5GZORRO

Grant Agreement 871533

H2020 Call identifier: H2020-ICT-2019-2
Topic: ICT-20-2019-2020 - 5G Long Term Evolution

D2.3: Update 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:
ALB	**V1.0**

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

Deliverable title:
D2.3: Update Design of the 5GZORRO Platform for Security & Trust

Start date of the project:	Contractual delivery date:	Actual delivery date:
01/11/2019 **(duration 30 months)**	**30/04/2021**	**30/04/2021**

Editor(s)
P. Chainho (ALB)

List of Contributors

Participant	Short Name	Contributor
Nextworks	NXW	P.G. Giardina, G. Carrozzo, J. Brenes, E. Bucchianeri
Fundaciò i2CAT	I2CAT	Adriana Fernández-Fernández, Carlos Herranz Claveras, Javier Fernández-Hidalgo, Shuaib Siddiqui
IBM Israel Science and Technology	IBM	K. Meth, D. Breitgand
Telefonica Investigacion y Desarrollo	TID	Diego Lopez
Ubiwhere	UW	P. Diogo
Fondazione Bruno Kessler	FBK	B., Rasoul
Universidad de Murcia	UMU	J.M. Jorquera Valero, P.M. Sánchez Sánchez, M. Gil Pérez, G. Martínez Pérez
Bartr Holding Limited	BTL	J. Taylor
Altice Labs	ALB	P. Chainho, J. Bonnet, A. Gouveia
Intracom	ICOM	M. Mertiri, A. Lekidis, V. Theodorou, D. Laskaratos
Atos Spain	ATOS	F. Díaz Bravo, G. Gómez Chávez
Malta Communications Authority	MCA	J. M. Mifsud, A. Sciberreas

List of Reviewers

Participant	Short Name	Contributor
ATOS	ATOS	F. Diaz
Altice Labs	ALB	J. Bonnet
Nextworks	NXW	G. Corrozzo
Fundacio i2CAT	I2CAT	Shuaib Siddiqui

Change History

Version	Date	Partners	Description/Comments
0.0	02-03-2021	ALB	Table of Contents
0.1	15-03-2021	ALB, UMU, ATOS, i2CAT, IBM, BTL, ATOS	1st round of contributions to chapter 2
0.2	31-03-2021	ALB, NXW, IBM, ICOM, UW, i2CAT	2nd round of contributions to chapter 2 and 1st round of contributions to Chapter 3.
0.3	09-04-2021	ALB, ICOM, ATOS, FBK, i2CAT, IBM	3rd round of contributions to chapter 2, 2nd round of contributions to Chapter 3, 1st round of contributions to Chapter 4.
0.4	14-04-2021	ALB, IBM, BTL, NXW, i2CAT, ICOM, ATOS, FBK	4th round of contributions to chapter 2, 3rd round of contributions to Chapter 3, 2nd round of contributions to Chapter 4, 1st Round of Contributions to Introduction and Conclusions. Review version.
0.5	19-04-2021	ALB, ATOS	Internal Review by ALB and ATOS
1.0	23-04-2021	ALB, UMU, IBM, NXW, IBM, i2CAT, ICOM	Comments from Internal Review addressed. Consolidation and final edition.
1.0	29-04-2021	NXW, i2CAT	QA before submission

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

This deliverable D2.3 updates the previously issued specifications contained in D2.1 and D2.2 with the most relevant findings arose along the first eighteen months of the 5GZORRO project. The architecture update presented in this document was triggered by the detailed technical specifications and the ongoing implementation work performed by workpackages WP3 and WP4.

Only the additional specifications are reported in this document with respect to deliverable D2.1 and D2.2. Therefore, the reader should refer to both referenced documents to get the full description of 5GZORRO Use Cases, associated Requirements and the resulting 5GZORRO Architecture.

Reported changes are mainly related to improvements of the operational workflows and derive from a more in-depth analysis for design of the software components done within WP3 and WP4. Some examples of major specification updates contained in this document include:

- A clearer view on how to cope with spectrum regulatory aspects, which resulted in major changes to the Spectoken-related Workflows.
- The introduction of a new functional element, namely the Abstract Resource Management, which is responsible to manage any types of 5G resources in the Zero Touch and Orchestration layer. This change has improved the flexibility of the 5GZORRO Architecture to ease its implementation. This change would also potentially improve 5GZORRO platform extensibility to support new types of 5G resources.
- Security and Trust Functional Block has been divided in three more granular and consistent functional blocks to better group the diverse functionalities.
- The SLA monitoring intelligence related functionalities have been converged into a single functional block.
- All the intelligence discovery functionalities have been converged into a single functional block.
- Decomposition of the Intelligent Slice and Service Management into more granular functional elements to separate business and technical level orchestration scopes. This design decision can also facilitate independent development of different functional areas and ensure better sustainability and exploitability of the assets through pluggable architecture.
- Major refactoring of Slice management related workflows including a clear segregation of intra- and cross-domain functionalities.

The reviewed 5GZORRO architecture reported in this document is more aligned with the software being implemented in WP3 and WP4.

1 Introduction

The main objective of this deliverable is to review and update the description of 5GZORRO Use Cases and associated Requirements - reported in D2.1 [1] - as well as the 5GZORRO Architecture design - reported in D2.2 [2]. Such updates consider the most relevant findings along the first phase (of eighteen months) of the project, notably the detailed technical specification [3][4] and implementation [5] work performed in WP3 and WP4.

The main outcome of this document is an updated functional architecture of 5GZORRO Platform including the update of workflows that illustrate the main operations required to support the Use Cases to be demonstrated. In addition, an analysis check of how 5GZORRO architecture fulfils identified requirements, is also provided.

The analysis and design of the software components carried on in WP3 and WP4, have inspired a revision of some workflow details. As expected in complex software systems, such work has contributed to clarify some more ambiguous aspects of the initial architecture design. In other cases, we had to revisit old discussions and pick-up previously discarded architectural designs.

The review performed in this document to 5GZORRO use cases and architecture has improved alignment between the higher-level functional view of 5GZORRO Platform and its more granular software view that is being specified and implemented in WP3 and WP4. Such work contributes to increase the strength of 5GZORRO foundations and to move on to a second implementation phase with more challenging features.

1.1 Document outline

This document is structured as follows:

- Section 2 provides the overall review of 5GZORRO use cases and 5GZORRO functional high-level architecture including the description of the main changes in each functional element.
- Section 3 updates how the functional elements interact in the most relevant operation patterns of the architecture.
- Section 4 analyses in detail how 5GZORRO architecture can fulfil the different requirements coming 5GZORRO use cases.
- Section 5 concludes the document.

2 Review of 5GZORRO use cases and architecture

The aim of 5GZORRO is to reduce the current gap that exists between the ongoing 5G implementations and the 5G service requirements, from the vertical industries. 5GZORRO leverages the novel concepts of Data-Driven/AI-based solutions, Distributed Ledger Technologies, and Cloud-Native based Technologies to i) support AIOps paradigm and enable automatic network operations, ii) implement multi-part end-to-end service and slice characterized by a high level of security and trust and iii) provide the high level of flexibility required by advanced 5G services.

As just recalled in D2.1 [1] and D2.2 [2], the main innovations 5GZORRO aims to bring into 5G are:

1. **Zero-touch/Automated Resource discovery using DLT/Blockchains.** With this solution, based on both DLT and AIOps technologies, different stakeholders are enabled to publish and trade their own services and resources, leveraging the Marketplace Application provided by 5GZORRO. The Marketplace is DLT-based, thus making the published offers immutable and easy to be discovered and classified. The discovery and classification processes are designed to be automatized, to minimize the human intervention (zero-touch).
2. **Intelligent 3rd party resource selection, request, and access/usage**. An AI-based process selects the most suitable offers among the ones present into the Marketplace blockchain, based on the requirements specified by the resource/service customer which are cross-checked with the historical data stored into the 5GZORRO operational Data Lake (data-driven ai-based decision). Once the proper resource has been selected, the transaction and all the legal aspects related to the acquisition, deployment, configuration, and access of the service are automatically addressed by the platform. The deployment and configuration aspects include the creation of the services and its seamless composition across different administrative domains (if required), while legal aspects may include the application of the agreed SLA and the monitoring and reaction to possible SLA violations.
3. **Trust establishment among multiple parties**. The guarantee that the resources and the services, available in the Marketplace, come from secure and trusted sources is mandatory. 5GZORRO aims to provide a set of services that guarantees the trust and the security among the parties involved into a business relationship, while allowing the automatic establishment of such a relationship.

A more detailed discussion can be found in the deliverables D2.1 [1] and D2.2 [2] where the 5GZORRO concept is widely discussed. The core specification elements of 5GZORRO use cases and architecture contained in those Deliverables have been carefully reviewed by the Consortium considering the main findings from WP3 and WP4 technical specification [3][4] and implementation work [5] performed so far. The results of this architecture review are reported in the following of this Chapter.

2.1 Updates to Roles and Stakeholders

2.1.1 Roles

No new roles are added into 5GZORRO business ecosystem, but the Marketplace DLT Node Operator has been removed since all members of 5GZORRO Marketplace have to operate one Marketplace DLT node. On the other hand, it is now clearer, Governance Administrators and Regulators are grouped into a single logical entity called 5GZORRO Administration Governance Board. A summary of 5GZORRO business roles is provided below:

The **Resource Provider** is the role in charge of the provision and management of resources used to realize communication services. In general, in 5GZORRO, resources can comprise computing, storage and networking capabilities, including network functions.

The **Service Provider** is the role that offers communication services that are realized on top of an infrastructure comprised by resources providing computing, storage and networking capabilities.

The **Resource Consumer** is the role that uses resources from Resource Providers to build and deliver Communication Services.

The **Service Consumer** or **customer** is the role that buys products and services from the Service Provider or receives free offers or services from Service Providers.

The **Governance administrator** is the role that has rights to take decisions on the governance of the 5GZORRO Marketplace, for example, to approve or reject new members into the Marketplace. 5GZORRO Governance Administrators are grouped into a single entity called 5GZORRO Administration Governance Board.

The **Regulator Authority** is the role in charge of supervising communication delivery business including the rights to use certain Communication Resources like licensed radio spectrum. The Regulator Authority is also part of the 5GZORRO Administration Governance Board where, according to the adopted Governance Model, may play a critical role e.g., may have veto power on some decisions like approval of new members.

The **Data Operator / Aggregator** is the role in charge of operating the 5GZORRO Public Data-Lake.

The **Data Supplier** is the role in charge of providing data collected/injected in the 5GZORRO Public Data-Lake.

The **Data Consumer** is the role that consumes data from the 5GZORRO Public Data-Lake.

2.1.2 Stakeholders

In terms of 5GZORRO Business Stakeholders no major changes were needed. Thus, the following list of stakeholders are still valid:

Verticals industries, e.g., manufacturing sector, media sector/CDN provider acquiring 5G communication services, usually play the Resource Consumer or Service Consumer role.

Communication Service Providers (CSPs), MNOs will be typically playing in 5GZORRO the role described for Service Providers. As explained in D2.1, CSPs may also play the Resource Consumer and Resource Provider roles as well.

The **Third-Party Resource Provider** is the stakeholder playing the role of a Resource Provider.

Software Vendors play the role of Resource Providers and offer virtual functions (VF) or Cloud-native Functions (CF) to onboard in the 5GZORRO catalogue or software solutions for the 5GZORRO platform (i.e., MANO stack, Data-lake components).

Regulator: plays the role of regulatory authority regarding communication resource sharing.

2.2 Updates to Use Cases and Related Requirements

2.2.1 Use Cases

In this Section the updates are reported for the use case descriptions and scenarios produced by the work in the 5GZORRO architecture design and the development of the various functional blocks. The objective is to only reflect the changes on the use cases, avoiding the repetition of the content provided in Deliverable D2.1 [1].

The only use cases that have undergone modifications are the dynamic spectrum allocation (use case 2) and the pervasive vCDN services (use case 3), as described in the next Subsections.

2.2.1.1 Use Case 2: Dynamic Spectrum Allocation

Within the development of the project, the spectrum resource modelling in the 5GZORRO platform became clearer, including the flows where the generation of Spectokens was needed. On the one hand, the Regulator stakeholder, the sole responsible entity of the spectrum management, will have the ability to generate spectrum certificates for spectrum resource providers, i.e., MNOs, that acquired the right to operate on the licensed spectrum. These spectrum certificates will act as verifiable claims in the 5GZORRO platform. On the other hand, a spectrum resource provider will use its spectrum certificate to generate Spectokens for a particular area.

The description of the Spectokens creation in D2.1 is not aligned with the abovementioned concept. In D2.1, the burden of creating Spectokens felt on the Regulator side, who later distributed the Spectokens among the spectrum providers to enable the spectrum market. Therefore, this Subsection introduces the necessary updates of the information given in D2.1 to match the new Spectoken generation process.

The updated UC2 flow is now shown on Figure 2-1.

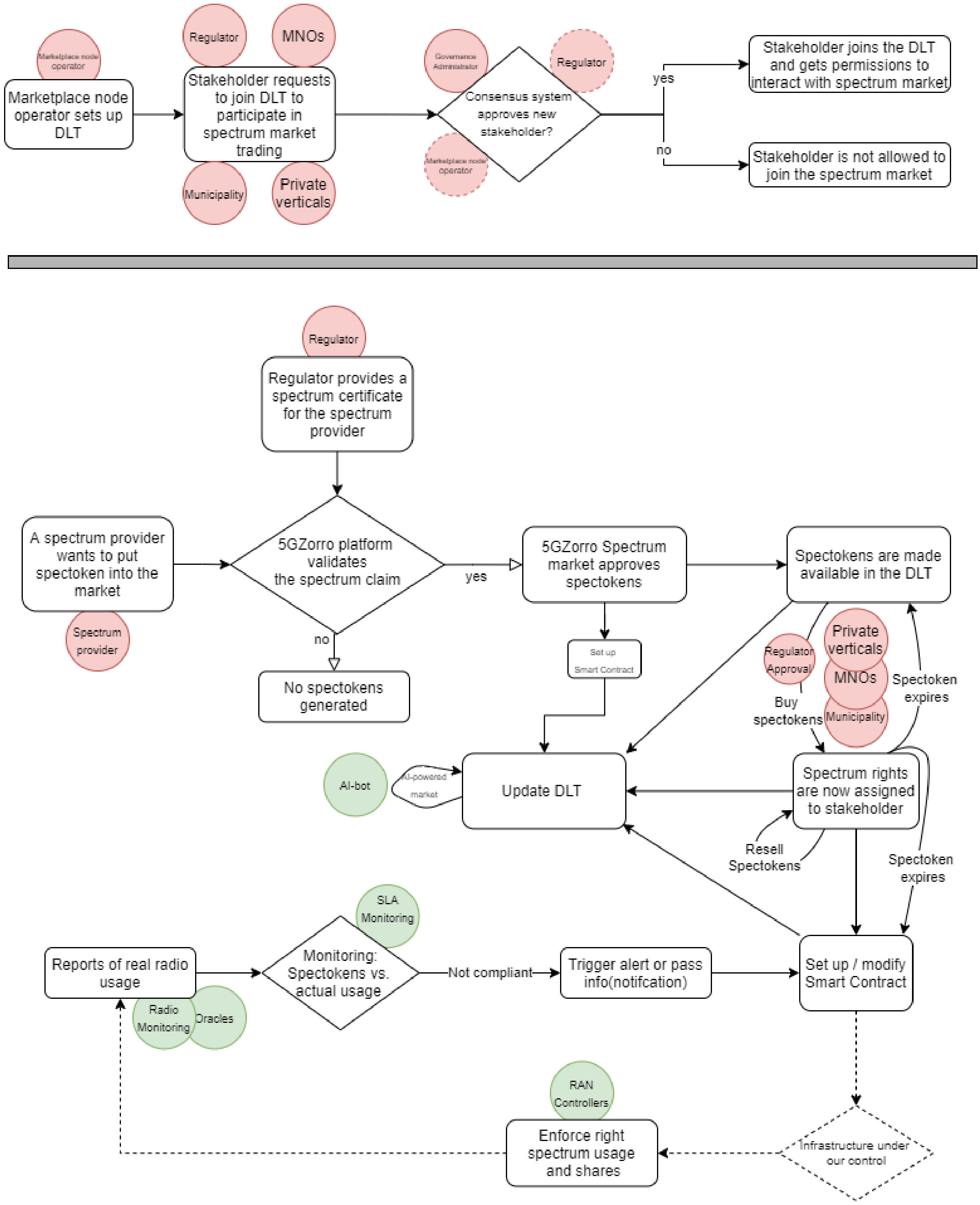

Marketplace node operator
Marketplace node operator sets up DLT
Regulator
MNOs
Stakeholder requests to join DLT to participate in spectrum market trading
Municipality
Private verticals
Governance Administrator
Regulator
Consensus system approves new stakeholder?
Marketplace node operator
yes
no
Stakeholder joins the DLT and gets permissions to interact with spectrum market
Stakeholder is not allowed to join the spectrum market
Regulator
Regulator provides a spectrum certificate for the spectrum provider
A spectrum provider wants to put spectoken into the market
Spectrum provider
5GZorro platform validates the spectrum claim
yes
no
No spectokens generated
5GZorro Spectrum market approves spectokens
Spectokens are made available in the DLT
Set up Smart Contract
Regulator Approval
Private verticals
MNOs
Municipality
Buy spectokens
Spectoken expires
AI-bot
AI-powered market
Update DLT
Spectrum rights are now assigned to stakeholder
Resell Spectokens
Spectoken expires
SLA Monitoring
Reports of real radio usage
Radio Monitoring
Oracles
Monitoring: Spectokens vs. actual usage
Not compliant
Trigger alert or pass info(notifcation)
Set up / modify Smart Contract
RAN Controllers
Enforce right spectrum usage and shares
Infrastructure under our control

Figure 2-1: Use Case 2: Dynamic Spectrum Allocation Workflow

The corresponding updated table on node setup is now Table 2-1.

Table 2-1: Marketplace node setup and Stakeholder Registration

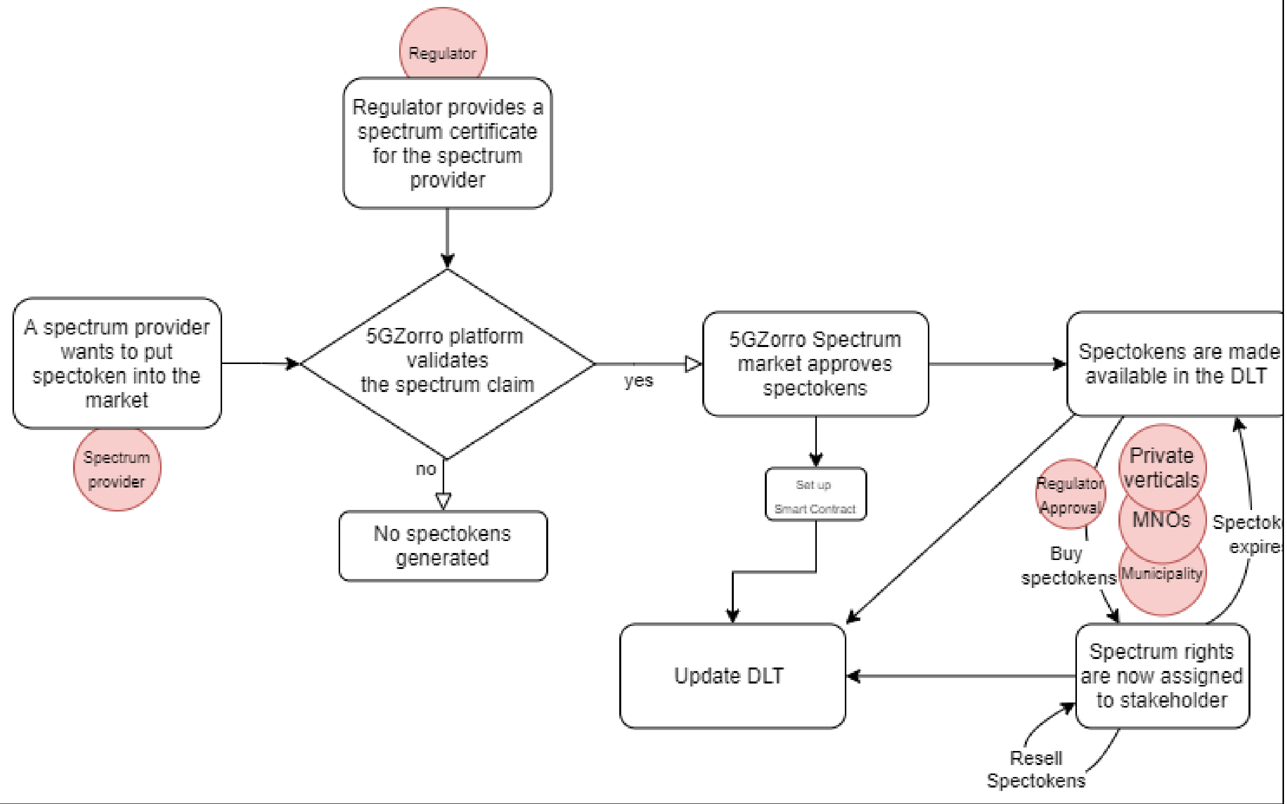
Procedure/ workflow	• A Stakeholder who wants to get some spectrum resources initializes a Marketplace node, configuring it to work in a private (enterprise network) • All members of the Marketplace Governance Board, including the regulator, get notified about the new Marketplace registration request. A governance check is performed to determine the authenticity of the stakeholder and to assign a certificate with which the stakeholder will have the rights to perform specific transactions on the Marketplace or to be rejected in case no consensus is obtained whenever such transaction is tried. • With a positive outcome of the check, the stakeholder obtains the digital certificate (credential) and is now able to perform transactions on the Marketplace. If the new stakeholder has the right to create Spectokens, the Regulator will create a verifiable claim with the stakeholder's spectrum capabilities, e.g., a list of licensed spectrum bands which the stakeholder has the right to operate outside the 5GZORRO platform. • The stakeholder accesses the 5GZORRO app or web interface that allows it to join the spectrum sharing Marketplace.

The corresponding updated table on introducing and trading Spectokens is now Table 2-2.

Table 2-2: Introducing Spectokens into the spectrum market and trading of Spectokens

Scenario Name	**UC2_2: Introducing Spectokens into the spectrum market and trading of Spectokens**
Rationale/ objective	This scenario deals with introducing Spectokens into the spectrum market and demonstrates how stakeholders can trade these Spectokens. Spectrum providers create Spectokens, after the Regulator's explicit permission when they obtained the spectrum certificate during the platform onboarding procedure and put these Spectokens in the spectrum market.
Storyboard	• A spectrum provider issues a Spectoken by providing the spectrum technical details (range of frequencies, area of application). • Spectrum resource providers must be validated to issue Spectokens by the Regulator. This privilege is obtained as a means of spectrum certificate. • The 5GZORRO platform validates the identity of the spectrum providers and the permissions associated as such and its spectrum capabilities. If the identity is validated and the Spectokens are not considered duplicates, the request to create Spectokens is approved and can be included in the Marketplace. • MNO/Verticals/Municipalities access the spectrum market and can see the available Spectokens. They now can buy or resell Spectokens.

	• Transferring Spectokens can be done without Regulator approval as long as the buyer has the correct spectrum trading credentials • After a successful transaction, be it generation or trading Spectokens, the new status of Spectoken distribution is kept in the Marketplace DLT. • The updated Spectoken assignment and availability is displayed in the spectrum sharing App.
Stakeholders involved	• Regulator Authority, Industry Verticals, M(V)NO, Municipalities
Pre-conditions	• All stakeholders must be registered in 5GZORRO and have to have their digital certificates in order to be able to interact with the Marketplace DLT.
Procedure/ workflow	• Regulator's identity as trusted stakeholder is confirmed (digital certificate) and access to the Marketplace is granted. • The spectrum provider's identity as trusted stakeholder is confirmed (digital certificate) and access to the Marketplace is granted. • The spectrum provider requests the creation of Spectokens and provides their details. • The Spectoken creation request is validated against the spectrum certificate issued by the Regulator to the spectrum provider. • If the new Spectoken creation is approved, the Marketplace DLT is updated. For that a transaction is performed on the Marketplace DLT. A smart contract is associated to the Spectoken (that determines the price, for example). • The new Spectoken distribution can now be consulted from the spectrum market app. • Stakeholders that play the role of Service Providers and Service Consumers (MNO/Industry vertical/municipalities) log into the spectrum market app to browse available Spectokens. • The stakeholder chooses one or more Spectokens via the app to be bought. • For issuing spectrum, the transaction is validated by checking the spectrum provider's spectrum certificate issued by the regulator. If the transaction is validated, then a smart contract is generated for spectrum trading. • The Marketplace DLT is now reflecting the new status of Spectoken. The smart contracts will reflect the sealed deals in the future.


Regulator
Regulator provides a spectrum certificate for the spectrum provider
A spectrum provider wants to put spectoken into the market
Spectrum provider
5GZorro platform validates the spectrum claim
yes
no
No spectokens generated
5GZorro Spectrum market approves spectokens
Set up Smart Contract
Update DLT
Spectokens are made available in the DLT
Regulator Approval
Private verticals
MNOs
Municipality
Buy spectokens
Spectok expire
Spectrum rights are now assigned to stakeholder
Resell Spectokens

Business models	Spectrum providers, subject to Regulator's recognition, can create Spectokens. Stakeholders, with proper authorisation from the Regulator, can trade these Spectokens.
Envisioned architectural functionality	Spectrum App Marketplace DLTs for keeping track of Spectoken distribution Marketplace DLT transactions to generate Spectokens and to buy them
KPIs	New Spectokens can be introduced within 5 minutes Transaction of registering Spectoken(s) can be completed within 1 minute Transaction of buying Spectoken(s) can be completed within 2 minutes
Benefits of 5GZORRO approach	Faster and more flexible trading of spectrum usage rights Secure transaction

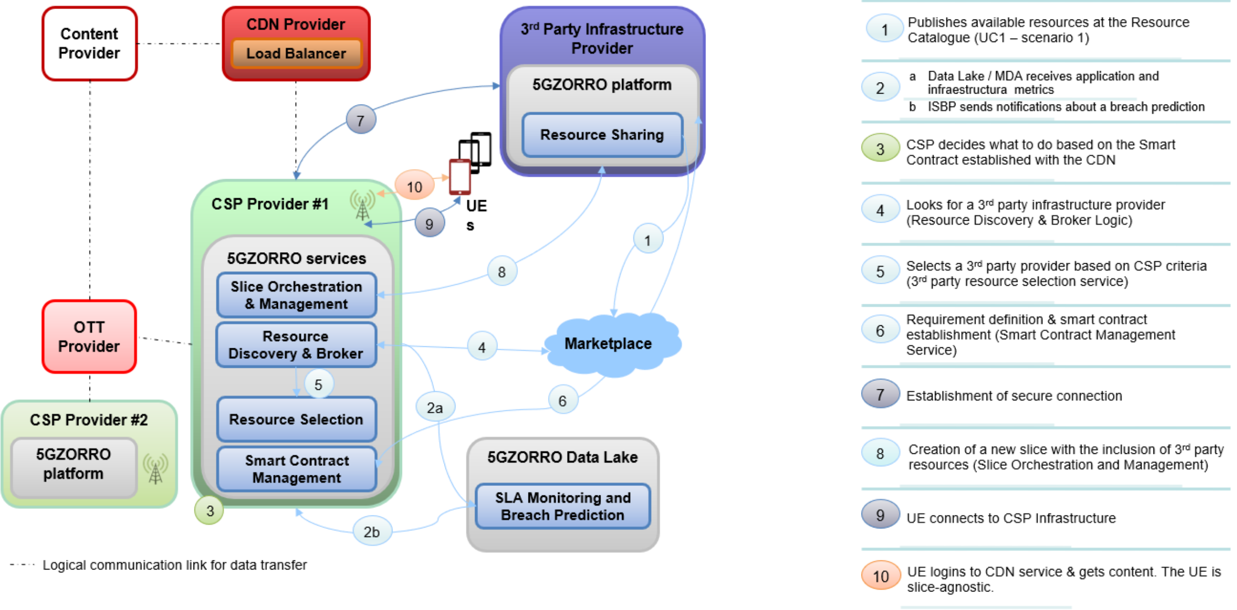
2.2.1.2 Use Case 3: Pervasive virtual Content Delivery Network services

The revision of this use case has originated two changes from Deliverable D2.1, derived from a better understanding of what will the 5GZORRO platform provide to the deployment of the services:

- The responsibilities of certain functionalities like the monitoring of the services or the management of the resources in the Marketplace needs some clarifications. This will be reflected in both scenarios below.
- One of the objectives of this pilot is to demonstrate the eLicensing Management service. This use case is conceptually the most suitable since is the one in that deals with the slice deployment and

scaling in 3rd party domains under certain conditions. For that, VNF vendors are included as stakeholders in both scenarios

In the generic workflow, depicted in Figure 2-2, the 5GZORRO Data Lake component was missing in D2.1, and their interactions with the steps 2a and 2b are added. Step 2a reflects the flow the monitoring data is received by the Data Lake component and published in the Intelligent SLA Breach Prediction (ISBP), and 2b how IBSP sends notifications to the CSP Provider.



