5G ZORRO

Grant Agreement 871533

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

D5.3: Business models and Validation of 5GZORRO security & trust framework

Intermediate version. Pending of EC revision. Do not cite

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: **871533**	Project Acronym: **5GZORRO**	Project title: **Zero-touch security and trust for ubiquitous computing and connectivity in 5G networks.**

Lead Beneficiary: **ATOS**	Document version: **v1.0**

Work package: **WP5 – Validation through Use Cases**

Deliverable title: **D5.3: Business models and Validation of 5GZORRO security & trust framework**

Start date of the project: **01/11/2019** **(duration 36 months)**	Contractual delivery date: **31.10.2022**	Actual delivery date: **11.11.2022**

Editor(s)
Esther Garrido (ATOS)

List of Contributors

Participant	Short Name	Contributor
Fundaciò i2CAT	I2CAT	Shuaib Siddiqui, Miguel Catalán-Cid, Adriana Fernández, Javier Fernández
Nextworks	NXW	Erin E. Seder, Pietro G. Giardina, Michael De Angelis, Juan Brenes, Giacomo Bernini
Universidad de Murcia	UMU	José María Jorquera Valero, Manuel Gil Pérez, Gregorio Martínez Pérez, Pedro Miguel Sánchez Sánchez
Intracom Telecom	ICOM	Marinela Mertiri
ATOS	ATOS	Esther Garrido, Guillermo Gómez
Malta Communications Authority	MCA	Antoine Sciberras, Andrew Caruana, Charlo Baldacchino, Jean-Marie Mifsud
University Carlos III of Madrid	UC3M	Borja Nogales
Ubiwhere	UW	Pedro Teixeira
IBM Israel Science and Technology	IBM	Katherine Barabash
Telefonica Innovacion y Desarrollo	TID	Andra Lutu, Diego López

List of Reviewers

Participant	Short Name	Contributor
Intracom Telecom	ICOM	Marinela Mertiri
IBM Israel Science and Technology	IBM	Katherine Barabash
Nextworks Srl	NXW	Giacomo Bernini

Change History

Version	Date	Partners	Description/Comments
0.0	15.07.2022	ATOS	Initial Table of Content with assignments
0.1	30.09.2022	ATOS, MCA, TID, IBM, NXW, I2CAT, ICOM	Inclusion of first draft contribution
0.2	09.10.2022	ATOS, MCA, TID, NXW,	Inclusion of second draft contribution

		I2CAT, ICOM, FBK, UMU, UC3M, UW	
0.3	28.10.2022	ATOS	Document ready for peer review
0.4	30.10.2022	ICOM, IBM	Peer review
0.5	07.11.2022	ATOS, MCA, TID, IBM, NXW, I2CAT, ICOM, FBK, UMU, UC3M, UW	Inclusion of final contribution and comments review
0.6	9.11.2022	NWX	Technical Review
0.8	11.11.2022	ATOS	Document ready for quality review
1.0	11.11.2022	I2CAT	Document review and 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

Nowadays, the consolidation of digitalization across all sectors and the impact of the societal changes, mainly driven by the Covid19 pandemic, have pushed the demand for network services beyond expectations. In this context, 5GZORRO vision has been not only to provide an enhanced connectivity layer for telcos to address this demand, but also to be a driver of the digital transformation, creating new market opportunities for all players embracing it. In the 5G/Beyond 5G era, 5GZORRO is aware that there is a growing need for telco resources, due to new envisioned use cases and new actors entering the ecosystem, who do not always have easy access to these specific resources.

The focus of 5GZORRO has been to create a platform to optimise available network resources, including spectrum, and to establish 5G services in an easy, flexible, automated, secure, and trustful manner. Moreover, as the consortium aims at kicking off a vibrant ecosystem around the platform, it has dedicated an entire project work package to demonstrate its feasibility and applicability. The work conducted has demonstrated that the 5GZORRO platform is viable because it is validated from a technological point of view and, also very importantly, it is legally compliant. From a business perspective, we conclude that 5GZORRO platform is marketable since it solves stakeholders' real problems with a limited investment.

To demonstrate that the platform is technically feasible, the consortium has defined three different use cases that leverage on the 5GZORRO platform in two integrated testbed settings: 5GBarcelona and 5TONIC. The 5GZORRO technologies have been deployed here and have been tested in different scenarios related to Smart Contracts for Ubiquitous Computing/Connectivity (UC1), Dynamic Spectrum Allocation (UC2) and Pervasive vCDN Services (UC3). Key UC requirements and KPIs have been defined for each scenario, as well as tests pre-conditions, steps and results, concluding that 5GZORRO platform meets the technical requirements necessary to operate properly. Tests have been done also around the requirements for the Global Operator concept, mapping it with the 5GZORRO framework and envisioning two different approaches for 5GZORRO global coverage (per-country 5GZORRO Marketplace instance and international 5GZORRO Marketplace with coordination), finally identifying challenges for future work. Besides, to facilitate the exploitation and usage of the 5GZORRO platform, this deliverable gives the necessary configurations for the different participant profiles (Cross-domain platform profile, Administration profile, Trader profile, Consumer profile, Regulator profile) and points out to a set of deployment scripts following the "Infrastructure as Code" paradigm for the platform deployment and provisioning, also detailing the dynamic bootstrapping of a new operator and the integration within the ecosystem.

To address the legal validation of the platform, the consortium has investigated European regulation that deals with electronic communication services and frequency spectrum, concluding that 5GZORRO promotes the development of a freely competitive market but also implements those necessary controls to allow for the oversight and intervention of the spectrum regulator. The 5GZORRO platform implements advanced business logic, AI and distributed ledger techniques to enable a marketplace where 5G-related resources can be traded securely amongst diverse but trusted stakeholders, based on market-driven business models to meet dynamic supply and demand. Contributions towards standardisation activities also position the 5GZORRO Marketplace well in relation to compliance on the relevant legal aspects explored through this legal validation.

Finally, the consortium has demonstrated the economic feasibility of the 5GZORRO platform to ease the adoption of 5GZORRO propositions. For assessment of the business model associated with running the 5GZORRO platform in different contexts (the UCs), partners have used the Value Proposition and Business Model Canvas templates. The problems and needs of related stakeholders have been highlighted, which mainly relate with the total cost of ownership, cumbersome tasks and the lack of trust among these parties. It has become evident that the 5GZORRO platform, with its different functionalities, can alleviate these challenges, thus helping us in the definition of 5GZORRO unique selling point. The consortium has

also reflected about the different activities needed to operate the platform and deliver 5GZORRO proposition, demonstrating that a profitable business can emerge from 5GZORRO project results, as costs are maintained below revenues in the different scenarios envisaged. Calculations have been made based on the configuration and setup of our project results, i.e., a prototype that is technical and legally feasible, but also acknowledging our competitive advantage when making projections. The fact that we have started exploitation activities with an early adopter that is part of the consortium (Malta Communications Authority), evaluating the set of functionalities needed to start operating the platform and create a minimum viable product (see deliverable D6.5 [1]), gives us indeed the confidence that 5GZORRO will enable cross-sector opportunities and open innovation for multiple parties.

1. Introduction

Deliverable D5.3 aims at giving an overall feasibility analysis of 5GZORRO platform from various perspectives: technical, legal and economic. It encompasses work from tasks T5.1, T5.2 and T5.3 (for the technical validation of the three Use Cases - UCs) and from task T5.4 (for the legal and economic validation of the platform).

As such, it contains the updated diagrams representing how the different components are deployed in the two project's testbeds: 5TONIC and 5GBarcelona, so that the validation of 5GZORRO architecture in three representative UCs can be performed. The configuration of the testbeds is directly linked with the set of validation tests defined for each of these UCs, for which, final results are also included in this deliverable as a conclusion of initial and intermediate results already delivered in D5.1 [2] and D5.2 [3]. For this reason, and for the sake of comprehensibility and completeness of this final validation document, some parts of these deliverables related to technical tests may be included also in the document at hand.

In close collaboration with WP6, the economic validation carried out in the framework of task T5.4 has analysed the possibilities of the 5GZORRO platform for a potential commercial exploitation, both internally by one or more project's partners as well as by third parties. As such, the market analysis conducted in task T6.3 has been very relevant in the economic validation in order to understand the context, reinforce the value proposition and make projections. Task T5.4 has, in turn, given input to task T6.3, as the validation of the platform has helped partners to identify business opportunities, like the dynamic spectrum trading setting in MCA premises to facilitate spectrum trading in the Maltese telecoms market or the plans for exploitation of the 5GZORRO Marketplace applied to the Global Mobile Network Aggregators concept, also described in this document. Besides, the business model and techno-economic analysis performed in task T5.4 has been a needed first reflection for the exploitation roadmap in task T6.3.

The other important part of the feasibility study has been the legal validation. Understanding how 5GZORRO platform is compliant with regulatory aspects on spectrum, blockchains, security and Artificial Intelligence (AI) has required the close monitoring of all these aspects. This is a fundamental step in order to facilitate a smooth adoption of the 5GZORRO system by all targeted stakeholders.

It is worth highlighting that part of the input used for the general validation of the platform has been collected from the targeted stakeholders through a survey designed for 5GZORRO and launched in January 2022 "Towards a dynamic marketplace for 5G resources".

1.1. Document outline

After this brief Introduction, that describes the purpose and vision of the document, this deliverable is structured in the following way:

Section 2 is dedicated to the technical validation of the overall 5GZORRO solution. First of all, the configuration of the two testbeds is given, followed by details of the final tests performed in the context of the three UCs. One additional subsection is devoted to the automated deployment of the platform, describing how the platform components are deployed depending on the profile and usage of the platform and pointing to the instructions available on the project GitHub. Additionally, we also provide a validation approach for integrating the marketplace functionalities in support of the Global Operator model, an exploitation path that some of the project's partners are exploring.

Section 3 is about the legal framework in relation to the different technologies underpinning the platform and how these comply with European regulatory aspects.

Section 4 contains all the work done to economically validate the 5GZORRO solution, the methodology followed and the results of its validation. Definition of the value proposition of 5GZORRO platform for the different configurations and stakeholders, business model canvas and techno-economic analysis are also provided.

After the conclusions in Section 5, we present in Annex I the input collected through the survey designed specifically to gather feedback from the targeted stakeholders, entitled "Towards a dynamic marketplace for 5G resources"

2. Technical Validation

This section focuses on the validation of the technical performance of the 5GZORRO platform applied in the three different proposed service settings, i.e., the UCs. The main aspects of this validation are the discovery of multi-party resources, the composition of slices across multiple infrastructures and providers, the evaluation of mechanisms for establishing zero-touch security and trust services, the testing of the spectrum sharing functionality and the testing of inter-operator analysis and monitoring for advanced and intelligent SLA management.

2.1. 5GZORRO Testbeds

To validate the proposed 5GZORRO architecture, three UCs were designed. These UCs defined the requirements for the different testbeds. In 5GZORRO, two testbeds have been setup, one in Barcelona (5GBarcelona) and one in Madrid (5TONIC).

These testbeds share some components. These are the 5GZORRO shared components (as for example the Datalake, Intelligent SLA Breach Prediction (ISBP) or the DLT network), which now are hosted at the 5GBarcelona testbed, but could also be hosted by an independent third party. That is possible because both testbeds are interconnected. Such interconnectivity not only allowed to have shared components, but enabled different scenarios, in which the true cross domain nature of 5GZORRO is showcased.

The following subsections describe in more detail what has been deployed in each of the testbeds as well as the updates with respect to previous deliverables.

2.1.1. 5GBarcelona Infrastructure for 5GZORRO

The 5GBarcelona testbed features two different virtual infrastructures, one hosting the platform and a second one where services are instantiated.

The platform has been deployed on top of a virtualized infrastructure, managed by a Virtual Infrastructure Manager (VIM). The project has selected OpenStack as VIM, a widely deployed open-source software for cloud deployments. In 5GBarcelona, OpenStack [55] has been deployed in a High Availability configuration, deployed over 5 physical servers. With the same virtual infrastructure, we can accommodate the developers' preferences, in terms of target for their components, whether they prefer to use virtual machines or containers managed by Kubernetes (k8s) [56].

5GBarcelona´s OpenStack hosts tens of virtual machines. Some are deployed to host 5GZORRO components directly as pure virtual machines, while others are used to host k8s nodes that form clusters in which other 5GZORRO components are deployed. The platform hosts a total of 3 k8s clusters (pltcmp cluster, DLT cluster and Datalake cluster)

Note that, as mentioned previously, there are certain components that are shared by both testbeds and these include the distributed DLT network, a common Datalake, ISBP and Smart Resource and Service Discovery (SRSD). The consortium decided that these will be hosted in the Barcelona testbed, but they could be hosted anywhere else, as for example in a third party infrastructure.

The other part in the infrastructure of the testbed, is where stakeholder´s services are deployed. For that purpose, another OpenStack instance has been deployed, this time over a single server. That OpenStack hosts several tenants and virtual machines deployed by the different stakeholders for the UCs.

Lastly, the radio equipment is connected to both virtual infrastructures, the infrastructure where the 5GZORRO platform runs and the infrastructure in which the services are deployed. In particular, the Barcelona testbed makes use of an Amarisoft Callbox Pro equipment [57], which acts as a 3GPP compliant eNB/gNB by means of Software-Defined Radio (SDR) technology and is able to provide up to 6 simultaneous radio cells operating at different frequencies and bands. On the infrastructure where we have the platform, we have deployed the radio controller which will configure the radio part as required by the different UC scenarios. The other infrastructure that the radio equipment is connected to, is the infrastructure used by stakeholders to deploy their services. As an example, in the case of 5G, the required 5G Core (virtual) instances get deployed in the infrastructure where the rest of the services get deployed and needs to be connected to the radio equipment.

Figure 1 below depicts the up-to-date configuration and setup for the 5GBarcelona testbed.

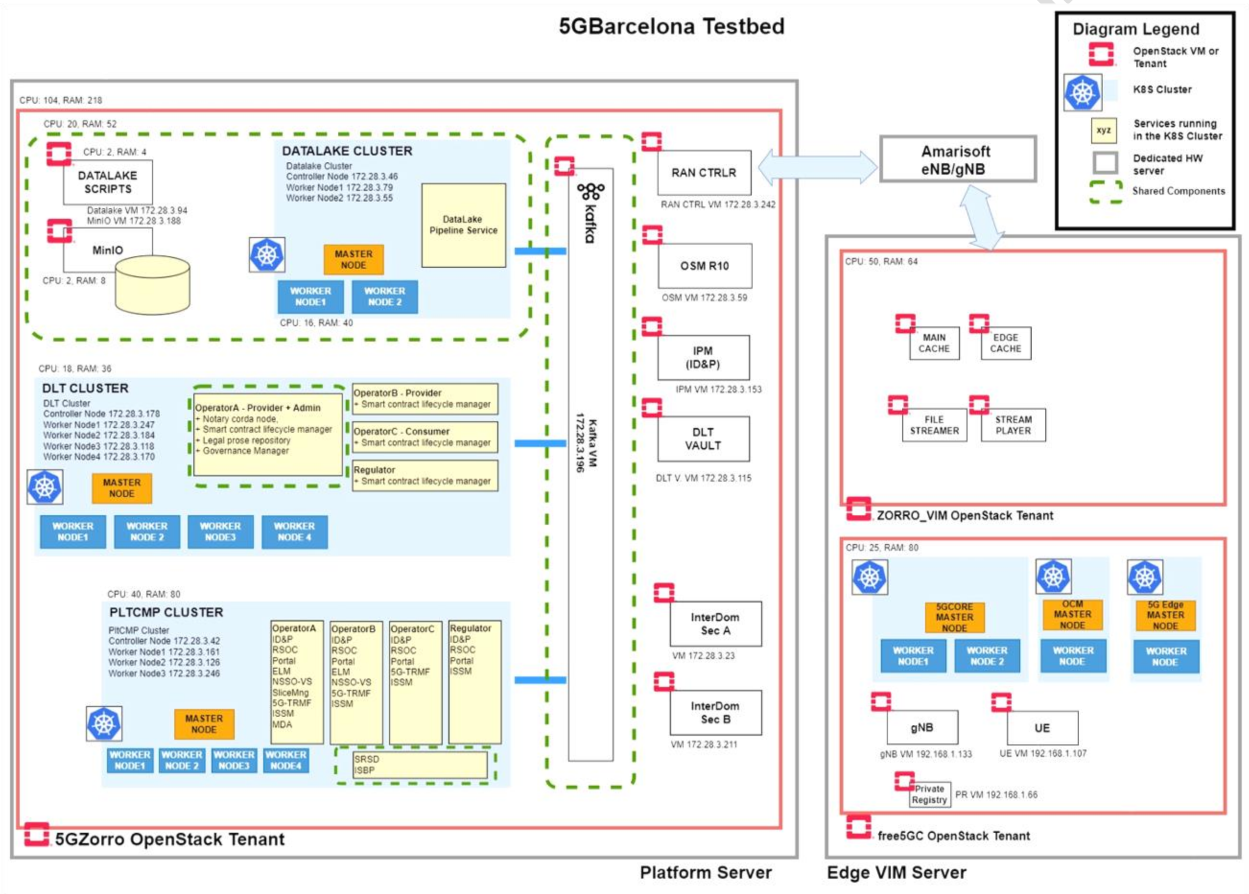


Figure 1: Overview of 5GBarcelona testbed configuration

2.1.2. 5TONIC Infrastructure for 5GZORRO

The 5TONIC testbed, as well as the resources made available under the context of the project, have not been altered with respect to the description available in D5.2 [3]. As already outlined, the testbed includes two OpenStack-implemented NFVIs, supporting the resource allocation and isolation for different purposes (*e.g.*, the deployment of the 5GZORRO platform modules) through their multi-tenancy capacity.

In addition to these resources, and with the aim of supporting the deployment of functionalities under a Trusted Execution Environment (TEE), the 5TONIC testbed incorporated a device with Intel Software Guard Extensions (SGX) support (more details in this regard in D4.1 [4]). The computational resources of this device are listed in the following table.

Table 1: Computational resources of device supporting TEE

	TEE Device Resources
Model	Intel NUC 10
CPU	Intel Core i7 10th Generation 10710U (6 cores)
RAM	64 GB DDR4
Storage	1 TB SSD
Network Connections	1 Gigabit Ethernet; 802.11b/g/n/ac/ax

On the other hand, and after being utilized to evaluate the portability of the platform (deploying the logical components of the 5GZORRO platform by replicating the design and implementation principles defined in an initial phase for the 5GBarcelona testbed), the 5TONIC testbed has been updated in this last stage of the project to accommodate the execution and development of the use cases (elaborated further in this document) defined within the scope of the project.

The 5TONIC testbed update consisted mainly in the deployment and configuration of the logical components of the 5GZORRO platform required by each of the UCs, as well as the creation of a new tenant to allow the deployment and configuration of a core 5G network using the free5Gc open-source tool [5]. In this aspect, the VPN service, available in 5TONIC, plays an important role, allowing to, on the one hand, enable the access to the module owners to carry out the appropriate configurations into the 5GZORRO platform modules; and on the other hand, enable the modules deployed on the testbed to interoperate with the shared components, deployed in 5GBarcelona (as mentioned above). Figure 2 illustrates graphically the updates addressed in the 5TONIC testbed.

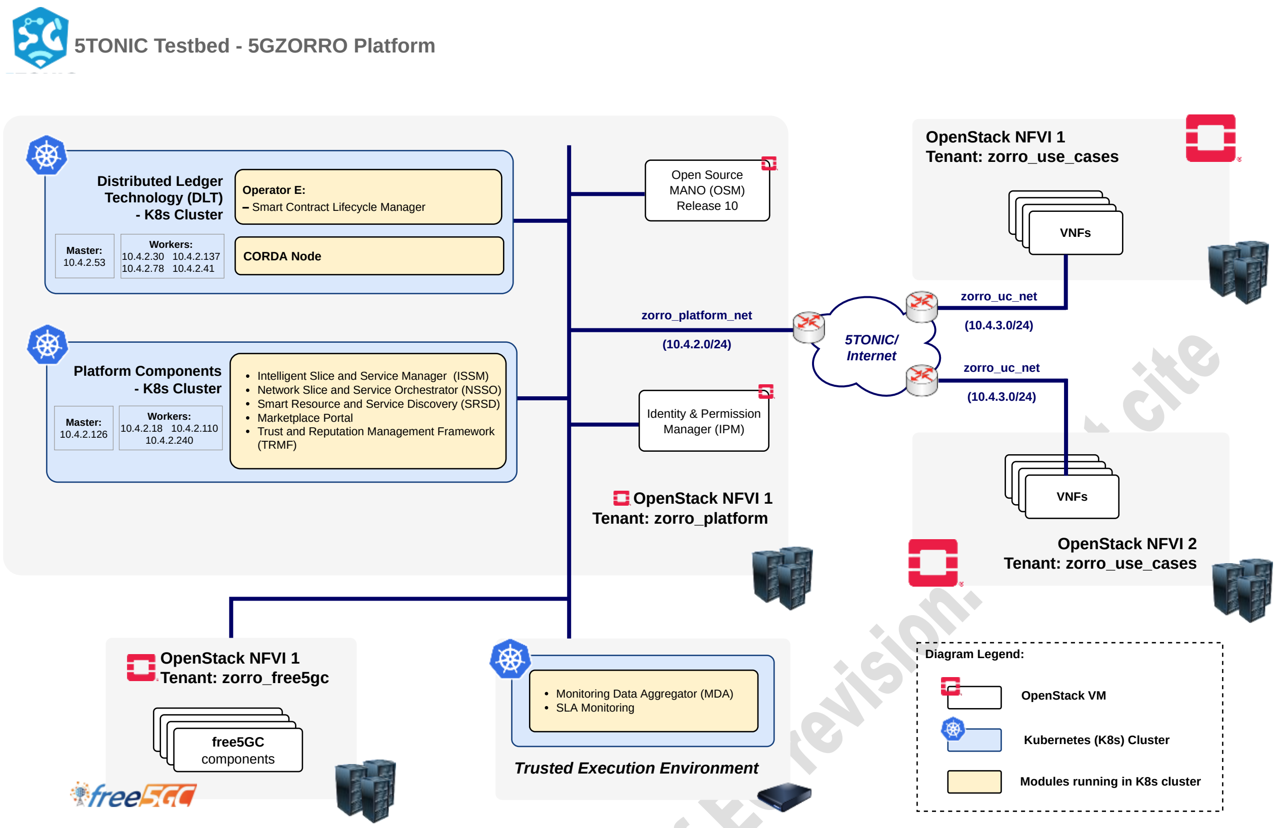


Figure 2: Overview of the logical components at 5TONIC testbed

2.2. UC1: Smart Contracts for Ubiquitous Computing/Connectivity

2.2.1. Description

As described in the previous WP5 deliverables, UC1 is focused on the leasing of resources between potentially distrusting/competing stakeholders, the associated commercial agreements that arise from this, and how their lifecycles are governed in a decentralised manner. The 5GZORRO decentralised marketplace has a number of stakeholders that may deploy varying ‘flavours’ of the platform depending on their desired role and associated required functionality. **¡Error! No se encuentra el origen de la referencia.** describes the stakeholders involved in the 3 scenarios of UC1. A full description of the anticipated stakeholder roles can be found in D2.1 [6].

The use case scenario used in the tests and demonstrations of UC1 involves an Automotive Vertical which uses the 5GZORRO Platform to lease an E2E service comprised of resources from multiple Providers, see Figure 3. The purpose of the service is to obtain the resources needed to make Over-the-air (OTA) updates on 5G-enabled cars while in remote storage. Specifically, Operator C builds an E2E service upon assets acquired from Operators a and b:

- 5G Core and RAN from Operator a
- 5G Edge (UPF) and OTA APP VNF (Firmware Update Agent) from Operator b

The Automotive Vertical (Operator e) acquires the E2E Service from Operator c. The scenario spans both tests beds, with Operators a, b, and c located in 5GBarcelona, and Operator e in 5TONIC, as shown in

Figure 4. Demonstrations of this scenario can be seen in the video "5GZORRO Final Event 2022 Demo 1 - Michael De Angelis, Nextworks" [8].

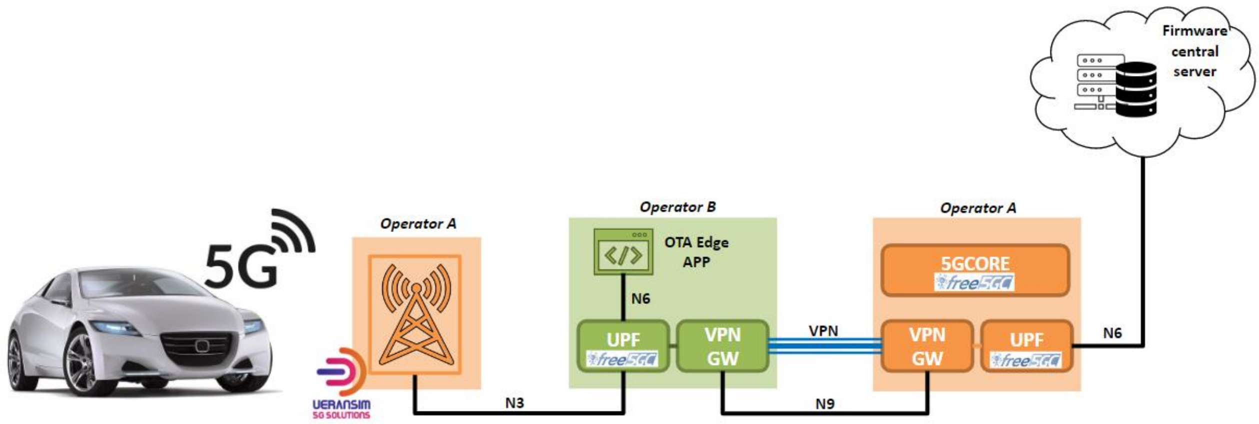


Figure 3 UC1 testing scenario

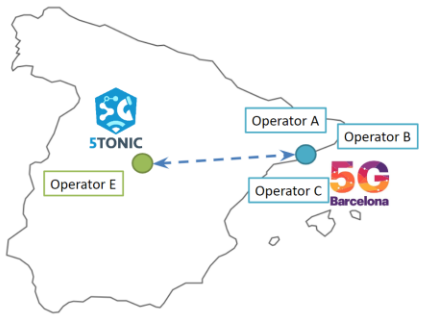


Figure 4 Location of Stakeholders of UC1

Table 2: Stakeholders involved in the scenarios of UC1

Stakeholder	Stakeholder Description	Roles
Operator A	Stakeholder with platform components deployed to support governance and trading functions	Resource Provider Governance Admin
Operator B	Stakeholder with platform components deployed to support trading functions	Resource Provider
Operator C	Stakeholder with platform components deployed to support trading functions	Resource Consumer Service Provider
Vertical (Operator E)	Consumer of the service	Service Consumer

2.2.2. Use Case 1 scenarios

The scenarios identified in D5.1 [2], and reported in the following sections, are designed to simulate the various permutations around the Communications Service Providers (CSP) being able to meet the needs of their customer. As described in D5.2 [3], this is namely the utilisation of the 5GZORRO Marketplace to procure resources and services that the CSP does not have in its portfolio, to offer a complete service to its customers. The goal of the scenarios is to demonstrate the trust and autonomy that underpin the 5GZORRO Marketplace, achieved through the utilisation of smart contracts and distributed ledger. Table 3 lists the tests reported in this deliverable (according to the test plan reported in D5.1 [2]) along with updated descriptions in view of the final 5GZORRO platform prototypes. The relevant project KPIs, defined in D5.1 [2], are also reported for each test.

Table 3: List of UC1 tests with results in D5.3

Original tests in scope of D5.3	Updated Tests	Applicable Scenario
Test UC1.6a Approval of an Agreement Legal Prose Template	This test has been merged into UC1.7 and UC1.8 for the two types of supported Legal Prose Templates	n/a
Test UC1.6b Approval of an Agreement Legal Prose Template including multiple service providers	This test has been merged into UC1.7 and UC1.8 for the two types of supported Legal Prose Templates	n/a
Test UC1.7a Approval of an SLA Legal Prose Template	Creation of an SLA Legal Prose Template, approval is implicit	Scenario 1.1: Slice composition from a single provider
Test UC1.7b Approval of an SLA Legal Prose Template including multiple service providers	Creation of an SLA Legal Prose Template including multiple service providers, approval is implicit	Scenario 1.2: Slice composition from multiple providers
Test UC1.8a Approval of a licensing agreement template	Automatic filling of an eLicense template	Scenario 1.1: Slice composition from a single provider
Test UC1.8b Approval of a licensing agreement template including multiple service providers	Automatic filling of an eLicense template for a composite Offer including multiple service providers, approval is implicit	Scenario 1.2: Slice composition from multiple providers
Test UC1.9a Agreement creation template	This test has been merged into UC1.15	n/a
Test UC1.9b Agreement creation template including multiple service providers	This test has been merged into UC1.16	n/a
Test UC1.10a SLA creation	This test has been merged into UC1.7	n/a
Test UC1.10b SLA creation including multiple service providers	This test has been merged into UC1.7	n/a
Test UC1.11 Product Offer creation	Unchanged	Scenario 1.1: Slice composition from a single provider
Test UC1.12 Multi provider Product Offer creation	Unchanged	Scenario 1.2: Slice composition from multiple providers
Test UC1.14a Intelligent resource discovery query by Resource Consumer	Unchanged	Scenario 1.1: Slice composition from a single provider

Test UC1.14b Intelligent resource discovery query by Resource Consumer including Offers from multiple Providers	Unchanged	Scenario 1.2: Slice composition from multiple providers
Test UC1.15 Resource Consumer purchases a Product Offer	Unchanged	Scenario 1.1: Slice composition from a single provider
Test UC1.16 Resource Consumer purchases multiple Product Offers from multiple provider	Unchanged	Scenario 1.2: Slice composition from multiple providers
Test UC1.17 SLA Breach detected	This test is a copy of a test in UC2 (section 2.3.4.2)	Scenario 1.3: Slice Lifecycle Management with analytics
Test UC1.18 Scaling action is attempted and blocked	This test is a copy of a test in UC3	Scenario 1.3: Slice Lifecycle Management with analytics
Test UC1.19 Agreement termination	Unchanged	Scenario 1.3: Slice Lifecycle Management with analytics
Test UC1.20 SLA Breach prediction	This test has been conducted in UC3 (section 2.4.2.1)	Scenario 1.3: Slice Lifecycle Management with analytics

2.2.2.1. Scenario 1.1 and 1.2: Slice composition tests

In Scenario 1.1, a Resource Consumer/Service Provider leases a set of resources from a single Resource Provider to create multi-resource services in the Marketplace. This represents the base scenario for the use case, demonstrating marketplace utilisation to support multi-resource slice establishment backed by a smart contract bi-lateral agreement and associated SLAs.

As an extension of Scenario 1.1, in Scenario 1.2 a Resource Consumer/Service provider leases a set of resources and services from multiple Resource Providers in order to compose the required service to meet the needs of the vertical customer. This represents multi-party and multi-resource slice establishment supported by smart contracts and associated SLAs and eLicenses. A full description of the test Scenarios can be found in D5.1 [2].

The following sections report the findings for the UC1 tests associated with these two scenarios not previously reported in D5.2 [3].

2.2.2.1.1. Creation of an SLA Legal Prose Template Test

The tests of the creation of an SLA Legal Prose Template, **UC1.7a/b**, involve the uploading of an SLA template file, shown in Figure 55, to the Platform for use in the creation of an SLA to be attached to a Product Offer. The test includes using the template to create an SLA and attaching the SLA to a Product Offer.

For UC1.7a, a single SLA template (*availability_template.zip*) is created by Operator A and used to create an SLA (*core_availability*) which is attached to a Product Offer (*OTA demo eucnc core*) of Operator A. For 1.7b, the template is used by Operator B to create an SLA which is attached to a different Product Offer (*OTA demo eucnc edge*) associated with Operator B. Figure 66 - Figure 99 demonstrate the testing process.

SLA Template
[...] SLA {{name}}

```
**Version:** 1.0

This SLA is valid between **{{startDateTime}}** and **{{endDateTime}}**.

### Named Parties

SLAProvider: **{{stakeholderName}}**

**{{description}}**

In the event of a conflict between the terms of this SLA and the terms of any other agreement with the named SLAProvider governing your use of the Service (the 'Agreement'), the terms and conditions of this SLA apply, but only to the extent of such conflict. Capitalized terms used herein but not defined herein shall have the meanings set forth in the Agreement.

## Service Commitment

The named SLAProvider will use commercially reasonable efforts to [...]. In the event a Service does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

## Service Credits

Service Credits are calculated as a percentage of the total charges paid by you for the applicable Service for the billing cycle in which [...].

The following rules are used to check if there is a service breach associated with the metric under analysis. The "operator" defines when a value is considered a violation (operator options: greater than or equal ".ge"; greater than ".g"; equal ".e"; less than ".l"; less than or equal ".le"):

1. A  **{{metric}}**(**{{unit}}**) value becomes a breach when it is **{{operator}}** than **{{referenceValue}}** plus **{{tolerance}}**.

We will apply any Service Credits only against future payments otherwise due from you for the Service. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the Service did not meet the Service Commitment. Service Credits will not entitle you to any refund or other payment from the named SLAProvider. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the Order Agreement, your sole and exclusive remedy for any unavailability, non-performance, or other failure by us to provide the Service is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

## SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension or termination of the Service, or any other Service performance issues: (i) caused by factors outside of our reasonable control, including any force major event or Internet access or related problems beyond the demarcation point of the Service; (ii) that result from any actions or inactions of you or any third party; (iii) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); or (iv) arising from our suspension or termination of your right to use the Service in accordance with the Order Agreement (collectively, the "SLA Exclusions").

## Definitions
- A "Service Credit" is a dollar credit, calculated as set forth above, that we may credit back to an eligible account.
```

Figure 5: SLA template file availability_template.zip. Source: [7]

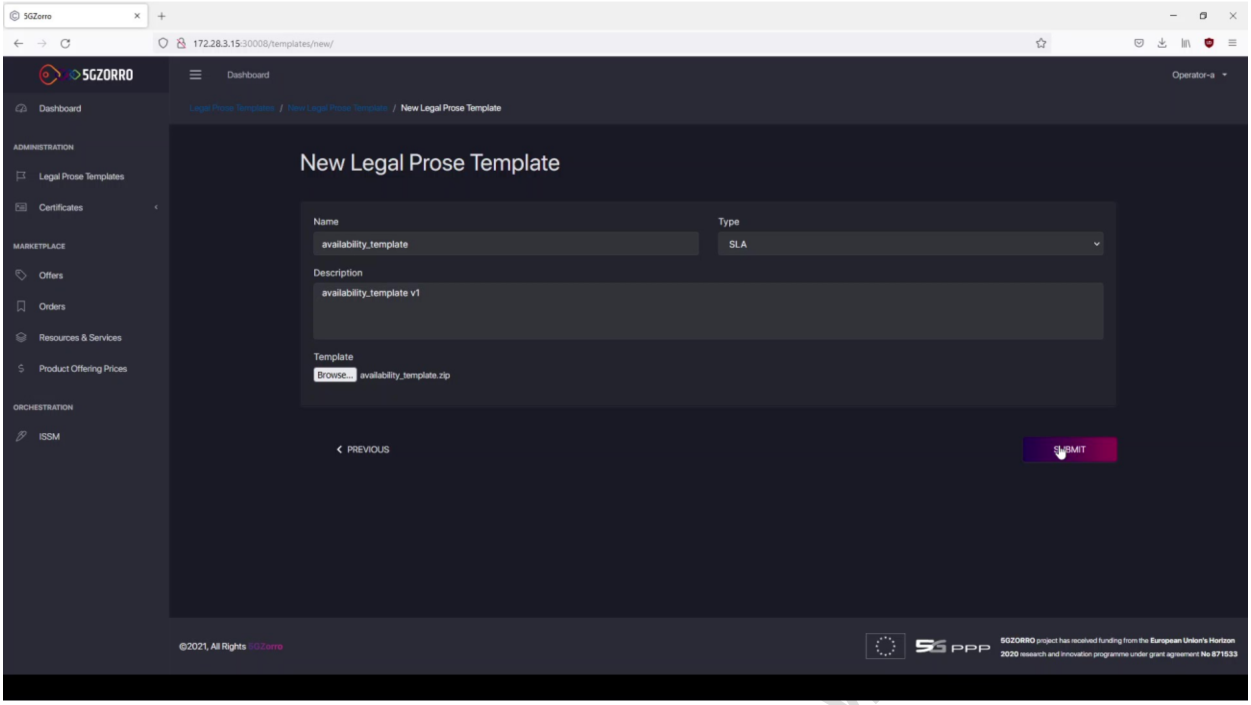


Figure 6: Uploading an SLA Template file to the Platform to create an SLA template object (availability_template)

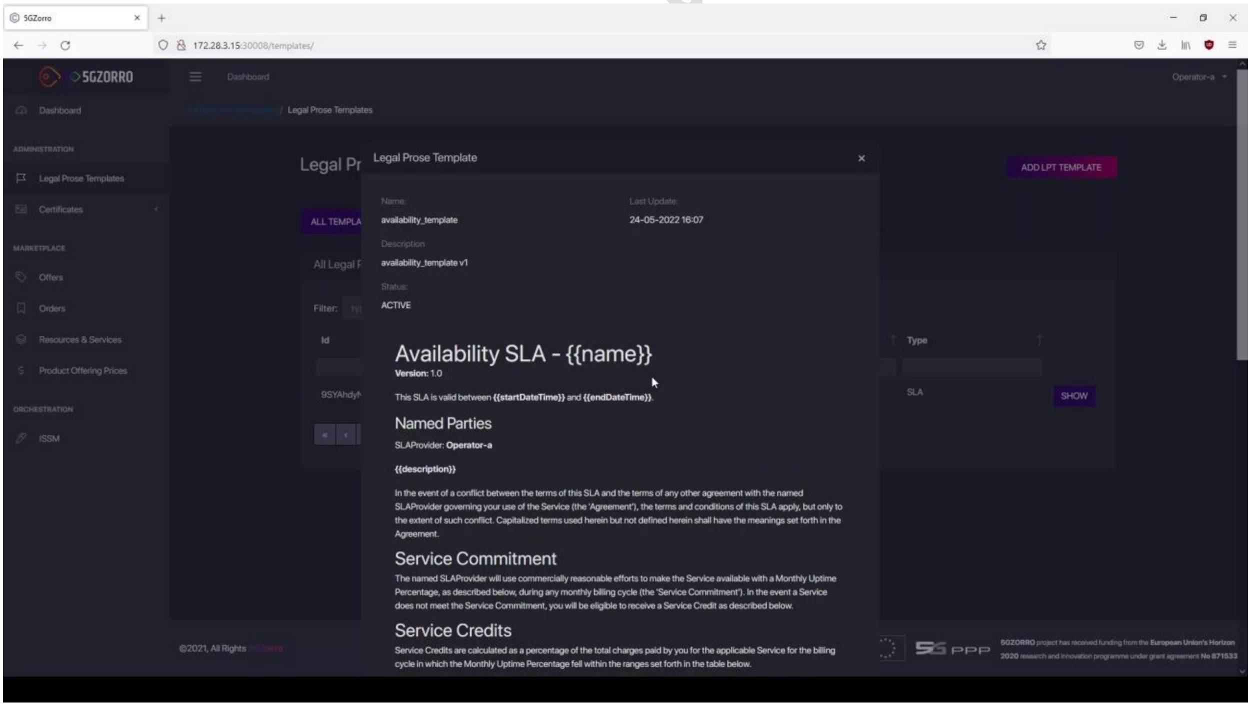


Figure 7: The SLA template (availability_template) can be viewed on the Portal

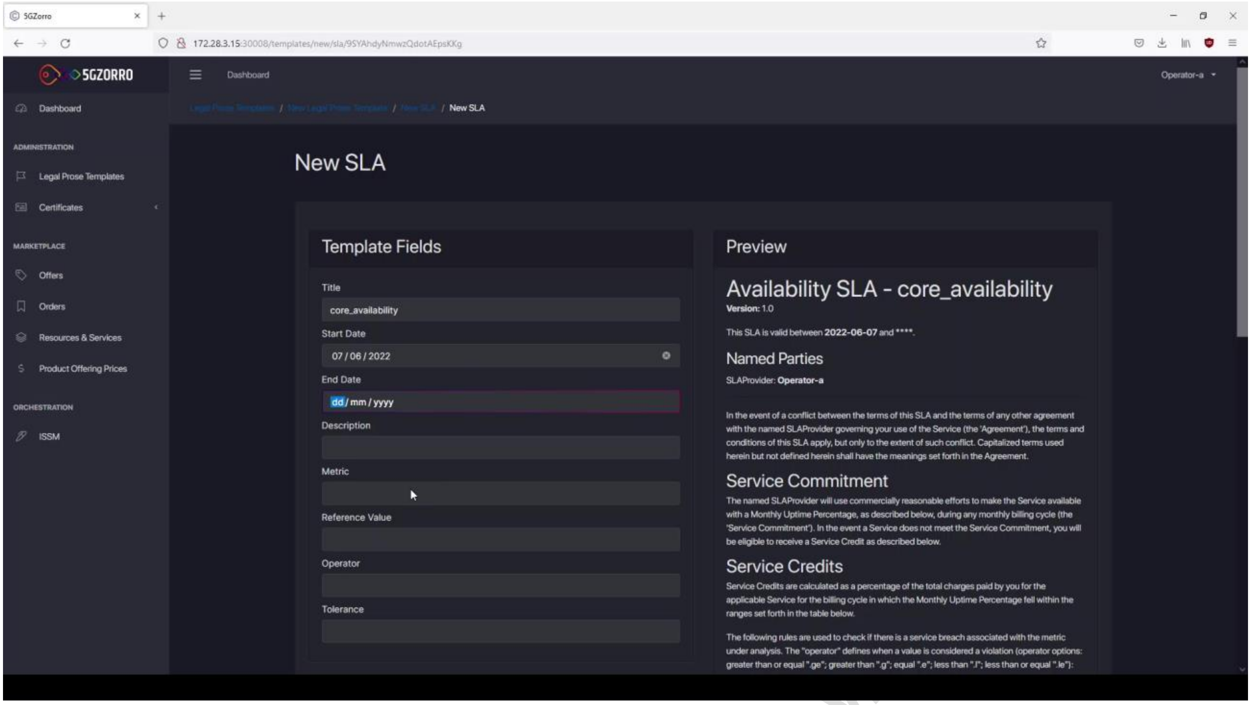


Figure 8: The SLA template (availability_template) can be filled through the Portal to create an SLA (core_availability)

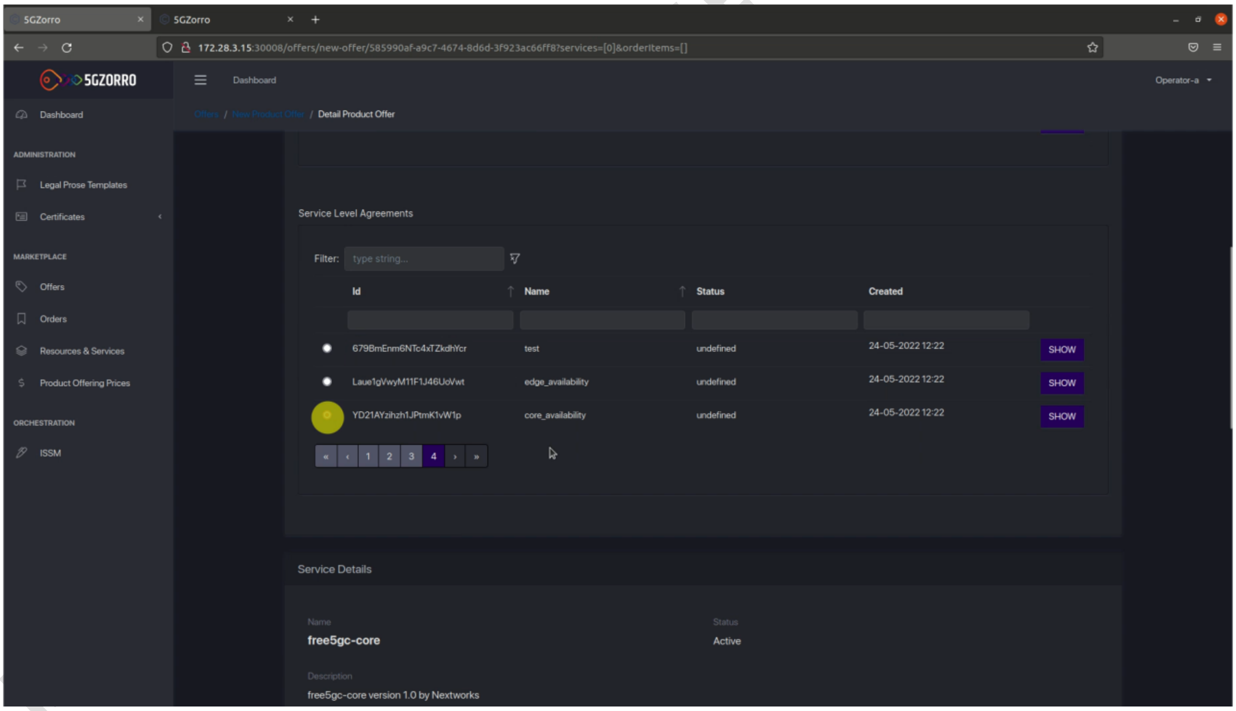


Figure 9: Selecting the SLA (core_availability) to attach to a Product Offer

Table 4: Creation of an SLA Legal Prose Template

UC1.7	**Creation of an SLA Legal Prose Template**
Testbed	5GBarcelona
Description	Service Provider uploads an uptime SLA Legal Prose Template, the template is then used to create an SLA and attached to an Offer

Use-case functionalities	Resource Provider creating a Resource Offer Service Provider creating a Service Offer	
Key Use-case requirements and KPIs	**[KPI3.1]** 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. **[KPI4.1]** Automatically discover and "inventorize" various types of resources (i.e., compute, storage, network at core, edge, far-edge), spectrum and services capabilities from different domains and service providers **[KPI4.2]** Implement/correlate technical service configurations and SLA monitoring interactions between multiple parties.	
Components	Identity & Permissions Manager Governance Manager Legal Prose Repository Marketplace Portal Governance Portal	
Test Procedure	Pre-conditions	The Service Provider has been onboarded onto the Portal
	Test Case steps	The SLA template (Figure 55) is uploaded to the Platform (Figure 66). The template is assigned with a unique ID and is accessed through the Portal and the contents are reviewed (Figure 77) and used for creating an SLA (Figure 8). The created SLA is filled and attached to an Offer (Figure 99)
Measurements	Methodology	video and screenshots
	Complementary measurements	none
	Calculation process	Observation from the Portal
Result	**[KPI3.1]** The KPI target was set as Smart Contract for 3 or more untrusted parties. The SLA is an integral part of the Smart Contract. In this test, Operator A attaches an SLA agreement to their respective Offer, to be purchased by Operator C in later tests (UC1.12 and UC1.16) and used to create a Composite Offer purchased by Operator E in the UC1 demo video #1 "5GZORRO Final Event 2022 Demo 1 - Michael De Angelis, Nextworks" [8]. **[KPI4.1]** The KPI target was set to distribution of resource updates and discovery in less than 10 mins. For this test, the resource can be considered the SLA template, which is stored locally for the operator. The time between the submission of the template and the availability of the template is therefore under 1 second. **[KPI4.2]** The KPI target was set as SLA measurements and validation from at least 3 operators involved in a multi-party service chain, however this test only involves actions up to the attachment of an SLA to Offers. Therefore, for this test, it is validated through the assignment by the Platform of an uploaded SLA template with a unique ID so it can be filled and attached to multiple Offers from multiple Providers.	

2.2.2.1.2. Creation of an eLicense Legal Prose Template Test

The tests of the creation of an eLicense Legal Prose Template, **UC1.8a/b**, involve the uploading of an eLicense template file, shown in Figure 1010, using the same process described in test 1.7 for the SLA. As with the SLA, the uploaded eLicense template can be viewed through the Portal (12). Unlike the SLA, the eLicense template can be automatically filled by the Portal at the time of Product Offer Price (POP) creation by selecting the template in the POP creation window (Figure 133).

```
# 5GZORRO License Agreement

For use of {{assetName}} according to the specification {{resourceId}} from the 5GZORRO Marketplace.

This License Agreement is made and effective as of {{startDateTime}} (the \"Commencement Date\") for the duration and limitations described in the Schedule (Exhibit A), by and between {{vendorCompany}}, a company organized and existing in
```

{{vendorCountry}}, with a registered address at {{vendorAddress}} (\"Vendor\") and a recognized and verified participant in the context of 5GZORRO ecosystem (\"Client\").

WHEREAS:

1. Client wishes to obtain a license to use {{assetName}} (a {{assetType}}) with unique identifier {{assetId}}, hereinafter, the \"Asset\", and

[...]

Item 1 – License Agreement

THE LICENSE AGREEMENT OF WHICH THIS SCHEDULE FORMS A PART IS DATED AS OF {{startDateTime}}] AND IS BY AND BETWEEN THE PARTIES REFERENCED IN ITEM 2 BELOW.

Item 2 – Name and Address of Vendor and Client

Vendor: {{vendorCompany}}, a company organized and existing in {{vendorCountry}}, with a registered address at {{vendorAddress}}.

Client: An authorized participant of the 5GZORRO ecosystem whose details are to be safely registered by the platform at the ordering time.

Item 3 – Other License Terms

{{pricingTerms}}

Item 4 – Commencement Date

The commencement date is {{startDateTime}}

Item 5 – Expiry Date

The expiry date is {{endDateTime}}

Item 6 – Description of Asset

The asset {{assetName}} comprises the functionalities described herein:

{{assetDescription}}

Item 7 – Format of Asset

The format of the asset {{assetName}} is of type {{assetType}} is given as a bundled software component with all dependencies and requirements to successfully execute it.

Item 8 – Approved Purpose.

The approved purpose for the use of the asset is solely under the management of the 5GZORRO platform. Not allowed to distribute, sell, License or sub-License, let, trade or expose for sale the Asset to a third party outside of the 5GZORRO platform.

Item 9 – License Fee

{{pricingDescription}}

Figure 10: eLicense template file availability_template.zip

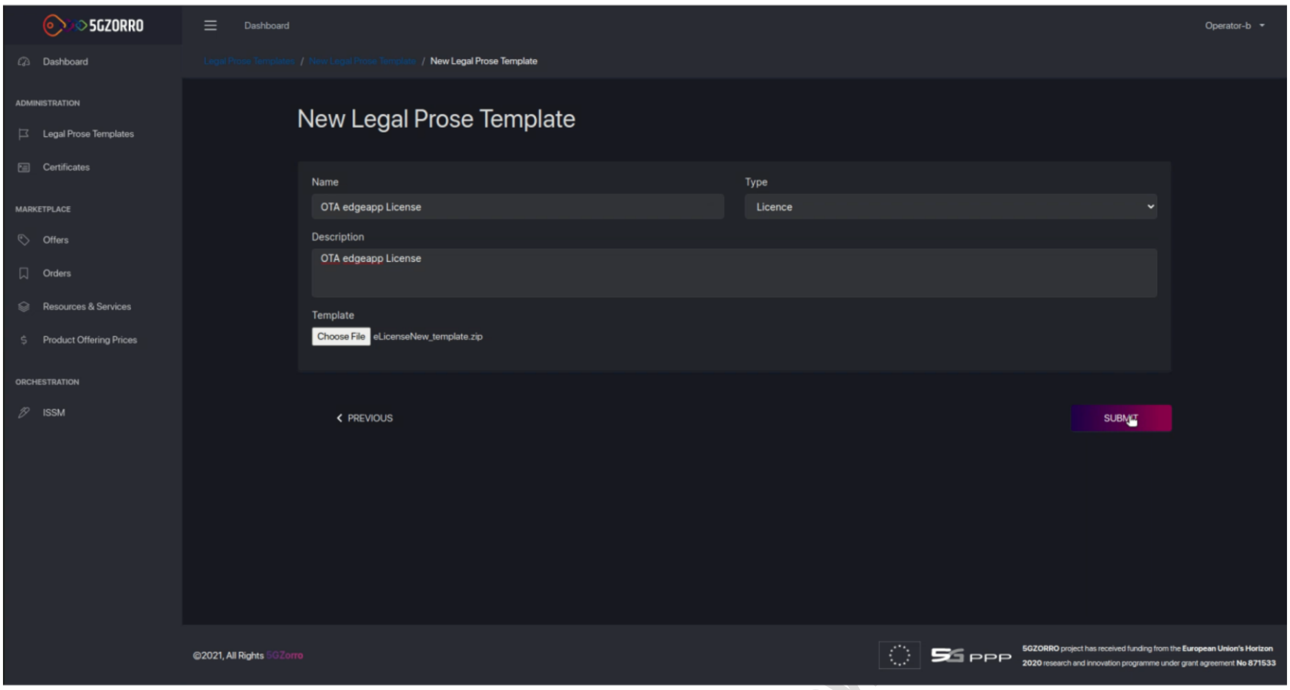


Figure 11: Uploading an eLicense Template file to the Platform to create an eLicense template object (OTA edgeapp License)

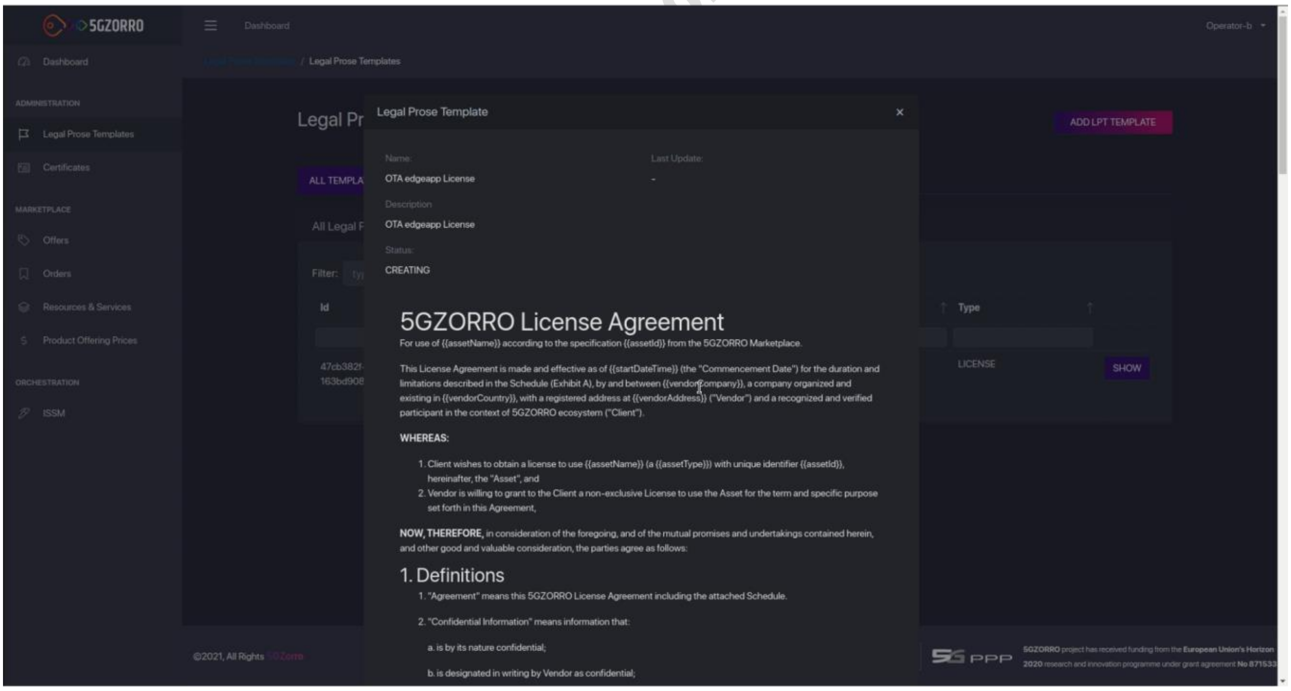


Figure 12: The eLicense template (OTA edgeapp License)) can be viewed on the Portal

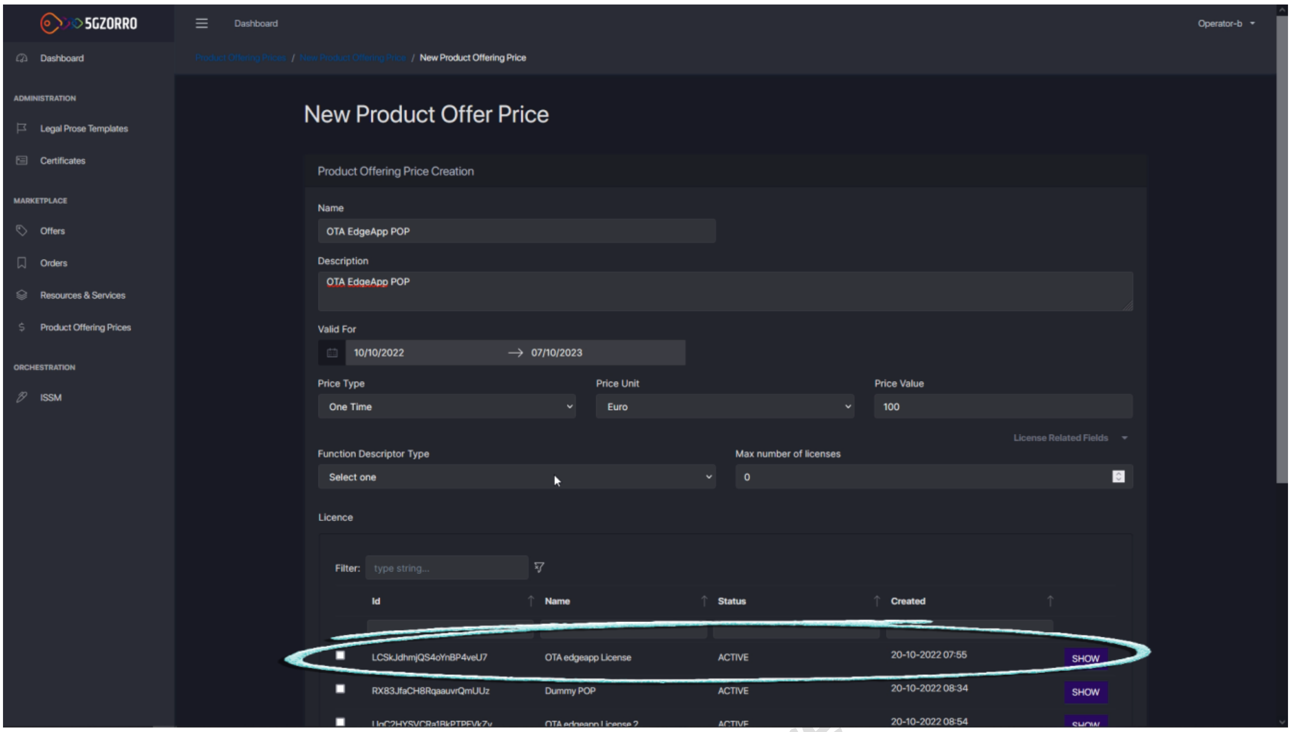


Figure 13: The eLicense template is automatically filled by the Portal when selected during Product Offer Price Creation for an asset

Table 5: Creation of a licensing agreement template

UC1.8	**Automatic filling of an eLicense template**	
Testbed	5GBarcelona	
Description	Service Provider uploads an eLicense Legal Prose Template. The template is then used to create an eLicense and attached to a POP	
Use-case functionalities	Resource Provider creating a Resource Offer Service Provider creating a Service Offer	
Key Use-case requirements and KPIs	**[KPI3.1]** 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. **[KPI4.1]** Automatically discover and “inventorize” various types of resources (i.e., compute, storage, network at core, edge, far-edge), spectrum and services capabilities from different domains and service providers	
Components	Identity & Permissions Manager Governance Manager Legal Prose Repository Marketplace Portal Governance Portal	
Test Procedure	Pre-conditions	The Service Provider has been onboarded onto the Portal
	Test Case steps	The eLicense template (Figure 1010) is uploaded to the Platform (Figure 1111**¡Error! No se encuentra el origen de la referencia.**). The template is assigned with a unique ID and is accessed through the Portal and the contents are reviewed (Figure 122) and filled when creating a POP (Figure 133)
Measurements	Methodology	video and screenshots

	Complementary measurements	none
	Calculation process	Observation from the Portal
Result	**[KPI3.1]** The KPI target was set as Smart Contract for 3 or more untrusted parties. As with the SLA, the eLicense is an integral part of the Smart Contract. In this test, Operator B attaches an SLA agreement to their respective Offer, to be purchased by Operator C in later tests (UC1.11 and UC1.15) and used to create a composite Offer purchased by Operator E in the UC1 demo video #1 "5GZORRO Final Event 2022 Demo 1 - Michael De Angelis, Nextworks" [8]. **[KPI4.1]** The KPI target was set to distribution of resource updates and discovery in less than 10 mins. For this test, the resource can be considered the eLicense template, which is stored locally for the operator. The time between the submission of the template and the availability of the template is therefore under 1 second.	

2.2.2.1.3. Product Offer creation Test

Product Offer creation involves compiling the information on location, resource/service description, valid time period, pricing and SLA, in the Portal to form an Offer object which is assigned a unique identifier and distributed to all catalogues of all registered Marketplace participants. These tests differ from UC1.4 and UC1.5, reported in D5.2 [3], in that they include a complete service with SLA and eLicenses on the resources and services.

For UC1.11, a single Product Offer for an edge resource and VNF service (*OTA EdgeApp Offer*) is created by Operator B, using the eLicense and POP created in UC1.7 attached to the edge resource (free5gc-edge), shown in Figure 144. This Offer is then viewed on the portal by Operator C (Figure 155). The time for the Offer distribution in the distributed catalogues of the Resource Providers for KPI4.1.1 has been previously measured and reported in D5.2 [3] and is again reported in Table 6.

The KPI measurements reported in Table 6 are defined as follows:

- **Total time for Offer creation** is defined as the time from submitting the request to the time the Offer is published on the Marketplace DLT
- **Local pre-storage time without DID** is the time from submitting the request to the time the Offer is stored on the local Resource and Service Catalogue of the Resource/Service Provider
- **Local pre-storage time** is the time from submitting the request to the time the Offer receives a DID from the ID&P
- **DLT publishing time** is measured as the time from when the Offer is assigned a DID to the time when the Offer has been published on the DLT
- **Total time for Offer publishing** is the time from when the Offer is stored on the local Resource and Service Catalogue of the Resource/Service Provider creating the Offer, to the time when the Offer appears on all catalogues of registered Resource/Service Consumers

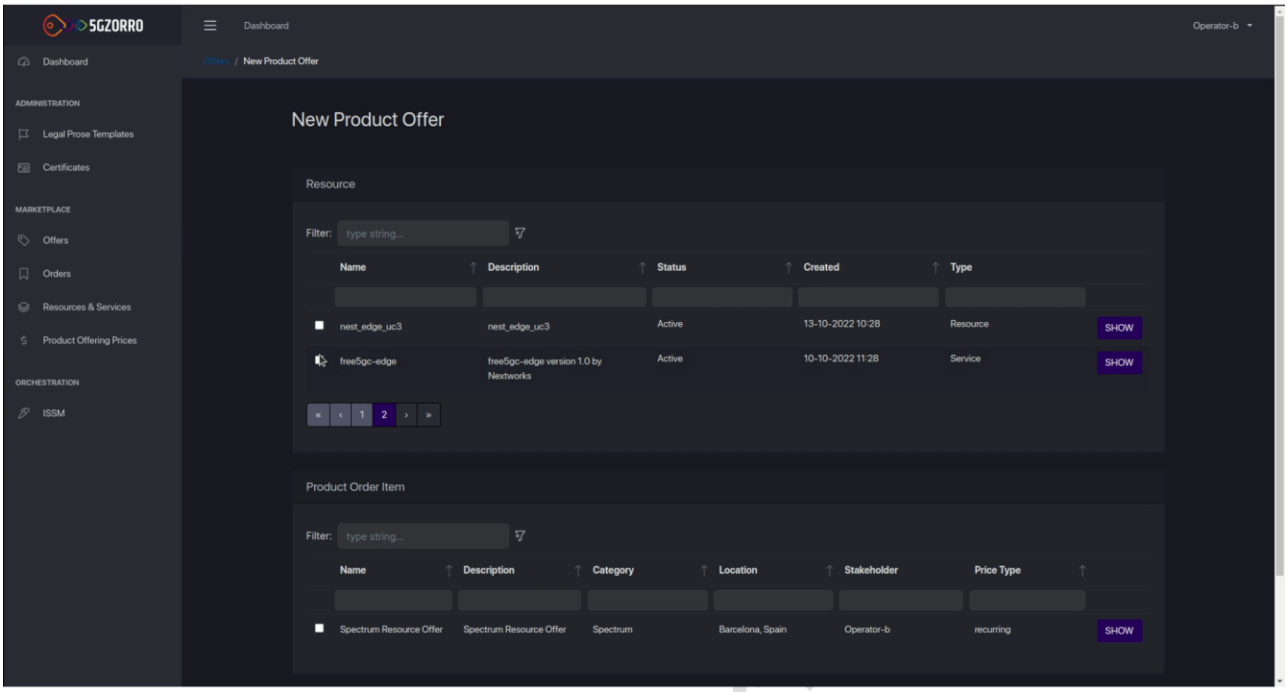
For KPI5.2, keeping with the related tests reported in D5.2 [3], the definition of the number of transactions handled by the Market for these tests is defined as the average times and standard deviations for the time from when the Offer is stored on the local catalogue to the time the Offer is published on the Marketplace DLT, see Table 6 for measurements.

UC1.12 extends UC1.11 to have a Product Offer for an edge resource and VNF from Provider B and a Product Offer for a 5G core and RAN network service (*OTA core demo*) from Provider A, with an availability

SLA (created in UC1.7) attached to the core resource. The Offers are then viewed on the portal (Figure 166).

