5GZORRO

Grant Agreement 871533

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

D.2.1. Use Cases and Requirements Definition

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)

Intermediate version. Pending of EC revision. Do not cite.

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: **V1.5**

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

Deliverable title:
D.2.1. Use Cases and Requirements Definition

Start date of the project: **01/11/2019 (duration 30 months)**	Contractual delivery date: **30.04.2020**	Actual delivery date: **31.05.2020**

Editor(s)
Aurora Ramos (ATOS), Fernando Díaz (ATOS)

List of Contributors

Participant	Short Name	Contributors
Fundació i2CAT	I2CAT	August Betzler, Adriana Fernandez, Javier Fernandez, Shuaib Siddiqui
Nextworks	NXW	Gino Carrozzo, Juan Brenes, Pietro G. Giardina
IBM Israel Science and Technology	IBM	Katherine Barabash
Telefonica Investigacion y Desarrollo	TID	Diego Lopez
Ubiwhere	UW	Pedro Diogo
Fondazione Bruno Kessler	FBK	Tejas Subramanya, Roberto Riggio
Universidad de Murcia	UMU	Gregorio Martínez, José María Jorquera Valero, Pedro Miguel Sánchez Sánchez, Manuel Gil Pérez
Bartr Holding Limited	BTL	Paul T. Henderson, James Taylor, Martyn Taylor
Altice Labs	ALB	José Bonnet, Paulo Chainho
Intracom	ICOM	Sergios Soursos, Marinela Mertiri
Atos Spain	ATOS	Aurora Ramos, Fernando Díaz
Malta Communications Authority	MCA	Antoine Sciberras

List of Reviewers

Participant	Short Name	Contributors
Altice Labs	ALB	Paulo Chainho
Malta Communications Authority	MCA	Antoine Sciberras
Fundació i2CAT	I2CAT	Shuaib Siddiqui
Nextworks	NXW	Gino Carrozzo

Change History

Version	Date	Partners	Description/Comments
0.1	2019/12/08	I2CAT, ICOM, ATOS	UC2 and UC3 first draft
0.12	2020/02/26	BTL	Comments and edits from BTL on UC1 and UC2
0.13	2020/03/02	ATOS	Added contributions from i2cat, BTL, INC, and ALB
0.16	2020/03/16	ATOS	ATOS and ALB Section 3 improvement. ICOM contribution to UC3. UMU comments
0.18	2020/04/07	ATOS	Merge of contributions from ATOS to section 3, BTL (section3 and 4), i2CAT (section3 and 4), ICOM in UC3 and FBK to UC2

0.19	2020/04/23	ATOS	Added contributions from BTL to UC1, i2CAT to UC2, UW review and NXW contribution to section 2.1, operational data lakes by IBM
0.20	2020/04/28	ATOS	Merge of contributions from UMU, I2CAT, BTL, NXW, ICOM, FBK in several sections
1.0	2020/05/12	ATOS	Version for internal review
1.2	2020/05/24	NXW	Question/Answers revision from technical coordinator
1.4	2020/05/27	ATOS	QA amendments
1.5	2020/05/31	I2CAT	Final version for submission

DISCLAIMER OF WARRANTIES

Table of Contents

List of Tables

List of Figures

Executive Summary

This document presents the results of the initial use cases description and requirements elicitation work conducted in the H2020 5GZORRO project. This R&D action has the overall objective to design, develop and validate in representative use cases a 5G architecture capable to incorporate zero-touch automation solutions for the orchestration of high volumes of ubiquitous and pervasive 5G services, with security and trust. For this, 5GZORRO will develop a zero-touch orchestration platform which will use Artificial Intelligence (AI) to govern the complexity of automation through the identification of usage patterns and cognition into operational data lakes, coupled with distributed ledger technologies to implement a scalable and secure solution for the interworking and accountability of different actors of the service composition chain.

This document provides a detailed description of the 5GZORRO use cases. Each use case is contextualised through a review of the specific state of the art aimed at identifying the expected novelty that will be introduced in the 5GZORRO project. Multiple scenarios are covered for each use case, in order to illustrate the behaviour expected using the 5GZORRO platform and identify various ways for stakeholders to interact among themselves.

Three Use Cases are proposed in 5GZORRO:

1. Sm*art Contracts for Ubiquitous Computing/Connectivity*: It covers mechanisms for the implementation of DLT-anchored Smart Contracts and Oracles with the objective of enabling decentralized trust for multi-party interactions and SLA management in trading of computing (and other) resources across edge and core parts of the network.

2. *Dynamic spectrum allocation*: It envisions Blockchain enabled spectrum markets, where shared spectrum usage right holders can trade and lease spectrum rights for a given area and time, enhancing spectrum efficiency while maintaining the QoS at the required level.

3. *Pervasive virtual Content Distribution Network Services (vCDN)*: It covers the capacity for delivering scalable, pervasive vCDN services including HQ video streaming (live and/or VoD), in situations with significant variations in the context of flash crowd scenarios e.g., video sharing in stadiums, or sharing breaking news live feed. This use case integrates also technology enablers and scenarios from Use Case 1 (for smart contracting of edge computing resources) and Use Case 2 (shared spectrum trading).