1 Publishes available resources at the Resource Catalogue (UC1 – scenario 1)

2 a Data Lake / MDA receives application and infraestructura metrics
b ISBP sends notifications about a breach prediction

3 CSP decides what to do based on the Smart Contract established with the CDN

4 Looks for a 3rd party infrastructure provider (Resource Discovery & Broker Logic)

5 Selects a 3rd party provider based on CSP criteria (3rd party resource selection service)

6 Requirement definition & smart contract establishment (Smart Contract Management Service)

7 Establishment of secure connection

8 Creation of a new slice with the inclusion of 3rd party resources (Slice Orchestration and Management)

9 UE connects to CSP Infrastructure

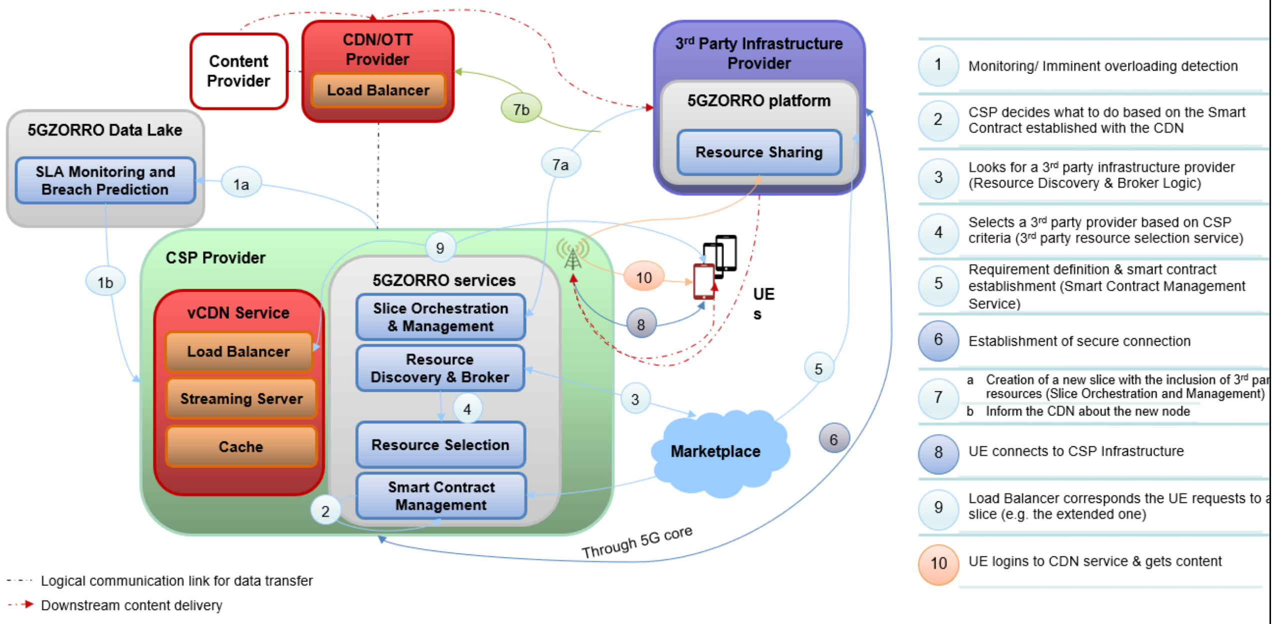
10 UE logins to CDN service & gets content. The UE is slice-agnostic.

Figure 2-2: (Use Case 3) acting as CPE respectively.

These changes related to the Intelligent SLA Breach Prediction, as detailed in the generic workflow. Also, it is important to notice that the CDN provider does not need to accept any new situation, since decision making is predefined inside a Smart Contract that will have an attached SLA.

Table 2-3: (Use Case 3) Low latency 3rd party Edge resources

Scenario Name	**Low latency 3rd party Edge resources**
Storyboard	While the vCDN service is running (i.e., the CDN VNFs are being executed at the CSP infrastructure), the Data Lake is receiving metrics about the edge servers' performance and the service quality delivered to the end users. To prevent hazardous conditions, the Intelligent SLA Breach Prediction (ISBP) module receives monitoring data, both application-level ones as exposed by the CDN service, and infrastructure ones (e.g., CPU, memory, I/O throughput) as provided by the MANO. Thus, the ISBP assesses breach predictions and sends notifications to interested parties through the integration fabric. For example, if the number of users connected to a specific CDN Edge Server exceeds a threshold value, the CSP will request additional resources to avoid reaching a saturation point regarding what was agreed in the smart contract. In addition to this request, the CDN/OTT may define a set of rules and configurations by which it approves the inclusion of 3rd party resources to the CSP scaling mechanism. Therefore, it will facilitate the CSP to take actions before the actual resource saturation takes place. When the CSP receives a request for extra resources it initially tries to satisfy this through its own infrastructure. If these resources are not sufficient, it will search for 3rd party infrastructure resources (Resource Discovery & Broker Logic), selects the 3rd party

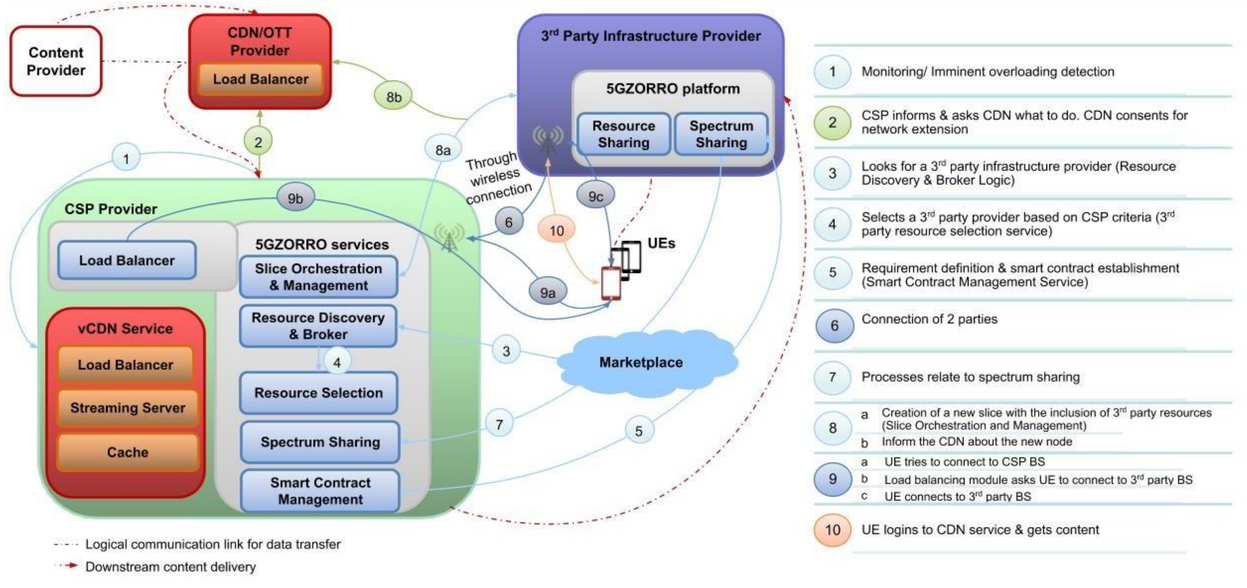
	infrastructure provider (3rd party resource selection service) and establishes a secure (VPN) connection with the 3rd party provider. Moreover, the requirements of the CSP infrastructure towards the 3rd party provider are defined and a smart contract between these two parties is established (Smart Contract Management Service). The extension of the current network slice (Slice Orchestration and Management) takes place over this connection which leads to the inclusion to the allocated 3rd party resources in the eventual setup as well as to the establishment and activation of CDN's VNFs on 3rd party resources. Furthermore, the CDN's Load Balancer oversees traffic splitting decisions and can redirect the user requests to the new slice. Therefore, the new UEs will be served through the same wireless network interface but from a different proxy server. In other words, the new slice will be like the older one until it exits the 5G Backhaul and Core Network. From that point on, the new slice, taking advantage of the low-latency connectivity, will extend to the edge server of the 3rd party infrastructure. From the content delivery perspective, the 3rd party edge infrastructure will host a streaming and a cache server. For instance, the content that is associated with the new slice instance will be cached on the third-party infrastructure. Next, the content will be delivered to the Base Station where the users are connected and the Base Station, in turn, will transmit the content to the UEs.
Stakeholders involved	• CSP (network operator) • VNF Vendors • 3rd party infrastructure provider • CDN/OTT service provider • End User
Procedure/ workflow	
	

Content Provider
CDN/OTT Provider
Load Balancer
3rd Party Infrastructure Provider
5GZORRO platform
Resource Sharing
5GZORRO Data Lake
SLA Monitoring and Breach Prediction
1a
1b
7a
7b
CSP Provider
vCDN Service
Load Balancer
Streaming Server
Cache
5GZORRO services
Slice Orchestration & Management
Resource Discovery & Broker
Resource Selection
Smart Contract Management
2
3
4
5
6
8
9
10
UE s
Marketplace
Through 5G core
Logical communication link for data transfer
Downstream content delivery
1 Monitoring/ Imminent overloading detection
2 CSP decides what to do based on the Smart Contract established with the CDN
3 Looks for a 3rd party infrastructure provider (Resource Discovery & Broker Logic)
4 Selects a 3rd party provider based on CSP criteria (3rd party resource selection service)
5 Requirement definition & smart contract establishment (Smart Contract Management Service)
6 Establishment of secure connection
7 a Creation of a new slice with the inclusion of 3rd par resources (Slice Orchestration and Management)
b Inform the CDN about the new node
8 UE connects to CSP Infrastructure
9 Load Balancer corresponds the UE requests to a slice (e.g. the extended one)
10 UE logins to CDN service & gets content

Table 2-4: (Use Case 3) 3rd party Edge acting as CPE

Scenario Name	**3rd party Edge acting as CPE**
Storyboard	In addition to the CDN/OTT monitoring, the CSP edge server is also monitoring the traffic as well as the resource usage for the serving area. Thus, in the case of increasing traffic, the Intelligent SLA Breach Prediction detects it and based on the rate of the traffic increment, it predicts the probability of resource depletion. Particularly, in this scenario, the overloading occurs at the Base Station. Note that the CSP acts before the actual congestion takes place. When the ISBP detects or predicts an excessive usage of resources, in order to avoid performance degradation and to keep on satisfying the SLA requirements, the CSP may accept the slice extension. This agreement between CDN/OTT and CSP providers can also have a proactive, rule-based character whereby the CDN provider has agreed beforehand upon the configurations of the inclusion of 3rd party resources. It will search (Resource Discovery & Broker Logic) and select (3rd party resource selection service) a 3rd party infrastructure resource provider as described in 4.4.5.1. Since the CSP and the 3rd party provider can have a wireless connection, this connection is employed for the instantiation of vCDN service components in the 3rd party infrastructure. This setup obviously includes aspects related to dynamic spectrum allocation, as the two Base Stations are in nearby areas and, thus, they should avoid using the same spectrum portions for eliminating radio interference issues. Moreover, the 3rd party infrastructure provider may own a limited spectrum for its private network and there may be cases where this spectrum is not enough for supporting the new users that connect to its radio interface. Therefore, the 3rd party infrastructure should be able to borrow extra spectrum bandwidth. Service provisioning is supported through a local 5G-NR (or other) wireless interface, effectively extending the service coverage area of the network operator. Therefore, the new UEs will be served through the 3rd party wireless network interface. Generally, there should be a CSP Base Station Assignment module (instead of a CDN Load Balancer) responsible for choosing the wireless interface where each user will be connected to. Regarding the new slice, this will be like the older one until it reaches the CSP Base Station. From that point, the new slice will extend to the edge server of the 3rd party infrastructure. From the CDN perspective, the 3rd party edge server will look like a new server where it can provide its content. For example, the content that is associated with the new slice instance will be cached on the third-party infrastructure and will be delivered to the users that are connected to the 3rd party Base Station.
Stakeholders involved	• CSP (network operator) • VNF vendors • 3rd party infrastructure provider • CDN/OTT service provider • End User

Procedure/ workflow



1 Monitoring/ Imminent overloading detection

2 CSP informs & asks CDN what to do. CDN consents for network extension

3 Looks for a 3rd party infrastructure provider (Resource Discovery & Broker Logic)

4 Selects a 3rd party provider based on CSP criteria (3rd party resource selection service)

5 Requirement definition & smart contract establishment (Smart Contract Management Service)

6 Connection of 2 parties

7 Processes relate to spectrum sharing

8 a Creation of a new slice with the inclusion of 3rd party resources (Slice Orchestration and Management)
b Inform the CDN about the new node

9 a UE tries to connect to CSP BS
b Load balancing module asks UE to connect to 3rd party BS
c UE connects to 3rd party BS

10 UE logins to CDN service & gets content

2.2.2 Requirements

Changes reported in the previous Sections for use case 1 and use case 2 have introduced some updates in requirements when compared with D2.1.

Only changed requirements are reported in Table 2-5 and in Table 2-6, below.

Table 2-5: Use case 2 requirement's list

ID	Type	Unique name/title	Requirement Priority	Domain	Description	Rationale (justification)	Related KPIs
UC2.3	User	Regulator Certification	MUST	Security	The regulator needs to have a certificate that allows its identification, necessary to apply the special rights to generate Spectokens	Regulator authority has special rights, i.e., to generate the spectrum certificates to allow spectrum resource providers to generate Spectokens. Its identity needs to be identifiable	Only with the certificate a certain set of actions are allowed, e.g., creating spectrum certificates.
UC2.9	System - Functional	5GZORRO NB API	MUST	Spectrum / Smart Contracts	The 5GZORRO platform needs to expose an API towards the DLT, so that any configuration determined in the smart contract can be applied on the radio infrastructure and a "slice" can be generated (see requirement UC2.11).	Radio configuration and "spectrum enforcement" are necessary to apply the requested configuration of the spectrum	A set of API calls can be executed from the 5GZORRO platform towards the DLT to obtain information about active smart contracts.

ID	Type	Unique name/title	Requirement Priority	Domain	Description	Rationale (justification)	Related KPIs
UC2.13	System - Functional	Support for Oracles	MUST	Spectrum / SLA management	In case we need to gather spectrum usage reports from external reporting tools, Oracles need to be supported. The oracle must resolve the spectrum offer verification claim by checking with the spectrum certificate (see Section 3.2). In case we need to gather spectrum usage reports from external reporting tools, Oracles also need to be supported. The underlying programmable DLT to be deployed must allow for the deployment of Oracles, so off-chain data can be retrieved by different smart contracts,	Oracles are required to support UC2.5. In case the spectrum usage is monitored by external tools, we will need Oracles to be able to communicate the readings to our system. In this scenario, Oracles may be required to support UC2.12 and 2.13 requirements related to spectrum usage and penalties enforcement, if such are not used correctly (transmission power above legal threshold and usage of such in unauthorised location)	An Oracle can be deployed to 1) validate the generation of Spectokens by checking the spectrum certificate of the spectrum provider; and 2) monitor the spectrum usage in the infrastructure of a third-party resource provider.
UC2.15	Business	Marketplace control	MUST	Marketplace	Only a spectrum provider with the certificate granted by the Regulator (5GZORRO stakeholder), can control and issue tokens into the market, controlling the supply in circulation.	The regulator decides who has the right to control the tokens are available on the market.	Stakeholders that don't have the regulator's certificate don't have access to the Spectoken creation.
UC2.16	Business	Marketplace control	MUST	Marketplace / Security	Only a spectrum provider with the certificate granted by the Regulator (5GZORRO stakeholder), can define what the different tokens represent (bandwidth, location where such spectrum can be used, maximum allowed transmission power and period of time).	Each Spectoken is defined by a set of parameters and these can only be set by the spectrum provider with the certificate granted by the regulator.	Stakeholders that don't have the regulator's certificate don't have access to the Spectoken management.

Table 2-6: Use case 3 requirement’s list

ID	Type	Unique name/title	Requirement Priority	Domain	Description	Rationale (justification)	Related KPIs
UC3.5	System-functional	Register (CDN) resources	MUST	Edge/Core cloud Distributed Ledgers	The CDN/OTT providers MUST be able to register resources (VNFs) such as streaming servers and content storage, to the resource and service catalogue	The resource and service catalogue will be used to share the VNFs between the different entities. The CDN needs to somehow share the VNFs that will compose the slice for the CDN delivery, to be spawned in the different resource providers. In other words, the VNFs must be exposed in the catalogue, but it won’t be publicly available. Only the 3rd party will be able to view and access it.	Particularly, the CSP temporarily stores the VNFs into the resource and service catalogue, so that the CSP may set them up into a selected 3rd party infrastructure provider. may set them up into its domain. Once this is completed, the CSP can remove the VNFs from the catalogue.
UC3.8	System-functional	Observable resource usage	MUST	Data Lakes	Traffic and resource usage MUST be observable (i.e., monitorable) at the edge server level	The CSP monitors its resource usage sends monitoring data to the Intelligent SLA Breach Prediction in order to predict a potential resource saturation.	(OBJ-1, Quantified target 1) 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).

ID	Type	Unique name/title	Requirement Priority	Domain	Description	Rationale (justification)	Related KPIs
UC3.10	System-functional	Excessive usage notification	MUST	Orchestration	Excessive usage of resources according to the current/valid SLA MUST be evaluated by the Intelligent SLA Breach Prediction	The CSP must have the option to decide what may happen in case new resources seem to be needed regarding the SLA established with the CDN.	In case that the CSP needs additional resources for the SLA fulfilment, it must proceed with the resource allocation, expanding either on its infrastructure or expand on 3rd party resources.
UC3.15	System-functional	Define requirements in Smart Contracts	MUST	Distributed Ledgers	The CSP MUST define requirements towards the 3rd party provider in a Smart Contract	The best way to establish the final SLA agreement between the CSP and the 3rd party is through a Smart Contract. Smart Contracts are preferred for these kinds of agreements as they facilitate the automatic and secure transactions of DLT assets.	(OBJ-3, Quantified target 1) 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

2.3 Updates to the High-level Reference Architecture

The 5GZORRO High Level reference architecture is depicted in Figure 2-3 and has not suffered any major update from the initial version reported in D2.2 [2]. It is still comprised by the same four major logical layers grouping different functionality types. Only the DLT Network used by Security and Trust Functions was renamed to "Identity and Trust DLT Network" to better express its role in the 5GZORRO architecture when compared with the "Marketplace DLT Network" used by the Resource/Service Trading Functions.

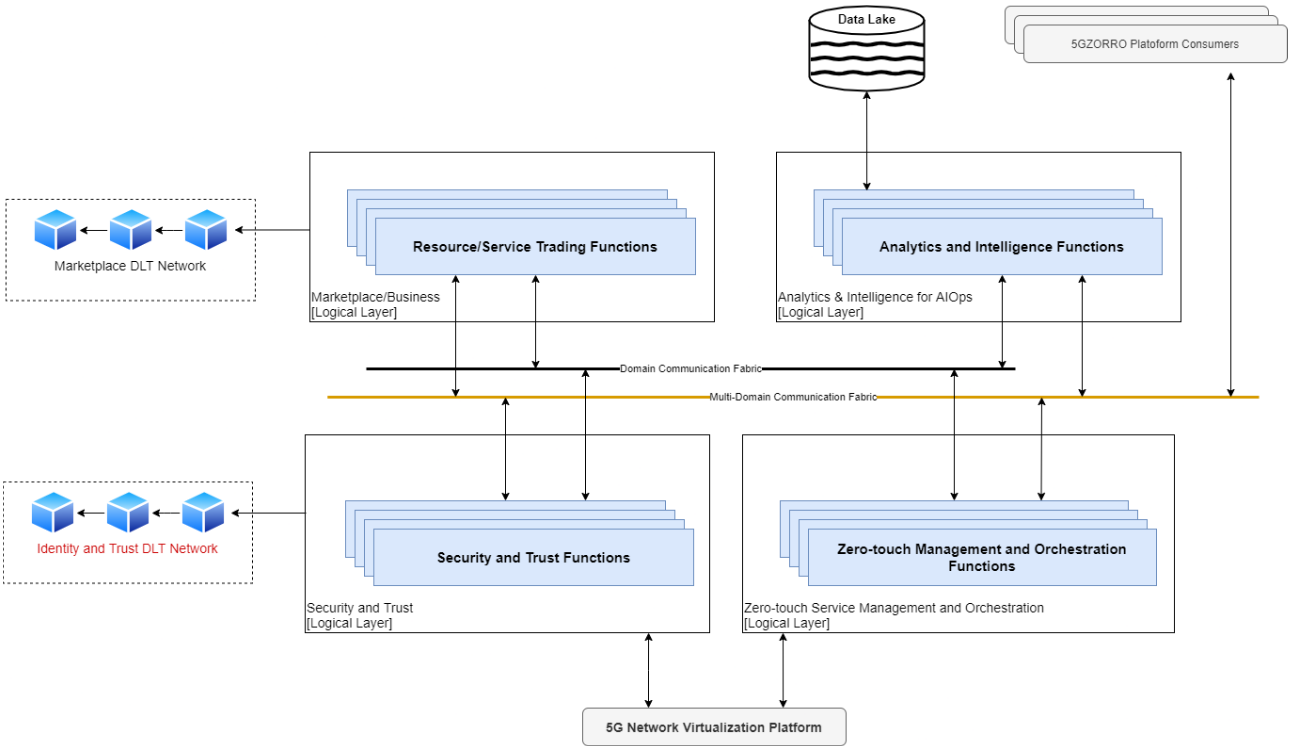

Data Lake
5GZORRO Platoform Consumers
Marketplace DLT Network
Resource/Service Trading Functions
Marketplace/Business
[Logical Layer]
Analytics and Intelligence Functions
Analytics & Intelligence for AIOps
[Logical Layer]
Domain Communication Fabric
Multi-Domain Communication Fabric
Identity and Trust DLT Network
Security and Trust Functions
Security and Trust
[Logical Layer]
Zero-touch Management and Orchestration Functions
Zero-touch Service Management and Orchestration
[Logical Layer]
5G Network Virtualization Platform

Figure 2-3: High Level 5GZORRO reference architecture

In each logical layer, a few functionalities have changed. These changes are highlighted in red, in the different figures introduced below, where functional elements populating each layer are depicted.

The **Zero Touch Management and Orchestration** layer (see Figure 2-4) provides the required functionalities to control the 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. The main change in this logical layer is the introduction of a new abstract functional element (Abstract Resource Management and Control) 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 is a new type of 5GZORRO functional block to address Spectoken related requirements coming from Use Case 2 (see Table 2-5). The main rationale for this change is to improve the comprehension of 5GZORRO Architecture as the initial design was not well perceived by the implementation teams. It would also potentially improve 5GZORRO platform extensibility to support new types of 5G resources.

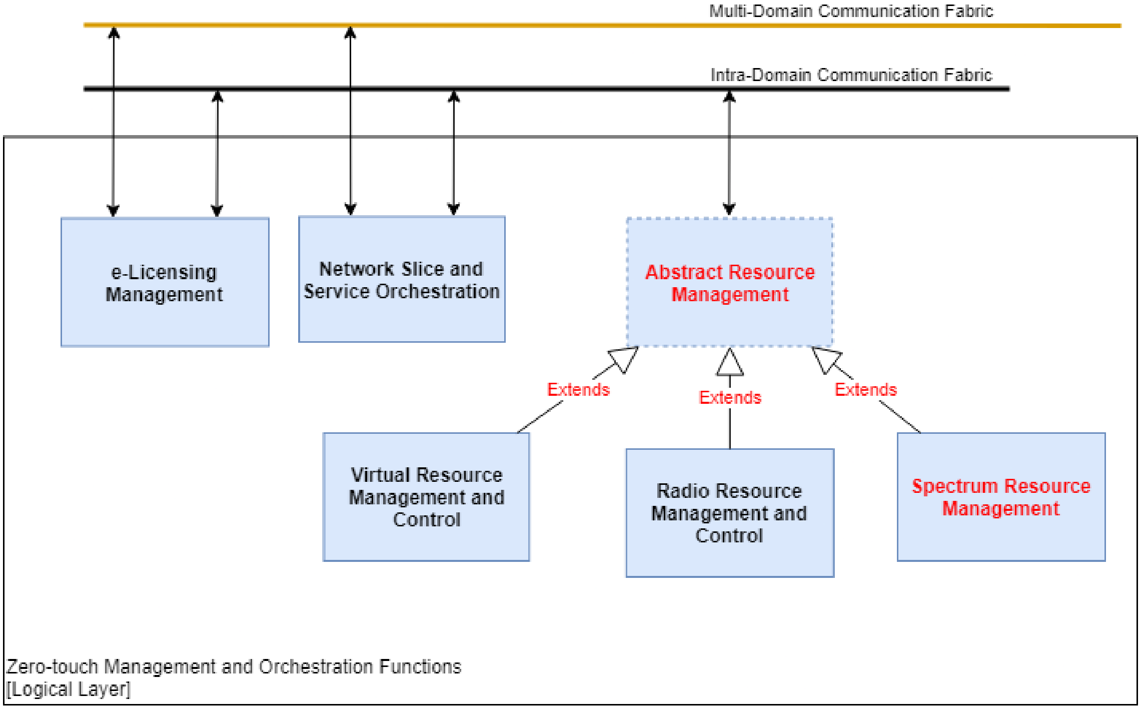

Multi-Domain Communication Fabric
Intra-Domain Communication Fabric
e-Licensing Management
Network Slice and Service Orchestration
Abstract Resource Management
Extends
Extends
Extends
Virtual Resource Management and Control
Radio Resource Management and Control
Spectrum Resource Management
Zero-touch Management and Orchestration Functions [Logical Layer]

Figure 2-4: Functional Elements populating the Zero Touch and Orchestration layer

The **Security and Trust layer** (see Figure 2-5) provides a generic framework to administrate the trust and security evaluation of internal entities and resources, and the ones from other stakeholders. Since multiple tasks are expected under security and trust scope in a multi-domain and multi-stakeholder scenario, the previous Trust & Security layer has been updated from D2.2. In particular, the 5GZORRO Security and Trust layer entail complicated and modular tasks owing to the number of fronts to be enveloped (see Figure 2-5). In this vein, the Security and Trust layer expects to guarantee 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 will secure the communication between multiple domains as well as exchanged information. Furthermore, the 5GZORRO Security and Trust layer aims to ensure an end-to-end trustworthiness establishment among different stakeholders based on previous experiences and recommendations. Hence, the trust management framework will make 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 layer is the choice of ensuring secure computation of critical tasks, guaranteeing security, reliability, and privacy-preserving. Finally, the Security and Trust layer 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 DLT technologies. It supports the creation, verification, and revocation of certificates as well as authentication and authorisation of identities across 5GZORRO domains.