Table 6: Measurements for UC1.11 and UC1.12

	Total time for Offer creation		**Local pre-storage time without DID**		**Local pre-storage time with DID**		**DLT publishing time**		**Total time for Offer publishing**	
	Average (sec)	STDEV (sec)	Average (sec)	STDEV (sec)	Average (sec)	STDEV (sec)	Average (sec)	STDEV (sec)	Average (sec)	STDEV (sec)
1 Operator 64 requests	20.91	8.19	**1.90**	**1.28**	**2.35**	**1.15**	**16.66**	**8.01**	**30.13**	**12.12**
1 Operator 128 requests	45.25	20.04	**4.84**	**3.03**	**6.18**	**2.85**	**34.22**	**19.29**	**59.24**	**27.25**
2 Operators 64 requests each	42.07	17.78	**6.00**	**5.87**	**6.43**	**5.24**	**29.64**	**15.94**	**65.55**	**30.52**



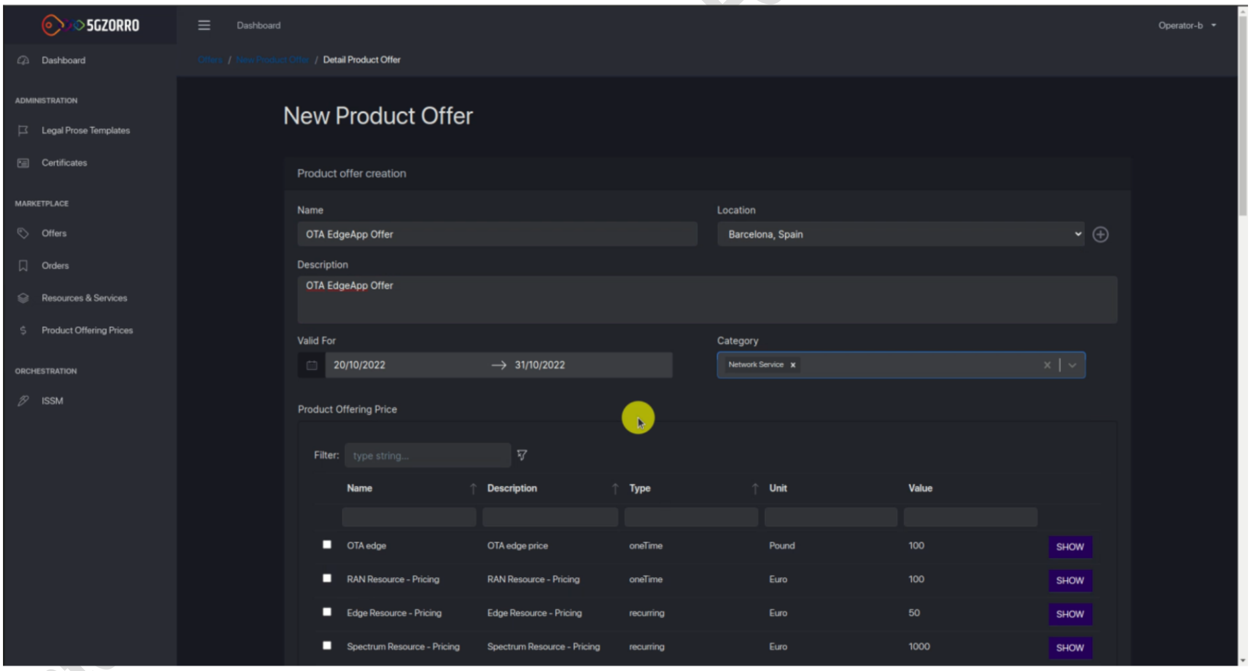


Figure 14: A single Product Offer for an edge resource and VNF service is created by Operator B, with an uptime SLA (created in UC1.7) attached to the edge resource

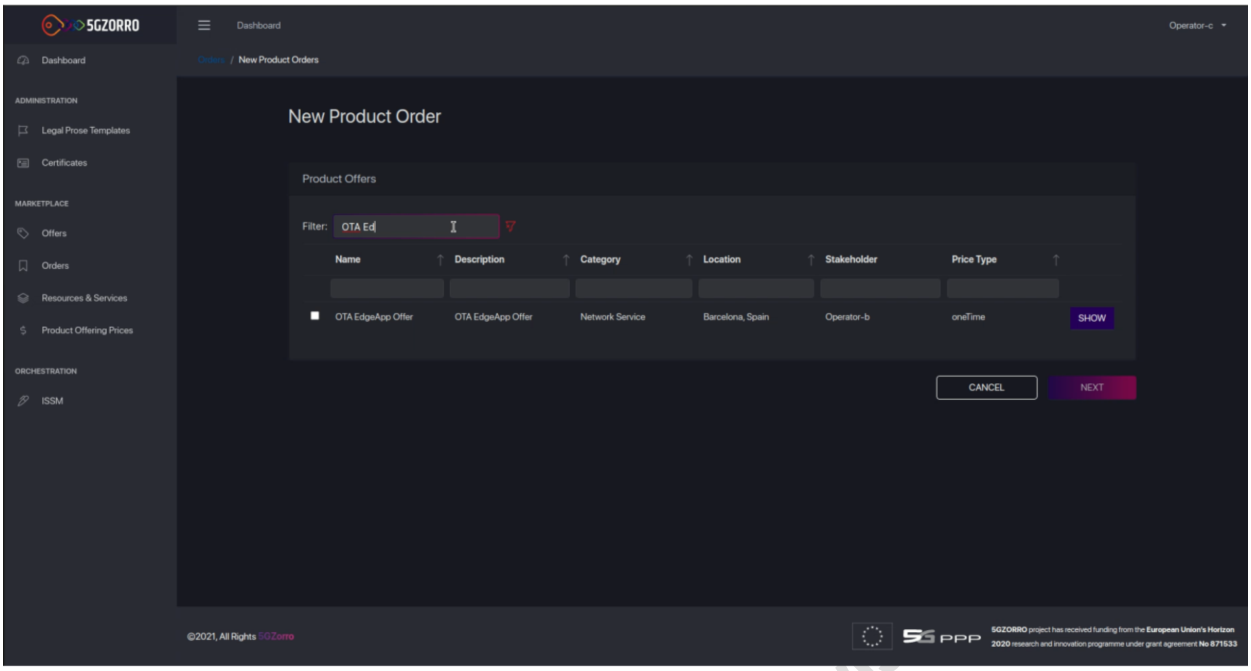


Figure 15: The Product Offer from Operator B is distributed and viewed on the portal by Operator C

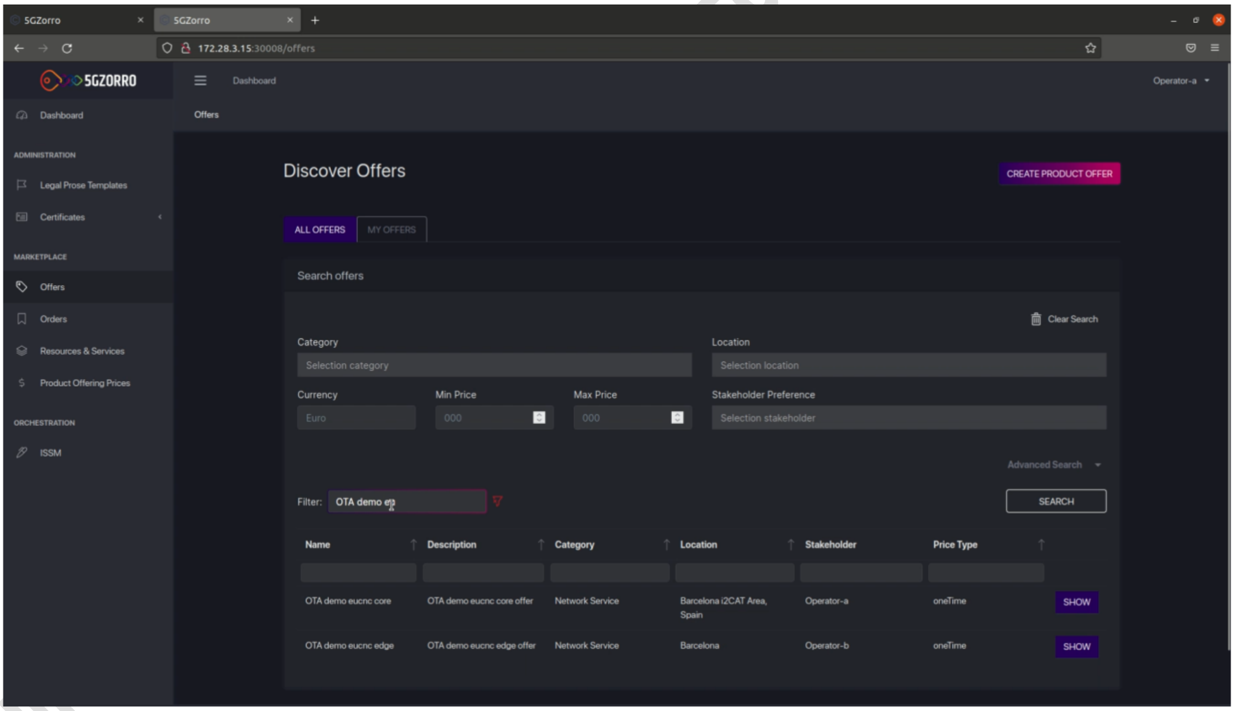


Figure 16: Multiple Product Offers from multiple Providers are viewed in the Portal

Table 7: Product Offer creation

UC1.11 and UC1.12	**Product Offer creation**
Testbed	5GBarcelona
Description	Resource Provider composes a Product Offer consisting of: • Edge Resource Offer

	• VNF application • elicensing terms for 2 instances (UC1.4 & UC1.8) Service Provider composes a Product Offer consisting of: • RAN Service (UC1.4) • Network Slice Service (core) (UC1.4) • Network Service (UC1.4) • Availability SLA (UC1.4 & UC1.7) The available Offers are viewed by a Consumer who uses them to create a composite Offer	
Use-case functionalities	Resource Consumer Request Service Consumer Request	
Key Use-case requirements and KPIs	**[KPI3.1]** 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. **[KPI4.1]** Automatically discover and "inventorize" various types of resources (i.e., compute, storage, network at core, edge, far-edge), spectrum and services capabilities from different domains and service providers **[KPI5.2]** Number of transactions per second handled by the market, which will determine the volume of spectrum transactions processed by the market.	
Components	Marketplace Portal Identity & Permissions Manager Catalogue Smart Contract Lifecycle Manager	
Test Procedure	Pre-conditions	Resource/Service Providers have been on-boarded onto the system
	Test Case steps	Operator B creates a Product Offer which is viewed by Operator C Operator A creates a Product Offer Operator C views the Offers from multiple operators
Measurements	Methodology	KPI measurements are performed using scripts to read timestamps from log files to determine times. See text above for details
	Complementary measurements	UC1.4 [3], UC1.7, UC1.8
	Calculation process	Log file timestamps and screenshots and video of the Portal
Result	**[KPI3.1]** the KPI target was determined to be Smart Contract for 3 or more untrusted parties**.** In this test, Operator B and Operator A create Offers, purchased by Operator C and used to create a Composite Offer purchased by Operator E, shown in the UC1 demo video #1 5GZORRO Final Event 2022 Demo 1 - Michael De Angelis, Nextworks [8]. **[KPI4.1]** the KPI target was set as the distribution of resource updates and discovery in less than 10 mins. For this test, the total time for Offer publishing was measured as the time from when the Offer is stored on the local Resource and Service Catalogue of the Resource/Service Provider creating the Offer, to the time when the Offer appears on all catalogues of registered Resource/Service Consumers, see Table 6 for measurements. **[KPI5.2]** the KPI target was set for 20 transactions/second. For this test, as in D5.2 [3] for tests UC1.4, the number of transactions handled by the Market is defined as the average times and standard deviations for the time from when the Offer is stored on the local catalogue to the time the Offer is published on the Marketplace DLT. For the various transactions measured, including total time for Offer creation, local pre-storage time without DLT, local pre-storage time, DLT publishing time, and total time for Offer publishing, the time varied from 2 to 66 seconds, see Table 6 for measurements.	

2.2.2.1.4. Intelligent resource discovery query by Resource Consumer Test

An intelligent resource Offer discovery involves using natural language to search the available resource and service Offers. The option is available in the Portal through the Offers->Search Offers page (Figure 177). For this test, Operator E performs an advanced search looking for a composite Network Service for edge and core resources in Barcelona.

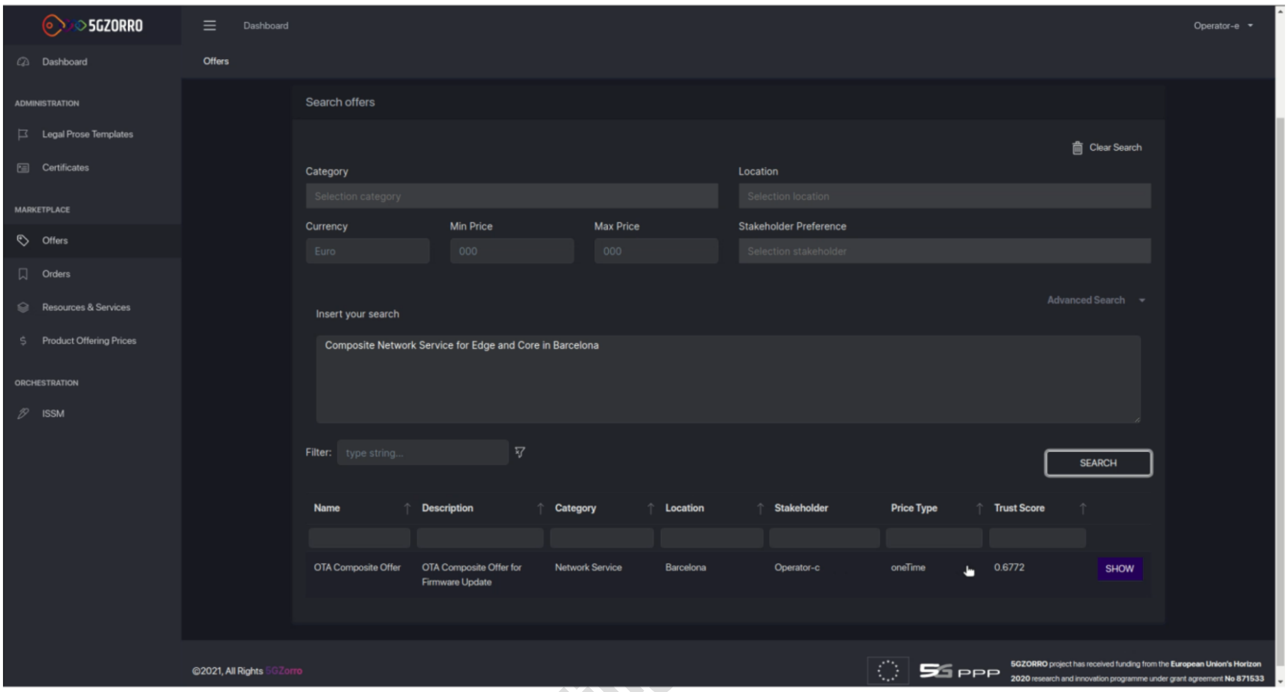


Figure 17 : Intelligent resource discovery query by Resource Consumer

Table 8: Intelligent resource discovery query by Resource Consumer

UC1.14	**Intelligent resource discovery query by Resource Consumer**	
Testbed	5GBarcelona	
Description	Resource Consumer performs an intelligent resource discovery query based on metrics received from breach prediction and virtual/radio resource management	
Use-case functionalities	Contract Lifecycle Management	
Key Use-case requirements and KPIs	**[KPI4.1]** Automatically discover and "inventorize" various types of resources (i.e., compute, storage, network at core, edge, far-edge), spectrum and services capabilities from different domains and service providers	
Components	Virtual/Radio Resource Managers Catalogue Smart Resource & Service Discovery	
Test Procedure	Pre-conditions	Resource Providers have posted Resource Offers on the Portal, a Resource Consumer has been onboarded onto the Platform
	Test Case steps	The Resource Consumer logs onto the Portal and selects the Offers tab, they then select Advance search and enter criteria for a desired resource (Figure 177).
Measurements	Methodology	Using a recording of the test to determine the time for the query to return results to the customer

	Complementary measurements	None
	Calculation process	Screenshots and video of the Portal
Result	**[KPI4.1]** The target for this KPI is the distribution of resource updates and discovery in less than 10 mins. The SRSD component of the 5GZORRO Platform is invoked by the Portal to process the advance resource search and returns matching results of all Offers. The matching Offers were returned in 8.24 seconds.	

2.2.2.1.5. Resource Consumer purchases a Product Offer Test

For UC1.15, the Consumer (Operator C) purchases an Offer by submitting a Product Order request (Figure 188) for the resource or service (OTA EdgeApp Offer from Operator B) that they wish to acquire. After the Order request, all involved parties (Consumer and Provider) can view the Order (Figure 199 and Figure 2020).

UC1.16 extends UC1.15, Operator C then purchases another Offer from Operator A. As with UC1.15, all involved parties (Consumer and Providers) can view the Order.

The measurements reported in Table 9 are defined as follows:

- **DID assignment time** is measured as the time from when the Order is saved in the local catalogue of the consumer to the time when the Order receives a DID from the ID&P
- **DLT publishing time** is measured as the time from when the Order is assigned a DID to the time when the Order has been published on the DLT
- **Total time for Order publishing** is related to KPI4.1.1 and is measured as the time from when the Order is saved in the local catalogue of the consumer to the time when the Order appears on the distributed catalogues of the other Marketplace users

Each of these measurements were performed for 3 different scenarios: A single user sends 64 Order requests, a single user sends 128 Order requests, and 2 users send 64 Order requests each.

For KPI5.2, the number of transactions per second handled by the market for this test pertains to the total time for all submitted Offers to have been published divided by the total number of Offers submitted. As reported in Table 10, for 128 Orders submitted quasi-simultaneously, the number of transactions per second has been measured at 0.5 transactions/second. This does not meet the target of 20 transactions per second set at the beginning of the project. Several factors influence this rate. These include the specific nature of the overall procedure, which encompasses two independent and subsequent DLT computation and publication (i.e., the DID generation in the Governance DLT and the order propagation in the Marketplace DLT). Specifically, such complex end-to-end procedure for order purchase, DLT publication and propagation was not originally considered when setting the KPI target.

Table 9: Measurements for UC1.15 and UC1.16

	DID assignment time		**DLT publishing time**		**Total time for Order publishing**	
	Average (sec)	STDEV (sec)	Average (sec)	STDEV (sec)	Average (sec)	STDEV (sec)
1 user 64 requests	**5.84**	**1.63**	**1.82**	**0.95**	**25.99**	**6.49**
1 user 128 requests	**11.72**	**7.38**	**2.76**	**2.68**	**44.02**	**15.23**

2 users 64 requests each	**6.45**	**5.77**	**3.92**	**5.32**	**53.23**	**17.34**

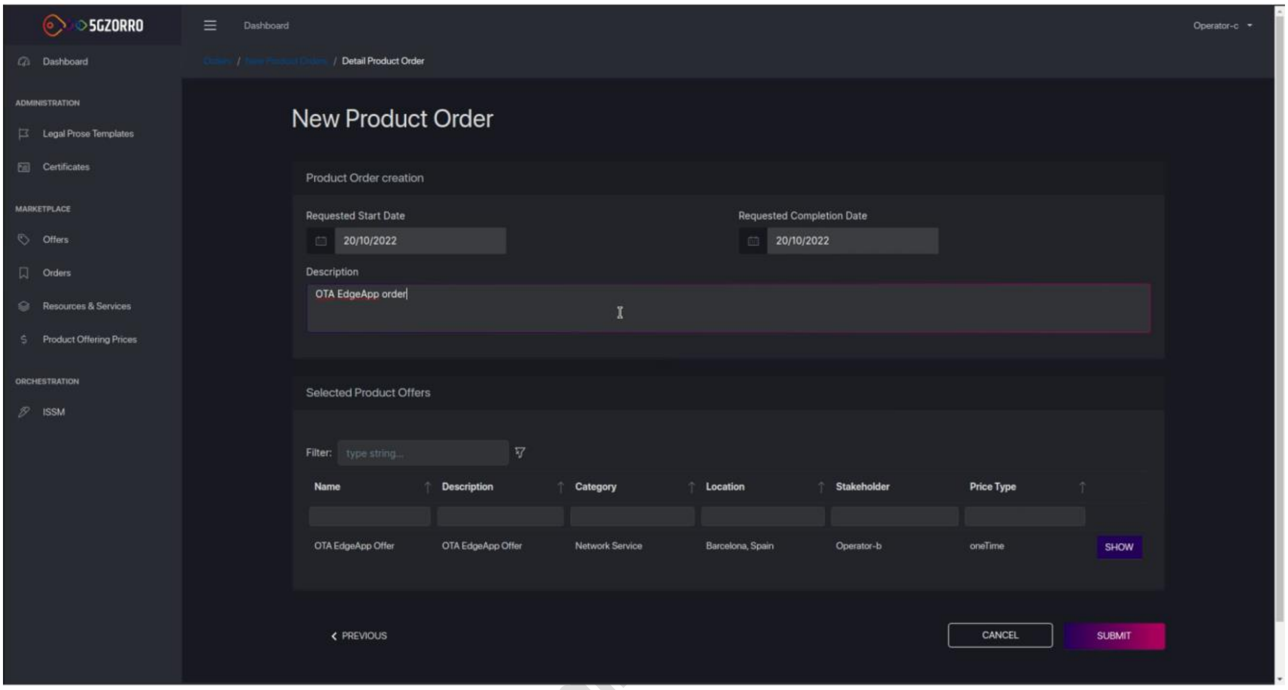


Figure 18: The Consumer (Operator C) submits a Product Order request through the Portal

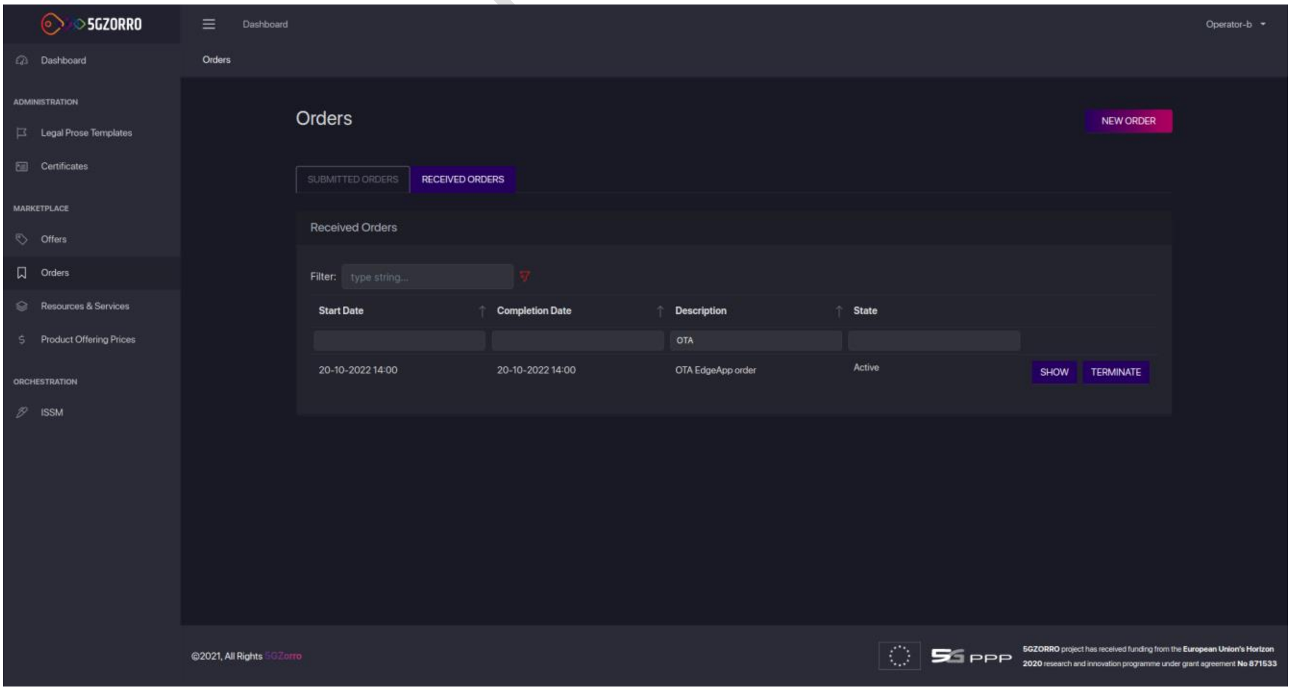


Figure 19: The provider of the OTA EdgeApp Offer (Operator B) views the Order submitted by Operator C

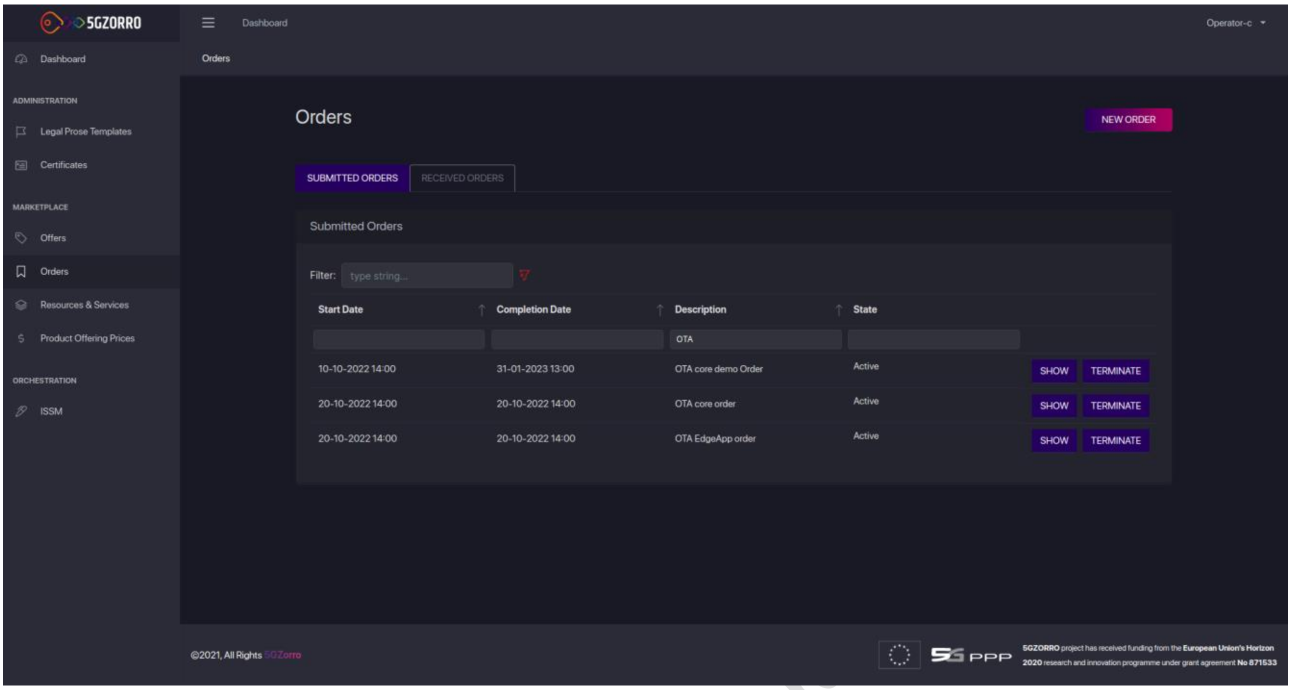


Figure 20: Operator C views all submitted Orders

Table 10: Resource Consumer purchases a Product Offer

UC1.15 and UC1.16	**Resource Consumer purchases a Product Offer**	
Testbed	5GBarcelona	
Description	UC1.15 Resource Consumer purchases a Product Offer from a Resource Provider by submitting a Product Order. UC1.16 Resource Consumer purchases multiple Product Offers from multiple providers.	
Use-case functionalities	Smart Contract Lifecycle Management	
Key Use-case requirements and KPIs	**[KPI3.1]** 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. **[KPI5.2]** Number of transactions per second handled by the market, which will determine the volume of spectrum transactions processed by the market.	
Components	Marketplace Portal Catalogue Smart Contract Lifecycle Manager Intelligent Network Slice & Service Optimization Virtual/Radio Resource Managers Service & Resource Monitoring Monitoring Data Aggregator Legal Prose Repository Intelligent SLA monitoring & breach prediction	
Test Procedure	Pre-conditions	Resource Providers (Operator B and Operator A) have created Offers for their resources. The Resource Consumer (Operator C) has been onboarded to the Platform
	Test Case steps	Operator C creates the Product Order by navigating to the Orders tab and selecting New Product Offer, first for

		the edgeApp Offer from Operator B, then the core Offer from Operator A.
Measurements	Methodology	KPI measurements are performed using scripts to read timestamps from log files to determine times. See text above for details
	Complementary measurements	UC1.4 [3], UC1.11, UC1.12
	Calculation process	Log file timestamps and screenshots and video of the Portal
Result	**[KPI3.1]** the KPI target was determined to be Smart Contract for 3 or more untrusted parties**.** In this test, Operator C creates 2 Product Orders from Offers from Operator A and Operator B. Operator C then uses these to create a Composite Offer purchased by Operator E, shown in the UC1 demo video #1 5GZORRO Final Event 2022 Demo 1 - Michael De Angelis, Nextworks [8][8]. **[KPI4.1]** the KPI target was set as the distribution of resource updates and discovery in less than 10 mins. For this test, the total time for Offer publishing was measured as the time from when the Offer is stored on the local Resource and Service Catalogue of the Resource/Service Provider creating the Offer, to the time when the Offer appears on all catalogues of registered Resource/Service Consumers, see Table 9 for measurements. **[KPI5.2]** the KPI target was set for 20 transactions/second. For this test, the total time for all submitted Offers to have been published divided by the total number of Offers submitted. For 128 Orders submitted quasi-simultaneously, the number of transactions per second has been measured at 0.5 transactions/second. See above text for discussion	

2.2.2.2. Scenario 1.3: Slice Lifecycle Management with analytics test

The findings of the remaining test, Test UC1.19 Agreement termination, is reported in Table 11.

2.2.2.2.1. Agreement termination Test

For UC1.19 the termination of an agreement for a Product Order is done through the Portal by the operator who purchased the Offer (Operator E), shown in Figure 21. The state of the Order is recorded on the DLT, and can be viewed through the Portal (Figure 222).

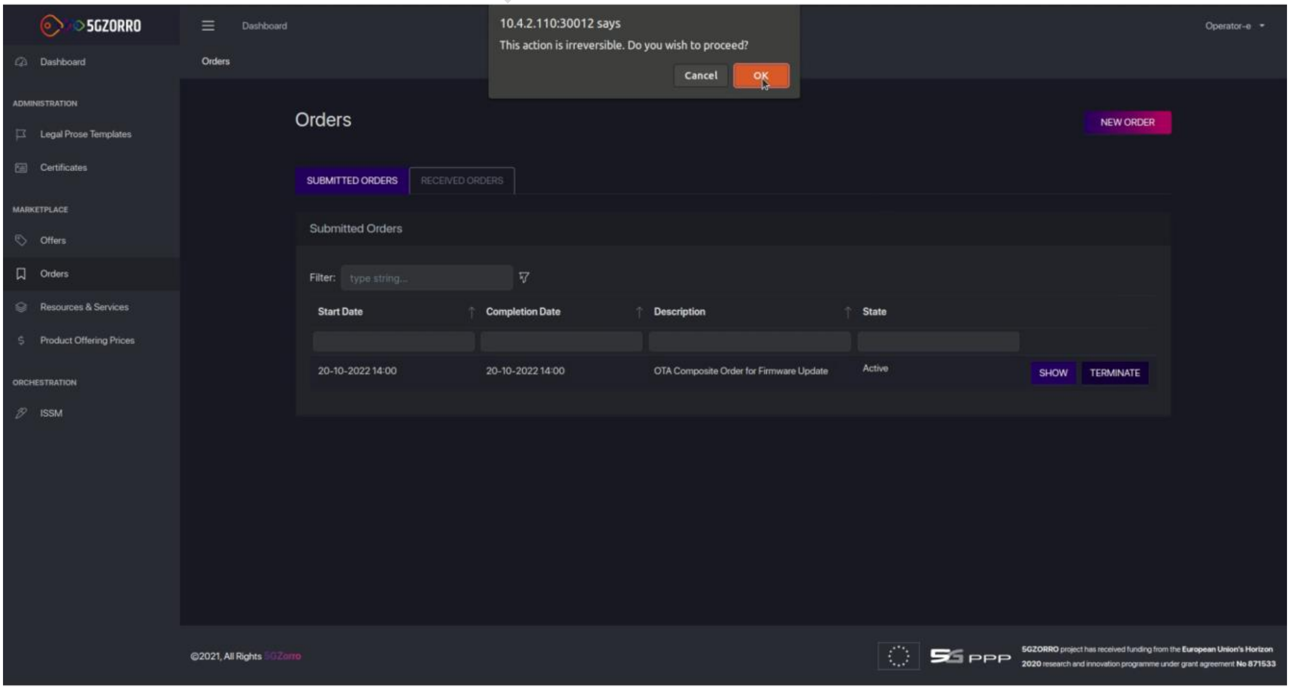


Figure 21: Operator E terminates an order on the Portal

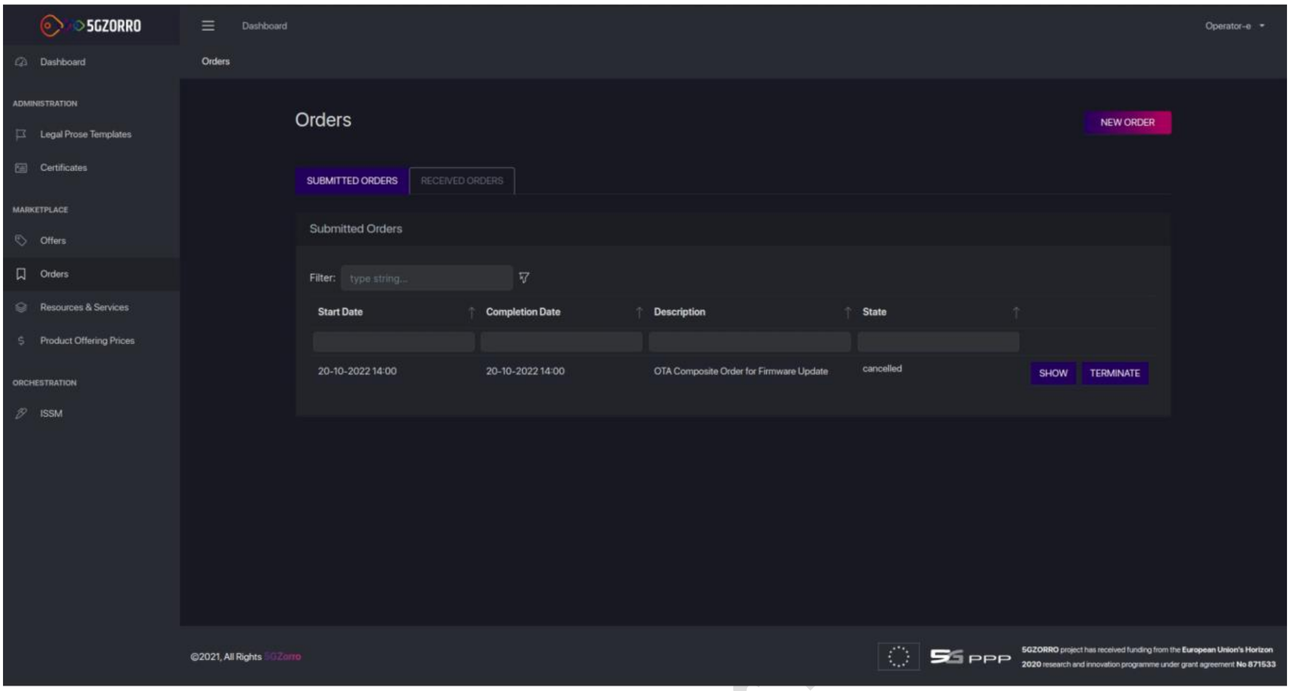


Figure 22: The state of the terminated order changes to cancelled

Table 11: Agreement termination

UC1.19	**Agreement termination**	
Testbed	5GBarcelona	
Description	Resource Consumer terminates an agreement	
Use-case functionalities	Smart Contract Lifecycle Management	
Key Use-case requirements and KPIs	**[KPI3.1]** 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	
Components	Marketplace Portal Smart Contract Lifecycle Manager Catalogue Virtual/Radio Resource Managers Service & Resource Monitoring Monitoring Data Aggregator	
Test Procedure	Pre-conditions	Operator E has submitted a Product Order which is in an active state
	Test Case steps	Operator E navigates to the Orders tab in the Portal The Terminate button is selected to terminate the Order Operator E views the current state of the terminated Order in the Portal
Measurements	Methodology	video and screenshots
	Complementary measurements	none
	Calculation process	Observation from the Portal

Result	**[KPI3.1]** the KPI target was determined to be Smart Contract for 3 or more untrusted parties**.** The pre-conditions of this test are that Operator B and Operator A create offers, purchased by Operator C and used to create a Composite Offer purchased by Operator E, shown in the UC1 demo video #1 "5GZORRO Final Event 2022 Demo 1 - Michael De Angelis, Nextworks [8]". Operator E then terminated the composite offer involving Operators A, B, and C. It is worth noting that for this agreement termination scenario, no specific timing measurements have been performed (mostly to due to an issue under fix at the time of writing in the propagation of order termination status update towards remote catalogues of involved parties. However, the same measurements carried out in section 2.2.2.2.1 are applicable for the agreement termination, considering the values reported in Table 9 for the offer propagation and publication, not considering in this case the DID generation process. Specifically, this results in having agreement termination completed in the order of tens of seconds for the measured scenarios (1 user 64 requests, 1 user 128 requests, 2 users 64 requests each).

2.3. UC2: Dynamic Spectrum Allocation

2.3.1. Description

As described in the previous WP5 deliverables, UC2 is focused on demonstrating Marketplace capabilities to trade licensed spectrum resources, configure the RAN elements of the relevant network slices accordingly, and monitor associated SLAs for breach verification and correction.

Regarding the involved stakeholders which operate in the decentralised marketplace, in this UC we have considered one spectrum regulator (Regulator A) and three resource traders (Operator A, Operator B and Operator C). Each operator takes a different role, as shown in Table 122.

Table 12: UC2 Stakeholders and regulator roles

<table>
<tr><th>Stakeholder name</th><th>Operator A</th><th>Operator B</th><th>Operator C</th><th>Regulator A</th></tr>
<tr><td rowspan="2">Stakeholder role</td><td>Spectrum & Radio/Slice resource provider</td><td>-</td><td rowspan="2">Resource Consumer</td><td rowspan="2">Spectrum Regulator</td></tr>
<tr><td>Radio/Slice resource provider</td><td>Spectrum resource provider</td></tr>
</table>

Note that role of Operators A and B are variable, since in this UC we have considered two different scenarios. In the first one, Operator A is able to provide both spectrum and radio resources; thus, it offers in the marketplace the spectrum and a non-configurable slice which is able to use this spectrum. Then, Operator C purchases both offers from Operator A and deploys the non-configurable 5G slice. On the other hand, in the second scenario, the spectrum is offered by Operator B, while Operator A only offers a configurable slice (i.e. with radio resources which can be configured on-demand by Intelligent Slice and Service Manager (ISSM)/Any Resource Manager (xRM)). Then, Operator C purchases both offers and combines them to deploy a configurable 5G slice.

2.3.2. Modelling of Spectokens

This section provides the final data models used for the primitive and derivative spectokens, updating the models that were introduced in Deliverable D3.3 [9] according to our final implementation (minor changes).

The primitive spectoken is issued by the Regulator and committed to the DLT reflecting the attributes of the associated spectrum license, after the Spectrum Certificate request becomes accepted by the Regulator (Spectrum Certificate Model was described in D5.2 [3]). As shown in Table 13, the primitive spectoken has the Regulator as maintainer and the Spectrum Resource Provider (SRP) as Owner, and also incorporates the Regulator DID. Then, as core information, it contains the parameters obtained from the accepted Spectrum Certificate, representing the main details of the leased spectrum license. The main difference with the model defined in D3.3 [9] is that, due to implementation limitations in the DLT, the hash of the license PDF file is not incorporated into the spectoken, since the used DLT is not able to store the PDF file. The regulator shall check anyway with the paper licence for the approval of the spectrum certificate. So, all in all, the hashed version of the paper licence, securely stored along with all the rest of the information would be a nice to have asset, though not mandatory, and it doesn't impact the defined workflows between regulator and spectrum provider.

Table 13: Primitive Spectoken information model

Attribute	Data type	Description	Example values	Observations
Maintainers	String	Operator who issued the spectoken (Owner, Location, Country)	"O: Regulator-A, L: Barcelona, C: Spain"	Must be a regulator in the case of the primitive spectoken
Owner	String	Operator how owns the spectoken	"O: Operator-A, L: Barcelona, C: Spain"	Must be a Spectrum Resource Provider (SRP) in the case of the primitive spectoken.
Regulator id	DID	DID of the Regulator that approved the spectrum license.		DID of the Regulator that approved the spectrum license.
Area	String	Country where the license applies to (nation-wide licenses are assumed).		Obtained from the spectrum certificate.
License Start time	String	License start time		License lease start time. Obtained from the spectrum certificate.
License End time	String	License end time		Obtained from the spectrum certificate.

Attribute	Data type	Description	Example values	Observations
Start DL	Double	Start DL frequency in MHz	3600	Obtained from the spectrum certificate.
End DL	Double	End DL frequency in MHz	3650	Obtained from the spectrum certificate
Start UL	Double	Start UL frequency in MHz	3600	Obtained from the spectrum certificate
End UL	Double	End UL frequency in MHz	3650	Obtained from the spectrum certificate
Duplex mode	String	Operation mode (TDD or FDD)	TDD	Obtained from the spectrum certificate
Band	Integer	Band number	n78	Obtained from the spectrum certificate.
Technology	String	Cellular technology to be used (4G or 5G)	5G	Obtained from the spectrum certificate.

¡Error! No se encuentra el origen de la referencia.3 depicts the final model of the primitive spectoken.

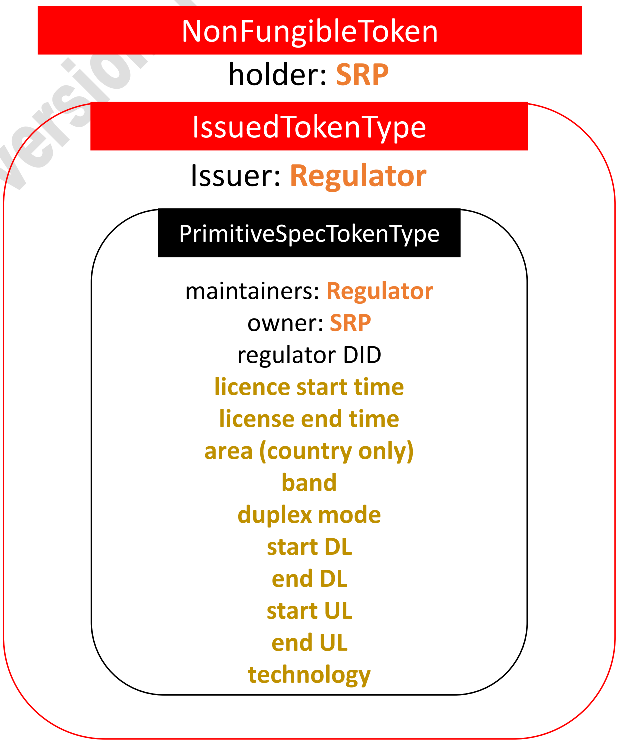


Figure 23: Primitive spectoken model

The derivative spectoken is issued and committed to the DLT reflecting the attributes of an associated spectrum offer, and is derived from an active primitive spectoken. In this case, the issuer and the maintainer roles are fulfilled by the Spectrum Resource Provider (SRP), while the holder and owner roles could be fulfilled either by the SRP itself or by a Spectrum Resource Consumer (SRC). In the first case, which corresponds to the non-configurable slice UC in this deliverable, the SRP offers a slice with RAN already configured according to this spectrum to one or multiple consumers, i.e., the spectrum is not leased and the SRP maintains its ownership over the spectrum. In the second case, which corresponds to the configurable slice UC in this deliverable, the SRC purchases the spectrum offer and is responsible of its usage; thus, it obtains the derivative spectoken as owner. **¡Error! La autoreferencia al marcador no es válida.** shows the content of the derivative spectoken, where main parameters are obtained from the Spectrum Offer (in this case, there are no significant changes compared to the model described in D3.3 [9]). **¡Error! No se encuentra el origen de la referencia.**4 depicts the final model of the derivative spectoken.

Table 14: Derivative spectoken information model

Attribute	Data type	Description	Example values	Observations
Maintainers	String	Operator who issued the spectoken(Owner, Location, Country)	"O: Regulator-A, L: Barcelona, C: Spain"	SRP
Owner	String	Operator how owns the spectoken	"O: Operator-A, L: Barcelona, C: Spain"	SRP or SRC
Primitive Spectoken	DID	Derivative spectoken unique ID		
Area	TMF Geographic Address Object	Area the spectoken applies to		According to the offer. It must be inside the country of the primitive spectoken
Start time	String	Spectoken lease start time		According to the offer. Spectoken lease start time
End time	String	Spectoken lease end time		According to the offer. Spectoken lease end time
Start DL	Double	Start DL frequency in MHz	3620	According to the offer. It must be inside the range of the primitive spectoken
End DL	Double	End DL frequency in MHz	3640	According to the offer. It must be inside the range of the primitive spectoken

Attribute	Data type	Description	Example values	Observations
Start UL	Double	Start UL frequency in MHz	3620	According to the offer. It must be inside the range of the primitive spectoken
End UL	Double	End UL frequency in MHz	3640	According to the offer. It must be inside the range of the primitive spectoken
Duplex mode	String	Operation mode	TDD	Same of the primitive spectoken
Band	Integer	Band number	n78	Same of the primitive spectoken

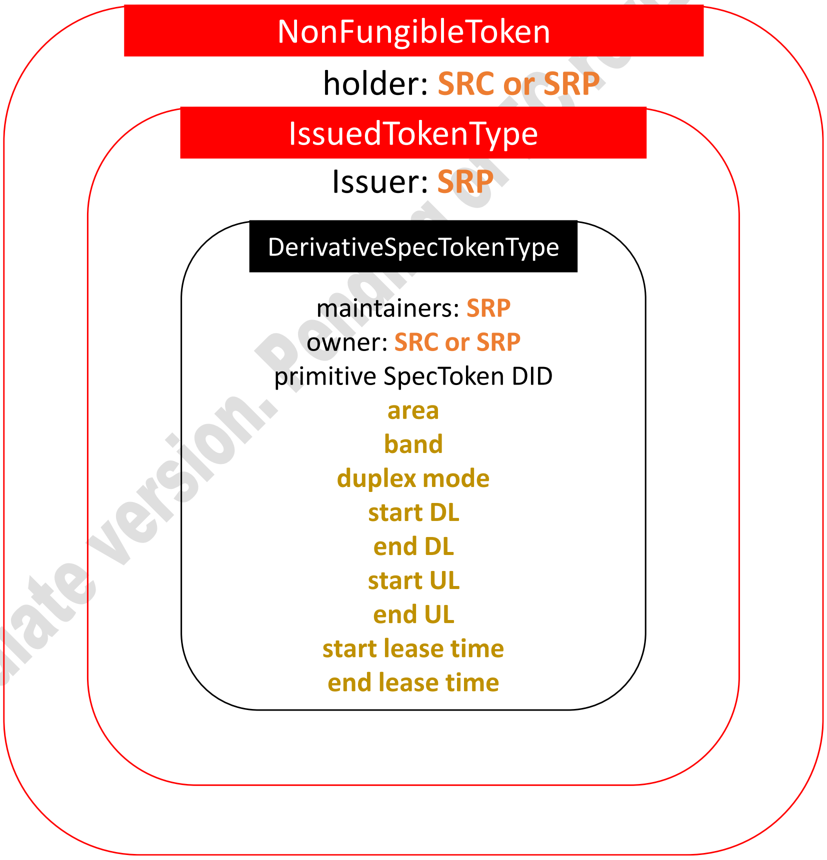


Figure 24: Derivative Spectoken model

2.3.3. Modelling of SLAs

We have modelled two different SLAs for the scenarios demonstrated in UC2, depending on the slice type: non-configurable and configurable. In the first case, as shown in Table 15, since the spectrum is not leased to the consumer, the SLA only captures the commitments of the SRP to provide a reliable RAN and

Spectrum; thus, SLA violations from the SRPs lead to compensations to the Consumer via Service Credits. In addition, the trust score of the Provider regarding this consumer becomes impacted.

Table 15: Non-configurable slice SLA template

Metric	SLA violation consequence	Observations
Reliability	Service Credits to Consumer	SLA violation occurs if the measured reliability the maximum number of UEs are below their defined threshold
Max. number of UEs	Service Credits to Consumer	
Interference	Service Credits to Consumer	SLA violation occurs if measured interference is above the threshold

SLA template

This SLA is valid between **{{startDateTime}}** and **{{endDateTime}}**.

Named Parties
SLAProvider: **{{stakeholderName}}**
This SLA rules the correct usage of a radio resource. The radio resource is leased, which implies the temporary transfer of rights and obligations of that particular resource.
In the event of a conflict between the terms of this SLA and the terms of any other agreement with the named SLAProvider governing your use of the Service (the 'Agreement'), the terms and conditions of this SLA apply, but only to the extent of such conflict. Capitalized terms used herein but not defined herein shall have the meanings set forth in the Agreement.

Service Commitment
The named SLAProvider will use reasonable efforts to provide a reliable RAN, as described in 1. below, for a maximum number of simultaneous active users, as described in 2. below, and to make the spectrum resource free of any incumbent activity that can be determined as interferences, as described in 3. below, during any monthly billing cycle (the 'Service Commitment') during any monthly billing cycle (the 'Service Commitment'). In the event a Service does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

Service Credits
Service Credits are calculated as a percentage of the total charges paid by you for the applicable radio resource for the billing cycle in which the reliability and maximum number of active users fell within the ranges set forth in the table below.
The following rules are used to check if there is a service breach associated with the metric under analysis. The \"operator\" defines when a value is considered a violation (operator option forced to be greater than \".g\" a reference value plus a tolerance\"):
1. The **{{reliability}}** (**{{%}}**) value becomes a breach when it is **{{.l}}** than **{{reliabilityReferenceValue}}** minus **{{reliabilityTolerance}}**.
2. The **{{cell_ue_count}}** **{{(units)}}** value becomes a breach when it is **{{.l2}}** than **{{cell_ue_countReferenceValue}}** minus **{{cell_ue_countTolerance}}**.
3. An **{{cell_neigh_sinr_db}}** (**{{dBm}}**) value becomes a breach when it is **{{.g1}}** than **{{cell_neigh_sinr_dbReferenceValue}}** plus **{{cell_neigh_sinr_dbTolerance}}**.
We will apply any Service Credits only against future payments otherwise due from you for the Service. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the Service did not meet the Service Commitment. Service Credits will not entitle you to any refund or other payment from the named SLAProvider. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one euro (1€). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the Order Agreement, your sole and exclusive remedy for any unavailability, non-performance, or other failure by us to provide the Service is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

SLA Exclusions
The Service Commitment does not apply to interferences: (i) caused by factors outside of our reasonable control; (ii) that result from any actions or inactions of you or any third party; (iii) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); or (iv) arising from our suspension or termination of your right to use the radio resource in accordance with the Order Agreement (collectively, the \\\"SLA Exclusions\\\").

Definitions

A \"Service Credit\" is a euro credit, calculated as set forth above, that we may credit back to an eligible account."

On the other hand, in the configurable slice case, since the spectrum is leased to the Consumer, it has some obligations regarding the usage of the spectrum. As shown in Table 16, these obligations are captured by the SLA and can lead to service termination and to redeem of the derivative spectoken.

Table 16: Configurable slice SLA template

Metric	SLA violation consequence	Observations
Interference	Service Credits to Consumer	SLA violation if interference is above the threshold (neighbour cell)
Effective Isotropic Radiated Power (EIRP)	Service Termination, derivative spectoken redeem	SLA violation if EIRP is above the threshold
Cell Location	Service Termination, derivative spectoken redeem	SLA violation if cell location is out of the area defined in the spectrum offer
Time to Deploy	Service Termination, derivative spectoken redeem	SLA violation if the spectrum is used after the time limit
SLA content		

This SLA is valid between **{{startDateTime}}** and **{{endDateTime}}**.

Named Parties
SLAProvider: **{{stakeholderName}}**
This SLA rules the correct usage of a spectrum resource. The spectrum resource is leased, which implies the temporary transfer of rights and obligations of that particular resource.
In the event of a conflict between the terms of this SLA and the terms of any other agreement with the named SLAProvider governing your use of the Service (the 'Agreement'), the terms and conditions of this SLA apply, but only to the extent of such conflict. Capitalized terms used herein but not defined herein shall have the meanings set forth in the Agreement.

Service Commitment
The named SLAProvider will use reasonable efforts to make the spectrum resource free of any incumbent activity that can be determined as interferences, as described in 1. Below, during any monthly billing cycle (the 'Service Commitment'). In the event a Service does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.
The taker of this SLA will commit to use the spectrum resource respectfully, without inducing severe interferences to the SLAProvider's public network in the surroundings of the spectrum resource as described in 2. Below, within the bounds of its area of application as described in 3., 4., 5. And 6., and within the timeframe described in 7., during any monthly billing cycle (the 'Service Commitment'). In the event a Service does not meet the Service Commitment, it will be terminated and the rights to use the spectrum will be revoked, as described in \"Service Termination\" clause.

Service Credits
Service Credits are calculated as a percentage of the total charges paid by you for the applicable spectrum for the billing cycle in which the interference fell within the ranges set forth in the formula below.
The following rules are used to check if there is a service breach associated with the metric under analysis. The \"operator\" defines when a value is considered a violation (operator option forced to be greater than \".g\" a reference value plus a tolerance\"):
1. An **{{cell_neigh_sinr_db}}** (**{{dBm}}**) value becomes a breach when it is **{{.g1}}** than **{{cell_neigh_sinr_dbReferenceValue}}** plus **{{cell_neigh_sinr_dbTolerance}}**.
We will apply any Service Credits only against future payments otherwise due from you for the Service. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the Service did not meet the Service Commitment. Service Credits will not entitle you to any refund or other payment from the named SLAProvider. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one euro (1€). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the Order Agreement, your sole and exclusive remedy for any unavailability, non-performance, or other failure by us to provide the Service is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

```
## Service Termination
SLA violations incurred by the taker of this SLA, where the usage of the spectrum resource violates the allowed transmission power, geolocation and/or timeframe to deploy, as described in the formulas below, will cause the termination of the Service and the revocation of the rights to use the spectrum resource. These actions will not entitle you to any refund or other payment from the named SLAProvider.
The following rules are used to check if there is a service breach associated with the metric under analysis. The \"operator\" defines when a value is considered a violation (operator option forced to be greater than \".g\" a reference value plus a tolerance\"):
2. The **{{cell_eirp}}** (**{{W}}**) value becomes a breach when it is **{{.g2}}** than **{{cell_eirpReferenceValue}}** plus **{{cell_eirpTolerance}}**.
3. A **{{location_latitude_coord}}** (**{{degrees1}}**) value becomes a breach when it is **{{.g3}}** than **{{location_latitude_coordReferenceValue}}** plus **{{location_latitude_coordTolerance}}**.
4. A **{{location_latitude_coord2}}** (**{{degrees2}}**) value becomes a breach when it is **{{.l1}}** than **{{location_latitude_coord2ReferenceValue}}** minus **{{location_latitude_coord2Tolerance}}**.
5. A **{{location_longitude_coord}}** (**{{degrees3}}**) value becomes a breach when it is **{{.g4}}** than **{{location_longitude_coordReferenceValue}}** plus **{{location_longitude_coordTolerance}}**.
6. A **{{location_longitude_coord2}}** (**{{degrees4}}**) value becomes a breach when it is **{{.l2}}** than **{{location_longitude_coord2ReferenceValue}}** minus **{{location_longitude_coord2Tolerance}}**.
7. The **{{time to deploy}}** (**{{s}}**) value becomes a breach when it is **{{.g5}}** than **{{TTDReferenceValue}}** plus **{{TTDTolerance}}**.

## SLA Exclusions
The Service Commitment does not apply to interferences: (i) caused by factors outside of our reasonable control; (ii) that result from any actions or inactions of you or any third party; (iii) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); or (iv) arising from our suspension or termination of your right to use the spectrum resource in accordance with the Order Agreement (collectively, the \\\"SLA Exclusions\\\").
## Definitions
A \"Service Credit\" is a euro credit, calculated as set forth above, that we may credit back to an eligible account."
```

2.3.4. Use Case 2 scenarios

The scenarios and test cases identified in D5.1 [2], and reported in the following sections, are designed to demonstrate the functionality and features of the different components and workflows of the 5GZORRO Marketplace involved in UC2. Table 17 lists the tests reported in this deliverable (according to the test plan reported in D5.1 [2] and the tests already demonstrated in D5.2 [3]) along with updated descriptions in view of the final 5GZORRO platform prototypes.

Table 17: List of UC2 tests with results in D5.3

Original tests in scope of D5.3	Comments	Applicable Scenario
Test UC2.6a: Selection of a spectrum resource offer	Section 2.3.4.1.3	Scenario 2.2: Resource selection by the resource consumer
Test UC2.6b: Selection of a slice offer	Section 2.3.4.1.2	Scenario 2.2: Resource selection by the resource consumer
Test UC2.8: Selection of a radio resource offer	Section 2.3.4.1.4	Scenario 2.2: Resource selection by the resource consumer
Test UC2.9a: Automatic selection of resources and slice composition	This test shows the intent-based search capabilities to find and select the resources, and	Scenario 2.2: Resource selection by the resource consumer

	the steps to compose a slice and purchase it. Section 2.3.4.1.1	
Test UC2.9b: Deployment of a slice with configurable radio infrastructure	Section 2.3.4.2.1	Scenario 2.3: SLA monitoring
Test UC2.9c: Deployment of a slice with non-configurable radio infrastructure	Section 2.3.4.2.2	Scenario 2.3: SLA monitoring
Test UC2.9d: Spectrum telemetry collection	Section 2.3.4.2.3	Scenario 2.3: SLA monitoring
Test UC2.9e: SLA breach detection on time to deploy spectrum	Not considered in the final evaluation; involves same features and workflows as UC2.9f and UC2.9g.	Scenario 2.3: SLA monitoring
Test UC2.9f: SLA breach detection on interference levels	Section 2.3.4.2.4	Scenario 2.3: SLA monitoring
Test UC2.9g: SLA breach detection on geofencing spectrum	Section 2.3.4.2.4	Scenario 2.3: SLA monitoring
Test UC2.9h: SLA breach correction on time to deploy spectrum	Not considered in the final evaluation; involves same features and workflows as UC2.9i and UC2.9j.	Scenario 2.3: SLA monitoring
Test UC2.9i: SLA breach correction on interference levels	Merged in test UC2.9f Section 2.3.4.2.4	Scenario 2.3: SLA monitoring
Test UC2.9j: SLA breach correction on geofencing spectrum	Merged in test UC2.9g Section 2.3.4.2.4	Scenario 2.3: SLA monitoring

2.3.4.1. Scenario 2.2: Resource selection by the resource consumer

This scenario aims at testing the selection and ordering of the different kinds of resource offers needed in 5GZORRO to compose a non-configurable and a configurable slice. The result of the consumption of the offers will always be a smart contract and, in case of a spectrum offer, a “derivative” spectoken. The tests described in this section demonstrate the procedures of intent-based search, slice order (non-configurable slice), and radio and spectrum orders (configurable slice).

2.3.4.1.1. Selection of resources based on Intent-based search

In order to find available offers, the 5GZORRO platform enables the consumers to perform intent-based searches in the portal by means of the Smart Resource and Service Discovery (SRSD). The developed intent-based search allows to use and combine specific keywords like “spectrum”, “slice”, the required band or the required location. In this UC we have tested the performance of this component when using the following searches: (i) “I want a slice in band 77 in Barcelona”, (ii) “I want a spectrum in band 77 in Barcelona”, and (iii) “I want a spectrum and slice in band 77 in Barcelona”.

¡Error! No se encuentra el origen de la referencia.5, Figure 266 and Figure 277 show the results of a slice, a spectrum, and a combined slice and spectrum intent-based search, respectively. Note the obtained list shows the associated trust-score of the offer, which quantifies the trust and reputation between the provider of the offer and the consumer.

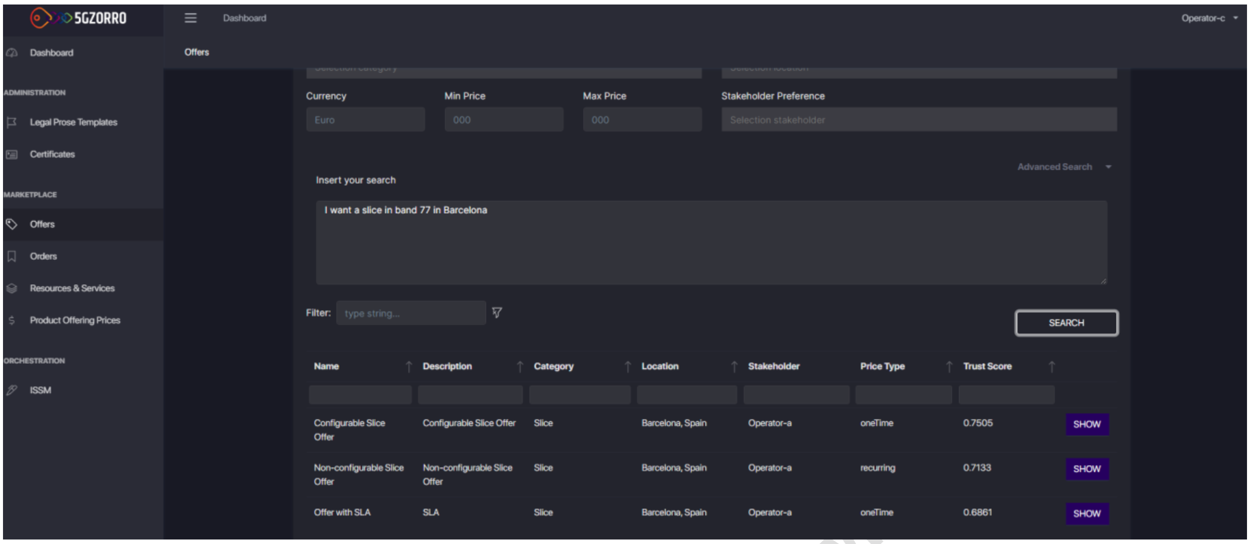


Figure 25: Intent-based search (slice)

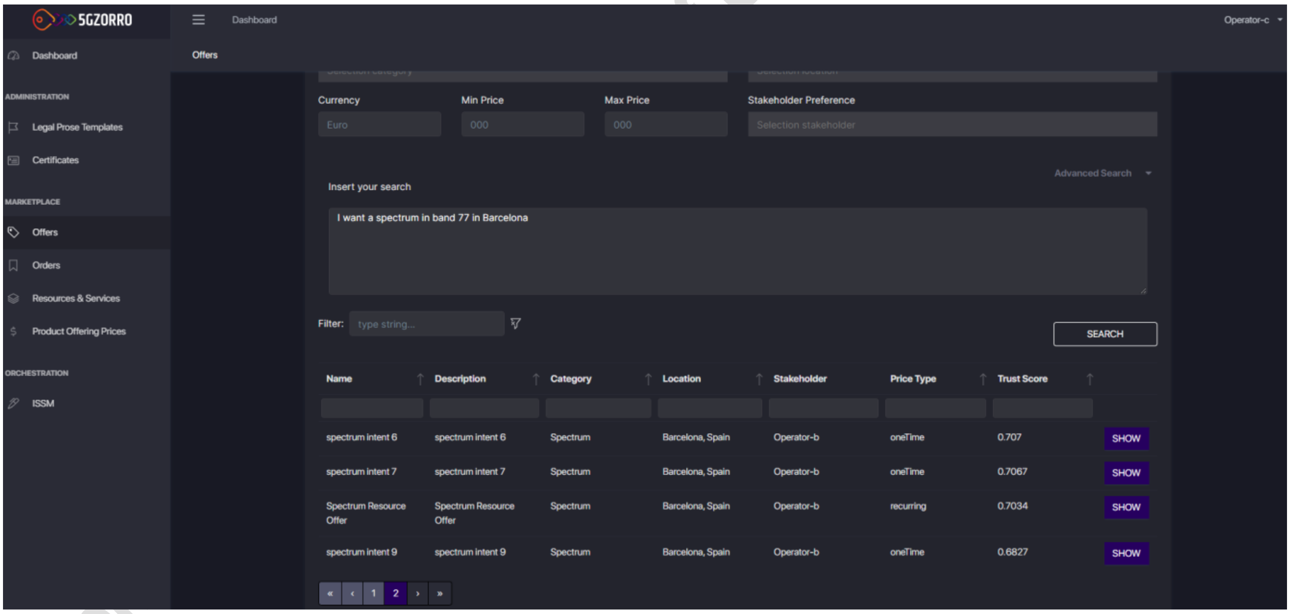


Figure 26: UC2.9a: Intent-based search (spectrum)

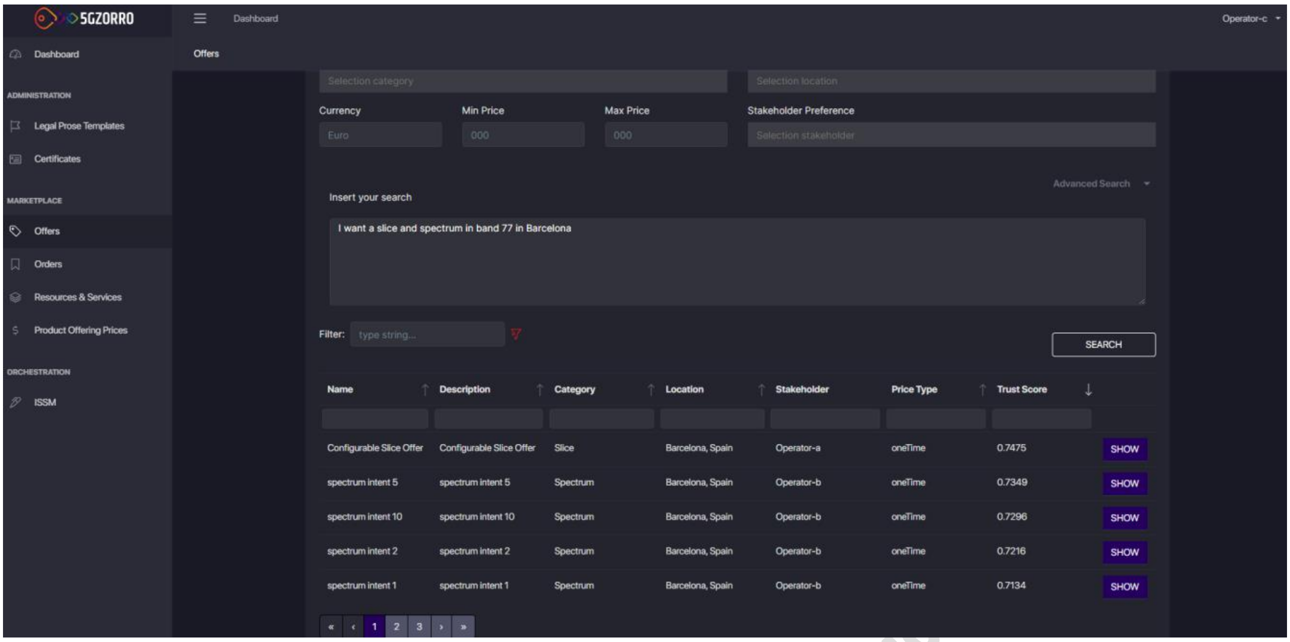


Figure 27: UC2.9a: Intent-based search (slice and spectrum)

The following table reports the findings for the UC2 test associated with this intent-based search feature.

Table 18: Intent-based search of slice and spectrum resources

UC2.9a	**Selection of resources based on Intent-based search**	
Testbed	5GBarcelona	
Description	The resource consumer (RC) realizes an intent-based search in the marketplace to find the spectrum and slice resources being offered.	
Use-case functionalities	Intent-based search of resources present in the catalogue. Utilization of trust values to order the results.	
Key Use-case requirements and KPIs	**[KPI1.1]** Support actual distributed multi-party service and business configurations. **[KPI4.1]** Automatically discover and "inventorize" various types of resources (i.e., compute, storage, network at core, edge, far-edge), spectrum and services capabilities from different domains and service providers **[KPI5.3]** The authenticity of the market agents, preventing double spending that would allow an agent to trade spectrum rights that it does not own. **[KPI7.1**] Lab validation environments for the three use cases.	
Components	Portal 5GZORRO Catalogue Smart Resource and Service Discovery (SRSD) 5G Trust and Reputation Management Framework (5G-TRMF)	
Test Procedure	Pre-conditions	Resource consumers and providers are onboarded Resources are onboarded and offered in the Marketplace
	Test Case steps	The RC logs in the Portal The RC opens the Offers page and uses Advanced Search The RC enters the required intent-based search
Measurements	Methodology	Video and screenshots.
	Complementary measurements	Measure the time it takes the Marketplace to return the offers
	Calculation process	Measured by inspecting the Portal and obtaining the time needed for showing the offers

Result	The offers are shown in the correspondent view. **[KPI1.1]** The KPI target was set to more than 3 providers/operators. In this test, Operator C searches for the resources offered by two additional operators (Operator A and B). Regulator was needed to permit spectrum orders from Operator B and the creation of the non-configurable order by Operator A.. **[KPI4.1]** The KPI target was set to distribution of resource updates and discovery in less than 10 mins**.** With 32 offers in the Marketplace, the average times for the intent-based search to return existent offers were: 7.2s (slice), 5.8s (spectrum) and 9.9s (spectrum and slice). With 42 offers (10 additional spectrum offers), the average times were: 7.7s (slice), 10.7s (spectrum) and 15.9s (spectrum and slice). **[KPI5.3]** KPI target was to verify the built-in property of Blockchains. This was determined during the on-boarding process as reported in D5.2 [3] **[KPI7.1]** KPI target was 3 lab testing environments**.** Tests were performed in the testing environment for UC3 in 5GBarcelona.