5GZORRO use cases are presented according to the standpoint of several stakeholders, such as vertical industries, software vendors, spectrum regulators, Communication Service Providers (CSPs), Mobile (Virtual) Network Operators (MVNOs) and third-party providers for both computing and telecommunication infrastructure. Gaps are identified, and a set of requirements taking into account existing technologies and trends are extracted. Finally, proposals on how to fill these gaps are discussed, envisioning the expected functionalities of the 5GZORRO platform.

This deliverable provides the basis for the design and implementation work that will be performed in the work packages 2, 3, 4 and 5 specially, where performance evaluation and validation through demonstrations of 5GZORRO architecture and solutions will be accomplished.

1. Introduction

1.1. Motivation, objectives and scope

This deliverable analyses for selected use cases some specific performance, security and scenario operations aspects that can be improved leveraging the 5GZORRO architecture and its secure intelligent orchestration services. Starting by sharing the interests of the consortium members along the project in the use of the aforementioned technologies, and guided by the use cases related to Smart Contracts, Spectrum Management & 3rd party edge resources, the 5GZORRO use cases are described to identify relevant scenarios and derive requirements for platform architecture design.

Therefore, the objectives of this deliverable include:

- To define stakeholders involved in the 5GZORRO architecture and services and the role they can play;
- To detail use cases for the new 5GZORRO architecture which can be relevant to demonstrate how the platform is expected to be used. Use cases include both business- and technical-oriented scenarios;
- To gather and prioritise requirements for architecture design and implementation from the selected use cases.

Use case scenarios and requirements identified in this deliverable represent a preliminary (though comprehensive) description of what the 5GZORRO architecture is expected to address. Use cases will be further refined and improved during the execution of the project, through a process of agile continuous improvement, which aims to take into account any new and/or improved requirements that may emerge as the planned design and implementation activities unfold during the project.

1.2. Document structure

The contents of this document are structured as follows:

In Section 2, the overall 5GZORRO vision is provided, focusing on the benefits that introduces network automation and distributed ledgers in discovering, brokering, trading and managing services with trust and security. The targeted 5GZORRO services to be offered in the platform are enumerated and described, with their proposed technological enablers that the Use Cases will use.

Section 3 describes the main actors and the possible roles they can take in the 5GZORRO value chain. Roles aim to sketch preliminary and general business stakeholders' relationships.

Section 4 covers the actual description of the Use Cases, providing details of their motivation, the starting points for work and enhancements planned during the project. The section describes the planned experiments, scenarios and initially identified tools to be used, as well as an initial list of Key Performance Indicators (KPIs) that will be evaluated as a proof of concept later in the project.

Section 5 provides the list of requirements captured from the analysis of the three use cases, which will be used as input to the platform architecture design task. Each requirement is characterised with a justification and related KPI targets. The methodology that has been adopted for requirement elicitation is also described.

Finally, section 6 completes the document with the main conclusions considering the project objectives and the current work done; it also describes the main issues found and the different strategies to solve them in order to complete the final specification.

2. 5GZORRO Service Concepts and Overview

2.1. Overall 5GZORRO Concept

The 5GZORRO concept and vision is based on the premise that current 5G Management and Orchestration (MANO) platforms cannot realize the full set of benefits 5G promised to introduce. In this sense, the available management architectures and solutions have not yet been completely adapted to the multi-domain scenarios and the heterogeneous ecosystems present in the target 5G deployments and are therefore preventing the exploitation of all their capabilities. On the one hand, these architectures and solutions need to be evolved in order to be capable to support compute, storage, network and spectrum resources from multiple operators. On the other hand, intelligent automation mechanisms need to be introduced in order to couple with the complexity of the network operations introduced by the new level of heterogeneity and the unprecedented amount of resources to be managed in network virtualization environments (1000s of virtual functions and lifecycles of virtualised services in a 5G NFV network).

In Figure 2-1 the 5GZORRO vision of near future 5G Network is depicted. Different providers across different geographical areas can collaborate to share, lease and use heterogeneous sets of resources that can be shared, traded and, above all, chained in order to provide true on-demand integration of ubiquitous resources in terms of computing, network, and storage, transparently across multiple technological and administrative domains.

