provided by the Resource Provider.

More specifically, the steps presented in Figure 7-6 can be described as follows:

Step 1: The *Intelligent 3rd party resource selection* module of the Resource Consumer makes an order to the Marketplace, through the *Resource and Service Offer Catalogue*. Through this order, the Resource Consumer requests for the resource offers provided by the Resource Provider. This differentiates from the respective workflow in D2.2, where this flow was initiated by the *Intelligent Network Slice and Service Orchestration,* now renamed into *Network Slice and Service Orchestration*, of the Resource Consumer, which explicitly proposed an agreement for the selected resources to the *Smart Contract Lifecycle Management*. However, given the updates on the functional components, this flow is initiated by placing an order to the Catalogue and the agreement setup is mainly a process of the Marketplace.

Step 2: An order consists of one or more product offers. Thus, when an order is received, then for each product offer, the *Resource and Service Offer Catalogue* queries the relevant *Virtual Resource Management and Control* in Resource Provider about product availability. In D2.2 this step was done by the *Smart Contract Lifecycle Management* functional block, because at that time it wasn't anticipated that the Resource and Service Offer Catalogue would interact directly with the *Virtual Resource Management and Control*.

Step 3: Theoretically, a product offer can consist of one or more resources and/or services. So, the *Virtual Resource Management and Control* extracts the resources and the services from the product offer. In this case, only edge computing resources will be included in the product offer.

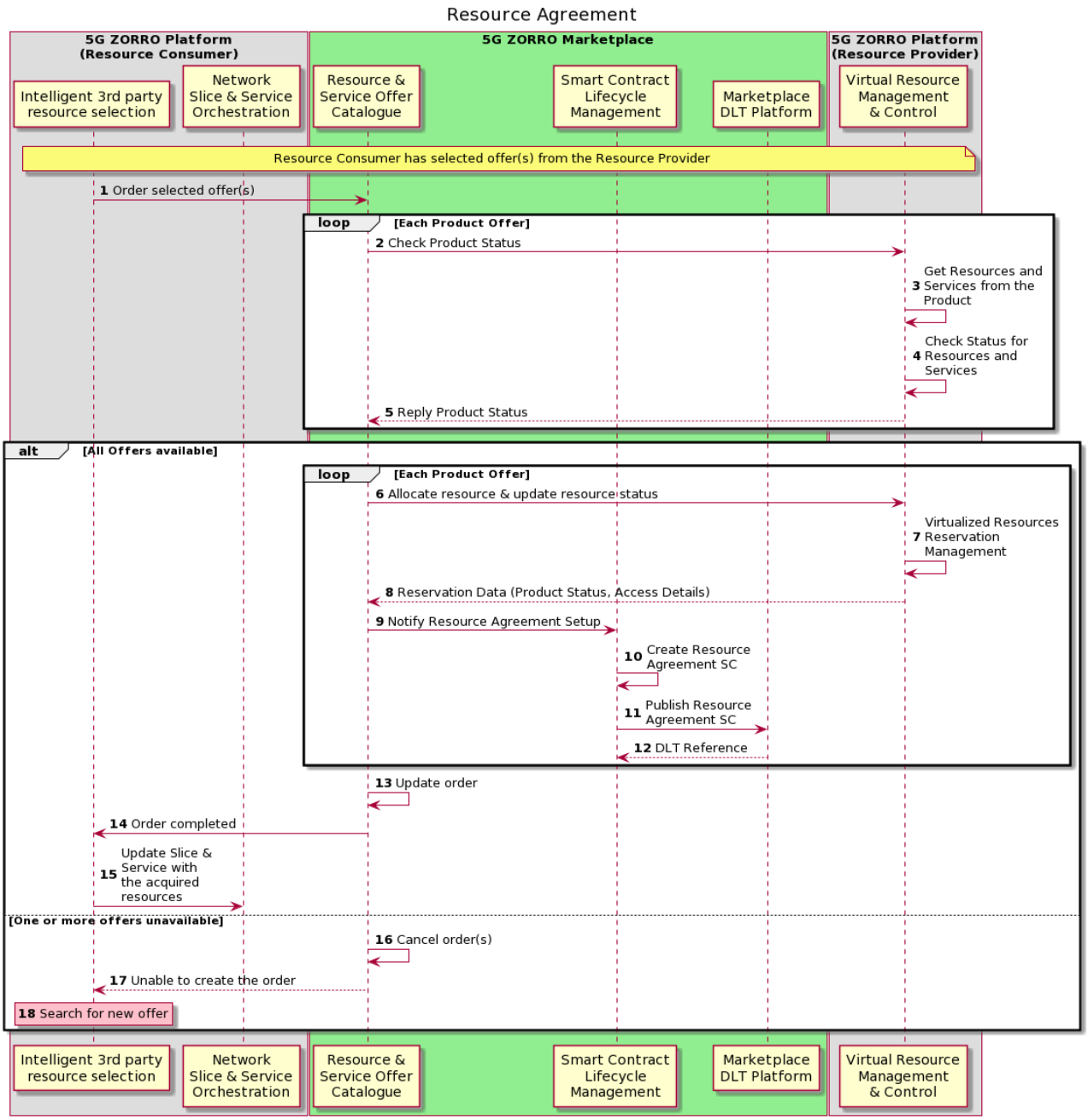

Figure 7-6: Workflow for Trustworthy Smart Contract Setup for edge compute resources

Step 4: If there are multiple resources or services in a product offer, then the *Virtual Resource Management and Control* checks the availability for each one of them. Steps 3 and 4 were not included in D2.2.

Step 5: The overall product status is returned to the *Resource and Service Offer Catalogue* which made the initial request, instead of the *Network Slice and Service Orchestration* which handled the request's reply in D2.2.

Steps 6 – 15: If all resources are available then the order can be completed. Contrary to the flow in D2.2, where the agreement finalization preceded the resource allocation, in the current version the order is reversed. More analytically, for each product offer, the *Resource and Service Offer Catalogue* asks the *Virtual Resource Management and Control* to allocate the product's resources and to update their status (step 6). Then, the *Virtual Resource Management and Control* handles the reservation of the virtual edge computing resources and replies with the necessary data, such as the product status and the resources' access details, back to the *Resource and Service Offer Catalogue* (steps 7-8). After that, the *Resource and Service Offer*

Catalogue asks the *Smart Contract Lifecycle Management* module to initiate the resource agreement setup (step 9). Based on the offer's details, the agreement is created in the form of a Smart Contract, the Smart Contract is signed by the involved parties and the consensus is reached at the DLT network (steps 10 – 12). When the above procedure succeeds for all the offers included in the order, the *Resource and Service Offer Catalogue* updates the order in the catalogue (step 13). Then, the consumer's *Intelligent 3rd party resource selection* is informed about the order completion and notifies the *Network Slice and Service Orchestration* to update the slice with the newly acquired resources (steps 14 – 15).

Steps 16 - 17: In a case that one or more requested resources are not available from the Resource Provider, the order is cancelled (step 16) and the resource selection process must restart (Step 18). as explained in Section 7.3.

Once the resource agreement is successfully established, the Resource Consumer (mentioned as Domain A in the images below) can leverage the resources provisioned by the Resource Provider (Domain B). As a result, an end user that was initially served by Domain A, may be redirected according to load balancing policies and get served by the Domain B. This process is separated into two flows. The first, in Figure 7-7, specifies 5GZORRO modules interactions required for the extension to the 3rd party resources, while the second, in Figure 7-8, presents the redirection of a User Equipment (UE) to the Resource Provider's Domain from a Vertical Service's perspective. The vertical service can be the virtual Content Delivery Network (vCDN) service, part of the 5GZORRO use case #3.

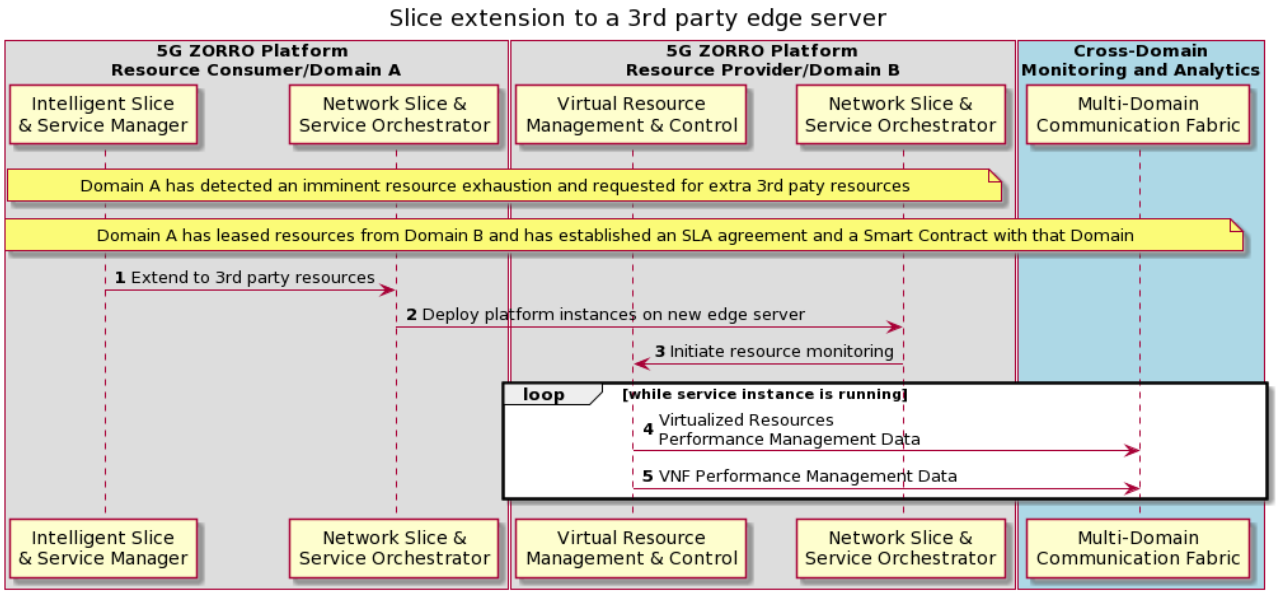

Figure 7-7: Workflow for slice extension to a 3rd party edge server

More specifically, in Figure 7-7, it is assumed that Domain A has detected an imminent resource exhaustion and searched for 3rd party resources. After completing the Smart Contract establishment, it proceeds with the slice extension towards Domain B's resources, as explained in the next steps (Figure 7-7):

Step 1: The Resource Consumer's *Intelligent Slice and Service Manager* sends a request to its *Network Slice and Service Orchestrator* to extend the slice to Domain B's resources.