2.3.4.1.2. Selection and order of a slice offer (non-configurable slice)

Once selecting the needed resources and offers, the next step for a consumer is to order the resources through the Marketplace. As aforementioned, in UC2 we have considered two different types of slices: non-configurable and configurable. In the first case, the Resource Consumer only needs to acquire a slice offer, which already contains a spectrum resource (i.e., Operator A provides both the slice and the spectrum). In such a case, a derivative spectoken is generated after the first transaction involving this slice (and the associated spectrum), with the Provider as issuer and holder, since the rights and obligations regarding the spectrum are maintained by this operator.

Figure 288 shows the non-configurable slice offer ordered by the RC, including the details of its non-configurable characteristics (accessible through show button).

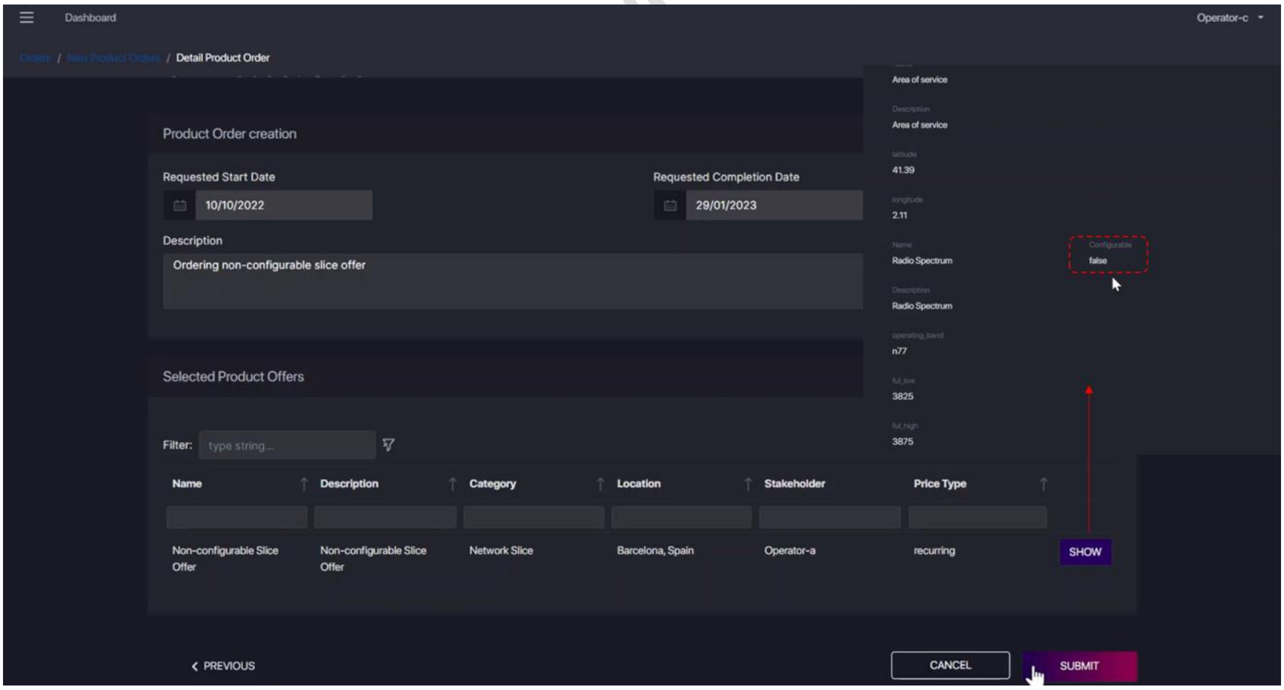


Figure 28: UC2.6b: Non-configurable slice order

Figure 299 and Figure 3030 show the status of the marketplace (Consumer and Provider views, respectively) after the transaction.

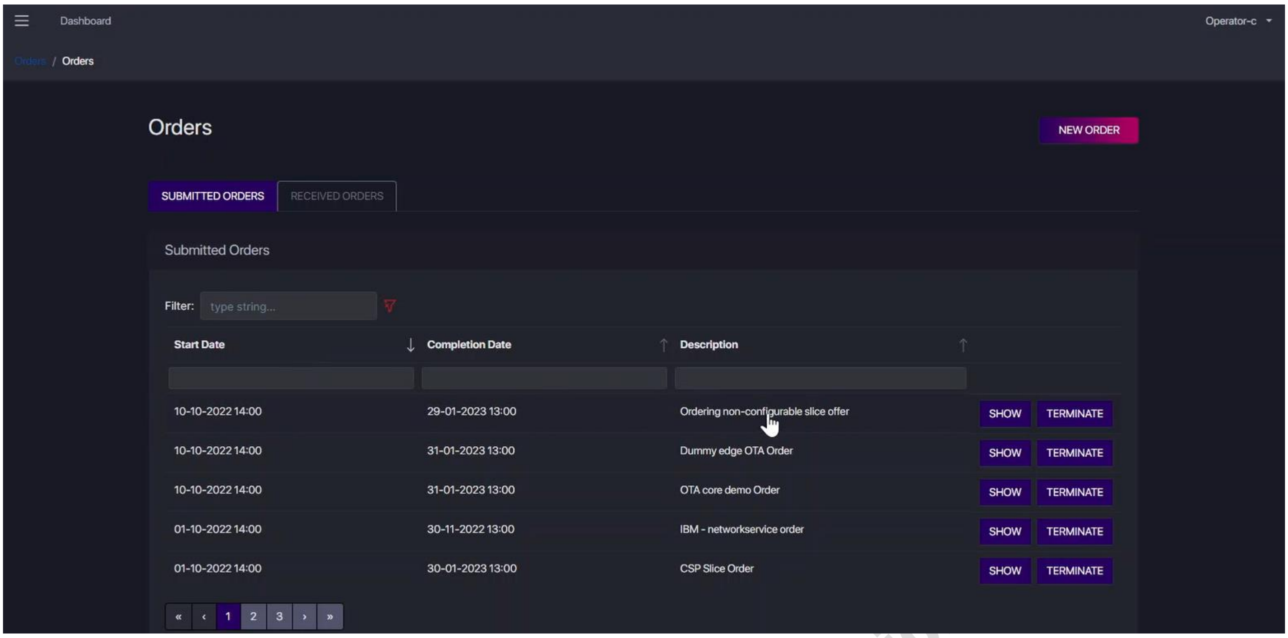


Figure 29: UC2.6b: Non-configurable slice order becomes active in the marketplace (consumer)

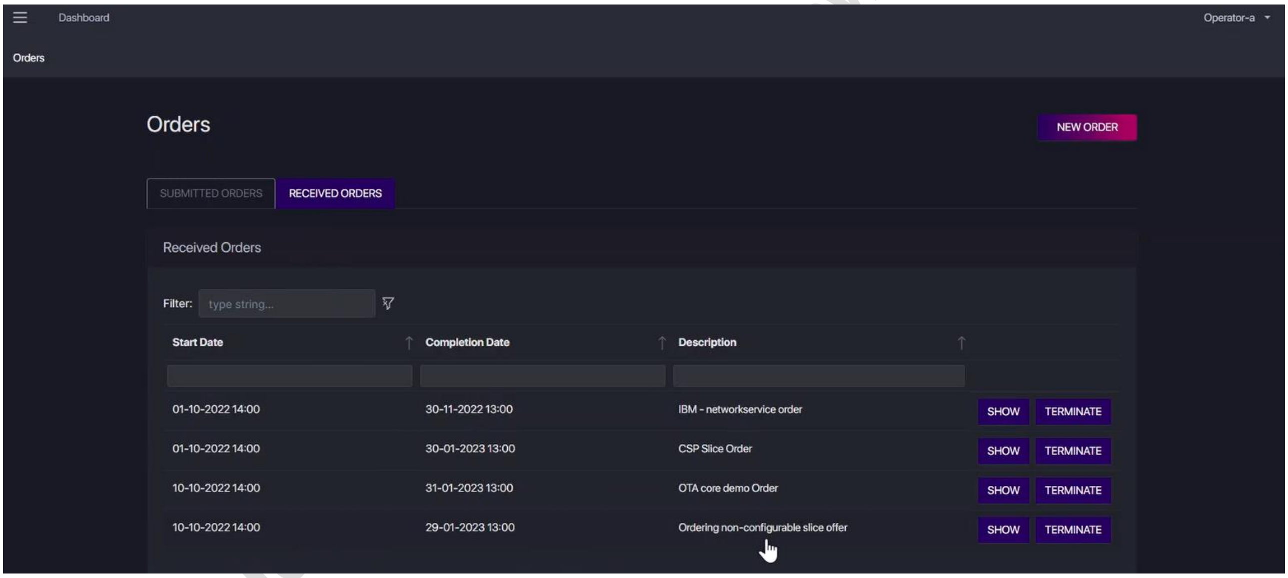


Figure 30: UC2.6b: Non-configurable slice order becomes active in the marketplace (provider)

Finally, Figure 3131 shows the content of CORDA's Vault (Operator A), which is accessible through the Smart Contract Life-Cycle Management (SCLCM) component.

```
[
  {
    "id": "012963c1-a3e1-4668-9eaf-0ce2637dbe7c",
    "startDl": 3800,
    "endDl": 4200,
    "startUl": 3800,
    "endUl": 4200,
    "startDate": "2021-05-17T00:00:00.000+00:00",
    "endDate": "2036-05-16T00:00:00.000+00:00",
    "duplexMode": "TDD",
    "band": 77,
    "technology": "5G",
    "country": "Spain",
    "ownerDid": "OD1ndI3xw0Pi6S14rgoa6F",
    "license": "Y5UnLgeudNLd6rooZh3YRy"
  }
]
```

(a) Primitive spectoken


```
[
  {
    "id": "9300ad53-51bd-4bae-a124-9492abfe3992",
    "startDl": 3825,
    "endDl": 3875,
    "startUl": 3825,
    "endUl": 3875,
    "startDate": "2022-10-10T10:00:00.000+00:00",
    "endDate": "2023-01-31T11:00:00.000+00:00",
    "duplexMode": "TDD",
    "band": 77,
    "technology": "5G",
    "country": "Spain",
    "price": 100,
    "primitiveId": "012963c1-a3e1-4668-9eaf-0ce2637dbe7c",
    "offerDid": "M7PMfY8wncM6Ej9MXKe8bM"
  }
]
```

(b) Derivative spectoken


```
[
  {
    "id": "5a9f790f-6433-4339-a286-1574f1792c91",
    "issuer": "RegulatorA",
    "holder": "OperatorA",
    "tokenType": "PrimitiveSpecTokenType - 012963c1-a3e1-4668-9eaf-0ce2637dbe7c"
  },
  {
    "id": "af484be1-9c93-463e-ae21-47d074a61ea5",
    "issuer": "OperatorA",
    "holder": "OperatorA",
    "tokenType": "DerivativeSpecTokenType - 9300ad53-51bd-4bae-a124-9492abfe3992"
  }
]
```

(c) NFTs

Figure 31: UC2.6b: (a) Primitive spectoken, (b) derivative spectoken and (c) associated Non Fungible Tokens (NFTs).

The following table reports the findings for the UC2 test associated with selection and order of a slice offer (non-configurable case).

Table 19: Selection and order of a slice offer (non-configurable slice)

UC2.6b	**Selection and order of a slice offer**	
Testbed	5GBarcelona	
Description	The resource consumer (RC) selects and orders a specific non-configurable slice through the portal.	
Use-case functionalities	Selection and order of a resource offer of type non-configurable slice present in the catalogue. Smart Contract Lifecycle Management. Derivative spectoken generation.	
Key Use-case requirements and KPIs	**[KPI1.1]** Support actual distributed multi-party service and business configurations. **[KPI5.3]** The authenticity of the market agents, preventing double spending that would allow an agent to trade spectrum rights that it does not own. **[KPI7.1]** Lab validation environments for the three use cases.	
Components	Portal 5GZORRO Catalogue Marketplace DLT Smart Contract Life-Cycle Manager (SCLCM) Governance DLT	
Test Procedure	Pre-conditions	Resource consumers and providers are onboarded Resources are onboarded and offered in the Marketplace The catalogue contains a non-configurable slice offer Resource consumer has done an intent-based search and knows which offer to acquire

	Test Case steps	The RC logs in the Portal The RC opens the Orders page and searches for the non-configurable offer The RC enters the required intent-based search The RC acquires the offer The offer becomes active in the Marketplace according to the generated smart contract. A derivative spectoken is generated (if first order using this slice and spectrum), being hold by the Provider
Measurements	Methodology	Video and screenshots
	Complementary measurements	none
	Calculation process	Observation from the Portal CORDA's Vault content (Provider)
Result	The generated orders are shown in the correspondent view. **[KPI1.1]** The KPI target was set to more than 3 providers/operators. In this test, Operator C selects the slice resources offered by Operator A. Regulator was needed to permit the creation of the non-configurable slice order (with an associated spectrum resource) by Operator A. **[KPI5.3]** KPI target was to verify the built-in property of Blockchains. This was determined during the on-boarding process as reported in D5.2 [3] **[KPI7.1]** KPI target was 3 lab testing environments. Tests were performed in the testing environment for UC3 in 5GBarcelona.	

2.3.4.1.3. Selection and order of a spectrum offer (configurable slice)

In the second case, the Resource Consumer (Operator C) acquires a spectrum offer from the Spectrum Provider (Operator B) and a slice offer from the Resource Provider (Operator A). The first transaction also comprehends the generation of a derivative spectoken, which is issued by Operator B and hold by Operator C, since in this case the rights of obligations to use the spectrum are temporary transferred to the consumer. Figure 322 shows the spectrum resource offer ordered by the RC through the Marketplace.

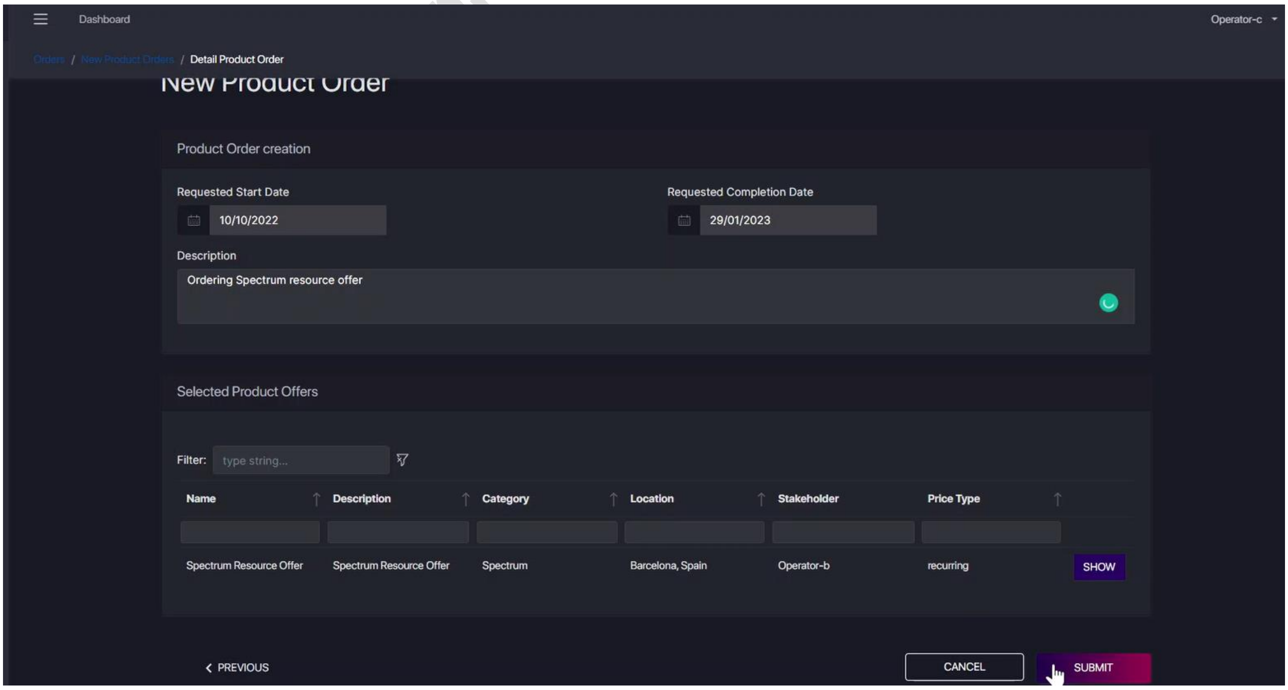


Figure 32: UC2.6a: Spectrum offer order

Figure 333 and Figure 344 show the status of the marketplace (Consumer and Spectrum Provider views, respectively) after the transaction.

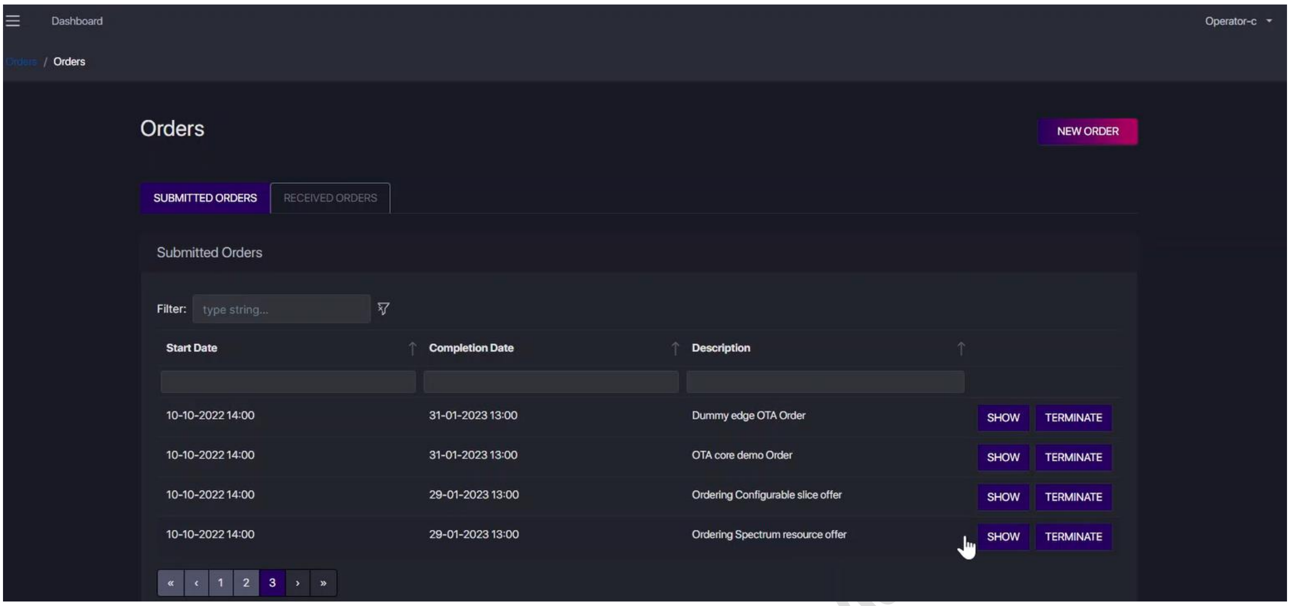


Figure 33: UC2.6a: Spectrum resource order becomes active in the marketplace (Consumer)

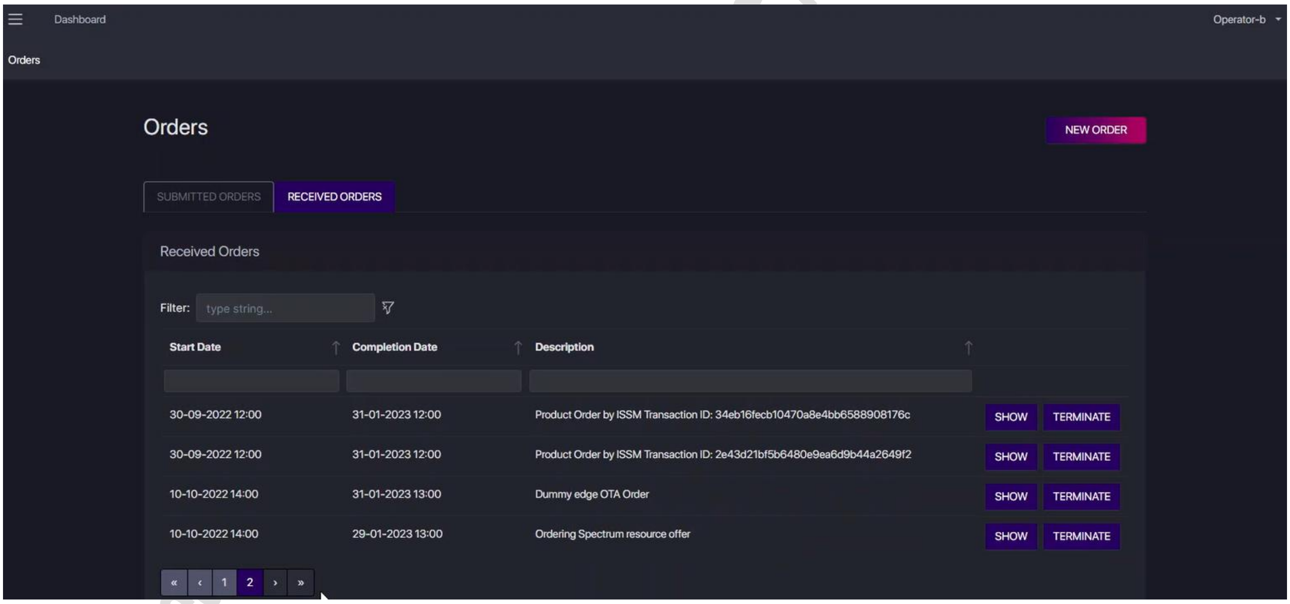


Figure 34: UC2.6a: Spectrum resource order becomes active in the marketplace (Provider)

Figure 355 and Figure 366 show the content of CORDA's Vault from Operator C and Operator B, respectively, after the transaction, which is accessible through the SCLCM component.

```
[
  {
    "id": "7b61bd38-0734-4579-bbc0-8b1e27e67aae",
    "startDl": 3700,
    "endDl": 3800,
    "startUl": 3700,
    "endUl": 3800,
    "startDate": "2021-05-17T00:00:00.000+00:00",
    "endDate": "2036-05-16T00:00:00.000+00:00",
    "duplexMode": "TDD",
    "band": 77,
    "technology": "5G",
    "country": "Spain",
    "ownerDid": "V7GMvKbYXujtJhZwiBdxCu",
    "license": "4vVX5mRvu3NMJNQtbRwLQB"
  }
]
```

(a) Primitive spectoken


```
[
  {
    "id": "1a2ef95a-9510-464b-bf36-ff2f451d09c7",
    "issuer": "RegulatorA",
    "holder": "OperatorB",
    "tokenType": "PrimitiveSpecTokenType - 7b61bd38-0734-4579-bbc0-8b1e27e67aae"
  }
]
```

(b) NFT Operator-B

Figure 35: UC2.6a: (a) Primitive spectoken and (b) associated NFT (Spectrum provider).


```
[
  {
    "id": "d10ea95e-e1b3-41a3-ba38-008006a1f460",
    "startDl": 3700,
    "endDl": 3750,
    "startUl": 3700,
    "endUl": 3750,
    "startDate": "2022-10-10T10:00:00.000+00:00",
    "endDate": "2023-01-31T11:00:00.000+00:00",
    "duplexMode": "TDD",
    "band": 77,
    "technology": "5G",
    "country": "Spain",
    "price": 1000,
    "primitiveId": "7b61bd38-0734-4579-bbc0-8b1e27e67aae",
    "offerDid": "Bk55zLjp38XZicd8ZeoJ1d"
  }
]
```

(a) Derivative spectoken


```
[
  {
    "id": "c02a4aa7-bee2-453f-9767-26135cbfa364",
    "issuer": "OperatorB",
    "holder": "OperatorC",
    "tokenType": "DerivativeSpecTokenType - d10ea95e-e1b3-41a3-ba38-008006a1f460"
  }
]
```

(b) NFT Operator-C

Figure 36: UC2.6a: (a) Derivative spectoken and (b) associated NFT (Spectrum Consumer).

The following table reports the findings for the UC2 test associated with selection and order of a spectrum offer (configurable case).

Table 20: Selection and order of a spectrum offer (configurable slice)

UC2.6a	**Selection and order of a spectrum offer**	
Testbed	5G Barcelona	
Description	The resource consumer (RC) selects and orders a specific spectrum offer through the portal.	
Use-case functionalities	Selection and order of a spectrum offer present in the catalogue. Smart Contract Lifecycle Management. Derivative spectoken generation.	
Key Use-case requirements and KPIs	**[KPI1.1]** Support actual distributed multi-party service and business configurations. **[KPI5.3]** The authenticity of the market agents, preventing double spending that would allow an agent to trade spectrum rights that it does not own. **[KPI7.1**] Lab validation environments for the three use cases.	
Components	Portal 5GZORRO Catalogue Marketplace DLT Smart Contract Life-Cycle Manager (SCLCM) Governance DLT	
Test Procedure	Pre-conditions	Resource consumers and providers are onboarded Resources are onboarded and offered in the Marketplace The catalogue contains at least one spectrum offer.

		Resource consumer has done an intent-based search and knows which offer to acquire
	Test Case steps	The RC logs in the Portal The RC opens the Orders page and searches for a spectrum offer. The RC enters the required intent-based search The RC acquires the offer The offer becomes active in the Marketplace according to the generated smart contract. A derivative spectoken is generated, being hold by the Consumer.
Measurements	Methodology	Video and screenhots.
	Complementary measurements	none
	Calculation process	Observation from the Portal CORDA’s Vault content (Provider and Consumer)
Result	The generated offers are shown in the correspondent view. **[KPI1.1]** The KPI target was set to more than 3 providers/operators. In this test, Operator C selects the spectrum resources offered by Operator B. Regulator was needed to permit the creation the spectrum resource offers. **[KPI5.3]** KPI target was to verify the built-in property of Blockchains. This was determined during the on-boarding process as reported in D5.2 [3] **[KPI7.1]** KPI target was 3 lab testing environments**.** Tests were performed in the testing environment for UC3 in 5GBarcelona.	

2.3.4.1.4. Selection and order of a radio offer (configurable slice)

Finally, in the configurable slice scenario, the Resource Consumer also needs to acquire a slice with configurable radio resources. In this case, this transaction does not trigger the generation of a spectoken, since no spectrum resource is involved. Figure 377 shows the configurable slice offer ordered by the RC, including the detail of its configurable radio resources (accessible through show button). Once acquired, the order becomes active in the portal as it was shown in the non-configurable case.

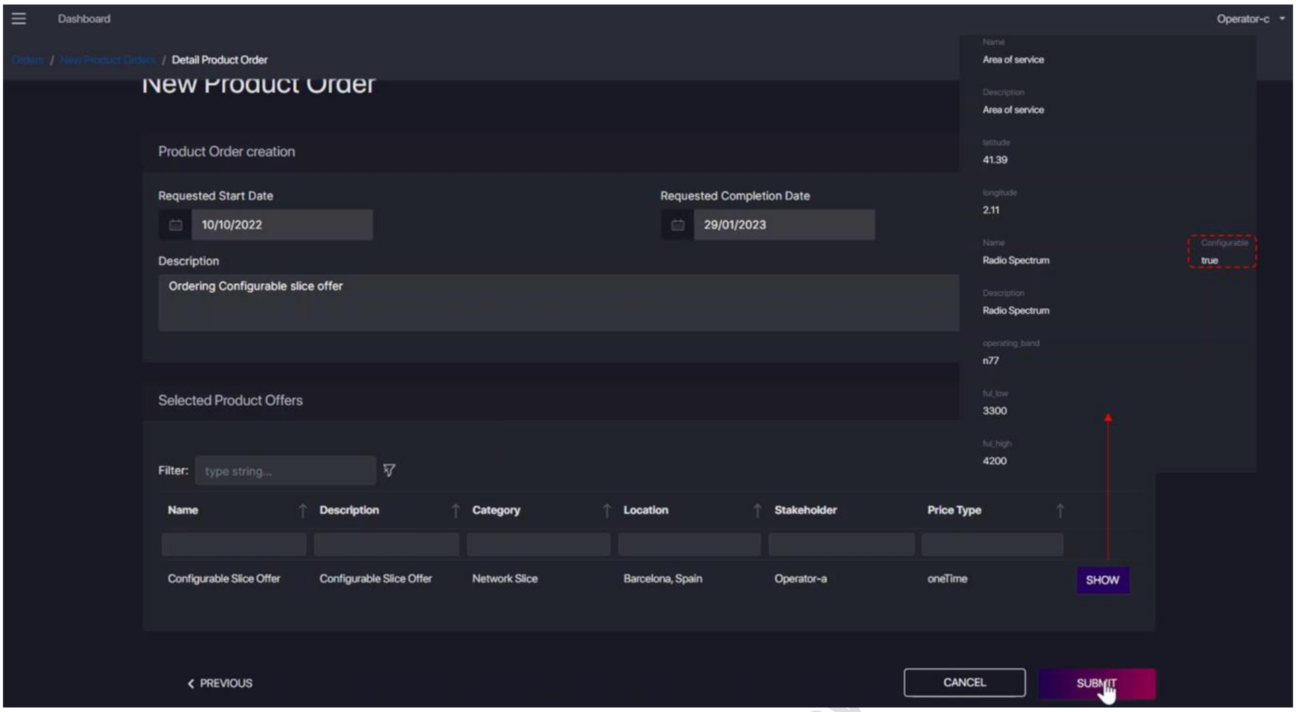


Figure 37: UC2.8: Order of a slice with configurable radio resources

Results of this test case are summarized in the following table.

Table 21: Selection and order of a radio offer (configurable slice)

UC2.8	**Selection and order of a radio offer**	
Testbed	5GBarcelona	
Description	The resource consumer (RC) selects and orders a specific slice with configurable radio resources through the portal.	
Use-case functionalities	Selection and order of a resource offer of type configurable slice present in the catalogue. Smart Contract Lifecycle Management.	
Key Use-case requirements and KPIs	**[KPI1.1]** Support actual distributed multi-party service and business configurations. **[KPI5.3]** The authenticity of the market agents, preventing double spending that would allow an agent to trade spectrum rights that it does not own. **[KPI7.1]** Lab validation environments for the three use cases	
Components	Portal 5GZORRO Catalogue Marketplace DLT Smart Contract Life-Cycle Manager (SCLCM) Governance DLT	
Test Procedure	Pre-conditions	Resource consumers and providers are onboarded Resources are onboarded and offered in the Marketplace The catalogue contains a configurable slice offer Resource consumer has done an intent-based search and knows which offer to acquire
	Test Case steps	The RC logs in the Portal The RC opens the Orders page and searches for the configurable offer The RC enters the required intent-based search

		The RC acquires the offer The offer becomes active in the Marketplace according to the generated smart contract.
Measurements	Methodology	Video and screenshots
	Complementary measurements	none
	Calculation process	Observation from the Portal
Result	The generated orders are shown in the correspondent view. **[KPI1.1]** The KPI target was set to more than 3 providers/operators. In this test, Operator C selects the slice resources offered by Operator A. **[KPI5.3]** KPI target was to verify the built-in property of Blockchains. This was determined during the on-boarding process as reported in D5.2 [3] **[KPI7.1]** KPI target was 3 lab testing environments**.** Tests were performed in the testing environment for UC3 in 5GBarcelona.	

2.3.4.2. Scenario 2.3: SLA monitoring

The slice deployment is the means to start a service over the radio nodes and start collecting spectrum-related telemetry data. We considered two differentiated scenarios, associated to non-configurable and configurable slices, as was introduced in Section 2.3.4.1.

From the point of view of the SLA breach monitoring and correction services, the main spectrum metrics considered in these tests are:

- Interference levels
- Location of the radio stations

SLA breaches are detected according to metric values and to the methods and thresholds defined in the SLAs of the spectrum and/or slice offerings, as was described in Section 2.3.3. Once detected, SLA breaches lead to specific procedures in the marketplace, according to the commitment specified in the SLAs. In particular, in this deliverable we demonstrate service termination and spectoken redeem in case of SLA breaches caused by the Resource Consumer (geofencing spectrum breach scenario), and the trust-score update in the case of SLA breaches caused by the Resource Provider (interference breach scenario). For the sake of simplicity, metric values were emulated in the Prometheus Exporters of the involved gNBs, since focus was on demonstrating the 5GZORRO's platform workflows and functionalities, not on capturing real RAN metrics.

2.3.4.2.1. Deployment of a slice with configurable radio infrastructure

In the case of the non-configurable slice, once the Consumer acquires a slice resource with configurable radio resources and a compatible spectrum resource (i.e., the RAN resources can be configured according to the spectrum characteristics), it is able to deploy it through the Intelligent Slice and Service Manager (ISSM). As shown in Figure 388, when selecting a configurable slice, the platform ensures that the Consumer also provides the spectrum order needed to instantiate it.

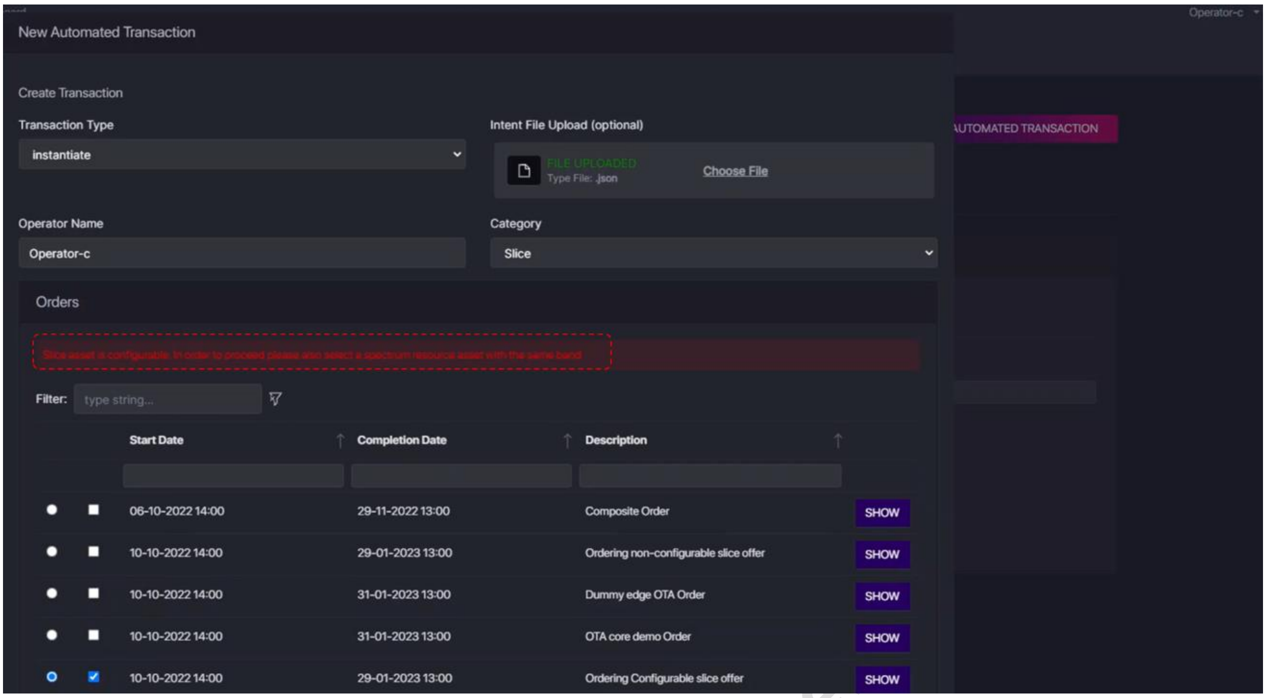


Figure 38: UC2.9b: Error while instantiating a configurable slice without a valid spectrum resource.

Figure 399 shows the creation of the slice deployment transaction. This triggers the automated operation of the different components involved in the slice deployment (i.e., ISSM, Network Slice and Service Orchestration (NSSO), xRM), which finalizes with the instantiation of the 5GCore and the configuration of the 5G RAN to provide the required service. As depicted in the figure, the consumer only needs to specify some parameters related to the service configuration (e.g., PLMNID, DNN, allowed IMSIs…).

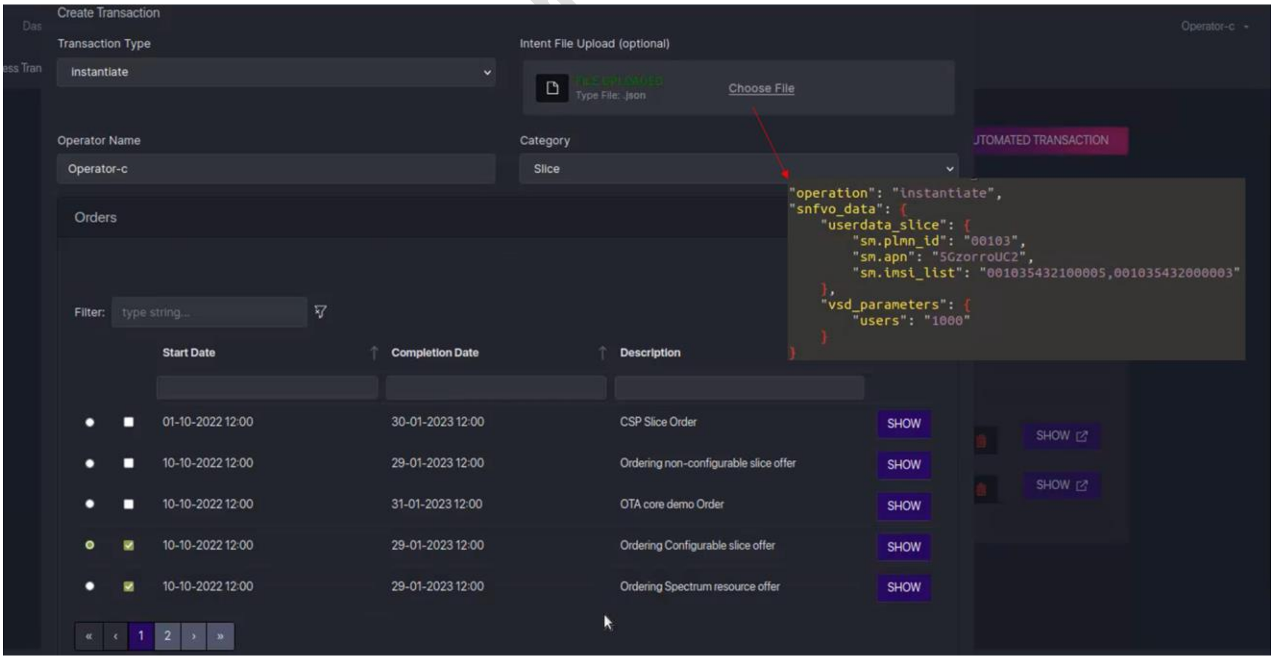


Figure 39: UC2.9b: Configurable slice instantiation

As aforementioned, the deployment of the slice instance triggers the operation of different platform components, including the ISSM of Operator C (Consumer), and the ISSM, the NSSO and the xRM of

Operator A (Slice provider). Figure 4040 and Figure 4141 show different screenshots of the different automated procedures managed by the ISSM.

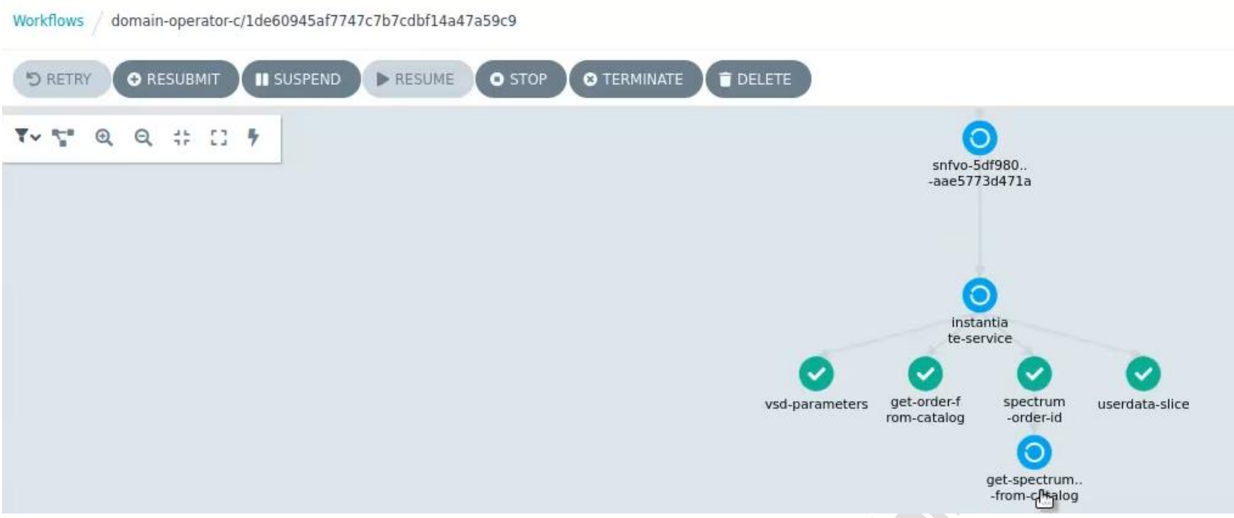


Figure 40: UC2.9: ISSM operations (Operator C)

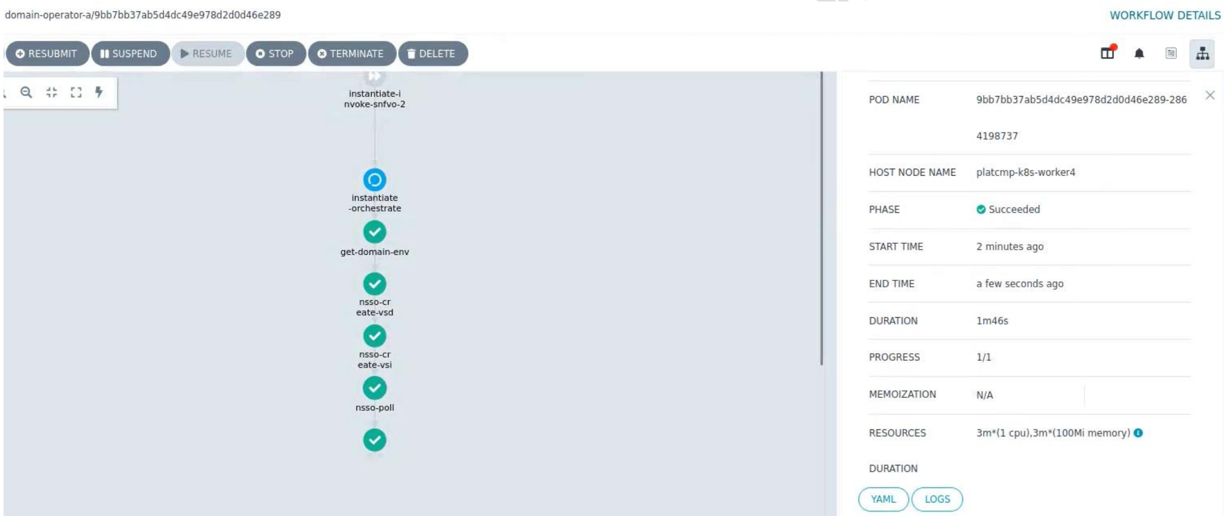


Figure 41: UC2.9: ISSM operations (Operator A)

Finally, the 5G Core gets deployed through the VIM and the 5G RAN gets configured according to the spectrum and slice parameters, allowing UEs to connect, as shown in Figure 422 and Figure 433, and finalizing the slice instantiation as depicted in Figure 444.

Figure 42: UC2.9b: 5G RAN (Amarisoft) configuration based on spectrum and slice parameters

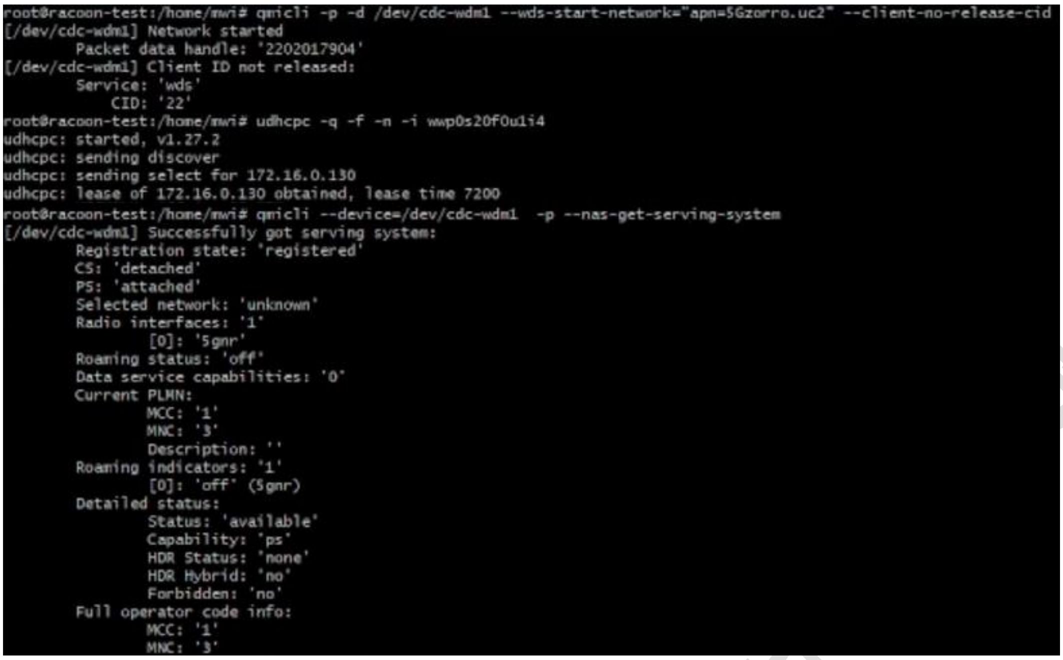


Figure 43: UC2.9b: UE (Quectel RM500Q modem) connection to deployed slice

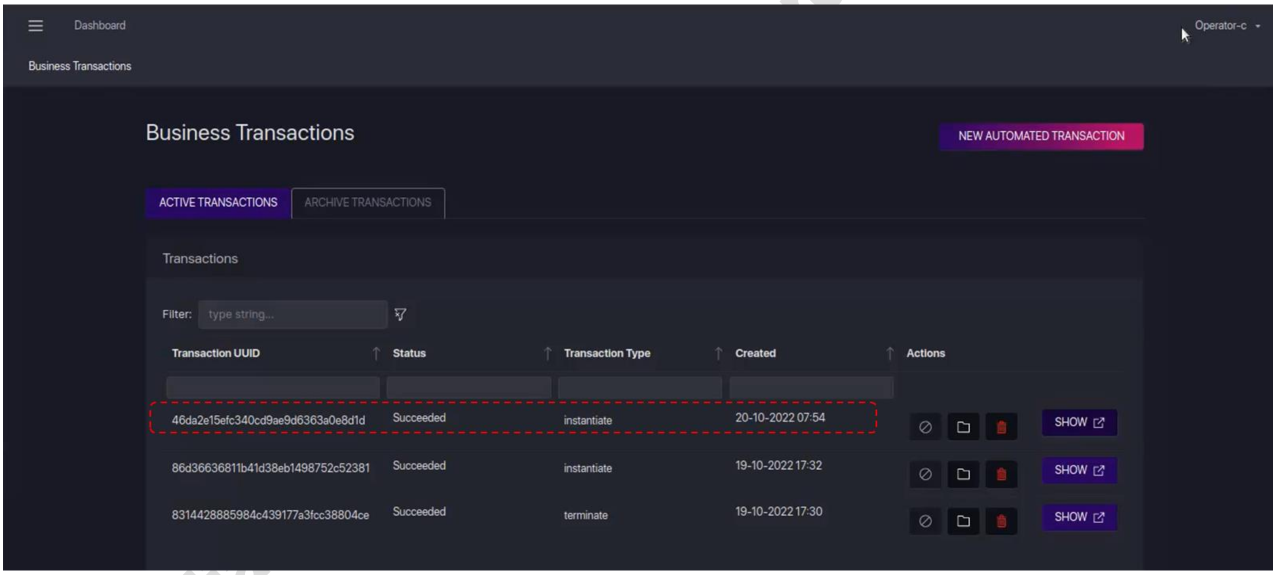


Figure 44: UC2.9b: Successful deployment of a configurable slice

The following table reports the findings for the UC2 test associated with the deployment of a configurable slice.

Table 22: Deployment of a slice with configurable radio

UC2.9b	Deployment of a slice with configurable radio
Testbed	5GBarcelona
Description	The resource consumer deploys a slice over a given geographical area by selecting a set of the radio and spectrum resources that the resource consumer acquired beforehand from the 5GZORRO Marketplace.
Use-case functionalities	Resource consumer performing a slice deployment joining slice and spectrum resources. Slice is deployed and available for UE connections.

Key Use-case requirements and KPIs	**[KPI1.1]** Support actual distributed multi-party service and business configurations. **[KPI5.1]** Time to process and enforce new spectrum transactions (i.e., from the moment the transaction is settled until the spectrum becomes available). **[KPI5.3]** The authenticity of the market agents, preventing double spending that would allow an agent to trade spectrum rights that it does not own. **[KPI7.1**] Lab validation environments for the three use cases	
Components	Portal Intelligent Slice and Service Manager Network Slice and Service Orchestrator (NSSO) Radio Resource Controller (rRM)	
Test Procedure	Pre-conditions	Resource consumer has acquired spectrum and configurable slice resources Resources are still available
	Test Case steps	The RC logs in the Portal The RC opens the ISSM page and selects “Instantiate” transaction type and “Slice” category The RC onboards an intent file with the characteristics of the slice The RC selects available slice and spectrum orders and triggers the instantiation ISSM (Operator C) onboards, loads and runs the SNFVO Spectrum parameters are retrieved from the spectrum order to configure the RAN Operator-A (slice provider) receives the orchestration request NSSO orchestrate and configure the slice, including 5GCore and RAN resources (spectrum and slice parameters) through the Slice Manager
Measurements	Methodology	Video and screenshots.
	Complementary measurements	Measure time needed for slice deployment.
	Calculation process	Observation from the Portal. ISSM logs. RAN logs and status (gNB, Core, UE).
Result	The slice gets instantiated and can be used by UEs. **[KPI1.1]** The KPI target was set to more than 3 providers/operators. In this test, Operator C selects the slice resources ordered from Operator A and the spectrum resources ordered from Operator B. Slice deployment involves the ISSM of Operator C and A. **[KPI5.1]** KPI target was to complete new spectrum transactions in less than 10 minutes. In this test, performed measurements shown an average between 3 and 4 minutes for deploying a slice once the transaction has been completed. **[KPI5.3]** KPI target was to verify the built-in property of Blockchains. This was determined during the on-boarding process as reported in D5.2 [3] **[KPI7.1]** KPI target was 3 lab testing environments**.** Tests were performed in the testing environment for UC3 in 5GBarcelona	

2.3.4.2.2. Deployment of a slice with non-configurable radio infrastructure

In the case of the non-configurable slice, once the Consumer acquires a slice resource with non-configurable radio resources, it is able to deploy it through the ISSM, since the needed spectrum is already associated with the slice resource. As in the configurable slice case, this triggers the operation of the different components involved in the slice deployment (ISSM, NSSO, xRM), which finalizes with the instantiation of the 5GCore and the configuration of the 5G RAN to provide the required service. For the sake of simplicity and space, screenshots are not included in this subsection since main steps are identical to the configurable use case. The following table reports the findings for this test.

Table 23: Deployment of a slice with non-configurable radio

UC2.9c	**Deployment of a slice with non-configurable radio**	
Testbed	5GBarcelona	
Description	The resource consumer deploys a slice acquired from the 5GZORRO Marketplace.	
Use-case functionalities	Resource consumer performing a slice deployment. Slice is deployed and available for UE connections.	
Key Use-case requirements and KPIs	**[KPI1.1]** Support actual distributed multi-party service and business configurations. **[KPI5.1]** Time to process and enforce new spectrum transactions (i.e., from the moment the transaction is settled until the spectrum becomes available). **[KPI5.3]** The authenticity of the market agents, preventing double spending that would allow an agent to trade spectrum rights that it does not own. **[KPI7.1**] Lab validation environments for the three use cases	
Components	Portal Intelligent Slice and Service Manager Network Slice and Service Orchestrator (NSSO) Radio Resource Controller (rRM)	
Test Procedure	Pre-conditions	Resource consumer has acquired non-configurable slice resources Resources are still available
	Test Case steps	The RC logs in the Portal The RC opens the ISSM page and selects "Instantiate" transaction type and "Slice" category. The RC onboards an intent file with the characteristics of the slice. The RC selects available order and triggers the instantiation. ISSM (Operator C) onboards, loads and runs the SNFVO. Operator-A (slice provider) receives the orchestration request. NSSO orchestrate and configure the slice, including 5GCore and RAN resources (only slice parameters) through the Slice Manager.
Measurements	Methodology	Video and screenshots.
	Complementary measurements	Measure time needed for slice deployment.
	Calculation process	Observation from the Portal. ISSM logs. RAN logs and status (gNB, Core, UE).
Result	The slice gets instantiated and can be used by UEs. **[KPI1.1]** The KPI target was set to more than 3 providers/operators. In this test, Operator C selects the slice resources ordered from Operator A. Slice deployment involves the ISSM of Operator C and A. **[KPI5.1]** KPI target was to complete new spectrum transactions in less than 10 minutes. In this test, performed measurements shown an average between 3 and 4 minutes for deploying a slice once the transaction has been completed. **[KPI5.3]** KPI target was to verify the built-in property of Blockchains. This was determined during the on-boarding process as reported in D5.2 [3]	

	[KPI7.1] KPI target was 3 lab testing environments**.** Tests were performed in the testing environment for UC3 in 5GBarcelona

2.3.4.2.3. Spectrum telemetry collection

Spectrum related telemetry is needed in order to monitor the SLAs associated to the spectrum or slice orders. During slice deployment, the NSSO instructs the Monitoring Data Aggregator (MDA) component to retrieve the needed RAN metrics from the Prometheus Server gathering them (gNBs implement a custom Prometheus Exporter). Then, the MDA periodically sends these metrics to the shared datalake according to a specified period (5 minutes by default). Reported metrics are linked to the transaction ID of the slice instance (see Figure 455), which will be used to identify slices incurring in SLA breaches.

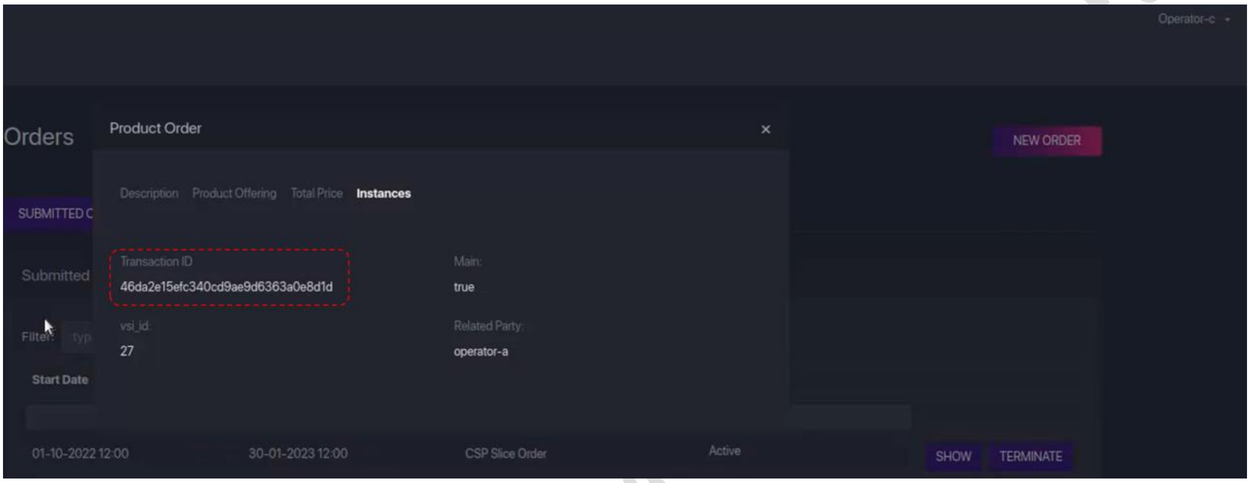


Figure 45: UC2.9d: Transaction ID used to link metrics and slice instances

Figure 466 shows an example of a RAN metric present in the Prometheus Server, while Figure 477 depicts how RAN metrics are incorporated to the datalake, linking them with different IDs like the aforementioned transaction ID or with the resource Id, which is used to get metrics according to a specific label in Prometheus (cell id in this case).

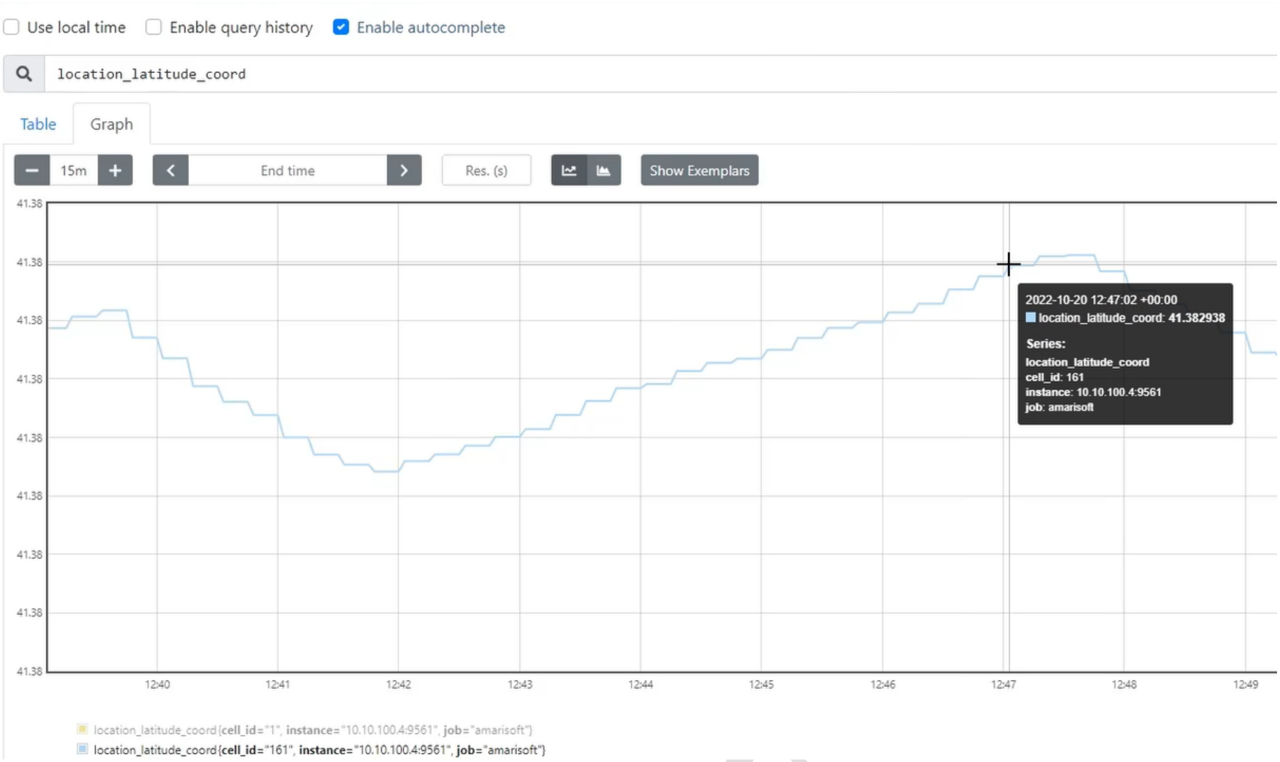


Figure 46: UC2.9d: RAN metrics available at the Prometheus Server


```
{
  "operatorID": "operator-a",
  "transactionID": "46da2e15efc340cd9ae9d6363a0e8d1d",
  "networkID": "6350ff52cd26c7000c33ef94",
  "monitoringData": {
    "metricName": "location_longitude_coord",
    "metricValue": 2.126622,
    "resourceID": "161",
    "instanceID": "6350ff52cd26c7000c33ef94",
    "productID": "P44RJzPQ9NWPE7QTDX4ZhA",
    "timestamp": "2022-10-20 12:38:33.533028"
  }
}
```


Figure 47: UC2.9d: RAN metrics available at the datalake

The following table reports the findings for test UC2.9d.

Table 24: Spectrum telemetry collection

UC2.9d	**Spectrum telemetry collection**
Testbed	5GBarcelona
Description	A slice is deployed with some radio infrastructure. At the deployment time, the radio resource manager of the 5GZORRO platform instructs the radio infrastructure to collect spectrum use metrics.
Use-case functionalities	Resource consumer performing a slice deployment. Slice is deployed and available for UE connections. RAN metrics are incorporated to the datalake and monitored.
Key Use-case requirements and KPIs	**[KPI1.1]** Support actual distributed multi-party service and business configurations.

	[KPI5.5] Ability to enforce the settled spectrum rights and obligations, which will build on lightweight Trusted Execution Environments (TEE) embedded in the radio access points to ensure that the reported spectrum measurements are faithful, and the spectrum allocations settled in the market are enforced. **[KPI7.1**] Lab validation environments for the three use cases	
Components	Radio resource manager (rRM) Monitoring data aggregator (MDA) Network Slice and Service Orchestrator (NSSO) Datalake	
Test Procedure	Pre-conditions	Resource consumer has deployed a slice through the ISSM
	Test Case steps	gNB exposes RAN metrics through Prometheus exporter RAN Prometheus Server gathers metrics MDA gets RAN metrics from the Prometheus Server and exposes them to the datalake
Measurements	Methodology	Video and screenshots
	Complementary measurements	none
	Calculation process	Observation from the Portal, Prometheus Server and datalake.
Result	Spectrum telemetry is available in the datalake. **[KPI1.1]** The KPI target was set to more than 3 providers/operators. In this test, Operator C operated the slice offered by Operator A and the spectrum offered by Operator B. **[KPI5.5]** The KPI target was to be able to detect spoofing attacks where a base station uses an allocation not authorized by the market. This test shows the capability of the base stations to report telemetry associated to the defined SLA and how it is incorporated to the datalake. **[KPI7.1]** KPI target was 3 lab testing environments**.** Tests were performed in the testing environment for UC3 in 5GBarcelona	

2.3.4.2.4. SLA breach detection and correction

During slice deployment, SLA monitoring is configured to monitor the SLA of the slice through an SLA event sent to the datalake by the ISSM. As shown in Figure 488, this event links the transaction ID of the slice with the SLA that was used during offer creation (see Figure 499).

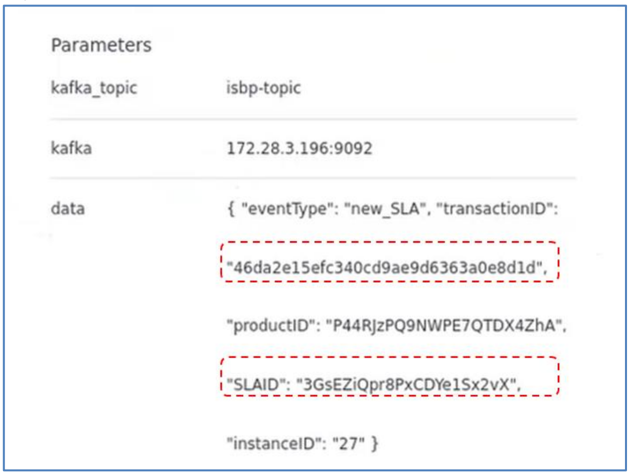


Figure 48: UC2: SLA event generation

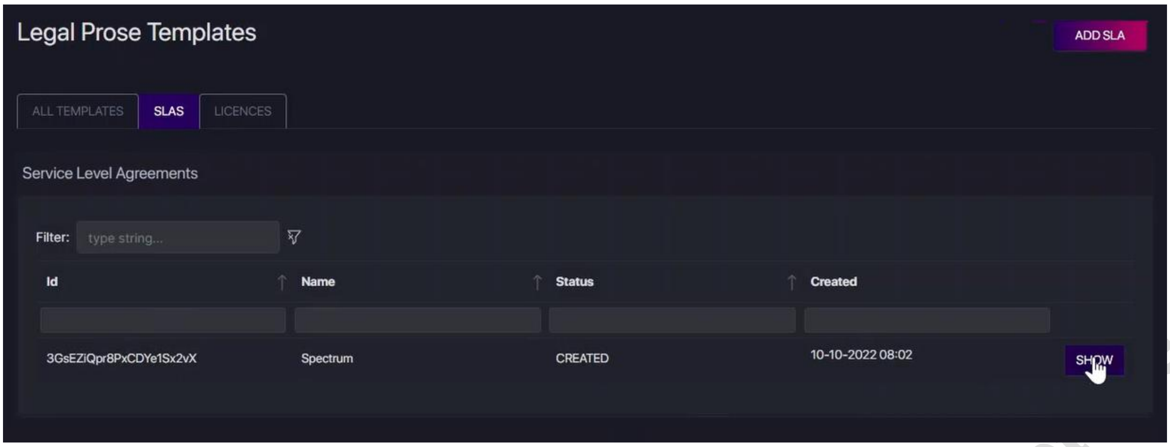
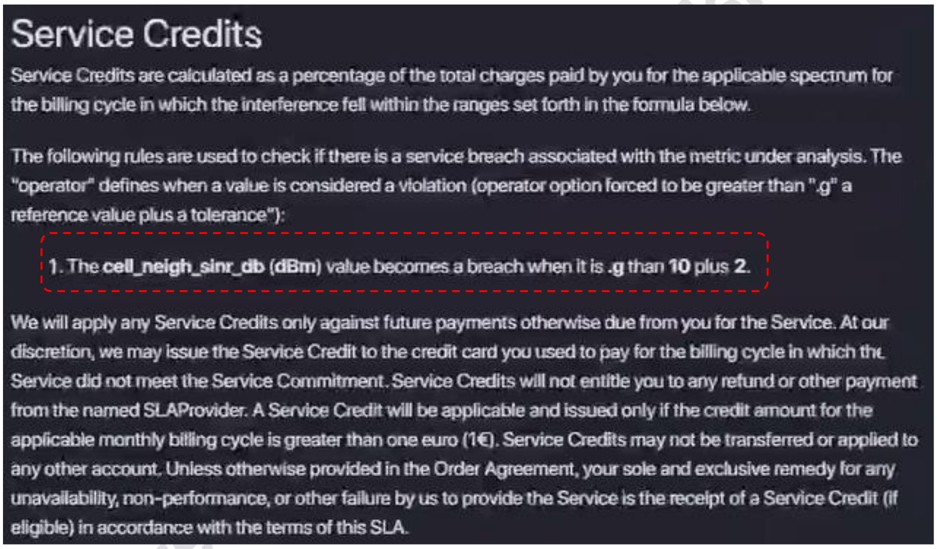


Figure 49: SLA associated to the spectrum/slice offer

The SLA template used in this scenario defined two different types of breaches. The first one, shown in Figure 5050 and evaluated in the test case UC2.9f, considers a compensation based on Service Credits to the Consumer in case of suffering interference from other networks.