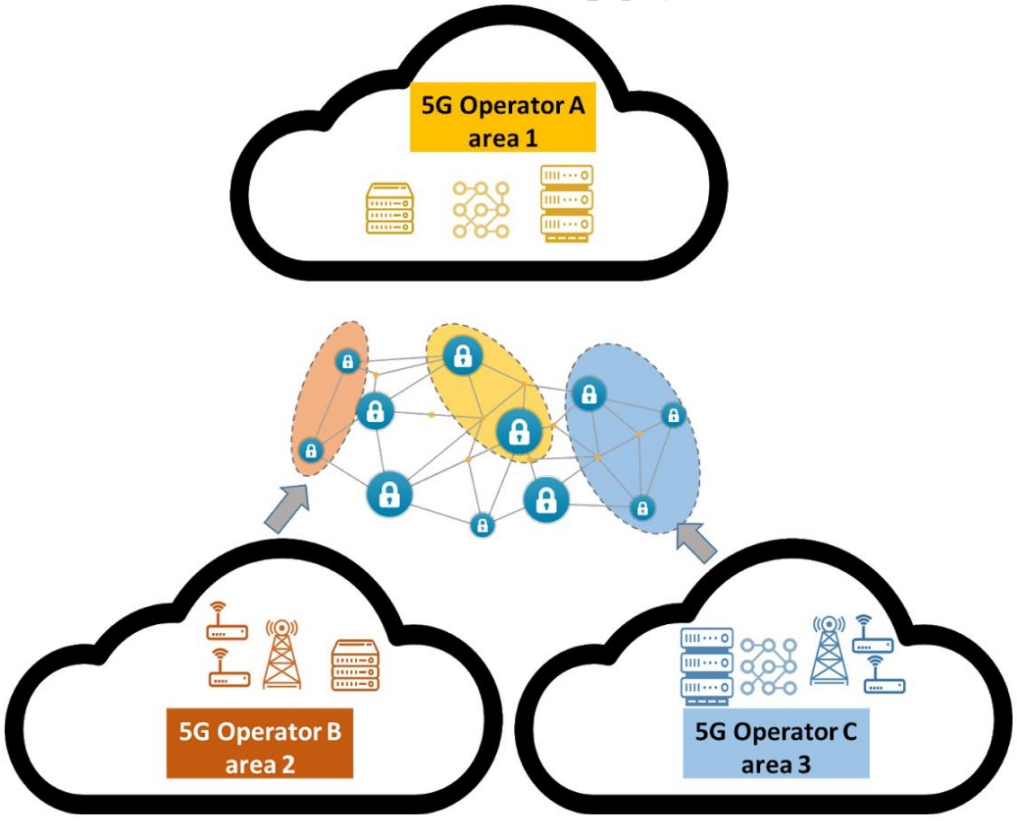


Figure 2-1 5GZORRO high level scenario of multi-operator 5G network

For the realisation of such a view, some core requirements need to be satisfied:

- *Full automation of network, service and security management.* An efficient 5G architecture should rely on improved zero-touch management for its network resources, services and should be capable of implementing trust and security in a multi-stakeholder environment. This will require seamless

end-to-end security orchestration, dynamic trust computation and trusted execution of the workloads across multiple domains.

- *Discovering, brokering and trading of resources*. Resources can belong to compute, storage or network segment and can be provided by operators and 3rd party providers.

In terms of computing, storage and network resources, the 5GZORRO architecture aims to allow smart discovery, registration and allocation of resources and service onboarding across different technological and administrative domains. Figure 2-2, shows the service deployment vision of 5GZORRO using intelligent selection of resources, and establishing appropriate trusted channels across multiple parties. In particular, the focus is set on enabling seamless use and composition of different virtualization technologies (i.e. virtual machines, containers, etc) present on different segments of the network, and on allowing more flexible and dynamic allocation of spectrum resources from the different licensed owners. The network administration, on the other hand, will be simplified and automated by means of AI and ML techniques leveraging new information sources.