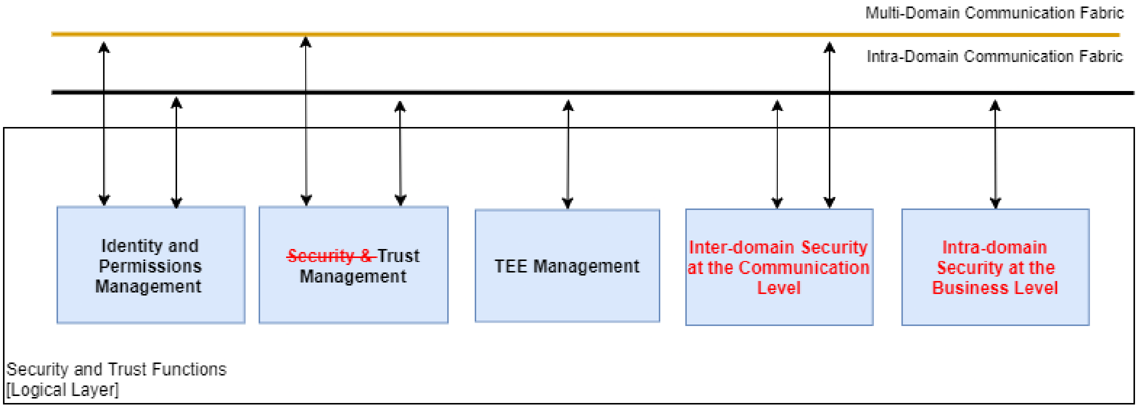

Multi-Domain Communication Fabric
Intra-Domain Communication Fabric
Identity and Permissions Management
~~Security &~~ Trust Management
TEE Management
Inter-domain Security at the Communication Level
Intra-domain Security at the Business Level
Security and Trust Functions [Logical Layer]

Figure 2-5: Functional Elements populating the Security and Trust layer

The **Marketplace and Business layer** (see Figure 2-6) enables the trading of 5G resources (including radio and spectrum resources) across different domains by using DLT Smart Contracts. In this logical layer, only the Smart Resource and Service discovery functional block was moved to the Analytics and Intelligence layer to enable the convergence of all related intelligence discovery functionalities into a single functional block.

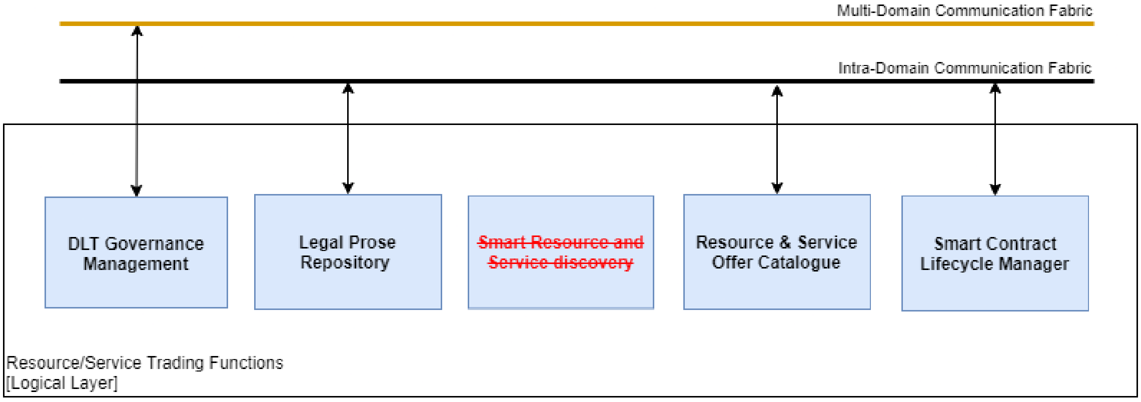

Multi-Domain Communication Fabric
Intra-Domain Communication Fabric
DLT Governance Management
Legal Prose Repository
~~Smart Resource and Service discovery~~
Resource & Service Offer Catalogue
Smart Contract Lifecycle Manager
Resource/Service Trading Functions [Logical Layer]

Figure 2-6: Functional Elements populating the Marketplace and Business layer

The **Analytics & Intelligence for AIOps** (see Figure 2-7) layer leverages Data Lake and AI technologies to provide data persistence, data share and data analytics, across 5GZORRO framework within and across domains. In this layer two major changes are reported:

- The convergence of SLA monitoring intelligence related functionalities in a single functional block by partially merging "Service & Resource Monitoring" into "Intelligent SLA breach predictor" but having the Monitoring Data Aggregation (MDA) functionalities separated into a new Functional Block. This separation allows having the right workflow, where MDA aggregates monitoring data prior to send it to the Data Lake while the SLA breach Prediction functionalities gets data from the Data Lake.
- The convergence of all related intelligence discovery functionalities into a single functional block by merging the “Smart Resource and Service discovery” coming from “Marketing and Business layer” into former “Intelligent third-party resource selection” functional block.

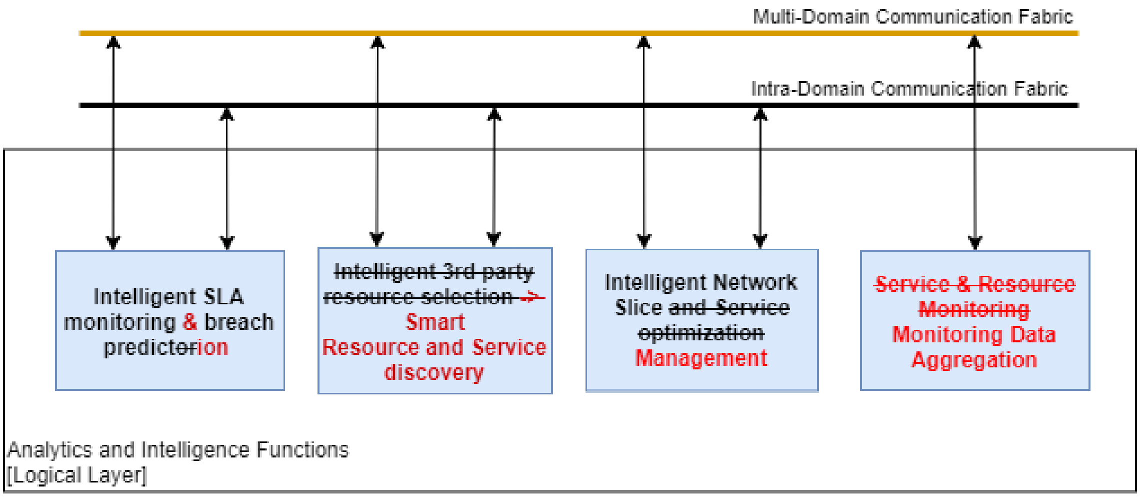

Multi-Domain Communication Fabric
Intra-Domain Communication Fabric
Intelligent SLA monitoring & breach predict~~or~~ion
~~Intelligent 3rd party resource selection ->~~ Smart Resource and Service discovery
Intelligent Network Slice ~~and Service optimization~~ Management
~~Service & Resource Monitoring~~ Monitoring Data Aggregation
Analytics and Intelligence Functions
[Logical Layer]

Figure 2-7: Functional Elements populating Analytics & Intelligence for AIOps layer

The **Communication Fabric** provides all the required functionalities to support the communication and interoperation across 5GZORRO framework in a loosely coupled way, within or across domains. No changes are reported for the **Communication Fabric** functionalities.

2.4 Functional blocks

Reviews of major changes for each 5GZORRO Functional Block, are provided in the following Sections.

2.4.1 DLT Governance Management

The 5GZORRO marketplace is subject to a governance model that is realised and enforced through this module. Underpinned by the Identity & Trust DLT and working closely with Identity and Permissions Management module, this functional block encapsulates the following functionalities:

- Processing of governance proposals relating to
  - Stakeholder onboarding
  - Legal Prose Template creation/revocation
  - Marketplace dispute resolution
- Verifiable Credential Issuance (according to governance voting) for Marketplace entities & resources
- Proposal voting by Governance Admins / Regulators via a Governance Portal
- Applying the agreed governance model business logic over all issued credentials

No major change is applied to specification in Deliverable D2.2 [2].

2.4.2 Resource & Service Offer Catalogue

The Resource & Service Offer Catalogue stores the available offers to be shared 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 and can be purchased by means of product orders.

In overall, the Resource & Service Offer Catalogue allows 5GZORRO stakeholders the following capabilities:

- Management of resource and service specifications
- Management of product offers
- Filtering of product offers
- Management of product orders

The Resource & Service Offer Catalogue provides these capabilities, while ensuring an up-to-date data storage among the distributed instances conforming the multi-party deployment scenario of the 5GZORRO platform.

No major change is applied to specification in Deliverable D2.2 [2].

2.4.3 Legal Prose Repository

The Legal Prose Repository's principal objective is to provide a set of approved templates for commercial agreements, SLAs, and licensing terms. It enables Marketplace stakeholders to propose the creation or revocation of legal prose templates. Following an approval process, templates are made available to all Marketplace Resource/Service providers for the purposes of defining terms (Agreements/SLAs/Licensing), which can later be associated with product offers published to the Catalogue. Approval is subject to the governance model imposed by the DLT Governance Management functional block, allowing administrators of the platform to review and approve/reject any proposed template.

The Legal Prose Repository itself therefore encapsulates the following capabilities:

- Propose New Legal Prose Template
- Query Templates
- Propose Legal Prose Template Revocation
- Approve/Reject template proposal based on governance decision

No major change is applied to specification in Deliverable D2.2 [2].

2.4.4 Smart Resource and Service discovery

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 [7] principles, this module leverages ML/AI techniques to allow the discovery of product offers that best satisfy the consumer needs.

In overall, the Smart Resource and Service Discovery allows 5GZORRO stakeholders the following capabilities:

- Classification of available product offers (based on pre-computed clusters)
- Intent-based discovery of available product offers
- Scoring of discovered offers based on ranking algorithms and the given intents

With respect to D2.2 [2], the Smart Resource and Service Discovery currently provides additional interfaces for 1) classifying product offers received from the Resource and Service Offer Catalogue functional block (Section 2.4.2) and 2) providing the discovered resource and service offers to further 5GZORRO functional blocks, such as the Intelligent Service and Slice Management (Section 2.4.16).

Additionally, the Smart Resource and Service Discovery also includes the Intelligent 3rd party resource selection functional block of D2.2, which is based on the scores for the discovered offers. Specifically, the Intelligent Service and Slice Management can invoke the Smart Resource and Service Discovery with given user intent to select the resource that matches the intent with the highest score.

2.4.5 Smart Contracts Lifecycle Management

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.

The Smart Contract Lifecycle Management core responsibilities are:

- Management of Agreement definition*
- Management of SLA definition *
- Deployment and tracking lifecycle events of the following:
    - Product Offers
    - Product Orders
    - Licensing Actions
    - SLA Violations

*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.

No major change is applied to specification in Deliverable D2.2 [2].

2.4.6 Identity Management and Permissions Management

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.

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 Decentralised Identifiers (DIDs) [10], DID Documents securely providing entities metadata (including entities cryptographic metadata like public keys), and Verifiable Credentials [11], and finally, a granular control access mechanism that standardises authorised access to data, resources, and services.

A major change from the initial functional specification in D2.2 [2] is the way how the Identity Management and Permissions Management functionalities are distributed across different domains in DID Agent Functionalities, securely communicating among each other by using P2P DID Communication protocols [12] and performing different DID Roles according to the role played by the 5GZORRO Stakeholder (see Figure 2-8). Each DID Agent holds an Identity and Trust DLT Wallet as described in Section 2.4.22. There are three main types of DID Agents:

Admin Issuer DID Agents have functionalities to issue Verifiable Credentials associated with 5GZORRO Entities including Stakeholders Credentials and Marketplace Offers Credentials. These functionalities are operated by 5GZORRO stakeholders playing the role of Governance administrator or the Regulator Authority i.e., stakeholders that are part of the 5GZORRO Administration Governance Board.

Holder DID Agents communicate with Admin Agents to request the issue of Verifiable Credentials. Issued credentials are stored and maintained by the Holder DID Agent. These functionalities are operated by 5GZORRO stakeholders playing the role of **Service Provider** or **Resource Provider.**

Verifier DID Agents communicate with Holder DID Agents to request presentation proof of Verifiable Credentials. These functionalities are operated by 5GZORRO stakeholders playing the role of **Service Consumer**, **Resource Consumer** or **Data Lake Operator.**

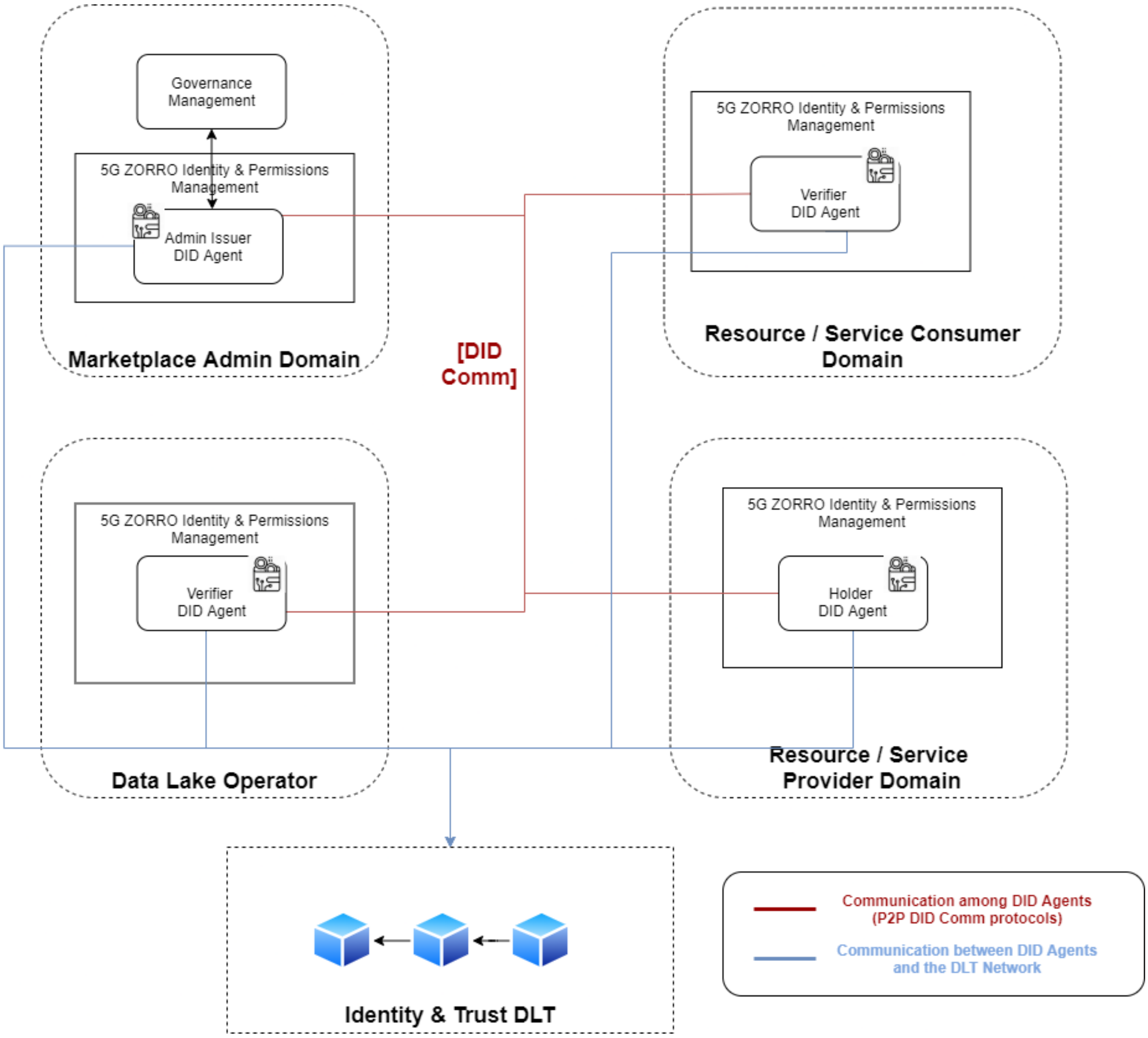

Governance Management
5G ZORRO Identity & Permissions Management
Admin Issuer DID Agent
Marketplace Admin Domain
5G ZORRO Identity & Permissions Management
Verifier DID Agent
Resource / Service Consumer Domain
[DID Comm]
5G ZORRO Identity & Permissions Management
Verifier DID Agent
Data Lake Operator
5G ZORRO Identity & Permissions Management
Holder DID Agent
Resource / Service Provider Domain
Identity & Trust DLT
Communication among DID Agents (P2P DID Comm protocols)
Communication between DID Agents and the DLT Network

Figure 2-8: Identity & Permissions DID Agents distributed among different 5GZORRO domains

2.4.7 Trust Management Framework

This Section encompasses the design, implementation, and validation of the required Trust Management Framework to incorporate an end-to-end establishment for 5GZORRO multi-tenant environments based on trust and reputation. In the 5GZORRO platform, the principal functionality of this framework is to handle the trust evaluation lifecycle of relationships between multiple 5GZORRO entities. Since the Trust Management Framework has been thoroughly explained in Deliverable 4.1 [4], we are not going to reintroduce many technical details but highlight the novel capabilities from Deliverable 2.2 [2].

Figure 2-9 depicts the four phases of 5GZORRO Trust Management Framework. 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 2-9, there are three principal interfaces that may be employed by the Trust Management Framework to gather trust information: The Data Lake platform, the Monitoring analytics, and the Security Management service. 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 set of Machine Learning (ML) and Deep Learning (DL) algorithms which may be utilized to determine stakeholder's trust score. Nevertheless, such algorithms are only ones of the most well-known and accurate techniques in the trust model literature, and they should be validated in subsequent deployment phases. On another hand, this module should withstand conventional trust model attacks such as collusion 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, policies, etc.,) since trust is considered as a long-term process, and in consequence, it is paramount to keep track over time. Regarding trust result 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, SLA violations, 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.

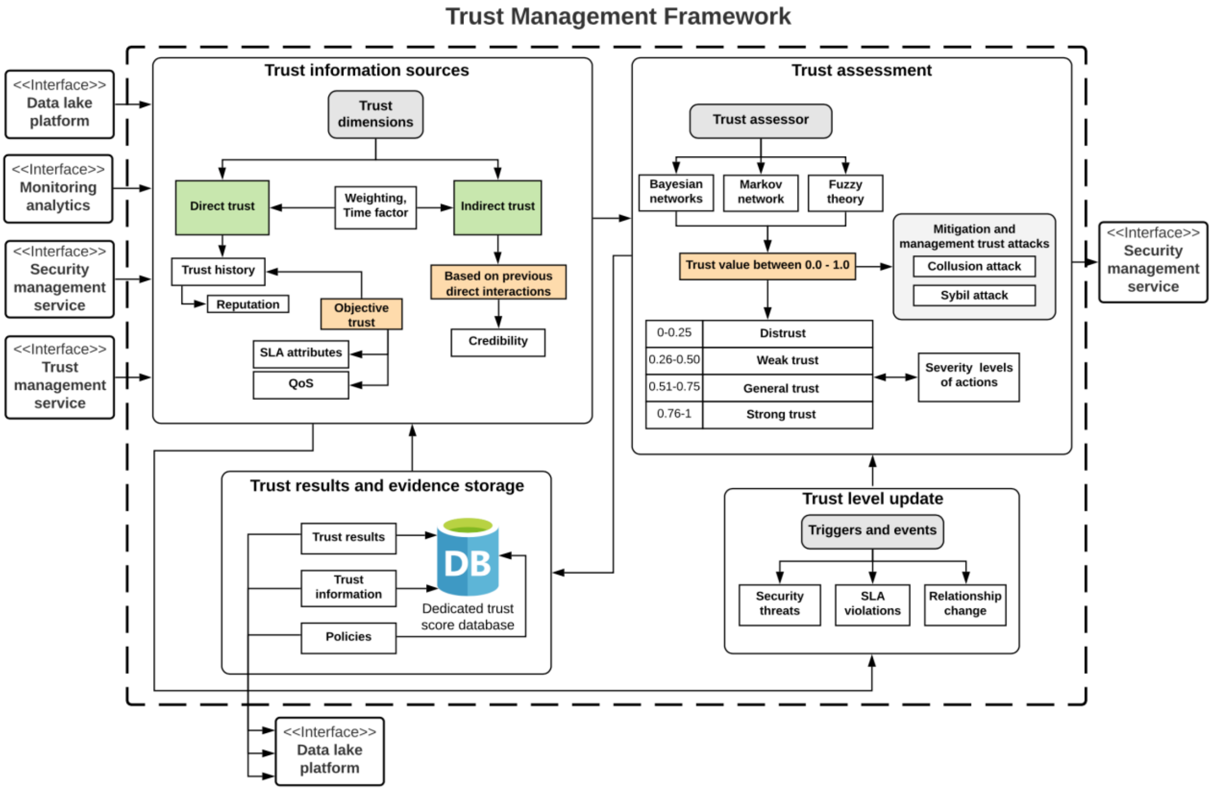

Trust Management Framework
<<Interface>> Data lake platform
<<Interface>> Monitoring analytics
<<Interface>> Security management service
<<Interface>> Trust management service
Trust information sources
Trust dimensions
Direct trust
Weighting, Time factor
Indirect trust
Trust history
Reputation
Objective trust
Based on previous direct interactions
Credibility
SLA attributes
QoS
Trust assessment
Trust assessor
Bayesian networks
Markov network
Fuzzy theory
Mitigation and management trust attacks
Collusion attack
Sybil attack
Trust value between 0.0 - 1.0
0-0.25
Distrust
0.26-0.50
Weak trust
0.51-0.75
General trust
0.76-1
Strong trust
Severity levels of actions
<<Interface>> Security management service
Trust results and evidence storage
Trust results
Trust information
Policies
DB
Dedicated trust score database
Trust level update
Triggers and events
Security threats
SLA violations
Relationship change
<<Interface>> Data lake platform

Figure 2-9: Trust Management Framework architecture

2.4.8 Trusted Execution Environment Management

With a focus on SCONE framework to enable TEE capabilities, 5GZORRO has adopted a hardware-based TEE approach, specifically Intel's SGX, as reported in D2.2 [2]. Furthermore, from a design perspective, the set of APIs defined for the Trusted Execution Environment Management service, as reported in D2.2, has been dropped in favour of a more robust, reliable, and already available set of APIs which are exposed by the SCONE framework (and reported previously in D4.1 [4]). When it comes to the instantiation of applications which are ready to be used in a TEE (Intel SGX), this functionality has not altered, but it is now offered following the Cloud Native way, meaning that such services need only to be instantiated using Kubernetes or Docker, with SCONE abstracting the interface within Intel SGX, thus not requiring the definition of specific APIs. Thus, from a design perspective, the interface with other components has not changed, and neither did the high-level functional capabilities.

With the SCONE framework allowing for secure and trusted instantiation of container-based services in a TEE environment, it has been recently determined its ability to work in an OpenStack and Kubernetes environment. Figure 2-10 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.

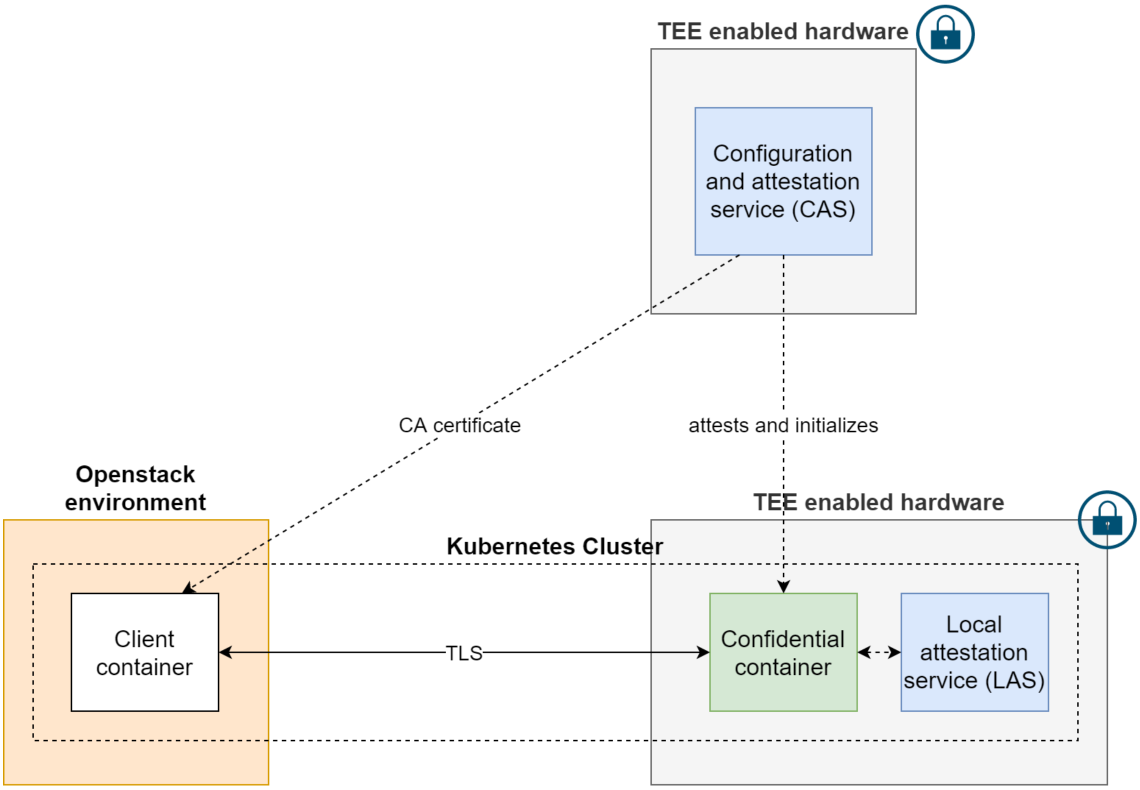


Figure 2-10: TEE cluster in an OpenStack and Kubernetes environment

The architecture is expected to enhance 5GZORRO's ability not just to run 5GZORRO core components in a TEE environment (such as the SLA Monitoring service, as well as the Monitoring Data Aggregation), but most importantly, the ability to offer Consumers with the ability to instantiate services in a pool of resources which may be, by nature, untrusted. The CAS component, made available by SCONE, will also be a new module that shall encompass the set of 5GZORRO core services. A single and centralised instance of such component will be enough to power all subsequent TEE-powered NFVI for attestation and configuration purposes (specific functionality already detailed in previous D4.1).

Once the integration process is complete, the overarching goal is to allow Resource Providers to onboard trusted hardware on to the Marketplace, allowing Resource Consumers to then exploit such resources by instantiating services in this new domain of trusted resources – an environment upon which, regardless of the provider's reputation, services will be running in a secure enclave with everything encrypted both in transit and during runtime (not even users with access to the OS will be able to inspect such container-based services) leveraging underlying SGX technology and cryptography involved.

2.4.9 Intra-domain Security at the Business Level

This functional block emerges from the subdivision performed over the previous Trust & Security Management. It aims to provide the security services in charge of detecting possible vulnerabilities and attacks inside each domain and apply the required countermeasures to mitigate them. 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 will collect internal resource and service metrics (such as network communications, resource usage, etc.) and apply ML/DL techniques to detect the attacks and mitigate them before they significantly affect infrastructure.

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.

The services provided by the inter-domain security module are described in Table 2-7.