Service Credits

Service Credits are calculated as a percentage of the total charges paid by you for the applicable spectrum for the billing cycle in which the interference fell within the ranges set forth in the formula below.

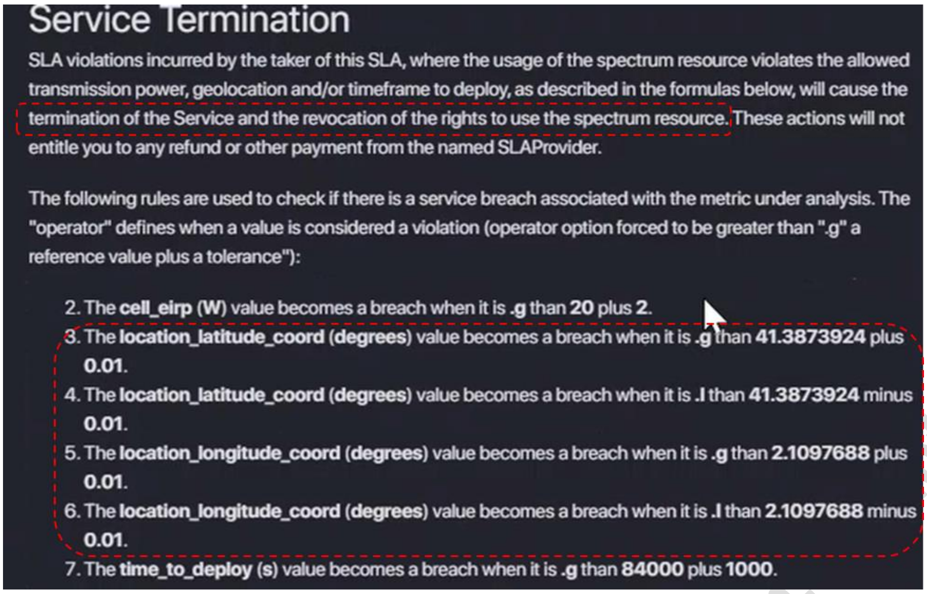
The following rules are used to check if there is a service breach associated with the metric under analysis. The "operator" defines when a value is considered a violation (operator option forced to be greater than ".g" a reference value plus a tolerance"):

1. The **cell_neigh_sinr_db (dBm)** value becomes a breach when it is **.g** than **10** plus **2**.

We will apply any Service Credits only against future payments otherwise due from you for the Service. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the Service did not meet the Service Commitment. Service Credits will not entitle you to any refund or other payment from the named SLAProvider. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one euro (1€). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the Order Agreement, your sole and exclusive remedy for any unavailability, non-performance, or other failure by us to provide the Service is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

Figure 50: UC2.9f: SLA considered in the interference-based breach

The second one, shown in Figure 51 and evaluated in UC2.9g, considers SLA breaches caused by the Consumer and whose severity will lead to service termination and derivative spectoken redeeming. The SLA template contemplates different metrics, like the maximum EIRP or the maximum time to deploy, but in this deliverable, we have focused on the metrics related to the geofencing breach (i.e., cell location).



Service Termination

SLA violations incurred by the taker of this SLA, where the usage of the spectrum resource violates the allowed transmission power, geolocation and/or timeframe to deploy, as described in the formulas below, will cause the termination of the Service and the revocation of the rights to use the spectrum resource. These actions will not entitle you to any refund or other payment from the named SLAProvider.

The following rules are used to check if there is a service breach associated with the metric under analysis. The "operator" defines when a value is considered a violation (operator option forced to be greater than ".g" a reference value plus a tolerance"):

2. The **cell_eirp (W)** value becomes a breach when it is **.g** than **20** plus **2**.
3. The **location_latitude_coord (degrees)** value becomes a breach when it is **.g** than **41.3873924** plus **0.01**.
4. The **location_latitude_coord (degrees)** value becomes a breach when it is **.l** than **41.3873924** minus **0.01**.
5. The **location_longitude_coord (degrees)** value becomes a breach when it is **.g** than **2.1097688** plus **0.01**.
6. The **location_longitude_coord (degrees)** value becomes a breach when it is **.l** than **2.1097688** minus **0.01**.
7. The **time_to_deploy (s)** value becomes a breach when it is **.g** than **84000** plus **1000**.

Figure 51: UC2.9g: SLA considered in the geofencing-based breach

In addition, in both cases, SLA breaches lead to a modification of the trust value computed by the 5G-TRMF. Therefore, in the case of the interference-related breach we evaluated this automated correction/mitigation done by 5G-TRMF, while in the geofencing-related breach we focused on demonstrating the corrections related to service termination and derivative spectoken redeeming.

Once a violation occurs and is captured by the RAN metrics, the SLA monitoring detects it and creates an SLA violation event, which is sent to the datalake. Figure 522 shows an example of SLA violation based on the suffered interference, which is captured by the portal of the Consumer as depicted in Figure 533.


```
{
  "id": "6fdb6f2f-43a6-49bd-8e5b-ac8868b41283",
  "productDID": "P44RJzPQ9NWPE7QTDX4ZhA",
  "transactionID": "46da2e15efc340cd9ae9d6363a0e8d1d",
  "sla": {
    "id": "3GsEZiQpr8PxCDYe1Sx2vX",
    "href": "http://172.28.3.178:31081/smart-contract-lifecycle-manager/api/v1/service-level-agreement/3GsEZiQpr8PxCDYe1Sx2vX"
  },
  "rule": {
    "id": "158040ec-c407-4045-a160-57c9d261355b",
    "metric": "cell_neigh_sinr_db",
    "unit": "dBm",
    "referenceValue": "10",
    "operator": ".g",
    "tolerance": "2",
    "consequence": null
  },
  "violation": {
    "actualValue": "14"
  }
}
```


Figure 52: UC2.9f: SLA violation related to interference (SLA monitor event)

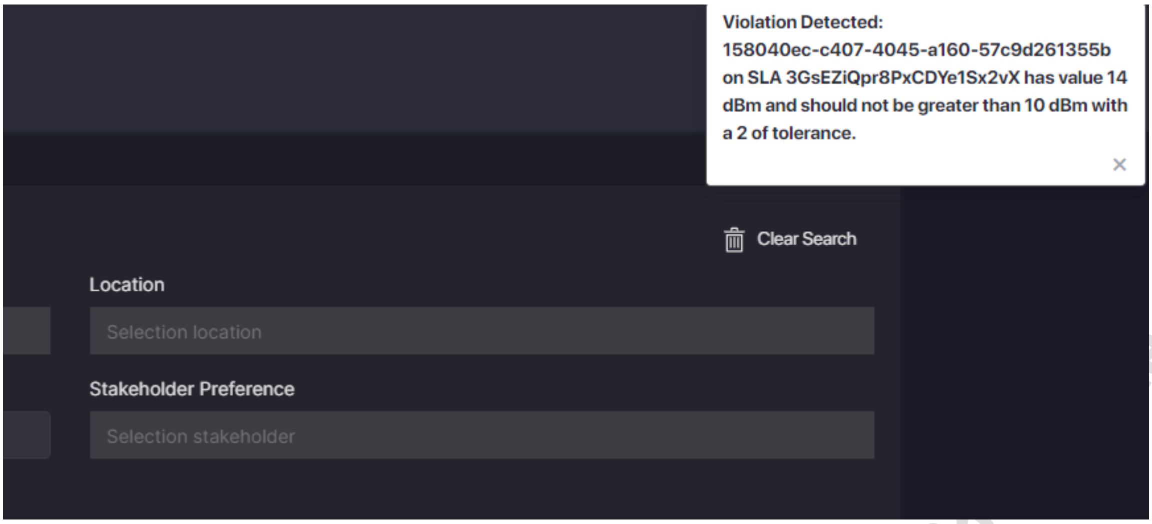


Figure 53: UC2.9f: SLA violation related to interference (Portal warning)

As aforementioned, the SLA violation is captured by the 5G-TRMF and leads to an update of the trust-score value between the consumer and the provider. Figure 54 shows an example of the 5G-TRMF logs generated after an SLA violation.

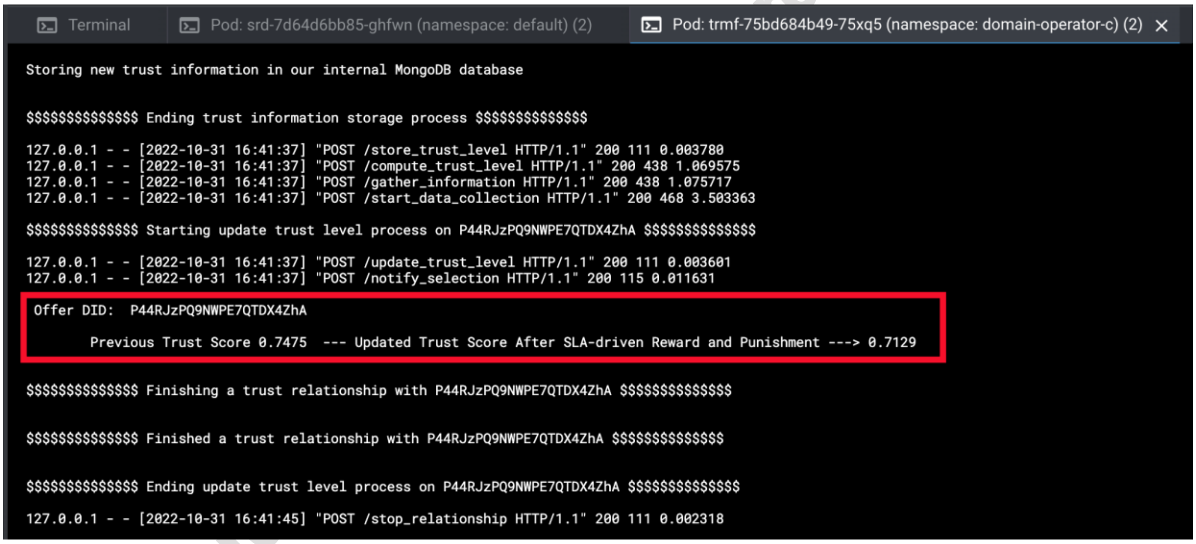


Figure 54: UC2.9f: SLA violation related to interference (5G-TRMF correction)

The following table summarizes the findings for this test.

Table 25: SLA breach detection and correction on interference levels

UC2.9f	SLA breach detection and correction on interference levels
Testbed	5GBarcelona
Description	The resource consumer deploys a slice over a given geographical area by selecting a set of the radio and spectrum resources that the resource consumer acquired beforehand from the 5GZORRO Marketplace. A rogue gNB operating in the same frequency range appears and generates high interferences to the UE. The interference is superior to the acceptable level agreed in the SLA of the smart contract. Demonstrated mitigation action is to update the trust score between consumer and producer.
Use-case functionalities	Slice is deployed and active

	Spectrum telemetry is available in the Datalake SLA breach is detected and notified Portal shows a notification 5G-TRMF captures the breach and updates trust score	
Key Use-case requirements and KPIs	**[KPI1.1]** Support actual distributed multi-party service and business configurations. **[KPI5.5]** Ability to enforce the settled spectrum rights and obligations, which will build on lightweight Trusted Execution Environments (TEE) embedded in the radio access points to ensure that the reported spectrum measurements are faithful, and the spectrum allocations settled in the market are enforced. **[KPI7.1**] Lab validation environments for the three use cases	
Components	Portal Radio Resource Controller (rRM) Monitoring data aggregator (MDA) Datalake SLA Monitoring 5G Trust and Reputation Management Framework (5G-TRMF)	
Test Procedure	Pre-conditions	Resource consumer has deployed a slice through the ISSM SLA was associated to this slice gNB is reporting metrics
	Test Case steps	gNB exposes RAN metrics through Prometheus exporter RAN Prometheus Server gathers metrics MDA gets RAN metrics from the Prometheus Server and exposes them to the datalake SLA monitoring gets metrics from datalake and analyses SLA breaches SLA monitoring detects an SLA breach based on metric values and SLA definitions SLA sends an SLA violation event to the datalake 5G-TRMF captures the violation and updates trust score Portal captures the violation and shows a warning
Measurements	Methodology	Video and screenshots
	Complementary measurements	none
	Calculation process	Observation from the Portal, TRMF logs and datalake.
Result	SLA violations are detected and corrected/mitigated **[KPI1.1]** The KPI target was set to more than 3 providers/operators. In this test, Operator C operated the slice offered by Operator A. SLA breaches caused an update of the trust-score among both operators. **[KPI5.5]** The KPI target was to be able to detect spoofing attacks where a base station uses an allocation not authorized by the market. This test shows the capability of prototype to detect and correct SLA breaches. **[KPI7.1]** KPI target was 3 lab testing environments**.** Tests were performed in the testing environment for UC3 in 5GBarcelona.	

In the case of the geofencing-related breach, the SLA monitoring component monitors exposed latitude and longitude values and compare them with the thresholds defined in the SLA. Figure 55:5 shows an example of an SLA violation caused by a gNB reporting a location out of the allowed area (based on the longitude metric). Figure 566 depicts how this violation is captured by the portal (in this case based on the latitude metric).

```
{
  "id": "d707a940-0283-4e89-bf63-550f9aeaf8d6",
  "productDID": "P44RJzPQ9NWPE7QTDX4ZhA",
  "transactionID": "46da2e15efc340cd9ae9d6363a0e8d1d",
  "sla": {
    "id": "3GsEZiQpr8PxCDYe1Sx2vX",
    "href": "http://172.28.3.178:31081/smart-contract-lifecycle-manager/api/v1/service-level-agreement/3GsEZiQpr8PxCDYe1Sx2vX"
  },
  "rule": {
    "id": "f64f6987-3af5-4451-9b77-a24d75c13328",
    "metric": "location_longitude_coord",
    "unit": "degrees",
    "referenceValue": "2.1097688",
    "operator": ".g",
    "tolerance": "0.01",
    "consequence": null
  },
  "violation": {
    "actualValue": "2.126622"
  }
}
```


Figure 55: UC2.9g: SLA violation related to geofencing (SLA monitor event)

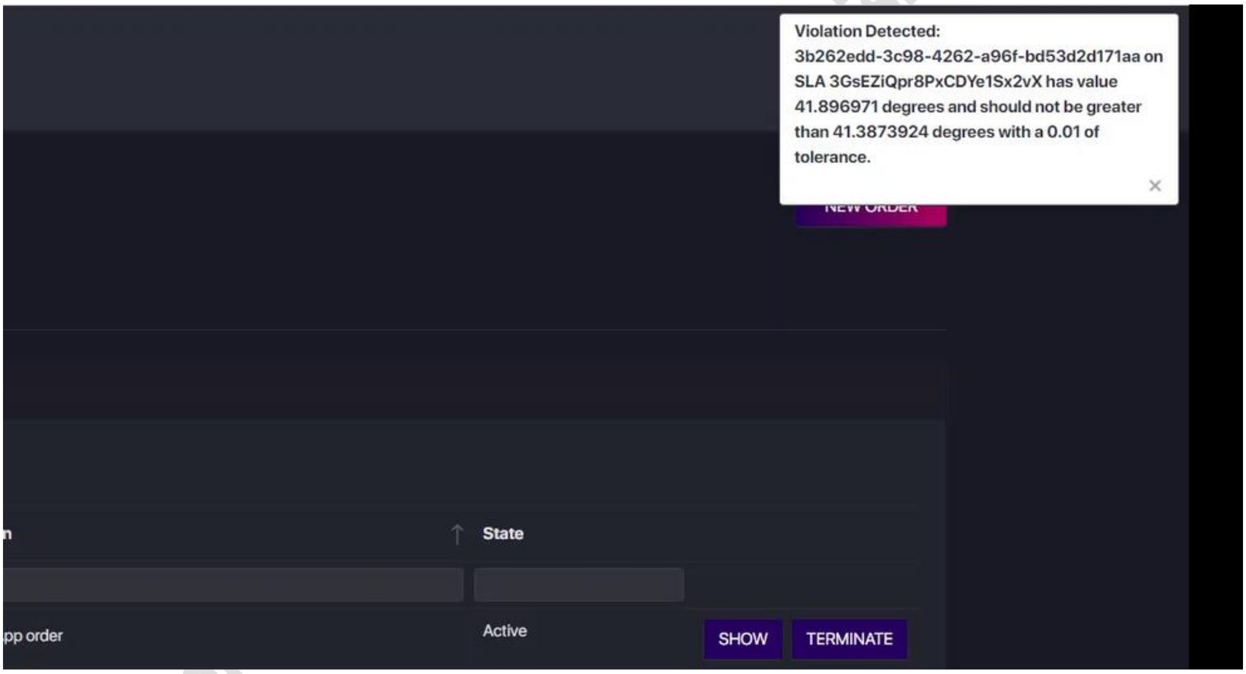


Figure 56: UC2.9g: SLA violation related to geofencing (Portal warning)

This warning is shown in the Portal of the providers related to the order; in this case, the spectrum provider and the slice provider. In its actual implementation, the platform requires the providers to manually finalize the slice and spectrum orders through the portal; nevertheless, future versions of the platform could automatize this procedure according to the definition of rules and consequences in the SLAs. Figure 577 and Figure 588 show the finalization the slice order through Operator A (Slice provider) portal, which also leads to the finalization of the slice instance linked to this order.

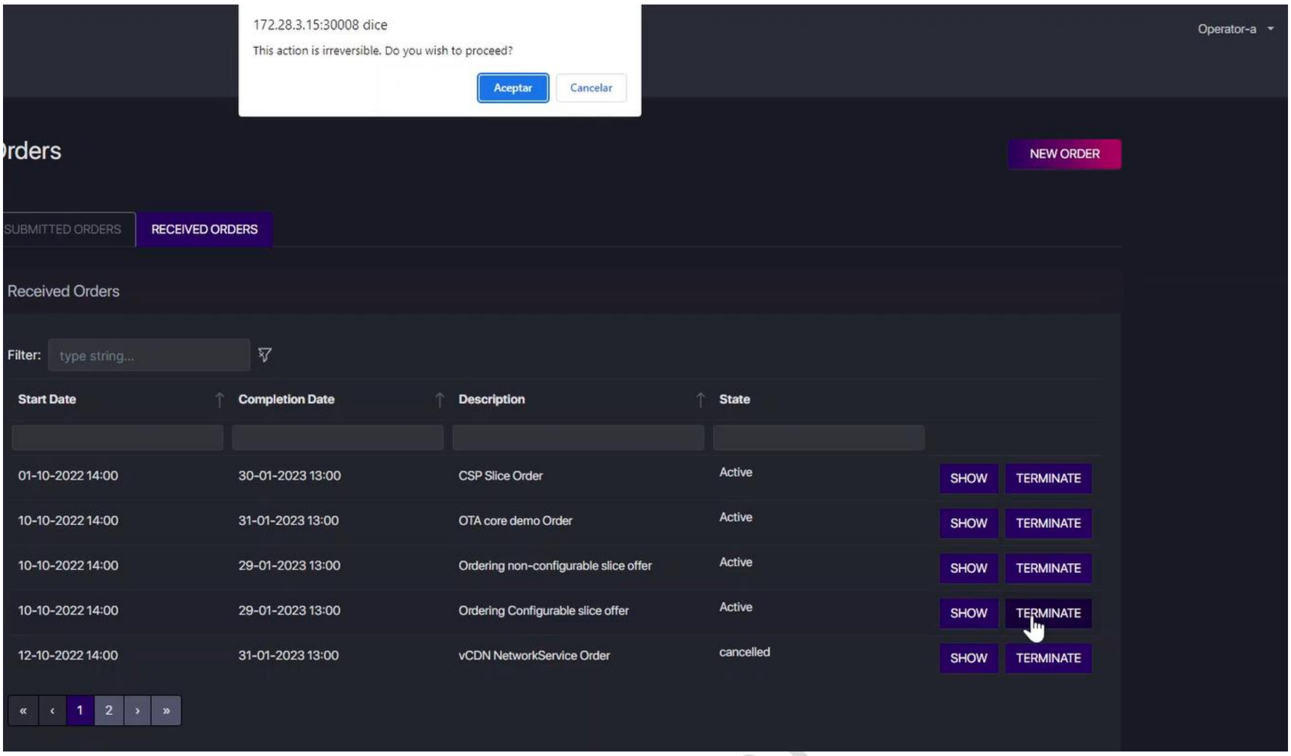


Figure 57: UC2.9g: Slice order termination by Operator A due to SLA breach

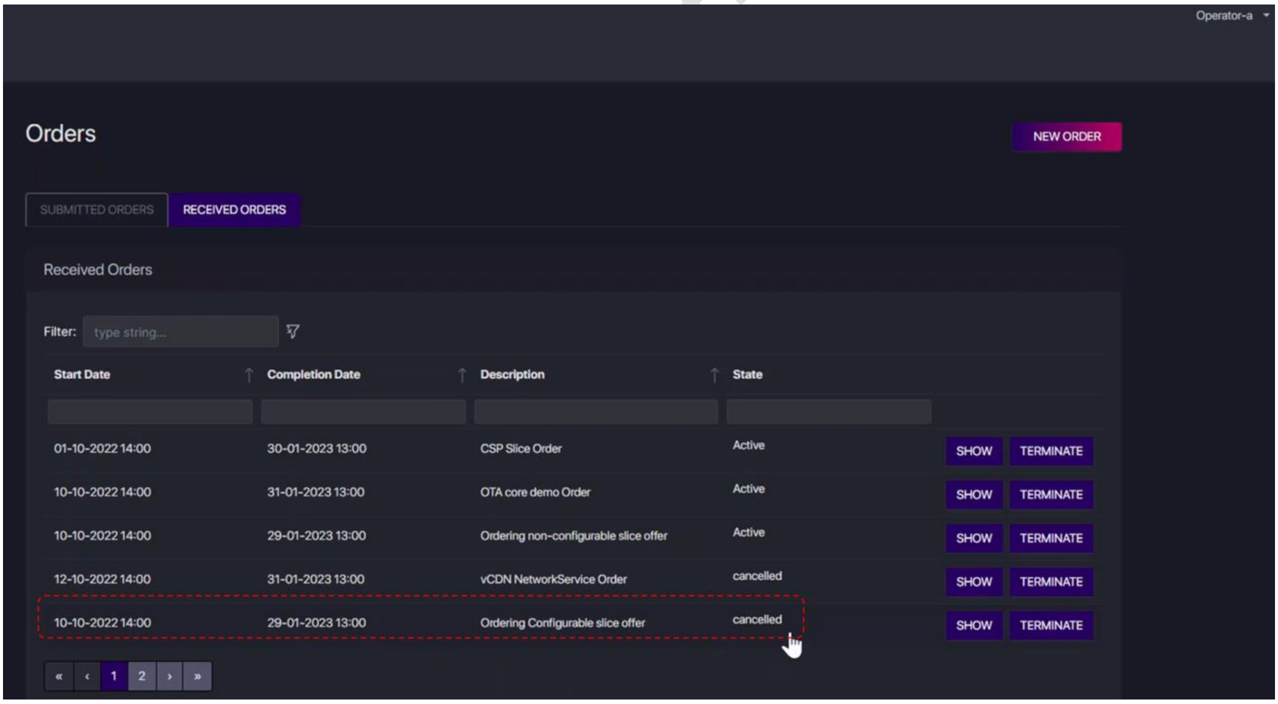


Figure 58: UC2.9g: Slice order becomes cancelled in the Marketplace

¡Error! No se encuentra el origen de la referencia.9 and Figure 60 show the finalization the spectrum order through Operator B (Spectrum provider) portal. This also leads to the redeem of the spectoken of

Operator C; i.e., the revocation of its rights to use the spectrum resource. Figure 61 shows that Operator C has no longer the NFT related to the redeemed spectrum resource.

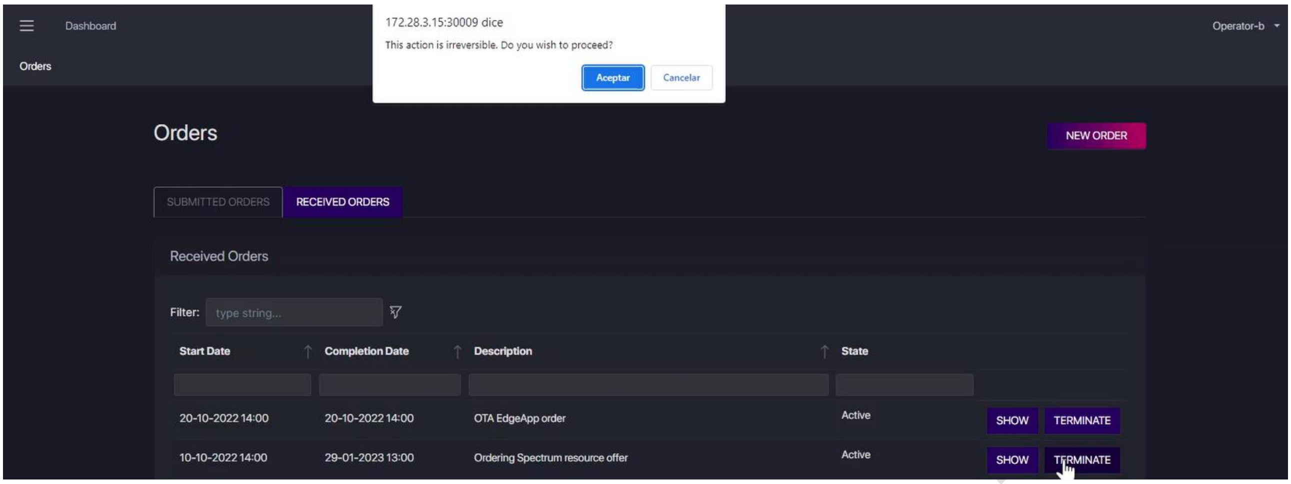


Figure 59: UC2.9g: Spectrum order termination by Operator B due to SLA breach

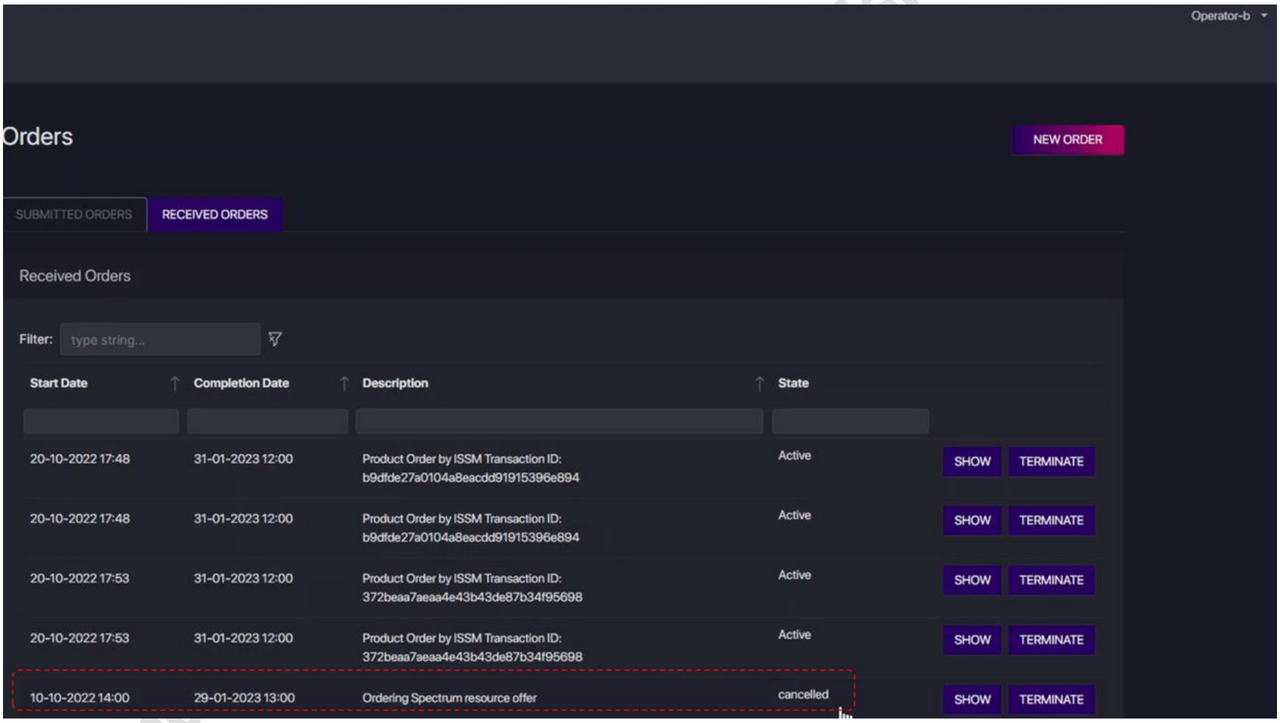


Figure 60: UC2.9g: Spectrum order becomes cancelled in the Marketplace

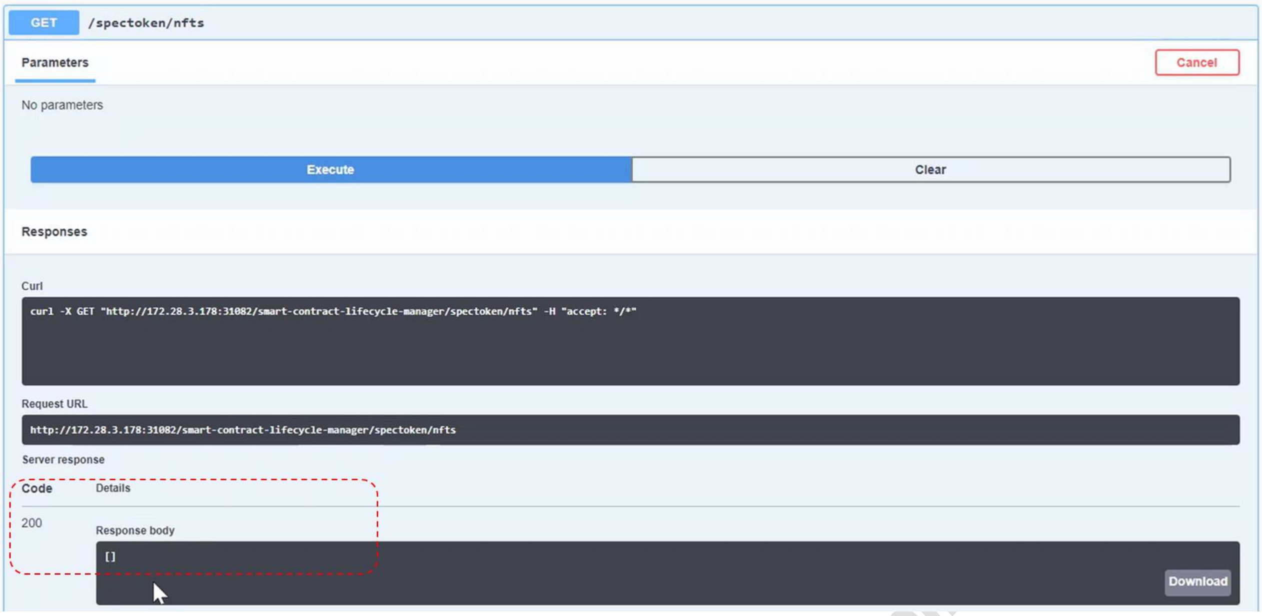


Figure 61: UC2.9g: Derivative spectoken redeeming due to SLA breach (Operators C CORDA's Vault content via SCLCM)

Finally, the following table summarizes the findings for test UC2.9g.

Table 26: SLA breach detection and correction on geofencing spectrum

UC2.9g	**SLA breach detection and correction on geofencing spectrum**
Testbed	5GBarcelona
Description	The resource consumer deploys a slice over a given geographical area by selecting a set of the radio and spectrum resources that the resource consumer acquired beforehand from the 5GZORRO Marketplace. The base station has mobility and goes beyond the limits of the spectoken. The SLA breach is detected and, as a consequence, the 5GZORRO platform performs the correction action and disables the radio transmissions and redeems the derivative spectoken.
Use-case functionalities	Slice is deployed and active Spectrum telemetry is available in the Datalake SLA breach is detected and notified Portal shows a notification Slice provider terminates slice order and instance Spectrum provider terminates spectrum order and redeems the associated derivative spectoken
Key Use-case requirements and KPIs	**[KPI1.1]** Support actual distributed multi-party service and business configurations. **[KPI5.5]** Ability to enforce the settled spectrum rights and obligations, which will build on lightweight Trusted Execution Environments (TEE) embedded in the radio access points to ensure that the reported spectrum measurements are faithful, and the spectrum allocations settled in the market are enforced. **[KPI7.1**] Lab validation environments for the three use cases
Components	Portal Monitoring Data Aggregator (MDA) Datalake SLA Monitoring Intelligent Slice and Service Manager (ISSM) Smart Contract Life-Cycle Manager (SCLCM) Radio Resource Manager (rRM)

	Network Slice and Service Orchestrator (NSSO)	
Test Procedure	Pre-conditions	Resource consumer has deployed a slice through the ISSM SLA was associated to this slice gNB is reporting metrics
	Test Case steps	gNB exposes RAN metrics through Prometheus exporter RAN Prometheus Server gathers metrics MDA gets RAN metrics from the Prometheus Server and exposes them to the datalake SLA monitoring gets metrics from datalake and analyses SLA breaches SLA monitoring detects an SLA breach based on metric values and SLA definitions SLA sends an SLA violation event to the datalake Portal captures the violation and shows a warning Slice Provider cancels the slice order, leading to the termination of the slice instance Spectrum Provider terminates the spectrum order, leading to the redeeming of the derivative spectoken
Measurements	Methodology	• Video and screenshots
	Complementary measurements	none
	Calculation process	Observation from the Portal (warnings, order status, slice instance status). CORDA’s vault status (Consumer). RAN status (gNB, Core and UE).
Result	SLA violations are detected and corrected/mitigated **[KPI1.1]** The KPI target was set to more than 3 providers/operators. In this test, Operator C operated the slice offered by Operator A and the spectrum offered by Operator B. SLA breach involves correction actions from Operator A and B. **[KPI5.5]** The KPI target was to be able to detect spoofing attacks where a base station uses an allocation not authorized by the market. This test shows the capability of prototype to detect and correct SLA breaches. **[KPI7.1]** KPI target was 3 lab testing environments**.** Tests were performed in the testing environment for UC3 in 5GBarcelona	

2.4. **UC3: Pervasive vCDN Services**

2.4.1. **Description**

As mentioned in D5.2 [3] and other deliverables,UC3 is based on ICOM's commercial offering for a CDN solution, i.e. fs|cdn™ Anywhere [54], which is modified to suit the project requirements. fs|cdn™ Anywhere is an end-to-end CDN solution, which, for the case of mobile clients, adopts the HTTP Live Streaming (HLS) and Dynamic Adaptive Streaming over HTTP (MPEG-DASH) protocols and creates a hierarchical topology of HTTP servers (e.g., content caches) to simulate a multicast delivery tree. These servers are placed at key locations on the Communication Service Provider’s (CSP's) network and allow access to all CDN subscribers. For the purposes of 5GZORRO, CDN edge network components are virtualized and offered as Virtual Network Functions (VNFs), thus leading to a virtual CDN (vCDN) solution. Additionally, there is a licensing system that accompanies the CDN solution, which commits a specific CDN deployment to a maximum number of end users.

Generally, the purpose of this use case is to allow cache servers to scale over 3rd party resources. In our scenarios, a CDN service provider leases a network slice instance from a CSP, including performance guarantees. In cases where the CSP's edge infrastructure cannot meet the demand, for example in high workload situations, an advanced agreement and service manager services (specifically, Intelligent SLA Breach Prediction (ISBP) and Intelligent Slice and Service Manager (ISSM)) trigger the resource discovery process in order to identify potentially usable 3rd party edge resources. The discovery process identifies candidate product offers and rates them based on how well they satisfy the request as well as on other profile information data related to the resource, such as trust attributes and pricing. After selecting the highest rated offer, the CSP's service manager orders it from the Marketplace. In the final stage, the network slice is extended to the 3rd party infrastructure, instantiating the service components on the new resources.

2.4.2. Use Case 3 Scenarios

Part of the scenarios and tests that were planned for UC3 have already been analysed in deliverables D5.1 [2] and D5.2 [3]. Particularly, in D5.1 an analysis and an initial plan of the use case were presented, while in D5.2 the UC3 description was extended with the results for the test cases related to Scenario 1 deployment in 5GBarcelona testbed. However, the scenarios analysed in the previous documents have been modified in the present deliverable, in order to showcase aspects of the 5GZORRO platform and technologies that are not covered in the tests reported in D5.2. Additionally, a new cross-testbed scenario (Scenario 4) is introduced for the first time in the current document.

In Table Table 27 we note the tests that were executed at 5GBarcelona testbed. These are the same as the ones mentioned in previous deliverables, with the addition of a new test case, namely Test UC3.3c, focused on the eLicense expiration. In the left column we list the tests whose results have been provided in D5.2, while in the right column those whose results are reported in the present document.

Table 27: UC3 tests in 5G Barcelona testbed (Scenario 2 and Scenario 3)

Tests presented in D5.2	Tests presented in D5.3
Test UC3.1a: CDN application deployment	Test UC3.2a: Predict RAN resource saturation
Test UC3.1b: SLA breach prediction validation	Test UC3.2b: Discovery and acquisition of RAN resource
Test UC3.1c: Discovery and acquisition of compute resources	Test UC3.2c: Slice extension to 3rd party radio and edge compute infrastructure
Test UC3.1d: Slice extension to 3rd party edge server	Test UC3.3c: eLicense expiration
Test UC3.1e: Traffic distribution to all CDN edge servers	
Test UC3.3a: Licensing validation with a single monitoring metric	
Test UC3.3b: Licensing validation with multiple monitoring metrics	

In the past we had mentioned that the Scenarios shown in Table 27 would be repeated on 5Tonic testbed. However, it was decided that there would not be too much value added in repeating the same scenarios in just a different testbed. So, it was preferred to replace those scenarios with a new one, namely Scenario 4, which expands onto both testbeds. This scenario is analysed in Section 2.4.2.3.

Table Table 28 summarizes the tests related to Scenario 4.

Table 28: UC3 tests for the cross-testbed scenario (Scenario 4)

Tests presented in D5.3
Test UC3.4a: CDN application deployment on 5G Barcelona
Test UC3.4b: CDN application deployment on 5Tonic
Test UC3.4c: Validate 5GZORRO services over TEEs

As shown in the above tables, we are considering 4 basic scenarios, for which the test cases are represented by UC3.1x, UC3.2x, UC3.3x and UC3.4x for Scenarios 1, 2, 3 and 4, respectively. As a quick reminder, the first scenario studies the need for a slice extension due to an impending overload of the CDN edge server located on the CSP site. Therefore, in this case we are looking for edge compute resources. On the other hand, the second scenario refers to the case where the CSP requests for both compute and RAN resources, as in this case the CSP Base Station is overloaded. In the third scenario, we include some licensing validation features, which are responsible for considering the licensing costs when implementing automated Network Slice adaptation and service instantiation. For more details about these scenarios, please refer to deliverables D5.1 [2] and D5.2 [3]. Finally, in the fourth scenario, we are showcasing the deployment of one service (i.e. CDN) over two testbeds, where each one supports different technologies.

The tests for the first three scenarios, i.e. tests UC3.1a – UC3.1e, UC3.2a – UC3.2c and UC3.3a – UC3.3c, are demonstrated only in 5GBarcelona testbed, where real RAN infrastructure is available for the project. On the other hand, Scenario 4 tests are implemented in both testbeds. Particularly, UC3.4a is executed at 5GBarcelona, while UC3.4b and UC3.4c at 5Tonic. Since in D5.2 [3][24] we presented the results of the 1st and 3rd scenarios, in the current document we analyse the execution of scenarios 2 and 4, as well as one new test that was added to Scenario 3. These tests are presented in the following sections.

2.4.2.1.Scenario 3.2: Slice extension to increase vCDN wireless coverage

Scenario 2, which is already described in D5.1 [2], is a core scenario presented in the current deliverable. As you may recall from that document, this scenario refers to the case where the CSP requests for both compute and RAN resources. An updated diagram is presented in Figure 62.

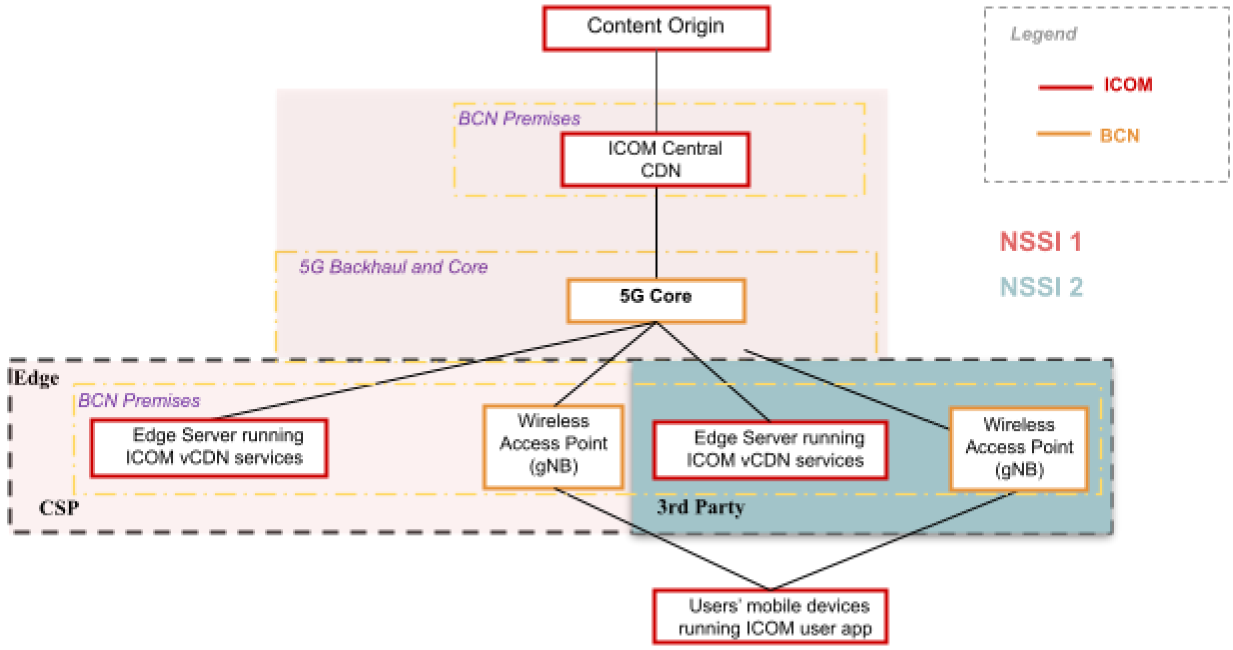


Figure 62: Deployment architecture for the 2nd scenario of UC3 (leasing compute and network resources)

2.4.2.1.1.TestUC3.2a: Predict RAN resource saturation

This Test Case refers to the prediction of the upcoming saturation at the RAN part and is already analysed in D5.2 [3]. It should be noted that for Scenario 2, we are not reporting the steps of slice ordering and instantiation, as this is the same as the Test UC3.1a, analysed in D5.2. In Table 29 we elaborate more on this Test Case. This is basically an extension of Table 5-7 of D5.2.

Table 29: Test UC3.2a - Predict RAN resource saturation

<table>
<tr><th>UC3.2a</th><th colspan="2">Predict RAN resource saturation</th></tr>
<tr><td>Description</td><td colspan="2">This is similar to UC3.1b that was tested in D5.2, except that in this case the RAN resources of the CSP are the ones to be extended. As we did in D5.2, a user emulator is used for generating requests to the edge cache, forcing it to reply to those requests. The goal is to create the conditions under which the radio part of CSP is considered as saturated. Due to unavailability of a dataset with an adequate number of RAN metrics that could be used to generate the Machine Learning (ML) models of ISBP, it was decided to use again an existing CDN dataset, as we did in previous deliverables. This dataset is basically a collection of various application metrics, gathered from a commercial CDN deployment. The metric that is more relevant to the specific scenario is the bandwidth generated by the edge cache, as we can assume that it also impacts the bandwidth that is in use in the radio (for the downlink). In other words, an increase in the application bandwidth, invokes an increase in the network bandwidth as well.</td></tr>
<tr><td>Key Use-case requirements and KPIs</td><td colspan="2">• [KPI4.2] Implement/correlate technical service configurations and SLA monitoring interactions between multiple parties
    ○ [KPI4.2.1] Services can be composed of one or more resources and from one or more providers.
• [KPI-UC3.8]. Prediction of SLA breach > 5 mins before the breach occurrence</td></tr>
<tr><td>Components and Configuration</td><td>Components</td><td>• Any Resource Manager (xRM)
• Monitoring Data Aggregator (MDA)
• Datalake</td></tr>
</table>

		• Intelligent SLA Breach Prediction (ISBP) • ISSM
	Configuration	• The Central CDN server includes the following software modules (deployed as VNFs): Packaging, Subscriber & Content Management, Streaming Server, Transcoding, Encryption, and Main Cache. • One of ICOM's CDN software modules named Edge Cache is deployed on the Edge server as VNF. • The 5GZORRO components, which are required for SLA monitoring and breach prediction, are integrated. • The data used for the test is the bandwidth generated by the edge cache. This is collected and passed to MDA.
Test Procedure	Pre-conditions	• CDN software components are up and running • Relevant 5GZORRO components are up and running • User connectivity is verified • The prediction model is already trained with an existing dataset • The original slice at the CSP side (Operator A) has already been purchased and instantiated
	Test Case steps	1. An emulator is sending requests to the CDN application, particularly to the edge cache that is instantiated in CSP side (Operator A). The number of requests per minute sent by the emulator follow the pattern of a true traffic, as it was extracted from a real commercial deployment. However, the number of requests has been downscaled, for practical reasons. 2. The emulator generates traffic to CSP's edge part, as the edge cache replies to each single request. 3. The SLA Breach Predictor receives application monitoring data, particularly the bandwidth generated by the edge cache, makes the predictions and, in case of a possible SLA violation, it notifies the ISSM (see Figure 633).
Measurements	Methodology	• Keep track of notification events coming from the ISBP
	Complementary measurements	Bandwidth
	Calculation process	• Bandwidth is the metric that is passed and used by ISBP, as indicated by the SLA. xRM retrieves this from application's statistics. Then MDA gets this metric and passes it to the Data Lake, where ISBP can find it. This whole process is done automatically • The KPIs mentioned are validation KPIs. Thus, no measurements are done for this test.
Result	When executing the test, it was not possible to generate an excessive traffic and actually stress the edge server. Thus, for the sake of testing, the threshold of the Service Level Objective (SLO), i.e. bandwidth, was set to lower levels. • **[KPI4.2]** The KPI target was set as SLA measurements and validation from at least 3 operators involved in a multi-party service chain, however this test only involves SLA agreements between 2 partners, i.e. CDN operator (Operator C) and CSP (Operator A). . More specifically, Operator C creates a CDN slice comprised of a slice offer and a CDN Network Service (NS) offer (see Figures Figure 644 and Figure 655). In this test, for practical reasons, both offers belonged to the same provider (Operator A), but they could also belong to different providers. In that case, the KPI could be considered as achieved. **[** • **KPI-UC3.8]** Achieved, given that the measurements are taken every 5 minutes and the prediction refers to the value that the metric will have in the next 5 minutes. Moreover, ISBP predicts that in the next 5 minutes a threshold will be crossed, as defined in the SLA objectives. As we will show in later tests, this gives just enough time to the orchestration platform to take action and prevent the threshold crossing.	

	The accuracy of the prediction model used was calculated to 96% for the training dataset and 85% for the actual data generated during the test.

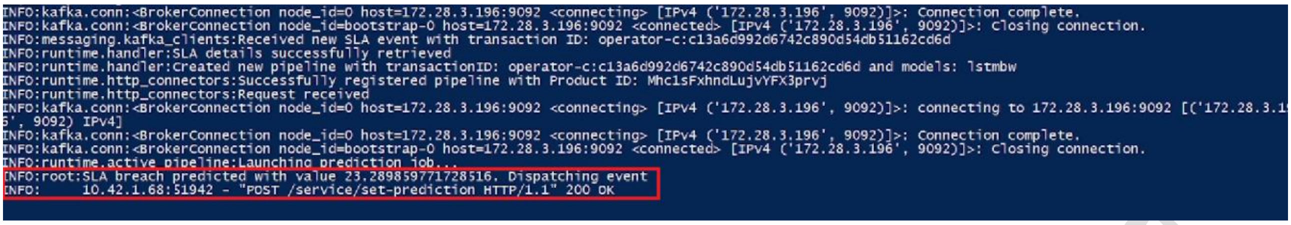


Figure 63: Test UC3.2a – An SLA breach is predicted (ISBP view)

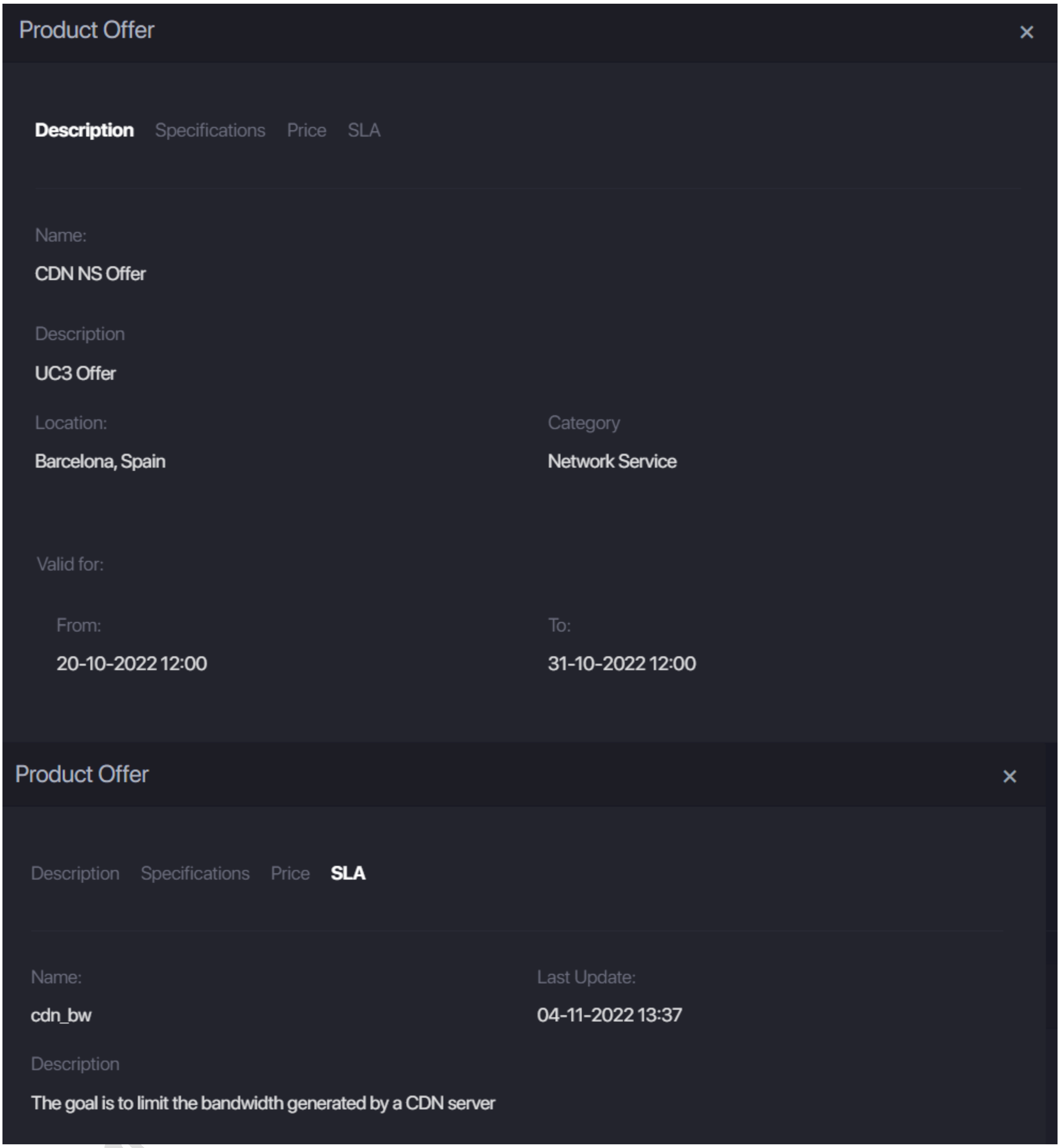


Figure 64: Test UC3.2a – CDN NS offer with SLA (Operator A's portal view)

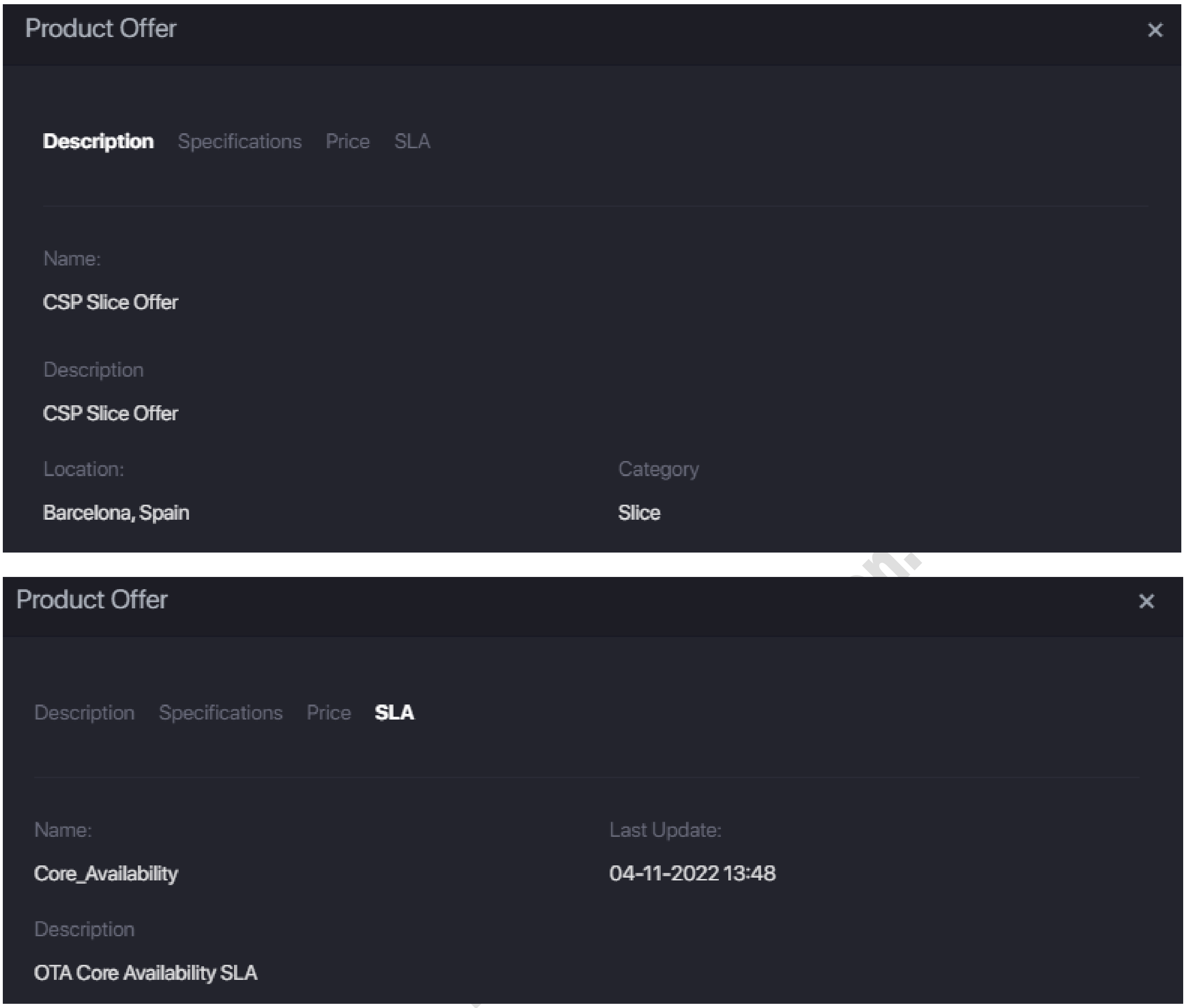


Figure 65: Test UC3.2a – Slice offer with SLA (Operator A's portal view)

2.4.2.1.2.TestUC3.2b: Discovery and acquisition of RAN resource

This test case addresses the evaluation of the resource discovery process to find both RAN and compute resources, as described in Table 30, which is an extension of Table 5-8 of D5.2 [3].

Table 30: Discovery and acquisition of RAN resource

UC3.2b	**Discovery and acquisition of RAN resource**	
Description	This is similar to UC3.1c that was tested in D5.2, with the added requirement of finding available RAN resources, additional to the compute ones.	
Key Use-case requirements and KPIs	• [KPI4.1] Automatically discover and "inventorize" various types of resources (i.e., compute, storage, network at core, edge, far-edge), spectrum and services capabilities from different domains and service providers. • [KPI4.2] Implement/correlate technical service configurations and SLA monitoring interactions between multiple parties ○ [KPI4.2.1] Services can be composed of one or more resources and from one or more providers.	
	Components	• ISSM

Components and Configuration		• SRSD • Marketplace • 5G Trust & Reputation Management Framework (5G-TRMF) • Any Resource Manager (xRM) • Catalogue • Smart Contract Lifecycle Manager (SCLCM)
	Configuration	Communication between 5GZORRO components has been established
Test Procedure	Pre-conditions	• SLA between CDN (Operator C) and CSP (Operator A) (Figures Figure 644 and Figure 655) • DLT network is configured • There are product offers in the catalogue (Figure 66) • 5GZORRO modules in all of the participating stakeholders are up and running
	Test Case steps	1. Repeat the steps in Table 29. 2. ISBP notifies the ISSM about the upcoming resource saturation (Figure 677). 3. ISSM triggers two times the SRSD, in order to search for RAN and compute resources in the Marketplace (Figure 688). 4. For each ISSM request, SRSD returns a list of offers, after consulting 5G-TRMF. 5. ISSM-O selects the final offers (Figure 699). 6. ISSM places an order for the selected resource offers, on behalf of Service Provider (Operator C). In this scenario, both offers belong to the same provider (Operator B). 7. The 3rd party resource provider (Operator B) accepts the orders (Figure 7070) and a new agreement is established.
Measurements	Methodology	• Monitor the involved 5GZORRO software modules
	Complementary measurements	None
	Calculation process	This is a validation test, so, no measurements are performed.
Result	• **[KPI4.1]** The KPI target was set to discover resources in the catalogue by all registered consumers within 5 minutes of being registered and verified. For this test, RAN and edge compute resources were considered. The time from a resource publication until the resource is visible to consumers was not calculated. But it was verified that these types of resources can be discovered when requested. • **[KPI4.2]** The KPI target was set as implementing technical service configurations and SLA monitoring interactions between multiple parties. For this test, this KPI can be considered as achieved. In addition to the SLAs mentioned in TestUC3.2a, a new SLA is created between Service provider (Operator C) and the selected 3rd party (Operator B). This SLA refers to the RAN resource offer that was ordered from Operator C (Figure 71).	

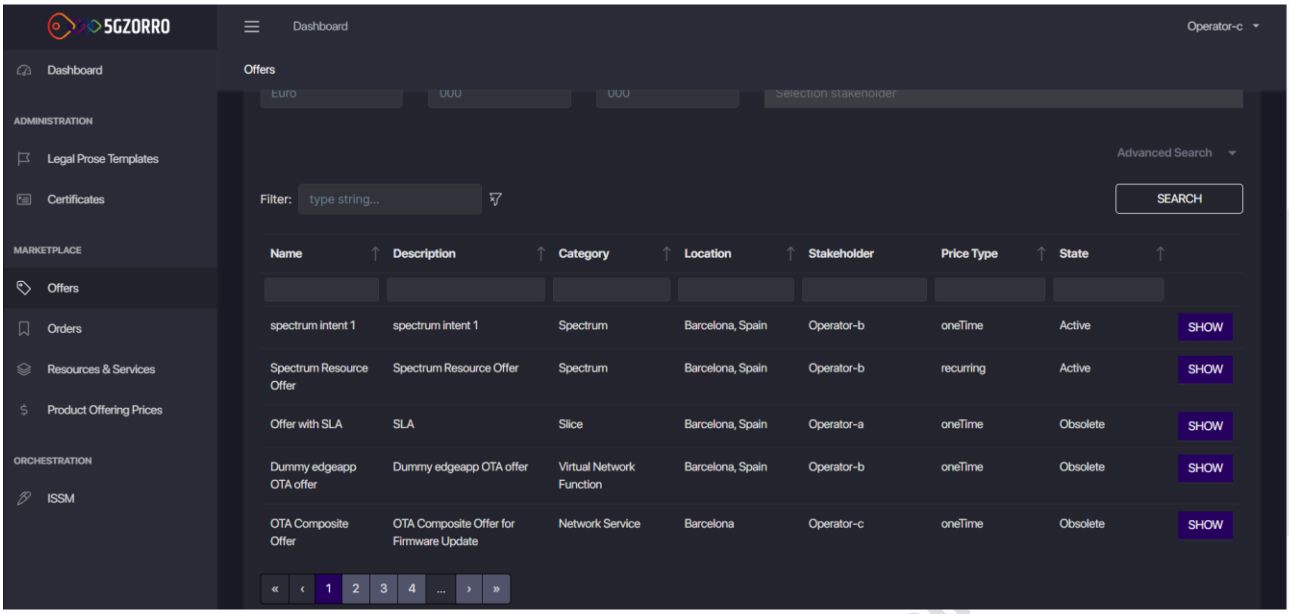


Figure 66: TestUC3.2b – List of available product offers (Operator C's Portal view)

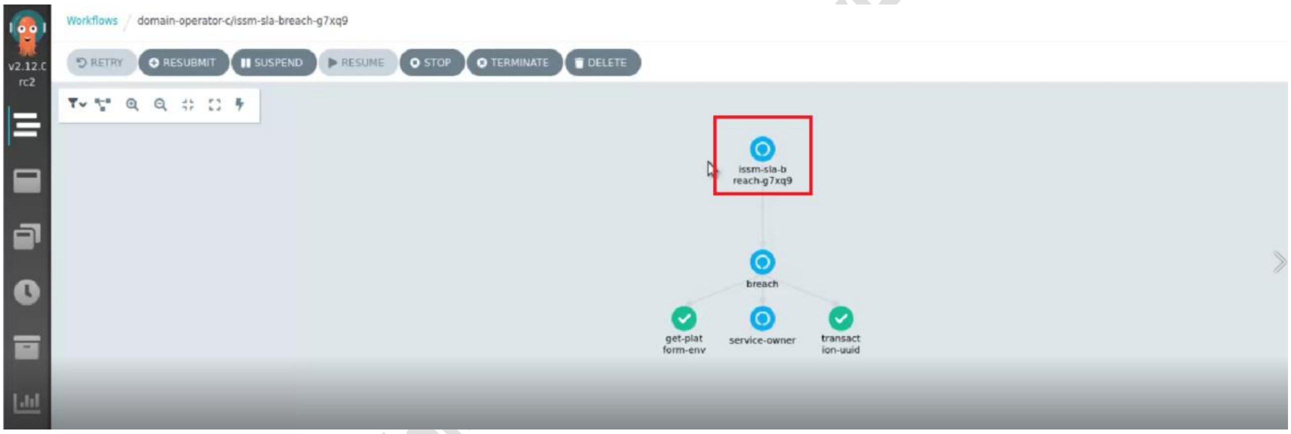


Figure 67: TestUC3.2b – ISSM receives an SLA breach prediction event (Operator C's ISSM view)

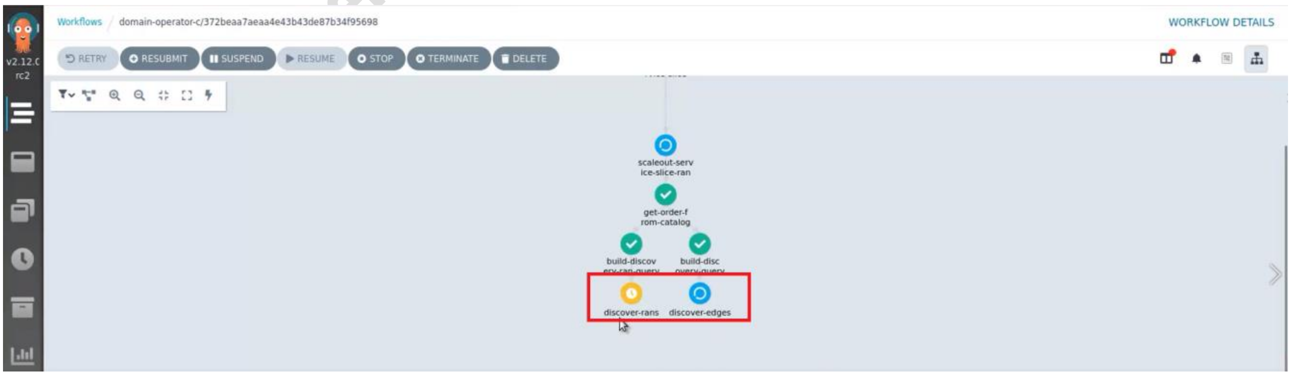


Figure 68: TestUC3.2b – ISSM looks for available 3rd party edge compute and RAN resources (Operator C's ISSM view)

Figure 69: TestUC3.2b – ISSM selects best edge compute and RAN resources (Operator C's ISSM view)

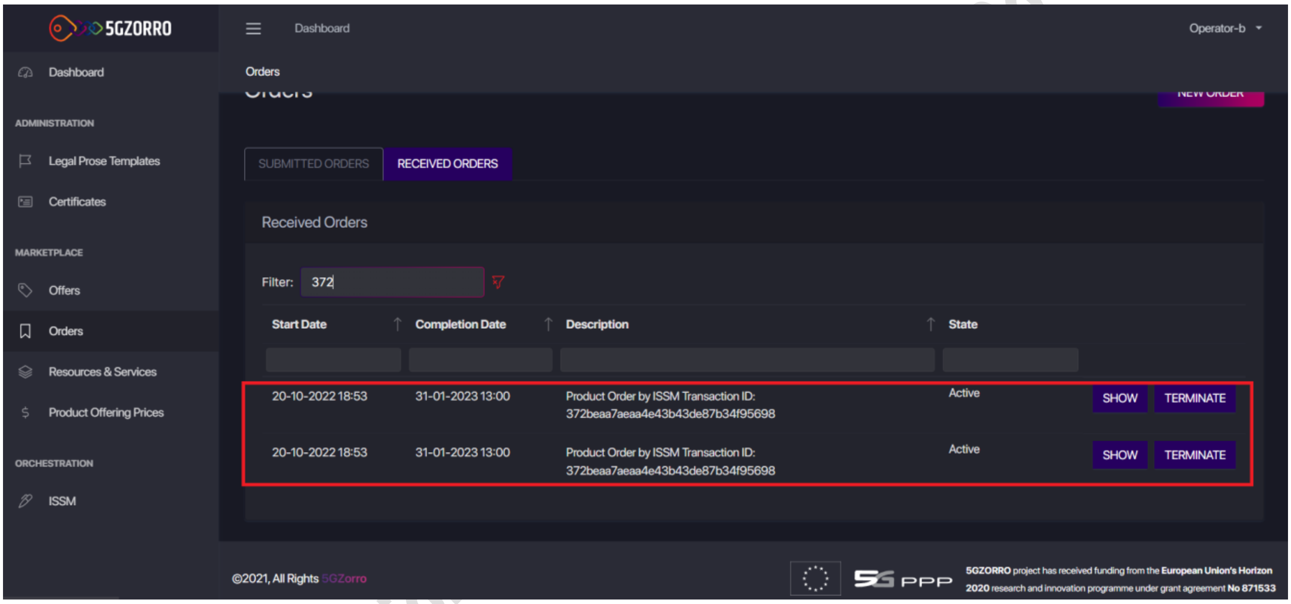


Figure 70: TestUC3.2b – Orders placed at Operator B form Operator C's ISSM (Operator B's portal view)

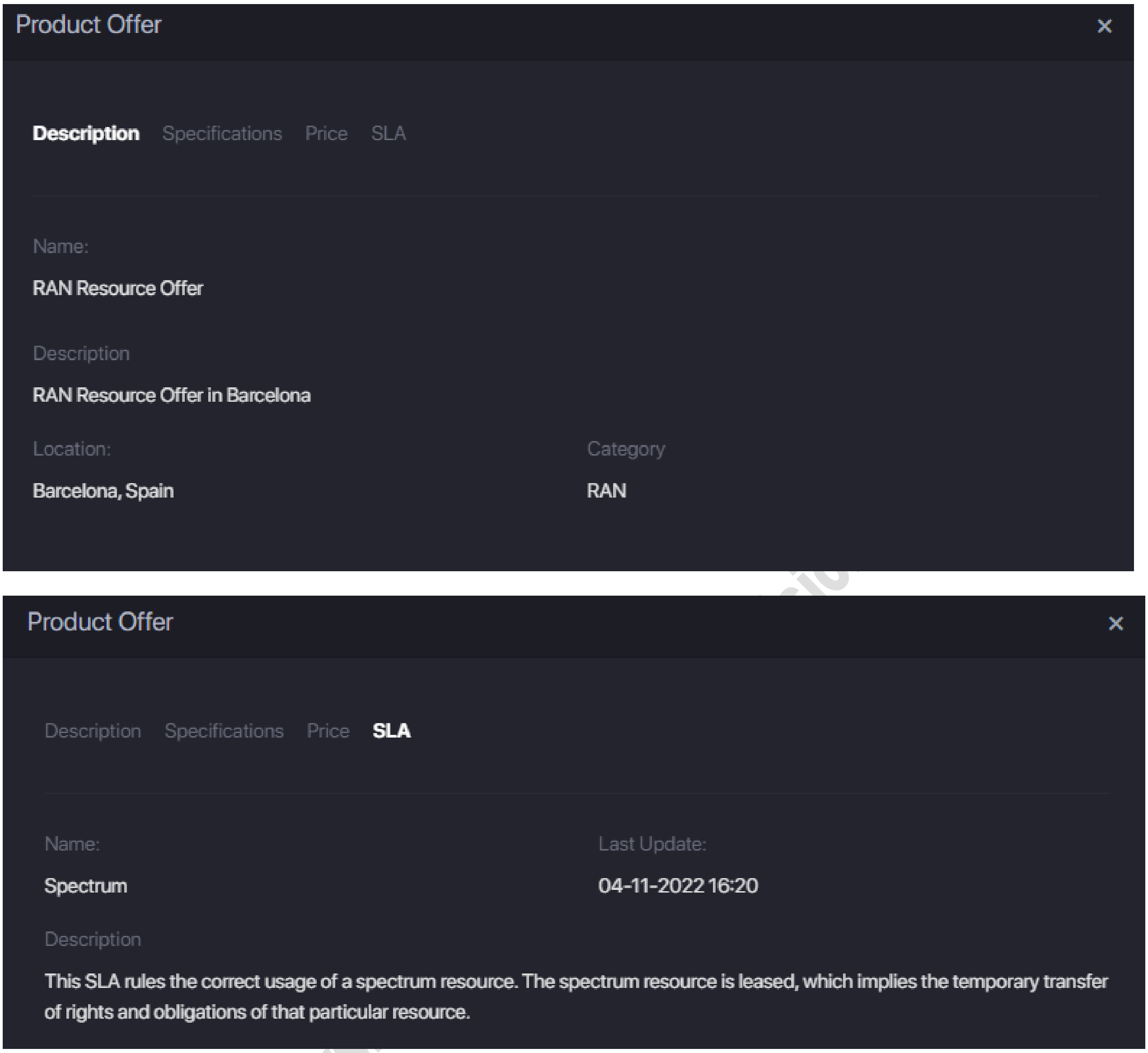


Figure 71: Test UC3.2b – RAN offer with SLA (Operator B's portal view)

2.4.2.1.3.TestUC3.2c: Slice extension to 3rd party radio and edge compute infrastructure

This test case refers to the process of extending the CDN network to the 3rd party infrastructure, as described in Table 31, which again is an extension of Table 5-9 of D5.2 [3].