Step 2: The *Network Slice and Service Orchestrator* of both Domains handle the deployment of the platform instances on the Resource Provider's edge server.

Step 3: In the Resource Provider (Domain B) side, the *Network Slice and Service Orchestrator* notifies the *Virtual Resource Management and Control*, so that the later will start monitoring the provided resources.

Steps 4 – 5: While the new service instance is active, the Resource Provider collects VNF and VIM monitoring data and sends them to the Cross-domain Monitoring and Analytics module, though the *Multi-Domain Communication Fabric*. These data can be aggregated and used in AI techniques to make predictions of the service performance for the near future.

Figure 7-8 illustrates the case where a User Equipment (UE) had been using a service provided by Domain A, when Domain A predicted the need for additional resources. Thus, Domain A leased resources from Domain B. After completing the Smart Contract establishment and the Slice extension towards Domain B's resources, load balancing mechanisms are activated to avoid overloading one of the edge servers. Then, based on load balancing decisions, the UE may be redirected to the 3rd party edge server and get served by Domain B.

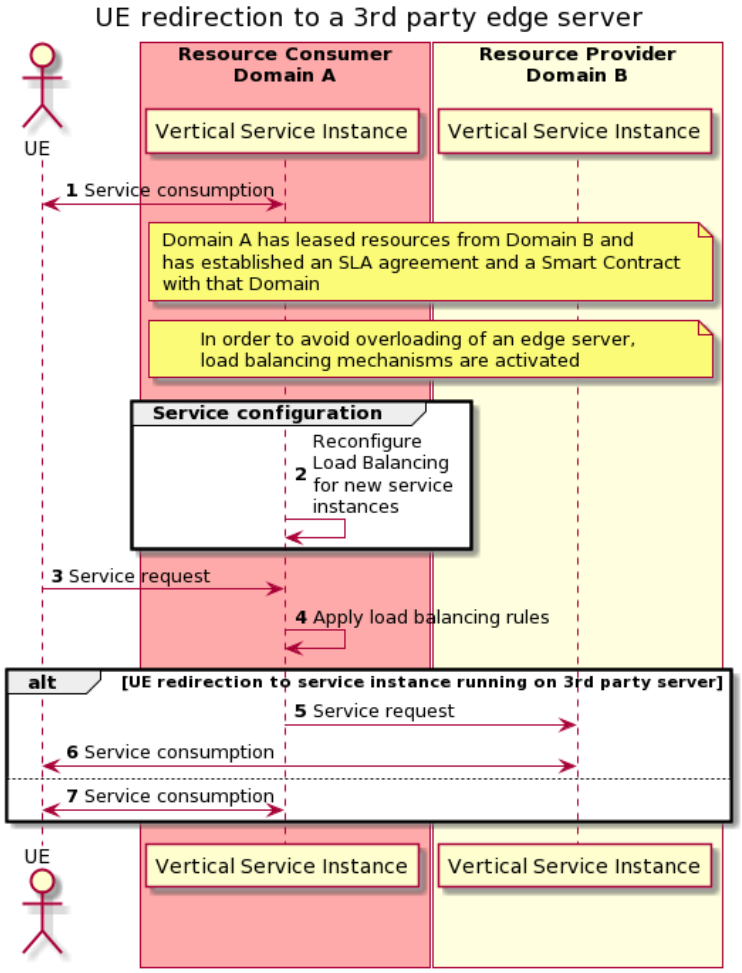

Figure 7-8: Workflow for UE redirection to a 3rd party edge server

The steps of the sequence diagram in Figure 7-8 are the following:

Step 1: The UE is being served by the Vertical Service Instance (e.g., CDN edge server) hosted at Domain A.

Step 2: After the slice extension to Domain B resources, the Vertical Service reconfigures its Load Balancing mechanisms, to take into consideration, the new Service Instance hosted at the newly allocated resources of the Resource Provider.

Step 3: The UE keeps sending service requests to the Service Instance of Domain A.

Step 4: The Vertical Service applies the load balancing rules in order to decide from which edge server the user will be served.

Steps 5 – 6: This is the case where a UE is redirected to Domain B. Particularly, the service request is forwarded to Domain B's Service Instance (step 5) and the User Equipment gets served by Domain B (step 6).

Step 7: The Load Balancing procedure decided to serve the UE by the Service Instance hosted at Domain A.

7.6 Trustworthy Slice setup with 3rd party resources

Figure 7-9 and Figure 7-10 depict an updated workflow of slice establishment with 3rd party resources where the 3rd party does not offer orchestration services and the orchestration is performed from within a domain that initiates the slice establishment. Main changes from the previous version of this workflow are as follows:

- Data Lake is included as an integral part of the workflow.
- ISSM's and NSSO interactions are explicitly presented.
- ISSM's components ISSM-WFM and ISSM-O and their interaction with the rest of the components is obviated.
- The interactions are rendered at a higher granularity.
- The unnecessary actions are removed.
- Components acting in Domain and Cross-Domain capacities are clearly segregated.
- An additional workflow initiator, such as Vertical administrator is added to accommodate a broader set of real-life scenarios.

3.6 Trustworthy Slice setup with 3rd party resources

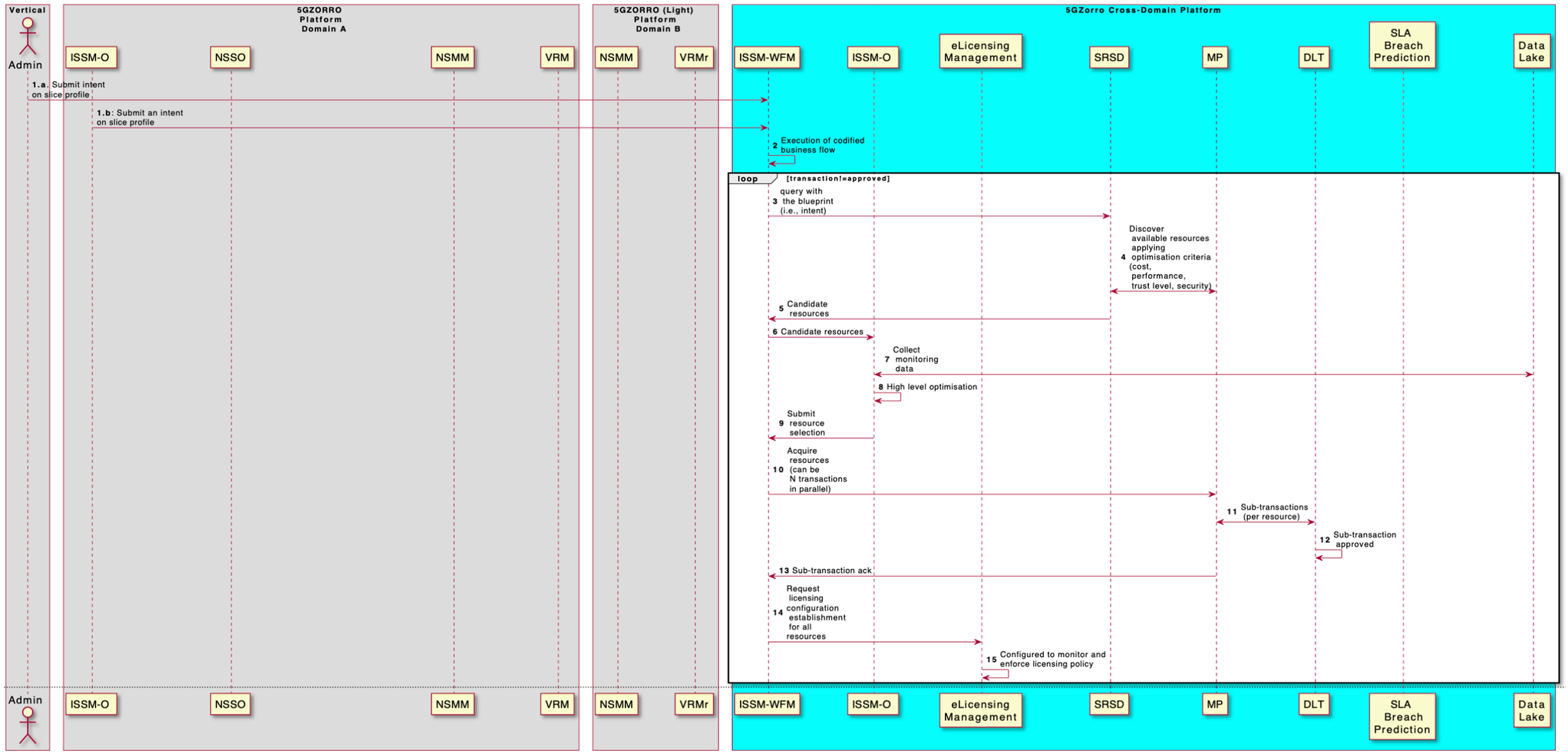

Figure 7-9: Trustworthy Slice Setup with 3rd Party Resources (1)