Table 2-7: Definition of Intra-domain Security service (per-domain level)

Service name**: Intra-domain security**			Type: ***Per-domain***
Capabilities	**Support (O|M)**	**Description**	
Start network infrastructure monitoring	**M**	This capability enables monitoring of the network traffic for different 5G infrastructure segments (i.e., core, RAN, MEC) through a virtual SPAN port configuration.	
Stop network infrastructure monitoring	**M**	This capability disables monitoring of the network traffic for different 5G infrastructure segments (i.e., core, RAN, MEC).	
Start platform monitoring	**M**	This capability enables monitoring of the network traffic that is exchanged by the 5GZORRO modules through the Communication fabric.	
Stop platform monitoring	**M**	This capability disables monitoring of the network traffic that is exchanged by the 5GZORRO modules through the Communication fabric.	
Get monitored interfaces	**M**	This capability allows to obtain the list of active monitoring interfaces.	
Get monitoring data	**M**	This capability allows to obtain diagnostics, logs and Packet Capture (PCAP) files from monitored interfaces.	
Set monitoring submodules	**M**	This capability sets the submodules of the Intra-domain security service that are used for detection of anomalies.	
Notes			
none			

2.4.10 Inter-domain Security at the Communication Level

This functional block emerges from the subdivision performed over the previous Trust & Security Management. It aims to provide the capabilities for generating secure point to point 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) functionalities (see Section 2.4.6) 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. Besides, for the key distribution process and the authentication between VPN instances, the Id&P framework is leveraged, taking advantage of its DLT-based security features.

The services provided by the inter-domain security module are described in Table 2-8:

Table 2-8: Definition of Inter-domain Security service (per-domain level)

Service name: **Inter-domain security establishment**		Type: ***Per-domain & 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.
Connect VPN	**M**	This capability enables to launch a secure communication between two stakeholders through a tunnel.
Disconnect VPN	**M**	This capability enables to finish a previous connection.
Notes		
none		

2.4.11 Communication Fabrics

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. No major changes here since WP3 and WP4 have not addressed yet this functional block. Currently, each module is implementing its own communication solution according to available technologies. See D2.2 [2] for the detailed description of this functional block.

2.4.12 Network Slice and Service Orchestration

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, to provide the associated communication services. No major changes here. See D2.2 [2] for the detailed description of this functional block.

2.4.13 e-Licensing 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, involving the operators and communication providers. Vendors will onboard their products specifying in the smart contract of the offer the license conditions, negotiation goal and constraints. The design of the service is focused on control the licenses at Virtual Function (VF) level, allowing the management of the licensing regardless of the location or the domain in which the VF is running. Besides, design contemplates the possibility of controlling the licenses of a Network Service, or a Network Slice composed by VFs from different providers.

The main evolution for this functional block regarding the last report in D2.2 [2] in the logical split of the functional block in two parts:

1. e-License Manager Core (eLMC) as a single point of presence inside the 5GZORRO Platform with the objective of centralizing TX and RX communications with the NSSO and the Marketplace.
2. e-License Manager Agent (eLMA) as a distributed subsystem living closer to the Operator's domain, which oversees the monitoring of the specific VFs registered under a given agreement (referred as Product Offering according to the Marketplace catalogue).

Figure 2-11 depicts the most important interfaces regarding this system. Arrows represented by solid lines refer to REST communications while those arrows represented by dotted lines show asynchronous communications.

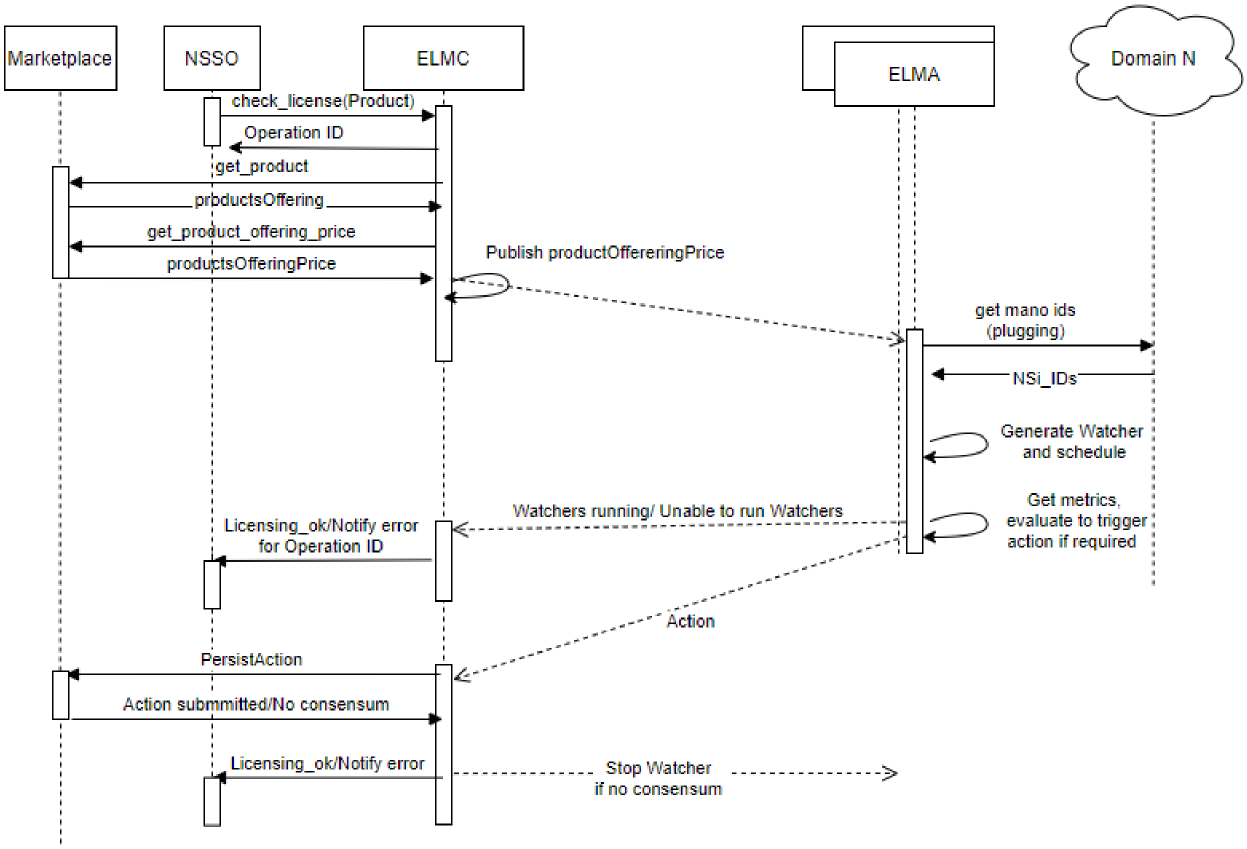

Marketplace
NSSO
ELMC
ELMA
Domain N
check_license(Product)
Operation ID
get_product
productsOffering
get_product_offering_price
productsOfferingPrice
Publish productOffereringPrice
get mano ids (plugging)
NSi_IDs
Generate Watcher and schedule
Get metrics, evaluate to trigger action if required
Watchers running/ Unable to run Watchers
Licensing_ok/Notify error for Operation ID
Action
PersistAction
Action submmitted/No consensum
Licensing_ok/Notify error
Stop Watcher if no consensum

Figure 2-11: e-Licensing Management in 5GZORRO

Looking at the eLMA sequence of events, it should be noticed how the registration of a product offering price (actual price attached to a specific property of a VF) triggers the creation of a watcher. Such watcher is a process that is customized to monitor a specific property of a running VFs inside the Operator's domain. Each eLMA is responsible for (1) the analysis of the metrics received by the watcher and (2) the evaluation of them regarding the licensing agreements registered in the product offering price object. Once this process of analysis and evaluation are performed, the eLMA decides if an action needs to be registered in the eLMC, and thus propagated to the marketplace for persist it. The eLMC has the global view of the agreements related to a certain product that may be deployed in several domains, so it is the entity responsible for performing the required actions in case of contract expiration notification.

2.4.14 Monitoring Data Aggregation

The 5GZORRO framework provides configurable service and resource monitoring as described in Section 2.4.15. The metric collection, in-Resource Owner 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 now 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 2.4.15) gets data from the Data Lake.

In a typical 5GZORRO scenario, a Resource Provider is required to enable monitoring and aggregation on behalf of a Resource Consumer when a resource is acquired from the marketplace in the context of a business transaction between Resource Provider and Resource Consumer. These transactions are managed by Intelligent Slice and Service Management (ISSM) as described in Section 2.4.16. Specifically, ISSM Workflow Management (ISSM-WFM) executes a pre-programmed business transaction flow that orchestrates and binds together multiple components of the platform which are involved in a specific transaction.

As part of this flow, ISSM-WFM passes a monitoring spec to NSSO (Section 2.4.12) when calling its NBI. This monitoring spec is derived from the resource offer as it is being published on a marketplace by the Resource Provider. The latter pre-onboards the resource descriptor with NSSO prior to publishing the resource offering on the marketplace. As part of the NSSO descriptor, monitoring specification is declared. This monitoring specification is then fully or partially reflected in a marketplace resource offer at the time of the offer publishing. It is important to stress the difference between the monitoring specification as it is reflected in the NSSO descriptor of a pre-onboarded resource and a monitoring spec of the resource offer. The latter is a proper subset of the monitoring functionality specified in the descriptor. However, more restricted monitoring capabilities can be provided by the Resource Provider when it registers a resource offer with the marketplace. The actual monitoring configuration is intimately connected to the SLA that accompanies the resource offer. Monitoring incurs costs and the Resource Provider should be capable to balance these costs with the benefits accrued through specific configurations. In general, higher granularity of monitoring will imply higher costs and therefore, higher prices.

If monitoring spec is not provided with the resource offer, a default configuration will be used by the Resource Provider as it is specified in the NSSO descriptor of the resource.

NSSO instantiates a resource and passes an instance of the monitoring spec that it receives from ISSM-WFM (which obtains it from the resource offer as described above) to MDA and activates MDA with respect to this specification. MDA annotates every data point that it publishes on the Data Lake.

Typically, the Resource Provider encrypts the data that is being published to the Data Lake with the public key of the Resource Consumer. The public key of Resource Consumer is managed by the Identity and Permissions Management (Id&P) functional block (Section 2.4.6). ISSM-WFM fetches the public key of the Resource Consumer from the Id&P and passes it to NSSO, which then passes it to the MDA. The latter uses it to encrypt the monitoring data.

2.4.15 Intelligent SLA monitoring & breach prediction

The Intelligent SLA monitoring and breach prediction functional block is part of the Analytics and Intelligence functional layer (Section 2.3). Based on D2.2 [2], it consists of two entities: 1) the SLA *Monitoring* service and 2) the *SLA Breach Prediction* service. The *SLA Monitoring* service collects, and analyses aggregated monitoring data to detect violations in SLAs, whereas the *SLA Breach Prediction* service collects, and analyses aggregated monitoring data using AI techniques to predict possible breaches in SLAs and detect anomalies. These services had no updates in terms of their functionality with respect to D2.2.

The main evolution though for the Intelligent SLA monitoring and breach prediction functional block with respect to D2.2 lies in its interactions with the other functional blocks of the 5GZORRO architecture, as shown in Figure 2-12. Specifically, it is currently placed within a closed-loop architecture that complies with the ETSI ZSM initiative [8]. Hence, it initially receives the details (id, name, description, metric, threshold) of a certain SLA, thus triggering the creation of a new ML operation, whose first step is to read the monitored metrics from the Data Lake (Section 2.4.23) and the Service and Resource Monitoring functional blocks (Section 2.4.14). These metrics are generated by the Virtual Resource Manager and passed to the Data Lake. Then, the Intelligent SLA monitoring and breach prediction block uses AI/ML techniques on the monitored metrics to provide service assurance by predicting violations of the metric threshold defined in the SLAs. Upon the prediction of SLA violations, notifications or alerts are generated, to be provided to the Intelligent Slice and Service Management functional block (Section 2.4.16). This block will assess the current operational status and decide how to handle detected or forecasted issues and anomalies. Finally, the Network Slice and Service Orchestration functional block (Section 2.4.12) is invoked to actuate the decision and thus act upon the managed resources and services.

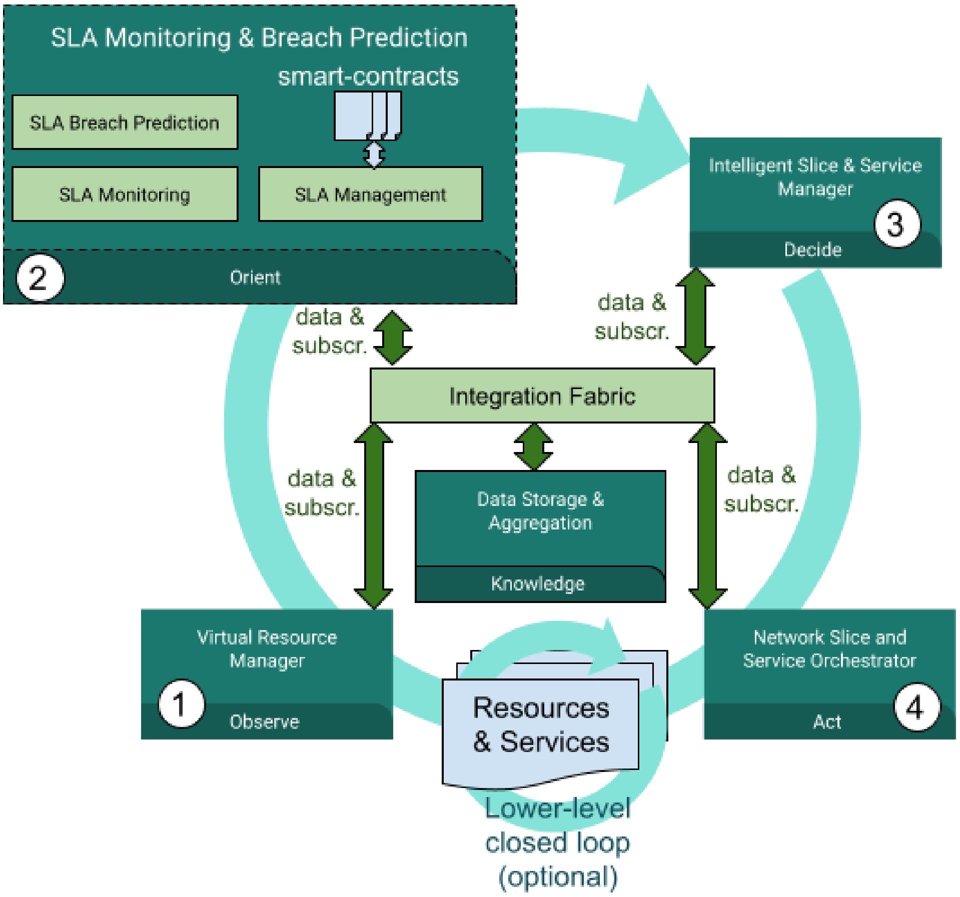


Figure 2-12: SLA Closed-Loop Architecture

The interactions between functional blocks in the closed-loop architecture are facilitated through the event-based, asynchronous interactions through the Multi-domain Communication Fabric (Section 2.4.11), which exposes data publication and subscription services, as well as services for the installation of data pipelines.

2.4.16 Intelligent Slice and Service Management

The 5GZORRO Intelligent and Automated Slice and Service Management (ISSM) functional block focuses on automated management of secured cross-domain slices and services within them.

ISSM is thus responsible for enforcing business transactions both at the system level by interacting with NSSO with alternative slicing technologies that might be developed in the future, as well as by managing business transaction contexts across the entire 5GZORRO platform allowing a principled, repeatable, auditable, and trustworthy interaction among the multiple components of the platform to realize a specific business flow.

One of the main problems faced by CSPs engaging in cross-domain collaboration is the lack of standards governing these interactions. On top of that, each CSP needs to protect its business and technical autonomy, so that it can execute its unique business processes while using its preferred technical tools. This situation is unlikely to change and therefore an “orchestrator-of-orchestrators” approach is not likely to succeed for cross-domain slice and service management, because it would lock CSPs in specific paradigms and stiffen the much-needed ability for fast innovation in cross-domain collaboration.

Our approach is instead to use a cloud-native portable orchestration mechanism that can be programmed without tying into a specific orchestration technology. To that end we use Cloud Native Foundation (CNCF) events and workflow management projects that offer Kubernetes native development and deployment of intelligent slice and services orchestration flows where events and flows are defined as Custom Resource (CR) instances of their respective Custom Resource Definitions (CRD), which seamlessly extend the Kubernetes ecosystem and therefore are fully portable. In summary, we propose using a least common denominator cloud native orchestration mechanism that allows to develop and onboard 5GZORRO platform-specific events and flows as if these events and flows were Kubernetes applications. The software component architecture aspects of this approach are described in detail in D4.1 [4]. In this deliverable, we will focus on the aspects of the functional architecture.

ISSM is responsible for the optimization of resource allocation to inter-domain slices subject to SLAs and cost-efficiency targets. Since D2.2 [2], the main architectural decisions have been twofold. First, we decided to cleanly separate between business and technical level orchestration concerns. Second, we decided to partition ISSM’s functionality into smaller components with well-defined scope to facilitate independent development of different functional areas and ensure better sustainability and exploitability of the assets through pluggable architecture.

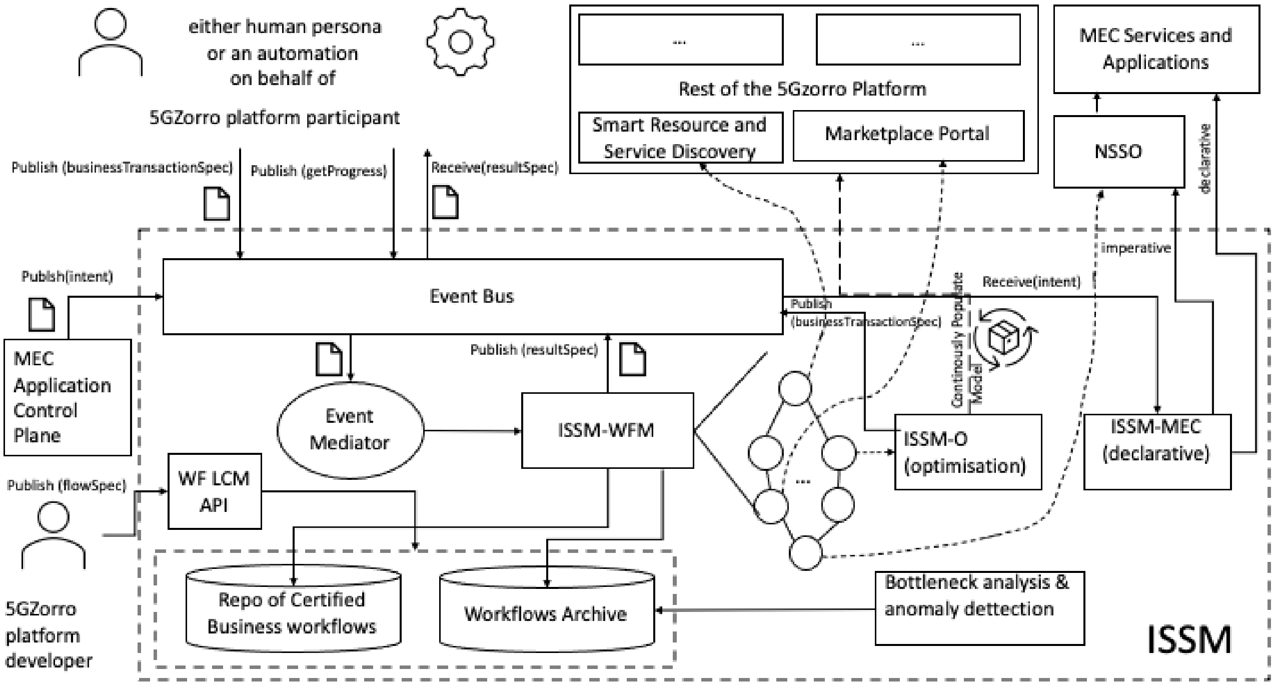

either human persona
or an automation
on behalf of
5GZorro platform participant
...
...
Rest of the 5Gzorro Platform
Smart Resource and Service Discovery
Marketplace Portal
MEC Services and Applications
NSSO
declarative
imperative
Publish (businessTransactionSpec)
Publish (getProgress)
Receive(resultSpec)
Publish(intent)
Event Bus
Publish (businessTransactionSpec)
Receive(intent)
Continuously Populate Model
MEC Application Control Plane
Publish (resultSpec)
Event Mediator
ISSM-WFM
ISSM-O (optimisation)
ISSM-MEC (declarative)
Publish (flowSpec)
WF LCM API
...
Repo of Certified Business workflows
Workflows Archive
Bottleneck analysis & anomaly dettection
5GZorro platform developer
ISSM

Figure 2-13: High Level ISSM Architecture

To that end the ISSM component comprises three main components:

- ***ISSM Workflow Manager (ISSM-WFM)***: executes orchestration workflows in a context of a business transaction, such as extending a slice across a second domain in cooperation with the Network Slice and Service Orchestration.
- ***ISSM Optimizer (ISSM-O):*** optimizes cost-efficiency trade-off of network services and slices required to be created in a context of a specific business transaction and continuously optimizes services and slices that have been already set up in previous transaction flow executions.
- ***ISSM*** and ISSM-***MEC Manager (ISSM-MEC)***: facilitates declarative cloud native style of managing applications executing in a MEC environment while collaboratively managing MEC infrastructure resources allocation and MEC services at the host and system levels, based on the intents communicated by an application control plane.

Figure 2-13 depicts a high level ISSM architecture, which blocks are further explained below.

2.4.16.1 ISSM-WFM

A CSP participating in 5GZORRO Platform publishes a business transaction specification (a declarative document) on a well-known topic of Event Bus. As an example of a business transaction consider cross-domain slice establishment (e.g., for the sake of dynamic slice scaling). An important architectural decision is made to cleanly separate between the high-level declarative intent (e.g., a GSMA NEST or plain English description) that defines a communication service in terms of bandwidth, latency, jitter, isolation level, etc., and specific resource offerings stipulating specific resource flavors. The logic of converting the high-level intents to specific resource offers is performed by the Smart Resource and Service Discovery component. All resource offers found by the Smart Resource and Service Discovery (see Section 2.4.4) represent possible candidate solutions from which ISSM-O selects resources to optimize a trade-off such as cost-efficiency.

A typical business transaction like this might be very complex and take considerable time because it spans multiple components in the 5GZORRO platform as illustrated in flows described in Section 3. Therefore, business transactions are executed asynchronously, and the transaction logic is pre-programmed by a developer of the 5GZORRO platform who is the only person who might add/remove/edit business workflows (consider Workflows in Section 3.6 and in Section 3.7, for example) when the 5GZORRO platform has to evolve to accommodate new component versions, new APIs and new orchestration flows. Thus, the ISSM-WFM provides a mechanism for sustaining the business logic of the platform into the future.

The business transaction spec is communicated to ISSM-WFM via Event Mediator. Upon receiving an event containing the business transaction spec as a payload, ISSM-WFM triggers an appropriate pre-programmed workflow from the workflow repository. A workflow is a document that defines the DAG of tasks that comprise the business workflow. In a specific business context, each task might reach out to different components of the 5GZORRO platform, such as Marketplace Portal, NSSO, Smart Resource and Service Discovery, Data Lake, etc. In the interest of conserving space and for the sake of simplicity, not all elements of the 5GZORRO platform are shown in the Figure 2-13.

The CSP who triggered the workflow, can query its progress, pause it or cancel it at any time. A 5GZORRO Platform Participant sees only those workflows that belong to it. All steps of a workflow execution are memorized and archived for future bottleneck analysis and anomaly detection.

For example, to procure resources from the marketplace, ISSM workflows interact with Smart Resource and Service Discovery Service specifying criteria (constraints) for the resources. Information obtained via this interaction is used to populate a model that is fed to ISSM-O, which performs optimisation of trade-offs involved with using specific slice and service resources discovered by Smart Resource and service Discovery.

ISSM-WMF is responsible for running a business flow of resource discovery and acquisition, the ISSM-O is responsible for the optimization of embedding these resources in the physical network substrate. Thus, ISSM-O finalizes resource selection on behest of ISSM-WFM (see Subsection 2.4.16.2).

When a workflow terminates either normally or abnormally, ISSM-WFM publishes a resultSpec document on a well-known topic of Event Bus to be consumed asynchronously by any of the involved personas in a specific business context of the workflow. To continue the above example, resource procurement workflow, after a series of resource discovery and optimization steps, results in a concrete declarative specification of service to be provisioned by the involved resource providers, e.g., network slices, network services, MEC systems, MEC application instances, etc. To accomplish this, resultSpecs created by the procurement flow are processed by ISSM-MEC and realized through interaction with the external actuators. If no MEC services or applications are involved, a shortcut is possible, in which ISSM-WFM interacts directly with an external actuator, such as NSSO.

With resources selection finalized by ISSM-O, ISSM-WFM requests instantiation of the resource offers by calling the NSSO NBI and passing it the monitoring spec as defined in subsection 2.4.14 and a filled in resource descriptor that NSSO understands. The NSSO uses product ID to instantiate the required number resources. The full resource identification is then a combination of business Transaction ID (assigned by ISSM-WFM), product ID (assigned by the marketplace), and product Instance ID (assigned by NSSO upon instantiation)

This way each resource instance is uniquely identified in the platform and the monitoring data in the Data Lake data is properly correlated to each resource instance while the concerns between the components are clean cut separated between the high-level business orchestration embodied by ISSM-WFM and technical orchestration of resources at the NSSO level.

In D4.1, we provide more details on ISSM-WFM API and software architecture involved.

2.4.16.2 ISSM-O

The goal of ISSM-O is to achieve the most cost-efficient slice or service resources allocation subject to constraints such as trust, security, and performance. Resources selected by ISSM-O are procured from the marketplace via the DLT mechanism. Since transactions are performed concurrently for multiple CSPs, a competition for resources potentially can lead to this cycle of resources discovery, optimisation, and procurement to be performed multiple times by a flow run by ISSM-WFM until either all resources required are acquired from the marketplace or – in case of repeated failures – the business transaction is aborted.

ISSM-O performs the resource optimization process in two levels. The first level of optimization happens in the cross-domain, and it is a high-level optimization. ISSM-O, as a component in the ISSM module, aims at making a cost-efficient trade-off of network services and slices required to be created in a context of a specific business transaction. The optimization process in ISSM-O performs continuously to optimise services and slices that have already been established in the previous transaction flow executions. Although we have focused on cost-efficiency aspects of the ISSM-O, it can be tuned to optimise different objectives.

ISSM-O is only accessible to ISSM-WFM and does not expose any service to other internal and external components of the 5GZORRO system. Interaction with ISSM-O is declarative Kubernetes style. The ISSM-WFM provides the ISSM-O with a set of resource offers that are acquired through the interaction with the Smart and Resource Discovery module.

Upon receiving the candidate resources by the ISSM-WFM, ISSM-O selects the most appropriate resource offers. The goal of ISSM-O is to achieve the most cost-efficient slice or service resource allocation subject to constraints such as trust, security, and performance. Resources selected by ISSM-O are procured from the Marketplace via the DLT mechanism. ISSM-O relies on the Network Slice and Service Orchestration to perform the technical side of the slice establishment or extension of slices on the involved domains.

The main architectural challenge regarding ISSM-O is making it pluggable to ensure sustainability. Since optimization problems faced by ISSM-O are NP-hard, to address a specific problem, a specialized heuristic or approximation usually is used to best exploit the problem properties. If a problem is sufficiently small and benign, it can be solved exactly by commercial-grade solvers, such as CPLEX [23] or Gurobi [24]. In other cases, methods like relaxation and rounding, column generation, etc. can be deployed.

2.4.16.3 ISSM-MEC

ISSM MEC Management (ISSM-MEC) functionality is depicted in Figure 2-14. Similarly, to ISSM-WFM, ISSM-MEC executes on a cloud native container orchestrator (Kubernetes) and exploits its extensibility through the Custom Resource Definition (CRD) mechanism to enrich Kubernetes' functionality with new APIs.

ISSM-MEC is very simple by design and acts as a universal translation layer between the rest of ISSM and the external environment specific actuators. To begin with, we plan to support two actuators: Network Slice and Service Orchestrator (NSSO) and an experimental cloud native MEC Platform (CNMP) that we plan to develop. In the future, we envision extensibility to support additional actuators.