Table 31: Slice extension to 3rd party radio and edge compute infrastructure

UC3.2c	**Slice extension to 3rd party radio and edge compute infrastructure**
Description	In addition to the VNF instantiation on the selected 3rd party, which was already validated in D5.2, in this test case we also demonstrate the inclusion of 3rd party's RAN in CSP's network. Therefore, a user initially connected to CSP's radio, will be able to connect to 3rd party's radio as well.
Key Use-case requirements and KPIs	• [KPI-UC3.4] Network Slice extension time < 2mins • [KPI-UC3.1] Deployment time for application components (VNFs, CNFs) < 5 mins • [KPI-UC3.5] Data rate between Central CDN Server & Edge Server > 200Mbps • [KPI-UC3.6] Latency between Central CDN Server & Edge Server < 20ms

	• [KPI-UC3.7] End-to-end Latency < 50ms	
Components and Configuration	Components	• ISSM • Network Slice & Service Orchestrator (NSSO) • eLicensing Manager (eLM) • xRM • 5G-TRMF +Security Analytics Service (SAS)
	Configuration	The 5GZORRO components should be configured accordingly in order to create the Network Slice Instance in 3rd party resources. More specifically, • ISSM: initiates the process of the slice creation by triggering the NSSO's of both domains (CSP's and 3rd party's). • NSSO: NSSOs on both domains update/create the slices and stich them • eLicensing: approves or denies the extension • xRM: is involved in slices update/creation and in the stitching • 5G-TRMF and SAS: Gathers security related monitoring data and processes them
Test Procedure	Pre-conditions	UC3.2b has been completed and ISSM knows how to access the 3rd party resources. For the sake of the test, the 3rd party is considered to be a tenant different from CSP. This means that it shares the same infrastructure with the CSP and they are at the same network, but they are isolated and don't communicate with each other before the slice extension.

	Test Case steps	• ISSM invokes to NSSO in charge of orchestrating the service on the 3rd party resource and:
		  o Requests the allocation and configuration of the RAN resource (Figure 722)
		  o Creates a Vertical Service Descriptor (VSD) that incorporates the vCDN cache descriptor (Figure 733)
		  o Requests the instantiation of the above VSD
		• The NSSO fulfils the VSD instantiation request by executing the following steps:
		  o VNF license check against the eLicensing Manager
		  o Instantiation of the service through the NVFO (OSM)
		  o Configuration of the MDA for collecting service metrics
		• The NSSO fulfils the RAN allocation request

Measurements	Methodology	The reported KPIs were calculated manually, by performing separated tests for each one.
	Complementary measurements	None
	Calculation process	• The deployment times are computed from ISSM logs • The throughput was measured with iperf tool, by sending TCP packets from the main cache (i.e. Central CDN server) to the edge cache. • The latency between edge cache and main cache was measured by sending 200 ping requests. • The latency between the user and CDN servers was measured by sending 1000 requests to each of the servers, i.e. the Central CDN server and the Edge Cache.
Result	The slice extension and the inclusion of the new Edge Cache into the CDN network is done successfully.	

	• **[KPI-UC3.4]** Network Slice extension time < 2mins: This was achieved. Generally, the time for the creation of the new slice at Operator B, as it was calculated from ISSM side, was 21s. However, this does not include the actual time that it took for the lower level orchestration services (e.g. OSM) to instantiate the slice, as it is infrastructure dependant (i.e. hardware capacity and capability). In other words, it is relevant to measure the overhead that 5GZORRO orchestration services add to the operator's orchestration services for the slice deployment time, which is then measured as 21 s. • **[KPI-UC3.1]** Deployment time for application components (VNFs, CNFs) < 5 mins: This was achieved. Generally, the time for the instantiation of the Network Service at Operator B, as it was calculated from ISSM side, was 22s. As in KPI-UC3.4, this is the overhead that 5GZORRO orchestration services add to the operator's orchestration services for the VNFs deployments. • **[KPI-UC3.5]** Data rate between Central CDN Server & Edge Server > 200Mbps: Achieved. The throughput from the edge cache to the main cache was, in average, 12.1 Gbps • **[KPI-UC3.6]** Latency between Central CDN Server & Edge Server < 20ms: Achieved. The average Round Trip Time was 0.954 ms • **[KPI-UC3.7]** End-to-end Latency < 50ms: Achieved. The average latency from the user to the CDN Central Service (that is the first connection to CDN) was 30.299 ms, while the latency between the user and the edge cache of the 3rd party (that is the actual video transmission) was 28.84 ms. We notice that for both servers, the latency is similar, as they are located in the same infrastructure, even though they are different tenants. The KPIs KPI-UC3.5/6/7 are application and infrastructure dependent and they are not related to 5GZORRO platform. The only impact that 5GZORRO has on these KPIs is that the CDN traffic passes through the security component (i.e. SAS) which is responsible for monitoring the traffic, detecting threads and updating 5G-TRMF accordingly. Therefore, this adds additional delays to the transmission of the flow. However, even so, the achieved values are well below the threshold that is set by CDN requirements. Moreover, it is interesting to note also the time that ISSM receives the breach prediction notification until a successful slice extension is completed was calculated to be around 5 minutes (on average it was 284 seconds). This time includes only the additional steps performed by ISSM (e.g. notification handling etc.), not the time of the slice instantiation that is performed by the orchestration services of an operator. Finally, after the instantiation of the new service instance on Operator B, it is verified that the user is connected to Operator B's RAN (Figure 744) and gets content from the edge cache that was instantiated there (Figure 755).

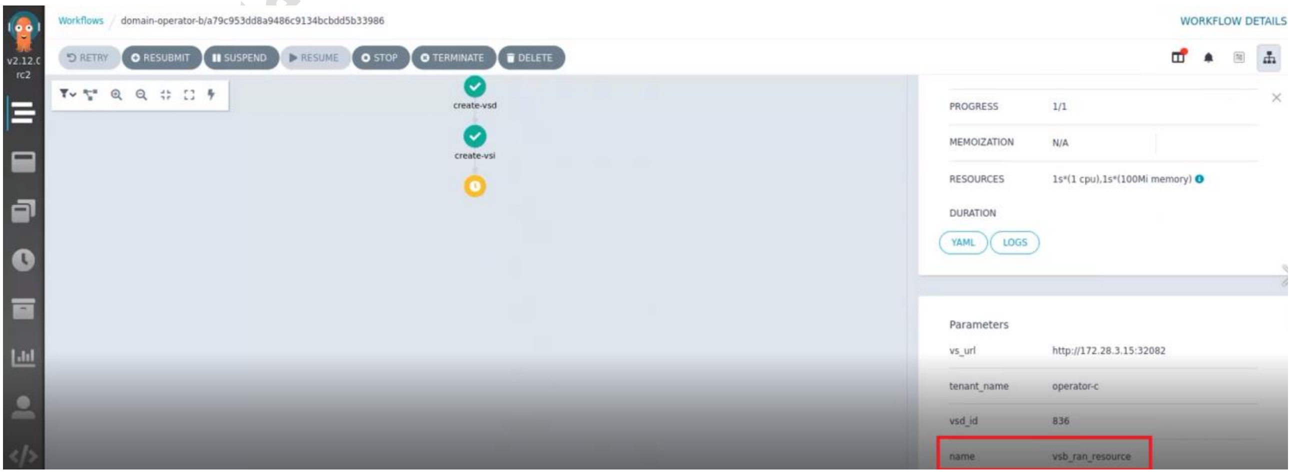


Figure 72: TestUC3.2c – Allocation of RAN resource in Operator B (Operator B's ISSM view)

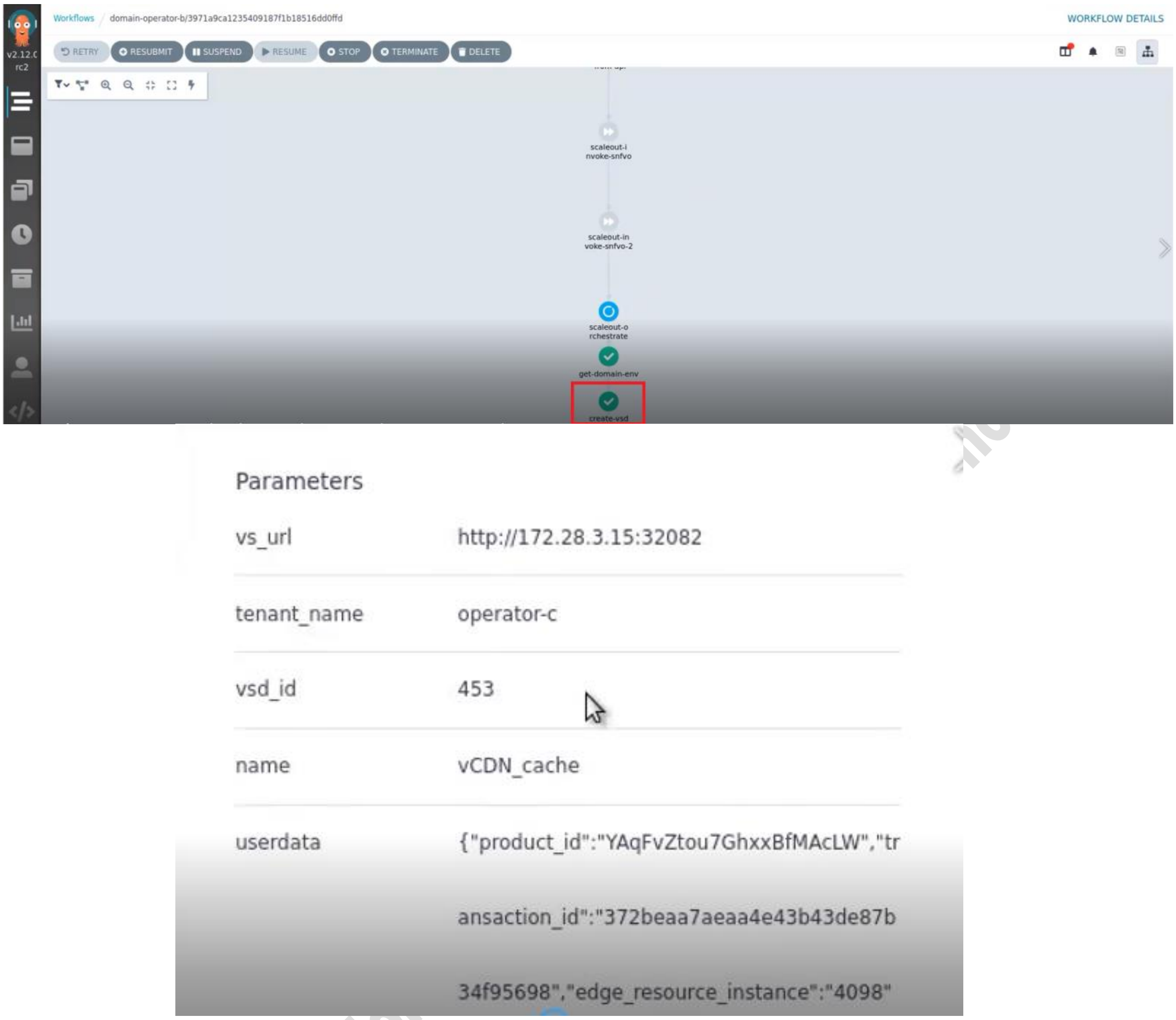


Figure 73: TestUC3.2c – Creation of VSD for vCDN service in Operator B (Operator B's ISSM view)

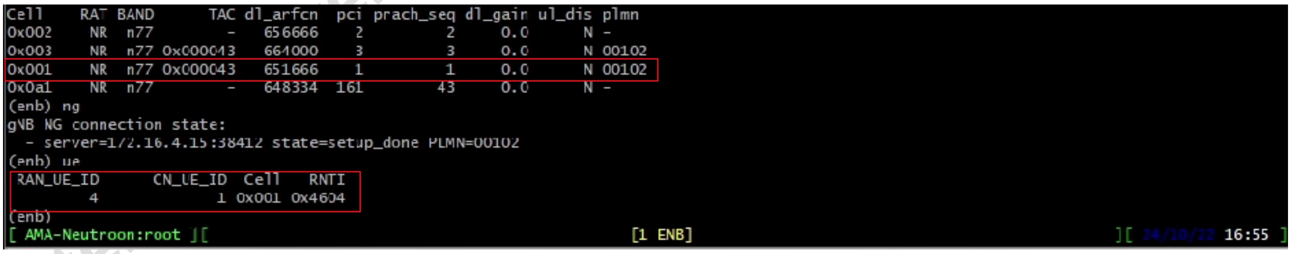


Figure 74: TestUC3.2c – A UE is connected to gNB #1, which belongs to Operator B (gNB view)

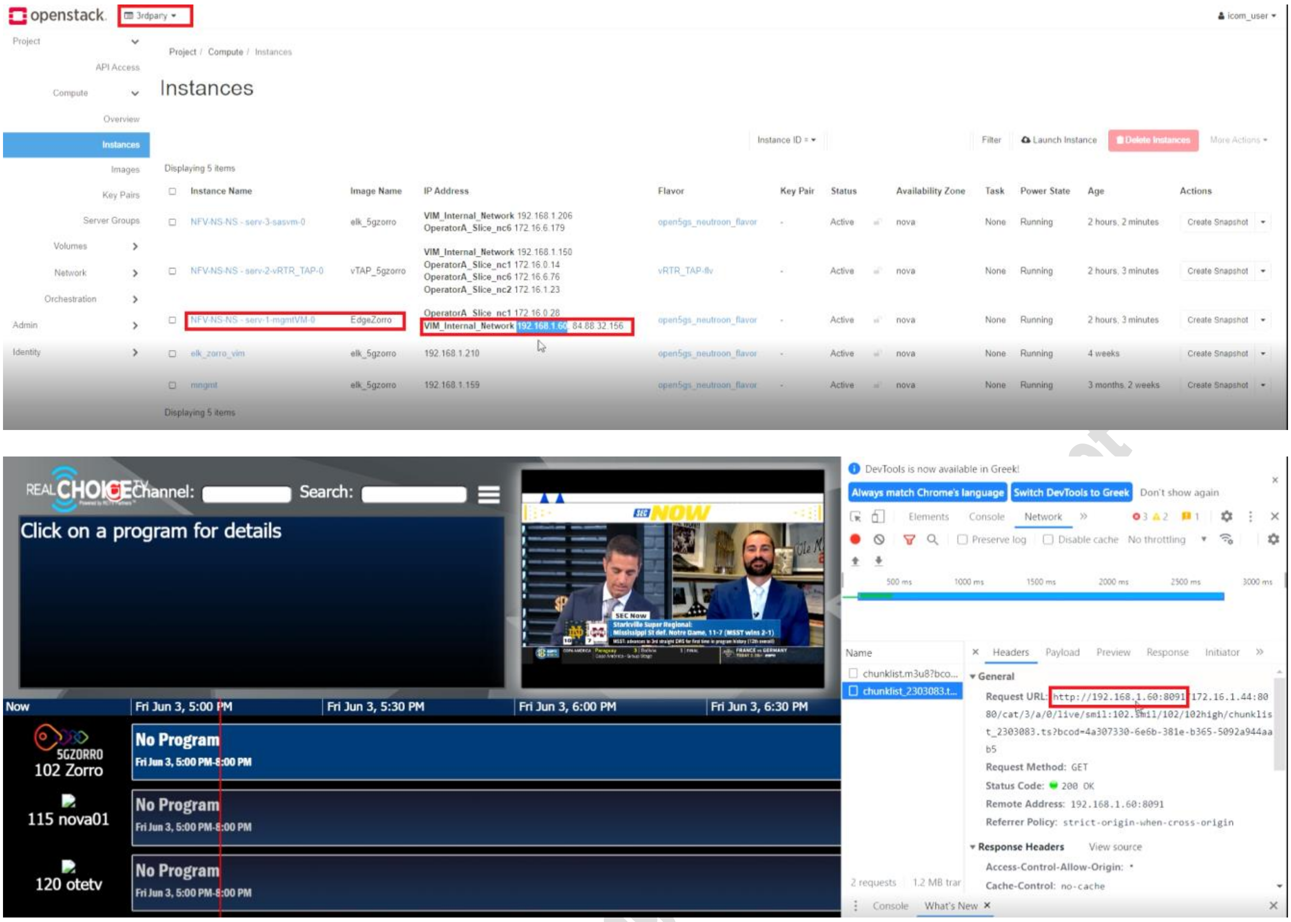


Figure 75: TestUC3.2c – Verifying that the user gets content from the edge cache located at the 3rd party resource provider (above: Openstack view, below: user view)

2.4.2.2.Scenario 3.3: Licensing validation

2.4.2.2.1.Test UC3.3c: eLicense expiration

This test case is reported for the first time in the present deliverable. The goal is to further test the 5GZORRO eLicensing functionalities, by validating the eLicense expiration flow. Table 32 analyses this scenario.

Table 32: eLicense expiration

UC3.3c	**eLicense expiration**	
Description	In this scenario we assume that a CDN edge cache VNF has already been instantiated and associated to an eLicense agreement. After some time, the license expires, triggering the service decommission and the release of resources. The goal of the test is to validate this flow.	
Key Use-case requirements and KPIs	No KPIs are measured in this test. It is just a validation of the related eLicensing feature.	
Components and Configuration	Components	• NSSO • xRM • eLM • Marketplace portal

	Configuration	The 5GZORRO components should be configured to handle the following operations: • NSSO: Handle the service decommission and release of resources • eLicensing: triggers the end of an eLicense • Marketplace portal: to show what happens in GUI
Test Procedure	Pre-conditions	A CDN edge cache VNF has already been instantiated and associated to an eLicense. More specifically, the test was done for the VNF instantiated at the 3rd party, at Test UC3.2c.
	Test Case steps	The eLM monitors, via the xRM, the utilization of a VNF that has a license expiration due soon. When the expiration time is reached, the eLM does the following: - eLM find all active NSs that are using the affected VNF. - eLM sends an update of the e-license in the DLT to the SCLCM. - eLM sends a notification to the Marketplace portal to display a pop up to the relevant user. - The portal triggers the service decommission flow. The NSSO stops and decommissions the affected NS
Measurements	Methodology	The eLM observes the execution of the VNFs and keeps the track of the time that are running. If the validity of the VNF ends for any reason, the eLM will be aware of this and send to the SCLCM the time of usage that this deployment had and alert the relevant actors to trigger a decommission flow.
	Complementary measurements	None
	Calculation process	No KPIs are measured in this test. It is just a validation of the presented flow.
Result	We ensure that ordering a virtualized service is monitored and managed end to end. VNF providers are assured that their offerings are not used after their offering period, and all relevant actors are notified of important events (See Figure 766 and Figure 777).	

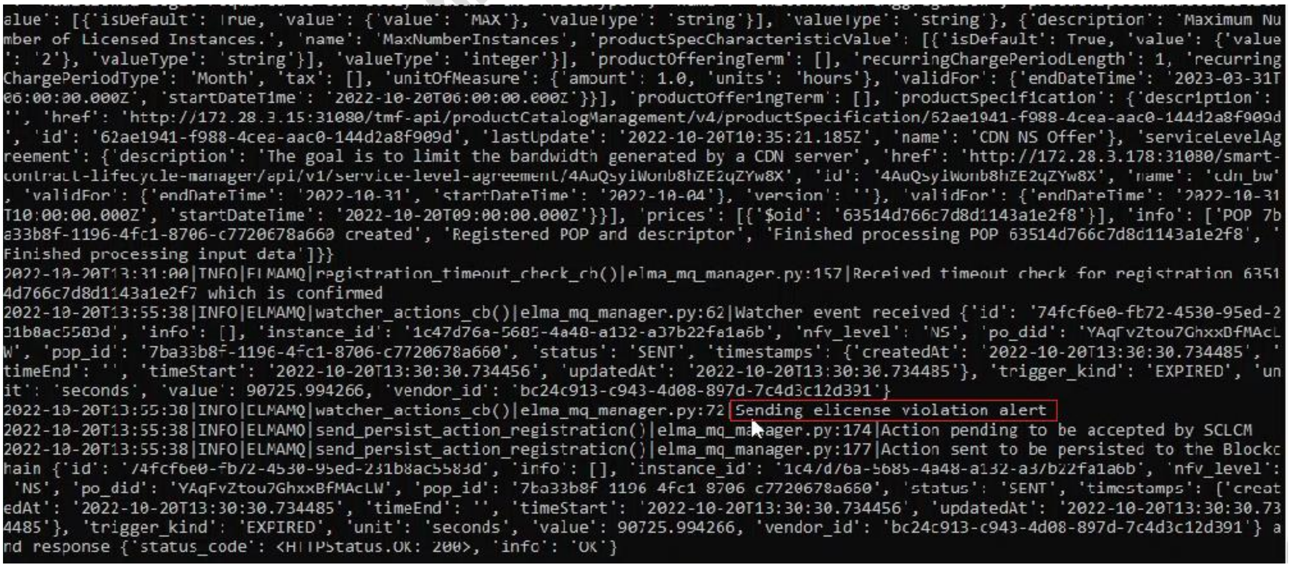


Figure 76: UC3.3c – Notification of eLicense expiration on the eLM view

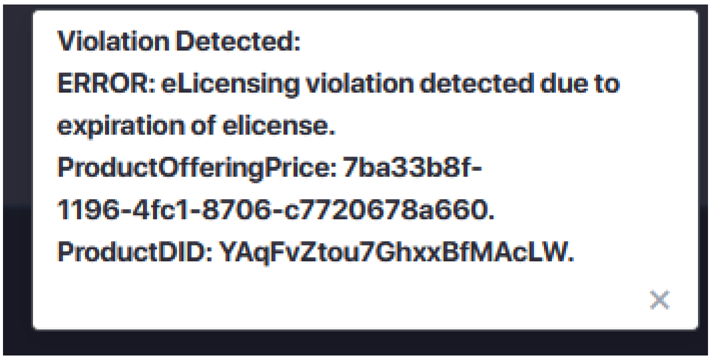


Figure 77: UC3.3c – Notification of eLicense expiration as it appears on the Portal

2.4.2.3. Scenario 3.4: Cross-testbed CDN deployment

The setup of this scenario is shown in Figure 788.

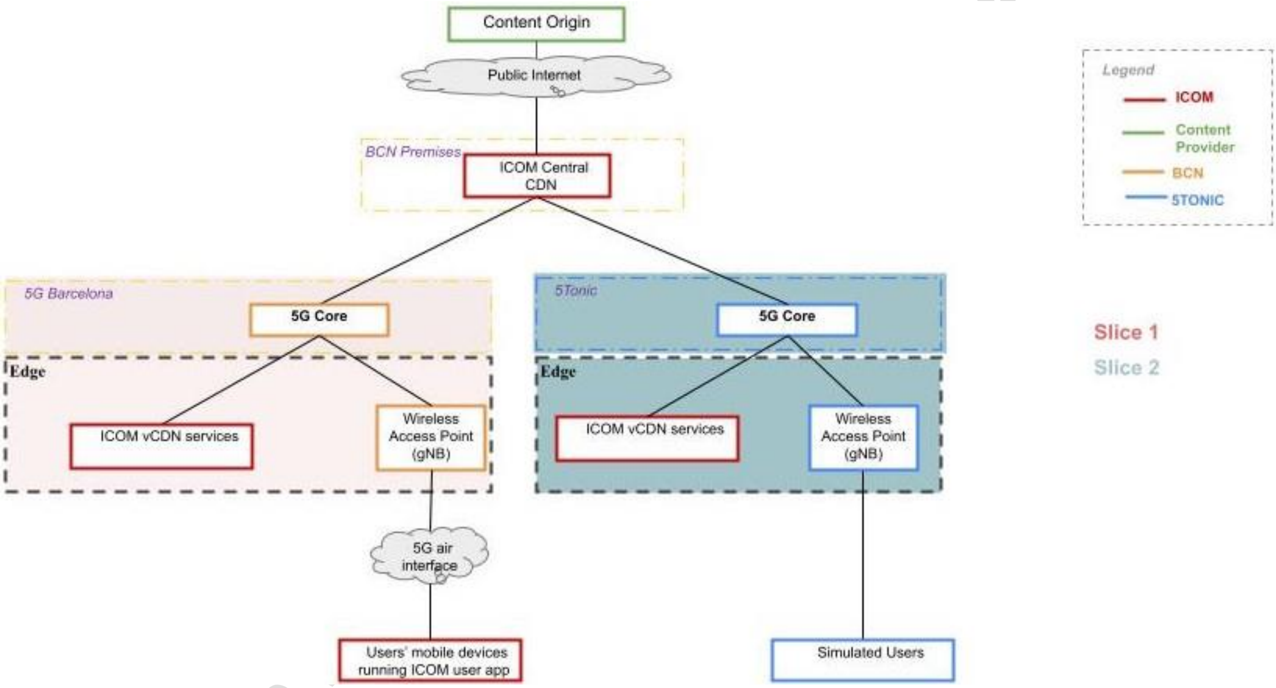


Figure 78: Deployment architecture for the 4th scenario of UC3 (cross-testbed service)

The concept of Scenario 4 is that a CDN provider (vertical) leverages 5GZORRO in order to provide its services to clients in different locations, where in each one, different technologies are supported. Particularly, in this scenario, we have one Service Provider who requests for a Slice Instance at Barcelona. To do this, the Service Provider gets into the Marketplace portal and manually searches for, selects and activates a slice resource offer and a Network Service resource offer (vCDN) at 5GBarcelona. Then, the Service Provider decides that it wants to also have service coverage in Madrid, so it asks for a network slice at Madrid. However, in this case, the resources will not be selected manually. On the contrary, an intent query will be made to Smart Resource and Service Discovery (SRSD) through the Portal. After that, the relevant 5GZORRO components, namely SRSD, 5G-TMRF, Intelligent Slice & Service Manager – WorkFlow Manager (ISSM-WFM) and ISSM – Optimiser (ISSM-O), will take over in checking the available resources, selecting the ones needed and instantiating them. Additionally, in this scenario, there is no offer in Madrid side that can completely cover the requirements in respect to the number of users or requests that can be supported. Therefore, the 5GZORRO platform will select offers, which combined can cover the specific service needs as specified in the intent, showcasing in this way the capabilities of ISSM Optimiser. As a result, there will be two vCDN caches on 5Tonic testbed.

All in all, in high level, the scenario can be summarised into two steps:

1. CDN provider uses the 5GZORRO platform to request for a CDN slice (Slice 1) in Barcelona. The slice is created at 5GBarcelona testbed using Open 5GS.
2. CDN provider uses the 5GZORRO platform to request for a CDN slice (Slice 2) in Madrid. The slice is created at 5Tonic using free5GC.

The slices between 5Tonic and 5GBarcelona are different, independent, E2E slices. There is no connection required between them. Also, they do not share the same 5G Core, as they belong to different Communication Service Providers (CSPs). It is interesting to note that the Monitoring Data Aggregator (MDA) and SLA Monitoring components are executed over Trusted Execution Environments (TEEs), in 5Tonic deployment.

2.4.2.3.1.Test UC3.4a: CDN application deployment on 5G Barcelona

This Test Case refers to the initial deployment of the CDN slice at the CSP site and is already described in D5.2 [3], where its execution on 5GBarcelona testbed was analysed. However, it is repeated in this scenario in order to re-evaluate it with the updated 5GZORRO platform, as well as to have a slice different from the one in Scenario 1, for the sake of clarity. Table 33 describes the test case.

Table 33: CDN application deployment on 5G Barcelona

UC3.4a	**CDN application deployment on 5G Barcelona**	
Description	This is similar to UC3.1b that was tested in D5.2, with the difference that the 5GZORRO modules and the infrastructure itself have changed from the time that UC3.1b was tested. Therefore, the relevant KPIs are calculated again.	
Key Use-case requirements and KPIs	• [KPI-UC3.1] Deployment time for application components (VNFs, CNFs) < 5 mins • [KPI-UC3.3] Network Slice creation time < 3mins • [KPI-UC3.5] Data rate between Central CDN Server & Edge Server > 200Mbps • [KPI-UC3.6] Latency between Central CDN Server & Edge Server < 20ms • [KPI-UC3.7] End-to-end Latency < 50ms	
Components and Configuration	Components	• ISSM • Marketplace Portal • Catalogue • SCLCM • NSSO • eLM
	Configuration	• The Central CDN server includes the following software modules (deployed as VNFs): Packaging, Subscriber & Content Management, Streaming Server, Transcoding, Encryption, and Main Cache. • One of ICOM's CDN software modules named Edge Cache is deployed on the Edge server as VNF.
Test Procedure	Pre-conditions	• Connectivity shall be available across all infrastructure components.
	Test Case steps	1. A CDN Service Provider (in this case it's Operator C in 5G Barcelona testbed) orders the slice and VNF offers from the CSP (Operator A)

		(**¡Error! No se encuentra el origen de la referencia.**9) and instantiates them. 2. An agreement is created between these two parties. 3. A user opens the CDN web application and select the content to watch (i.e. channel *102 Zorro*) (**¡Error! No se encuentra el origen de la referencia.**80). 4. The Edge server starts streaming the content (**¡Error! No se encuentra el origen de la referencia.**80).
Measurements	Methodology	The reported KPIs were calculated manually, by performing separated tests for each one.
	Complementary measurements	None
	Calculation process	• The deployment times are computed from ISSM logs • The throughput was measured with iperf tool, by sending TCP packets from the main cache to the edge cache, which are both located in Barcelona. • The latency between edge cache and main cache was measured by sending 200 ping requests. • Since the edge cache is in the same infrastructure with the Central CDN, as it was the case with TestUC3.2c, it is safe to assume that the latency between the user and the CDN servers is similar to the one calculated in that test. So, no separate measurement was performed for this KPI and this test.
Result	• **[KPI-UC3.1]** Deployment time for application components (VNFs, CNFs) < 5 mins: This was achieved. Generally, the time for the instantiation of the creation of the VNFs, as it was calculated from ISSM side, was 22s. As in Test UC3.2c, this is the overhead that 5GZORRO orchestration services add to the operator's orchestration services for the VNFs deployments. • **[KPI-UC3.3]** Network Slice creation time < 3mins: This was achieved. Generally, the time for the instantiation of both CSP slice and vCDN cache at Operator A, as it was calculated from ISSM side, was around 3mins (in average it was 175 seconds). Therefore, the time for the slice creation only is less than 3 minutes. However, it is important to note that the metric that is reported here does not include the actual time that it took for the lower level orchestration services to instantiate the slice. In other words, we report only the overhead that 5GZORRO orchestration services add to the operator's orchestration services for the slice deployment time. • **[KPI-UC3.5]** Data rate between Central CDN Server & Edge Server > 200Mbps: Achieved. The throughput from the edge cache to the main cache was, in average, 13.8 Gbits/sec • **[KPI-UC3.6]** Latency between Central CDN Server & Edge Server < 20ms: Achieved. The average Round Trip Time was 0.394 ms • **[KPI-UC3.7]** End-to-end Latency < 50ms: Achieved. It is similar to KPI-UC3.7 reported in Table 31 In general, KPIs KPI-UC3.5/6/7 are application and infrastructure dependent and they are not related to 5GZORRO platform.	

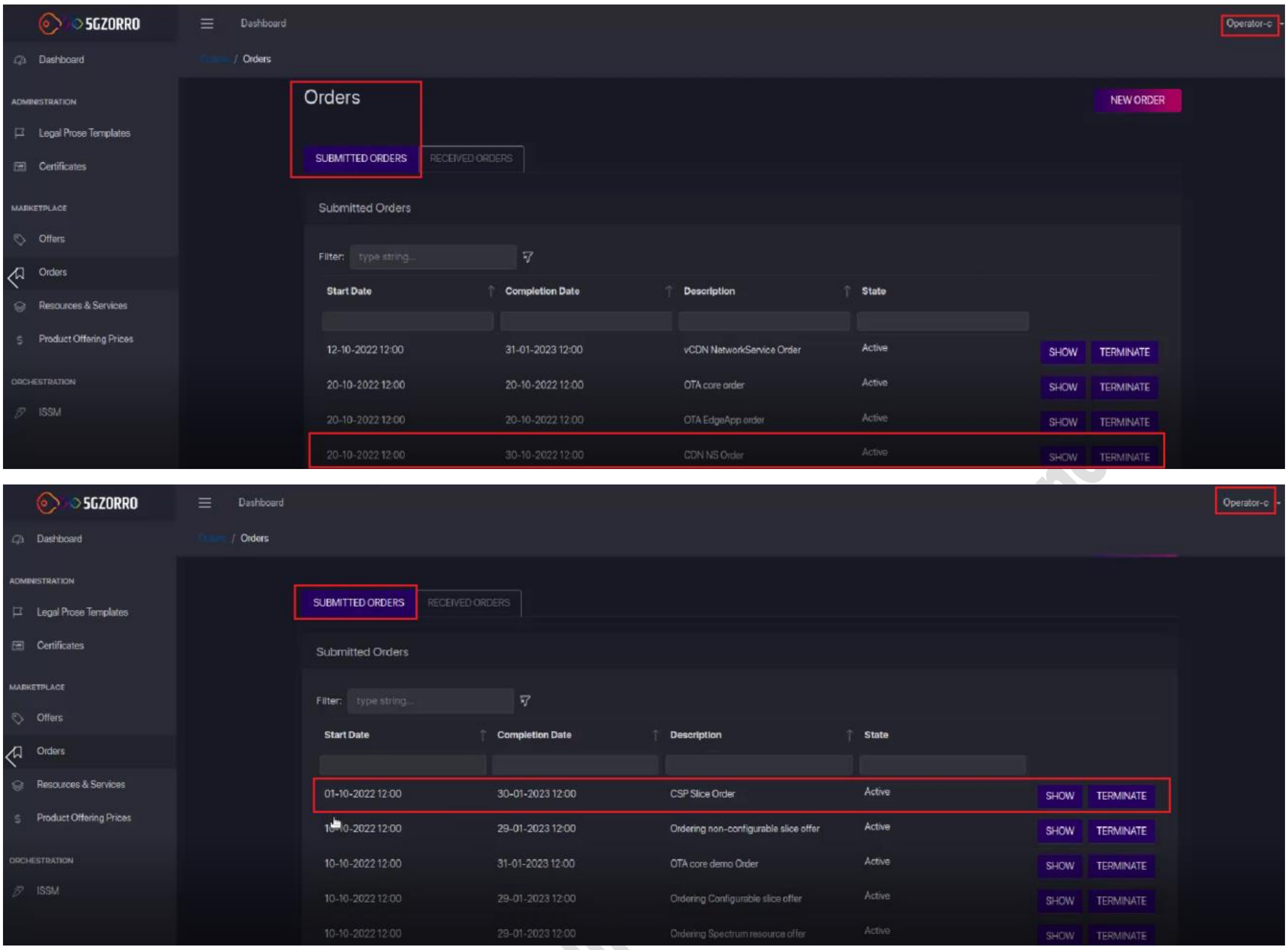


Figure 79: TestUC3.4a – Orders placed at Operator A form Operator C (Operator C's portal view) (above NS product order, below: slice product order)

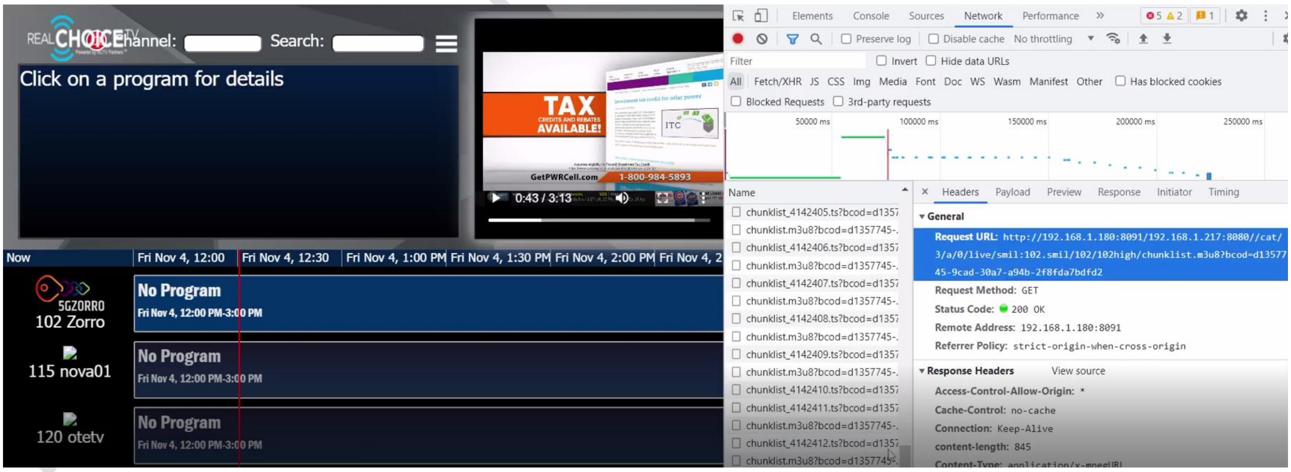


Figure 80: TestUC3.4a – A user sees content from the edge cache located at Operator A in Barcelona (user view)

2.4.2.3.2. Test UC3.4b: CDN application deployment on 5Tonic

This Test Case refers to the deployment of a second CDN slice at a different CSP, located at Madrid. In general, the goal is to validate and evaluate the deployment of the CDN VNFs over the 5Tonic testbed, configure the slice and verify initial connectivity between all components. Emphasis is placed on evaluating aspects related to ease and speed of development. Additionally, it aims at evaluating the E2E connectivity across all CDN components, by examining, for example, the aspects related to data rate and latency achieved. For more details, see Table 34.

Table 34: CDN application deployment on 5Tonic

UC3.4b	**CDN application deployment on 5Tonic**	
Description	In this case, the CDN Service Provider orders the slice and VNF offers from a CSP (Operator E) in 5Tonic and instantiates them. Also, an agreement between these two parties is created. In contrast to UC3.4a, here we assume that, for the compute part, it is not possible to find one single offer that satisfies the requirements. Thus, we have to order two offers, which together complete the requirements. Therefore, two edge caches will be instantiated in 5Tonic.	
Key Use-case requirements and KPIs	• [KPI-UC3.1] Deployment time for application components (VNFs, CNFs) < 5 mins • [KPI-UC3.3] Network Slice creation time < 3mins • [KPI-UC3.5] Data rate between Central CDN Server & Edge Server > 200Mbps • [KPI-UC3.6] Latency between Central CDN Server & Edge Server < 20ms • [KPI-UC3.7] End-to-end Latency < 50ms • [KPI4.2] Implement/correlate technical service configurations and SLA monitoring interactions between multiple parties • [KPI5.6] Agnostic support of various radio technologies, to ensure that the market will work regardless of the considered radio technology	
Components and Configuration	Components	• ISSM • Marketplace Portal • Catalogue • SCLCM • NSSO • eLM • SRSD
	Configuration	• Similar to UC3.4a
Test Procedure	Pre-conditions	• Connectivity shall be available across all infrastructure components.
	Test Case steps	1. The CDN Service Provider (Operator C) orders the slice and VNF offers from the CSP at 5Tonic (Operator E) and instantiates them. Contrary to Test UC3.4a, in this case the offers are not selected manually. Instead, and indent query is made to SRSD (through the portal) and then the final selection is made by ISSM-Optimiser (ISSM-O) 2. An agreement is created between these two parties. 3. A user opens the CDN web application and select the content to watch (i.e. channel *102 Zorro*) (**¡Error! No se encuentra el origen de la referencia.**81). 4. The Edge server starts streaming the content (**¡Error! No se encuentra el origen de la referencia.**81).
Measurements	Methodology	The reported KPIs were calculated manually, by performing separated tests for each one.
	Complementary measurements	None

	Calculation process	• The deployment times are computed from ISSM logs • Throughput was measured with iperf tool, by sending TCP packets from the main cache located in Barcelona to the edge cache located in Madrid. • The latency between edge cache and main cache was measured by sending 200 ping requests • The latency between the user and CDN edge cache deployed in 5Tonic was measured by sending ping requests to that server. Since the connection of the UE to the Central CDN happens only one time (in order to get the edge cache IP) it is wasn’t considered relevant to measure the latency to that server
Result	• **[KPI-UC3.1]** Deployment time for application components (VNFs, CNFs) < 5 mins **and [KPI-UC3.3]** Network Slice creation time < 3mins: These KPIs were achieved. Generally, the total time of the free5GC slice deployment in Operator E is around 36 seconds. In this case, the slice creation is handled exclusively by ISSM-MEC, so there are no additional delays in the deployment times. • **[KPI-UC3.5]** Data rate between Central CDN Server & Edge Server > 200Mbps: Achieved. The throughput from the edge cache to the main cache was, in average, 220 Mbps. • **[KPI-UC3.6]** Latency between Central CDN Server & Edge Server < 20ms: Achieved. The average Round Trip Time was 12.936 ms • **[KPI-UC3.7]** End-to-end Latency < 50ms: Achieved. The average latency between the user and the edge cache deployed on 5Tonic was 2.485 ms. This is a lot smaller than the latency achieved for the users in Barcelona (see Table 31). This is because of the differences between the 2 testbeds. For example, in 5Tonic we have a simulated user (a VM) and a simulated radio infrastructure, while in Barcelona we have real devices. • **[KPI4.2]** The KPI target was set as SLA measurements and validation from at least 3 operators involved in a multi-party service chain. For this scenario, the KPI is achieved, as Operator C maintains agreements with both Operator A (at 5GBarcelona) and Operator E (at 5Tonic) for the same service. • **[KPI5.6]** Agnostic support of various radio technologies, to ensure that the market will work regardless of the considered radio technology: Achieved. The two testbeds have different radio technologies (real radio in 5G Barcelona managed through Amarisoft and simulated radio in 5Tonic with free5GC) and the 5GZORRO can use both. This is transparent to the user of the platform (e.g. Operator C) As mentioned in Table 33, KPIs KPI-UC3.5/6/7 are application and infrastructure dependent and they are not related to 5GZORRO platform.	

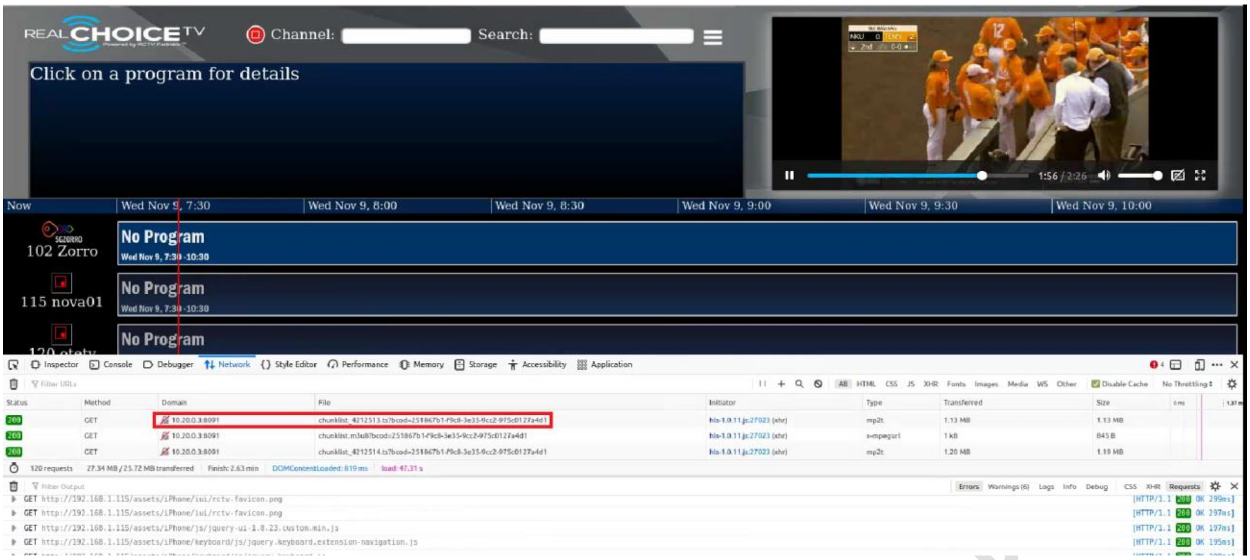


Figure 81: TestUC3.4b – A user sees content from the edge cache located at Operator E in Madrid (user view)

2.4.2.3.3.Test UC3.4c: Validate 5GZORRO services over TEEs

This Test Case focuses on the validation of the Trusted Execution Environments (TEEs) functionalities. The component that runs over TEE is the MDA. For more details, see Table 35.

Table 35: Validate 5GZORRO services over TEEs

UC3.4c	**Validate 5GZORRO services over TEEs**	
Description	In this case, we are showcasing MDA over TEE in 5Tonic testbed.	
Key Use-case requirements and KPIs	No KPIs are calculated. This is just a validation test	
Components and Configuration	Components	• MDA • Datalake • TEE
	Configuration	• MDA: gets monitoring data from xRM and sends them to the Datalake • Datalake: this is where the monitoring data are stored • ’TEE: A secure environment where MDA is running
Test Procedure	Pre-conditions	• UC3.4b is completed • MDA is deployed on TEE
	Test Case steps	1. Enable a certain monitoring specs 2. Retrieve all the existing monitoring specs
Measurements	Methodology	• Deploy MDA on TEE and invoke the MDA API
	Complementary measurements	-
	Calculation process	-
Result	The following figures presents the result of an invocation of the MDA API to	

1. Enable a certain monitoring spec. The tested spec was to monitor the transaction of the product with 10 of the operator A and that could be monitored via OSM. The metric in specifc verifies if the average availability is within the appropriated values.

```
root@node1:~# curl -X 'POST' 'http://10.233.7.126:4000/settings' -H "accept: application/json" -H "Content-T
ype: application/json" -d "{\"transaction_id\":\"ab51f3e1-7b61-4f9d-85a4-9e9f366b593b\",\"instance_id\":\"21
\",\"product_id\":\"10\",\"data_source_type\":\"OSM\",\"topic\":\"operator-a-in-0\",\"monitoring_endpoint\":
\"http://osm:4500/monitoringData?match=metric_name&start=start_time\",\"timestamp_start\":\"2022-12-20T11:04
:34.030387\",\"timestamp_end\":\"2022-12-20T11:05:34.030387\",\"metrics\":[{\"metric_name\":\"availability\"
,\"metric_type\":\"availability\",\"aggregation_method\":\"AVG\",\"step\":\"1m\",\"step_aggregation\":\"2m\"
}],\"tenant_id\":\"operator-a\",\"context_ids\":[{\"resource_id\":\"10\",\"network_slice_id\":\"22\",\"paren
t_id\":\"10\"}]}"
{"id":"0dc3e6bf-e282-406a-83fa-43570e667048","created_at":"2022-11-04T18:40:05.521446","updated_at":null,"tr
ansaction_id":"ab51f3e1-7b61-4f9d-85a4-9e9f366b593b","instance_id":"21","product_id":"10","topic":"operator-
a-in-0","monitoring_endpoint":"http://osm:4500/monitoringData?match=metric_name&start=start_time","timestamp
_start":"2022-12-20T11:04:34.030387","timestamp_end":"2022-12-20T11:05:34.030387","metrics":[{"metric_name":
"availability","metric_type":"availability","aggregation_method":"AVG","step":"1m","step_aggregation":"2m","
next_run_at":"2022-12-20T11:04:34.030387","next_aggregation":"2022-12-20T11:06:34.030387"}],"status":1,"tena
nt_id":"operator-a","context_ids":[{"resource_id":"10","network_slice_id":"22","parent_id":"10"}]}root@node1
:~#
root@node1:~#
root@node1:~#
root@node1:~# curl -X 'GET' 'http://10.233.7.126:4000/settings' -H 'accept: application/json'
[{"id":"0dc3e6bf-e282-406a-83fa-43570e667048","created_at":"2022-11-04T18:40:05.521446","updated_at":null,"t
ransaction_id":"ab51f3e1-7b61-4f9d-85a4-9e9f366b593b","instance_id":"21","product_id":"10","topic":"operator
-a-in-0","monitoring_endpoint":"http://osm:4500/monitoringData?match=metric_name&start=start_time","timestam
p_start":"2022-12-20T11:04:34.030387","timestamp_end":"2022-12-20T11:05:34.030387","metrics":[{"metric_name"
:"availability","metric_type":"availability","aggregation_method":"AVG","step":"1m","step_aggregation":"2m",
root@node1:~#
```

And

2. Retrieve all the existing monitoring specs

```
root@node1:~# curl -X 'POST' 'http://10.233.7.126:4000/settings' -H "accept: application/json" -H "Content-T
ype: application/json" -d "{\"transaction_id\":\"ab51f3e1-7b61-4f9d-85a4-9e9f366b593b\",\"instance_id\":\"21
\",\"product_id\":\"10\",\"data_source_type\":\"OSM\",\"topic\":\"operator-a-in-0\",\"monitoring_endpoint\":
\"http://osm:4500/monitoringData?match=metric_name&start=start_time\",\"timestamp_start\":\"2022-12-20T11:04
:34.030387\",\"timestamp_end\":\"2022-12-20T11:05:34.030387\",\"metrics\":[{\"metric_name\":\"availability\"
,\"metric_type\":\"availability\",\"aggregation_method\":\"AVG\",\"step\":\"1m\",\"step_aggregation\":\"2m\"
}],\"tenant_id\":\"operator-a\",\"context_ids\":[{\"resource_id\":\"10\",\"network_slice_id\":\"22\",\"paren
t_id\":\"10\"}]}"
{"id":"0dc3e6bf-e282-406a-83fa-43570e667048","created_at":"2022-11-04T18:40:05.521446","updated_at":null,"tr
ansaction_id":"ab51f3e1-7b61-4f9d-85a4-9e9f366b593b","instance_id":"21","product_id":"10","topic":"operator-
a-in-0","monitoring_endpoint":"http://osm:4500/monitoringData?match=metric_name&start=start_time","timestamp
_start":"2022-12-20T11:04:34.030387","timestamp_end":"2022-12-20T11:05:34.030387","metrics":[{"metric_name":
"availability","metric_type":"availability","aggregation_method":"AVG","step":"1m","step_aggregation":"2m","
next_run_at":"2022-12-20T11:04:34.030387","next_aggregation":"2022-12-20T11:06:34.030387"}],"status":1,"tena
nt_id":"operator-a","context_ids":[{"resource_id":"10","network_slice_id":"22","parent_id":"10"}]}root@node1
:~#
root@node1:~#
root@node1:~#
root@node1:~# curl -X 'GET' 'http://10.233.7.126:4000/settings' -H 'accept: application/json'
[{"id":"0dc3e6bf-e282-406a-83fa-43570e667048","created_at":"2022-11-04T18:40:05.521446","updated_at":null,"t
ransaction_id":"ab51f3e1-7b61-4f9d-85a4-9e9f366b593b","instance_id":"21","product_id":"10","topic":"operator
-a-in-0","monitoring_endpoint":"http://osm:4500/monitoringData?match=metric_name&start=start_time","timestam
p_start":"2022-12-20T11:04:34.030387","timestamp_end":"2022-12-20T11:05:34.030387","metrics":[{"metric_name"
:"availability","metric_type":"availability","aggregation_method":"AVG","step":"1m","step_aggregation":"2m",
root@node1:~#
```

The second step proves that the monitoring spec was indeed enabled in the MDA running on TEE, therefore proving that the component running on TEE can still keep its functionality.

2.4.3. Main lessons learned and main challenges addressed on TEE

The Trusted Execution Environments are a cutting-edge technology that enables establishing root-of-trust and end-to-end secure communications as well as providing characteristics such as tamper-resistant and trustworthiness. The Trusted Execution Environment Security Management module aims at providing those functionalities that allow 5GZORRO to protect their tenant service or application running in a computing node against a stakeholder with malicious intentions.

Concretely, 5GZORRO has analysed the design, deployment and execution of different services and well-known applications such as the MDA component designed in the project or technologies such as Prometheus or OpenAir interface (OAI).

When it comes to the Monitoring Data Aggregator (MDA), it has been primarily selected to be run under a TEE in order to assure the aggregation, processing/computation integrity of SLA monitoring data. As Table 35 shows, the MDA instantiated on the 5TONIC Intel NUC was able to get monitoring data from xRM and send them to the Datalake, enabling critical workloads to go across different tenants and stakeholders with no losses in security. Besides, the data being processed is deemed trustworthy since we keep the same level of trust in the resulting processed data. The successful execution of this task under TEE was due to the 5GZORRO development of a TEE Manager and its APIs, which allowed registering a platform component in the TEE as well as retrieving attestation information of the component.

ISBP (Intelligent Service Branch Predictor) was also considered and deployed on TEE, once again proving that applications without complex build processes can be run on the TEE based on Intel SGX while communicating with the external services the ISBP requires.

Prometheus - the source of the data - was also considered for running on TEE. However, since SCONE requires that the binary running is a Position Independent Executable (PIE) binary, the sconification of Prometheus required complex changes in the build processes, namely the usage of a different compiler (gccgo) than the one used in the official build process. Since the compiler is not fully ported, missing low-level methods from the syscalls package and methods with different naming rendered the Prometheus build process arduous. Nevertheless, we developed a set of patches [10] so as to attempt to fix previous issues once we have identified the principal issue to run Prometheus on SCONE. Yet, after multiple combinations, the tentative patches did not allow fixing the issues related to the Prometheus compiler.

Another well-known software tested under our Trusted Execution Environment Security Management module was the OpenAir interface on the RAN segment. In this case, the SCONE framework encountered a number of hitherto unusual compilation problems at an early stage. In particular, all OAI components could not be compiled, as the required linux-image-lowlatency linux-headers-lowlatency for OpenAirKernelMainSetup gave an error during the sconification process, even after adding these dependencies to the Sconify Docker image used for building the OAI.

The implemented and tested TEE solution is based on the Intel SGX Instruction Set Extension. From the hardware-based solutions analyzed and described in D2.2 [10] and D2.4 [12] - Arm's TrustZone, Intel SGX, Intel Trusted Execution Technology - the Intel SGX solution resulted to be the most effective solution in terms of :

- Easiness to use with the SCONE framework after analysing the state-of-the-art. Yet, once development and deployment tasks started, a set of unexpected issues related to the used technologies arose. Thereby, the selected software components and technologies had a direct impact on the ease of use.
- Goal in mind - Intel Trusted Execution Technology focused on performing measurements on the platform components (boot loader, firmware, hypervisor, operating system) and verifies them against pre-calculated white list values - not on the applications running on the computer
- Scope of application - Arm's TrustZone is system-wide and some components should not be running on TEE. In addition, it requires each application to be partitioned/changed (unlike SCONE + Intel SGX)

Since the Intel SGX is complex to use and requires changing source code to call specific methods that use Intel SGX Instructions, the SCONE framework was leveraged to avoid manual conversion of existing applications.

It was possible to build a proof of concept system based on the SCONE framework, on an Intel NUC with a processor featuring SGX support and run and test the MDA successfully by invoking its API successfully. However, it was also possible to conclude that not only the usage of TEE is difficult to showcase - designed by obscurity, not much information is provided on the enclave or the application running on the TEE - but most importantly that everything should not run on TEE. Since TEE changes the program instructions - either manually or automatically through SCONE - this may create difficulties in compiling binaries as we previously described for Prometheus or OAI.

Future tasks on TEE should consider this as a privileged environment not fit for all applications -only very specific applications should be candidates to run within TEE. In addition, complex binaries should be avoided since TEE changes the program instructions, might require different compilation processes and/or compilers and might even require fixing the compiler itself (example of Prometheus) - all very time consuming, complex and error-prone.

Finally, different solutions not based on Intel SGX should be considered carefully. At the time of the proposal, a TEE based on Intel SGX was the most prominent solution on the state-of-the-art since its introduction in 2015 with the 6th generation of processors. However, Intel announced in January 2022 that future Intel Xeon Scalable Processors could be unable to support of the current Intel SGX although there are currently no plans to deprecate Intel SGX on the supported Intel Xeon Scalable processors [13][14]. A clear successor for Intel SGX was not clear until Intel released in August 2022 the first source code version of Intel Trust Domain Extensions (TDX) [14][13]**¡Error! No se encuentra el origen de la referencia.**, a new Intel technology that extends Virtual Machines Extensions (VMX) and Multi-Key Total Memory Encryption (MKTME) with a new kind of virtual machine. In this vein, Intel is currently making a technology shift from previous hardware-based solutions (like Intel SGX is) to new software-based products, which is fully aligned with the development and orchestration philosophy of future networks.

2.5. Summary of KPI validation

This section provides a summary view of the validation of 5GZORRO KPIs, as defined in the Description of Action and processed in WP5 as part of the UC1, UC2 and UC3 technical validations reported in the previous sections. Specific details on the KPI measurements and achievements are provided in the sections 2.2, 2.3, and 2.4 above, as well as in D5.2 [3] for those KPI that were already validated.

All in all, the table shows that 5GZORRO fully achieved large part of the defined KPIs, with just a couple that can be considered partially achieved.

Applicable Technical / Business KPI (general target)	KPI Target	Specific KPI	UC	Achievement (PASSED)	Measurement	Testcase reference
[KPI1.1] Support actual distributed multi-party service and business configurations.	More than 3 providers /operators of virtualized resources or services for spectrum, radio/edge/core compute & network.	**[KPI1.1.1]** New Resource Providers, Resource Consumers, Service Providers are enrolled into the platform.	UC 1 UC 2	PASSED	1 – 4 stakeholders	UC1.1, UC1.2, UC1.3, UC2.1, UC2.2, UC2.3, UC2.4
		[KPI1.1.2] Each stakeholder participating in the 5GZORRO Marketplace is approved	UC 1 UC 2	PASSED	N/A	UC1.1, UC1.2, UC1.3, UC2.1, UC2.2, UC2.3, UC2.4

Applicable Technical / Business KPI (general target)	KPI Target	Specific KPI	UC	Achievement (PASSED)	Measurement	Testcase reference
		[KPI1.1.3] Acceptance/rejection (consensus) when joining of a new node to the DLT network should be completed in less than 15 minutes.	UC 1 UC 2	PASSED	Processing of a request: 10 - 11s Approval: 2s	UC1.1, UC1.2, UC1.3, UC2.1, UC2.2, UC2.3, UC2.4
		[KPI1.1.4] All actors have a unique identity that derives from their organisation's identity. Permissions are assigned to a new Resource Provider / Service Provider to allow them to offer resources/services.	UC 1 UC 2	PASSED	N/A	UC1.1, UC1.2, UC1.3, UC2.1, UC2.2, UC2.3, UC2.4
		[KPI1.1.5] The process of bootstrapping a DLT node and provisioning 5GZORRO services should take no longer than 1 hour. Permissions are assigned to a new Resource Provider / Service Provider to allow them to offer resources/services.	UC 1 UC 2	PASSED	N/A It was not possible to measure the actual time in current tests, but it was no more than a few minutes	UC1.1, UC1.2, UC1.3, UC2.1, UC2.2, UC2.3, UC2.4

Applicable Technical / Business KPI (general target)	KPI Target	Specific KPI	UC	Achievement (PASSED)	Measurement	Testcase reference
[KPI3.1] 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	Smart Contract for 3 or more untrusted parties	**[KPI3.1.1]** Smart Contract for 3 or more 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.	UC 1	PASSED	N/A	UC1.4, UC1.5, UC1.7, UC1.8, UC1.11, UC1.12, UC1.13, UC1.15, UC1.16, UC1.19
		[KPI3.1.2] The addition of a new resource offer to the catalogue should complete in less than 1 minute (from transaction request to being committed to the ledger).	UC 1	PASSED	The time for a resource offer to be published and distributed to all catalogues was measured as 30-60 seconds, depending on the volume of submitted offers	UC1.4, UC1.5, UC1.11, UC1.12, UC1.13
[KPI4.1]Automatically discover and "inventorize" various types of resources (i.e., compute, storage, network at core, edge, far-edge), spectrum and services capabilities from different domains and service providers	Distribution of resource updates and discovery in less than 10 mins	**[KPI4.1.1]** Resources are discoverable in the catalogue by all registered consumers within 5 minutes of being registered and verified.	UC 1 UC 2 UC 3	PASSED	<30 – 66 s	UC1.4, UC1.5, UC1.7, UC1.8, UC1.11, UC1.12 UC1.13, UC1.14, UC1.15, UC1.16, UC2.5c, UC2.9a UC3.1c, UC3.2b

Applicable Technical / Business KPI (general target)	KPI Target	Specific KPI	UC	Achieveme nt (PASSED)	Measurement	Testcase referenc e
[KPI4.2]Implement/correlate technical service configurations and SLA monitoring interactions between multiple parties	SLA measurements and validation from at least 3 operators involved in a multi-party service chain	**[KPI4.2.9] [KPI-UC3.1]** Deployment time for application components (VNFs, CNFs) < 5 mins	UC 1 UC 3	PASSED	22s - 75 s (depending on the test)	UC1.7, UC1.8, UC3.1a, UC3.1d, UC3.2c, UC3.3a, UC3.3b, UC3.4a, UC3.4b
		[KPI4.2.10] [KPI-UC3.2] Deployment time for the complete graph of CDN application < 90 mins	This KPI refers to the setup and instantiation of the centralized CDN services on the provided infrastructure, which was 5G Barcelona. Eventually, this process was done manually, and not through 5G-ZORRO components, so there was no value in calculating this KPI. Generally, these central services were created one time at the beginning of the UC3 trials and remained stable and active until the end of the project. It was the edge caches that were provided as VNF or NS offers and that were instantiated dynamically.			
		[KPI4.2.11] [KPI-UC3.3] Network Slice creation time < 3mins	UC 3	PASSED	In the range of a few seconds. In some cases it was close to, but still less than, 3 minutes	UC3.1a, UC3.4a, UC3.4b
		[KPI4.2.14] [KPI-UC3.6] Latency between Central CDN Server & Edge Server < 20ms	UC 3	PASSED	For the edge cache in 5G Barcelona: 0.3 – 1.1 ms For the edge cache in 5Tonic: 12.9 ms	UC3.1a, UC3.1d, UC3.1e, UC3.2c, UC3.4a, UC3.4b
		[KPI4.2.16] [KPI-UC3.8] Prediction of SLA breach > 5 mins before the breach occurrence	UC 3	PASSED	On true positive, the prediction is done at least 5 minutes before the actual occurrence	UC3.1b, UC3.2a
[KPI5.1] Time to process and enforce new spectrum transactions (i.e., from the moment the transaction is settled until the spectrum becomes available).	Complete new spectrum transactions in less than 10 minutes.		UC 3	PASSED	In the range of 3 and 4 minutes (slice deployment)	UC2.9b, UC2.9c
[KPI5.2] Number of transactions per second handled by the market,	20 transactions/second		UC 1	PARTIALLY PASSED	5 spectrum certificate requests/minu	UC1.4, UC1.5 UC1.11,

Applicable Technical / Business KPI (general target)	KPI Target	Specific KPI	UC	Achievement (PASSED)	Measurement	Testcase reference
which will determine the volume of spectrum transactions processed by the market.			UC 2		te and 30 spectrum certificate request decisions / minute. For Order transactions the measured rate was 0.5 transactions per second	UC1.12, UC1.14, UC1.15, UC1.16, UC2.5, UC2.7,
[KPI5.3] The authenticity of the market agents, preventing double spending that would allow an agent to trade spectrum rights that it does not own.	Verification of the built-in property of Blockchains.		UC 2	PASSED	Determined during on-boarding process	UC2.1, UC2.2, UC2.3, UC2.4
[KPI5.5] Ability to enforce the settled spectrum rights and obligations, which will build on lightweight Trusted Execution Environments (TEE) embedded in the radio access points to ensure that the reported spectrum measurements are faithful, and the spectrum allocations settled in the market are enforced.	Be able to detect spoofing attacks where a base station uses an allocation not authorized by the market.		UC 2	PARTIALLY PASSED	TEE implementation was not possible. However, performed tests show the capacity of the platform to monitor RAN telemetry associated to defined SLAs, to expose this telemetry to the datalake and to detect and correct SLA breaches.	UC2.9d, UC2.9f, UC2.9g
[KPI7.1] Lab validation environments for the three use cases.	3 lab testing environments for UC1, UC2, UC3 - suitable for TRL4 goals.		UC 1 UC 2 UC 3	PASSED	3 UCs tested on 5GBarcelona testbed	By inspection
[KPI7.2] Demonstration of the three use cases in relevant testbed at 5GBarcelona and 5TONIC	At least 1 demonstration for each of the use cases - suitable for TRL5/6 goals.	UCs to be deployed in 5GBarcelona and 5Tonic testbeds.	UC 1 UC 2 UC 3	PARTIALLY PASSED	Demonstrations for UC1 and UC3 have been done in both testbeds, UC2 demonstrations have been done in 5GBarcelona	By inspection

2.6. Automated Platform Deployment and Installation

In order to facilitate the exploitation and usage of the 5GZORRO platform, a dedicated activity targeting the platform deployment and installation automation has been set up. The objectives of the activity include, in particular:

- Definition of the modular deployment architecture that aims at organizing the platform components in a set of deployment profiles that correspond to different sets of functionality and usage of the platform.
- Definition of the target deployment platform and the physical layout underlying the platform deployment to accommodate for the above architecture.
- Provide a set of deployment scripts and configurations following the “Infrastructure as Code” paradigm for the platform provisioning.
- Ensure and, if necessary, adapt the single components to the automation process requirements.