3.6 Trustworthy Slice setup with 3rd party resources (continue)

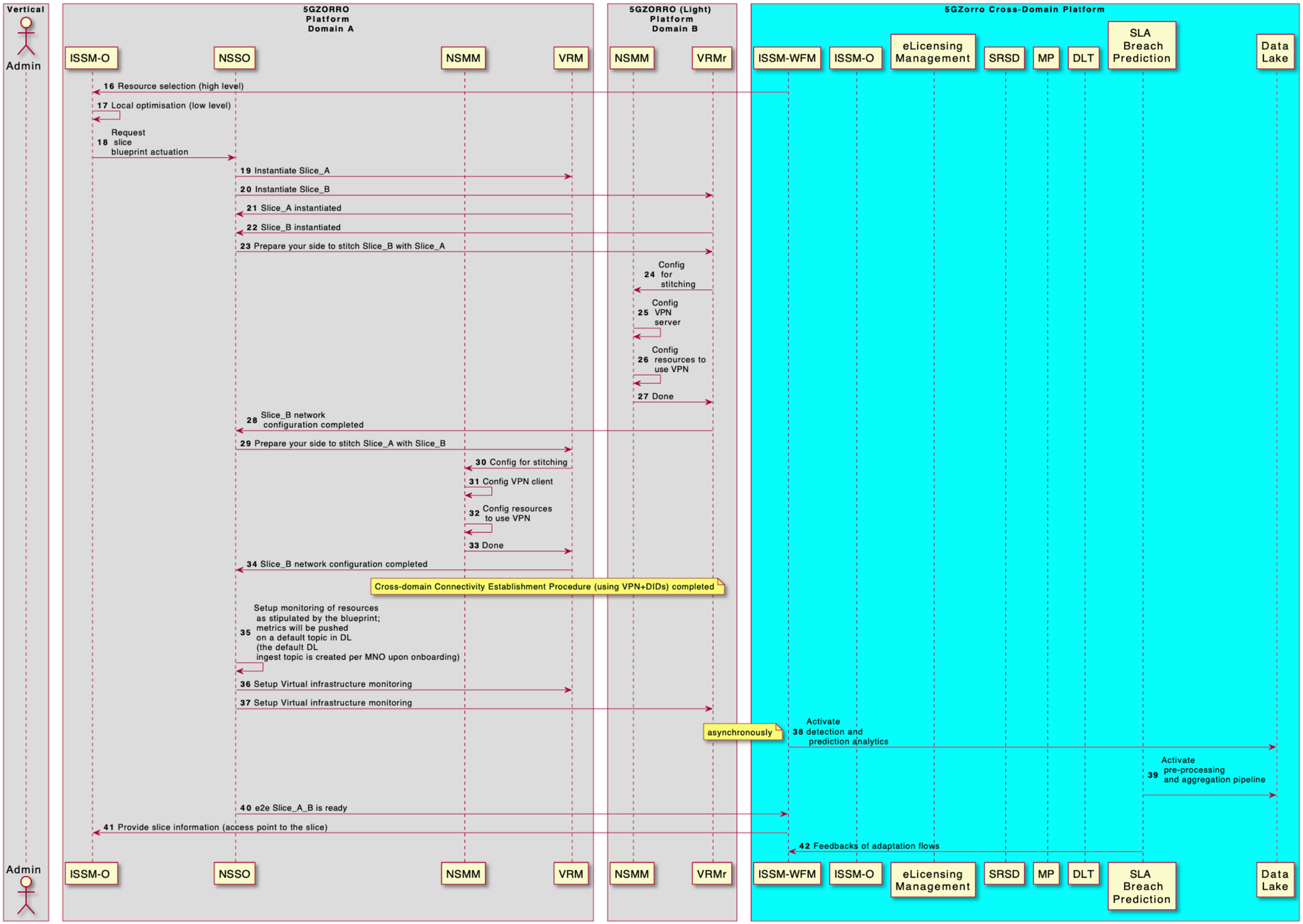

Figure 7-10: Trustworthy Slice Setup with 3rd Party Resources (2)

7.7 Trustworthy Slice setup with 3rd party orchestrated services

Figure 7-11, Figure 7-12, and Figure 7-13 describe an updated workflow for trustworthy slice setup with 3rd party orchestration services. The updates are analogous to the workflow of the previous Section and the workflow is similar. The main differences are:

- NSSO of Domain A does not manage VRM of Domain B, but rather delegates this to NSSO of Domain B
- Domain B has local (i.e., intra-domain role) ISSM-O that allows it to perform local optimization when actuating high level resource selection performed by ISSM-O acting in cross-domain role

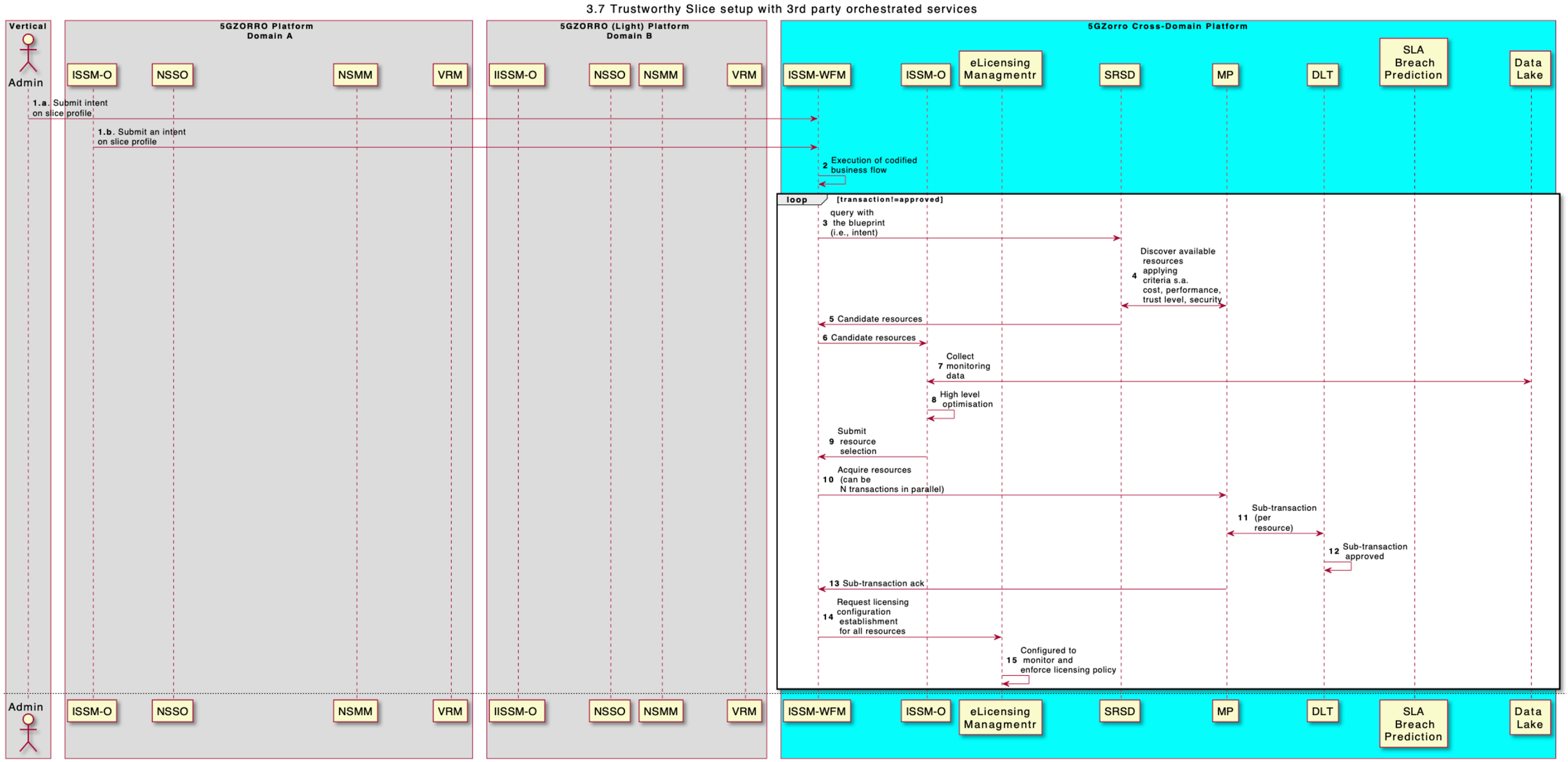

Figure 7-11: End-to-end flow of trustworthy cross-domain slice establishment (1)