ISSM-MEC translates the intent-based requests for instantiating/managing Services, Slices, and Edge applications into the interactions with the orchestration software (e.g., NSSO). Being part of 5GZORRO ISSM, ISSM-MEC participates in fine-grained event-driven workflow-based design of and acts as an intelligent link to NSSO and CNMP.

ISSM-MEC receives the MEC application intents through the Event Bus of ISSM.

The intents involve resource types at the edge level (compute, storage, and network), which in case of cross-domain MEC services and applications have been procured from the marketplace as part of a corresponding ISSM-WFM workflow. These services, applications and resources are instantiated via Actuators, e.g., NSSO that interacts with Points of Presence (PoP) of the edge platforms.

CNMP MEC platform is envisioned to use Kubernetes both as NFVI and control plane exploiting its declarative orchestration capabilities. ISSM-MEC dispatches declarative deployment requests to the Kubernetes based MEC platform in the form of Custom Resources (CR) that are being watched by the corresponding Controllers inside CNMP (much like ISSM-MEC Controller watches CRs that are dispatched to it by ISSM-WFM). These controllers execute logic that continuously reconciles between the *desired* state of a MEC service or application as expressed in the intent (CR) with the *observed* state. This deployment and management pattern is known as *Operator* and it is considered one of the more popular cloud-native best practices [13].

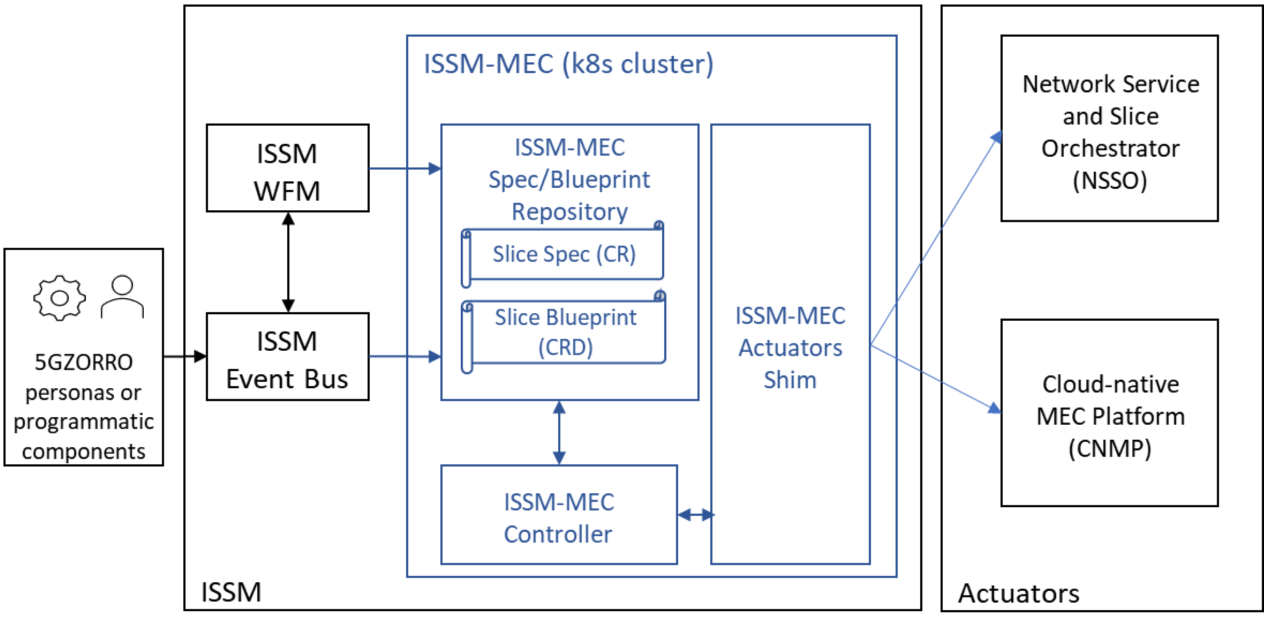

ISSM-MEC (k8s cluster)
ISSM WFM
ISSM Event Bus
5GZORRO personas or programmatic components
ISSM-MEC Spec/Blueprint Repository
Slice Spec (CR)
Slice Blueprint (CRD)
ISSM-MEC Actuators Shim
ISSM-MEC Controller
ISSM
Network Service and Slice Orchestrator (NSSO)
Cloud-native MEC Platform (CNMP)
Actuators

Figure 2-14: ISSM-MEC architecture

As part of ISSM, ISSM-MEC Management does not provide any individual service or has any associated APIs. It interacts with the rest of ISSM through the message bus and adheres to the information model for fetching/parsing messages posted there. On the Southbound Interface, ISSM-MEC is a client for the relevant APIs exposed by the actuators, namely NSSO and CNMP. In the latter case a standard interaction with Kubernetes API server is expected.

2.4.17 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 [2].

This new architecture considers the feedback received from deliverables D3.1 [3] and D4.1 [4] 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, whose initial design is reported in D4.1.

To embed this software architectural choice into the new 5GZORRO functional architecture, this new ARMC FB 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, properly specialised and extended by derived functional blocks:

- Management of resource description and specification, e.g., Descriptors, images, etc.
- Monitoring of the managed resources, in terms of performance, usage and fault statistics.

2.4.18 Virtual Resource Management and Control

With respect to the first design discussed in D2.2 [2], the Virtual Resource Management functional block has undergone some changes in the set of services offered by this module. All the declared functionalities of resource lifecycle management have been removed to avoid any overlap, as they are already covered by the 5GZORRO orchestration stack. Services like the management of software images, network management and monitoring of resource data remain under the control of the VRM.

Furthermore, the VRM functionalities have been extended in order to support the 5GZORRO Resource and Service Offer Catalogue (RSOC), with the aim of providing a service to be able to perform translations of the definitions of the Virtual resources, from technical information models e.g., ETSI SOL-006 [6] towards proper TM Forum information models, supported by the RSOC.

All these updates and extensions to the VRM functional block are reported in D4.1 [4] as part of the software design that implements it.

2.4.19 Radio Resource Management & Control

With respect to the first design discussed in D2.2 [2], the Radio Resource Management functional block has experienced some modifications with respect to the set of services formerly offered. All the declared functionalities of RAN resource lifecycle management have been removed. The Radio Resource Management simply offers a service to the 5GZORRO orchestrator to manage RAN slices (creation, modification, removal) and another service to provide RAN slice statistics to the Resource Monitoring service in the Virtual Resource Management.

The services provided by the Radio Resource Management functional block are described in Table 2-9Table 2-8:

Table 2-9: 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 slice sub-nets	**M**	Manages the RAN slice sub-nets that are deployed within the domain. The slice composition in terms of RAN resource technologies is determined by the 5GZORRO orchestrator based on the SLA and the infrastructure availability in the considered domain.
Provide RAN slice sub-net statistics	**M**	Provide regular information regarding the status of a RAN slice sub-net.
Notes		
none		

2.4.20 Spectrum Resource Management & Control

In alignment with the modular design of the resource management in 5GZORRO, with dedicated functional blocks per type of resource, it is necessary to define a Spectrum Resource Management & Control module. The spectrum Resource Management & Control functional block exposes services that are related to the provision of the technical details of the spectrum resource. The availability of the services depends on the role of the stakeholder. On the one hand, the spectrum resource management exposes two services to spectrum resource providers: a service to provide to the Marketplace with the spectrum technical details of the Spectoken; and another service to provide the utilisation status of the spectrum resources of a particular resource provider. On the other hand, the spectrum resource management exposes to spectrum resource consumers their list of acquired spectrum resources in the 5GZORRO platform. The monitoring of the spectrum use relies on external functional blocks, as the Radio Resource Management & Control or an Oracle to interface with a third-party radio infrastructure. The three services exposed by the Spectrum Resource Management & Control service are listed in Table 2-10.

Table 2-10: Definition of Spectrum Resource Management & Control service (domain level)

Service name: **Radio Resource Management & Control**		Type: ***Per-domain***
Capabilities	**Support (O|M)**	**Description**
Provide spectrum resource details	**M**	The spectrum resource provider triggers the generation of a spectrum resource offer (Spectoken) by providing the spectrum technical details (frequency ranges, area of application) in its own domain. The service will convey this information to the Service and Resource Marketplace Catalogue in its own domain to start the generation of the Spectoken as described in Section 3.2.
Get spectrum resource status	**M**	The Spectrum Resource Management & Control monitors the utilization status of the spectrum resources published in the 5GZORRO Service and Resource Marketplace Catalogue. The spectrum resource status can be available in the Catalogue, removed from the Catalogue, or in use by a third-party stakeholder.
Store spectrum resource details	**M**	The stakeholder obtains information on spectrum resources obtained in the 5GZORRO platform. This information is populated on the spectrum resource consumer domain

		every time a Spectoken is acquired, as described in Section 3.4.
Notes		
none		

2.4.21 Marketplace DLT platform

The Marketplace DLT platform encapsulates the elements giving rise to cross-domain trust, decentralisation and an immutable record of Marketplace transactions and agreements. Whilst remaining agnostic to the specific DLT implementation technology, the initial realisation of the 5GZORRO marketplace will demonstrate functionality through a Corda implementation. An abstraction layer provided by the Smart Contract Lifecycle Manager provides the integration point for other suitable DLTs to be utilised in the future. An implementation of this interface will be developed to integrate the Corda with the Marketplace.

Each identified stakeholder will deploy a DLT node and interact with it through its own Smart Contract Lifecycle Manager. Smart Contracts, contract states and flows will govern the business model, processes, and transaction finality in conjunction with Notaries (additional validating nodes deployed by Governance Admin stakeholders).

Oracles will be developed to support the necessary integration points where off-chain data or attestation is required to support DLT transactions. These oracles are:

- Governance Admin Oracle – to support verification of verifiable credential presentations for access control and permissions such as Spectrum ownership
- Resource Management Oracle – to integrate with resource managers for the purposes of confirming resource deployment/availability status

Since D2.2 [2], no major functional changes are reported.

2.4.22 Identity and Trust DLT platform

The Identity and Trust DLT platform is the key enabler to provide trusted interactions across domains by leveraging W3C Decentralised Identifiers (DIDs) [10] and associated Verifiable Credentials [11]. 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, revocation registries, issuer public keys, and so on. The Identity & Permissions Verifiers learn with certainty the 5GZORRO Governance Board have attested something by checking digital signatures against the Identity and Trust DLT Platform.

Since D2.2 [2], no major functional changes are reported for the Identity and Trust DLT Platform in this deliverable.

2.4.23 Data Lake Platform

Since D2.2 [2], the Data Lake services have been refined and narrowed down to what is needed for 5GZORRO to store and manipulate large amounts of data. The 5GZORRO Data Lake provides the following basic services.

- Data Storage, e.g., S3-compliant Object Storage such as Ceph [14] or Minio, databases, etc
- Messaging / streaming capability, e.g., Kafka [16]
- Runtime: Docker [17]
    - Container orchestrator: Kubernetes [18]
    - Serverless, e.g., Knative, FaaS, Tekton

- Workflow management tools, e.g., Argo[19]
- Event mechanisms, e.g., Argo Events

The underlying technology to allow automated deployment, scaling, and management of programs that manipulate the data is Kubernetes. As the project progresses, we anticipate that services of the Data Lake will expand to include also:

- Metadata Services
- Analytics tools, e.g., Spark, TensorFlow, Kubeflow
- Data Transformation services, e.g., Hadoop, Spark [15]

The basic interfaces provided by the Data Lake, beyond registering with the Data Lake, are to provide specifications of analytics pipelines that will run using the Data Lake infrastructure.

2.4.24 5G Network Virtualization Platform

This functional block is an abstraction that represents the set of tools in charge of control and manage the underlying virtualised infrastructure where slices and services are deployed. There are no major changes in this functional block with respect to what already discussed in D2.2 [2] and here we reported the decisions taken so far concerning the set of tools to be utilised (Given the feedbacks received from both D3.1 [3] and D4.1 [4]), as this topic has been left open in D2.2. Opensource MANO (OSM) [21] has been selected as NFVO (support to Sonata [22] is under discussion) and OpenStack [20] as VIM. Kubernetes [18] has been selected to cover the role of VIM for the Containerised Network Function (CNF) while its deployment as MANO to orchestrate cloud-native network slices is still under discussion.

3 Updated Operational flows

This chapter provides a review of the main 5GZORRO operational flows reported in D2.2 [2], by highlighting the main changes.

3.1 Stakeholder 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 other 5GZORRO Marketplace members. Since D2.2 [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 5G 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 3-1 shows the exact steps of the certificate generation workflow, described below:

Step 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.

Step 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 selected Admin Agent by using the DID Comm Issue Credential protocol. The Governance Manager handles the registration request and applies the adopted Governance Model to take a decision about the new Marketplace member candidate (e.g., all Governance Board Administrators must vote). 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 it.

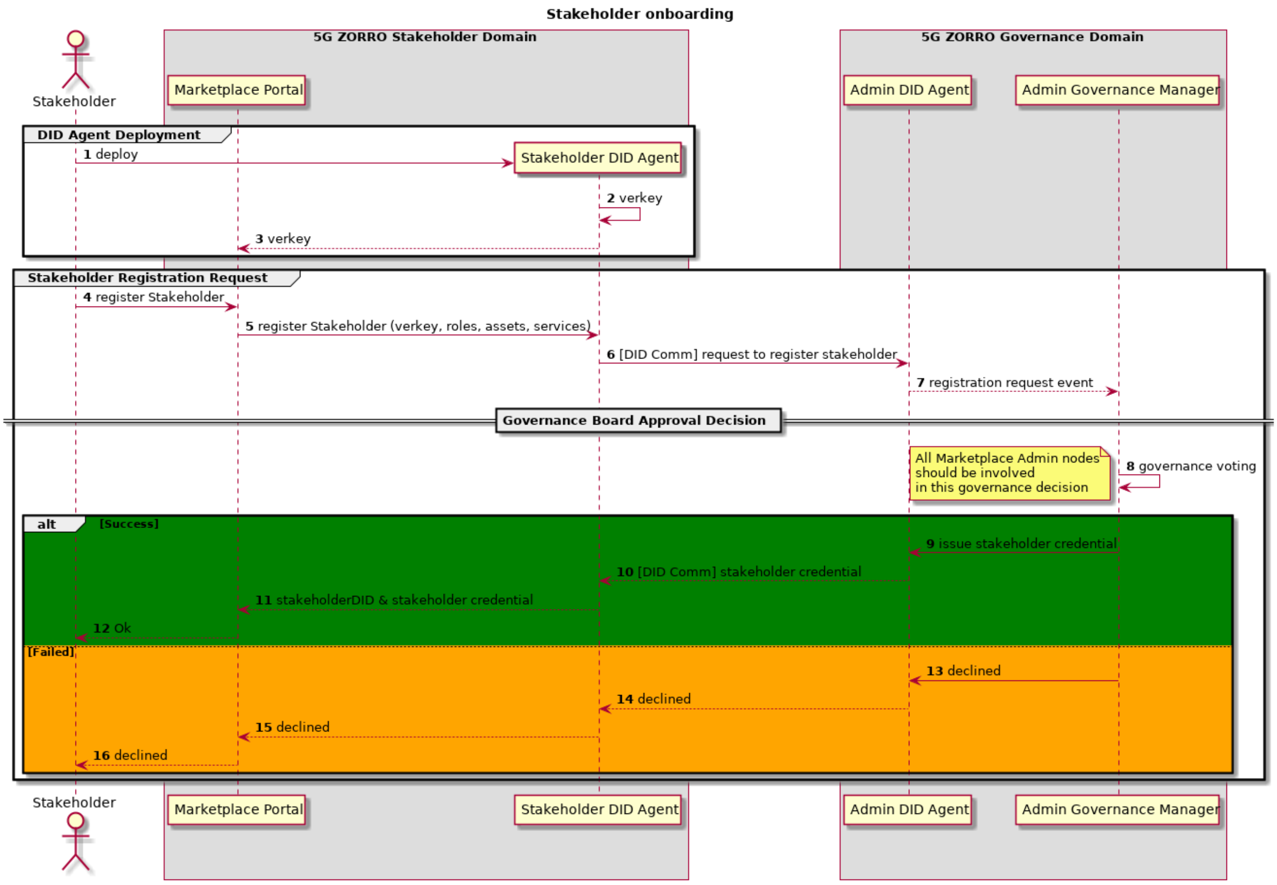

Stakeholder onboarding
5G ZORRO Stakeholder Domain
5G ZORRO Governance Domain
Stakeholder
Marketplace Portal
Admin DID Agent
Admin Governance Manager
DID Agent Deployment
1 deploy
Stakeholder DID Agent
2 verkey
3 verkey
Stakeholder Registration Request
4 register Stakeholder
5 register Stakeholder (verkey, roles, assets, services)
6 [DID Comm] request to register stakeholder
7 registration request event
Governance Board Approval Decision
All Marketplace Admin nodes should be involved in this governance decision
8 governance voting
alt [Success]
9 issue stakeholder credential
10 [DID Comm] stakeholder credential
11 stakeholderDID & stakeholder credential
12 Ok
[Failed]
13 declined
14 declined
15 declined
16 declined
Stakeholder
Marketplace Portal
Stakeholder DID Agent
Admin DID Agent
Admin Governance Manager

Figure 3-1: Stakeholder Onboarding in 5GZORRO marketplace

3.2 Publishing a Spectoken Resource Offer

The spectrum offer modelling in the 5GZORRO platform has been largely discussed, spanned over several fruitful discussions with several partners, which helped the consortium better understand the spectrum's regulatory aspects and what a Spectrum Regulator would expect from the 5GZORRO platform in what concerns to dynamic spectrum trading. As a result, we identified the necessary modifications in generating Spectokens and trading them in the 5GZORRO spectrum market.

Modifications regarding the Dynamic Spectrum Trading use case in D2.1 [1] are presented in Section 2.2 of this document. The following text substitutes the publishing a Spectoken resource offer workflow described in D2.2 [2], Section 6.2, completely.

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 3-2 shows the exact steps of the certificate generation workflow, described below:

1. The Regulator fills the spectrum capabilities of an SRP in the Regulator's 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

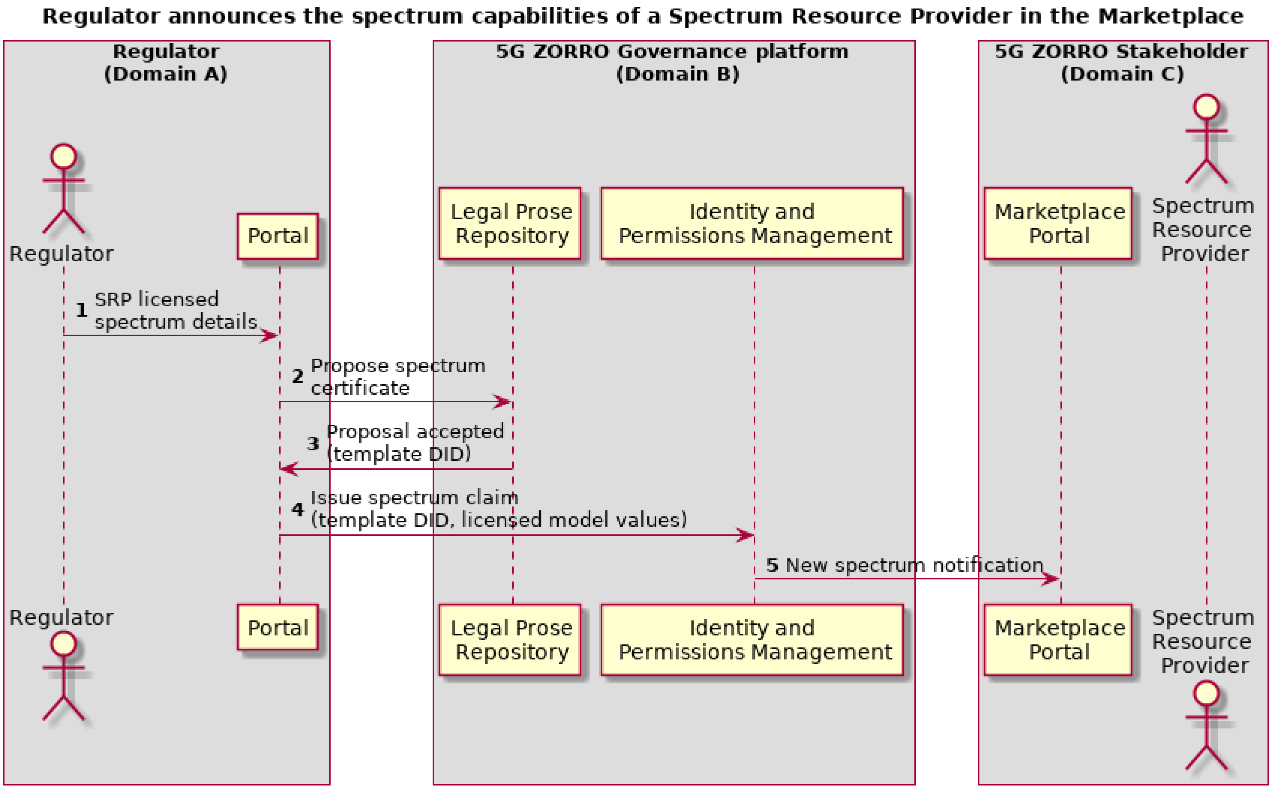

Regulator announces the spectrum capabilities of a Spectrum Resource Provider in the Marketplace
Regulator (Domain A)
5G ZORRO Governance platform (Domain B)
5G ZORRO Stakeholder (Domain C)
Regulator
Portal
Legal Prose Repository
Identity and Permissions Management
Marketplace Portal
Spectrum Resource Provider
1 SRP licensed spectrum details
2 Propose spectrum certificate
3 Proposal accepted (template DID)
4 Issue spectrum claim (template DID, licensed model values)
5 New spectrum notification

Figure 3-2: Spectrum certificate generation workflow

Figure 3-3 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

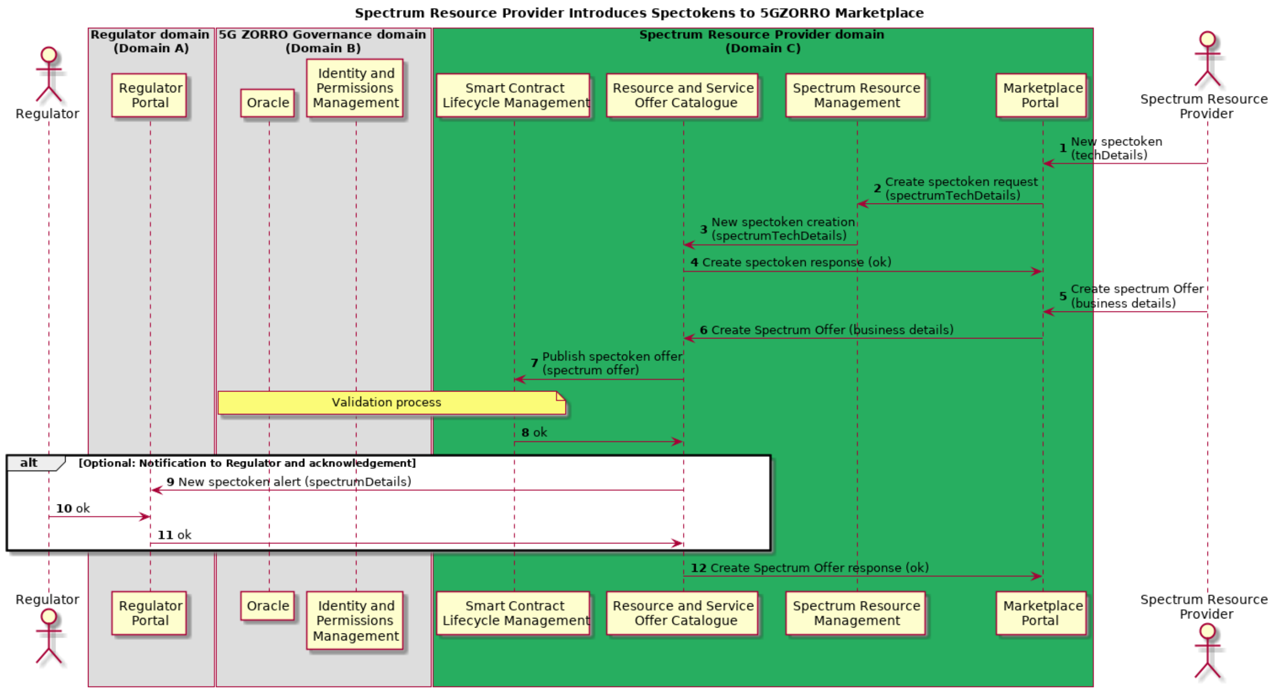

Spectrum Resource Provider Introduces Spectokens to 5GZORRO Marketplace
Regulator domain (Domain A)
5G ZORRO Governance domain (Domain B)
Spectrum Resource Provider domain (Domain C)
Regulator
Regulator Portal
Oracle
Identity and Permissions Management
Smart Contract Lifecycle Management
Resource and Service Offer Catalogue
Spectrum Resource Management
Marketplace Portal
Spectrum Resource Provider
1 New spectoken (techDetails)
2 Create spectoken request (spectrumTechDetails)
3 New spectoken creation (spectrumTechDetails)
4 Create spectoken response (ok)
5 Create spectrum Offer (business details)
6 Create Spectrum Offer (business details)
7 Publish spectoken offer (spectrum offer)
Validation process
8 ok
alt [Optional: Notification to Regulator and acknowledgement]
9 New spectoken alert (spectrumDetails)
10 ok
11 ok
12 Create Spectrum Offer response (ok)

Figure 3-3: 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

3.3 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 [2], the workflow depicted in Figure 3-4 focus 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 3-4, completely substitutes the similar workflow described in D2.2, Section 6.3.

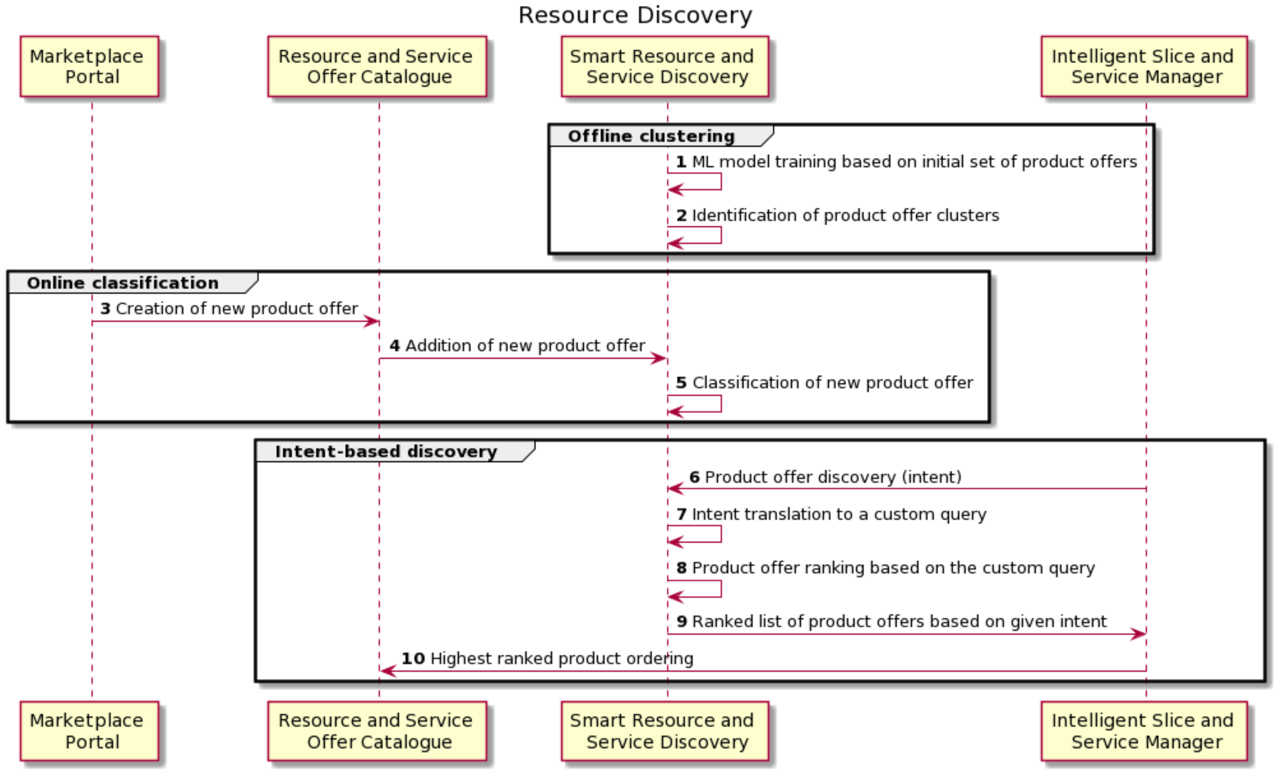

Resource Discovery
Marketplace Portal
Resource and Service Offer Catalogue
Smart Resource and Service Discovery
Intelligent Slice and Service Manager
Offline clustering
1 ML model training based on initial set of product offers
2 Identification of product offer clusters
Online classification
3 Creation of new product offer
4 Addition of new product offer
5 Classification of new product offer
Intent-based discovery
6 Product offer discovery (intent)
7 Intent translation to a custom query
8 Product offer ranking based on the custom query
9 Ranked list of product offers based on given intent
10 Highest ranked product ordering
Marketplace Portal
Resource and Service Offer Catalogue
Smart Resource and Service Discovery
Intelligent Slice and Service Manager

Figure 3-4: 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.