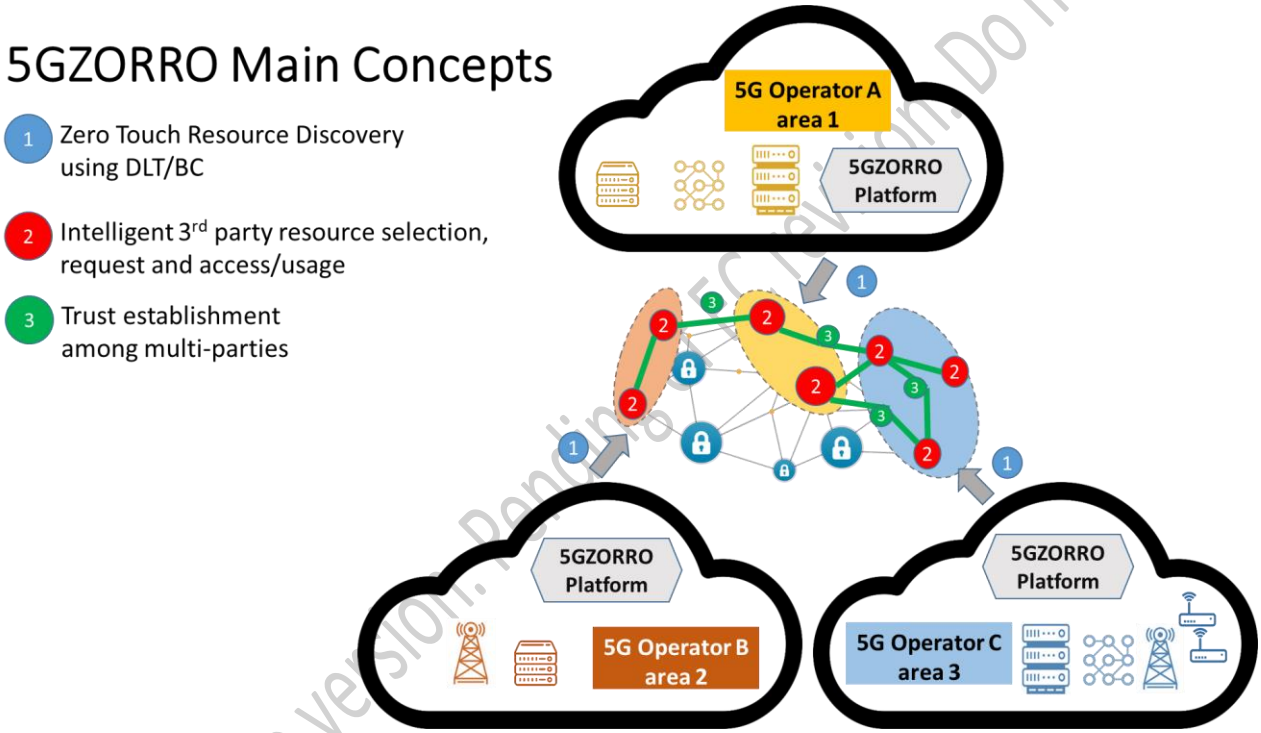


Figure 2-2 5GZORRO main concepts

The 5GZORRO platform will run in each operator domain to support the functionalities previously described. This platform will rely on different technological enablers, such as Artificial Intelligence engines (based on machine learning frameworks and algorithms), Distributed Ledger Technologies (DLTs), Service Meshes and Data Lakes. It will follow a service based architecture design (such as the ones proposed in [1] and [2]) to offer different types of services: (i) Smart Contracts Management; (ii) Resource Discovery & Brokering; (iii) Intelligent third-party virtual resource selection; (iv) Spectrum trading and sharing; (v) Secure SLA Monitoring.

In the following sections we further detail the 5GZORRO services and their technological enablers, which the different use cases of the project aim to use to implement their operation scenarios.

2.2. 5GZORRO Services

Service name	Description	Technological enabler
Smart Contracts and Management (Resource Marketplace and catalogue)	5GZORRO aims to provide a real-time and decentralized market to enable dynamic networking and computing resource trading capabilities (including spectrum resources). 5GZORRO leverages the tokenization of assets concept, enabled by DLTs based Smart Contracts, to support trading operations with specific SLA requirements. Parties that are in principle untrusted to each other, will be able by means of 5GZORRO to negotiate, set-up and operate a new technical/commercial relationship via a Smart Contract for 3rd-party resource leasing/allocation with associated SLA. Examples of resources that can be traded in this way with 5GZORRO are: (i) Transport network provided by a fixed telco operator; (ii) 5G Radio Spectrum licensed to a wireless telco operator; (iii) Wi-Fi hotspot operated by a municipality; (iv) Enterprise network infrastructure; (v) Residential Wi-Fi Routers. The trade of these assets between two or more 5GZORRO stakeholders, is governed by smart contracts and requires a high level of trust among them that should not depend on central third-party trustful entities e.g. PKI certificate authorities. Inclusion of external data sources supporting the smart contract is foreseen and will be provided by means of Oracles. A key feature of the 5GZORRO Marketplace is a decentralized catalogue that holds the collection of 5GZORRO product offers available to be traded among providers and consumers. See more details at section 4.2.3.	Distributed Ledgers
Security and Trust	5GZORRO offers this service to enable the establishment and orchestration of security in multi-stakeholders and multidomain scenarios. This includes the integration of zero trust hardware platforms (TEE -Trusted Execution Environments) as the main enabler to generate trust for the monitoring information and the end-to-end secure communications. Procedures to detect and react to security vulnerabilities across multiple domains will be implemented using the Zero-touch approach.	Trusted Execution Environments,
Resource Discovery and Brokering	Application programming interfaces (APIs) will be offered by the 5GZORRO architecture to allow business agents to discover, “inventorize” and share heterogeneous resources	Distributed Ledgers,