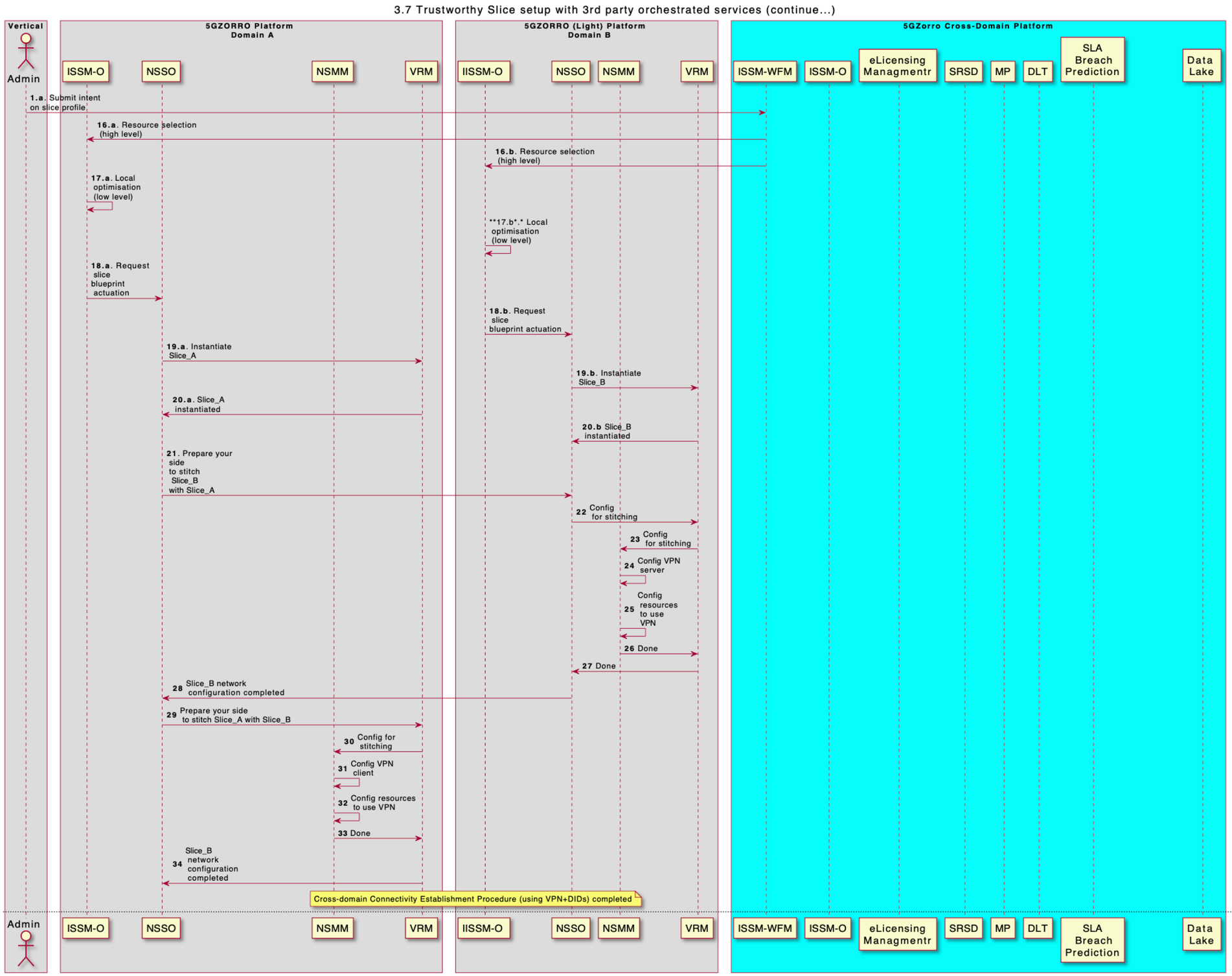

Figure 7-12: End-to-end flow of trustworthy cross-domain slice establishment (2)

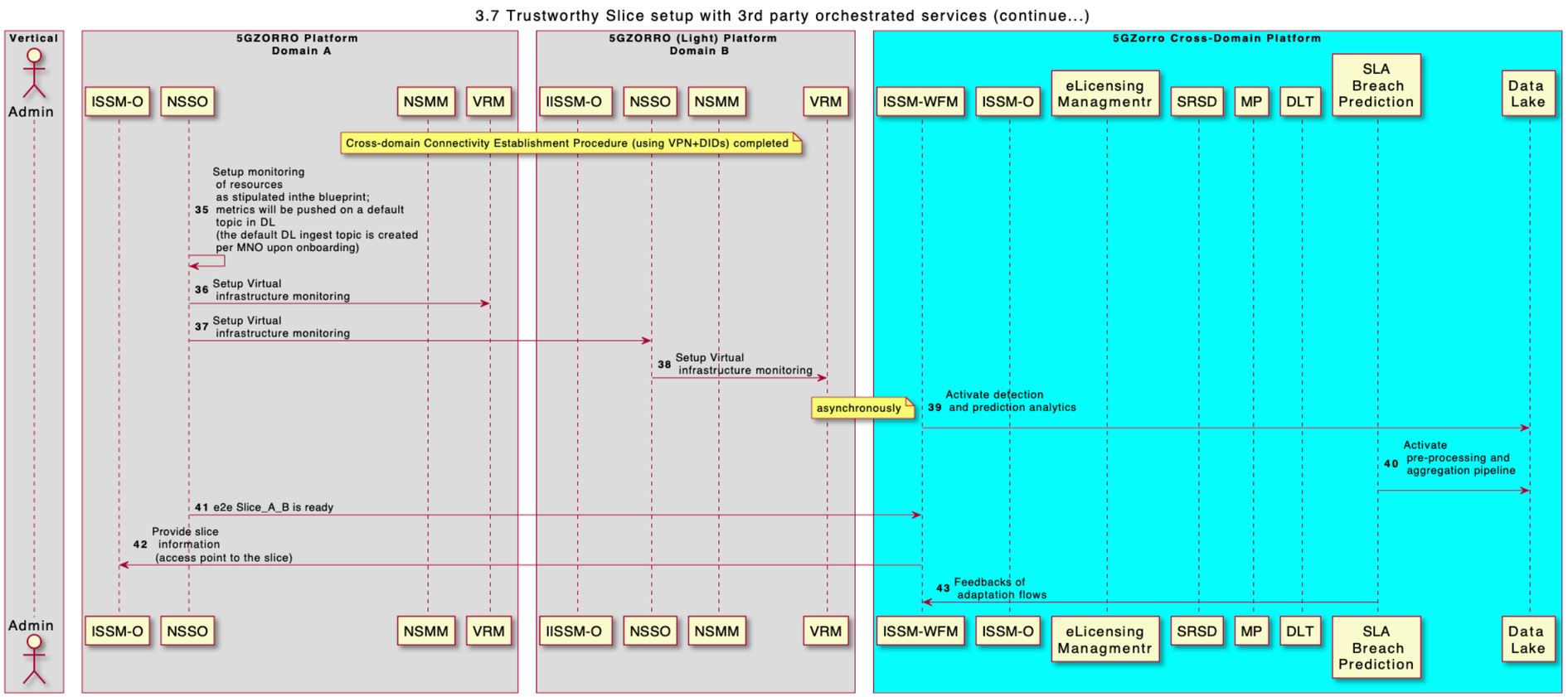

Figure 7-13: End-to-end flow of trustworthy cross-domain slice establishment (3)

7.8 Trustworthy e-licensing control

This section details the call flows that describe the sequence of operations within components of 5GZORRO involved in the e-licensing management, previously introduced in section 3.5 and specified in Section 5.3.14. Figure 7-9 illustrates graphically the operations performed for the licensing check at VF instantiation time while Figure 7-15 shows those that take place on a scheduled loop during the VF instance lifecycle.

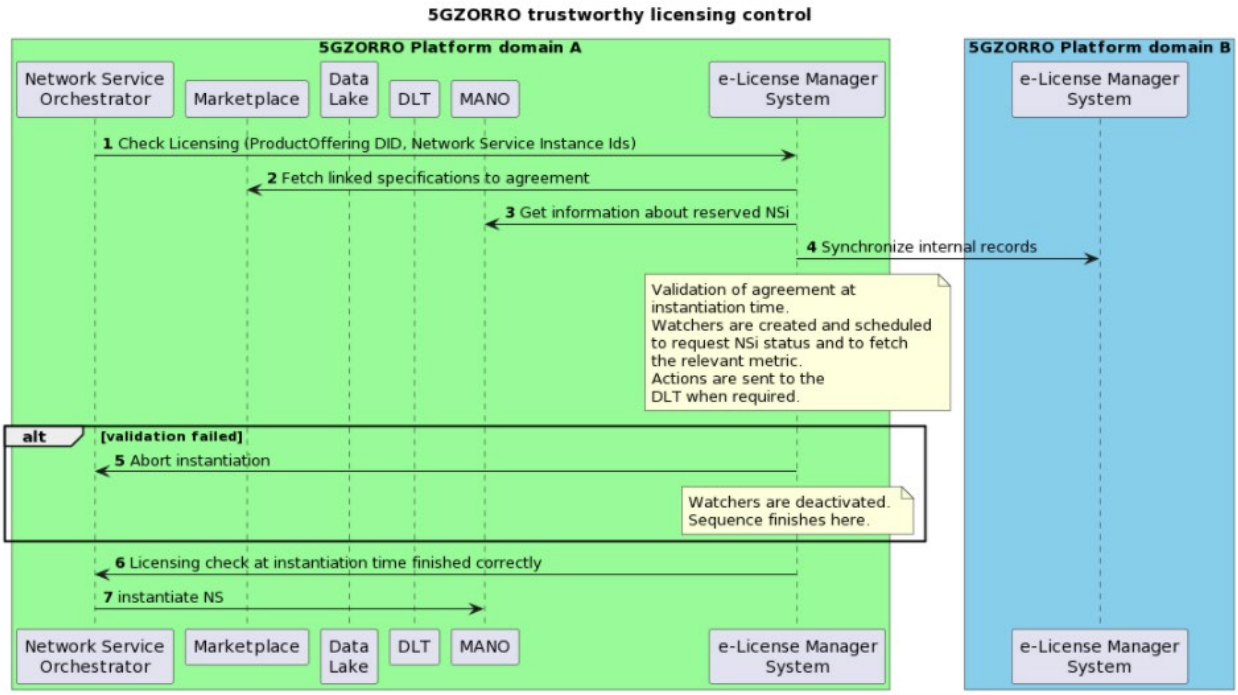

Figure 7-14: Trustworthy licensing control. Instantiation validation

Step 1: The NSSO or the ISSM-MEC block triggers the licensing check

Steps 2-4: The e-Licensing Manager obtains further details from the marketplace, the MANO layer and the neighbouring instances of the e-licensing system to perform the validation of the information provided in step 1.