3.4 Trustworthy Smart Contract Setup for spectrum

The workflow on trustworthy smart contract setup for spectrum defined in D2.2 [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 Spectokens for its particular use. 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.

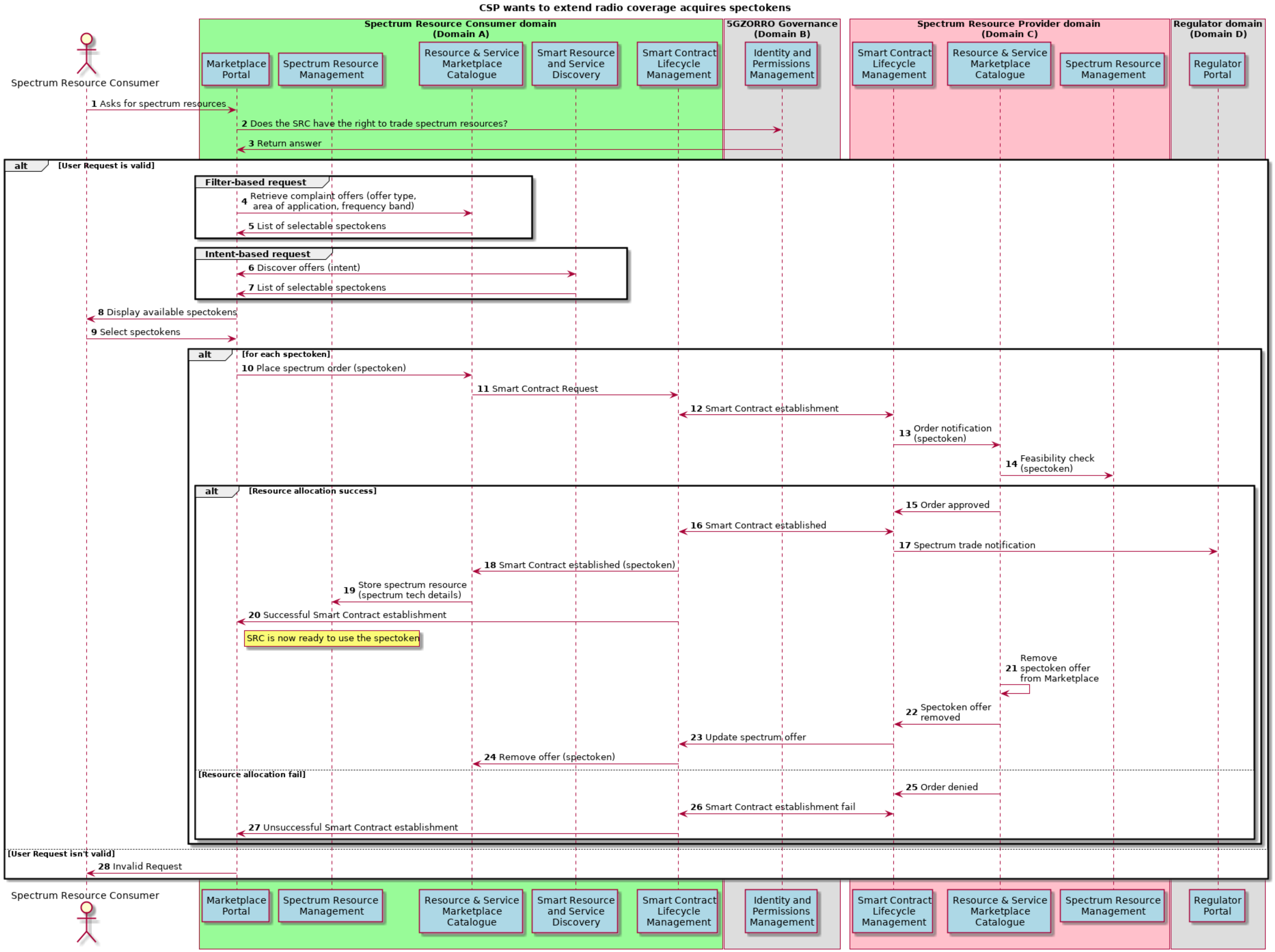

CSP wants to extend radio coverage acquires spectokens
Spectrum Resource Consumer domain (Domain A)
5GZORRO Governance (Domain B)
Spectrum Resource Provider domain (Domain C)
Regulator domain (Domain D)
Spectrum Resource Consumer
Marketplace Portal
Spectrum Resource Management
Resource & Service Marketplace Catalogue
Smart Resource and Service Discovery
Smart Contract Lifecycle Management
Identity and Permissions Management
Smart Contract Lifecycle Management
Resource & Service Marketplace Catalogue
Spectrum Resource Management
Regulator Portal
1 Asks for spectrum resources
2 Does the SRC have the right to trade spectrum resources?
3 Return answer
alt [User Request is valid]
Filter-based request
4 Retrieve complaint offers (offer type, area of application, frequency band)
5 List of selectable spectokens
Intent-based request
6 Discover offers (intent)
7 List of selectable spectokens
8 Display available spectokens
9 Select spectokens
alt [for each spectoken]
10 Place spectrum order (spectoken)
11 Smart Contract Request
12 Smart Contract establishment
13 Order notification (spectoken)
14 Feasibility check (spectoken)
alt [Resource allocation success]
15 Order approved
16 Smart Contract established
17 Spectrum trade notification
18 Smart Contract established (spectoken)
19 Store spectrum resource (spectrum tech details)
20 Successful Smart Contract establishment
SRC is now ready to use the spectoken
21 Remove spectoken offer from Marketplace
22 Spectoken offer removed
23 Update spectrum offer
24 Remove offer (spectoken)
[Resource allocation fail]
25 Order denied
26 Smart Contract establishment fail
27 Unsuccessful Smart Contract establishment
[User Request isn't valid]
28 Invalid Request
Spectrum Resource Consumer
Marketplace Portal
Spectrum Resource Management
Resource & Service Marketplace Catalogue
Smart Resource and Service Discovery
Smart Contract Lifecycle Management
Identity and Permissions Management
Smart Contract Lifecycle Management
Resource & Service Marketplace Catalogue
Spectrum Resource Management
Regulator Portal

Figure 3-5: CSP who wants to extend radio coverage acquires Spectokens

Figure 3-5 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 Portal. If the SRC is not authorised to purchase Spectokens, jump to step 27.
4. The 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 Portal.
6. If the SRC provided an intent instead of the Spectoken characteristics, the 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 Portal.
10. For each selected Spectoken, the 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 not authorised to participate in the spectrum trading in the 5GZORRO platform.

3.5 Trustworthy Smart Contract Setup for edge computing

The operational flow diagram illustrated in Figure 3-6 describes the processes involved in the automatic, trustworthy resource agreement setup, focusing on the leasing of edge compute resources. In this figure, the Resource Consumer has already selected one or more resource offers provided by the Resource Provider. Figure 3-6 is an updated version of the Resource Agreement workflow presented in D2.2 [2], Section 6.5. The main differences are that the *Intelligent Network Slice and Service Orchestration* is now renamed into *Network Slice and Service Orchestration* and how the workflow is initiated gas been modified, as explained in the next paragraphs. Another key update from D2.2 is that the Resource and Service Offer Catalogue can interact directly with the *Virtual Resource Management and Control*, instead of passing the requests through the *Smart Contract Lifecycle Management* functionalities. Moreover, Figure 3-6 has extended the workflow of D2.2 with additional steps, to be more descriptive. Finally, in D2.2, the agreement finalization preceded the resource allocation, while in the current version the order is reversed. This is because we first need to be sure that the resource allocation can be successfully realized and then complete the respective agreement.

More specifically, the steps presented in Figure 3-6 can be analysed 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 given by the Resource Provider. This differentiates from the respective workflow in D2.2, since that flow was started from 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, it was decided that this flow should be initiated by placing an order to the Catalogue and the agreement setup should be 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 can consist on 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 offer.

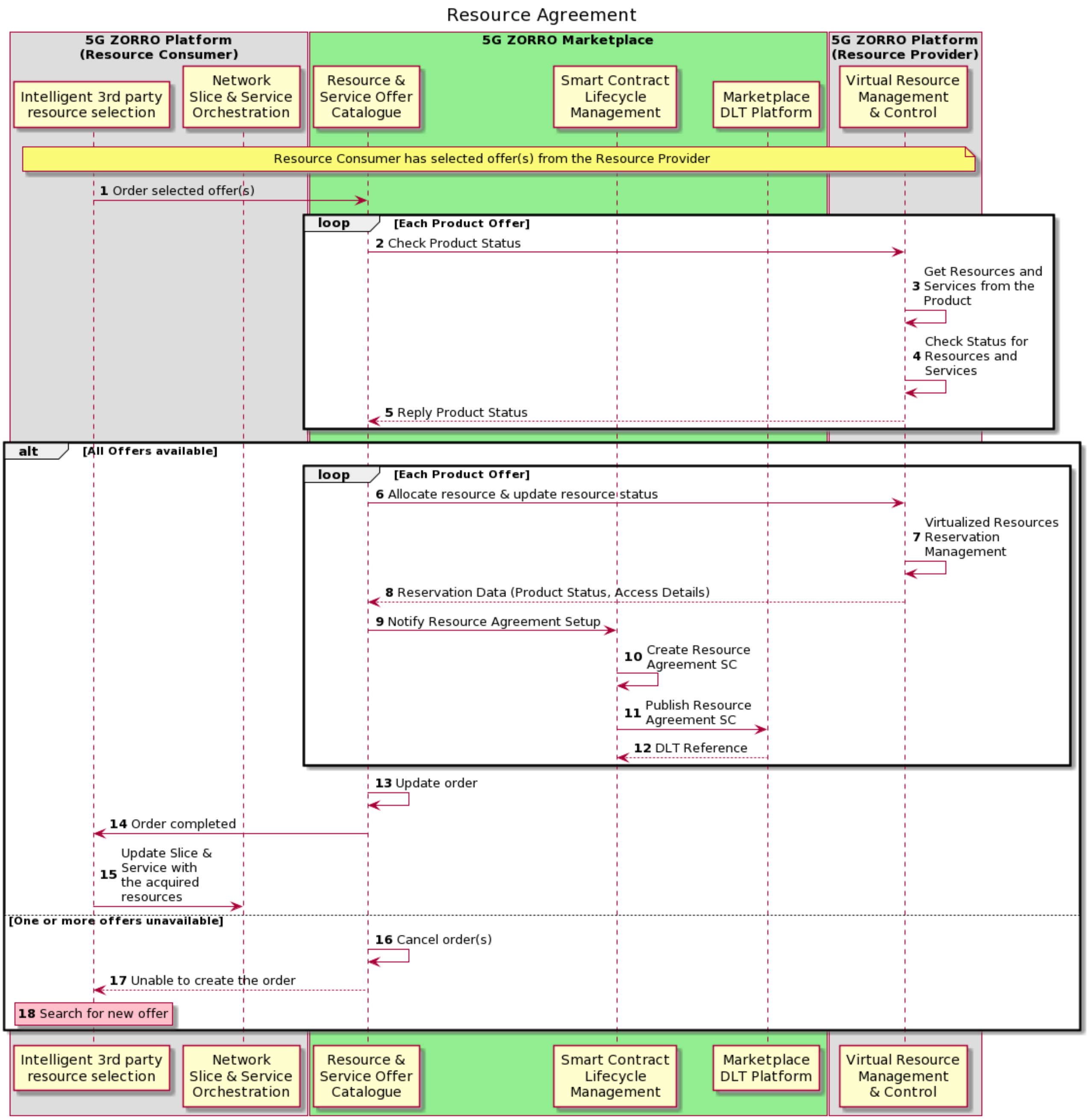

Resource Agreement
5G ZORRO Platform (Resource Consumer)
5G ZORRO Marketplace
5G ZORRO Platform (Resource Provider)
Intelligent 3rd party resource selection
Network Slice & Service Orchestration
Resource & Service Offer Catalogue
Smart Contract Lifecycle Management
Marketplace DLT Platform
Virtual Resource Management & Control
Resource Consumer has selected offer(s) from the Resource Provider
1 Order selected offer(s)
loop [Each Product Offer]
2 Check Product Status
3 Get Resources and Services from the Product
4 Check Status for Resources and Services
5 Reply Product Status
alt [All Offers available]
loop [Each Product Offer]
6 Allocate resource & update resource status
7 Virtualized Resources Reservation Management
8 Reservation Data (Product Status, Access Details)
9 Notify Resource Agreement Setup
10 Create Resource Agreement SC
11 Publish Resource Agreement SC
12 DLT Reference
13 Update order
14 Order completed
15 Update Slice & Service with the acquired resources
[One or more offers unavailable]
16 Cancel order(s)
17 Unable to create the order
18 Search for new offer

Figure 3-6: Workflow for Trustworthy Smart Contract Setup for edge compute resources

Step 4: If there are multiple resources or services on a product, 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. For 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 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 from 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 from involved parties and consensus is reached at the DLT network (steps 10 – 12). When the above procedure is completed 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 notifies the *Network Slice and Service Orchestration* to update the slice with the newly acquired resources (steps 14 – 15).

Step 16 - 17: In case that one or more requested resources are no longer available by the Resource Provider, order is cancelled (step 16) and the resource selection process must be repeated as explained in Section 3.3 (steps 17 – 18).

Once the resource agreement is successfully established, the Resource Consumer (mentioned as Domain A in the images below) is able to leverage on resources provisioned by the Resource Provider (Domain B). Therefore, an end user that was initially served by Domain A, may be redirected to Domain B, according to load balancing policies, and get served by the second domain. In D2.2, this process was shown in a single flow diagram. However, in the current deliverable we separated it into two flows (Figures Figure 3-7 and Figure 3-8), in order to analyse 5GZORRO modules interactions that are required for the extension to the 3rd party resources, as depicted in Figure 3-7. On the other hand, Figure 3-8 describes 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 Contend Delivery Network (vCDN) service, that is described as a use-case of 5GZORRO.

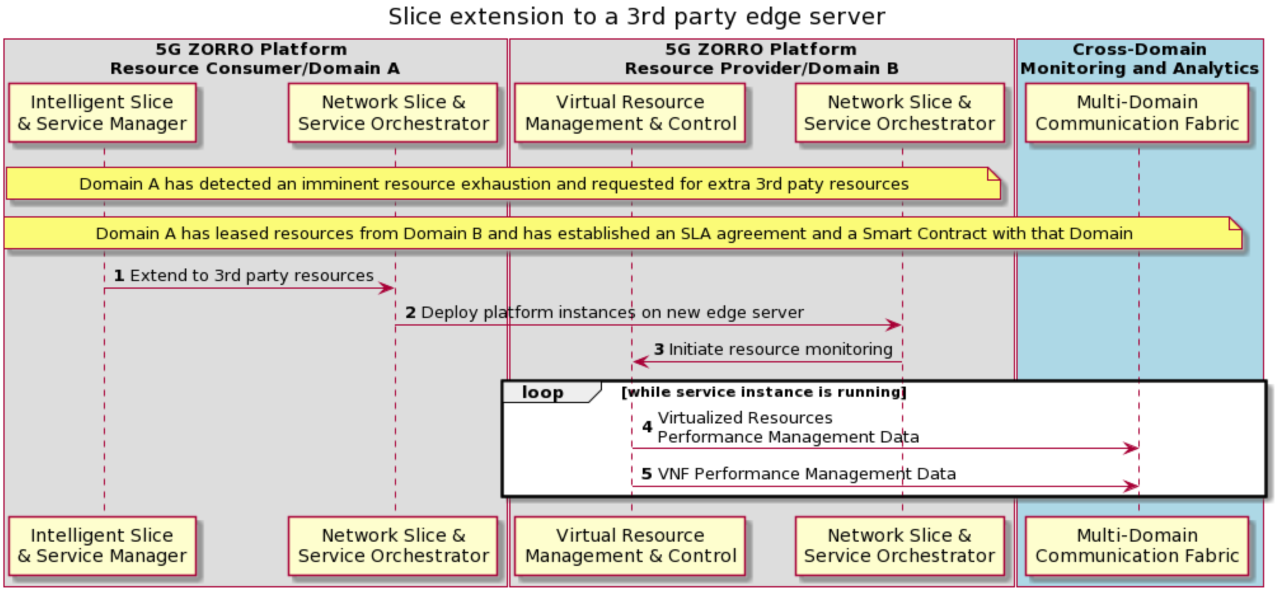

Slice extension to a 3rd party edge server
5G ZORRO Platform
Resource Consumer/Domain A
5G ZORRO Platform
Resource Provider/Domain B
Cross-Domain
Monitoring and Analytics
Intelligent Slice & Service Manager
Network Slice & Service Orchestrator
Virtual Resource Management & Control
Network Slice & Service Orchestrator
Multi-Domain Communication Fabric
Domain A has detected an imminent resource exhaustion and requested for extra 3rd paty resources
Domain A has leased resources from Domain B and has established an SLA agreement and a Smart Contract with that Domain
1 Extend to 3rd party resources
2 Deploy platform instances on new edge server
3 Initiate resource monitoring
loop
[while service instance is running]
4 Virtualized Resources Performance Management Data
5 VNF Performance Management Data

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

More analytically, in Figure 3-7, 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 3-7):

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 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 will be aggregated and used in AI techniques to make predictions of the service performance for the near future.

Figure 3-8 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.

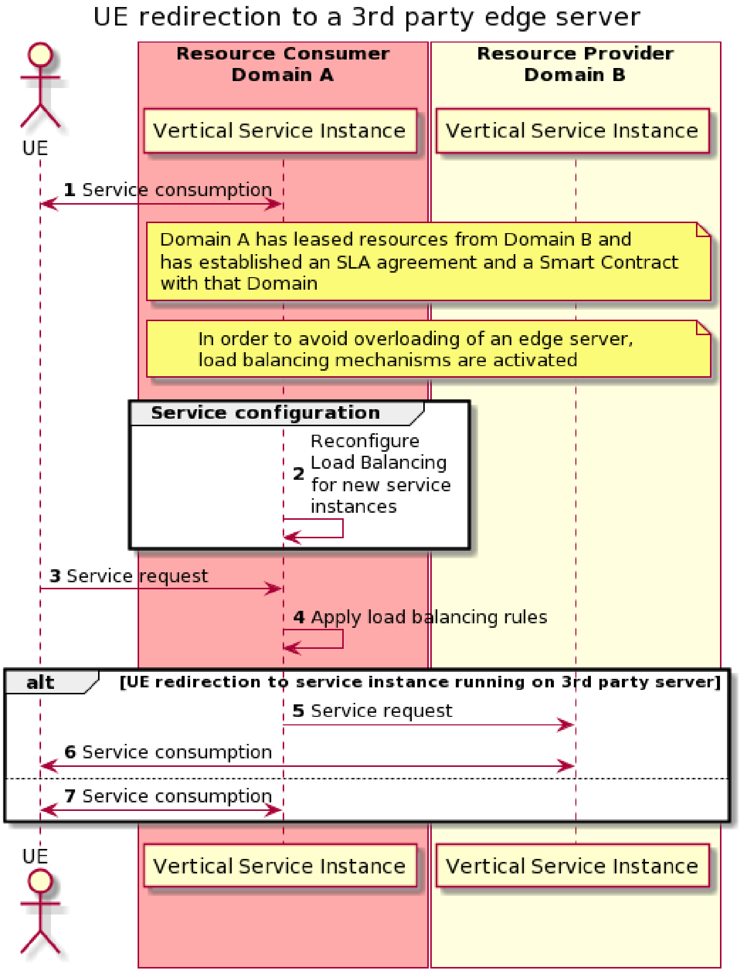

UE redirection to a 3rd party edge server
Resource Consumer Domain A
Resource Provider Domain B
UE
Vertical Service Instance
Vertical Service Instance
1 Service consumption
Domain A has leased resources from Domain B and has established an SLA agreement and a Smart Contract with that Domain
In order to avoid overloading of an edge server, load balancing mechanisms are activated
Service configuration
2 Reconfigure Load Balancing for new service instances
3 Service request
4 Apply load balancing rules
alt
[UE redirection to service instance running on 3rd party server]
5 Service request
6 Service consumption
7 Service consumption
UE
Vertical Service Instance
Vertical Service Instance

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

The steps of the sequence diagram in Figure 3-8 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 keep service the UE by the Service Instance hosted at Domain A.

3.6 Trustworthy Slice setup with 3rd party resources

Figure 3-9 and Figure 3-10 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.

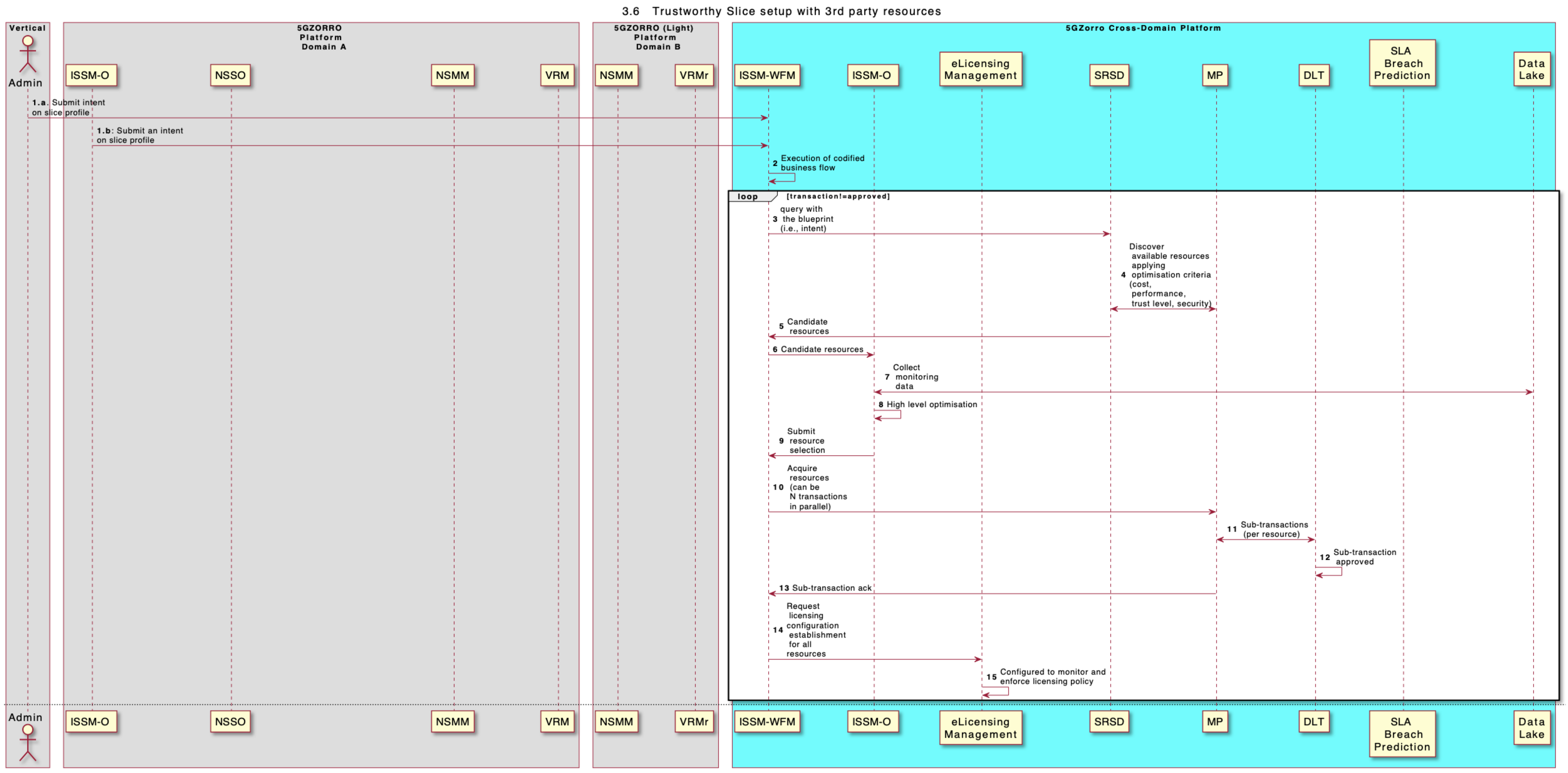

3.6 Trustworthy Slice setup with 3rd party resources
Vertical
Admin
5GZORRO Platform Domain A
ISSM-O
NSSO
NSMM
VRM
5GZORRO (Light) Platform Domain B
NSMM
VRMr
5GZorro Cross-Domain Platform
ISSM-WFM
ISSM-O
eLicensing Management
SRSD
MP
DLT
SLA Breach Prediction
Data Lake
1.a. Submit intent on slice profile
1.b: Submit an intent on slice profile
2 Execution of codified business flow
loop [transaction!=approved]
3 query with the blueprint (i.e., intent)
4 Discover available resources applying optimisation criteria (cost, performance, trust level, security)
5 Candidate resources
6 Candidate resources
7 Collect monitoring data
8 High level optimisation
9 Submit resource selection
10 Acquire resources (can be N transactions in parallel)
11 Sub-transactions (per resource)
12 Sub-transaction approved
13 Sub-transaction ack
14 Request licensing configuration establishment for all resources
15 Configured to monitor and enforce licensing policy