Service name	Description	Technological enabler
	(i.e. spectrum, virtualized radio access, virtualized edge/core, software defined WAN, etc.). The API exposed will incorporate Intent-based technologies to enable AI-driven agents to discover the most suitable set of resources.	Intent-based API
Intelligent 3rd party resource Selection	This service enables 5GZORRO stakeholders to determine the most suitable set of 3rd party resources to be used given a specific set of service requirements and SLAs. Intent-based features will be used to allow the interaction with AI-based business agents.	Intent-based API
Network Slicing and Orchestration	5GZORRO aims to offer enhanced Network Slicing and Orchestration services, which exploit the capabilities introduced by the Smart Contracts and Management, Intelligent 3rd party resource Selection and Security and Trust services to enable service provisioning and orchestration on top of the multi-domain environment of 5GZORRO. Heterogeneous virtualization technologies (i.e. Virtual Machines (VMs), Containers, etc) will coexist and be used as part of the infrastructure supporting the deployment of the network services. This will allow a seamless composition of the resources (i.e. from cloud-based core resources to micro-data centers at smart city IT infrastructures like edge computing at street cabinets or at lampposts). Service mesh technologies will be used to provide connectivity between different network service segments. The increased network administration complexity introduced by this inter-domain (and heterogeneous) network slicing capabilities will be addressed with the usage of inter-domain operation data lakes and zero-touch. Operational data lakes will ease the access to inter-domain operation information coming from diverse monitoring sources, which the zero-touch modules will use to support full AI-based automation. Furthermore, the Network Slice and Network Service lifecycle management actions will also use automatic VNF license enforcement procedures which will provide support for dynamic service provisioning.	Intent-based APIs, Service Meshes, Data lakes
VNF e-licensing	The VNF e-licensing service will allow the establishment of vendor independent license agreements, using different license templates. This license agreements will be attached to VNF/NS instances, and will be integrated into the NFV MANO lifecycle workflows to: (i) manage location independent VNFs from 3rd party edge to core datacenter; (ii) Allow instantiation of Network Services using VNFs from several VNF providers.	Distributed Ledgers

Service name	Description	Technological enabler
	Smart contracts will be used to support licenses across multiple administrative domains.	
SLA Monitoring	The SLA Monitoring service enables retrieval of service and resource SLA and KPI related information. Within the 5GZORRO platform, specific modules will extract the information from the 5G operation data lake and provide improved correlation capabilities. In other words, this service will offer a set of APIs which will interact with the underlying architectural components to aggregate and abstract the cross-domain monitoring information, in order to provide reports assessing the service KPI information and the SLA fulfilment	Data lakes

Table 2-1 5GZORRO services

In order to realize these novel services, the 5GZORRO architecture uses a layered approach as shown in Figure 2-3.