Step 5: If the validation at instantiation time fails, all interested parties are informed and the e-Licensing Manager System gets ready for a new request.

Step 6-7: If the licensing check finishes correctly, the Network Service Orchestrator continues with the instantiation and configuration procedure.

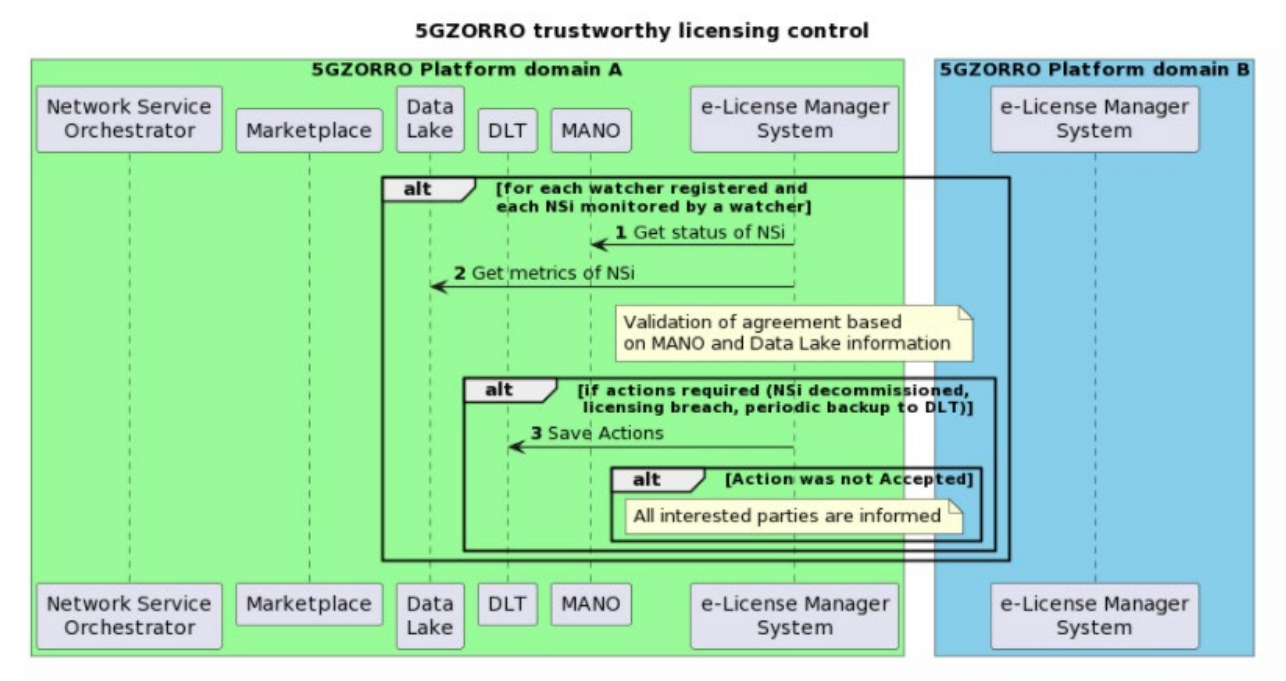

Figure 7-15 Trustworthy licensing control. Periodic validation

Steps 1-2: Watchers are scheduled to obtain the latest information from MANO and data lake about the instances being monitored for the same license. Based on it, a new validation check is performed to ensure that there is no breach of licensing constrains.

Step 3: This step is performed under the DLT procedure to add an entry in the blockchain and will return an ACK or an error if the entry fails to be persisted. In this case, interested parties such as the VNF vendor will be notified that there is an error in the control of their software.

7.9 Intelligent SLA monitoring & breach prediction

Figure 7-16 shows the Workflow for the SLA Breach Prediction. Basically, this is like the one presented in D2.2 The only difference is that, for a better presentation, Figure 7-16 shows only the SLA Monitoring of one Domain, which can be a Resource and/or Service Provider.

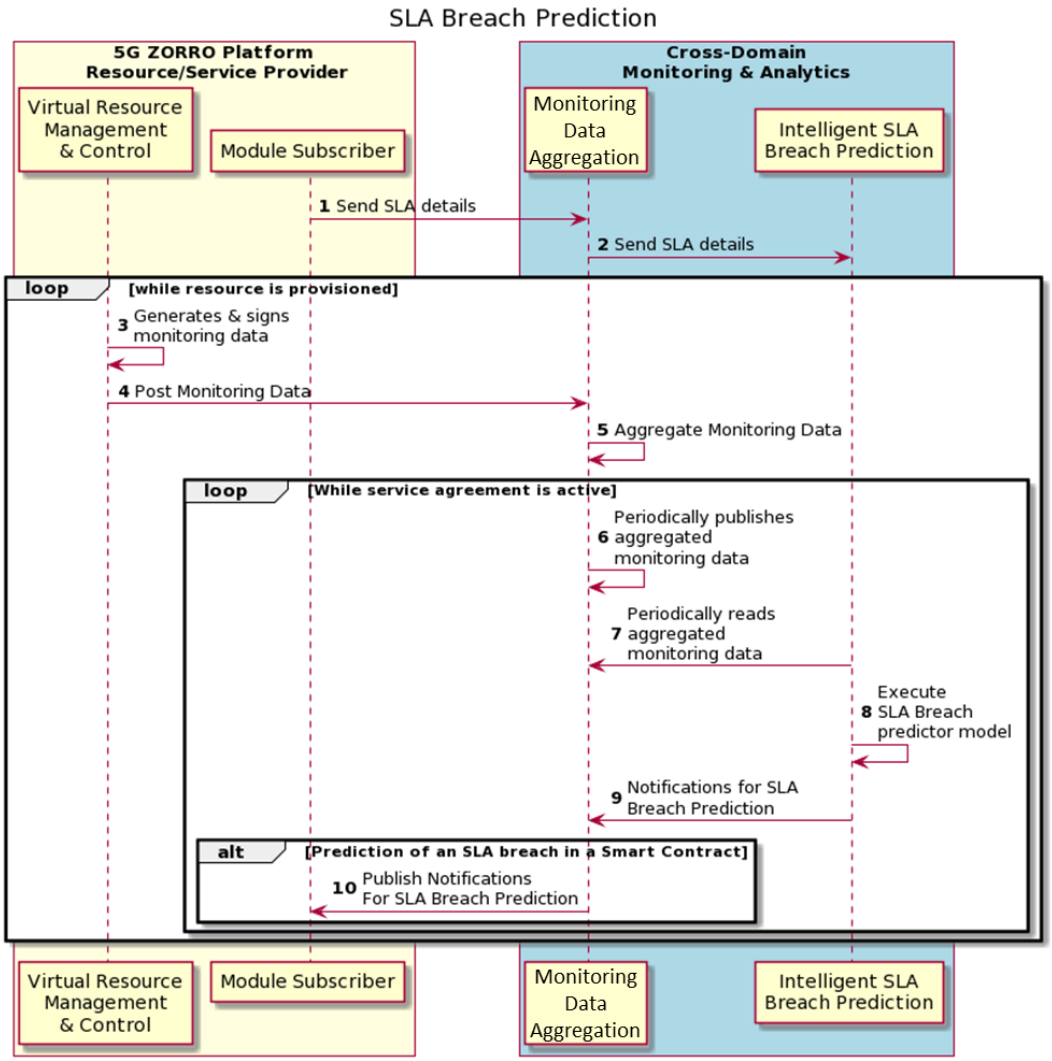

Figure 7-16: *Workflow for SLA Breach Prediction*

Figure 7-16 is analysed in the following steps:

Steps 1 – 2: The Resource/Service Provider requests from the Cross-Domain Monitoring and Analytics (i.e., the Data Lake) to start the algorithms for the SLA Breach Prediction.

Steps 3 – 4: Monitoring data is recorded in the Data Lake, through the *Monitoring Data Aggregation*.

Step 5: In turn, the *Monitoring Data Aggregation* module analyses and aggregates the ingested data according to specifications defined in the Smart Contract.

Steps 6 – 7: *Service and Resource Monitoring* periodically publishes the aggregated monitoring data, which can then be retrieved by the *Intelligent SLA Monitoring and Breach Prediction* module in order to train the Machine Learning (ML) model.

Step 8: The ML model is executed at certain time intervals.

Steps 9 – 10: In case that an SLA Breach is predicted, the Resource/Service Provider is informed accordingly and takes actions according to predefined rules.