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

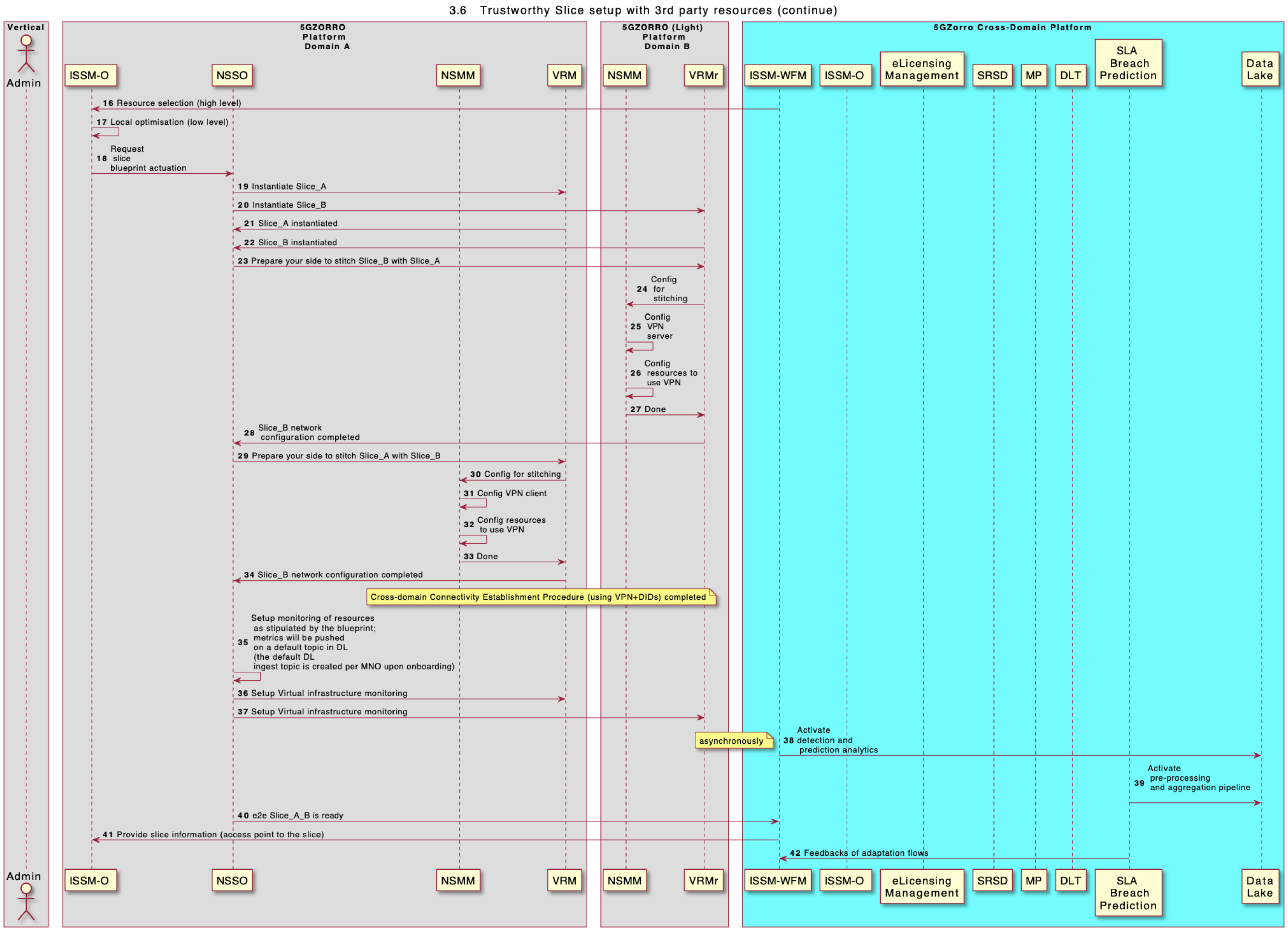

3.6 Trustworthy Slice setup with 3rd party resources (continue)
Vertical
Admin
5GZORRO Platform Domain A
ISSM-O
NSSO
NSMM
VRM
5GZORRO (Light) Platform Domain B
NSMM
VRMr
5GZorro Cross-Domain Platform
ISSM-WFM
ISSM-O
eLicensing Management
SRSD
MP
DLT
SLA Breach Prediction
Data Lake
16 Resource selection (high level)
17 Local optimisation (low level)
18 Request slice blueprint actuation
19 Instantiate Slice_A
20 Instantiate Slice_B
21 Slice_A instantiated
22 Slice_B instantiated
23 Prepare your side to stitch Slice_B with Slice_A
24 Config for stitching
25 Config VPN server
26 Config resources to use VPN
27 Done
28 Slice_B network configuration completed
29 Prepare your side to stitch Slice_A with Slice_B
30 Config for stitching
31 Config VPN client
32 Config resources to use VPN
33 Done
34 Slice_B network configuration completed
Cross-domain Connectivity Establishment Procedure (using VPN+DIDs) completed
35 Setup monitoring of resources as stipulated by the blueprint; metrics will be pushed on a default topic in DL (the default DL ingest topic is created per MNO upon onboarding)
36 Setup Virtual infrastructure monitoring
37 Setup Virtual infrastructure monitoring
asynchronously
38 Activate detection and prediction analytics
39 Activate pre-processing and aggregation pipeline
40 e2e Slice_A_B is ready
41 Provide slice information (access point to the slice)
42 Feedbacks of adaptation flows
Admin
ISSM-O
NSSO
NSMM
VRM
NSMM
VRMr
ISSM-WFM
ISSM-O
eLicensing Management
SRSD
MP
DLT
SLA Breach Prediction
Data Lake

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

The textual description of the workflow depicted in Figure 3-9 and Figure 3-10 is provided below to facilitate the figures comprehension.

- **Step 1.a/1.b:** The workload starts with Intelligent Slice and Service Optimiser (ISSM-O) acting in a Domain role or an Administrator from within a vertical submitting a declarative intent describing slice requirements, a slice *profile*, to ISSM-WFM.
- **Step 2:** ISSM-WFM invokes a pre-coded business logic workflow (the following steps are orchestrated by this workflow and to this end, ISSM-WFM plays the role of an integration medium binding various components of the platform together to achieve the end goal – slice profile realization)
- **Step 3:** ISSM-WFM queries Smart Resource and Service Discovery (SRSD) component, passing it the slice profile (i.e., the intent).
- **Step 4:** The Smart Resource and Service Discovery module interacts with the Marketplace Portal (MP) to discover current resource offerings relevant to this slice profile.
- **Step 5:** ISSM-WFM retrieves a universe of pre-ranked resource offerings, representing possible candidate resources
- **Step 6:** ISSM-WFM passes the candidate solutions to ISSM-O acting in a cross-domain capacity to perform a high-level resource optimization.
- **Step 7:** ISSM-O acting in the cross-domain role complements the set of resources with the monitoring information from the Data Lake
- **Step 8:** ISSM-O acting in the cross-domain role performs an optimization to arbitrate among the candidate solutions and finalizes a decision on the resource set that should be procured from the marketplace.
- **Step 9:** ISSM-O cross-domain returns a finalized selection of resources per domain that should be used in the slice construction.
- **Step 10:** ISSM-WFM executes transactions to acquire resources proposed by ISSM-O against the marketplace portal
- **Steps 11—15:** The Marketplace Portal executes sub-transactions against the DLT to fulfil the resource acquisition. Steps 3 – 9 execute in a loop, because a competition on resources acquisition is possible and resource selection and re-optimisation might have to be performed continuously until either all resources are acquired, or a transaction is aborted due to too many failures (the latter would terminate the workflow). For each resource successfully acquired, ISSM-WFM requests licensing configuration from the eLicensing Management module and the eLicensing Management component configures licensing policy for each resource
- **Step 16:** At this point, the resources are acquired, and their license policies are configured. To allow for local optimization within a domain, ISSM-WFM passes the resources selection to ISSM-O acting in the domain role.
- **Step 17:** After performing a local optimization, ISSM-O requests profile instantiation from NSSO
- **Step 18:** NSSO instantiates a slice subnet in Domain A via NBI of the Virtual Resource Manager (VRM) of Domain A
- **Step 19:** in parallel with the previous step, NSSO requests instantiation of the Virtual Resource Manager (VRM) of Domain B
- **Steps 20—21:** the slice subnets in Domain A and Domain B are successfully instantiated
- **Step 22:** the slice subnets are now ready for “stitching” and NSSO requests the VRM of Domain B to configure the slice subnet of Domain B to be stitched with that of Domain A

- **Step 23:** VRM of Domain B requests VPN configuration of VPN by calling to the Network Service Mesh Manager (NSMM) of Domain B
- **Steps 24 – 26:** configuration is taking place in Domain B
- **Step 27:** the status of configuring slice subnet in Domain B is reported to NSSO of Domain A
- **Steps 28 – 34:** the steps analogous to Steps 19 – 21 are carried out in Domain A. Upon completing these steps, the slice is instantiated and ready for use
- **Step 35:** NSSO configures itself to initialize monitoring of the resources involved with the slice as stipulated in the slice blueprint
- **Step 36 - 37:** NSSO activates Monitoring and Data Aggregation (MDA) components of VRMs in Domain A and Domain B respectively, passing them the globally unique identifiers that should annotate the monitoring data that will be reported to the Data Lake by each domain's MDA via MNO's default in-topic of the Data Lake's Kafka bus. The global ID is formed as a combination of a globally unique business transaction ID generated by ISSM-WFM, productID (a marketplace-wide unique ID that was allocated to a resource offer by the Marketplace Portal upon the offer creation), and the resource instance ID, which is a specific instance of a resource offer obtained by NSSO upon instantiation of a resource
- **Step 37:** ISSM-WMF configures and activates SLA Monitoring and Breach Prediction module via its NBI to inform it about the newly established slice monitoring data that is about to arrive to the Data Lake (asynchronously), so that the SLA Monitoring and Breach Prediction can now track this data and apply algorithms to predict SLA breaches. This is done asynchronously with domain level configurations.
- **Steps 38 -- 39:** The SLA Monitoring and Breach Prediction module configures itself and activates an analytic pipeline inside the Data Lake that would perform the analytics itself in situ in the Data Lake
- **Step 40:** The slice is reported as ready for operation to ISSM-WFM
- **Step 41:** ISSM-WFM provides the PoP information about the slice
- **Step 42:** The slice now is in the operational state. ISSM might now receive events from the SLA Monitoring and Breach Prediction on its event bus as the slice is continuously exploited. These events are picked up by ISSM-O (the optimization component of ISSM) and might trigger slice adaptation flows in ISSM-WFM. One such flow is exactly this flow, if the optimization algorithm of ISSM-O concludes that a slice should be re-established cross domain with different resources to a mitigate SLA breach.

3.7 Trustworthy Slice setup with 3rd party orchestrated services

Figure 3-11, Figure 3-12, and Figure 3-13 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., domain role) ISSM-O that allows it to perform local optimization when actuating high level resource selection performed y ISSM-O acting in cross-domain role

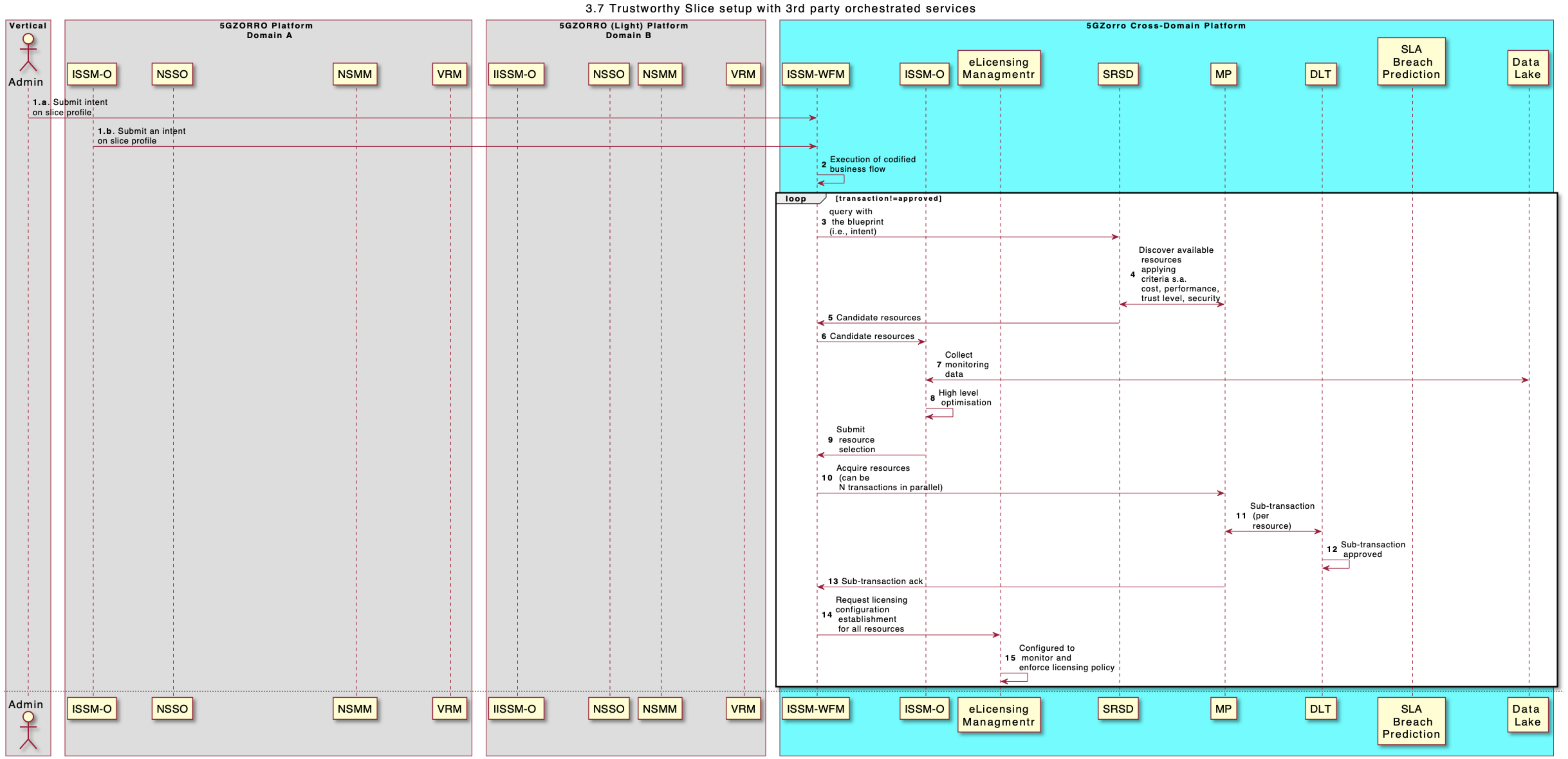

3.7 Trustworthy Slice setup with 3rd party orchestrated services
Vertical
5GZORRO Platform Domain A
5GZORRO (Light) Platform Domain B
5GZorro Cross-Domain Platform
Admin
ISSM-O
NSSO
NSMM
VRM
IISSM-O
NSSO
NSMM
VRM
ISSM-WFM
ISSM-O
eLicensing Managmentr
SRSD
MP
DLT
SLA Breach Prediction
Data Lake
1.a. Submit intent on slice profile
1.b. Submit an intent on slice profile
2 Execution of codified business flow
loop [transaction!=approved]
3 query with the blueprint (i.e., intent)
4 Discover available resources applying criteria s.a. cost, performance, trust level, security
5 Candidate resources
6 Candidate resources
7 Collect monitoring data
8 High level optimisation
9 Submit resource selection
10 Acquire resources (can be N transactions in parallel)
11 Sub-transaction (per resource)
12 Sub-transaction approved
13 Sub-transaction ack
14 Request licensing configuration establishment for all resources
15 Configured to monitor and enforce licensing policy
Admin
ISSM-O
NSSO
NSMM
VRM
IISSM-O
NSSO
NSMM
VRM
ISSM-WFM
ISSM-O
eLicensing Managmentr
SRSD
MP
DLT
SLA Breach Prediction
Data Lake

Figure 3-11: End-to-end flow of trustworthy cross-domain slice establishment (1)

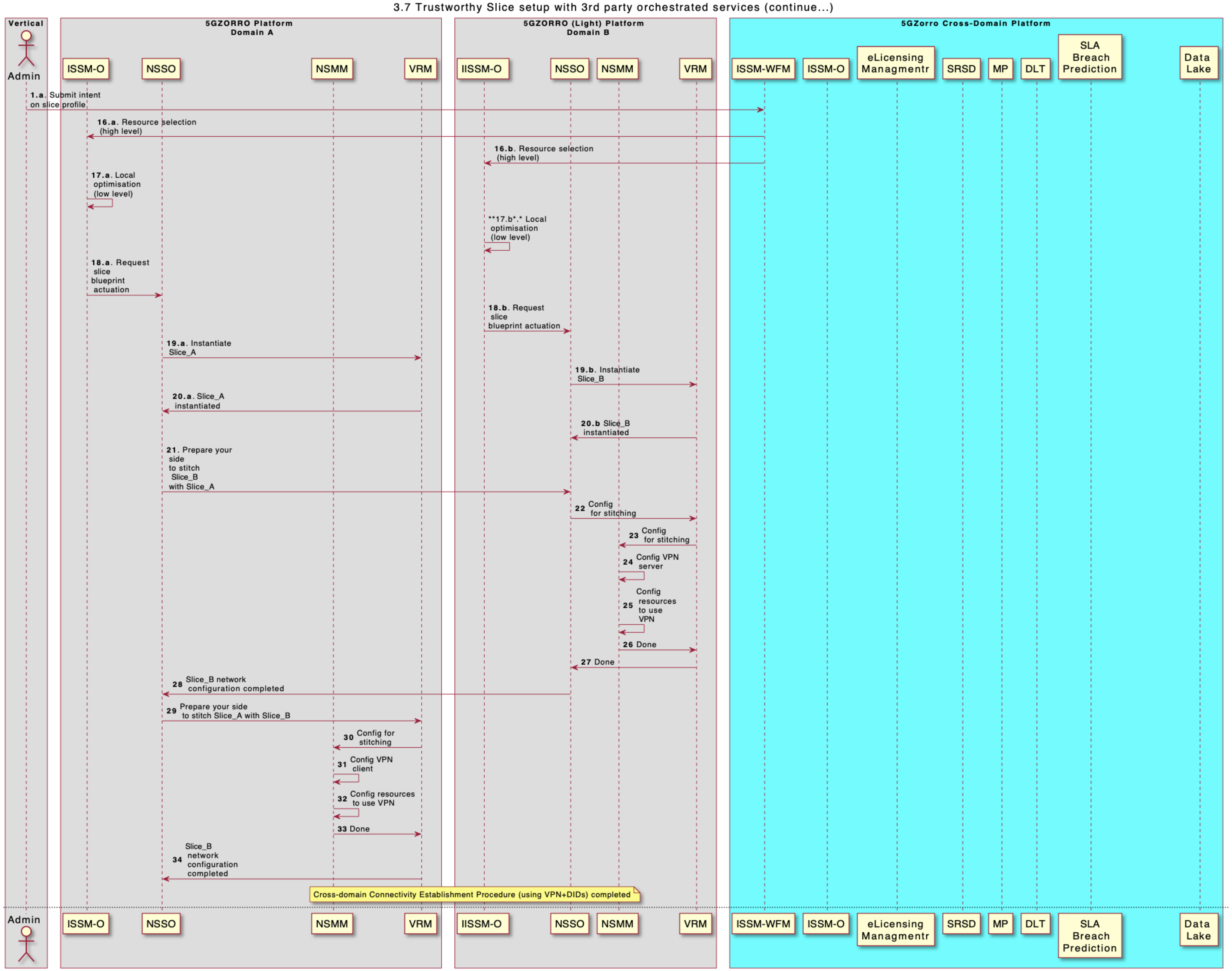

3.7 Trustworthy Slice setup with 3rd party orchestrated services (continue...)
Vertical
Admin
5GZORRO Platform Domain A
ISSM-O
NSSO
NSMM
VRM
5GZORRO (Light) Platform Domain B
IISSM-O
NSSO
NSMM
VRM
5GZorro Cross-Domain Platform
ISSM-WFM
ISSM-O
eLicensing Managmentr
SRSD
MP
DLT
SLA Breach Prediction
Data Lake
1.a. Submit intent on slice profile
16.a. Resource selection (high level)
16.b. Resource selection (high level)
17.a. Local optimisation (low level)
**17.b*.* Local optimisation (low level)
18.a. Request slice blueprint actuation
18.b. Request slice blueprint actuation
19.a. Instantiate Slice_A
19.b. Instantiate Slice_B
20.a. Slice_A instantiated
20.b Slice_B instantiated
21. Prepare your side to stitch Slice_B with Slice_A
22 Config for stitching
23 Config for stitching
24 Config VPN server
25 Config resources to use VPN
26 Done
27 Done
28 Slice_B network configuration completed
29 Prepare your side to stitch Slice_A with Slice_B
30 Config for stitching
31 Config VPN client
32 Config resources to use VPN
33 Done
34 Slice_B network configuration completed
Cross-domain Connectivity Establishment Procedure (using VPN+DIDs) completed

Figure 3-12: End-to-end flow of trustworthy cross-domain slice establishment (2)

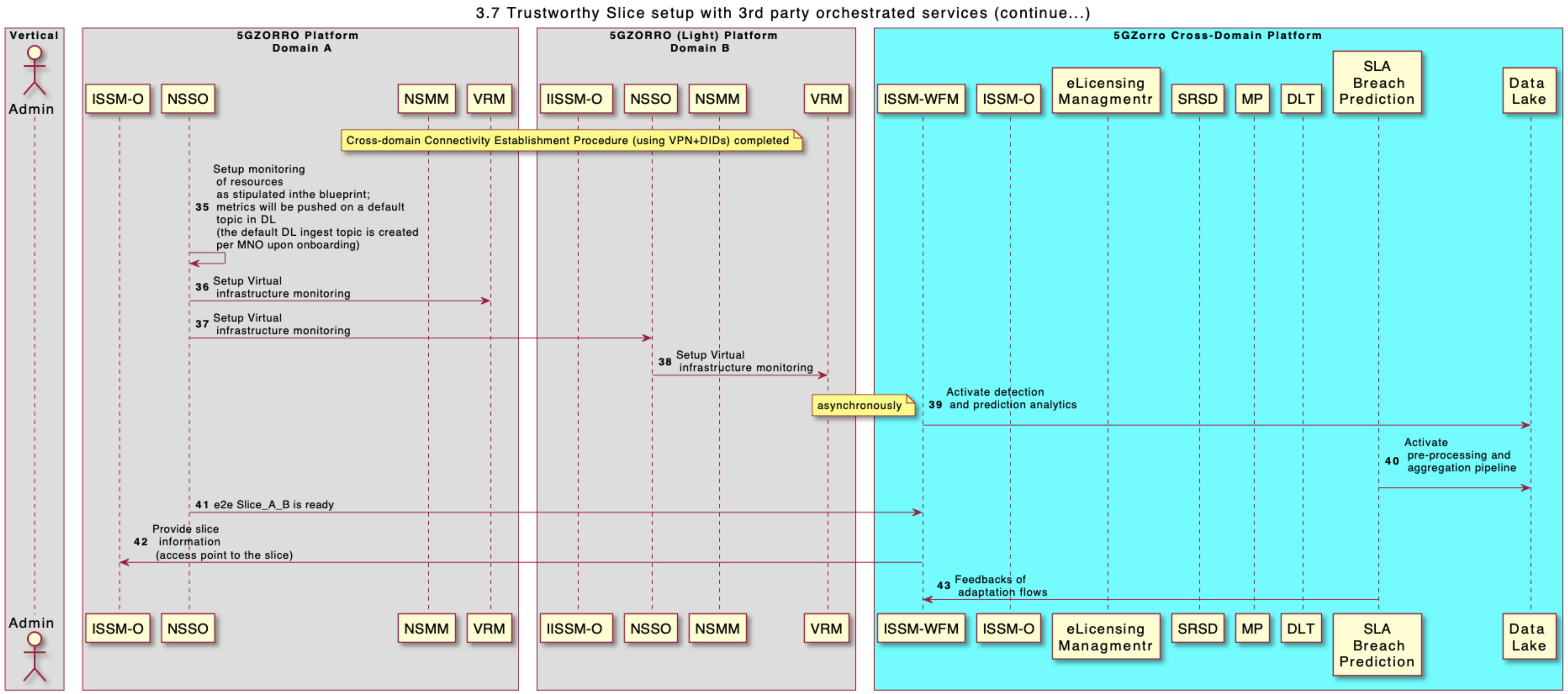


Figure 3-13: End-to-end flow of trustworthy cross-domain slice establishment (3)

3.8 Trustworthy e-licensing control

In this Section is detailed the operational pattern that describes the sequence of operations involved in the e-licensing management, previously introduced in D2.2 [2]. There are no updates regarding the workflow, but the names of the components which the eLicensing Manager interacts are modified, like the 5G Network Virtualization platform or the Network Slice and Service Orchestrator.

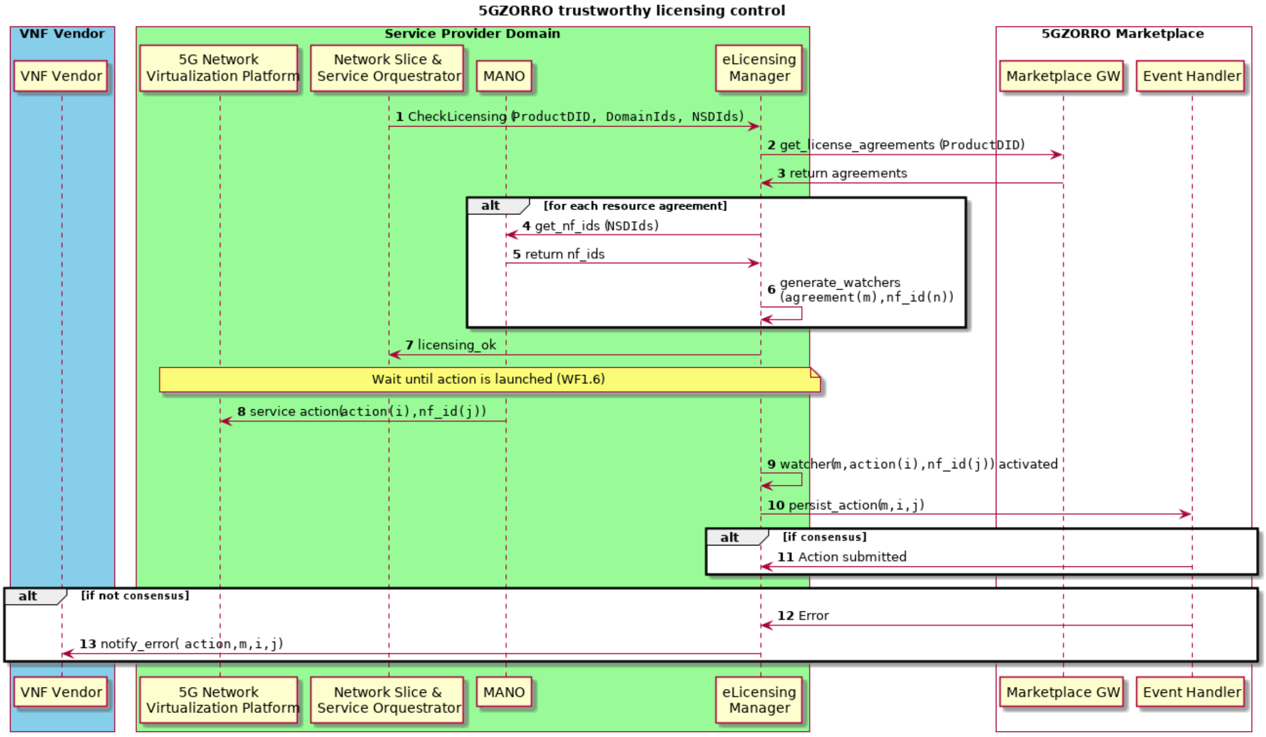

5GZORRO trustworthy licensing control
VNF Vendor
Service Provider Domain
5GZORRO Marketplace
VNF Vendor
5G Network Virtualization Platform
Network Slice & Service Orquestrator
MANO
eLicensing Manager
Marketplace GW
Event Handler
1 CheckLicensing (ProductDID, DomainIds, NSDIds)
2 get_license_agreements (ProductDID)
3 return agreements
alt [for each resource agreement]
4 get_nf_ids (NSDIds)
5 return nf_ids
6 generate_watchers (agreement(m),nf_id(n))
7 licensing_ok
Wait until action is launched (WF1.6)
8 service action(action(i),nf_id(j))
9 watcher(m,action(i),nf_id(j)) activated
10 persist_action(m,i,j)
alt [if consensus]
11 Action submitted
alt [if not consensus]
12 Error
13 notify_error(action,m,i,j)
VNF Vendor
5G Network Virtualization Platform
Network Slice & Service Orquestrator
MANO
eLicensing Manager
Marketplace GW
Event Handler

Figure 3-14: Trustworthy licensing control

Step 1: The Network Slice and Service Orchestrator (NSSO) block triggers the licensing checking in the service that is going to be created/modified before the deployment of the software components by the MANO.

Steps 2-3: The e-Licensing Manager requests to the marketplace the related agreements for each of the software components inside the product DID.