To achieve this goal, the implementation of the automation procedure relies on a series of assumptions regarding the underlying infrastructure and the organization of the entities and stakeholders within the ecosystem:

- Kubernetes [56] is used as a platform for the deployment of various 5GZORRO components and software modules. More Kubernetes clusters may be engaged to host different parts of the platform; the deployment model of single components is agnostic to the topology of the infrastructure.
- The interaction between the components relies either on the REST APIs exposed by the different components or on the data streams implemented and managed by Kafka that is used as message bus between the different components (e.g., with the Datalake).

With respect to single components, in order to make the process completely automated, the following requirements should be satisfied:

- Compatibility with Cloud-Native Architecture paradigm and with Kubernetes using Docker containers as the way for providing the components for the deployment.
- Avoid manual configuration of the components so that all the configuration steps may be implemented as supporting administration scripts to run at the deployment phase.
- Avoid using environment-specific container configurations or implementations (e.g., no external service references – DBs, queues, endpoints - hardcoded).
- Use declarative component configurations in order to facilitate a specific deployment setup (e.g., using where possible environment variables).

It is important to note that, while for the majority of the components these requirements have been satisfied, in some cases it was necessary to change or extend the component code and/or the provided deployment configurations. The proposed changes have been integrated into the source code projects of the individual components.

The detailed information about how to deploy the platform, about the deployment configuration and different deployment scenarios, together with the deployment scripts and code, is available at the corresponding GitHub repository [15].

2.6.1. Definition of the deployment profiles

Following the use case scenarios and the platform implementation in these regards, we identify the following set of profiles that logically corresponds to the different types of the platform usage and different stakeholders involved:

- **Cross-domain platform profile**. A set of common components that are shared between all the stakeholders and are used for cross-cutting concerns and scenarios. This refers, e.g., to Datalake, communication bus, DLTs, etc.
- **Administration profile**. The profile represents the components used for the platform governance and for the tasks behind the governance activities. This includes administration ID&P, legal prose repository, etc.
- **Trader profile**. The profile represents a stakeholder that actively participate to the ecosystem offering various services and resource through marketplace. This profile uses the components that are necessary to perform the resource provisioning (Provider activities) as well as the resource consumption (Consumer activities)
- **Consumer profile**. The profile represents a stakeholder that aims at acquiring the resources. Note that while this may be designated as a separate role, no specific components are associated. Instead, it uses a subset of the components that is common to all the stakeholders, e.g., service and offering catalogue, the underlying DLT nodes, ID&P agent, etc.
- **Regulator profile**. The profile represents the regulator stakeholder and covers a subset of components to perform this role.

More detailed mapping of the components on different roles is represented in Deliverable D3.2 [16]. The deployment profiles are organized in a hierarchical manner so that the "overarching" platform profile is composed of the stakeholder profiles and each of those refers to the deployment recipes of the single components.

2.6.2. Definition of the deployment platform

Based on the above model and assumptions, the automation approach aims at providing an infrastructure creation and installation procedure at two levels: infrastructure creation and deployment of components. The separation of the two levels is fundamental from the portability point of view; it is sufficient to adapt the infrastructure creation scripts to a new type of infrastructure without affecting the component deployment (apart from the configuration parameters).

Infrastructure creation. For what concerns the infrastructure creation, Kubernetes has been selected as the primary target platform of the deployment, for its scalability, portability, and management capabilities. When this was not possible, the component installation has been achieved with the apps containerized on top of the standalone Virtual Machines (VMs). More specifically, the infrastructure creation is achieved as follows:

- Terraform [17] scripts are used to create the necessary underlying infrastructure and activate Kubernetes cluster(s) on top of it. To facilitate the experimentation, MS Azure Cloud infrastructure has been used.
- In these settings the Terraform scripts initiates the creation of the required node pool for the cluster, activates the Azure Kubernetes Service, creates necessary additional VMs, set's up the network and Internet configuration of the cluster to facilitate the access to the platform from outside.

While there are different deployment scenarios possible, the one used for the nominal case (also presented in the figure below) makes the following assumptions:

- A single Kubernetes cluster is used for all the deployment, for cross-domain profile and for different stakeholders. The isolation is achieved with the different Kubernetes namespaces.
- Where possible, a single database cluster is used (e.g., for PostgreSQL, for Mongo DB). The database isolation is achieved through the corresponding security mechanisms and database isolation within the cluster.
- All the components of different stakeholders that should be exposed externally, are made available through a common domain, where different stakeholders have their own domain name of a higher level.

Please note, that these assumptions are not strictly mandatory; their usage is only for the nominal case in order to facilitate the basic deployment. It is possible to organize the infrastructure in a different manner and the parametrization is achieved through the individual component configuration. The following figure demonstrates the nominal deployment architecture.

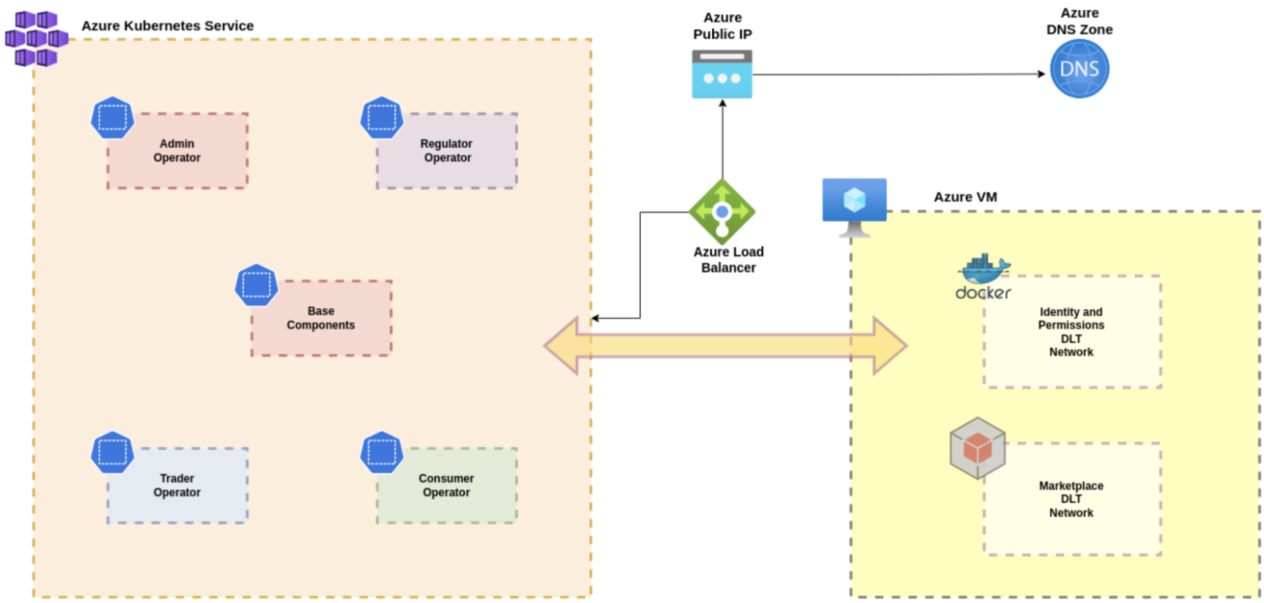


Figure 82: Nominal deployment architecture with the automation deployment procedure

Component deployment. For what concerns the component deployment, the configuration of the platform is mainly defined with the Helm chart [70] that composes the underlying component profiles. For most of the components the implementation has been performed in a way that the component can run in Kubernetes, providing the Docker container definitions, and in some cases Helm charts or other Kubernetes deployment scripts. For the purpose of automation, within the presented task the following activities have been performed:

- If necessary, adjust the implementation to adhere to the component automation requirements. The manual configurations procedures have been replaced with the automated scripts and all the configuration properties have been made explicit and moved to the deployment configuration values.
- When not provided, the definition of Docker image configurations for the component to be deployed in container.
- When not provided, the definition of the Helm chart for the deployment of the component on Kubernetes.

- Adjust the Helm charts in order to support more flexible way of deployment (in a nominal architecture, but also under hypothesis of distributed and parameterized version).

While in most cases it was possible to achieve the Kubernetes-based deployment, for some components this was not possible. More specifically, the two DLTs (VON Network and Corda Network with the Smart Contracts) required a separate installation based on conventional Virtual Machines. One of the reasons for this choice is the incompatibility of the currently used underlying technology (e.g., Blockchain Automation Framework, BAF) with the Kubernetes versions supported by MS Azure. In this case, the automation of the deployment is achieved directly with the Ansible scripts that trigger the infrastructure and the components deployment.

Deployment configuration. The configuration of the deployment process relies on two types of inputs: (i) definition of the deployed profiles to be activated and (ii) configuration of individual profiles and components. As for the deployed profiles, it is necessary to specify which profile should be deployed (admin, regulator, etc). This applies both for the Helm-based deployment (for the platform components) and for the VM-based deployment (for DLT nodes).

As for the configuration, it is important to note that most of the configurations are pre-predefined, given the network and component dependencies. The properties that should be configured explicitly include:

- Naming of the stakeholder components as those are critical for the component communications (e.g., endpoints, databases, etc);
- Properties related to the external access to the platform: information about the domain name, domain server management, subdomains, SSL certificates provisioning, etc.

It is important to note, that the deployment information, configuration files, are available as a part of the corresponding automation process repository. The deployment relies on a shared Docker image repository, where all the component images are made available by the corresponding partners.

2.6.3. Dynamic bootstrapping of a new operator and integration with the ecosystem

The nominal deployment scenario described in the previous subsection assumes that the set of the operators is pre-defined at the moment of the overall platform deployment. An important scenario that the platform should implement refers to the case when a new operator wants to join the ecosystem and is going to deploy a subset of the components relevant for his operations in a way they are integrated with the rest of the platform.

Given the overall architecture of the platform, the creation of the infrastructure for the new operator amounts to:

- Preparation of the operator profile configurations to be appropriately connected to the cross-domain platform components (e.g., Datalake, Kafka, etc).
- Deployment of the corresponding profile components on a Kubernetes infrastructure. It is possible for the operator to have its own Kubernetes cluster, deployed on premise or in Cloud and managed separately.
- Deployment of the marketplace DLT node used by the operator and connected to the rest of the network.

The detailed information about the procedure for the deployment of a standalone operator is available on the GitHub repository [15].

2.7. Enabling the Global Operator Model with 5GZORRO

Recently, we have been witnessing a sharp increase in the demand for connecting extremely heterogeneous terminals that operate globally in different environments around the world, with varying performance requirements. This surging demand in global/ubiquitous cellular connectivity comes both from the massive number of connected IoT devices as well as from people who are progressively switching (together with all their devices) to a digital nomad lifestyle. The rise of a large, new group of traveling, remote workers is one of the prevailing side-effects of the COVID19-impacted work world. This growing digital nomad community across the globe is fuelling the demand for international seamless connectivity. Support for things roaming globally is now critical for IoT vertical applications, from connected cars to smart meters.

The “Global SIM” is now a product that individuals and IoT companies demand, and it is being satisfied by a new breed of providers of mobile communications, the Mobile Network Aggregators (MNA). Similarly to MVNOs, MNAs rely on the infrastructure of MNOs to provide services, marketing themselves as “Global Operators”. Instead of relying on a single base MNO, MNAs multiplex their clients across multiple MNOs in order to ensure optimal service and sustained quality of experience (QoE), without the added cost of operating the network.

Roaming and the associated ecosystem are essential pillars that support MNAs’ operations in multiple countries, without the need of finding a local communication provider in every country where their end-users operate. MNAs benefit from the extensive global network infrastructure that international carriers (e.g., incumbent tier-one operators such as Vodafone, Tata, Telefonica, or Orange) have been shaping for the past decades.

The emerging MNA model is appealing to the Internet companies, which now crossed into the telco world, such as Google's Fi Project [58]. Furthermore, cloud communication platforms as a service (CPaaS) such as Twilio [59] or EMnify [60] provide MNA services by aggregating networks at the international level, thus aiming for global service, and making connectivity available through simple interfaces to application and service developers world-wide.

2.7.1. Taxonomy and limitations of the current operator models

There are several types of mobile operators with different operation models available in the market today; we capture these configurations in Figure 833.

@HOME	**Traditional MNO**	**Light MVNO**	**Full MNVO**	**Light MNA**	**Full MNA**
Sales	MNO	Light MVNO	Full MNVO	Light MNA	Full MNA
Core	MNO	Base MNO	Full MNVO	Base MNO	Full MNA
Radio	MNO	Base MNO	Base MNO	Base MNO	Base MNO

Figure 83: Types of MNOs

An MNO is an entity that owns (or has the exploitation rights) of a cellular network (i.e., base stations, network core, spectrum, etc). This was the initial operation model deployed to provide mobile communication services. Examples of MNOs include Vodafone, Orange, O2, AT&T, NTT to name a few.

Later on, the MVNO operation model emerged. Specifically, the MVNO is an entity that offers mobile network services to end-users, but does not own nor operate fully a cellular network. The MVNO is defined by its lack of ownership of radio spectrum resources.

In order to operate, an MVNO needs to have agreements in place to access the network of a base MNO. The implementation of the MVNO varies, and thus there are many different types on MVNOs. The type of MVNO is determined by how "thick" or "thin" a technological layer the MVNO adds over its access to its base MNO's network.

A *light* MVNO is a service provider that has its own customer support, marketing, sales and distribution operations, and may have the ability to set its tariffs independently from the retail prices of the base MNO. One such example is giffgaff [61] in the UK, which uses O2 UK as a base MNO. A *full* MVNO has a core network implementation operating essentially the same technology as an MNO, only missing their own radio network. They thus run their own core network, and rely on a base MNO who can offer access to radio resources. One example is Sky Mobile, which operates as a full MVNO in the UK, using O2 UK as a base operator.

Much more recently, we have witnessed the emergence of a new type of MVNO, namely the MNA. While "traditional" MVNOs have agreements with a single base MNO, an MNA is an MVNO that exploits more than one base MNO, either in one single economy, or across different economies. Examples of MNAs include Google Fi, Truphone [62], Twilio or Lycamobile [63]. Aggregating multiple base MNOs allows the MNA's customers to dynamically change the base MNO to which they attach. This change of base MNOs depends on different factors, including policy, coverage or performance.

We further classify MNAs into *full* MNAs or *light* MNAs , depending on whether they operate their own core network or not. We also differentiate the MNAs based on the geographic coverage of the multiple base MNOs they aggregate. In the general case, the base MNOs aggregated can cover the same or different geographic regions. A particular case is when the different base MNOs aggregated provide coverage in different geographic regions that do not overlap, notably different economies. If this is the case, we call this specific type of MNA a multi-country MVNO. These multi-country MVNOs usually have commercial offers in each of the different economies where they operate.

We acknowledge that, as in most taxonomies, there are corner cases that we cannot neatly classify into one of the categories. In our case, there is the case where a full MVNO has a commercial agreement with one or several IP Packet Exchange (IPX) Provider (IPX-P), and does not depend on a specific base MNO (e.g., the MVNO might use global IMSI ranges). In this case, with a single agreement, the MVNO has "direct" access to several base MNOs located in different economies, depending on the footprint of the IPX-P. This configuration lies somewhere between the full MNA and the full MVNO, since it has a single agreement but connects to multiple base MNOs. We call this the "Global Mobile Network Operator (GMNO)" model, which currently depends on the IPX-P. In this section, we argue that, leveraging the 5GZORRO framework, we can extend the Global Operator model to integrate the Marketplace functionalities within the operator. This brings back control to the Global Operator on the end-user performance and SLA-compliance towards its customers.

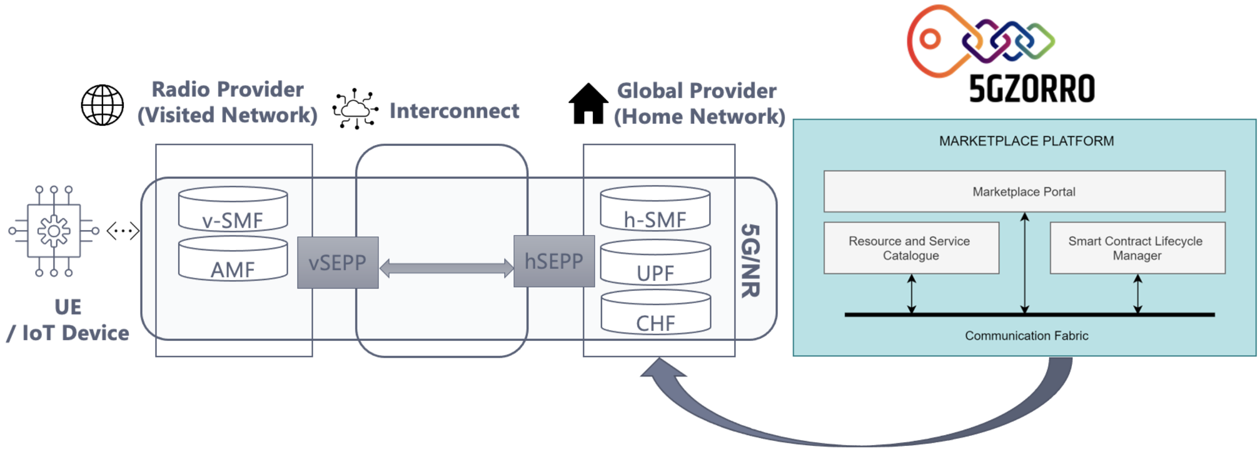


Figure 84. Integration of 5GZORRO platform with the Global Operator model.

2.7.2. Global Operator requirements and mapping to the 5GZORRO Framework

The existing operational models of MNAs rely on pre-negotiated bilateral agreements with some operators in some of the countries where they operate (e.g., this is the case of Truphone). In some cases, the global operator relies on the IPX-P (i.e., the international carrier) to obtain access to radio resources world-wide, and establish its global footprint (e.g., this is the case of Twilio). MNOs usually deploy the home-routed roaming (HR) configuration for international roaming. This configuration results in an added latency penalty for the end-user, especially when the other end of the communication is located topologically close to the visited location of the roaming device (i.e., this implies a hairpin data path from the visited country to the home country where the MNO hosts its core network and then back to the visited country, where the device operates, and the application server resides as well). We observe a similar behaviour for some MNAs currently commercially active. The difference, however, comes from the capability of the MNA to change their base MNO (nationally and internationally), thus implicitly also changing their "home" location as well (in the case of the light MNAs).

The Global Operator model we present next is uniquely enabled by the 5GZORRO framework, and registers as a stakeholder within the Marketplace Platform, which then also allows it to use its unique smart contracts management platform. We argue that 5GZORRO meets the main requirements of the global operator model and tackles some of the current major limitations of existing MNA models.

In this section, we detail the Global Operator model requirements that we have identified, and show how the 5GZORRO framework responds to each requirement. Figure 85 gives an overview of the Global Operator architecture, which depends on the existing infrastructure of operators and cloud providers. Unlike existing operating models, the main idea is that the global operator runs its own core network, and dynamically moves the UPF to ensure the performance requirements of its end-users (and tackle the latency penalty of home-routed roaming).

Furthermore, instead of relying solely on a single base MNO (like other MVNOs or MNAs), the global operator aggregates the radio resources on multiple operators within the same country, where its end-user devices operate.

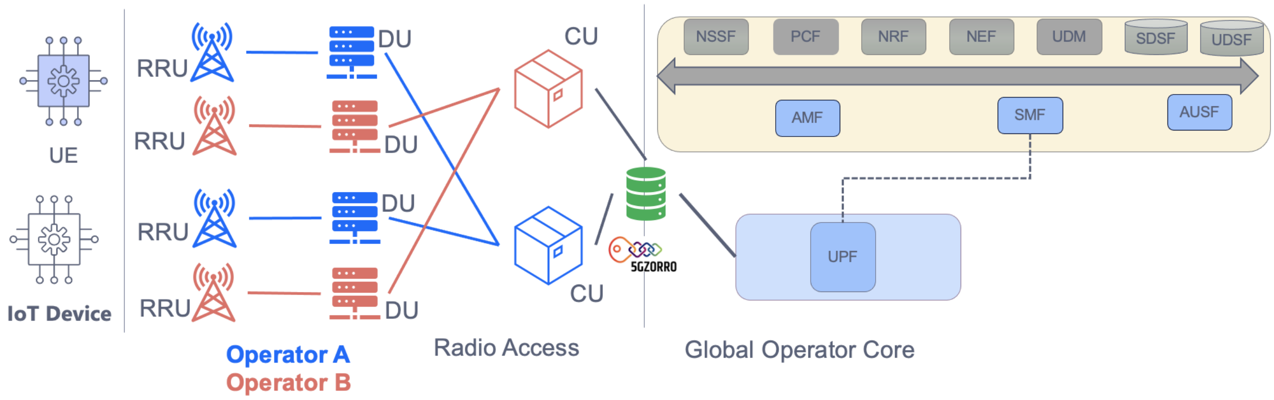


Figure 85: Global Operator architecture enabled by 5GZORRO

The following requirements are identified for the Global Operator:

- The Global Operator requires a dynamic approach to interconnection with multiple base operators, whose radio resources it needs in each country where it operates.
    - Leveraging the 5GZORRO framework, the global operator can use the smart contract lifecycle manager to attain the dynamics in terms of legal agreements with base operators in every country where it operates
- The global operator must aggregate radio resources from multiple incumbent operators within the country where its devices operate.
    - Using the 5GZORRO framework, the global operator can register as a stakeholder in the 5GZORRO Marketplace within each country where its devices operate (where we assume the Marketplace is also available), from where it can see resource offers from all available providers and bid on them.
- The global operator should run its own core network (typically, in a single country, while leveraging local infrastructure), and leverage 5G Control and User Plane Separation (CUPS) to move the UPF closer to the end-user devices in order to tackle the performance requirements of its customers. The global operator should rely on location-driven resources discovery, and ensure the best performance for the end-user devices
    - The 5GZORRO Marketplace allows access not only to radio providers, but also cloud infrastructure providers; thus, the global operator can use these to deploy its UPF within the country where its devices operate, avoiding home-routed roaming.

2.7.3. Components and Configuration

The 5GZORRO-enabled Global Operator extends the 5GZORRO platform internationally, to cover resources in different countries. We envision two different approaches for 5GZORRO global coverage: (i) per-country 5GZORRO Marketplace instance, where in the Marketplace portal the stakeholder can select the country where to access resources; or (ii) International 5GZORRO Marketplace with coordination.

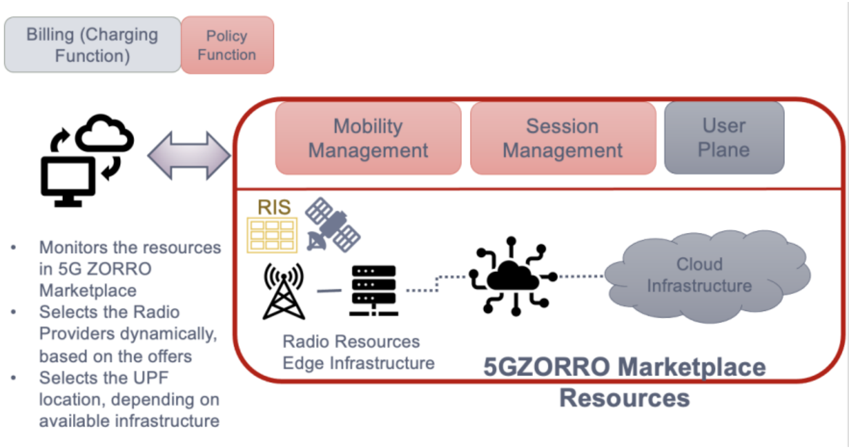


Figure 86: Overview of the Global Operator integration with 5GZORRO

2.7.3.1. Per-country 5GZORRO Marketplace instances

The Global Operator registers as stakeholder within each national 5GZORRO Marketplace, thus also obtaining an MCCMNC to operate as entity within the associated national market. In other words, the global operator would become an MNA within each country, aggregating the radio resources of different operators that own radio resources within the national market. This interaction would be easily verifiable by the corresponding regulator entity.

To show the benefit of aggregating radio resources from multiple radio network providers, we leverage a large-scale nation-wide crowdsourced measurements campaign that capture coverage (signal strength parameters for 4G/LTE) with the UK for all available operators (namely, Virgin Media O2 UK, EE, Vodafone and Three UK). The dataset we use (which is not public and thus cannot be referenced) spans a period of 90 days and includes measurements from operational end-user devices (smartphones). We argue that the coverage improvement is a proxy for improved reliability of connection, which is required in the case of specific IoT verticals (e.g., smart energy meters, fleet tracking).

Challenges (for future work): The GMNO requires fast inter-operator handover. To enable this, we require a device identity that each MNOs within the marketplace can use for authenticating the end-user. We can enable eSIM profile swap for the end-user when connecting to a new radio provider. Alternatively, we leave for future work the design of a unique identity provider that is recognized by all resources providers within the ecosystem.

Table 36: Global Operator deployment using 5GZORRO Platform

	Global Operator Model
Description	We build a Global Operator (GMNO) using the 5GZORRO framework, assuming an extended Marketplace, with instances in the different economies where the GMNO's customers operate. The GMNO runs its own core network, and relies on at least one IPX-P for international carrier services. Leveraging 5GZORRO, the GMNO can rent radio resources from any provider, based on geo-location and performance requirements.
Key Use-case requirements and KPIs	• The GMNO requires a dynamic approach to interconnection with multiple base operators, whose radio resources it rents in each economy where it operates. The SCLCM allows for dynamic settling of legal contracts between the GMNO and the resource providers. • Using eSIM technology, the GMNO installs in the local devices new profiles corresponding to the radio providers whose resources it rents.

	• The GMNO monitors the performance of the established connectivity via the 5GZORRO Datalake, and leverages the SLA breach detection service to trigger a handover to a different resource provider that can ensure meeting the customer SLA.	
Components and Configuration	Components	• Smart Contract Life-Cycle Manager (SCLCM) • Marketplace Portal and resources catalog • Monitoring data aggregator (MDA) • Datalake • SLA Breach detection service • Trust and Reputation Management Framework (TRMF) • Radio Resource Controller (rRM) • Intelligent Slice and Service Manager (ISSM) • Network Slice and Service Orchestrator (NSSO)
	Configuration	• The stakeholders within 5GZORRO that offer radio resources are eSIM-compatible, and can offer a profile to be installed within the end-user device connecting via the GMNO. • The GMNO's UPF can be deployed on cloud/edge infrastructure available through the 5GZORRO Marketplace.
Test Procedure	Pre-conditions	• The 5GZORRO framework covers resources across international markets, following either (i) per-economy instantiation, where the available resources are confined within the geo-political border of a specific economy or (ii) international centralized approach, where the location of the resources overpasses the limits of specific borders of a specific economy.
	Test Case steps	1. In the case of the per-economy instantiation of the 5GZORRO Marketplace, we measure the benefit in terms of reliability and improved coverage that aggregating multiple radio resource providers can offer to the GMNO's end-users. 2. In the case of the International 5GZORRO Marketplace, we measure the benefit of placing the UPF in a location that would ensure reduced end-to-end latency between the end-user and the application server.
Measurements	Methodology	The measurements are extracted from end-user specific metrics.
	Complementary measurements	Monitoring metrics: • Connection reliability improvement through radio resource aggregation • eSIM profile swap latency • Inter-operator handover latency • End-to-end latency reduction via UPF placement optimization.
	Calculation process	1. For the per-economy instantiation of the 5GZORRO Marketplace, our goal is to show that there are significant benefits for the end-user by aggregating radio resources from different providers within the same economy and given the same geo-location. For this, we rely on crowdsourced signal strength measurements for all mobile operators that own radio infrastructure within the UK. 2. For the international 5GZORRO Marketplace, we use AWS infrastructure to test the UFP placement with respect to specific locations of the end-user and the target application server.
Result	For the two use cases we present, we started doing some initial measurement validation in order to quantify the benefit of the global operator renting resources from different providers. We focused on performance metrics, such as delay or radio coverage improvements. We report the initial results in more detail in Sections 2.7.3.1 and 2.7.3.2.	

2.7.3.2. International 5GZORRO Marketplace

The Global Operator registers as stakeholder within the Marketplace with a shared mobile code similar to 901, which the ITU currently reserves for global networks which surpass the political and national borders, such as satellite networks (e.g., Inmarsat) or off-aircraft communication providers (e.g., Aeromobile/Telenor).

Using the unique 5GZORRO platform, a global operator can easily access radio resources globally (across different economies) and manage smart contracts with providers world-wide. Within the International 5GZORRO Marketplace, the global operator can access multitude type of resources, including satellite or off-aircraft radio antennae, edge or cloud compute resources, regardless of their country-level locations. In other words, it can use radio resources located in a specific economy, but leverage cloud resources from another economy to host the UPF, depending on the location of the application server of the vertical in question.

Under this scenario, the GMNO can optimize the placement of the UPF in order to minimize the end-to-end latency from the end-user devices to the application server (which, in a global deployment scenario, might be in a different economy than the end-user device).

We utilise the edge (wavelength), local and regional deployments of Amazon global infrastructure to deploy control and user plane functions of open-source 5G implementations (namely, Open5GS [64] and UERANSIM [71]).

Infrastructure. The setup we build aims to emulate different roaming configurations. For this, we rely on the global infrastructure including both storage and compute services that AWS offers. This includes:

- a *regional* infrastructure with data centres deployed in a region (e.g., US East/Ohio region). Within this deployment, a cluster of isolated and physically separated data centres are found in a geographical area.
- a *local* infrastructure hosted as an extension of regional infrastructure to run latency sensitive and high bandwidth applications. For example, Netflix uses AWS local zone deployments for their content creation process.
- an *edge* infrastructure hosted within telecommunications providers' data centres and connected to the operator's 5G network. We consider this as first point a user can breakout to the Internet from MNOs network.

We show in Figure 877 the experimental setup we use in order to test the benefits of moving the UPF closer to the end-user, in the visited country where they actually connect. This setup is meant to mimic the operations of a global operator that runs its core in one country but deploys services all over the world. We show that by using 5G CUPS, the provider is able to offer better performance to its end-users. This proof of concept only relies on one cloud infrastructure provider (AWS). We argue that the global operator would benefit greatly from renting resources across different cloud providers, as well as from different radio network providers. We argue that managing this is possible using 5GZORRO. The framework allows the global operator to rent resources in different markets from different providers.

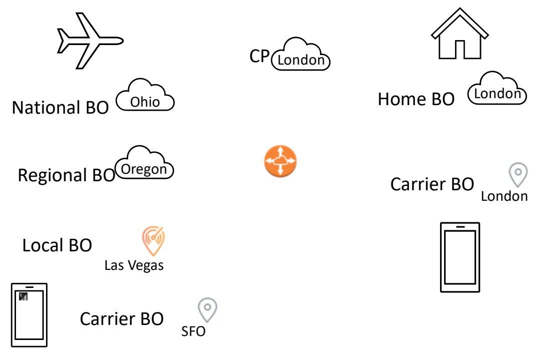


Figure 87. Experimental Setup for testing the UPF placement closer to the end-user, in the visited country

Table 37: Locations of deployed UPF and DNN names as identified by the UEs to breakout at a visited location (namely, US or Germany)

	UK		US				EU (Germany)	
Breakout Type	Home (London	Edge (Vodafone)	Edge (Verizon)	Local (Las Vegas)	Regional (Oregon)	National (Ohio)	Edge (Vodafone)	Regional (Frankfurt)
DNN	edge.london	home	edge.sfo	local.las	regional.or	national.oh	edge.ber	edge.fra

Connectivity. For our pilot deployment, we assume an end-user with 5G connectivity who has their network home location in the UK. To emulate the user roaming behaviour, we test two different scenarios, where the user roams in two locations: (i) in the US (San Francisco) and (ii) within Europe (Berlin, Germany). With current 4G/LTE technologies, the default roaming configuration would be HR roaming, where the traffic is routed back to the UK. We argue that, by using 5G CUPS at the core, we can keep the control plane functions in the trusted, centralized home network location, while dynamically moving the user plane function with the roaming user. We handle this connectivity by deploying control and user planes built using Open5GS [64]. We deploy the control plane, which includes Session Management Function (SMF) and Access and Mobility Management Function (AMF), at the regional infrastructure in the user's home location (London, UK). The user plane enables breakout to the internet, and hence we deploy it across multiple locations in the US and EU (as per Table 37). The selection of UPF to breakout is chosen by the DNN setting in the 5G UE. We use UERANSIM to deploy a simulated environment of 5G RAN and 5G UE in the edge infrastructure.

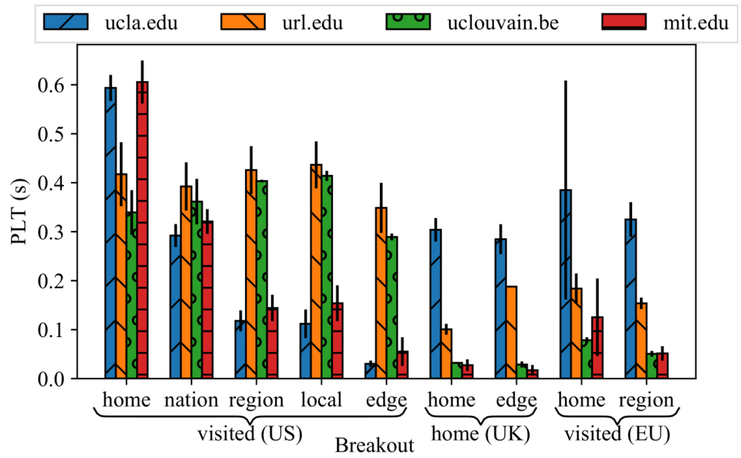


Figure 88. Page load time to different websites in function of the breakout point considered for the roaming configuration

Results. In order to capture the end-user performance under the scenarios we include in Table 37 we measure web performance. We focus on the web page load time (PLT) as the representative metric. We use as target four websites, namely, www.ucla.edu in the US, www.uclouvain.be in Belgium, www.url.edu in Spain and www.mit.edu, which is served by a CDN. We show our results in Figure 88. We use as a baseline the measurements for the non-roaming scenario (marked “home (UK)” in Figure 88). The goal of our measurements analysis is to establish which roaming configuration can offer the same performance that the end-use enjoys while at home. We find than when content is served by a CDN, the regional breakout configuration offers comparable performance to the no-roaming scenario, regardless of the location where the end-user travels (e.g., US or Germany, in our case). This is a direct consequence of the close location of the content replica to the end user, which is dictated by the location of the breakout point. From the case of end-user roaming in the US, we see that the local breakout configuration yields similar performance to regional breakout, likely as a result of the small distance between the locations of the infrastructures used in this scenario.

When a CDN is not serving the web content, the distance between the location of the end-user breakout point and the content location impacts the web performance. For example, if edge breakout in San Francisco offers the optimal performance for accessing content hosted in California (ucla.edu), we see this is no longer the case when accessing content hosted in Europe (uclouvain.be, url.edu). The PLT we measure in this latter case is, in fact, similar to the one we measure under the HR roaming configuration. The same is true for accessing US-based content from Germany, under the regional breakout configuration. Surprisingly, however, we find that the PLT for Europe-hosted web content is slightly smaller in the US (San Francisco) edge breakout scenario than all of the other configurations (local/regional/national/home breakout). We conjecture that this is a side-effect of relying on the carrier’s infrastructure (i.e., Verizon), while for the other configurations the AWS private backbone impacts the delays between the various instances.

Challenges (for future work): 5GZORRO to enable global billing: we would need to enable payments in every economy using a single currency (i.e., enable payments to the resource owners via popular cryptocurrencies such at bitcoin or ether, regardless of their geo-location and established fiat currency).

2.7.4. Example use-cases of the GMNO

2.7.4.1. Energy Smart Meters.

Smart Grid applications have received increasing attention in the past years, with regulation pushing for mandatory deployment of metering devices in consumer premises. Specifically, the UK Government is committed to ensure that every home and small business in the country is offered a smart meter as part of the Smart Metering Implementation Programme (SMIP). Though these devices are inherently stationary (they do not change location), their connectivity proves challenging at times, with many end-users reporting issues with their devices. In order to answer to these challenges, the UK regulator decided to back the Data Communication Company (DCC) as the single, secure, smart metering network in the UK. The DCC is a licensed monopoly and non-profit organisation in charge of rolling out the smart meter network in Britain.

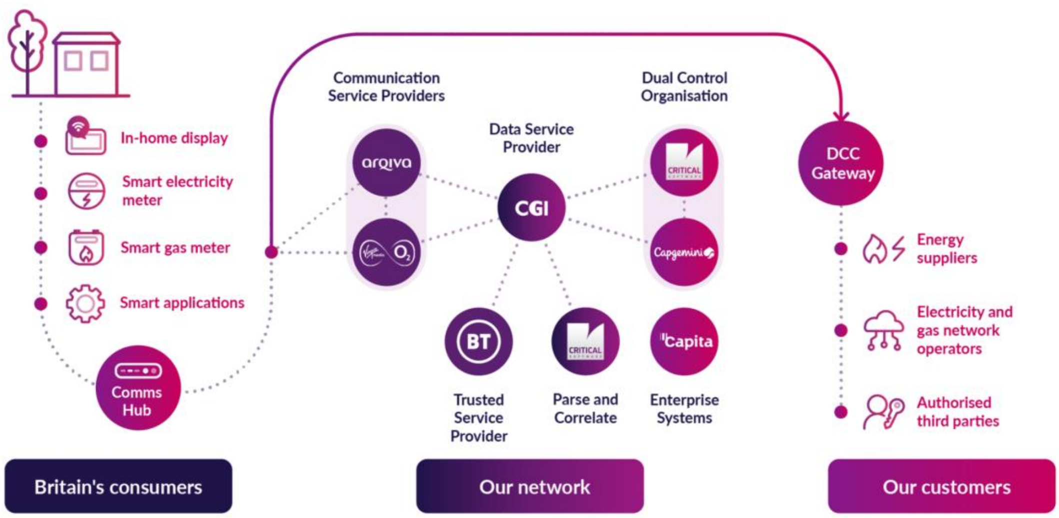


Figure 89: EXAMPLE: The DCC Network for Smart Meters in the UK. Source: [65]

The operator aggregates at the national level resources from two radio providers (satellite and mobile towers), and focuses on providing increased security for the communication between consumers and energy suppliers. We argue that we can enable a similar model using 5GZORRO. Moreover, the use of DLT allows for easy auditing and price control, as required by the regulator. This would be an immediate application of the global operator model enabled by the per-country 5GZORRO Marketplace configuration.

2.7.4.2. Global Shipment Company.

This IoT vertical specializes in moving freight across Europe, including maritime and inland shipping, with real time tracking of freight data, smart containers, and IoT tracking solutions made possible via the IoT connectivity by the global operator. One such example of global operator is Marlink, which offers managed connectivity to MSC Mediterranean Shipping Company, the world's largest container line [29].

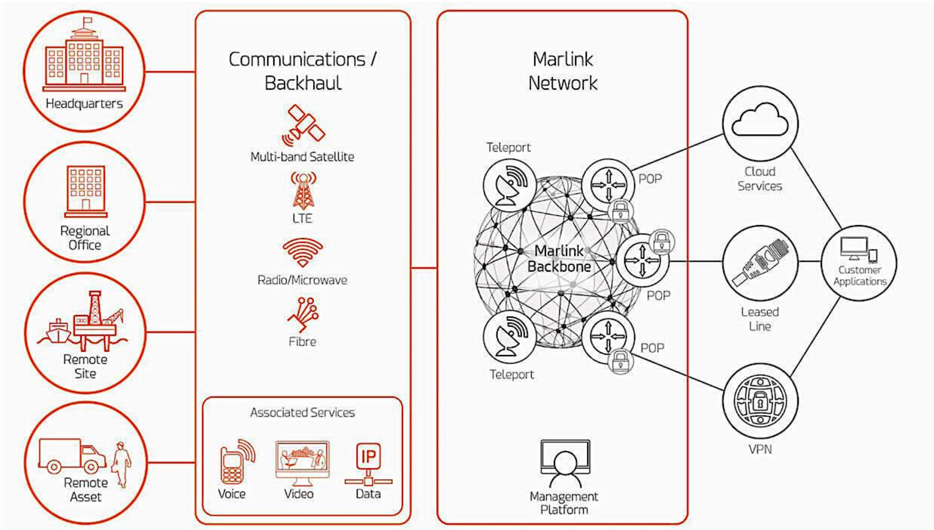


Figure 90: Example: Marlink's Intelligent Hybrid Network. Source: [66]

Marlink is an example of global operator focused on connecting people and assets around the globe and across all markets where conventional connectivity cannot reach or is not available. The operator aggregates satellite, LTE, radio/microwave and fibre communication resources to connect various IoT verticals with their customer applications.

We argue that 5GZORRO can enable a similar model of operating, which would be a direct application of the international 5GZORRO Marketplace. However, this approach is currently limited, as we would also need to enable a billing framework that enables global charging of the end-users.

3. Legal Validation

The purpose of the legal validation analysis is to identify the contextual relationship between the 5GZORRO Marketplace and the legal obligations which may be relevant or necessitate compliance with by any such marketplace stakeholder.

It is not the scope of this analysis to take a generalised view of the marketplace as a business which, naturally, would require compliance with all the aspects related to running such an endeavour, including laws concerning trade, tax, employment and so forth. Rather, this analysis looks at the regulatory ramifications arising from the interplay in the application of innovative technologies, such as artificial intelligence and distributed ledgers within a digital marketplace that deals with electronic communications services and frequency spectrum. This analysis has also been limited to the EU market and hence focuses on regulations emanating from EU law.

Regulation evolves with the pace of technological innovation. As of lately, policy makers have been busy addressing the now commonplace use of AI, the application of distributed ledgers within digital markets dealing with crypto assets and the prevalence of digital platforms as information gate keepers, as well as new rights and obligations in relation to data access and use. At an EU level, various proposals calling for compliance on these fronts are in the process of or have recently been enacted as legislative instruments. Decades long regulation focusing on the allocation and management of frequency spectrum and the oversight of electronic communications providers has been updated to reflect new market realities, along with regulations calling for increased security oversight to safeguard the functioning of society and the economy. The ensuing analysis will delve into each of these aspects.

3.1. 5GZORRO and the digital marketplace

At EU level, the principal regulatory developments related to digital and online marketplaces relates to the Digital Services (DSA) and Digital Markets Acts (DMA) [35] and the Platform to Business regulation (P2B) [36]. Together, these packages establish a comprehensive set of rules for all digital services, spanning social media, online marketplaces and other online platforms operating in the EU. The DMA aims at addressing unfair market practices or barriers to competition, the DSA focuses on aspects concerning illegal and harmful content and the ensuing obligations of online platforms, whereas the P2B regulation seeks to establish a fair market for businesses which use online platforms to serve consumers.

All three regulations referenced in the previous paragraph carefully define their addressees and provide for various exemptions. Of relevance are exemptions in relation to the size of the business, where small and micro businesses are largely exempted, and the definition of online intermediation service providers as providers of services to consumers outside of their trade activities. In this regard, it can be argued that the marketplace established by 5GZORRO falls outside of the scope of these regulations due to its scope and nature.

3.2. 5GZORRO and AI

5GZORRO's use of distributed artificial intelligence to implement cognitive network orchestration and management merits a brief discussion on developments in relation to AI regulation. Various proposals are in the works to regulate different facets related to the use of Artificial Intelligence in high-risk settings, liability rules, as well as prohibitions [37]. An initial analysis of the proposed obligations indicates that the 5GZORRO Marketplace operator would not be subject to regulations meant to address high-risk activities as the platform's functionality falls outside of their current scope.

Trust and reputation management techniques applied to natural persons are also subject to these proposed regulations, with prohibitions and limits when applied to natural persons. This aspect would also fall outside of the 5GZORRO context as the platform is meant to serve business and enterprise.

3.3. 5GZORRO and blockchain

Distributed Ledger Technology (DLT) underpins key 5GZORRO functionality, including that enabling distributed security and trust, the digitisation of spectrum licences and smart contract functionality. The increasing use of DLTs and blockchain within financial markets and beyond has instigated EU policy makers to seek legal certainty and to establish a clear regulatory regime in areas pertaining to blockchain-based applications. Outside of financial markets, the principal development relates to the proposed Markets in Crypto-Assets Regulation (MiCA) where crypto-assets are defined as the “digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology” [38].

5GZORRO’s approach to digitising a spectrum certificate, to create spectrum tokens or ‘spectokens’ and the trading/leasing of such assets between marketplace stakeholders suggests that scrutiny should be placed on this evolving regulatory landscape. Nonetheless, the choice of a non-fungible approach to digitising spectrum assets (NFT) currently exempts the 5GZORRO Marketplace from this proposed regulation, which “does not apply to crypto-assets that are unique and not fungible with other crypto-assets, whose value is attributable to each crypto-asset’s unique characteristics and the utility it gives to the token holder”.

3.4. 5GZORRO and smart contracts

Within the 5GZORRO Marketplace, two or more stakeholders can trade, set-up and operate a new technical and commercial relationship via a Smart Contract, hence enabling third-party resource leasing and enforcing service-level agreements.

The use of smart contracts to enforce rules enables a high-level of automation and is the cornerstone of the 5GZORRO zero-touch functionality. Notably, the absence of general directives or provisions at EU level [39] that establish clear rules for smart contracts may pose a risk to the 5GZORRO stakeholders when seeking to acknowledge the legally binding effects of smart contracts or when seeking protection from contracting parties in cases of foreclosure. The lack of harmonisation across EU Member States in this regard gives rise to legal uncertainty in cases of cross border contracts.

The recent move by EU policy makers to propose regulating data access and use [40] puts forward various requirements which are specific to data-sharing smart contracts, including the need for robustness, safe termination, data archiving and access control. The Data Act also establishes the need for smart contracts meeting harmonised standards. Such proposed measures may be viewed as a precursor to wider legal instruments seeking to establish legal certainty in the use of smart contracts across the EU. Beyond smart contracts, the proposal principally focuses on the rights and obligations in relation to data access and use when this is the result of a product or related service transaction. The current text may suggest that the 5GZORRO platform falls within the scope of this regulation and could be subject to its obligations. 5GZORRO’s contribution to the standardisation landscape and to the work being undertaken within ETSI to establish a specification for smart contracts (as reported in D6.3 [69]), is therefore of high relevance.

3.5. 5GZORRO and security

The onset of 5G has given rise to significant regulatory activity on security fronts. At an EU level, a recommendation on the cybersecurity of 5G networks [41] has resulted in the proliferation of legal instruments across EU member states to specifically address the security of the 5G ecosystem. Guidelines on security measures and a 5G supplement were also published by the EU agency for cybersecurity [42]**¡Error! No se encuentra el origen de la referencia.**. Measures addressing the security of 5G are wide ranging and require mobile network operators to, amongst others, implement strategic measures focusing on risk-management practices as well as technical measures such as the security of the supply chain, access management and control, software management and vendor diversification.

Security is a central theme within the 5GZORRO architecture and has led to notable results across architecture and software development, published papers and contributions to standardisation activities within the ETSI Zero-touch network and Service Management (ZSM) standardisation group. A prospective 5GZORRO Marketplace operator will however need to follow closely the rapidly evolving regulatory landscape in relation to cybersecurity legislation and ensure compliance. Whilst such legal obligations cannot be dismissed as minor in nature, the operational design of the 5GZORRO Marketplace posits that the platform's administrator is a mobile network operator. Familiarity with and capacity to meet the relevant legal obligations is hence highly likely.

3.6. 5GZORRO and radio spectrum

In December 2018 the EU adopted new telecom rules aimed at modernising the European regulatory framework for electronic communications [43]. The provision of electronic communications networks and services remains subject to various regulatory obligations. In this regard, the 5GZORRO platform cannot be considered as an electronic communications network or service provider, as the network components and services exchanged through the platform are being provided by MNOs, who themselves are subject to this regulation.

These rules also place renewed emphasis on the shared use of radio spectrum alongside traditional approaches where spectrum is not shared but is granted through individual and exclusive rights of use. The latter approach provides regulatory guarantees against interference at the expense of spectrum efficiency, which can however be mitigated through the trading or leasing of assigned but unused or underutilised spectrum.

In the pursuit of an optimal balancing act between spectrum efficiency and effective use, collaboration in research and development projects which explore innovative and dynamic spectrum solutions, including those enabled by artificial intelligence and blockchain technologies is necessary [44]**¡Error! No se encuentra el origen de la referencia.**. The 5GZORRO Marketplace, where platform stakeholders can trade/lease spectrum resources in real time and meeting dynamic requirements for frequency range, place and time, has been designed from the outset with such objective, whilst ensuring a high level of compliance in relation to spectrum regulation. It envisions a diverse set of platform participants comprising spectrum resource providers (MNOs) and spectrum resource consumers (other MNOs or verticals) trading resources. Within this context, the presence of the regulator, as an active participant on the platform was foreseen to ensure compliance on various fronts.

The allocation of, trading or leasing of individual rights of use of radio spectrum necessitates regulatory oversight to ensure that the obligations emanating from the spectrum licence are observed. The related processes enabled by 5GZORRO were appropriately modelled to capture and digitise relevant features of the spectrum licence. These are in turn used to create a spectrum certificate from which a Primitive spectoken with the relevant attributes is derived. Traded resources are captured within a smart contract and allocated on the basis of spectokens derived (Derivative spectokens) and intrinsically linked to their primitive.

The resource management architecture employed by 5GZORRO also ensures that spectrum resources are allocated with the intent of minimising interference, resolving location and time of use conflicts by design. Such an approach supports the principles of shared and efficient use of generally authorised spectrum and contributes to the advancement of allocation models based on coordinated use such as the 'club use' model.

Various stages require the explicit approval of the regulator stakeholder to confirm and validate the rights of use and to allow trading/leasing. Oversight is also afforded to cater for any resulting actions which the regulator may be required to take in order to address aspects such as foreclosure or the concentration of rights of use. This positions the 5GZORRO platform well in relation to current and future compliance on spectrum regulation fronts.

3.7. Data for AIOps

Since 2017, when the term AIOPs has first appeared to mean AI (Artificial Intelligence) for Ops (Operations), the method of using data for managing complex operations was adopted by many organizations. This approach allows simplifying the cumbersome operation management through features like anomaly detection, fault management, root cause analysis, capacity planning, etc.

Telecommunications is a powerhouse of complex IT operations and for this industry the value of data-driven automation for provider sustainability and improving customer experience cannot be overestimated. Over recent years, we witness the appearance and the adoption of AIOPs techniques and tools created specifically for the Telecommunication industry (references: Solutions blog: How AIOps-enabled Automation can help the Telco Operations Centre - Mycom OSI (mycom-osi.com) ; AIOps Solution for Telecom Industry | The Ultimate Guide (xenonstack.com) ; 24569 AIOps report report (BMC) ; Transforming Telco Operations with AIOps | IBM). These tools greatly enhance operators' efficiency by offering features like proactive customer support, network fault prediction and prevention, anomaly detection of BSS performance, network and IT security, etc., by building models for the normal network behaviour, using these models for alerting on the abnormal situations, and, more recently, computing predictive insights and recommendations.

As AIOPs paradigm is proving its value to the management of complex networking infrastructures, including 5G, there are several industry specific *data related* issues that still require research attention. Some issues are technical and stem from the domain specific operational reality of even a single operator. Some other issues are related to a multi-provider multi-domain nature of the evolving Telecommunication industry, and, more broadly, to the ultimate case of multi-cloud and edge networking where Telco providers will most probably become important players. While the former type of issues is addressed by industry committees (references: 3GPP Network Data Analytics Function (NWDAF). The Cornerstone for Autonomous 5G Networks - FutureNet World), issues of the latter type are new and do not have ready to use solutions:

- Complex multi-modal nature of 5G/6G operational data. Do we need common standard data models? And, how we stich the models to enable reasoning across technology domains – RAN, core, transport, Internet, and Cloud networks?
- Data ownership and sharing. Do we really need (all) the data to be shared? If yes, can operators be incentivized to engage in sharing their operational data (with peers, with clients, with suppliers)? Will regulation be needed?

- Data protection. How we ensure that data sharing/isolation rules can be transparently established by data owners and trustworthily enforced by the system, in very dynamic environments?

In 5GZORRO, we have approached these issues through creating a 5G specific data analytics engine for AIOPs, named 5GZORRO operational Datalake, architected to address some of the issues above. First, we have decoupled the *operational data provider* from the *operational data consumer*. Operational data provider is realized through the MDA component that collects data on behalf of its owning resource or service provider. The data is then fed into the Datalake's data store through dedicated secure channel, to be accessed and processed only by authorized analytics components, such as SLA breach detection and SLA breach prevention. This approach has been validated through testbed and use cases integration as described earlier in this document. The most prominent results are achieved in the context of UC3, where the required operational telemetry collection is possible without concerns of sensitive data exposure to other participants of the 5GZORRO ecosystem. This is not always the case; for example, in a case of detecting interference with respect to the acquired spectrum usage (see Section **¡Error! No se encuentra el origen de la referencia.**), it is not yet clear what party should perform the measurements and incur the overhead of developing and operating the related MDA.

While we have fully achieved the technical validation of our multi-provider AIOPs approach, its business validation will require additional liaisons and research work. We have initialized this as part of the TechTalk#4 delivered in May 2022 with the goal of drawing attention to this important subject of data for AIOPs in the Telecommunication sector.

3.8. **Telco services**

The foundation of connectivity services regulation in Europe is the principle of the so-called *network neutrality*, a concept coined when Internet services started to be defined and provided, and the strategy in support of a *Digital Single Market*, with connectivity services at the core of the so-called second pillar.

The second pillar of the Digital Single Market Strategy is associated with the *digital environment*, understood as the digital network itself and all the ancillary elements in support of this digital market. The strategy is focused on three main objectives [30]:

- Making the Digital Single Market sustainable and simple to use.
- Making access to networks and services reliable and affordable.
- Making the market to adapt to changes in its environment.

A special emphasis is also put on the protection of personal data, one of the European flagships in digital space. These objectives call from an evolution in telecommunication regulations, still underway, and imply a necessary reflection on the rules that enabled the advent of Internet services, guaranteeing a fair competition framework among telcos and content and service providers. The evolution of mobile networks, towards 5G and beyond, makes this reflection even more necessary. The 5GZORRO approach to open, interoperable marketplaces for infrastructures, functions, and services, relaying on intent declarations of the different actors and dynamic trust assessment constitutes a bold step towards the goals of this single market. 5GZORRO-based services can be considered a spearhead into Digital Single Market Strategy, supporting a better founded evolution of related regulation activities.

The basic framework for network neutrality in the EU is defined by Regulation 2015/2120 of the European Parliament and Council, "laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union" [31]. According to the general interpretation of this regulation, as provided by BEREC [32], European network service providers are "prohibited from blocking or slowing down of internet traffic, except where necessary”. These exceptions are related to the compliance with legal order (addressing Lawful Interception principles common in laws on all kinds of telecommunication services), to the application of the necessary means to ensure integrity and security (acknowledging the shared critical infrastructure nature of the network), and the management of exceptional network congestion (permitting the application of traffic management in specific cases). The exceptions require that all equivalent traffic categories are treated impartially.

Network neutrality is a controversial issue, given there is no clear definition for it and many of the models currently applied for it correspond to the early days of Internet services. A briefing of the European Parliament [33], associated to the EU Regulation mentioned above, acknowledges at least four main definitions, ranging from specific requirements on traffic processing to general principles around openness and freedom. And how these principles translate into technical standards and associated regulations need to be periodically re-assessed as technology evolves, as in many other ICT fields: think about personal data and AI, just to give an example. The evolution of the network-based services enabled by 5G and beyond, and the potential critical applications associated to this evolution obsoletes the original fairness rules inspired by a best-effort network. Furthermore, with the advent of hexascalers and the associated trends towards centralization of connectivity and services [34], the threats to network service openness and open competition have dramatically change, demanding a reassessment of the mechanisms to address these threats at all levels, including technologies, best practices, policies and regulations. Compositional capacities, as the ones in the 5GZORRO approach, can become a touchstone for an evolution of the practical rules for new network neutrality concepts. These new concepts will be required to addresses correctly the challenges associated to the emergence of the edge-network-cloud continuum that is taking shape in these days.

In what relates to security and privacy, the EU has made protection of personal data one of its flagships in digital space, making European norms in this are a global reference. The regulations to be considered mostly regards aspects of the data protection legislation (most notably, GDPR [67]) and its national interpretations, and the Directive 2016/1148 of the European Parliament and Council, “concerning measures for a high common level of security of network and information systems across the Union” [68], that defines minimum security controls for information and network security. Given the utmost care the 5GZORRO proposal has applied on security and privacy enforcement, it is clear that those services built by means of 5GZORRO-based platforms will be exemplary in these aspects.

Finally, an important issue, which has been around for some time and attracted very high interest with the pandemic situation and the recent political unrest in Eastern Europe, is related to *data and technological sovereignty*, with special emphasis on cloud-based infrastructures. The European Commission has started different studies on cloud contracts, analysing how existing specific and general legal principles apply to certain key contractual issues, and the economic impact of unfair and unbalanced terms **¡Error! No se encuentra el origen de la referencia.**. These studies may well constitute the foundation for further regulation on the identified gaps.

Specific initiatives to retain technology sovereignty has been launched, with GAIA-X [45] as flagship. GAIA-X is committed to develop a framework for the control and governance of any existing cloud/edge technology stack to obtain transparency, controllability, portability and interoperability across data and services. In the long term, there is the aspiration of a European strategic autonomy in ICT technologies. As an enabler for the open consumption of integrated network and cloud services, the 5GZORRO proposal is extremely well positioned to address fairness requirements in cloud-based contracting, as well as to enhance European technology sovereignty.

4. Economic Validation

The economic validation of the 5GZORRO platform is intended to assess its market feasibility and ease the adoption of 5GZORRO propositions. This validation is underpinned by the analysis of the platform business model applied to the three different UCs and a technoeconomic analysis of our platform prototype.

4.1. Methodology

4.1.1. For the business model

To assess the business model associated with running the 5GZORRO platform in a competitive context, partners are using the Business Model Canvas [46] template, a tool to describe how to create, deliver, and capture value with the project's main result.

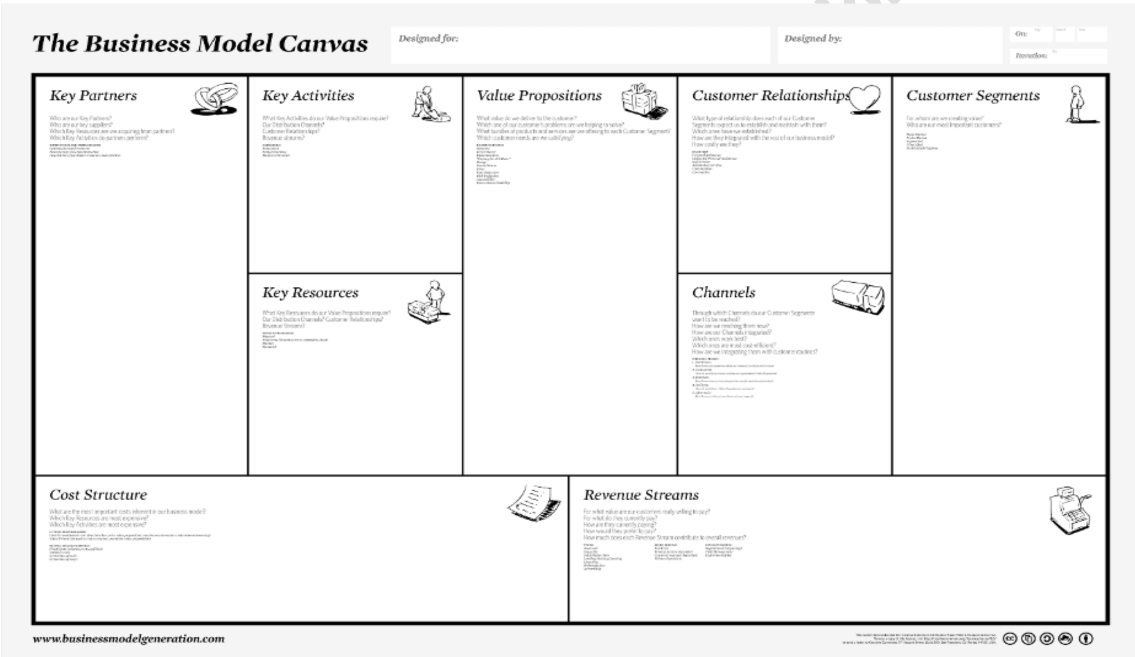


Figure 91: Business Model Canvas template by A. Osterwalder

The project's main result is the 5GZORRO platform, that encompasses all the different software components developed in the project. These software components are individually or jointly owned by two or more project partners. These partners will reflect on their business idea and opportunities related to these concrete components in the context of task T6.3: Exploitation and Roadmap [1]. The aim the economic validation is to validate the whole 5GZORRO platform from a business perspective and for that we rely on the three UCs, which are the means to demonstrate the different capabilities of the platform by applying it to different contexts.

The blocks of the business model canvas tool are the following:

- Customer Segments – for whom 5GZORRO results are creating value.
- Value Proposition – a single and compelling sentence that explains the uniqueness of the solution.
- Channels – how we can reach 5GZORRO customer segments with the value proposition it has to offer and how we are supplying them what they need/want.

- Customer Relations – the measures we can take to acquire and maintain relations with 5GZORRO customer segments.
- Key Resources – the assets required in order to supply the customer segments with 5GZORRO value proposition.
- Key Activities – the main elements we need to focus on in order to deliver the value proposition for 5GZORRO customers.
- Key Partnerships – identifying suppliers/partners who allow the business model to function and operate successfully.
- Cost Structure – recording all the costs which the business model incurs in order to operate successfully.
- Revenue Streams – after having supplied the customer segments with what they desire, we aim at generating a profit from the commercial relationship. This block aims at identifying these sources of revenue.

The exercise started with the definition of the Value Proposition of the 5GZORRO platform for the different customer segments and applied to the three UCs defined in the project. For this first assessment, the consortium used the Value Proposition Canvas [47] template, a tool to identify the added value 5GZORRO can deliver to its target market.

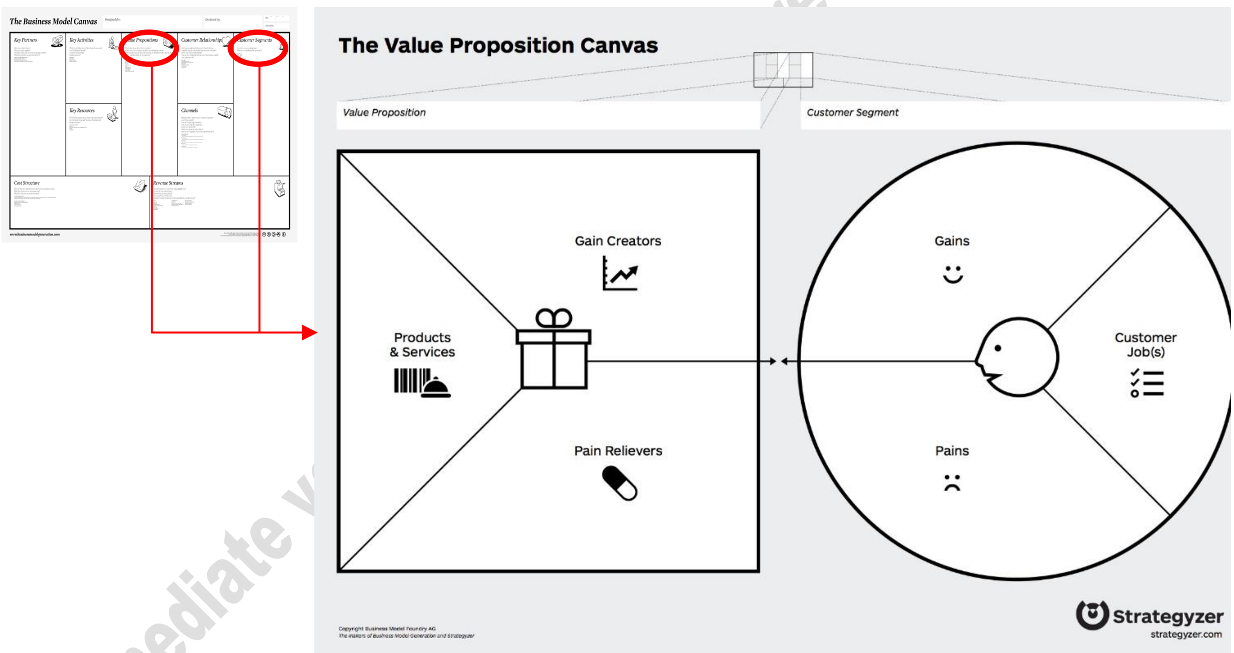


Figure 92: Value Proposition Canvas template by A. Osterwalder

Guided by T5.4 leader, the Consortium has used this tool to understand the different profiles that would most use the 5GZORRO platform ("Customer") and brainstorm about the value it can offer to them. So, first of all, these different profiles were listed and for each of them, the **Customer Jobs**, that describe what customers are trying to get done in their work in relation to our idea; then the **Gains**, describing the outcomes customers want to achieve or the concrete benefits they are seeking and, finally, the **Pains**, that describe anything that annoys customers before, during, and after trying to get a job done or simply prevents them from getting a job done. With these initial insights, partners completed the so called "Customer Profiles". Afterwards, they reflected upon the "Value Map", the list of the **Products and Services** the 5GZORRO platform value proposition is built around, the **Gain Creators** that describe how these 5GZORRO products and services (the different functionalities) can create customer gains and the **Pain Relievers**, illustrating how these products and services can alleviate customer pains.

This exercise was done online in weekly meetings during Q4 in 2021 (building on partners own experience, some of them represent the profile being targeted, like operators, or know them very well as they have them as their own customers). The questions used in the meetings to think about the different parts of the Value Proposition Canvas were:

- What does this UC want to demonstrate?
- What are the profiles involved and the role they take?
- Who would pay for enrolling in the 5GZORRO platform and enjoy this functionality-the profile 5GZORRO benefits most?
- What are the main benefits for which these profiles would pay?