7.10 Intelligent Network Slice and Service optimization

In Figure 7-17, we show the workflow for Intelligent Network Slice and Service Optimization (ISSM-O) upon detecting any breach prediction by the Intelligent SLA Monitoring and & Breach Prediction Module. Step 1.a

and 1.b indicate that the Virtual Radio Resource Managers inside the domains monitor their managed entities and push this monitored data to the Data Lake functional element in the cross-domain on a periodic interval. Upon receiving the notification about breach prediction by the Intelligent Slice and Service Manager - Workflow Manager (ISSM-WFM), it starts a business flow (it is simply a high-level intent) and forwards it to the Smart Resource and Service Discovery (SRSD). In this stage, the SRSD module translates the high-level intent to resource requests (still high-level resources like computing, geographical location of resources, and so on) and submits it to the Marketplace Portal (not shown in this diagram). After getting the candidate resource offers from the Marketplace, SRSD sends them to the ISSM-WFM module. These high-level resource offers, including the monitoring data received from the Data Lake, will be given to the ISSM-O module in the cross-domain platform. step 7, a high-level optimization for resources happens, where the ISSM-O module finds a set of high-level resources that best suits the slice request. After that, in steps 8.a and 8.b, the ISSM-O modules in the domains will be informed about the high-level requests that they have, so they need to perform another level of optimization, which is optimization in a lower level. After performing low-level optimization by the ISSM-O modules in both domains, the results of the optimization will be given to the Network Slice and Service Optimization (ISSMO) for slice establishment and stitching sub-slices. The rest of the process for establishing and stitching the slices in given in the trustworthy slice setup with 3rd party resources workflow.

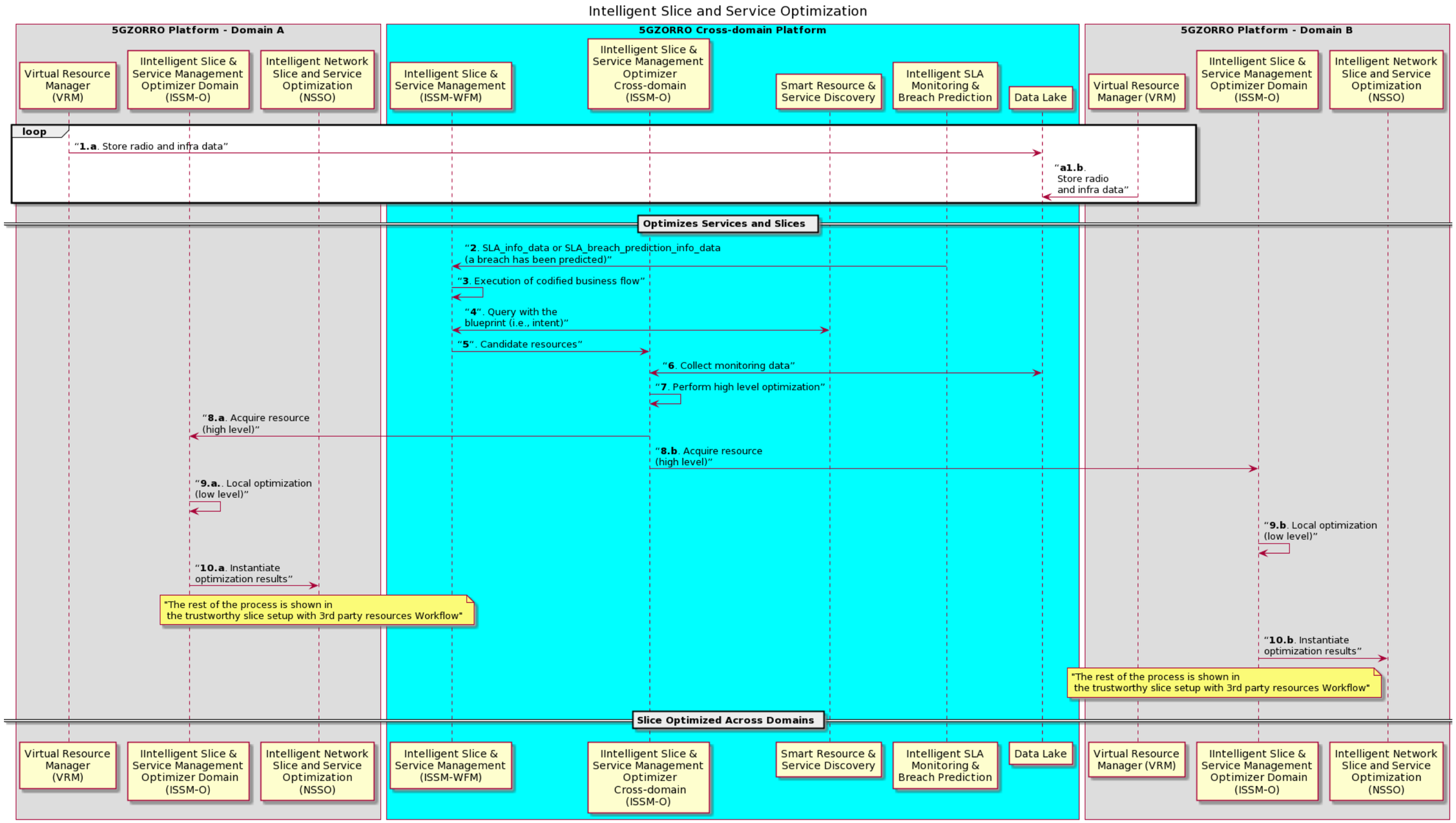

Figure 7-17: Intelligent Network Slice and Service Optimization

8 Conclusions

This deliverable provides the final design of the 5GZORRO high-level architecture and represents the final outcome of the architecture design work performed in the project.

This deliverable provides an update of the specifications presented in D2.2 and D2.3 and has to be considered as a stand-alone self-contained document providing full details on the final design choices, functional blocks identification, services offered and functionalities supported by the 5GZORRO architecture. Specifically, the updates and final content of this design document incorporate the feedback from the implementation and use case validation activities carried out in the project.

A summary of the specific contributions of the presented design elements and overall architecture to the 5GZORRO objectives and related KPIs is also provided in Table 8-1 in terms of applicable design artefacts. The 5GZORRO software implementation and use case experimental validation activities have the objective to achieve and demonstrate the target KPI metrics.

Table 8-1: Contribution to 5GZORRO objectives and KPIs.

OBJECTIVE	Target KPIs	Applicable Design Artifact
OBJ-1. Define a system level architecture combining zero-touch automation solutions and distributed ledger technologies to enable a secure, flexible and multi-stakeholder combination and composition of resources and services in 5G networks.	• *Support actual distributed multi-party service and business configurations (KPI target: more than 3 providers/operators of virtualized resources or services for spectrum, radio/edge/core compute & network).*	See Section 5.3.1 for DLT Governance management.
	• *Inject and process operational service data (configurations and runtime monitoring and logging) into a multi-party 5G Operational Data Lake (KPI target: at least 10 heterogeneous and diverse operational data sets streamed into 5G Operational Data Lake from various data sources, at least one per provider/operator).*	See Section 5.3.21 for DataLake functional block and Section 5.3.16 for Intelligent SLA Monitoring & breach prediction workflow.
	• *Expose open APIs to application layer for processing operational data for analytical processes, which discover and "inventorize" various types of resources (KPI target: all external 5GZORRO APIs are exposed via open and public specifications).*	See Section 5.3.4 for Smart Resource and Service discovery.
	• *Automate the overall service lifecycle management with seamless use of heterogeneous virtualization platforms (i.e., VMs and containers, interconnected with various levels and forms of service meshes) across different providers (KPI target: completion of end-to-end provisioning in less than 5 mins, service deletion in less than 1 min).*	See Section 5.3.13 for Network Slice and Service Orchestration, Section 7.10 for Intelligent Network Slice and Service optimization, and Section 5.3.18 for Abstract Resource Management and Control.
	• *Support a real-time market for dynamic spectrum allocation allowing business agents to trade on spectrum allocations in space and time (KPI target: Time from transaction to spectrum availability in less than 10 minutes; support of 5GNR, LTE and WiFi technologies).*	See Section 5.3.19 for Marketplace DLT platform and Section 7.4 for Trustworthy Smart Contract setup for spectrum workflow.
OBJ-2. Design and prototype a security and trust framework, integrated with 5G service management platforms, to demonstrate Zero-Day trust establishment in distributed multi-stakeholder environments and automated security management to ensure	• *Provide mechanisms for zero touch trust automation in multi-domain scenarios on top of a 5G service management framework (KPI target: to cover up to 4 different stakeholders as part of the automated trust establishment process and to enable its automatic renegotiation when a stakeholder is joining or leaving the trust link).*	See Section 5.3.7 for Identity and Permission management, Section 5.3.8 for Trust Management and 5.3.9 for Trust Execution Environment management functional blocks.
	• *Enhance a 5G service management framework enabling the detection of security vulnerabilities and compromises and the provision of a set of potential countermeasures to mitigate them using a zero-touch approach (KPI target: identifying 6 different types of common attacks*	See Section 5.3.10 for Intra-domain Security at the Business Level and 5.3.11 for Inter-domain Security at the Communication Level