Step 4-5: If the service has software components with licensing constraints associated, the e-Licensing Manager requests the identifier used by the MANO for each component.

Step 6: Once retrieved the agreements and the mano identifiers, the e-Licensing Manager creates the watchers. These watchers observe the MANO and monitors the potential actions performed in the software components related to the licensing agreements associated to them. Each e-Licensing Manager is responsible for the reporting of the actions in its domain, so will only observe its own infrastructure manager.

Step 7: ACK licensing OK

Steps 8-9-10: When the MANO engine performs some action in the virtualization platform, the watcher will trigger the alert and launch the transaction for the implied agreement, action and nf_id to the Marketplace.

Step 11-12-13: these steps are 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, in step 13, the VNF vendor will be notified that there is an error in the control of their software...

3.9 Intelligent SLA monitoring & breach prediction

Figure 3-15 shows the Workflow for the SLA Breach Prediction. Basically, this is like the one presented in D2.2 [2]. The only difference is that, for a better presentation, Figure 3-15 shows only the SLA Monitoring of one Domain, which can be a Resource and/or Service Provider.

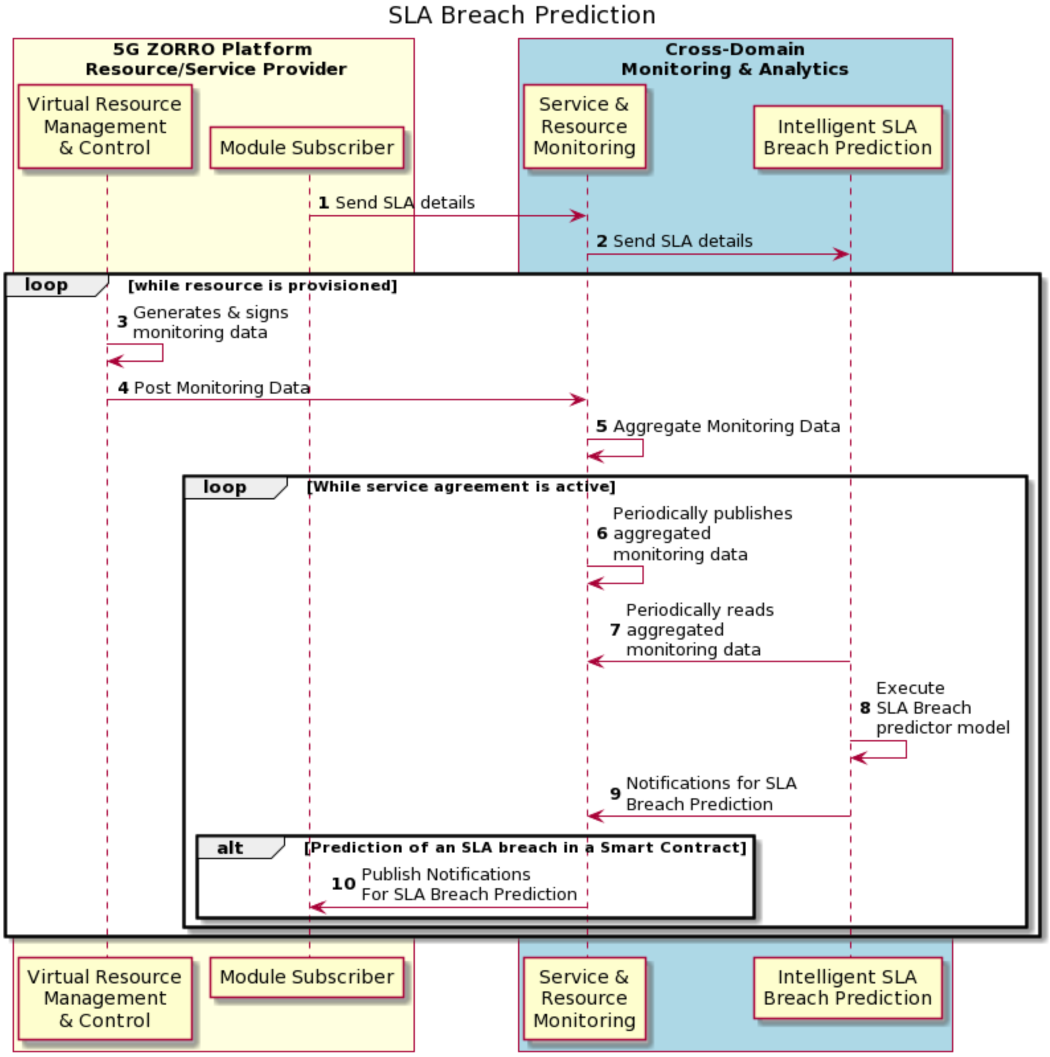

SLA Breach Prediction
5G ZORRO Platform
Resource/Service Provider
Cross-Domain
Monitoring & Analytics
Virtual Resource Management & Control
Module Subscriber
Service & Resource Monitoring
Intelligent SLA Breach Prediction
1 Send SLA details
2 Send SLA details
loop [while resource is provisioned]
3 Generates & signs monitoring data
4 Post Monitoring Data
5 Aggregate Monitoring Data
loop [While service agreement is active]
6 Periodically publishes aggregated monitoring data
7 Periodically reads aggregated monitoring data
8 Execute SLA Breach predictor model
9 Notifications for SLA Breach Prediction
alt [Prediction of an SLA breach in a Smart Contract]
10 Publish Notifications For SLA Breach Prediction
Virtual Resource Management & Control
Module Subscriber
Service & Resource Monitoring
Intelligent SLA Breach Prediction

Figure 3-15: *Workflow for SLA Breach Prediction*

Figure 3-15 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 *Service and Resource Monitoring*.

Step 5: In turn, the *Service and Resource Monitoring* 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.

3.10 Intelligent Network Slice and Service optimization

In Figure 3-16, 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 Manager 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.

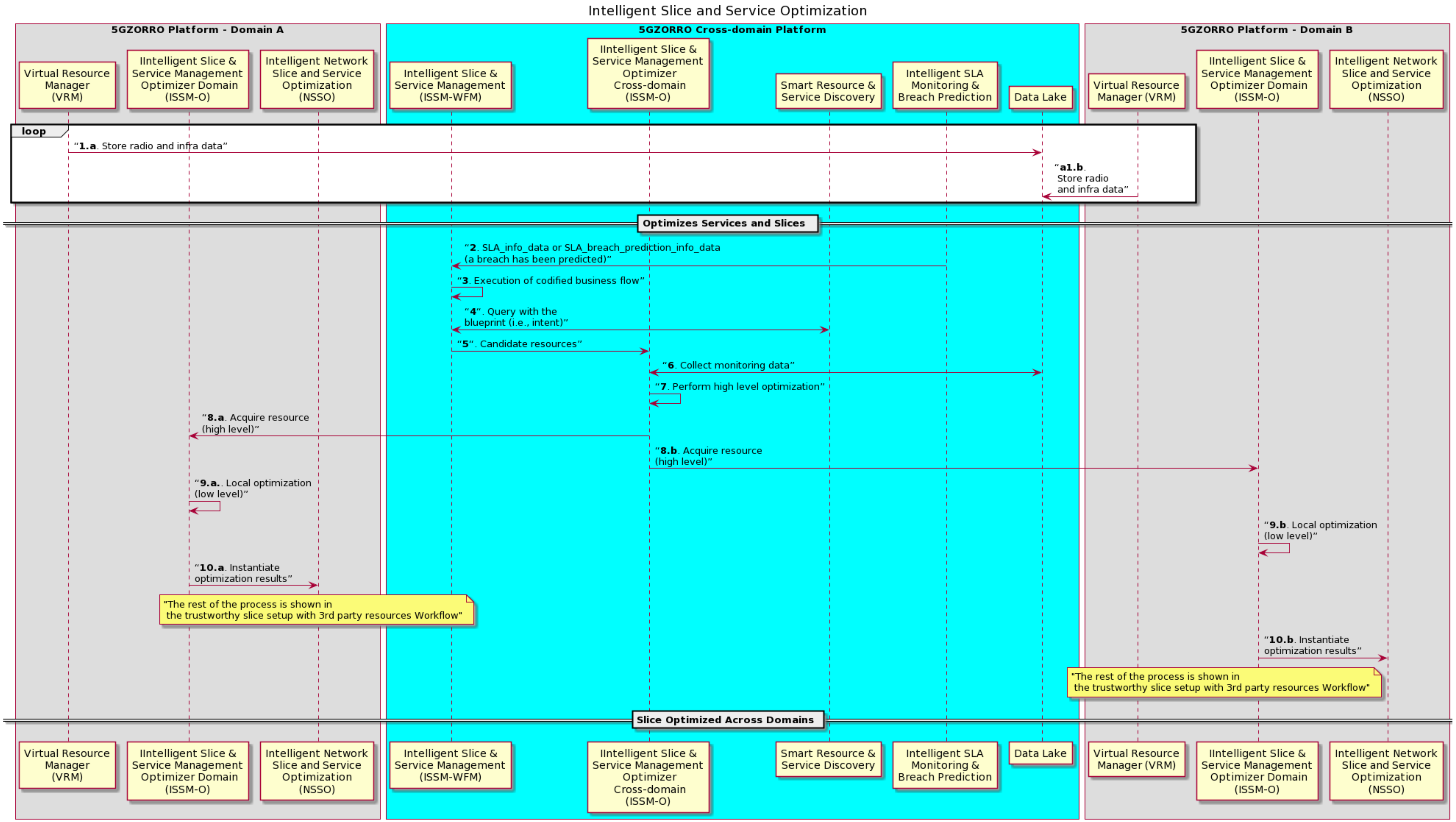

Intelligent Slice and Service Optimization
5GZORRO Platform - Domain A
5GZORRO Cross-domain Platform
5GZORRO Platform - Domain B
Virtual Resource Manager (VRM)
IIntelligent Slice & Service Management Optimizer Domain (ISSM-O)
Intelligent Network Slice and Service Optimization (NSSO)
Intelligent Slice & Service Management (ISSM-WFM)
IIntelligent Slice & Service Management Optimizer Cross-domain (ISSM-O)
Smart Resource & Service Discovery
Intelligent SLA Monitoring & Breach Prediction
Data Lake
Virtual Resource Manager (VRM)
IIntelligent Slice & Service Management Optimizer Domain (ISSM-O)
Intelligent Network Slice and Service Optimization (NSSO)
loop
“1.a. Store radio and infra data”
“a1.b. Store radio and infra data”
Optimizes Services and Slices
“2. SLA_info_data or SLA_breach_prediction_info_data (a breach has been predicted)”
“3. Execution of codified business flow”
“4”. Query with the blueprint (i.e., intent)”
“5”. Candidate resources”
“6. Collect monitoring data”
“7. Perform high level optimization”
“8.a. Acquire resource (high level)”
“8.b. Acquire resource (high level)”
“9.a.. Local optimization (low level)”
“9.b. Local optimization (low level)”
“10.a. Instantiate optimization results”
"The rest of the process is shown in the trustworthy slice setup with 3rd party resources Workflow"
“10.b. Instantiate optimization results”
"The rest of the process is shown in the trustworthy slice setup with 3rd party resources Workflow"
Slice Optimized Across Domains

Figure 3-16: Intelligent Network Slice and Service Optimization

4 Matching to 5GZORRO Requirements

In this Section, the 5GZORRO Architecture is analysed to check how it fulfils the 5GZORRO requirements defined in D2.1 [1] and reviewed in this deliverable in Section 2.2.

Table 4-1: Smart Contracts for Ubiquitous Computing/Connectivity requirement's fulfilment analysis

ID	Type	Unique name/title	Requirement Priority	How it is Fulfilled
UC1.1	Business	Business Resource provider DLT management	MUST	Each Resource Provider must deploy a Marketplace Platform
UC1.2	Business	Business Resource provider onboarding	MUST	The Resource Provider onboarding is mainly supported by the Governance Management as well as by the Identity Management and Permissions Management functionalities as described in Section 3.13.1
UC1.3	Business	Marketplace Governance Model	MUST	The Marketplace Governance Model is managed by the Governance Management functionalities
UC1.4	Business	Marketplace Governance neutrality	SHOULD	The Governance Management exposes a highly abstract interface that is agnostic of the Governance Model
UC1.5	Business	Resource provider onboarding approval process	MUST	The Resource Provider onboarding is mainly supported by the Governance Portal and the Governance Management functionalities
UC1.6	User	Resource Provider registration action	MUST	The Stakeholder registration process is supported by the Marketplace Portal
UC1.7	User	Notifications about Resource Provider registrations process	MUST	The stakeholder is notified by using the Communication Fabric functionalities
UC1.8	System – Functional	Resource Provider registration information	MUST	The Resource Provider (and any 5GZORRO stakeholder, in general) uses the Marketplace Portal to provide the required information
UC1.9	System - Non-functional	Identity Management	MUST	Provided by the Identity Management and Permissions Management functionalities
UC1.10	System - Functional	User permissions	MUST	Provided by the Identity Management and Permissions Management functionalities
UC1.11	System - Functional	Resources tokenization	MUST	Provided by the Smart Contracts Lifecycle Management

ID	Type	Unique name/title	Requirement Priority	How it is Fulfilled
UC1.12	User	Resource registration action	MUST	Mainly provided by the Marketplace Portal and by the Resource & Service Offer Catalogue or by Zero touch enabled management functionalities including the Intelligent Network Slice and Service optimization
UC1.13	Business	Resources certification by regulators	COULD	Resources are certified by using the Governance Portal and the Identity Management and Permissions Management functionalities
UC1.14	System - Functional	Resource provisioning management	MUST	Mainly provided by the Resource & Service Offer Catalogue
UC1.15	User	Resource discovery action	MUST	Mainly provided by the Resource & Service Offer Catalogue
UC1.16	Business	Resource Consumers	MUST	Each Resource Consumer must deploy a Marketplace Platform
UC1.17	User	Service Offer Creation Action	MUST	Mainly provided by the Marketplace Portal and by the Resource & Service Offer Catalogue
UC1.18	System - Functional	Resource certification management	MUST	Resource certification are supported by the Identity Management and Permissions Management functionalities
UC1.19	System - Functional	Resource Definition Language	SHOULD	Provided by the Marketplace PortalRepositoryRepositoryRepositoryRepositoryRepositoryRepository
UC1.20	System - Functional	Resource Offer Approval	MUST	Mainly supported by the Smart Contract Life-cycle management and by the Identity Management and Permissions Management functionalities
UC1.21	User	Resource request	SHOULD	Provided by the Marketplace Portal
UC1.22	System - Functional	Resources request criteria	SHOULD	Provided by the Marketplace Portal
UC1.23	System - Functional	Resources Match	SHOULD	Provided by the Marketplace Portal and by the Resource & Service Offer Catalogue
UC1.24	System - Functional	Resources Match	COULD	Provided by the Smart Resource and Service discovery functionalities
UC1.25	System - Functional	Resources Match notification	SHOULD	Provided by Communication Fabric functionalities
UC1.26	System - Functional	Service Offer Smart Contract	MUST	Provided by the Smart Contracts Lifecycle Management
UC1.27	System - Functional	Service Offer Approval	MUST	Mainly supported by the Smart Contract Life-cycle management and by the Identity Management and Permissions Management functionalities

ID	Type	Unique name/title	Requirement Priority	How it is Fulfilled
UC1.28	System - Functional	Trusted Execution Environments	SHOULD	To be supported by TEE functionalities
UC1.29	System - Functional	Service Agreement	MUST	Mainly supported by the Smart Contract Life-cycle management and by the Identity Management and Permissions Management functionalities according to the Business Agreement DID Document
UC1.30	User	Stakeholder notifications	SHOULD	The parties involved in the agreement are notified by using the Communication Fabric functionalities.
UC1.31	System - Functional	Smart Contract SLA monitoring	MUST	Smart Contract SLA monitoring is mainly supported by the Smart Contract Life-cycle management and by the smart contract itself as well as by the Intelligent SLA monitoring & breach prediction functionalities. See the associated operational pattern in Section 3.93.9 for more details.
UC1.32	System - Functional	SLA breaches management	MUST	SLA breaches are managed by the Smart Contract Life-cycle management and by the smart contract itself as well as by the Intelligent SLA monitoring & breach prediction functionalities. See the associated operational pattern in Section 3.93.9 for more details.
UC1.33	System - Function	Stakeholder notifications	SHOULD	The parties involved in the agreement are notified by using the Communication Fabric functionalities.
UC1.34	System - Function	Licensing monitoring	MUST	To be provided by the e-Licensing Management functionalities
UC1.35	Business	Pricing Updates	COULD	Smart contracts update should be supported by the Resource & Service Offer Catalogue and by the Smart Contract Life-cycle management functionalities
UC1.36	System - Functional	Resource Definition Language licensing capabilities	MUST	Mainly supported by the Legal Prose Repository functionalities
UC1.37	Business	Token life-cycle management	MUST	To be supported by the Smart Contract Life-cycle management functionalities

Table 4-2: Dynamic Spectrum Allocation Use case requirement's fulfilment analysis

ID	Type	Unique name/title	Requirement Priority	How it is Fulfilled
UC2.1	User	Spectrum Market Authentication	MUST	Provided by the Identity Management and Permissions Management functionalities
UC2.2	User	Spectrum Market App Access (App/Browser)	MUST	Provided by the Marketplace Portal
UC2.3	User	Regulator Certification	MUST	Provided by the Regulator Stakeholder Verifiable Credential handled by the Identity Management and Permissions Management functionalities
UC2.4	User	Visualize own Spectokens and Smart Contracts	MUST	Mainly provided by the Marketplace Portal
UC2.5	System - Functional	Spectoken Creation	MUST	Mainly provided by the Resource Catalogue, the Spectrum Resource Management, the Identity Management and Permissions Management and the Smart Contract Life-cycle Management functionalities. For more details, see the Spectoken Resource Offer Publishing operational pattern at Section 3.2
UC2.6	System - Functional	Tracking DLTs	MUST	Mainly provided by the Smart Contract Life-cycle Management functionalities
UC2.7	System - Functional	Spectoken Trading	MUST	Mainly provided by the Marketplace Portal, the Resource Catalogue, the Spectrum Resource Management, and the Smart Contract Life-cycle Management functionalities. See the Trustworthy Smart Contract Setup for spectrum operational pattern at Section 3.4, for more details
UC2.8	System - Functional	Smart Contracts	MUST	Mainly provided by the Smart Contract Life-cycle Management functionalities
UC2.9	System - Functional	5GZORRO NB API	MUST	Mainly provided by the Radio Resource Management and the Network Slice and Service Orchestration functionalities
UC2.10	System - Functional	Slice Management Modules	MUST	Mainly provided by the Network Slice and Service Orchestration functionalities
UC2.11	System - Functional	Spectrum monitoring	MUST	Mainly provided by Intelligent SLA monitoring & breach prediction functionalities as well as by the Radio Resource Management
UC2.12	Business	SLA checking	MUST	Mainly provided by Intelligent SLA monitoring & breach prediction functionalities
UC2.13	System - Functional	Support for Oracles	MUST	To be provided by the Smart Contract DLT and the DID Admin agent to verify spectrum offer claims in its certificate.

ID	Type	Unique name/title	Requirement Priority	How it is Fulfilled
UC2.14	System - Functional	AI powered trading agents	WOULD	At this point there is no functionality to support this requirement. To be further analysed for the 2nd phase as a new functionality for the Analytics & Intelligence for AIOps logical plane
UC2.15	Business	Marketplace control	MUST	Mainly provided by the Resource Catalogue and the Identity and Permissions Management functionalities. See the Spectrum certificate generation operational pattern at Section 3.2, for more details
UC2.16	Business	Marketplace control	MUST	See how UC2.15 requirement is fulfilled
UC2.17	Business	Marketplace access control	MUST	Mainly provided by the Governance Manager and the Identity and Permissions Management functionalities
UC2.18	User	Marketplace access control (from app)	MUST	To be provided by the Identity and Permissions Management functionalities
UC2.19	System Functional	Application interaction with the Smart Contracts	MUST	To be provided by the Marketplace Portal and the Identity and Permissions Management functionalities
UC2.20	System Functional	DLT deployment	SHOULD	To be provided by the Smart Contract DLT
UC2.21	User	DLT deployment	MUST	To be provided by the Smart Contract DLT
UC2.22	User	Re-selling of spectrum	SHOULD	See how UC2.7 is fulfilled
UC2.23	User	Onboarding/ Request to register node	MUST	The Marketplace Platform includes a Smart Contract DLT node that must be deployed before a stakeholder can apply to be a member of the 5GZORRO Marketplace. See Section 3.13.1 for more details.
UC2.24	User	Onboarding / Permissions level	MUST	To be supported by the Stakeholder Verifiable Credential managed by the Identity and Permissions management functionalities.

Table 4-3: Pervasive vCDN Services Use case requirement's fulfilment analysis

ID	Type	Unique name/title	Requirement Priority	How it is Fulfilled
UC3.1	Business	Network slice request	MUST	To be mainly provided by the Service Catalogue, the Network Slice and Service Orchestration and the Smart Contract Life-cycle Management functionalities.
UC3.2	System-functional	Discovery process launch	SHOULD	To be mainly provided by the Intelligent Network Slice and Service optimization functionalities
UC3.3	System-Functional	3rd party resource intelligent selection parameters	SHOULD	To be mainly provided by the Intelligent Network Slice and Service optimization functionalities
UC3.4	System-functional	Service components migration	MUST	To be mainly provided by the Network Slice and Service Orchestration and the Virtual Resource Manager functionalities. See the Trustworthy Smart Contract Setup for edge computing operational pattern in Section 0 for more details.
UC3.5	System-functional	Register (CDN) resources	MUST	To be mainly provided by the Resource and Service Catalogue and the Virtual Resource Management functionalities.
UC3.6	System-functional	Instantiate/configure (CDN) resources	MUST	To be mainly provided by the Network Slice and Service Orchestration and the Virtual Resource Management functionalities.
UC3.7	System-functional	Fast resource deployment/migration	COULD	To be supported by the Network Slice and Service Orchestration and the Virtual Resource Management functionalities.
UC3.8	System-functional	Observable resource usage	MUST	To be supported by the Abstract Resource Management functionalities as well as by the Monitoring Data Aggregation functionalities
UC3.9	System-functional	Predictable resource overloading	MUST	To be supported by Intelligent SLA monitoring & breach prediction functionalities
UC3.10	System-functional	Excessive usage notification	MUST	To be supported Communication Fabric which endpoint should be defined in the Business Agreement DID Document.
UC3.11	System-functional	Rule-based scaling mechanisms	COULD	Can be supported by Smart Contracts Lifecyle Management, which will handle the contract between CDN and CSP that defines these rules, and the Intelligent Network Slice and Service optimization functionalities, which will apply the rules.
UC3.12	System-functional	Search for infrastructure resources	MUST	To be provided by Resource & Service Offer Catalogue functionalities

ID	Type	Unique name/title	Requirement Priority	How it is Fulfilled
UC3.13	System-functional	Intelligent selection of infrastructure resources	MUST	To be provided by Intelligent Network Slice and Service Optimization as well as the Smart Resource and Service Discovery functionalities
UC3.14	System-functional	Secure connectivity between CSP and 3rd party	MUST	To be provided by Inter-domain Communication Fabric functionalities
UC3.15	System-functional	Define requirements in Smart Contracts	MUST	To be provided by Smart Contracts Lifecycle Management functionalities
UC3.16	System-functional	Notification acceptance	MUST	To be provided by Network Slice and Service Orchestration functionalities
UC3.17	System-functional	Dynamic spectrum allocation	MUST	To be encapsulated by the Spectrum Resource Management functionalities.
UC3.18	System-functional	Extra spectrum bandwidth	MUST	To be provided by Intelligent Network Slice and Service optimization functionalities as well as the Resource and Service Offer catalogue
UC3.19	System-functional	Licensing schemes	MUST	To be supported by the Resource and Service Offer catalogue that will use the TMF poductOfferingPrice object to define the licensing schemes. The Legal Prose Repository will manage the smart contract templates in accordance with the licensing schemes associated.
UC3.20	System-functional	Licensing attestation	MUST	To be supported by e-Licensing Management functionalities
UC3.21	System-functional	Licensing system placement	MUST	To be supported by e-Licensing Management functionalities. As described in Section 2.4.13, an instance of the e-Licensing Manager agent is deployed in each operator domain.

5 Conclusions

This deliverable updates 5GZORRO Use Cases and Requirements, high-level reference architecture, its main functional blocks as well as the main operational flows between these functional elements. The updates of this specification include refinements and more detailed designs for the various services which incorporate decisions and feedback from phase 1 technical specification and implementation performed in WP3 and WP4.

This report is a critical input for phase 2 implementation cycle where more challenging new features are planned.

6 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 D3.1 – "Design of the evolved 5G Service layer solutions", Jan 2021

[4] 5GZORRO Consortium, Deliverable D4.1 – "Design of Zero Touch Service Mgmt with Security & Trust solutions", Jan 2021

[5] 5GZORRO Source Code GitHub Repositories - https://github.com/5GZORRO/

[6] ETSI SOL-006 Network Functions Virtualisation (NFV) Release 2; Protocols and Data Models; NFV descriptors based on YANG Specification - https://www.etsi.org/deliver/etsi_gs/NFV-SOL/001_099/006/02.07.01_60/gs_nfv-sol006v020701p.pdf

[7] ETSI, Zero-touch network and Service Management and Orchestration; VNF Descriptor and Packaging (ZSM); Means of Automation, GR ZSM 005 - V1.1.1, May 2020.

[8] 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

[9] 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

[10]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/

[11] 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/

[12] DID Communication. Available online: https://identity.foundation/working-groups/did-comm.html

[13] Operator Deployment and Management Pattern. Available online: https://kubernetes.io/docs/concepts/extend-kubernetes/operator/

[14] Ceph, https://ceph.io/

[15] Apache Spark – Unified Analytics Engine for Big Data, https://spark.apache.org/

[16] Apache Kafka – A distributed streaming platform, https://kafka.apache.org/

[17] Docker. URL: https://www.docker.com/

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

[19] Argo Workflows and Pipelines. URL: https://argoproj.github.io/projects/argo

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

[21] 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/

[22] MEF LSO Sonata APIs FAQ, v6, June 2020, URL: https://5growth.eu/wp-content/uploads/2019/11/D2.1-Initial_Design_of_5G_End-to-End_Service_Platform.pdf

[23] IBM CPLEX Optimizer, https://www.ibm.com/analytics/cplex-optimizer

[24] GUROBI Optimizer, https://www.gurobi.com/

7 Abbreviations

5G IA	5G Infrastructure Association
AIOps	Artificial Intelligence for IT operations
CNF	Cloud Native Function
DAG	Directed Acyclic Graph
DoA	Description of Action
DID	Distributed Identifier
DL	Deep Learning
DLT	Distributed Ledger Technology
EC	European Commission
Id&P	Identity and Permissions
IPR	Intellectual Property Rights
ISSM	Intelligent Slice and Service Management
LCM	Life-Cycle Management
MANO	Management and Orchestration
MEC	Multi-access Edge Computing
ML	Machine Learning
MDA	Monitoring Data Aggregation
NBI	Northbound Interface
NFV	Networks Function Virtualization
NFVI	Networks Function Virtualization Infrastructure
NFVO	Networks Function Virtualization Orchestrator
NS	Network Service or Network Slice depending on the context
NSSO	Network Slice and Service Orchestrator
NSM	Network Service Mesh
PPP	Public Private partnership
RSOC	Resource and Service Offers Catalogue
SBA	Service Based Architecture
SBI	Service Based Interface
SC	Smart Contract
SDO	Standard Developing Organization
SGX	Software Guard Extensions
SM	Service Mesh
TEE	Trust Execution Environment
VC	Verifiable Credential
VF	Virtual Function
VIM	Virtual Infrastructure Manager
VNF	Virtual Network Function
VNFM	Virtual Network Function Manager
VRM	Virtual Resource Management and Control
WG	Working group
WP	Work Package
ZSM	Zero Touch Service Management

<END OF DOCUMENT>