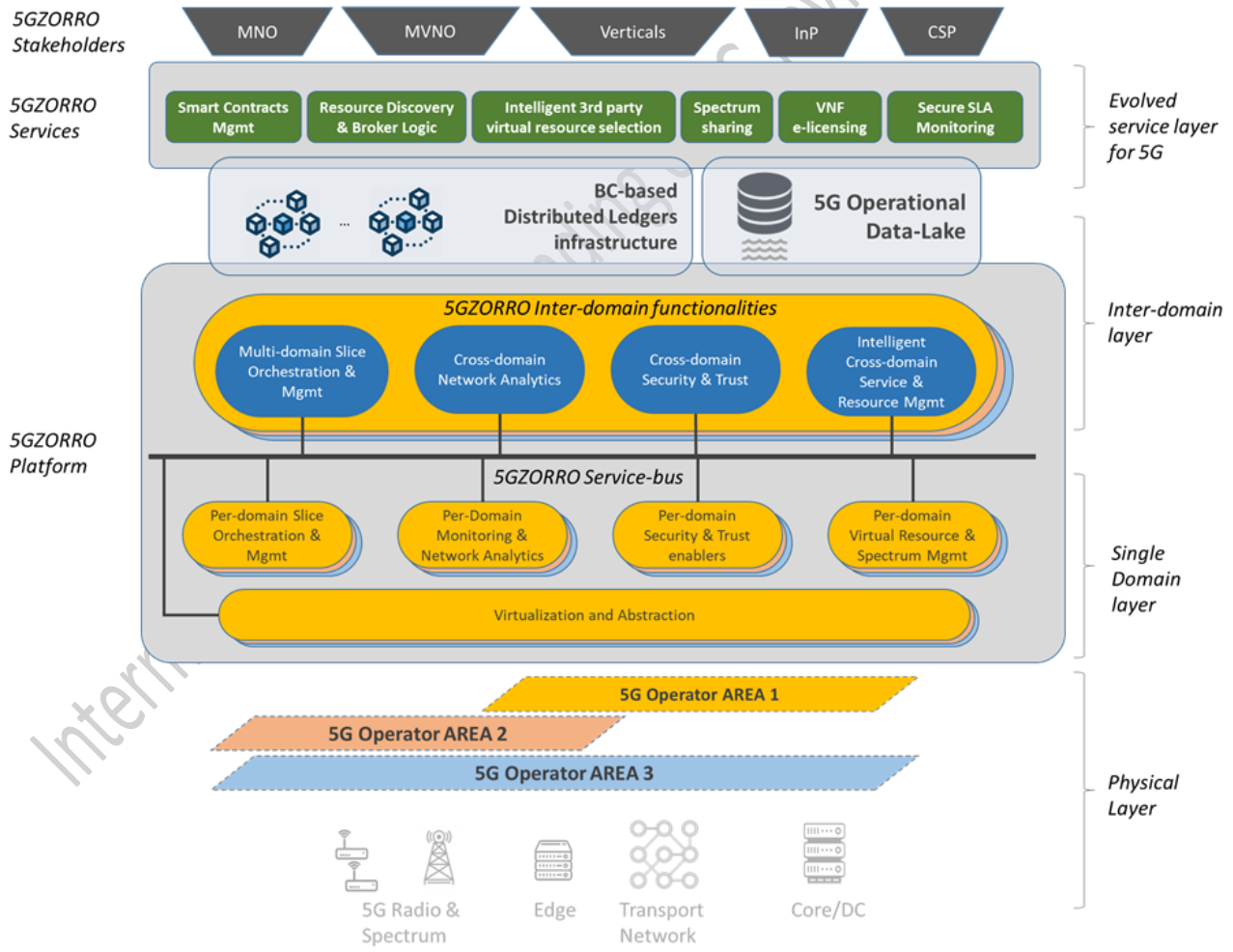


Figure 2-3 5GZORRO high-level architecture

The bottom most part is represented by the Physical layer, which contains the network and computing resources, including the novel spectrum resources, offered by the different 5G operators. On top of the Physical layer, two different layers implement all the functionalities 5GZORRO will provide in terms of Slice and Orchestration, monitoring of the network, Security and Trust, and Virtual Resource management (including the Spectrum). The Single domain layer embraces all the modules included to support the functionalities on the resources under its own administrative control, while the Inter-domain layer contains the counterpart modules for the cross-domain. This latter layer of the platform is the one interacting with the 5G Operational Data-Lake and with the Distributed Ledgers. The uppermost layer of the architecture includes the 5GZORRO services.

2.3. Technological enablers

2.3.1. Distributed Ledger Technologies

Distributed Ledger Technology (DLT) refers to the technological infrastructure and protocols that allows simultaneous access, validation, and record updating in an immutable manner across a network spread across multiple entities or locations. DLT allows for storage of all information securely and accurately using cryptography. This information can be accessed using "keys" and cryptographic signatures. Once the information is stored, it becomes an immutable database and is governed by the rules of the network. Key facets of the DLT are:

- The ledger records all transactions to date and the current 'world state'.
- Smart contracts. gather the business agreements between parties and oracles feed smart contracts with data from outside their network.
- A consensus model ensures consistency across the network.

Enterprise DLT's offer additional features over and above that offered by popular public DLTs, these include Private Transactions, Private Data, Role-Based Access Control, Identity Management Services for user management, authentication and policy management, and pluggable elements such as consensus to address key enterprise use cases that are not trivially satisfied by public DLT's. Typically, this results in:

- improved performance - higher transaction throughput / low latency transaction confirmation as a result of alternative consensus models.
- known participant identities– addressing Know Your Customer (KYC), Anti-money laundering (AML) requirements.
- privacy & confidentiality of transactions.

The introduction of these enterprise features inevitably results in trade-offs with regards to the level of decentralization and transparency of transactions & data.

2.3.1.1. Smart contracts

Smart contracts are programmable components of the DLT that encapsulate the agreed business model of parties wishing to interact with the ledger and cannot be tampered with; they represent an enforceable agreement. In general, smart contracts consist of a combination of both computer code, a programmable transaction protocol that defines the business terms of the contract, and legal prose that reflects that the computer code constitutes part of the binding legal agreement between the parties, and is therefore also legally binding. Some differing smart contract models in use are:

- Account-based model (e.g. Ethereum [3]): In an account-based model a smart contract defines a set of functions that govern valid interactions. Applications invoke a smart contract to generate transactions that are recorded on the ledger. Smart contracts can hold state, for example a set of

tokens and their current owners, and a defined interface governs valid interactions and subsequently applies associated validation rules before a transaction can be submitted to the ledger.

- Unspent Transaction Output (UTXO) model: this differs to the previous model in that contract state is stored as a UTXO in a transaction. Contracts manage contract state by taking a transaction proposal and applying a set of validation rules to the input/output states of the transaction to ensure that any change of state is valid. Smart contracts are executed by multiple peers (in-line with the governance/consensus model of the network) and as such, for consensus to be reached I.e. a transaction is verified and submitted to the ledger, smart contract execution MUST be deterministic.

2.3.1.2. Oracles

In many cases, a transaction's contractual validity depends on some external piece of data, such as the current exchange rate. However, if we were to let each participant evaluate the transaction's validity based on their own view of the current exchange rate, the contract's execution would be non-deterministic: some signers would consider the transaction valid, while others would consider it invalid. As a result, disagreements would arise over the true state of the ledger. Oracles are the means by which we can address non-determinism. If a smart contract requires additional information in order to perform transaction validation, then it can call out to an oracle; a trusted service on the network. An oracle might perform validation of an existing fact or provide data external to the network. The implementation naturally differs across DLTs but ultimately the oracle is a trusted service that can be called upon to provide a signed fact on chain for use in the execution of a smart contract. Where a single trusted oracle is not sufficient/appropriate multiple oracles can be used and the results combined to give a level of distributed trust pertaining to the fact. Depending on the use case, the level of distributed trust will vary. One example of this would be to use a multi-signature transaction to get Fx rates from multiple brokers.