OBJECTIVE	Target KPIs	Applicable Design Artifact
trusted and secure execution of offloaded workloads across domains in 5G networks	*to software infrastructures and provide a complete set of countermeasures -filter traffic, divert it to a honeynet, send an alert to the system admin, etc.- for each of them).*	
	• *Support the integration of zero trust hardware platforms (TEE - Trusted Execution Environments) as a root of trust for the monitoring of information and the establishment of end-to-end secure communications enabling critical workloads to go across different tenants and different stakeholders (KPI target: research on the integration evolution of three TEE platforms --one provided by a project partner-- and two other commercial ones to support a fast and secure establishment of end-to-end cross-slice communications for critical workloads).*	See Section 5.3.9 for Trust Execution Environment management functional block.
OBJ-3. Define a Smart Contract ecosystem anchored on a native distributed ledger to allow commercial and technical data provided by 3rd-party users to be standardised and mapped into Smart Contracts, which can be initiated "at will" between multiple untrusted parties.	• *Ability for untrusted parties to negotiate, set-up and operate a new technical/commercial relationship via a Smart Contract for 3rd-party resource leasing/allocation with associated SLA (KPI target: Smart Contract for 3 or more untrusted parties).*	See Section 5.3.3 for Legal Prose Repository functional block, Section 5.3.5 for Intelligent 3rd party resource selection, Section 5.3.13 for Network Slice and Service Orchestration. See Section 7.6 for Slice setup with 3rd party resource workflow.
OBJ-4. Define solutions for secure, automated and intelligent resource discovery, brokerage and selection, operation with SLA to facilitate workload offloading to 3rd-party resources supporting pervasive computing across multiple 5G domains.	• *Automatically discover and "inventorize" various types of resources (i.e., compute, storage, network at core, edge, far-edge), spectrum and services capabilities from different domains and service providers (KPI target: distribution of resource updates and discovery in less than 10 mins).*	See Section 5.3.4 for Smart Resource and Service discovery and Section 7.3 for Resource discovery workflow.
	• *Implement/correlate technical service configurations and SLA monitoring interactions between multiple parties (KPI target: SLA measurements and validation from at least 3 operators involved in a multi-party service chain).*	See Section 5.3.15 for Monitoring Data Aggregation, Section 5.3.16 for Intelligent SLA Monitoring & breach prediction and Section 5.3.21 for Data lake platform.
	• *Support intent-based API to guide the AI-driven resource discovery system (KPI target: open 5GZORRO API specification for resource discovery).*	See Section 5.3.4 for Smart Resource and Service discovery and Section 5.3.5 for Intelligent 3rd party resource selection.

OBJECTIVE	Target KPIs	Applicable Design Artifact
OBJ-5. Define and prototype a secure shared spectrum market to enable real-time trading of spectrum allocations between parties that do not have a pre-established trust relationship.	• *Time to process and enforce new spectrum transactions (i.e., from the moment the transaction is settled until the spectrum becomes available) (KPI target: complete new spectrum transactions in less than 10 minutes).*	See Section 5.3.2 for Resource and Service offer catalogue and Section 7.2 for Spectoken Resource offer publishing.
	• *Number of transactions per second handled by the market, which will determine the volume of spectrum transactions processed by the market (KPI target: 20 transactions/second).*	Covered in WP5 (D5.2, D5.3)
	• *The authenticity of the market agents, preventing double spending that would allow an agent to trade spectrum rights that it does not own (no explicit KPI target: verification of the built-in property of Blockchains).*	See Section 5.3.2 for Resource and Service offer catalogue and Sec 5.3.7 for Identity and Permission management.
	• *Linkability between market agents and their associated radio access points, which will allow to provide the appropriate spectrum rights to each access point (KPI target: <10M cell towers should be linkable by the system, which is a reasonable EU nation-wide deployment).*	Covered by WP5 (D5.3)
	• *Ability to enforce the settled spectrum rights and obligations, which will build on lightweight Trusted Execution Environments (TEE) embedded in the radio access points to ensure that the reported spectrum measurements are faithful, and the spectrum allocations settled in the market are enforced (KPI target: Be able to detect spoofing attacks where a base station uses an allocation not authorized by the market).*	Covered in WP4 (D4.4, D4.3)
	• *Agnostic support of various radio technologies, to ensure that the market will work regardless of the considered radio technology (KPI target: 5GNR, LTE and WiFi will be supported).*	See Section 5.3.18.2 for Radio Resource Management and Control functional block.
OBJ-6. Realize a cloud-friendly network software licensing framework for location independent network appliances execution.	• *Enable the creation of license agreement templates associated to VNF/NS instances (KPI target: create templates attached to eContract detailing name, context, license conditions, negotiation goal and constraints).*	See Section 5.3.3 for Legal Prose Repository. See Section 5.3.14 for e-Licensing management and Section 7.8 for Trustworthy e-License control workflow.
	• *Generate vendor independent license token to manage location independent VNFs from 3rd party edge to core datacenter (KPI target: license service creates generic tokens to latter run any vendor VNF across at least 2 network segments).*	See Section 5.3.14 for the definition of the e-Licensing management and Section 7.8 for Trustworthy e-License control workflow.

OBJECTIVE	Target KPIs	Applicable Design Artifact
	• *Instantiate Network Services with VNFs from diverse providers (KPI target: use eContract to include VNF licensed by at least 3 different providers).*	See Section 5.3.14 for the definition of the e-Licensing management
OBJ-7. Validate the 5GZORRO zero-touch automation, security and trust in relevant use cases for the implementation of Smart Contracts for Ubiquitous Computing/Connectivity, Dynamic Spectrum Allocation, and Pervasive virtual CDN services over 3rd-party edge resources.	*No specific target to be covered by architecture design*	n/a
OBJ-8. Ensure the long-term success of the project through standardization and dissemination in scientific, industrial, and commercial fora, and by contributing to relevant open source communities & SDOs also exploring synergies with other EU initiatives and projects.	*No specific target to be covered by architecture design*	5GZORRO architecture includes and is aligned with many SDO design documents and specifications whenever applicable, as reported in Section 4.

9 References

[1] 5GZORRO Consortium, Deliverable D2.1 – "Use Cases and Requirements Definition", May 2020

[2] 5GZORRO Consortium, Deliverable D2.2 – "Design of the 5GZORRO Platform for Security & Trust", Oct 2020

[3] 5GZORRO Consortium, Deliverable D2.3 – "Updated design of the 5GZORRO Platform for Security & Trust", Apr 2021

[4] 5G; Management and Orchestration; Concepts, Use Cases and Requirements (3GPP TS 28.530 Version 15.0.0 Release 15), October 2018. https://www.etsi.org/deliver/etsi_ts/128500_128599/128530/15.00.00_60/ts_128530v150000p.pdf.

[5] GSMA NG.116 - Generic Network Slice Template, V 3.0, 22 May 2020available online: https://www.gsma.com/newsroom/wp-content/uploads/NG.116-v3.0.pdf

[6] ETSI TS 123.501 5G; System Architecture for the 5G System, V15.2.0 June 2018, available online: https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/15.02.00_60/ts_123501v150200p.pdf

[7] 3GPP 5G, Management and orchestration, 5G Network Resource Model (NRM); 3GPP TS 28.541 version 15.4.0 Release 15available online: https://www.etsi.org/deliver/etsi_ts/128500_128599/128541/15.04.00_60/ts_128541v150400p.pdf

[8] https://www.tmforum.org/about-tm-forum/

[9] http://webfunds.org/guide/ricardian.html

[10]Tejas Subramanya, Roberto Riggio, "Centralized and federated learning for predictive VNF autoscaling in multi-domain 5G networks and beyond", IEEE Transactions on Network and Service Management, pp. 63-78, 2021

[11]ETSI GR NFV-EVE 012; Network Functions Virtualisation (NFV) Release 3; Evolution and Ecosystem; Report on Network Slicing Support with ETSI NFV Architecture Framework, v3.1.1, December 2017, available online: https://www.etsi.org/deliver/etsi_gr/NFV-EVE/001_099/012/03.01.01_60/gr_nfv-eve012v030101p.pdf

[12] 3GPP TR 28.801 Telecommunication management; Study on management and orchestration of network slicing for next generation network, V15.1.0, January 2018, available online: https://www.3gpp.org/ftp//Specs/archive/28_series/28.801/28801-f10.zip

[13] ETSI GS NFV-SOL 005; Network Functions Virtualisation (NFV) Release 3; Protocols and Data Models; RESTful protocols specification for the Os-Ma-nfvo Reference Point, V3.3.1, September 2020, available online: https://www.etsi.org/deliver/etsi_gs/NFV-SOL/001_099/005/03.03.01_60/gs_NFV-SOL005v030301p.pdf

[14]ETSI zero-touch network and Service Management (ZSM), Reference Architecture, ETSI GS ZSM 002 V1.1.1, August 2019, available online: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/002/01.01.01_60/gs_ZSM002v010101p.pdf

[15]AWS License Manager. AWS. Web: https://aws.amazon.com/license-manager/

[16] Google How Licensing Works. Google. Web: https://support.google.com/a/answer/6309862?hl=en

[17]TM Forum, SLA Handbook [TMF GB917Release 3.1]

[18]Leitner, P., Michlmayr, A., Rosenberg, F. and Dustdar, S., 2010, July. Monitoring, prediction and prevention of sla violations in composite services. In *2010 IEEE International Conference on Web Services* (pp. 369-376). IEEE.

[19] Hussain, W., Hussain, F.K., Hussain, O. and Chang, E., 2015, November. Profile-based viable service level agreement (SLA) violation prediction model in the cloud. In *2015 10th international conference on P2P, parallel, grid, cloud and internet computing (3PGCIC)* (pp. 268-272). IEEE.

[20]Tang, B. and Tang, M., 2014, September. Bayesian model-based prediction of service level agreement violations for cloud services. In *2014 Theoretical Aspects of Software Engineering Conference* (pp. 170-176). IEEE.