After that, T5.4 leader summarised the input to describe in few words and for every profile, what would be the main benefit for them (the Value Proposition). It was then circulated to all the partners for confirmation and final input to agree on the different value proposition sentences.

When the value was clear, partners continued discussing about the rest of the business model canvas blocks in four different internal workshops, the first part held in Q4-2021 (two sessions) and the second part in Q1-2022 (two sessions)

The consortium has also requested the support of the Horizon Results Booster (HRB) service of the EC to work further on business models and the exploitation roadmap. The request was made on the 6th of May 2022 and, since then, T5.4 leader and the Exploitation Manager have been working with the HRB experts compiling the necessary materials in preparation of the two half-day workshops that gathered the whole consortium on the 5th and the 7th of October 2022. The findings of the workshop and the feedback given by the HRB experts have enriched our analysis and, as such, is embedded in sections 4.2 and 4.3.

Besides, we have also received from external stakeholders through interaction with them in the different events planned until the end of the project (like EuCNC in June 2022 and Final Event on the 27th of October 2022) and through the online survey launched in January 2022 "Towards a dynamic marketplace for 5G resources" (analysis of the survey included in Annex I), promoted through the project's social media channels and the events where 5GZORRO was present (MWC '22, EuCNC '22, BEREC plenary on the 6th of October 2022, etc.). The survey has been active until the end of the project as a way to keep our audience engaged and enhance our final result.

4.1.2. For the techno-economic analysis

The techno-economic analysis (TEA) is an evaluation of a solution with the aim of selecting the most cost-efficient choice for a certain scenario and performance requirements. It aims at the identification of the most efficient pathways for technological development and assesses how this technology might be successfully deployed in a profitable way.

For the 5GZORRO platform TEA, we have adapted the methodology by Miroslaw Kantor [19] to the particularities of our project and the data available to us.

The Kantor methodology for TEA considers three steps: scope, calculations and evaluation. The process starts defining the <u>Scope</u> of the question under analysis and detailing the inputs for the study based on a market analysis. The second step is <u>Calculations</u>, making a distinction between economic calculations (estimation of costs and revenues) and technical calculations, in which the performance metrics of the proposed solution are estimated. The final step, the <u>Evaluation</u>, is based on the outcomes – economic and technical – of the calculations step. This step is split between investment analysis and performance analysis. The first part is an estimation of the (expected) profitability of the solution being analysed, while the second is a comparison of the different alternatives, making trade-offs of costs vs. performance.

As indicated by [20], *the readiness level of a project influences not only assumptions, quality and availability of data, but also and foremost the decisions of metric and consequently results and interpretability*. As the 5GZORRO platform will not be a complete and qualified system at the end of the project (as it is indeed a validated prototype reaching TRL4/5), to the three step methodology considered by Kantor, we will adapt the three steps and add a final one that has to do with Risk and Uncertainty analysis.

In the following lines, we provide a more detailed description of the TEA methodology that has been applied for the analysis in section 4.3:

Scope

The question under analysis is the deployment and operation of the 5GZORRO platform. As input for this step, we will consider 5GZORRO market analysis.

The level of detail and the point in time at which the market evaluation takes place depends on the grade of technological development. In early stages, what should be investigated are the main opportunities and space for the technology, together with a first identification of alternatives and benchmarks, so the analysis conducted at the beginning of the project (D6.4 [18]) is very relevant now for the TEA and should precede the cost estimation supporting a proper identification of expenditures. In D6.4, the consortium analysed also key aspects regarding the industrial impact of 5GZORRO research results beyond the evolution of telecommunications technologies, i.e. the regulatory implications of the 5GZORRO solutions and the impact of 5GZORRO on media, AI, finance/banking and other sectors. It may be the case that new market sensibilities drive a second iteration of the market analysis. In fact, in the context of T5.4 the respective partners are monitoring regulatory aspects and evolutions in spectrum, blockchains, security and AI topics (section 3 of this document), thus giving input to this step of the 5GZORRO TEA methodology.

Calculations

The cost analysis in combination with the revenues constitute the economic model.

For the cost analysis we will perform an estimation of costs, that means quantifying total costs on the basis of operational (OpEx) and capital (CapEx) expenditures.

According to the Investopedia [48], operational expenses are the *day-to-day expenses a company incurs to keep its business operational* while capital expenses are *major purchases a company makes that are designed to be used over the long term*.

Both categories can be broken down, providing additional information for further analysis on profitability in the next step (Evaluation). As such, a distinction can be made between infrastructure and operational cost components. Infrastructure costs are typically bundled under CapEx and can have failure-rates and replacement periods into account. Operational costs are modelled using manpower and operational processes and are typically bundled under OpEx.

In any case, it should be taken into account that, by the end of the project, the consortium will be delivering a proof of concept of the main functionalities targeted by 5GZORRO platform and not a minimum viable product (MVP) working in an operational environment. The development of an MVP is in the scope of the exploitation roadmap included in D6.5 [1]. This implies that costs calculations are based on the lab infrastructure that we are using and on and the values of KPIs that we are considering in the technical validation. As next step, a cost optimization exercise will need to be done by potential investors putting in place a scalable and operational IT infrastructure.

Revenues will be calculated based on the subscription rate discussed in the Business Model Canvas activity and taking into account the description of the market (market size). The market size in turn can be estimated using the customer adoption model or dedicated market research figures. The customer adoption model deals with identifying our target market, awareness and interest. A good estimation for this can be the input collected through the survey “Towards a dynamic marketplace for 5G resources”.

Technical parameters are essential for techno-economic evaluation. For example, if network monitoring and recovery mechanisms are essential for the reliable service delivery of the 5GZORRO platform, these costs need to be evaluated. However, as we are not evaluating an MVP, we base our assumptions on the performance indicators that are being calculated in T5.1, T5.2 and T5.3 activities.

Evaluation

This step aims at offering a qualitative overview of the economic performance of the 5GZORRO platform, adding insights on the platform's development to compare alternatives and/or thresholds. The aim is to serve for guiding decisions about the allocation of resources and the definition of investments.

Investment analysis combines all cash flows (costs and revenues) to make a decision on the profitability of the investment project. According to [21], optimal profitability indicators are recommended for each specific technology readiness level. For our case, we will use the payback period. These profitability indexes will be calculated taking into account the figures estimated in the previous step.

The payback period refers to the amount of time it takes to recover the cost of an investment, that is, the length of time an investment reaches a breakeven point. It can be calculated dividing the initial investment by the annual cash flow (revenues-costs).

Performance analysis is based on the economic and technical calculations. The relation between cost and reliability also should be considered. Improvement of reliability performance is typically associated with additional investment costs, but we will need to keep CapEx and OpEx at reasonably low level to be able to offer an economical solution.

Risk and Uncertainty

Every evaluation developed on assumptions and estimates inevitably produces uncertainty in results. For TEA, uncertainty is mainly caused by errors in input data and the characteristics of the context in which the analysis is performed [20]. However, decision makers need to be informed on the reliability of positive results, as well as on which technical and economic parameters have the potential to influence most the profitability of the investment.

There are two main tools that can be used to deal with TEA's uncertainty: sensitivity analysis and scenario analysis. We will use scenario analysis to consider contextual variations and possible future events that may affect our results, setting three possibilities for the uncertain variables: a pessimistic, a most probable and an optimistic scenario.

4.2. Business Model

Following the methodology described in section 4.1.1, we include here the business model analysis for the 5GZORRO platform.

4.2.1. 5GZORRO Platform description

The 5GZORRO project is working on new security and trust solutions for multi-domain and multi-stakeholder scenarios in 5G and beyond networks. As main result of the project, the 5GZORRO platform enables multiple stakeholders, across different technologies and geographical span, to trade/lease heterogeneous resources: spectrum, computing, network, storage, and virtual network functions (VNFs). The goal is to optimise, depending on their business role, the available network resources and establish 5G services in an easy, flexible, automated, secure, and trustful manner, ultimately fulfilling the need for secure services and allocating them according to demand.

The 5GZORRO platform provides different capabilities in support of a telecom marketplace for trading and acquiring multi-provider 5G product offers, with smart contracts based on DLTs, and AI operations through cross-domain zero-touch service, network and security management. So, it is through this digital marketplace that the different participants along the 5G value chain (including users within industry verticals, service providers, network operators and the spectrum regulator), can trade 5G-related resources and services based on dynamic commercial needs and in a zero-touch, secure and trusted way, thus perceiving the value of the 5GZORRO platform, the project's result that we are validating.

In the 5GZORRO Marketplace, the different participants can trade with resources and/or services, meaning:

- 5GZORRO resources: all kind of assets comprising the infrastructure used to realize communication services. In general, resources are computing, storage and networking capabilities including Virtual Network Functions (VNFs);
- 5GZORRO services: communication services offered to end-user customers that are built on top of 5GZORRO resources.

So 5GZORRO allows supply and demand meet dynamically following market-driven business models, promoting the development of a freely competitive market but also implementing the necessary controls for regulatory oversight and intervention.

4.2.2. 5GZORRO value proposition

In this section, we reflect upon the first block of the Business Model Canvas tool, the "Value Proposition" for the different stakeholders or "Customer Segments" identified by the partners with the help of the three use cases. After that, and with the help of the HRB experts, we have validated 5GZORRO value proposition from the perspective of the main customer, independently of the UCs.

4.2.2.1.UC1: Smart Contracts for Ubiquitous Computing/Connectivity

This UC demonstrates the application of 5GZORRO platform in the use of smart contracts between different parties. With 5GZORRO platform, the needed resources and services are leased and, thanks to the smart contracts, the connectivity in the agreed areas is guaranteed, avoiding infrastructure and management investments.

The profiles involved in this demonstration are telco operators or CSPs that play the role of resource provider or resource consumer. The resource consumer can, for its part, compose a service offer and act as a service provider.

<u>Telco Operator (CSP) as resource provider</u>

- Profile

A CSP that owns spare resources at a given time.

- "Voice of the customer"

CSPs think that they could handle their resources more efficiently if they could lease them when they are not in use. But the drawback is the cumbersome work associated to it, as there is a need to sign contracts with the resource consumers and monitor the resource consumption to assure that the terms of the licences are respected.

- Mapping 5GZORRO platform

With 5GZORRO platform, resource providers can easily register their resources and add any associated licence agreements. Besides, the platform allows non-trusting parties to engage with others (they would not be able to do it without a trusted 3rd Party).

- 5GZORRO platform Value Proposition for a resource provider CSP

"5GZORRO offers real-time dynamic and automated leasing and provisioning of spare resources in a secure manner, capitalising on otherwise wasted resources in the current cumbersome contract scheme.

Moreover 5GZORRO offers means to automatically monitor and consume information related to SLAs linked to resource consumptions and service performances".

Telco Operator (CSP) as resource consumer

- Profile

A CSP that lacks resources and services to be able to offer a complete service to its customers. It can also compose a service, to be offered in the marketplace, leasing resources from one or more resource providers.

- "Voice of the customer"

CSPs refer to trust as a main issue when dealing with other CSPs and software vendors.

- Mapping 5GZORRO platform

5GZORRO platform offers a smart resource discovery for consumers by means of a catalogue where resource consumers can procure resources and services (not having themselves) to offer a complete service to their customers. Smart contracts are used in 5GZORRO platform to establish Zero-touch provisioning of resources and associated legal agreements between parties. Trust is addressed in 5GZORRO platform, building trust scoring based on historical reputation and recommendations.

- 5GZORRO platform Value Proposition for a resource consumer CSP

"With 5GZORRO, E2E services can be compiled from dynamically leased resources of multiple providers and offered directly to the customer in a secure manner"

Software Vendor

- Profile

Vendors offer their VNFs to allow other stakeholders to use their products to compose customized services.

- "Voice of the customer"

No existing marketplace for VNFs offers that can be automatically combined with service and slice offers by other stakeholders (i.e., resource and service providers), with native orchestration capabilities to automatically deploy and configure VNF instances.

- Mapping 5GZORRO platform

With 5GZORRO platform, vendors can onboard their software products (in the form of virtual functions) to be exposed in the 5GZORRO catalogue and offered as resources in the marketplace

- 5GZORRO platform Value Proposition for a software vendor

"Enrolling in a digital marketplace like 5GZORRO can facilitate the trading of network functions, increasing their commercial possibilities"

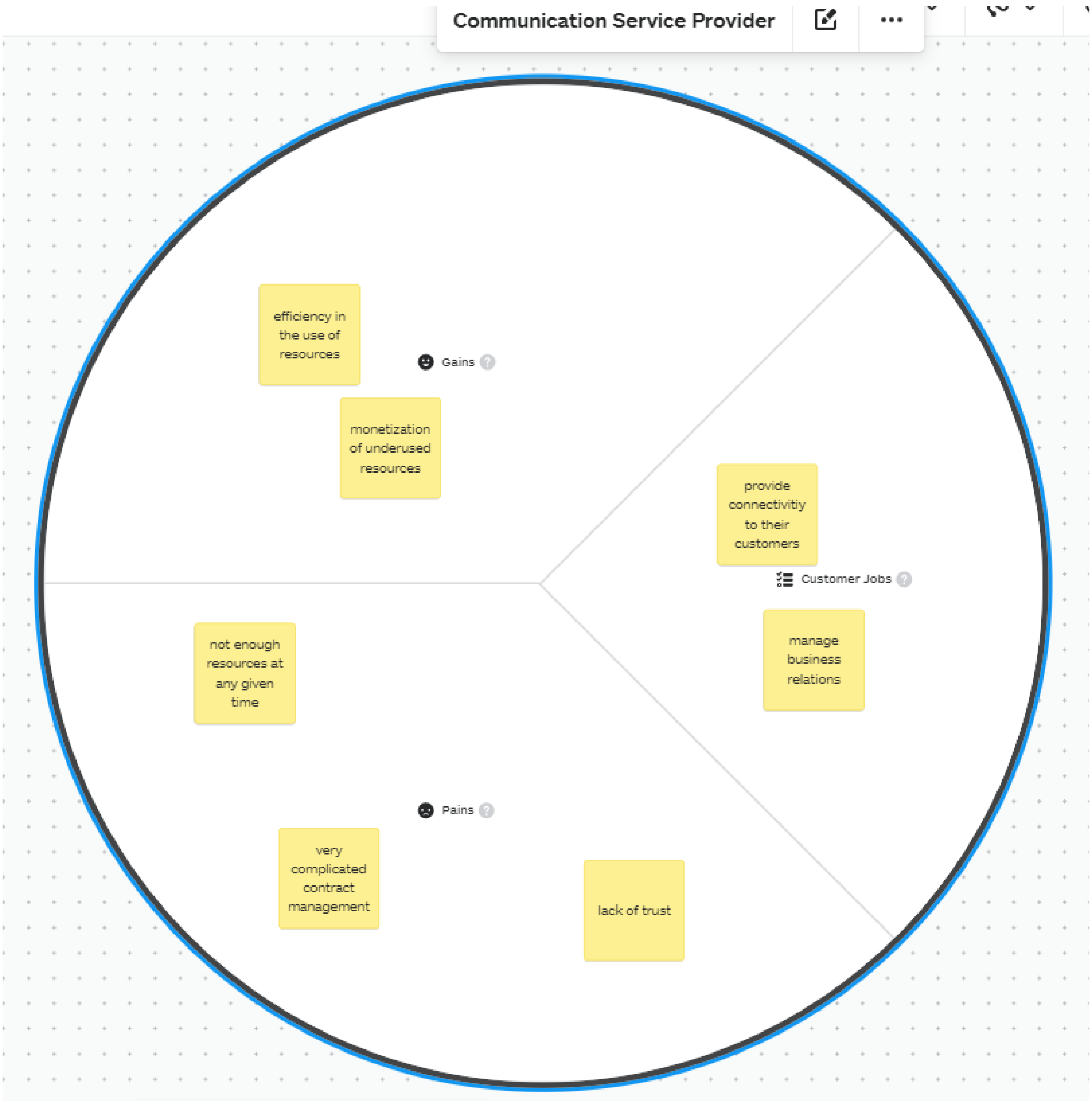


Figure 93: Screenshot of a phase of the VPC exercise

4.2.2.2. UC2: Dynamic Spectrum Allocation

One of the UC2 scenarios wants to demonstrate how different parties (concessionaire, vertical, telco operator) can trade with spectrum in the 5GZORRO platform. More information and detailed description of UC2 scenarios is given in D5.2 [24]. In this section, we focus on the value that the related stakeholders can perceive from the 5GZORRO platform applied to this particular context.

<u>**Concessionaire**</u>

- Profile

The concessionaire's role is that of an intermediary, operating on behalf of a regulator for spectrum which is being administered on a club use [49] approach. This model ensures that the regulator is not directly present on the platform, so as to limit smart contracts to civil law, without venturing into criminal or administrative law aspects.

- “Voice of the customer”

Concessionaire’s job is to coordinate the use of the shared spectrum for a specific period of time and in a specific location in an efficient manner. As this entails dealing with different stakeholders, there is obviously an administrative overhead, so there are benefits in coordinating these stakeholders efficiently on a single platform in an automated and in a trustful manner. Another pain that this stakeholder experiments is the management of interference in an effective manner, typical to when channels are assigned manually, thus resulting in a poor service.

- Mapping the 5GZORRO platform

Spectrum is a scarce resource. Non-shared spectrum, granted through individual and exclusive rights of use, provides regulatory guarantees against interference but at the expense of spectrum efficiency.

With the 5GZORRO platform, the concessionaire can generate spectrum offers on the platform so as to coordinate the use of shared spectrum (on behalf of the regulator). Spectrum can be managed very efficiently with the 5GZORRO platform, as after an offer is consumed, it makes it available again for other customers. The concessionaire can grant an individual right to access a shared spectrum, for a specific period of time and in a specific location, while managing interference in an effective manner to a vertical (e.g. club use model) and also to other operators. Hence, the platform can be used to coordinate the shared use of spectrum, assign channels automatically, coordinating time and location requirements with the aim of overcoming potential interference issues.

- 5GZORRO platform Value Proposition for a concessionaire

“With 5GZORRO, the highest efficient an effective spectrum use is ensured, promoting the development of a freely competitive market but also implementing the controls necessary to allow for regulatory oversight and intervention as may be necessary”

<u>Vertical</u>

- Profile

Verticals are companies that focus on a niche or specialised market spanning multiple industries. The advent of 5G and the emergence of related use cases on industry verticals is placing demands on network resources and services, including spectrum.

- “Voice of the customer”

Verticals have to provide managed services, including connectivity, to their own customers. Depending on their business strategy, verticals would either need a network slice or, if they already have the necessary infrastructure and knowledge, they might be interested in only securing spectrum to deploy a private network, allowing them further control of their infrastructure.

Ultimately, the focus of industry verticals is in providing managed services to their customers, while minimizing the time and effort spent in dealing with the technical and legal aspects of deploying 5G connectivity. They highlight the difficulty in negotiating with different Mobile (Virtual) Network Operators and sometimes from different countries resulting in dealing with several contractual agreements, legal issues even in foreign languages. All in all, there is an overhead in configuration changes to maintain consistent managed services. Besides, Verticals stress that when they have to deal with new providers, the lack of trust is a problem for them. Additionally, they have to be very careful to comply with GDPR aspects.

- Mapping the 5GZORRO platform

When a Vertical opts to deploy its own network and seeks to acquire rights of use to spectrum through the 5GZORRO platform (from a concessionaire or from an operator), Verticals can set up a network with a certain quality of service, and thanks to an automatic assignment of channels there will be minimal to no interference in the bands. Besides, Verticals can benefit from a great dynamicity, as they can use shared spectrum or leased spectrum through the platform to meet their needs, returning the spectrum when it is no longer needed i.e. spectrum resources can scale up and down automatically.

Besides, stakeholders in the 5GZORRO platform are authenticated and granted access, keeping untrusted parties out. And even if a player is new, not having done any transaction yet, the 5GZORRO platform provides a way for trusting it based on reputation scores.

Moreover, the resource offer cost optimization functionality also highlights the ability of the 5GZORRO platform, through AI techniques, to find the most cost-efficient resource for the spectrum consumers among a set of resources that are available in the marketplace.

Indeed, the availability of a marketplace where vertical customers can acquire rights of use to spectrum via spectrum trading to deploy their own private network is an added value, especially when combined with automation and trust provided by the 5GZORRO platform. This is especially of interest and relevant for industry 4.0 verticals, and for those private/public interactions (e.g. the PNI-NPN scenarios for public network integrated non-public network).

- 5GZORRO platform Value Proposition for a Vertical

"With 5GZORRO you can scale up and down dynamic spectrum to meet your needs in a fast, automated, cost efficient and easy way, always in a secured environment"

<u>Telco operator (CSP)</u>

- Profile

Telco operators are communication service providers or CSPs. They need to offer connectivity solutions to their customers but have limited resources, including spectrum, so they may want to extend their capabilities under certain needs.

- "Voice of the customer"

Telco operators tend to be reluctant to share their licensed spectrum resources with third parties (other telco operators), in order not to reduce any commercial advantage they may have. But telco operators that are not able to participate in spectrum auctions would find it very convenient if they could trade or lease licensed spectrum from another operator.

In December 2018 [50], the EU adopted new telecom rules aimed at modernising the European regulatory framework for electronic communications. These rules place renewed emphasis on the shared use of radio spectrum. From a regulatory viewpoint, spectrum sharing can be achieved by allowing the collective use of spectrum, whereby multiple users can share the resource simultaneously without requiring a licence.

Non-shared spectrum, which is granted through individual and exclusive rights of use, provides regulatory guarantees against interference at the expense of spectrum efficiency, which can however be mitigated through the trading or leasing of assigned but unused spectrum. Besides, Telco operators might welcome the increased revenue they could get from sharing some underutilized resources temporarily. In any case, these spectrum transactions should be overseen by the Regulator to avoid market distortion and to carry out the necessary due diligence.

- Mapping the 5GZORRO platform

Through the 5GZORRO platform the National Regulator Authority responsible for spectrum management can validate a provider's spectrum certificate - a digital certificate that the CSP publishes to the platform, against the spectrum licence which the Regulator himself has issued. In this manner, only trusted and verified stakeholders with spectrum rights of use can publish spectrum offers on the 5GZORRO platform. Besides, the platform can continuously monitor whether the use of the actual spectrum is correct and fulfils the active spectrum SLAs. If this use is not correct, the 5GZORRO platform allows the regulator to remove spectrum certificate and thus effectively halting the possibility of publishing any further spectrum offers, issue temporary bans on potential spectrum consumers and also annul an active spectrum offer and trade.

When a telco operator leases spectrum with other stakeholders in the 5GZORRO Marketplace, this can be restricted to specific geographical areas and regions, where for example the telco operator does not have specific market interests, optimizing the use of the spectrum for the provider.

In addition, operators can benefit from the 5GZORRO platform to increase their spectrum pool by purchasing spectrum offers from other operators. This is applicable in those cases where a given operator may need to acquire the rights of use of additional spectrum resources to cover a specific area/region. This of course may depend on specific national regulations but could favour the business and market opportunities of local/regional telco operators. In this case, the regulator's active participation in the 5GZORRO platform guarantees that no operator can exceed the spectrum caps stipulated for spectrum auctions and thus avoiding market distortion.

- 5GZORRO platform Value Proposition for a telco operator

"Thanks to the 5GZORRO platform, an operator can maximize the monetary value it can reap from the rights of spectrum use it has been assigned by trading underutilized spectrum, and have the possibility of acquiring new rights of use once the need arises, minimizing its capital expenditure"

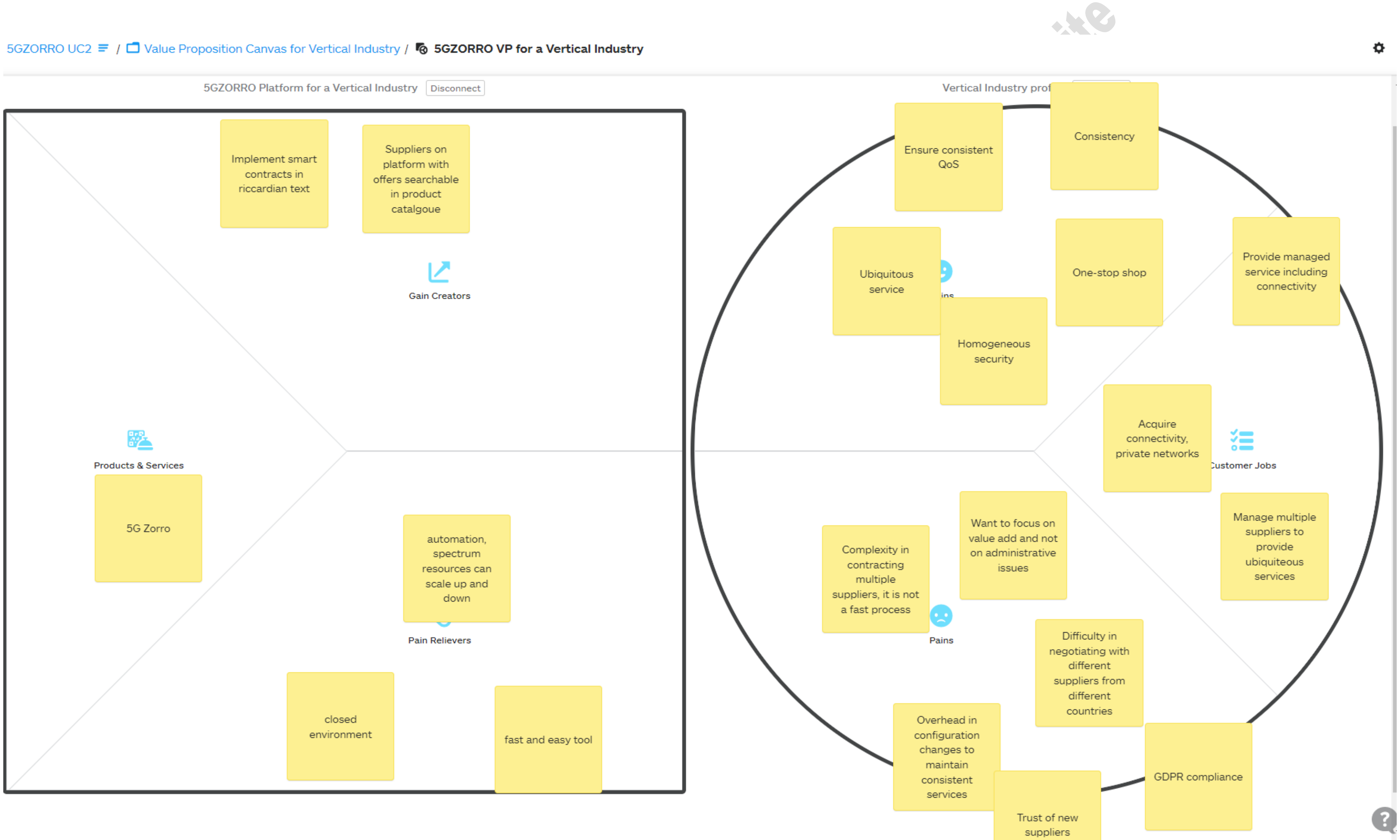


Figure 94: Screenshot of a phase of the VPC exercise

4.2.2.3. UC3: Pervasive vCDN Services

UC3 wants to demonstrate the 5GZORRO platform capabilities of dynamically and automatically scaling 5G services to 3rd party infrastructure resources. For that, UC3 focuses on a concrete example that consists of a CDN solution with streaming servers and content caches hosted on a CSP infrastructure. The different profiles involved in UC3 are the CDN / OTT service provider, the Communication Service Provider (CSP) and a 3rd party resource provider.

CDN Service provider

- Profile

The CDN service provider is the operator of the content delivery network. In our context, the CDN provider leases network slices from the CSP in order to provide the CDN service.

- "Voice of the customer"

CDN service providers' aim is to give CDN end users a good quality of service, so their main pain is when the CSP they have an agreement with can't comply with it and the CDN end users have delays or even service discontinuation. Besides, they would like the terms of the agreements with CSPs to be easier to verify and also to provide CDN services to more end users at a time. On the security and trust perspective, CDN service providers claim that when the CSPs use external resources for running their software, they may not trust (some of) the external Resource Providers (3rd parties) and also it is a pain when they are unable to solve security breaches in the event of non-compliance with SLA-based contracts.

- Mapping the 5GZORRO platform

The 5GZORRO platform provides AI-driven SLA breach prediction functionalities that would help in minimizing the effect when CSPs have no more resources to allocate. Also, it is worth to highlight the ability/option of a CDN Service Provider to find and order resources from the Marketplace in a trustful and automated way and avoiding conflicts in standardisation terms with the services already published.

- 5GZORRO platform Value Proposition for a CDN Service provider

"Through the use of the 5GZORRO platform, the CDN provider is able to maintain a constant Quality of Service for its customers regardless of the increased traffic (as long as there are available resources in the Marketplace) as the use of 3rd party resources looks like an extension of the network infrastructure. 5GZORRO platform will help increase user engagement thanks to an enhanced user experience. Thus, revenues for the CDN provider will be increased with a minimum cost from the CDN side thanks to the use of dynamic, on demand resource allocation"

Telco operator (CSP)

- Profile

CSPs usually own the resources and infrastructure that is used in order to give the needed services to CDN providers. This means that the CSP leases a network slice instance to the CDN service provider including performance guarantees based on a service workload profile. The case of video content delivery is especially demanding since video streaming has strict requirements with respect to viewing quality.

- "Voice of the customer"

CSPs claim that when they have no more resources to allocate at a specific area, leasing new resources in near real-time is expensive and time consuming for them. Additional management and operational complexity are needed for regulating/controlling the access and use of the resources, as contracts are signed manually. They also need to monitor the consumption of resources to be able to bill accordingly and this is not done automatically, hence, prone to errors. Besides, they need a trusted relationship with the resource provider.

It is important for the CSP to understand the available resources in a certain area. For example, understand where the new capacity is needed and be able to deploy the new capacity resources close to that location.

CSPs also highlight that for them is a clear advantage to be able to lease their resources to other CSPs when they don't need them but, of course, monitor the operational functions of these leased resources.

- Mapping the 5GZORRO platform

With the 5GZORRO platform, CSPs can lease resources on demand, having the possibility to lease only the required number of resources and for the required period of time (avoiding extra costs of unused resources) and, also, the ability to choose, from a variety of options, the least expensive resource that is closest to its needs. Indeed, the 5GZORRO Marketplace can offer an intelligent filtered query/selection of product offers based on location, automating and accelerating the identification of proper/appropriate providers of resources of interest.

Moreover, the 5GZORRO Marketplace offers a single access point to discover all the product offers available. This facilitates the process of service delivery, as it minimizes the overhead (in terms of time) in the best product offer selection process with respect to traditional B2B interactions.

The 5GZORRO platform can offer a degree of automation in all of the phases of a service/product delivery (from offer discovery, to selection, activation and zero-touch operation).

- 5GZORRO platform Value Proposition for a telco operator - CSP

"The CSP, by leveraging upon the 5GZORRO platform, is able to offer advanced services to its vertical customers, ensuring that the SLA requirements will be always satisfied, and that the communication service will continue to run smoothly in spite of the increased traffic. Additionally, it may take advantage of the 5GZORRO services in order to optimize its own operation and resource exploitation. In respect to acquisition of 3rd party resources, 5GZORRO exploits services that facilitate the automated selection of resources, which are based on AI techniques. Another business benefit for the CSP is the reduction of CapEx and OpEx, since it will be able to lease edge resources neither bought nor operated/maintained by itself"

Resource provider

- Profile

In our context, resource providers lease their unexploited resources, increasing in this way their profits. They dynamically form agreements with CSPs to allow them to enhance either their own services or the quality of service offered to verticals (e.g. CDN providers).

- "Voice of the customer"

Resource providers indicate that they need to sign contracts with CSPs manually. Service provisioning and license renewing operations are complex, error prone and time consuming. They also claim that honesty in providing recommendations on the resources used is not always feasible, so they might not be trusted by some CSPs.

- Mapping the 5GZORRO platform

Automation (and trust) provided by the 5GZORRO platform is a key benefit for the resource providers that decide to participate to the 5GZORRO Marketplace and platform ecosystem.

The 5GZORRO platform gives the possibility to improve the efficient and effective use of resources, especially in cases where the provider has spare resources not used for its own services/products, as these will be the resources to publish in the marketplace catalogue. Thus, the resource provider exploits all its infrastructure without hindering their internal processes/applications.

Moreover, security mechanisms are applied in the 5GZORRO platform in order to be sure that a resource consumer will not harm the resource provider (and vice versa).

The 5GZORRO platform mechanisms for on-demand discovery include better promotion of resources that are highly rated, according to the satisfaction that other parties had with them previously. This is a nice benefit for good compliants.

Besides, when shared resources/infrastructures are offered to the consumers through the 5GZORRO platform, proper resource isolation and separation mechanisms are in place to minimize interferences in concurrent use of these resources.

- 5GZORRO platform Value Proposition for a resource provider

"A resource provider is prompted to dynamically rent its unexploited resources in order to increase its revenues. Generally, the infrastructure provider may own a number of resources that are not utilized for an extended period of time. Thus, it is possible that it would prefer to have the option to lease part of its unexploited resources, so as to take full advantage of them. This is achievable with the proposed 5GZORRO system, where the leasing of resources is automatically and dynamically realized, without hindering the 3rd party network operation"

Figure 95: Screenshot of a phase of the VPC exercise

4.2.2.4. 5GZORRO value proposition for the Telco operator

On the 5th of October 2022, partners participated in a workshop organised by the HRB experts. In this workshop, and building on the previous exercises that reflected about the Value Proposition in the three UCs, partners discussed about the main value 5GZORRO provides to the telco operator.

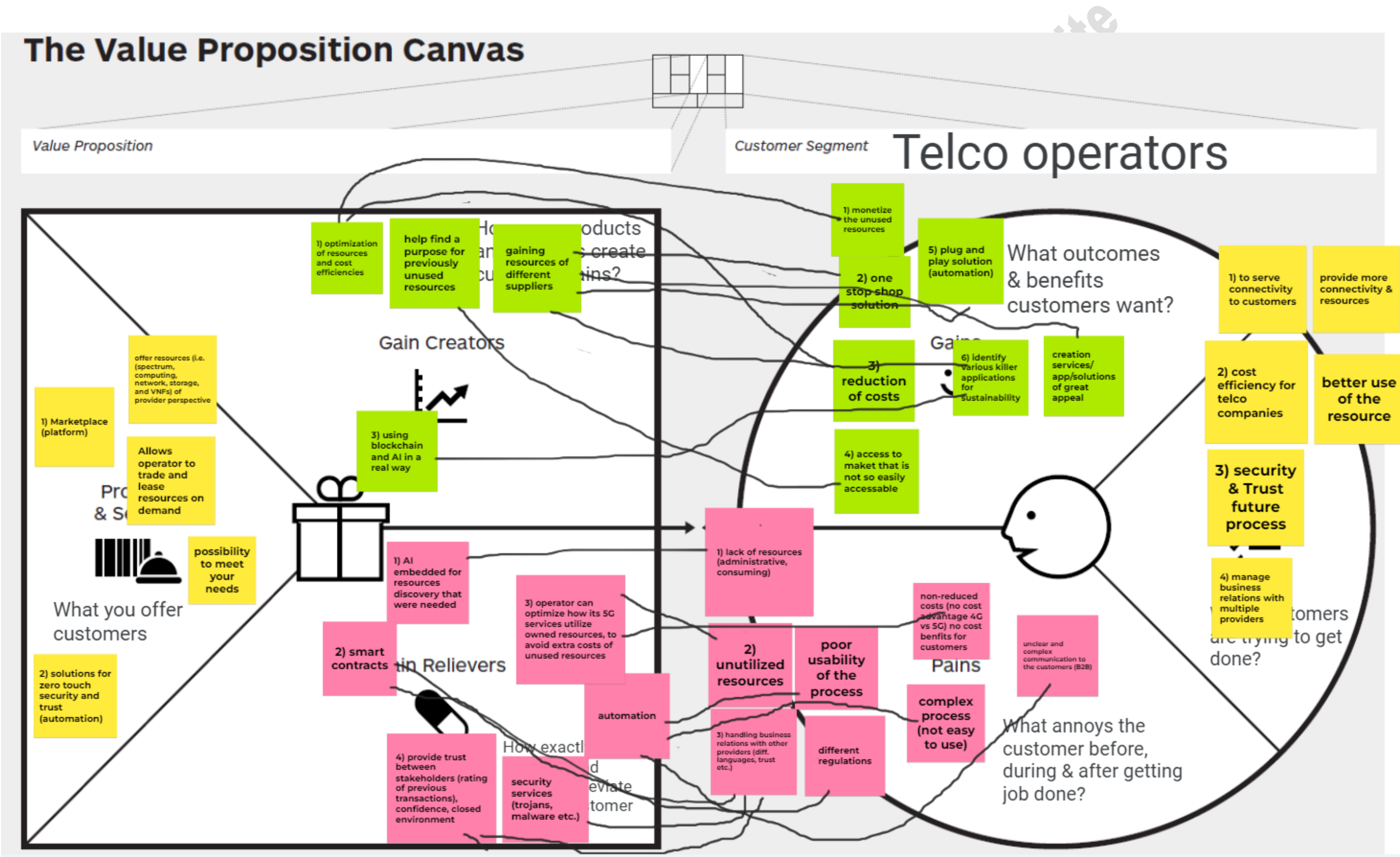


Figure 96: Screenshot of the VP exercise done with the HRB experts

Figure 97: Screen shot of the VP agreed in the HRB workshop

It becomes quite clear that our unique selling proposition for telco operators is that operating and trading resources in the 5GZORRO Marketplace will decrease their total cost of ownership. We will be able to quantify it after the collaboration with MCA in the development of 5GZORRO MVP, as explained in D6.5 [1].

4.2.3. 5GZORRO business canvas blocks

Once the consortium has a clear idea of who can benefit from the 5GZORRO platform ("Customer Segments") and what are the main benefits these customers segments can get ("Value Proposition"), we move to the other blocks of the canvas to analyse the different activities needed to provide a technological platform to match a demand and supply side and facilitate transactions between these sides, so that the customers get these benefits (5GZORRO Marketplace). Equally important is to reflect upon where associated costs lie and the possible sources of revenue. Ultimately, the consortium aims at demonstrating that a profitable business can emerge from 5GZORRO project results, maintaining costs below revenues.

This exercise was also validated with the HRB experts, using the lean canvas approach, which encompasses the different business model canvas blocks, also adding some reflections about the key metrics and the unfair advantage.

Key Activities

To operate the 5GZORRO platform, its software needs to be maintained, bugs and issues have to be fixed and new functionalities added attending to the marketplace participants' requirements. In some cases, we foresee some kind of customization activities to integrate with customers' legacy systems and also standardisation tasks to allow the platform set up an interface with other vendors' components. There will be installation work needed to onboard a new participant and work to be done when a participant decides to exit that cannot be overseen. Marketing activities, like promotional videos, recorded webinars for training sessions, organization of events etc. are also planned if we want to get more players onboard and maintain our customer base. Also important will be the management of the customers' relations to attend their needs and give prompt solutions to their requests.

Figure 98: Screenshot of a phase of the BMC exercise

Regarding IP of the platform, this is made of different components and each of these components is owned by one or more project partners. The party that is willing to operate the platform should secure its IP talking with these partners and agreeing on the model to be able to exploit it, in other words, managing partners' relations (this has been discussed as part of T6.3 activities).

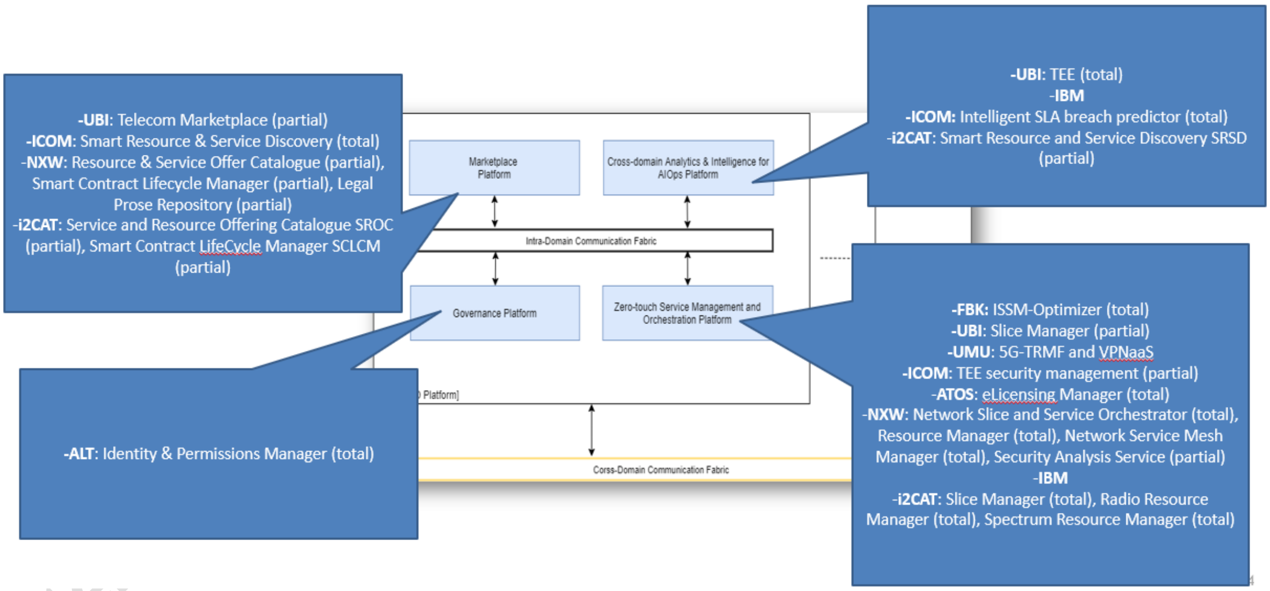


Figure 99: 5GZORRO platform modules and components, with ownership

Other activities foreseen are the legal activities and needed authorizations related to the regulator role.

When we identify the "platform management" activity, we are thinking of the role leading and coordinating all these necessary activities and monitoring the performance of the platform to take informed decisions.

Key Resources

The first thing we need to run the platform is the 5GZORRO platform software itself. Depending on the customer role, the list of components to be installed will vary. In any case, there are some components that are centralised (DLT, Datalake, Smart Resource and Service Discovery and Intelligent SLA Breach

Predictor) and precisely for these components, we will need servers where we can have this software installed. To have the software maintained and to introduce new required functionalities or customizations, we will need technical staff, the number of people will vary depending on the amount of the transactions in the marketplace. Personnel in charge of the business development activities will also be needed, as the marketplace should be populated to attract new players. Personnel will need of course material for the day to day business and, with respect to public and private funding, we assume that we will need this funding in the early stages to propel the business. We are doing this exercise precisely to get investors' attention and demonstrate that it is worth investing in this solution.

Figure 100: Screen shot of a phase of the BMC exercise

Key Partnerships

It is foreseen that some kind of partnerships will be needed in order for the marketplace to be a vibrant community. The consortium has been discussing about the preferred way to run the business model. We foresee a neutral entity (5GZORRO platform operator) that pays for the different activities needed to run the marketplace (hosting the centralized components, tech/maintenance support, marketing, e-payment platform, etc.) and charges the marketplace players a fee to compensate these costs.

Figure 101: Screen shot of a phase of the BMC exercise

<u>Channels</u>

The online channel will be the common way to communicate with potential players and to interact with already engaged parties and partners. A web site, as well as the email, will be the preferred tools. Marketing partners will have also to maintain social media accounts to convey relevant content and keep followers engaged. Key partners' own channels and networks will also be a good way to create awareness and raise curiosity. In a second phase, when the potential marketplace player is already engaged, physical meetings will be necessary to define needs and requirements and, ultimately, close agreements.

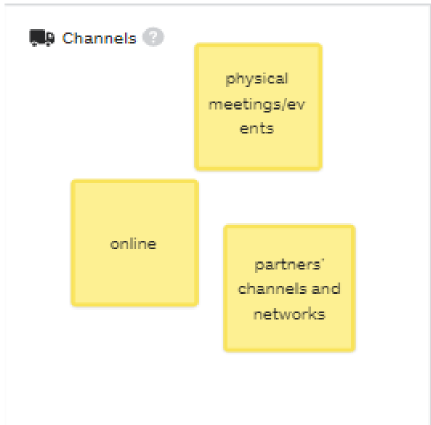


Figure 102: Screen shot of a phase of the BMC exercise

<u>Customer Relationships</u>

Partners have reflected here about the type of relationship each Customer Segment expects us to establish and maintain with them, as the type of customer relationships influences the overall customer experience. Long-term relationships are expected with a mix of automated services (that can recognize individual customers and their characteristics, and offer information related to orders or transactions) and personal assistance that can be through physical meetings, calls or by e-mail. Partners also recognize user communities as a good way to become more involved with customers and to facilitate connections between community members.

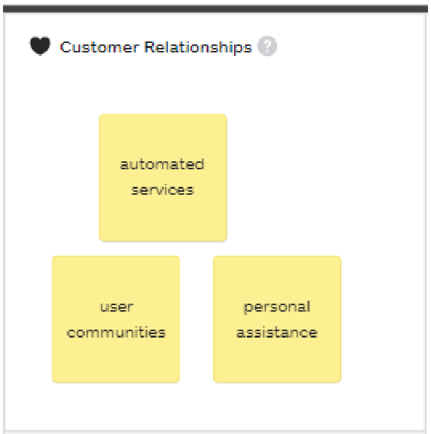


Figure 103: Screen shot of a phase of the BMC exercise

<u>Cost Structure</u>

First costs to consider are the ones related with the needed hardware, as some of the components of the platform need to be hosted centrally, so we will need a cloud provider for this. Installation costs to onboard a new participant should also be in scope. The 5GZORRO platform components will be released under an opensource licence, namely Apache 2.0, but this does not mean that the software cannot be monetised. Some of the partners may choose to package their software adding some extra functionalities and exploit it with some cost associated (this is a discussion of T6.3).

General business costs (cost of energy, office rent, material for the day to day business), personnel, events fees and travel costs should also be taken into account.

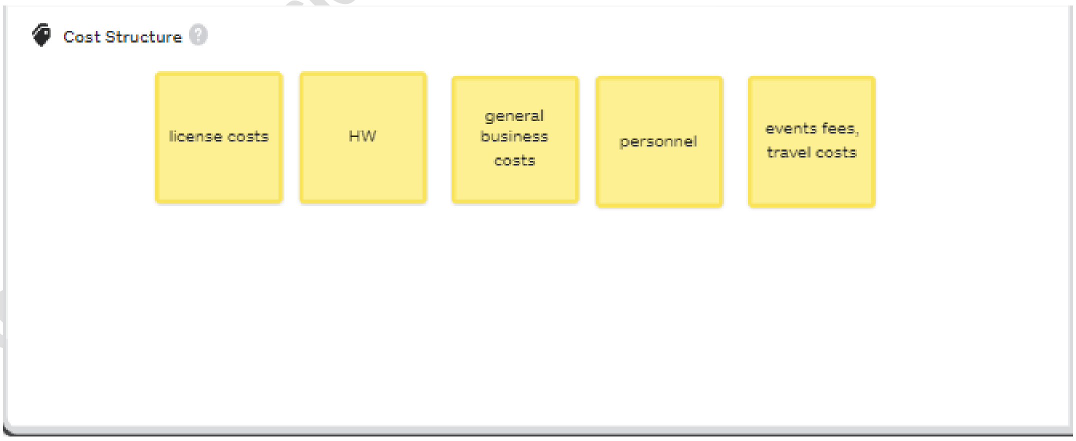


Figure 104: Screen shot of a phase of the BMC exercise

<u>Revenue Streams</u>

This is a critical part. We have reflected about the needed activities and resources, acknowledging there is a cost associated to them. Now we need to reflect about the possible sources of revenue that can compensate these costs, otherwise, the business will not be profitable.

Partners basically see two different sources for revenue. The main one is the fee that the participants in the marketplace will be requested to pay for trading resources, but we can also consider some placeholders for paid advertisement when the marketplace is more mature. Additionally, there can be another source of revenue in consultancy fees for integration with customers' legacy systems or other kind of customizations needed.

So, it is clear for us that the players in the marketplace will have to pay for trading in this space. The partners have been thinking about the details with the help of a questionnaire and, consequently, in a dedicated session devoted to discussing about the responses obtained.

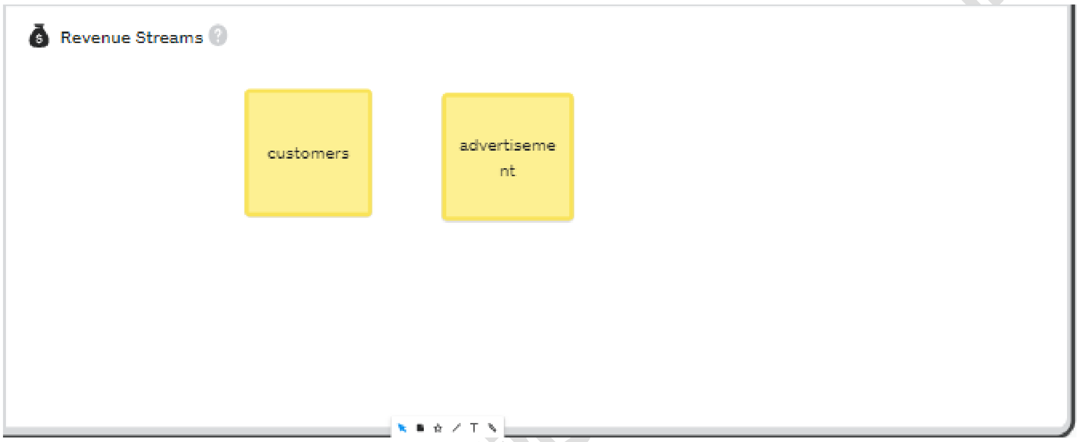


Figure 105: Screen shot of a phase of the BMC exercise

- <u>Who would pay for taking part?</u>

There were three choices for this question: only the founding members of the 5GZORRO Marketplace, only new members (entering to trade in the marketplace) or that paying or not should depend on the role members take. The rationale behind this last choice is that marketplaces become more attractive because as they grow bigger, they get stronger, with network effects that drive long lasting and high margin growth. So, if resource providers, for example, do not have to pay a fee, but can benefit from trading with their resources, then enrolling in the marketplace will be very attractive for them. If the marketplace gives the possibility to choose among a wide range of offers from a variety of resource providers, it will be attractive for resource consumers, that will be willing to pay for this possibility.

The majority of the partners think that one role in the marketplace could enrol for free (at least pay less) as the marketplace needs to be populated quickly with resources to be attractive for others, followed very closely by the ones thinking that all players should pay.

- <u>What can they do in the marketplace?</u>

Partners were given two choices for this question. By paying for enrolling in the marketplace, the interested party can trade with resources and, besides, they can have access to educational material or a discount in the events that could be organized.

All the partners agreed on the first assumption, just trading resources with other players.

- <u>When will they pay?</u>

For this question, there were multiple options: pay at the moment of the enrolment, pay every month/year a flat rate, only pay when a transaction is made and, as final choice, pay a fixed fee every month/year and then a variable rate depending on the cost of the transaction (a percentage).

All the partners were in favour of the last option. Partners think that the first and second choice are easy to manage, but someone may not feel the value of being in the marketplace, whereas someone will abuse the resources. About the third option, they think this would be attractive for players, but the platform operator will not be certain to cover fixed costs.

Additionally, the consortium believes that there should be an exit fee if the participant decides to step out before the date agreed, as onboarding a new participant is a costly process not worth investing in for a short period of time.

- How can we estimate the fee(s)?

For the estimation of the fee, the consortium is relying on the potential customers' willingness to pay. The economic value the players can perceive when enrolling in the marketplace can be calculated (i) comparing costs of their activities with or without 5GZORRO to calculate savings and estimating new revenues and also by (ii) calculating the fixed costs of running the platform. Additionally, the survey "Towards a dynamic marketplace for 5G resources" is asking respondents if they would consider purchasing use or access to such a marketplace service, so this is also a good indicator to calculate the fee.

- Would there be any incentive?

About incentives, half of the partners think players should pay after a number of transactions. The other half is equally divided between those who think players should pay after a trial period and those who would prefer a discount increase on the variable rate related to an increase in continuous period of members' subscription.

On the 7th of October 2022 took place the second workshop with the HRB experts about the business canvas and exploitation roadmap activities. In preparation for this workshop and building on the previous reflections with the project partners, T5.4 leader prepared the lean canvas shown below.

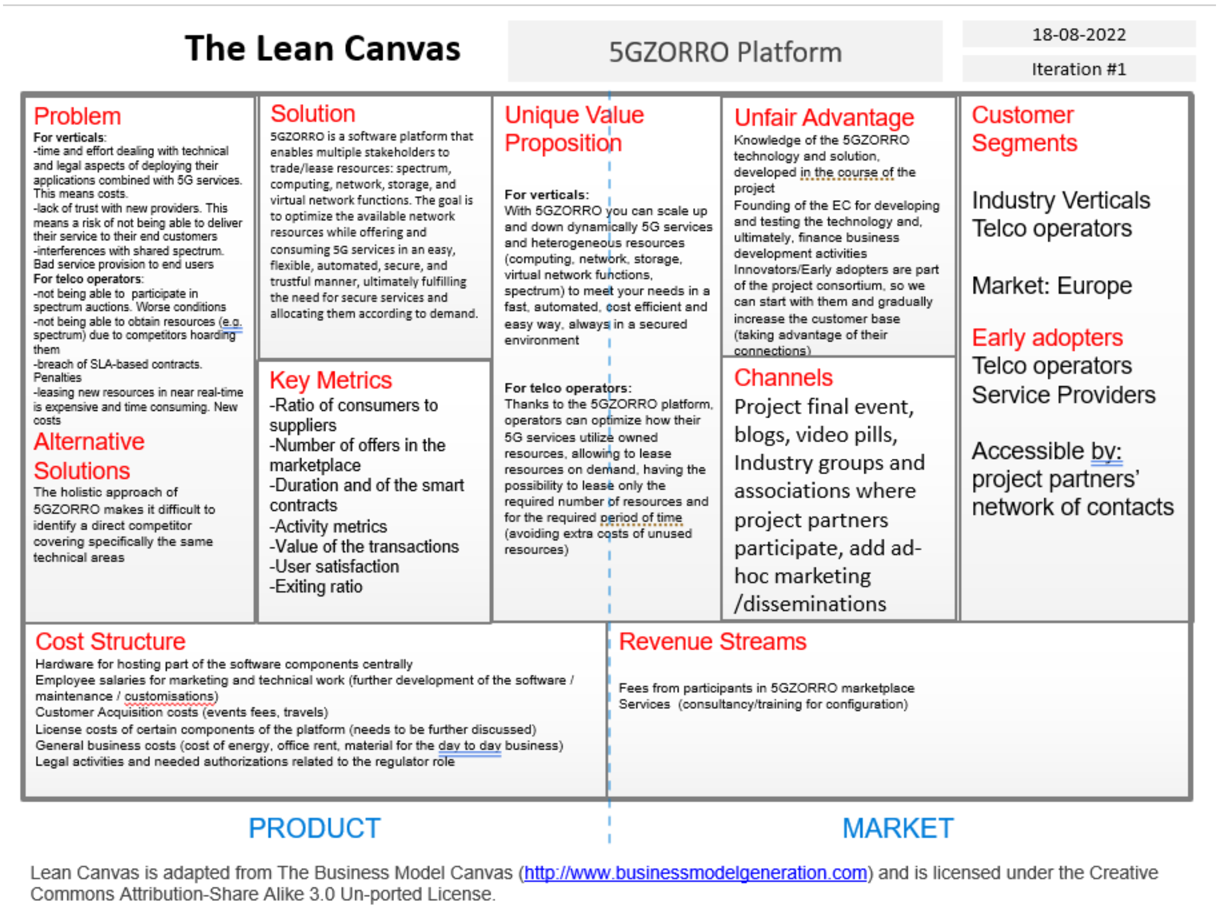


Figure 106: Screenshot of the lean canvas presented to the HRB

The lean canvas approach brings to the discussion an important aspect when planning the development of a product, the Key Metrics. The Key metrics are a set of indicators to monitor the progress of the business to know whether it is off to a good start, when it is thriving, when it is struggling, and how and when to intervene to get it back on track.

Partners discussed about it in a dedicated call and acknowledged that the marketplace will only thrive if there are enough offers in the catalogue and they are contracted at the right time for the cycle to start again. Therefore, having resources that are not tied up for a long period of time is essential for this wheel to turn healthily. In relation to this, partners are sharing some reflections for the moment the MVP is developed and the business is running:

- Ratio of consumers to suppliers needs to be balanced (50:50s, 60:40s, 70:30s at worse)
- Offers need to come in steadily from a number of suppliers (no significant dominance in the supply chain)
- Duration of smart contracts and their lifecycle dictates the pace of supply and consumption feed
- Activity metrics, i.e. how long a participant (consumer/supplier) has been active in a given time and their inactivity is a good indicator to visualize
- Value (in monetary terms) of deals/smart contracts is also important along with the frequency and quantity of deals. However, we also acknowledge that low-value orders with a fast delivery time could be also a good business
- The number of exiting participants is also a metric to consider

As described by the Marketplace Academy [51], KPIs to be measured should come from different perspectives of the business, a good approach would be to monitor usage of the marketplace, transactions made (probability of a visit leading to a transaction, supplier-to-consumer ratio, repeat purchase ratio), business metrics related to revenue, profitability, and customer acquisition as well as user satisfaction metrics.

This input fuelled the discussion on the business model for 5GZORRO platform with the experts, being it the needed first reflection for the exploitation roadmap in T6.3.

4.3. Technoeconomic Analysis

4.3.1. Scope

In D6.4 [18], the consortium analysed the industrial ecosystem where 5GZORRO results could potentially impact, highlighting how 5GZORRO can address operators' concerns about high investments in terms of capital and operational expenditures. Big market players [22] acknowledge that to cope with capacity and coverage needs in the 5G/6G era, CSPs will need to consider new ownership models to reduce cost and make 5G deployments feasible, underlining the relevance of resources sharing. According to McKinsey [23], *"operators have been able to reduce the total cost of ownership by up to 30 percent while improving network quality through sharing a variety of both active and passive equipment".*

An updated view of the market trends in D6.5 [1], reveals that disaggregation, moving the network workloads to shared or public infrastructure, will make OpEx the key cost component for operators, which can be reduced by increasing automation and resource flexibility. Besides, disaggregation fosters the use of third-party platforms, and, in this kind of business relations, an increasing confidence in external services is needed. In 2021, TMForum [24] conducted a survey among CSPs and their suppliers concluding that many operators have already started to build digital ecosystems with partners, executing proofs of concepts and even launching limited marketplaces. Encouraged by 5G, IoT and edge technologies, many of largest carriers in the world have significant interest in becoming a telco marketplace, connecting telco assets, customer needs and partner capabilities in an ecosystem.

In section 4.2.1 of this deliverable, 5GZORRO platform is presented as a set of functionalities aligned with previous needs and market trends in support precisely of a telecom marketplace for sharing telco resources. 5GZORRO framework for smart contracts, and the application of AI-driven efficient and automated network operation across domains, has demonstrated that it can improve the usage of resources and ease pervasiveness of 5G services in the network, thus leading to reduce operational expenses. Then, we clearly conclude that there is a market opportunity around 5GZORRO. This assumption is also sustained by the results of the survey "Towards a dynamic marketplace for 5G resources" launched by the project in January 2022. As shown in the Annex I, the 83% of the telco operators that responded to the survey think that the possibility of acquiring or providing resources, such as edge-CDN or virtual network functions, based on actual needs, to meet temporary or location-specific requirements is attractive for them.

4.3.2. Calculations

As identified in section 4.2.3, there are certain costs involved if the platform is deployed in an operational environment and the marketplace is up and running with stakeholders involved in transactions. One of these costs is related with the IT infrastructure. The partners have been discussing how to calculate the IT resources needed taking into account the information at our disposal and the fact that the outcome of the project is a proof of concept and not an MVP, meaning cost calculation will be based only on assumptions. We concluded that the better approach was to take the configuration of one of the project's testbeds, specifically 5GBarcelona (see section 2.1.1), since this configuration has permitted us to achieve the agreed values of the technical KPIs and also the platform operation by different types of stakeholders.

Considering a local deployment of the platform, in a potential business setting, we can foresee that one Regulator and two or three operators could enrol in the 5GZORRO Marketplace. Additionally, several other resource providers, offering computational capacity and network functions could also be expected.

According to the 5GBarcelona testbed architecture, which has been dimensioned for one Regulator and three operators, there are five physical servers for hosting the software and needed services: 2 compute nodes and 3 nodes dedicated to the controller. If the deployment option were to use physical servers, 5GZORRO platform would need 80 CPUs and 256GB RAM. Additionally, the numbers for 1 controller (3 for high availability) as reported from 5GBarcelona would be 12 vCPUs, 96GB RAM and 2 disks SSD 931GB. But the option of physical servers will require, additionally, a dedicated team for OpenStack installation and configuring, as well as a controller. In order to facilitate the operation of the platform at the beginning, avoiding high CapEx investment, our option has been to go for a cloud environment, so that we pay more on a monthly basis but get all these configurations done. In consequence, and based on our calculations, the resources needed (compute nodes) for operation of the platform by one Regulator and three operators will be 104 CPUs and 218GB RAM. As for the disk, we calculate that 4TB will be enough.

Once we have clarified these infrastructure requirements, we have matched the figures with the list of deployed components per profile and the resources needed for these components. As a result, we have been able to estimate the percentage of CPU, RAM and disk needed for each profile.

Stakeholder	Resource Provider A /Admin		
Location	BCA		
Description/Platform Actions			
Lists RAN and 5G core resources on the Marketplace Fills and attaches SLA, in theory also eLicense			
Component	**Resources**		
	CPU	RAM	Disk
Kafka			
Portal	2	6	20
LPR	1	2	
eLM	0.5	0.5	1.5
RSOC			
xRM	4	6	10
ID&P	0.5	1	10
SCLCM	1	2	5
SRSD	8	16	100
DLT node	4	2	10
DLT services	6	8	20
ISSM	12	12	1500
NSSO	2	8	20
TRMF	1	1	10
Intrasecurity	2	2	20
Datalake	10	20	210
ISSM Optimizer	0	0	0
MongoDB	1	1	
RabbitMQ			
NFVO			
MDA	0.5	2	0.2
NSMM	2	4	10
VPNaaS	2	2	10
SLA-M			
Totals	**59.5**	**95.5**	**1956.7**
	CPU	RAM	Disk

Stakeholder	Resource Provider B		
Location	BCA		
Description/Platform Actions			
Lists Edge resource on the Marketplace Fills and attaches SLA, in theory also eLicense			
Component	**Resources**		
	CPU	RAM	Disk
Kafka			
Portal	2	6	20
LPR	1	2	
eLM	0.5	0.5	1.5
RSOC			
xRM	4	6	10
ID&P	0.5	1	10
SCLCM	1	2	5
SRSD	8	16	100
DLT node	4	2	10
ISSM	12	12	1500
NSSO	2	8	20
TRMF	1	1	10
Intrasecurity	2	2	20
ISSM Optimizer	0	0	0
MongoDB	1	1	
RabbitMQ			
NFVO			
MDA	0.5	2	0.2
NSMM	2	4	10
VPNaaS	2	2	10
SLA-M			
	43.5	**67.5**	**1726.7**
	CPU	RAM	Disk

Stakeholder	Resource Consumer/ Service Provider C		
Location	BCA		
Description/Platform Actions			
Does not have resources, does have VNFs Purchases resources and creates a ns offer comprised of RAN, core, Edge, and VNF Creates a Service order			
Component	**Resources**		
	CPU	RAM	Disk
Kafka			
Portal	2	6	20
LPR	1	2	
eLM	0.5	0.5	1.5
RSOC			
xRM	4	6	10
ID&P	0.5	1	10
SCLCM	1	2	5
SRSD	8	16	100
DLT node	4	2	10
ISSM	12	12	1500
TRMF	1	1	10
Intrasecurity	2	2	20
NSSO	0	0	0
ISSM Optimizer	1	1	
MongoDB			
RabbitMQ			
NFVO	0.5	2	0.2
MDA	0.5	2	0.2
SLA-M			
	38	**55.5**	**1686.9**
	CPU	RAM	Disk

Stakeholder	Regulator		
Location	BCA		
Description/Platform Actions			
Approves Stakeholder onboarding request			
Component	**Resources**		
	CPU	RAM	Disk
Kafka			
Portal			
RSOC			
ID&P	0.5	1	10
	0.5	**1**	**10**
	CPU	RAM	Disk

Figure 107: List of deployed components per profile and resources needed

To make a cost estimation of this configuration, the consortium has consulted MS Azure pricing calculator, obtaining the following results with the testbed configuration (1 Regulator, 3 Operators):

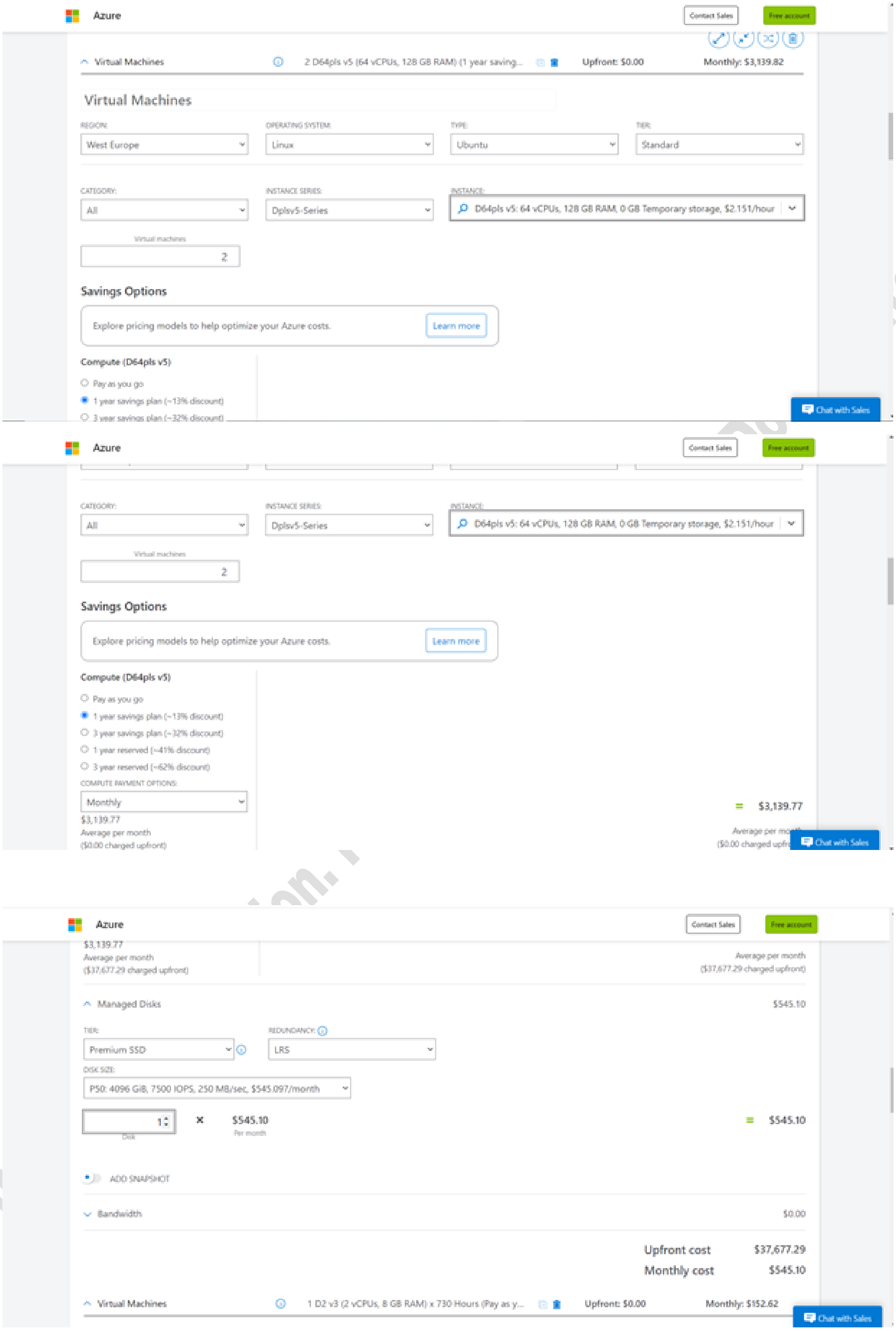


Figure 108: Some screenshots of MS Azure when calculating infrastructure costs for 1 Regulator and 3 Operators

This means that the infrastructure cost for hosting one Regulator and three operators A, B and C will be 37.677,29$ + (545.10$ x 12) = 44.218,49$ per year or 3.684,87$ per month. Prices are given in US Dollars, but the request was made on the 27th of October 2022, when the exchange rate was 1:1, so we take the same figures for the calculation in Euros, 44.218,49€ per year or 3.684,87€ per month.