2.3.2. Operation Data Lake

Data lake technology is created for systems that require processing of large amounts of data originating from different sources, arranged in different formats, and having different attributes [4]. As opposed to data warehouse technology, data lakes do not require the entering data to be uniform or structured in any predefined way. Instead, ingested data is structured and unified inside the data lake's internal data processing engine that prepares it for consumption by data users, e.g. analytics and algorithms that implement the required business logic. Usually, the business case that data lake serves dictates the requirements, such as the richness and the scale of the data and the data sources, the structure of data processing pipeline, and the way prepared data is fed to consuming components. Such operational data lakes have recently been envisioned as part of AIOps [5] systems created to support for smooth and correct functioning of complex IT environments, such as clouds. The AIOps paradigm revolves around a concept of operational data and involves smart and efficient data collection (capture, monitoring, telemetry), governed and intelligent data storage over time (data lake), and advanced data analytics (statistics, machine learning, artificial intelligence) to provide valuable insights actionable in the context of every concrete business story. In 5GZORRO, data lake technology will help automating the operation of the 5GZORRO platform and of all the different 5G environments it manages. The operational data lakes will take care of collection, preparation, storage, and targeted delivery of all operational data relevant to correct and efficient functionality of 5GZORRO platform.

2.3.3. Trusted Execution Environments

The Trusted Execution Environment (TEE) [6] is an isolated processing environment in which applications can be securely executed irrespective of the rest of the system, in particular on a separated kernel. The main contributions provided by TEEs are to ensure the data and code loaded within the kernel to be protected regarding to integrity and confidentiality [7], and also to enrich the previous trusted platforms. Another key aspect is that both data and applications stored within the TEE are cryptographically protected. Therefore,

TEEs supply a stand-alone execution environment, and guarantee integrity of applications running (such as memory inputs, CPU registers, kernel execution threads, and sensitive I/O). What is more, Trusted Execution Environments are also able to withstand the physical attacks made on the system's main memory, as well as software attacks [8].

Thus, TEEs are a crucial element that allows increasing the security level of any company, platform or entity where sensitive data is managed and executed. 5GZORRO will use them to enforce trusted analysis on raw data source, and to secure the information that agents declare in the marketplace and Distributed Ledger. Another application of TEE could be the execution of applications containing sensitive data on the infrastructure of a third party, which is being used because the owner of the sensitive data is not able to supply with its own resources the demand of requests it has at a specific time. Through a TEE, the owner of the sensitive data can derive certain critical tasks in the infrastructure of a third party without putting at risk the integrity and confidentiality of its data. Another example could be to guarantee the attestation of the trustworthiness of data being submitted to the Distributed Ledger Technology.

2.3.4. Service meshes

Service Mesh is a networking pattern designed to simplify the communication between the modules building a modern Cloud-Native application. Originally designed for Container-based Microservice Applications, their current application environment includes also VM-based applications, and they are quickly evolving for enabling the seamless connectivity of different cloud environments (hybrid and multi-cloud).

Service meshes decouple the business logic of components in a cloud application from the networking logic, including all of those aspects concerning the network observability, control and security policies. In each microservice (e.g. inside a container), a proxy module is introduced, called Sidecar, that is in charge to enable connectivity with other services of the Cloud Application. In this way, each service will contact the others by interacting directly with its own local Sidecar which, in turn, encapsulates the complex logic regulating the service-to-service exchange mechanism.

The communication network between services, built by their interconnected Sidecars, implements the Service Mesh Data Plane. The Data Plane can be controlled and configured through proper APIs exposed by Sidecars, implementing the so-called Service Mesh Control Plane that provides a mechanism for specifying security policies, providing authentication and gather metrics from the Data Plane.

The communication in the Data Plane may be established at different layers of the network stack, and mainly depends on how the framework enabling the mesh implements its own Sidecars. ISTIO [9] is a Service Mesh framework that provides Sidecars that operates between the L7 (Application Layer) and L4 (Transport Layer). Network Service Mesh (NSM) [10] is another example of framework for service meshes that provides L3/L2 (Network/Data Link Layer) connectivity. It has been designed to work in complex low-level networking scenarios, including the service connectivity over VPN. Finally, the communication between the service can be event-based and realized by a special type of Service Mesh called Event Mesh.

3. Roles and Stakeholders

This section provides the first description of all the possible roles that are part of the 5GZORRO value chain (section 3.1) while section 3.2 describes how those roles are generally played in 5GZORRO as preliminary and general business stakeholders relationships which is the basis for the use cases described in section 4. Further business analysis and alternative business models for the use cases will be tackled in work packages 5 and 6 of the project.

3.1. 5GZORRO Roles

The identified 5GZORRO roles and their interaction with the 5GZORRO functional components, are depicted in Figure 3-1 and described below.