[21]A Gentle Introduction to Long Short-Term Memory Networks by the Experts, Jason Brownlee, https://machinelearningmastery.com/gentle-introduction-long-short-term-memory-networks-experts/

[22] ARIMA Model – Complete Guide to Time Series Forecasting in Python, https://www.machinelearningplus.com/time-series/arima-model-time-series-forecasting-python/

[23]Decentralized Identifiers (DIDs) v1.0. Drummond Reed; Manu Sporny; Markus Sabadello; Dave Longley; Christopher Allen. W3C. 28 July 2020. W3C Working Draft. Available online: https://www.w3.org/TR/did-core/

[24] Sporny, M., Longleyy, D., and Chadwick, D. Verifiable Credentials Data Model 1.0. Expressing verifiable information on the Web. W3C Recommendation 19 November 2019. Available online: https://www.w3.org/TR/vc-data-model/

[25]Jingwen Wang, Xuyang Jing, Zheng Yan, Yulong Fu, Witold Pedrycz, and Laurence T. Yang. 2020. A Survey on Trust Evaluation Based on Machine Learning. ACM Comput. Surv. 53, 5, Article 107 (October 2020), 36 pages.

[26] Xu Chen, Yuyu Yuan, Lilei Lu, and Jincui Yang. 2019b. A multidimensional trust evaluation framework for online social networks based on machine learning. IEEE Access 7 (2019), 175499–175513.

[27] Tung Doan Nguyen and Quan Bai. 2018. A dynamic Bayesian network approach for agent group trust evaluation. Computers in Human Behavior 89 (2018), 237–245.

[28]Mrabet, M., Saied, Y. B., & Saidane, L. A. (2019). CAN-TM: Chain Augmented Naïve Bayes-based Trust Model for Reliable Cloud Service Selection. *ACM Transactions on Internet Technology (TOIT)*, *19*(4), 1-20.

[29] Xia, H., Zhang, S. S., Li, Y., Pan, Z. K., Peng, X., & Cheng, X. Z. (2019). An attack-resistant trust inference model for securing routing in vehicular ad hoc networks. IEEE Transactions on Vehicular Technology, 68(7), 7108-7120.

[30]Soleymani, S. A., Abdullah, A. H., Zareei, M., Anisi, M. H., Vargas-Rosales, C., Khan, M. K., & Goudarzi, S. (2017). A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing. IEEE Access, 5, 15619-15629.

[31] Singh, K., & Verma, A. K. (2018). A fuzzy-based trust model for flying ad hoc networks (FANETs). International Journal of Communication Systems, 31(6), e3517.

[32]ETSI zero-touch network and Service Management (ZSM), Requirements based on documented scenarios, ETSI GS ZSM 001 V1.1.1, October 2019, available online: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/001/01.01.01_60/gs_ZSM001v010101p.pdf

[33]5GZORRO Consortium, Deliverable D2.2 – "Design of the 5GZORRO Platform for Security & Trust", Oct 2020

[34]5GZORRO Consortium, Deliverable D2.3 – "Update Design of the 5GZORRO Platform for Security & Trust", April 2021.

[35] TM Forum Geographic Address Management API User Guide, TM Forum Specification, TMF673, Release 18.5.0, January 2019.

[36]CORDA 4.5 Documentation – CORDA API Section, https://docs.corda.net/docs/corda-os/4.5.html

[37]Open Source MANO, ETSI-hosted project to develop an Open Source NFV Management and Orchestration (MANO) software stack aligned with ETSI NFV. URL: https://osm.etsi.org/

[38]Kubernetes. URL: https://kubernetes.io/

[39]Openstack. Open Source Cloud Software. URL: https://www.openstack.org/

[40] Open Network Operating System (ONOS) open source SDN controller for building next-generation SDN/NFV solutions. URL: https://www.opennetworking.org/onos/

[41] Resource Catalog Management API REST Specification, TM Forum Specification, TMF634, Release 17.0.1, December 2017.

[42] Service Catalog Management API REST Specification, TM Forum Specification, TMF633, Release 18.5.0, January 2019.

[43] Product Catalog Management API REST Specification, TM Forum Specification, TMF620, Release 19.0.0, July 2019.

[44]N. Ford, "Comparing Service-based Architectures", available on-line http://nealford.com/downloads/Comparing_Service-based_Architectures_by_Neal_Ford.pdf

[45]3GPP; Technical Specification Group Core Network and Terminals; 5G System; Technical Realization of Service Based Architecture; 3GPP TS 29.500 version 17.0.0 Release 17, September 2020, available online:

[46]Argo Workflows and Pipelines. URL: https://argoproj.github.io/

[47]ETSI zero-touch network and Service Management (ZSM), Terminology for concepts in ZSM, ETSI GS ZSM 007 V1.1.1, August 2019, available online: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/007/01.01.01_60/gs_ZSM007v010101p.pdf

[48]ETSI Network Functions Virtualisation (NFV), Architectural Framework, ETSI GS NFV 002 V1.2.1, December 2014, available online: https://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf

[49] ETSI Network Functions Virtualisation (NFV), Management and Orchestration, ETSI GS NFV-MAN 001, V1.1.1, December 2014, available online: https://www.etsi.org/deliver/etsi_gs/NFV-MAN/001_099/001/01.01.01_60/gs_NFV-MAN001v010101p.pdf

[50]Experiential Networked Intelligence (ENI); System Architecture, September 2019. https://www.etsi.org/deliver/etsi_gs/ENI/001_099/005/01.01.01_60/gs_ENI005v010101p.pdf.

[51]https://inform.tmforum.org/features-and-opinion/blockchain-based-telecom-infrastructure-marketplace-enables-pop-up-networks-and-on-the-fly-business-models/

[52] TM Forum Product Catalog Management API, https://github.com/tmforum-apis/TMF620_ProductCatalog

[53] https://www.tmforum.org/vertical-industry-telcos-federated-dlt-based-marketplace/

[54]ITU-T DLT reference architecture https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d31.pdf

[55] ETSI White paper – "An Introduction of Permissioned Distributed Ledger (PDL)" - https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP48-PDL.pdf

[56]MEF 3.0 overview, https://www.mef.net/service-standards/

[57]MEF LSO Sonata APIs FAQ, v6, June 2020, https://www.mef.net/wp-content/uploads/MEF-faq-MEF-LSO-Sonata-APIs.pdf

[58] MEF-LSO-Sonata-SDK (Release Candidate 5), https://github.com/MEF-GIT/MEF-LSO-Sonata-SDK

[59] Service Operations Specification MEF 55. Lifecycle Service Orchestration (LSO): Reference Architecture and Framework. https://www.mef.net/Assets/Technical_Specifications/PDF/MEF_55.pdf

[60]Communications Business Automation Network. https://cban.net/

[61] Communications Business Automation Network (CBAN) Whitepaper version 1.0. https://9db836f3-ccf1-4990-82a6-3036d6f8890a.filesusr.com/ugd/d18226_4bb3582cc7314f649cdaf56811e93d6e.pdf

[62] CBAN Reference Architecture, January 2020. https://9db836f3-ccf1-4990-82a6-3036d6f8890a.filesusr.com/ugd/d18226_545a1ea92d814206957a0d4d41a73a17.pdf

[63] CBAN MVP Definition Data on Demand, January 2020. https://9db836f3-ccf1-4990-82a6-3036d6f8890a.filesusr.com/ugd/d18226_223d1039cc044bd09b1b88ed8b6b20c5.pdf

[64]ITU-T (2018) ITU-T. Y.3054. Framework for trust-based media services.

[65]ETSI (2020) Electronic Signatures and Infrastructures (ESI); Global Acceptance of EU Trust Services. https://www.etsi.org/deliver/etsi_tr/103600_103699/103684/01.01.01_60/tr_103684v010101p.pdf

[66]ISO (2018) Framework of trust for processing of multi-sourced data. Available online: https://www.iso.org/standard/74844.html

[67]Corda | Leading DLT Platform for Regulated Industries - https://www.corda.net/

[68]Hyperledger Indy - https://www.hyperledger.org/use/hyperledger-indy

[69]Hyperledger Aries - https://www.hyperledger.org/use/aries

[70]Open Data Hub, https://opendatahub.io/

[71]OpenTelemetry: High-quality, ubiquitous, and portable telemetry to enable effective observability - https://opentelemetry.io/

[72]FeedForward Neural Networks: An Introduction - https://media.wiley.com/product_data/excerpt/19/04713491/0471349119.pdf

[73]Intel® Software Guard Extensions (SGX) - https://www.intel.it/content/www/it/it/architecture-and-technology/software-guard-extensions.html

[74]Open Portable Trusted Execution Environment - https://www.op-tee.org/

[75]Trustonic - https://www.trustonic.com/technology/

[76]ISTIO. URL: https://istio.io

[77] NSM, Network Service Mesh. URL: https://networkservicemesh.io/

10 Abbreviations and Definitions

10.1 Definitions

No definition introduced in this deliverable.

10.2Abbreviations

5G IA	5G Infrastructure Association
AIOps	Artificial Intelligence for IT operations
CNF	Cloud Native Function
CSP	Communication Service Provider
DoA	Description of Action
DID	Decentralized Identifier
DLT	Distributed Ledger Technology
EC	European Commission
IPR	Intellectual Property Rights
LCM	LifeCycle Management
MANO	Management and Orchestration
NFV	Networks Function Virtualization
NFVI	Networks Function Virtualization Infrastructure
NFVO	Networks Function Virtualization Orchestrator
NS	Network Service or Network Slice depending on the context
NSM	Network Service Mesh
PPP	Public Private partnership
SBA	Service Based Architecture
SBI	Service Based Interface
SC	Smart Contract
SDO	Standard Developing Organization
SM	Service Mesh
VIM	Virtual Infrastructure Manager
VNF	Virtual Network Function
VNFM	Virtual Network Function Manager
WG	Working group
WP	Work Package
ZSM	Zero Touch Service Management