Similarly, we calculated infrastructure costs individually for Operator B and Operator C in order to calculate these costs for enrolling a new operator in the platform. Operator A holds the role of the administrator, so there will be no more than one of this type and there is no need to calculate enrolment costs.

Microsoft Azure Estimate						
Your Estimate						
Service category	Service type	Custom name	Region	Description	Estimated monthly cost	Estimated upfront cost
Compute	Virtual Machines		West Europe	1 D48pls v5 (48 vCPUs, 96 GB RAM) (1 year savings plan), Linux, (Pay as you go); 1 managed disk – P30; Internet egress, 100 GB outbound data transfer from West Europe routed via Microsoft Global Network	$148.68	$14,127.08
Compute	Virtual Machines		West US	1 D2 v3 (2 vCPUs, 8 GB RAM) x 730 Hours (Pay as you go), Windows (License included), OS Only; 0 managed disks – S4, 100 transaction units; Inter Region transfer type, 5 GB outbound data transfer from West US to East Asia	$152.62	$0.00
Support			Support	0	$0.00	
			Licensing Program	Microsoft Customer Agreement (MCA)		
			Billing Account			
			Billing Profile			
			Total	301.3	$14,127.08	

Figure 109: Export of infrastructure costs calculation from MS Azure for one Operator B

The cost structure in section 4.2.3 reveals that we should also consider other costs. License costs have been discarded at this point, although this should be reassessed when creating a product out of the prototype. However, typical business costs and salaries are also included in this analysis. Our estimation is that one technical person part time could cover the necessary technical activities to operate the platform and another person for marketing and business development activities. That would make a total cost per month of approximately 4000€, as shown in the table below. Costs have been calculated on a monthly basis. In a real setting scenario, CapEx costs derived from running 5GZORRO platform may have to be taken into account and distributed monthly over the years depending on assets life time.

Table 38: Costs for operating the platform in the testbed setting

Cost Category	Price/month
Infrastructure	3.684,87
Salaries	4.000
Business operation/other indirect costs	200
Total(€)	7.884,87
	Price/year
Total(€)	94.618,44
Rounded down to the nearest whole value(€)	94.618

For revenues calculation, we need to estimate market size. In our prototype configuration, we have three operators (one of them taking the administrator role) and one regulator. This could be the average estimation, taking into account the number of operators in European countries [52] (Italy: 4, UK: 4, Greece: 3, Germany: 3, Portugal: 3, Spain: 4, France: 4) and the willingness to pay that we foresee based on 5GZORRO value proposition, market figures (see Scope in section 4.3.1) and the input of the survey.

On top of the fixed costs, we have decided that a 5% profit margin to cover initial investment will be applied. This initial investment is needed to create an MVP out of our prototype, as the exploitation roadmap in D6.5 [1] describes. From this final figure, we are able to derive the price the marketplace members in this configuration would have to pay to make the business sustainable. Discussions among partners and results of the survey indicate that the regulator will join the platform free of charge, although it generates some costs, but lower than those generated by other types of platform participants. Partners also discussed if the price should be linked with the costs each type of participant generates, but finally, and for the sake of simplicity, we decided to put the same price for all of them. It should not be forgotten that, in addition to this flat price, partners also expect that a percentage of the costs of the transactions carried out in the marketplace can be taken and, therefore, this will have to be added to the final profit. Additionally, as indicated in section 4.2.3, customization and customers' technical support activities can be also monetized.

Table 39: Calculating the price for stakeholders enrolling the platform

Type of Stakeholder	Number
Op A (Admin)	1
Op B (resource provider)	1
Op C (resource consumer)	1
Regulator	1
Financials	
Number of paying stakeholders	3
Fixed Costs (infra+other)(€)	94.618
Margin(€)	4.730,9
Total to cover(€)	99.348,9
Revenue from each(€)	**33.116,3**

4.3.3. Evaluation

In the scenario that we are considering, we assume 15.000€ of initial investment that will be needed to transit from the prototype at the end of the project to the MVP (this is something analysed in the context of the exploitation roadmap in WP6, in the exploitation roadmap). We foresee also that it can easily be three participants in Y1, five in Y2 and seven in Y3. With these numbers, and the costs calculated in previous step, we are able to estimate the payback period with the help of a model created.

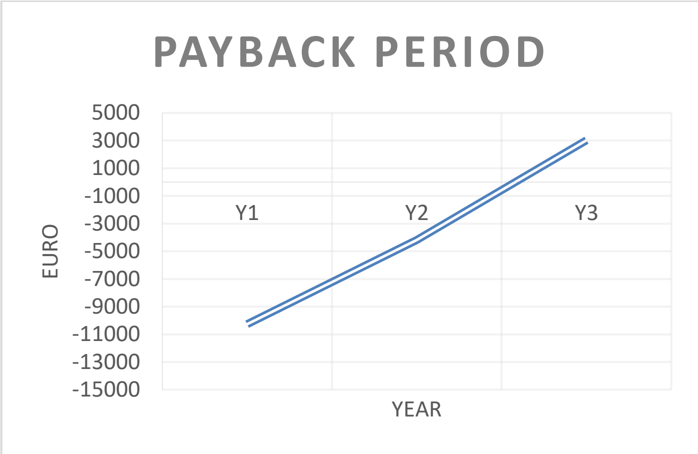
Payback period on an investment is the amount of time it takes to save the amount of money initially invested. As we foresee uneven cash flows over the years, due to the fact that we expect an increasing number of participants and, therefore, more costs but also more revenue, we cannot apply the formula that divides the initial investment by the annual cash flow. Instead, we need to calculate the cumulative cash flows for each period, as we have done in the excel model, and then represent it in a graph.

Table 40: Projections of a most probable scenario

	Y1	Y2	Y3
Op A	1	1	1
Op B	1	2	2
Op C	1	2	3
Regulator	1	1	1
Number of stakeholders	3	5	6
Fixed Costs (infra+other) (€)	94.618	121.736	144.150
Margin (€)	4.730,9	6.086.8	7.207.5
Total to cover (€)	99.348,9	127.822.8	151.357.5
Revenue from each (€)	33.116,3	25.564.56	21.622.50

Table 41: Calculation of payback period in the most probable scenario

Year	Cash Flows (€)	Cumulative (€)	Payback Period
0	-15.000	-15.000	
1	4.730,9	-10.269,1	
2	6.086,8	-4.182,3	2,58
3	7.207,5	3.025,2	



In conclusion, taking into account that the initial investment will be covered with the margin, the excel model reveals that, in this exercise, it will take slightly more than 2,5 years to recover this money.

It needs to be noted that translating these initial calculations and the prototype to a market ready MVP will require iterations (as new costs will need to be covered) and a proper evaluation of different approaches of this model. In fact, there are several variables in the model that we can modify until we arrive at a configuration that the whole team, including the investment partner, agrees with. This exercise represents just an initial validation that, creating the MVP and operate it can be a profitable business.

This model allows us for example to analyse different variations on the profit margin and its consequences on the enrolment price and the payback period. Similarly, as the number of participants increase, one can opt for decreasing the flat price, taking into account that the revenues generated by the application of the percentage fee on the transaction will be higher, or, on the other hand, maintain the initial price and recover the investment earlier. The consortium has agreed that a good strategical business approach will be to reduce the flat price over the time. This means we will recover the investment later, but, alternatively, the marketplace will be more attractive, so that the point may be reached when the flat price will be residual. The consortium also thinks that the number of participants will increase rapidly. In this kind of ecosystem environments, the fact that one type of participants enrols, opens the door to other participants that feel attracted by the business opportunity of trading resources with them. And having more participants of this second type will, in turn, ease the engagement of new participants of the first type.

Performance analysis maps the economic and the technical calculations. In this analysis, economic calculations have been done in relation to the technical calculations made in section 2 of the document, where technical performance of the platform is evaluated for a specific configuration of the testbeds. When creating an operational product, the relation between cost and performance also should be carefully considered. This framework analysis that combines technical deployment, performance indicators, legal implications, costs and revenues will have to be used in an iterative way to find the adequate balance for a cost-effective solution.

4.3.4. Risk and Uncertainty

Partners acknowledge that the economic analysis is based on the project result (i.e., a prototype) and that a number of estimations have been done. Projections have been based on partners' educated guess, considering the data available and collecting input from different expert fora. However, the consortium believes that there are uncertainties that will need to be handled.

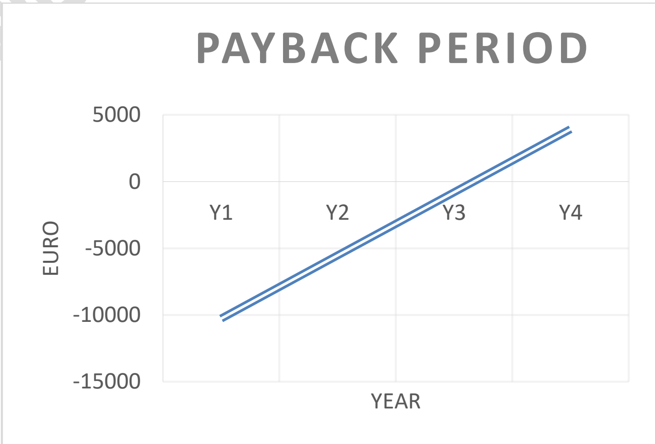
In the previous section, we have assessed the platform business-wise taking into account the most likely scenario, which in turn is based on market figures and the survey's input. We should also consider a scenario where there is low customer acceptance, or one competitor emerges that overperforms, with the consequence of no new participants enrolling in the platform over the time. There are other risks that may appear because of the current global economic uncertainties like the slowing growth, a high and persistent inflation, etc. or even linked with the team developing the MVP, which may exceed important resource constraints, such as the budget of the product development project.

Table 42: Projections of a pessimistic scenario

	Y1	Y2	Y3	Y4
Op A	1	1	1	1
Op B	1	1	1	1
Op C	1	1	1	1
Regulator	1	1	1	1
Number of stakeholders	3	3	3	3
Fixed Costs (infra+other) (€)	94.618	94.618	94.618	94.618
Margin (€)	4.730,9	4.730,9	4.730,9	4.730,9
Total to cover (€)	99.348,9	99.348,9	99.348,9	99.348,9
Revenue from each (€)	33.116,3	33.116,3	33.116,3	33.116,3

Table 43: Calculation of payback period in the pessimistic scenario

Year	Cash Flows (€)	Cumulative (€)	Payback Period
0	-15.000	-15000	
1	4.730,9	-10.269,1	
2	4.730,9	-5.538,2	
3	4.730,9	-807,3	3,17
4	4.730,9	3.923,6	



This will be the pessimistic scenario, where the initial investment would not be recovered until year 3. In our opinion this is a long period for recovering an investment. To minimize these risks, we have analysed an exploitation roadmap in WP6 and have started exploitation activities with an early adopter that is part of the consortium (Malta Communications Authority), evaluating the minimum set of functionalities (MVP) needed to start operating the platform. The fact that it is a member of the project has permitted us to start early to co-define these needs, in the context of the EU funding. This, together with the fact that MCA is a regulator, and, as a consequence, legal aspects have been well taken care of, provides us certainly a competitive advantage.

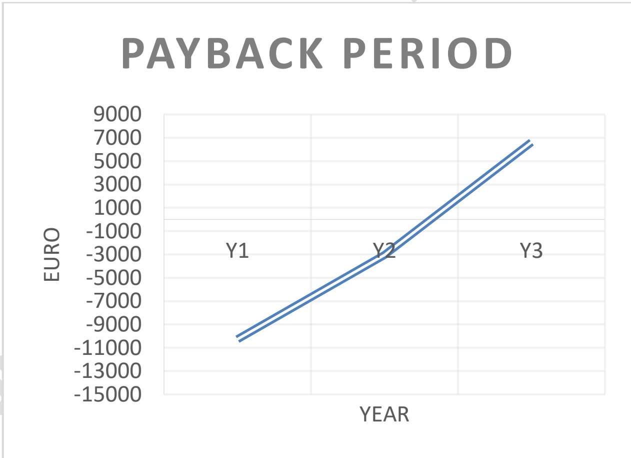
Given the uncertainty, it may be also reasonable to analyse an optimistic scenario, where new participants are progressively being registered.

Table 44: Projections of an optimistic scenario

	Y1	Y2	Y3
Op A	1	1	1
Op B	1	2	3
Op C	1	4	7
Regulator	1	1	1
Number of stakeholders	3	7	11
Fixed Costs (infra+other) (€)	94.618	144.150	193.682
Margin (€)	4.730,9	7.207,5	9.684,1
Total to cover(€)	99.348,9	151.357,5	203.366,1
Revenue from each (€)	33.116,3	21.622,5	18.487,83

Table 45: Calculation of payback period in the optimistic scenario

Year	Cash Flows (€)	Cumulative (€)	Payback Period
0	-15.000	-15.000	
1	4.730,9	-10.269,1	
2	7.207,5	-3.061,6	2,32
3	9.684,1	6.622,5	



In this configuration, the return of the investment will be after just over two years.

After having analysed these three scenarios, it worth highlighting that when developing the product, a detailed risk analysis should be done. Competition in the business environment has grown rapidly in recent years and companies try to be innovative by launching new products or services before the competition does. There is a lot of work behind this journey and allocation of resources should be done in an optimal way, rest assured the close collaboration among the different teams. In this context, it is easy to understand that many things can go wrong and, consequently, there are many risks to be managed. There are a lot of companies that develop new products, but only a few succeed in doing it correctly, the ones that are able to optimize not only the development process but the risk management behind it as well.

5. Conclusions

This deliverable has reported about the validation activities that partners have carried out to demonstrate that 5GZORRO platform is feasible from three distinctive perspectives: technical, legal and economic.

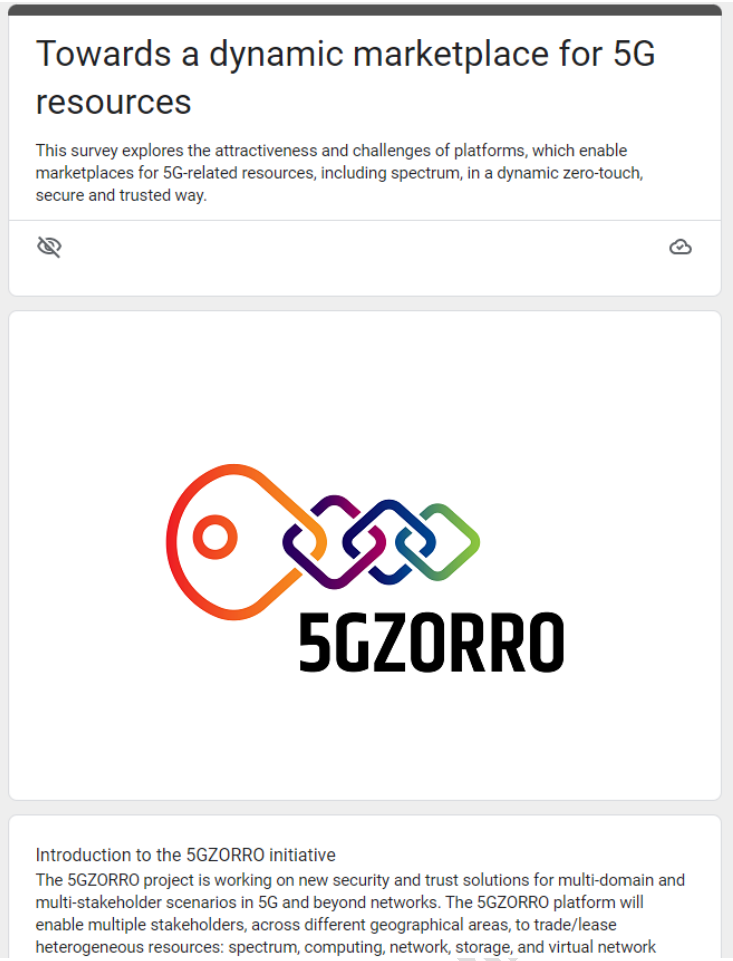
The work conducted has been based on the results we have obtained in the project, the 5GZORRO prototype applied to three different use cases and deployed in a testbed configuration. UC1 describes an Automotive Vertical which uses the platform to lease an E2E service composed by resources from multiple Providers that may not have a prior trusted relationship. It demonstrates how 5GZORRO facilitates the leasing of resources between them, the associated commercial agreements and how their lifecycles are governed in a decentralised manner. The consortium has produced a video that shows these interactions in different scenarios [8]. UC2 demonstrates the Marketplace capabilities to trade licensed spectrum resources, configure the RAN elements of the relevant network slices accordingly, and monitor associated SLAs for breach verification and correction. UC3 deals with a CDN service provider that leases a network slice instance from a CSP and, at a certain point, the CSP's edge infrastructure cannot meet the demand. The platform then triggers a resource discovery process in order to identify potentially usable 3rd party edge resources and rates them based on previous performance, trust and pricing. In the end, the platform extends the network slice to the 3rd party infrastructure, instantiating the service components on the new resources. All these platform capabilities have been tested and measured against defined KPIs, a summary of which is provided in section 2.5.

But the platform is not only capable of these technical functionalities, it is also legally compliant. The consortium has paid good attention to it, anticipating the deployment of the platform in an operational environment. European regulation on pillar technologies of the platform, like AI, Blockchain and Smart Contracts, as well as on digital marketplaces, radio spectrum and other telco services have been carefully screened to ensure that the platform can operate in the European market.

The business aspect has also been considered in order to technically develop a solution that is well received in the market because it addresses real problems and needs of stakeholders. In this sense, feedback from third parties, collected in the form of a survey (results in Annex I), as well as through the communication and dissemination activities of the project, has been carefully considered. In addition, the consortium has discussed possible ways to operate the platform to make it a profitable business and, to facilitate the task, has documented the process to automate the deployment and installation of all components depending on the profile of the user that enrols in the 5GZORRO Marketplace (information provided in section 2.6).

As a conclusion, we can state that 5GZORRO platform is ready to evolve into a market ready solution in the form of a minimum viable product (MVP), as it works from a technological point of view and, equally important, complies with legal aspects and solves real problems with a reduced investment. To get to that point and impact society and European industry, partners are defining the roadmap and related exploitation activities in the scope of WP6. The work done in this deliverable related to business and technoeconomic models is being taken as starting point, but will need to be iterated and adapted to new circumstances as the creation of the MVP progresses. The early adopters of the solution and their business plans explained in D6.5[1], will indeed smooth the process.

6. Annex I – 5GZORRO Survey



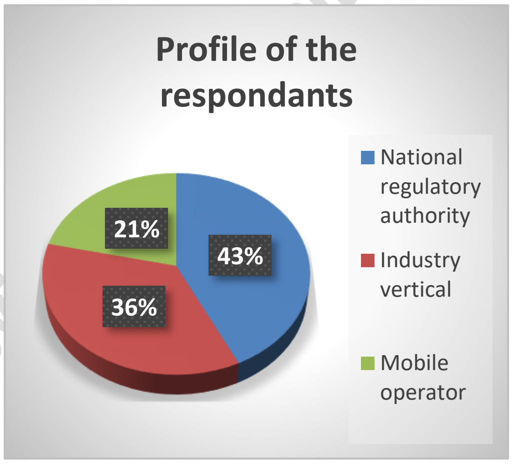
Towards a dynamic marketplace for 5G resources

This survey explores the attractiveness and challenges of platforms, which enable marketplaces for 5G-related resources, including spectrum, in a dynamic zero-touch, secure and trusted way.

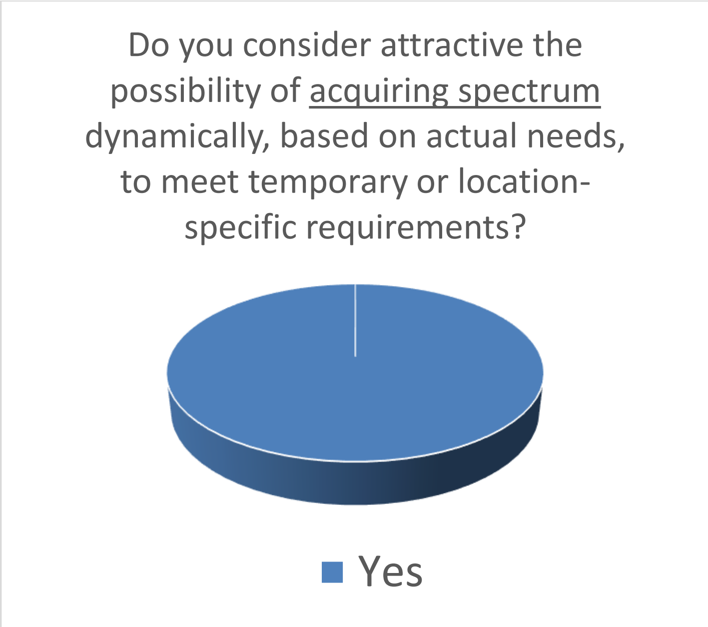
5GZORRO

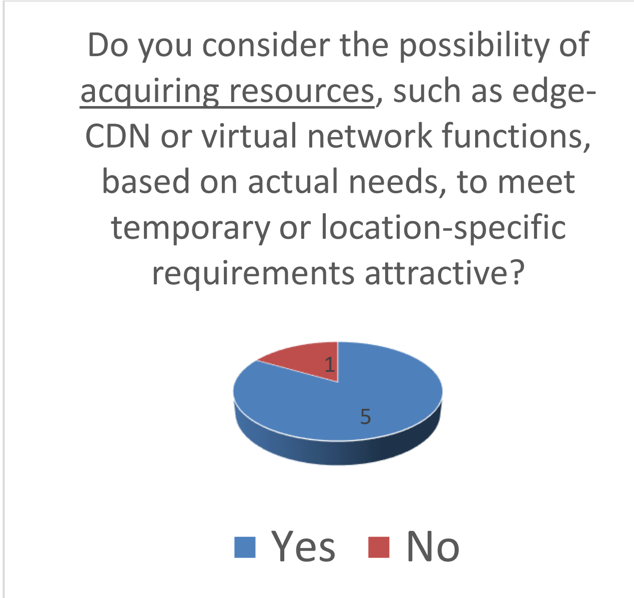
Introduction to the 5GZORRO initiative

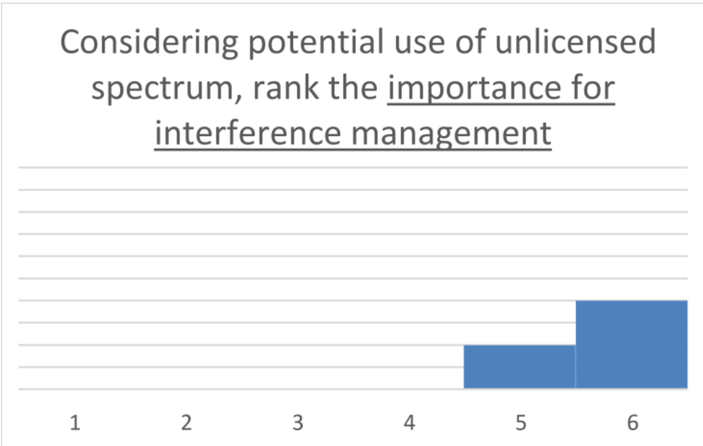
The 5GZORRO project is working on new security and trust solutions for multi-domain and multi-stakeholder scenarios in 5G and beyond networks. The 5GZORRO platform will enable multiple stakeholders, across different geographical areas, to trade/lease heterogeneous resources: spectrum, computing, network, storage, and virtual network

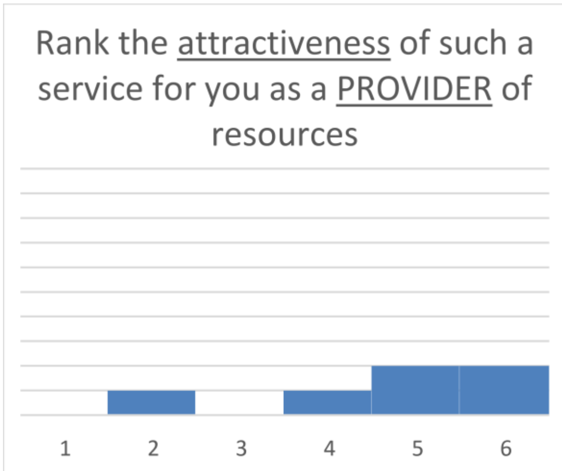


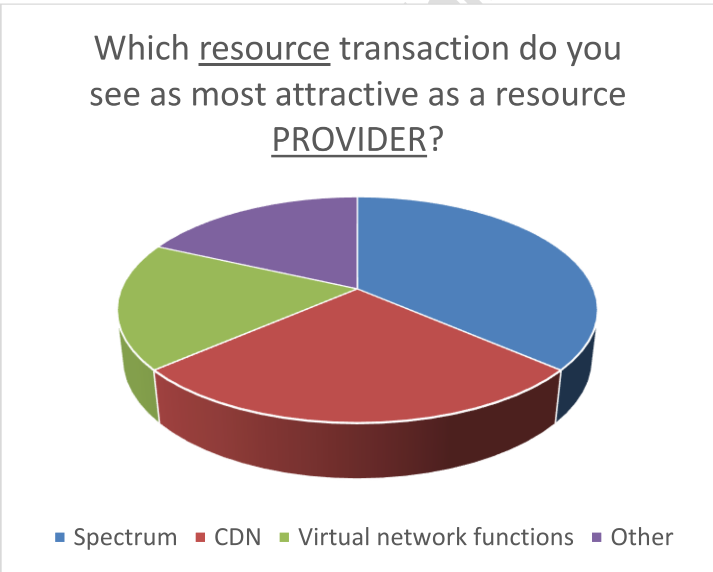
MOBILE OPERATOR

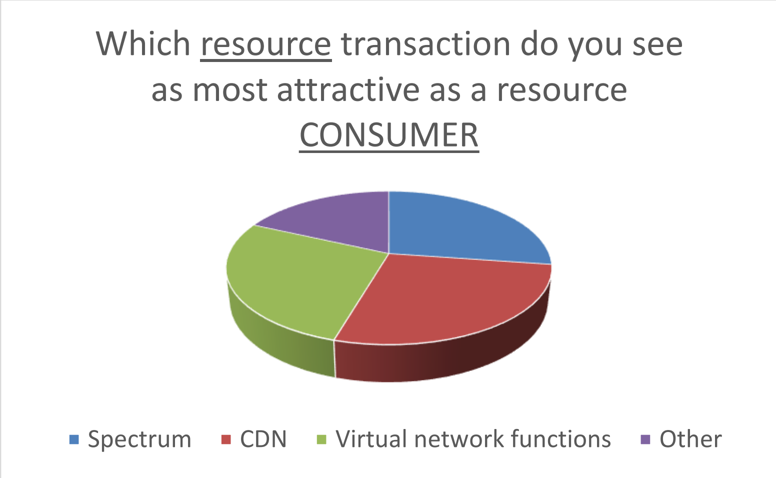

Do you consider attractive the possibility of acquiring spectrum dynamically, based on actual needs, to meet temporary or location-specific requirements?
Yes

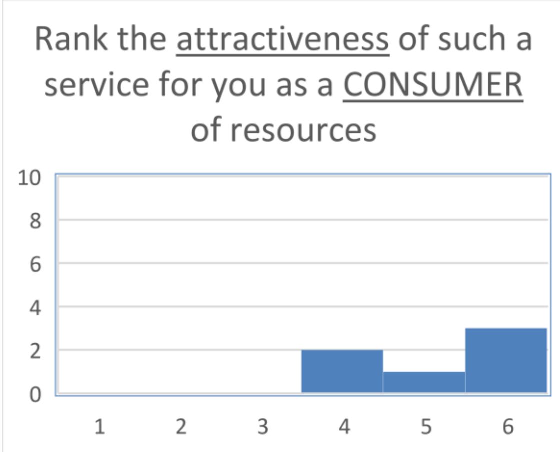

Do you consider the possibility of acquiring resources, such as edge-CDN or virtual network functions, based on actual needs, to meet temporary or location-specific requirements attractive?
1
5
Yes
No

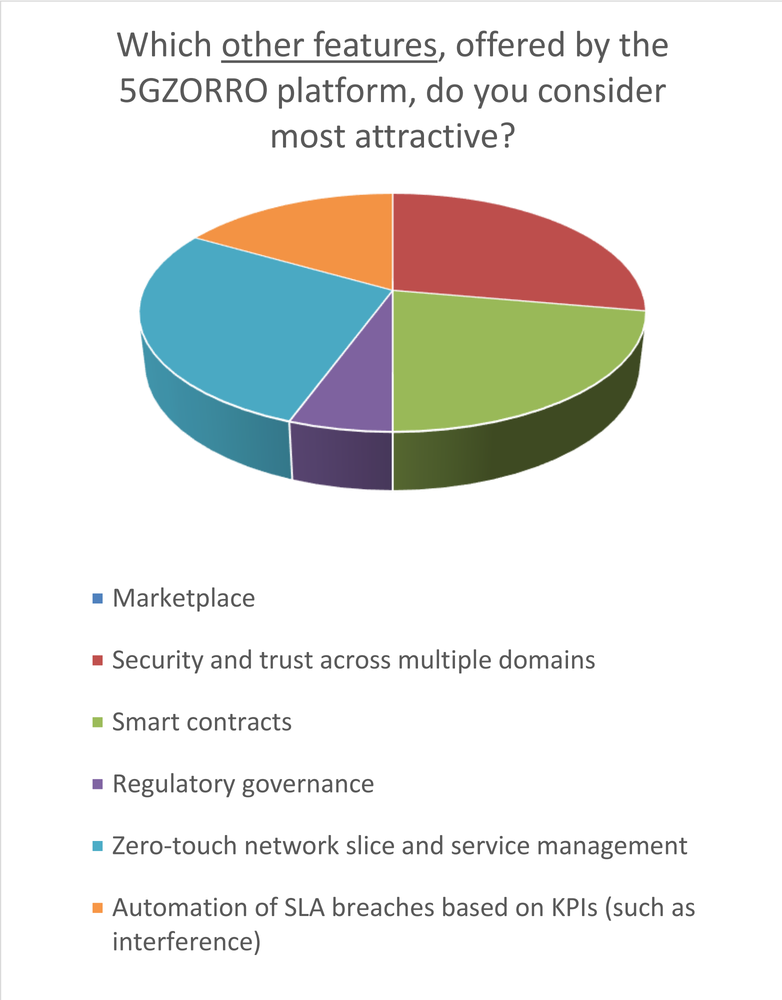

Considering potential use of unlicensed spectrum, rank the importance for interference management
1
2
3
4
5
6

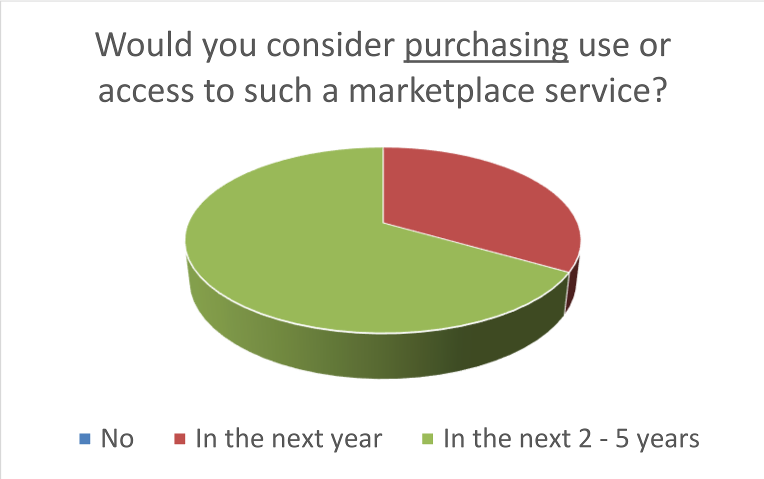

Rank the attractiveness of such a service for you as a PROVIDER of resources
1
2
3
4
5
6

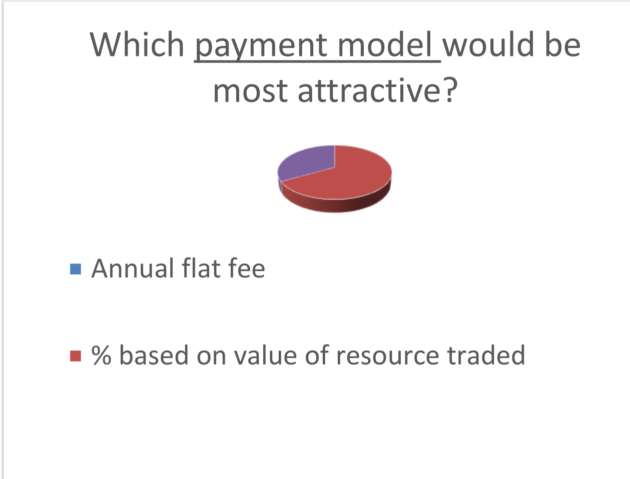

Which resource transaction do you see as most attractive as a resource PROVIDER?
Spectrum
CDN
Virtual network functions
Other

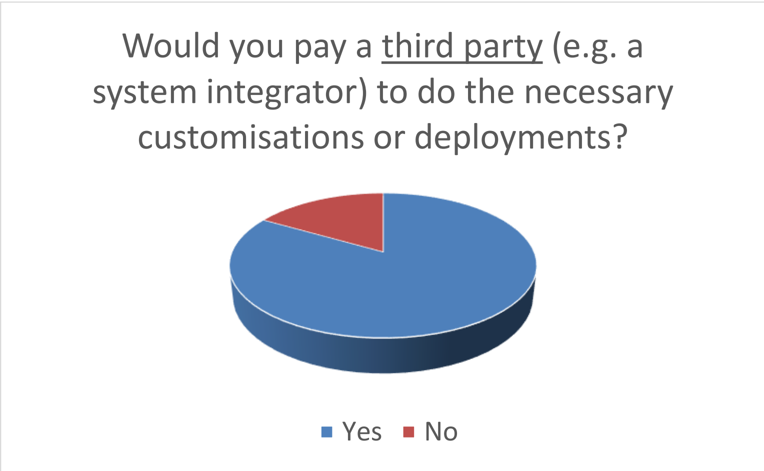

Which resource transaction do you see as most attractive as a resource CONSUMER
Spectrum
CDN
Virtual network functions
Other


Rank the attractiveness of such a service for you as a CONSUMER of resources
10
8
6
4
2
0
1
2
3
4
5
6

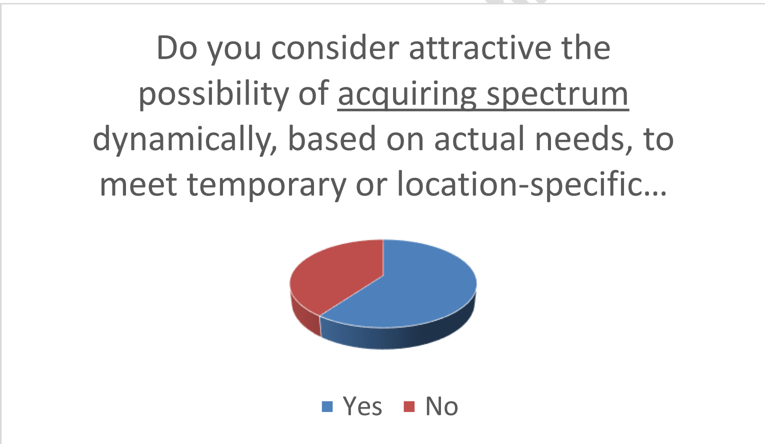

Which other features, offered by the 5GZORRO platform, do you consider most attractive?
Marketplace
Security and trust across multiple domains
Smart contracts
Regulatory governance
Zero-touch network slice and service management
Automation of SLA breaches based on KPIs (such as interference)

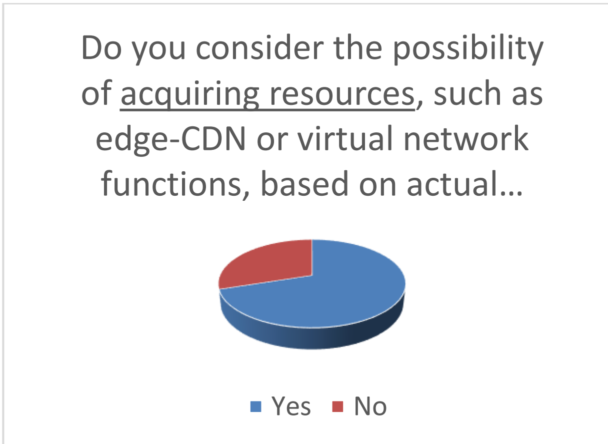


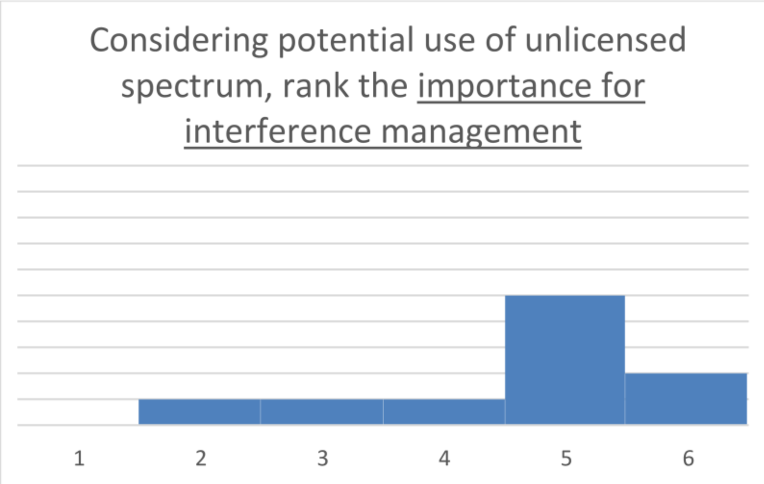


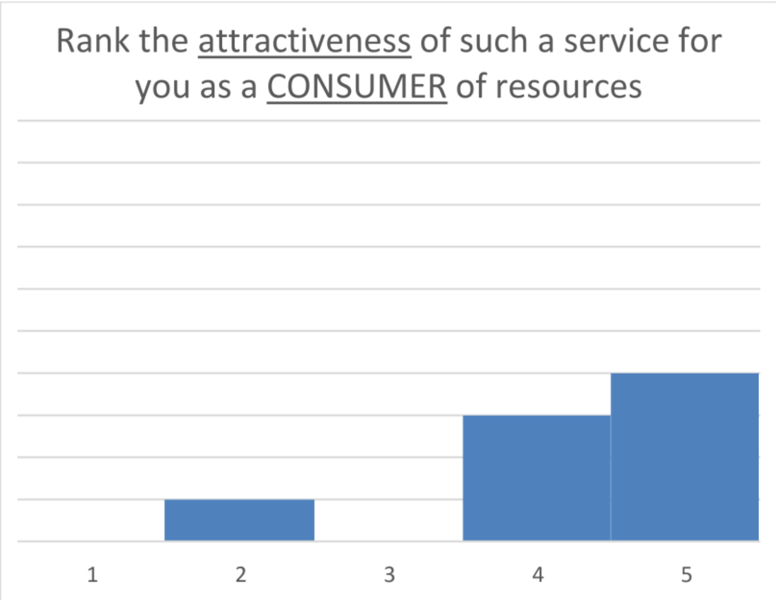


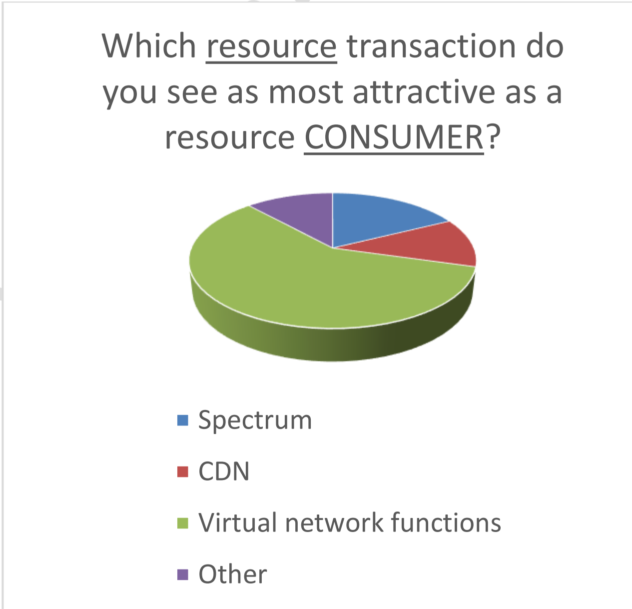
VERTICAL INDUSTRY

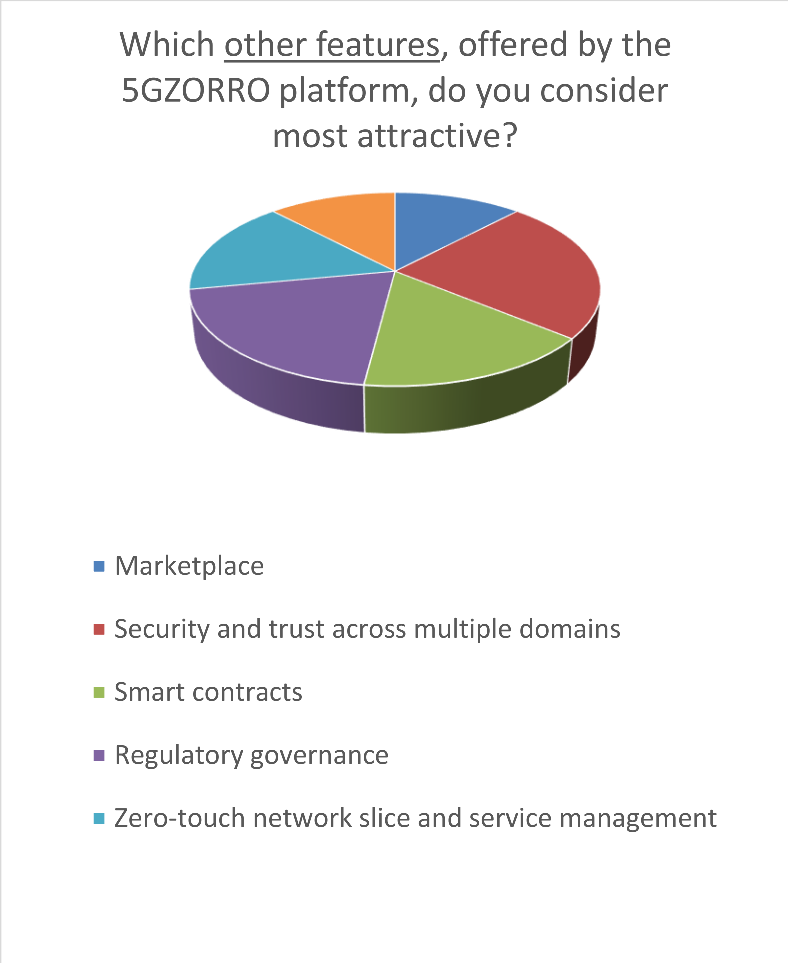


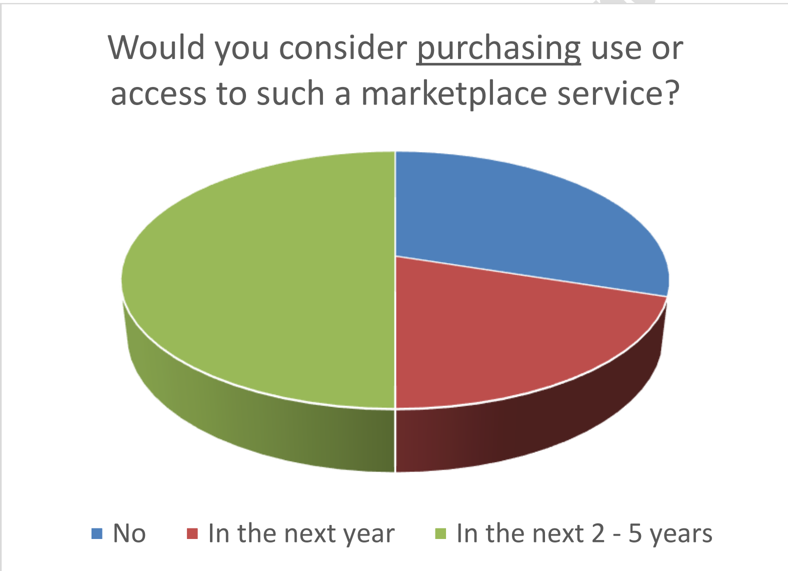


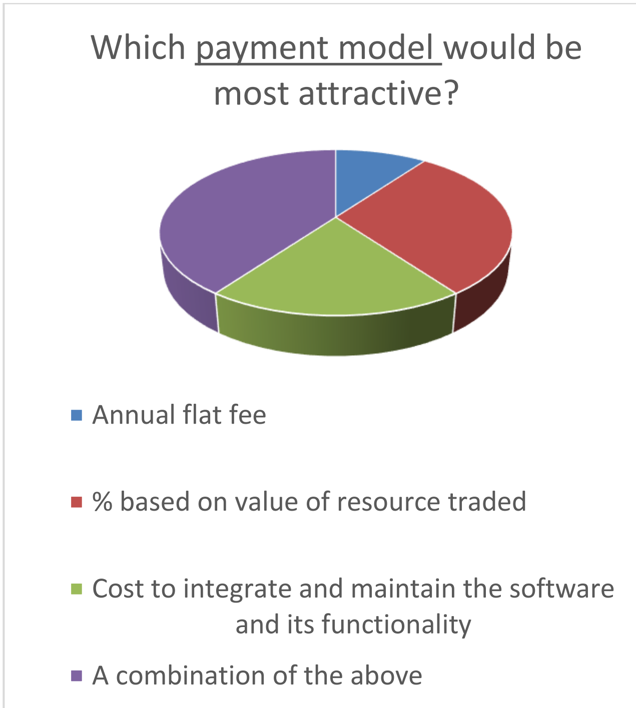

Considering potential use of unlicensed spectrum, rank the importance for interference management
1
2
3
4
5
6

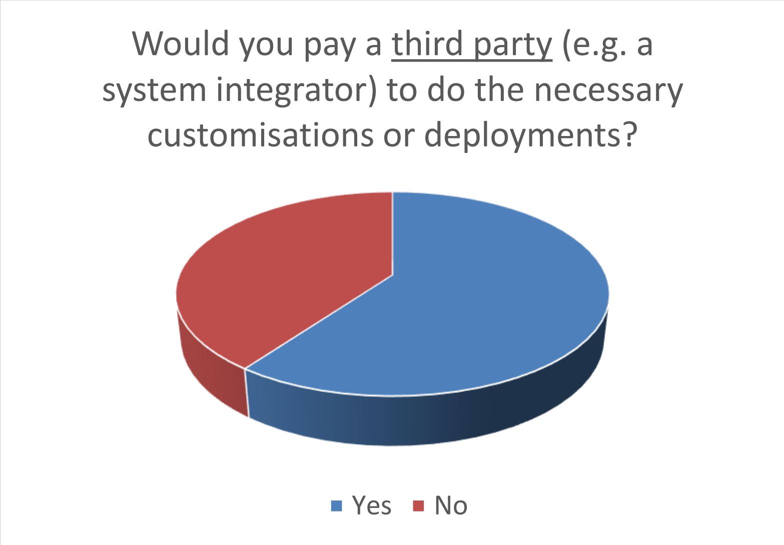

Rank the attractiveness of such a service for you as a CONSUMER of resources
1
2
3
4
5


Which resource transaction do you see as most attractive as a resource CONSUMER?
Spectrum
CDN
Virtual network functions
Other

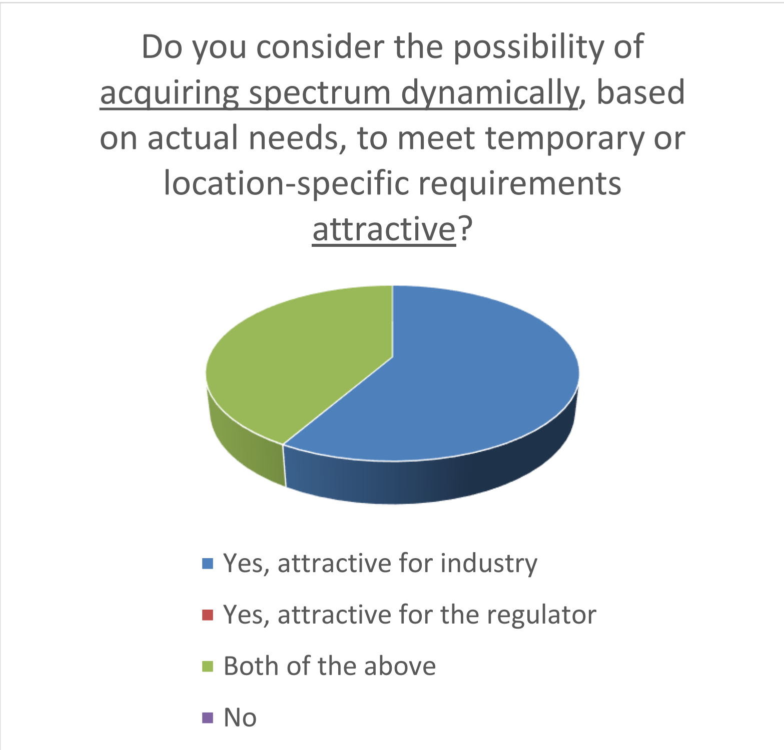

Which other features, offered by the 5GZORRO platform, do you consider most attractive?
Marketplace
Security and trust across multiple domains
Smart contracts
Regulatory governance
Zero-touch network slice and service management

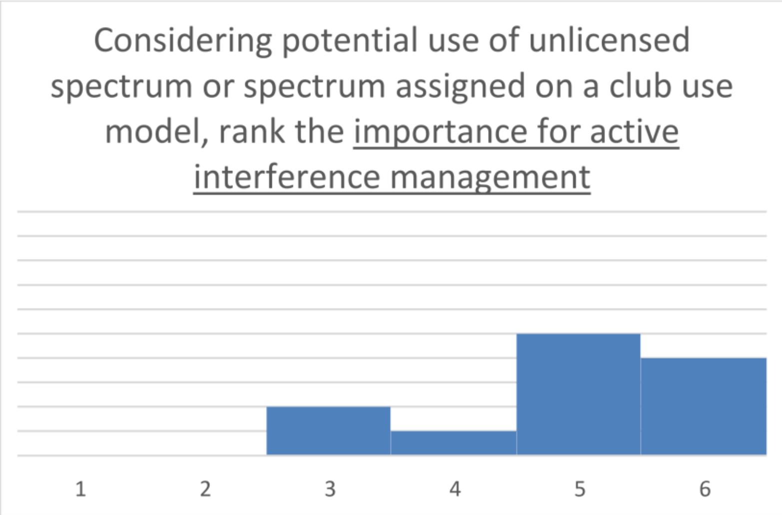

Would you consider purchasing use or access to such a marketplace service?
No
In the next year
In the next 2 - 5 years


Which payment model would be most attractive?
Annual flat fee
% based on value of resource traded
Cost to integrate and maintain the software and its functionality
A combination of the above

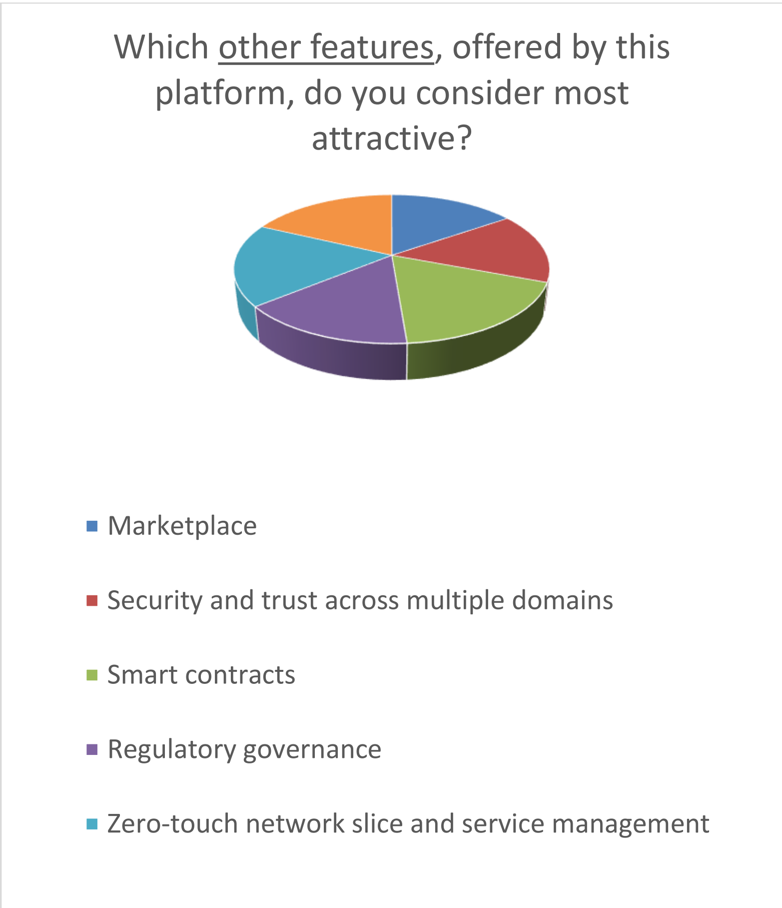

Would you pay a third party (e.g. a system integrator) to do the necessary customisations or deployments?
Yes
No

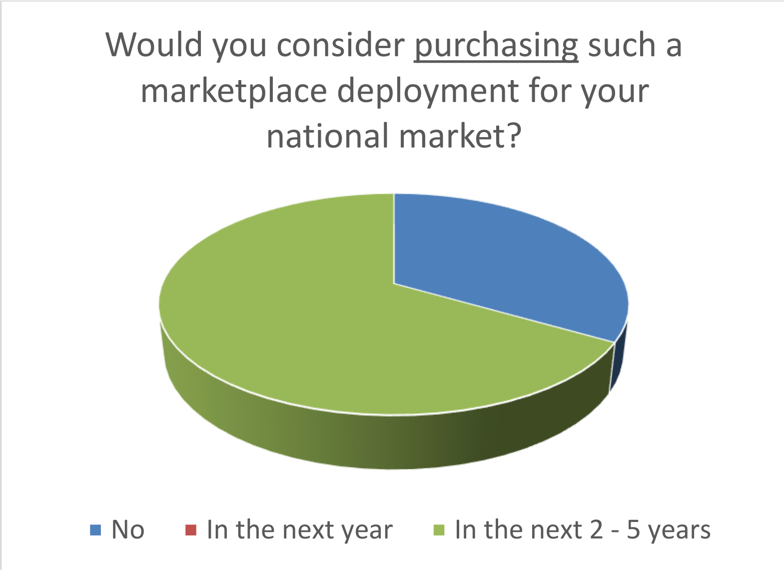
REGULATORS

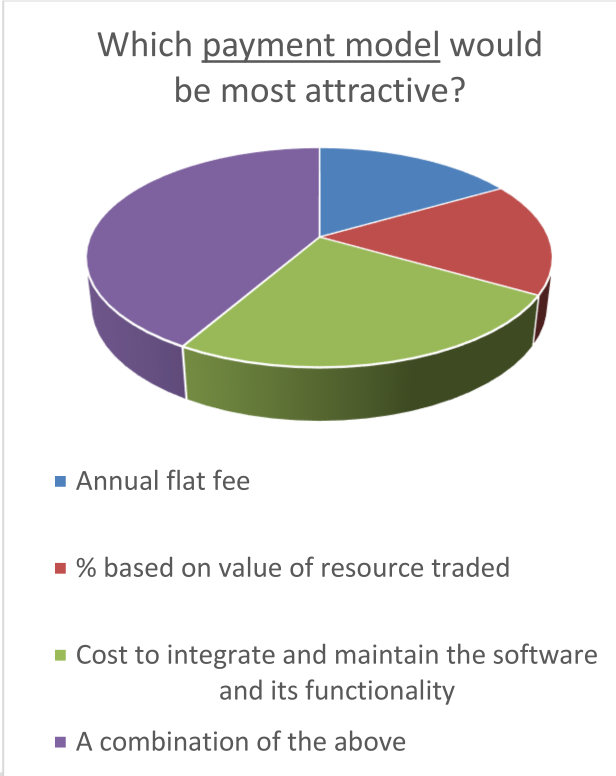

Do you consider the possibility of acquiring spectrum dynamically, based on actual needs, to meet temporary or location-specific requirements attractive?
Yes, attractive for industry
Yes, attractive for the regulator
Both of the above
No

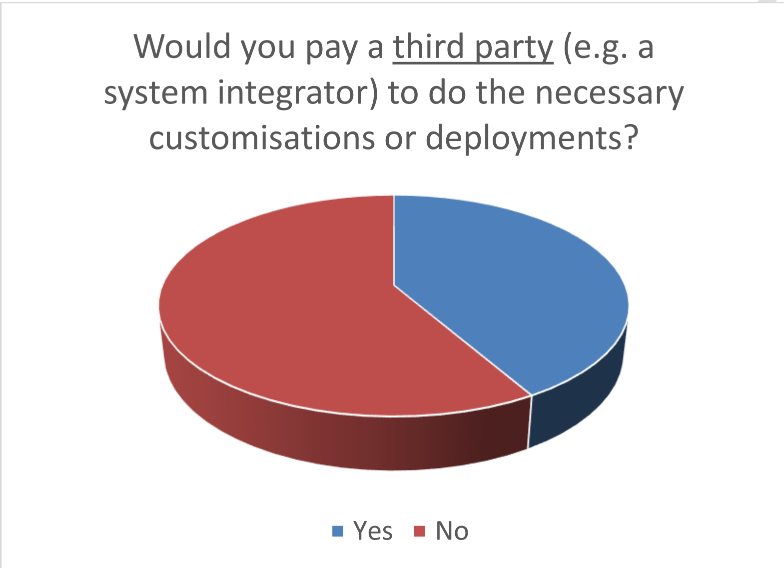

Considering potential use of unlicensed spectrum or spectrum assigned on a club use model, rank the importance for active interference management
1
2
3
4
5
6


Rank the attractiveness of such a service for you as a REGULATOR
1
2
3
4
5
6


Which other features, offered by this platform, do you consider most attractive?
Marketplace
Security and trust across multiple domains
Smart contracts
Regulatory governance
Zero-touch network slice and service management


Would you consider purchasing such a marketplace deployment for your national market?
No
In the next year
In the next 2 - 5 years


Which payment model would be most attractive?
Annual flat fee
% based on value of resource traded
Cost to integrate and maintain the software and its functionality
A combination of the above


Would you pay a third party (e.g. a system integrator) to do the necessary customisations or deployments?
Yes
No

References

[1] 5GZORRO Consortium, Deliverable D6.5 – 'Exploitation Plan and Roadmap', October 2022

[2] 5GZORRO Consortium, Deliverable D5.1 – 'Use case validation plan and testbed design', April 2021

[3] 5GZORRO Consortium, Deliverable D5.2 – 'Intermediate Validation Results', January 2021

[4] 5GZORRO Consortium, Deliverable D4.1 – 'Design of Zero Touch Service Management with Security & Trust Solutions', January 2021

[5] Free5GC, an open-source project for 5th generation (5G) mobile core networks, [Online], Available: https://github.com/free5gc/free5gc (accessed on October 11, 2022)

[6] 5GZORRO Consortium, Deliverable D2.1 – 'Use cases and requirements definition', May 2020

[7] https://aws.amazon.com/elastictranscoder/sla/

[8] https://www.youtube.com/watch?v=4MiDZur_nd4

[9] 5GZORRO Consortium, Deliverable D3.3 – 'Final design of the evolved 5G Service layer solutions', April 2022

[10] https://github.com/5GZORRO/TEE/tree/main/prometheus

[11] 5GZORRO Consortium, Deliverable D2.2 – 'Design of the 5GZORRO Platform for Security & Trust', October 2020

[12] 5GZORRO Consortium, Deliverable D2.4 – 'Final design of the 5GZORRO Platform for Security & Trust', April 2022

[13] https://www.intel.com/content/www/us/en/support/articles/000089326/software/intel-security-products.html

[14] https://www.intel.com/content/www/us/en/developer/articles/technical/intel-trust-domain-extensions.html#inpage-nav-5

[15] https://github.com/5GZORRO/platform-automation

[16] 5GZORRO Consortium, Deliverable D3.2 – 'Prototypes of evolved 5G Service layer solutions, June 2022

[17] https://www.terraform.io/ (accessed on October 12, 2022)

[18] 5GZORRO Consortium, Deliverable D6.4 – 'Initial market and business opportunities analysis ', July 2020

[19] Kantor, Miroslaw & Wajda, Krzysztof & Lannoo, Bart & Casier, Koen & Verbrugge, Sofie & Pickavet, Mario & Wosinska, Lena & Chen, Jiajia & Mitcsenkov, Attila. (2010). General framework for techno-economic analysis of next generation access networks. 2010 12th International Conference on Transparent Optical Networks, ICTON 2010. 1 - 4. 10.1109/ICTON.2010.5549342.

[20] Zimmerman, A., Wunderlich, J., Buchner, G., Müller, L., Armstrong, K., Michailos, S., Marxen, A., Naims, H., Mason, F., Stokes, G., & Williams, E. (2018). TechnoEconomic Assessment & Life-Cycle Assessment Guidelines for CO2 Utilization. https://doi.org/10.3998/2027.42/145436

[21] Buchner, G. A., Zimmermann, A. W., Hohgräve, A. E., & Schomäcker, R. (2018). Techno-economic Assessment Framework for the Chemical Industry—Based on Technology Readiness Levels. Industrial & Engineering Chemistry Research, 57(25), 8502–8517. https://doi.org/10.1021/acs.iecr.8b01248

[22] https://www.nokia.com/networks/insights/network-sharing-in-the-5g-world/

[23] https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/network-sharing-and-5g-a-turning-point-for-lone-riders

[24] Exploring marketplaces for software & services | TMForum - Inform

[25] 5GZORRO Consortium, Deliverable D5.2 – 'Intermediate Validation Results', January 2021

[26] 5GZORRO Consortium, Deliverable D4.1 – 'Design of Zero Touch Service Management with Security & Trust Solutions', January 2021

[27] 5GZORRO Consortium, Deliverable D5.1 – 'Use case validation plan and testbed design', April 2021

[28] https://github.com/5GZORRO/TEE/tree/main/prometheus (accessed on November 11, 2022)

[29] https://marlink.com/msc-mediterranean-shipping-company-the-worlds-largest-container-line-accelerates-its-digital-transformation-using-marlink-solutions/ (accessed on September 10, 2022)

[30] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192

[31] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R2120&rid=2

[32] https://www.berec.europa.eu/en/all-you-need-to-know-about-the-open-internet-rules-in-the-eu-0

[33] https://www.europarl.europa.eu/RegData/etudes/STUD/2014/518751/IPOL_STU(2014)518751_EN.pdf#page=20

[34] https://www.ietf.org/blog/consolidation/

[35] https://ec.europa.eu/commission/presscorner/detail/en/IP_22_4313

[36] https://digital-strategy.ec.europa.eu/en/policies/platform-business-trading-practices

[37] https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

[38] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

[39] https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654180/EPRS_STU(2020)654180_EN.pdf

[40] Data Act - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068&from=EN

[41] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks

[42] https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc

[43] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2482

[44] https://rspg-spectrum.eu/wp-content/uploads/2021/06/RSPG21-022final_RSPG_Opinion_Spectrum_Sharing.pdf

[45] https://gaia-x.eu/

[46] https://www.strategyzer.com/canvas/business-model-canvas

[47] https://www.strategyzer.com/canvas/value-proposition-canvas

[48] https://www.investopedia.com/ask/answers/112814/whats-difference-between-capital-expenditures-capex-and-operational-expenditures-opex.asp

[49] http://www.emergonline.org/wp-content/uploads/2018/12/EMERG-BEREC-workshop-on-5G_Marco-Petracca.pdf

[50] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2482

[51] https://www.sharetribe.com/academy/measure-your-success-key-marketplace-metrics/

[52] https://en.wikipedia.org/wiki/List_of_mobile_network_operators_of_Europe

[53] (https://www.intel.com/content/www/us/en/products/docs/processors/core/core-technical-resources.html, Datasheet 1, section 3.5)

[54] fs|cdn™ Anywhere CDN solution. Web. [http://www.intracom-telecom.com/en/products/telco_software/iptv_multiplay/fs_cdn.htm]

[55] https://www.openstack.org/

[56] https://kubernetes.io/

[57] https://www.amarisoft.com/app/uploads/2022/10/AMARI-Callbox-Ultimate.pdf

[58] https://fi.google.com

[59] https://www.twilio.com/

[60] https://www.emnify.com/

[61] https://www.giffgaff.com/

[62] https://www.truphone.com/

[63] https://www.lycamobile.co.uk/

[64] https://open5gs.org/

[65] https://www.smartdcc.co.uk/our-smart-network/

[66] https://www.msc.com/en/about-us

[67] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[68] https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[69] 5GZORRO Consortium, Deliverable D6.3 – 'Final Dissemination and Communication Report', October 2022

[70] https://helm.sh/

[71] https://github.com/aligungr/UERANSIM

7. Abbreviations and Definitions

7.1. Definitions

No definitions introduced in this deliverable.

7.2. Abbreviations

5G-TRMF	5G-enabled Trust and Reputation Management Framework
AI	Artificial Intelligence
CSP	Communication Service Provider
DID	Distributed IDentifier
DLT	Distributed Ledger Technology
DMA	Digital Markets Act
DSA	Digital Services Act
EC	European Commission
ELM	E-Licensing manager
HLS	HTTP Live Streaming
Id&P	Identity and Permissions Manager
ISBP	Intelligent SLA Breach Predictor
ISSM	Intelligent Slice & Service Manager
MDA	Monitoring data aggregator
MNO	Mobile Network Operator
MPEG-DASH	MPEG Dynamic Adaptive Streaming over HTTP
NFV	Networks Function Virtualization
NFVI	Networks Function Virtualization Infrastructure
NFVO	NFV Orchestrator
NS	Network Services
NSSO	Network Slice and Service Orchestrator
OTT	Over-The-Top
P2B	Platform to Business
POP	Product Offer Price
RAN	Radio Access Network
rRM	Radio Resource Manager
SCLCM	Smart Contract Lifecycle Manager
SLA	Service Level Agreement
SLO	Service Level Objective
SRP	Spectrum Resource Provider
SRSD	Smart Resource and Service Discovery
UC	Use Case
UE	User Equipment
vCDN	virtual Content Distribution Network
VIM	Virtual Infrastructure Manager
VM	Virtual Machine
VNF	Virtual Network Function
VSD	Vertical Service Descriptor
WP	Work Package
xRM	virtual/network/compute/radio/spectrum Resource Manager
ZSM	Zero touch network & Service Management

<END OF DOCUMENT>