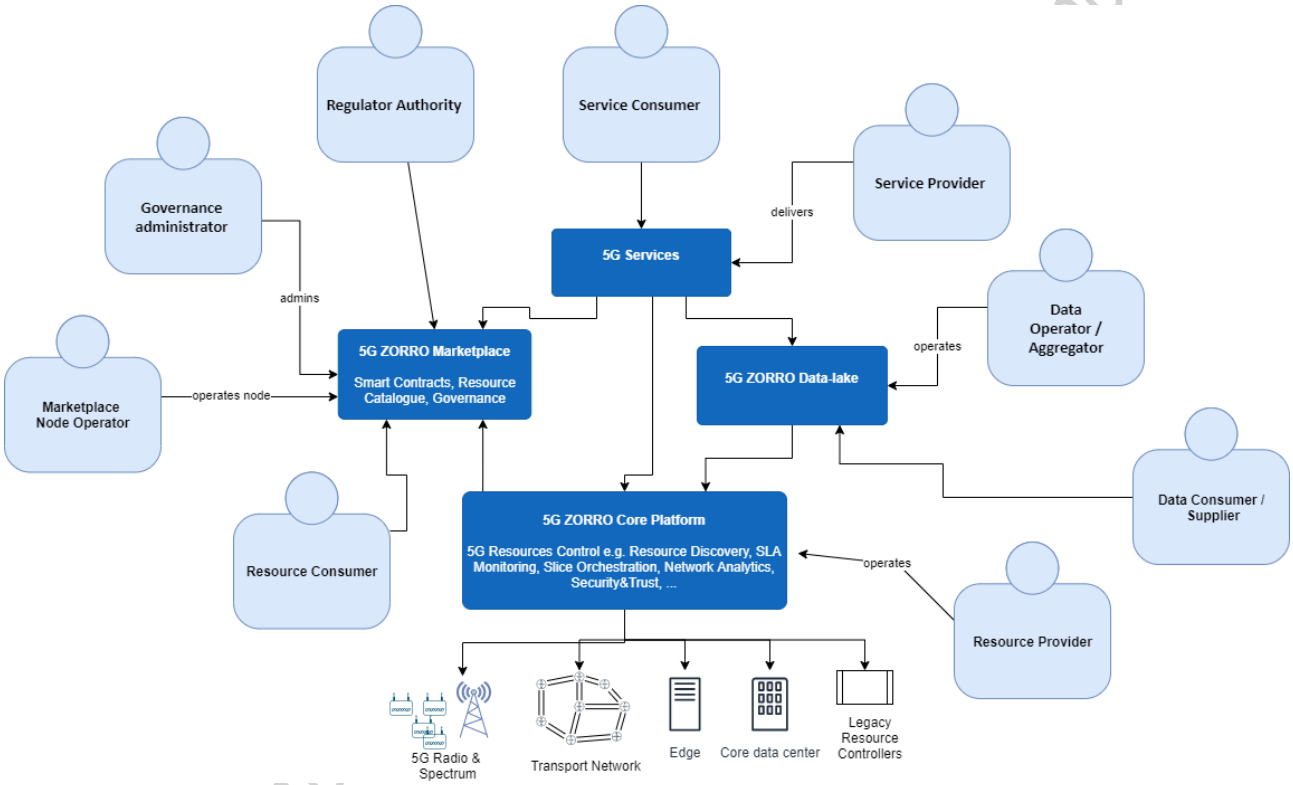


Figure 3-1 5GZORRO roles

The **Resource Provider** is the role in charge of the provision and management of resources used to realize communication services. In general, in 5GZORRO, resources can comprise computing, storage and networking capabilities, including network functions. Resource management activities include management of strategies, capabilities, lifecycles, catalogues, inventories, topologies, installations, activations, alarms, problems, performance, mediation, usage statistics and support. We could contemplate separately:

- Cloud resource provider that provides compute and storage resources.
- Network provider that provides network resources.
- Software provider that provides Network function resources.

The **Service Provider** is the role that offers communication services that are realized on top of an infrastructure comprised by resources providing computing, storage and networking capabilities. In case the Service Provider is not managing the resources used, it also plays the role of a Resource Consumer from the Resource Provider perspective.

The **Resource Consumer** is the role that uses resources from Resource Providers to build and deliver Communication Services i.e. it also plays the Service Provider role from the Service Consumer perspective. The business relationship between the Resource Consumer and the Resource Provider is governed by a set of appropriate Smart Contracts executed in a DLT Platform.

The **Service Consumer** or **customer** is the role that (either being played by an individual stakeholder a person or an organization stakeholder an enterprise, typically played by vertical industries in the 5G context) buys products and services from the Service Provider or receives free offers or services from Service Providers. Service Consumers can also be other service providers who resell the services, to other service providers.

The **Marketplace Node Operator** is the role in charge of operating at least a Marketplace node and thus participating in the Smart Contract lifecycle and in the Catalogue offers and requests.

The **Governance administrator** is the role that has rights to take decisions on the governance of the 5GZORRO Marketplace, for example, to approve or reject new members into the Marketplace.

The **Regulator Authority** is the role in charge of supervising communication delivery business including the rights to use certain Communication Resources like licensed radio spectrum.

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

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

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

3.2. 5GZORRO Stakeholders

In this section the envisioned 5GZORRO business stakeholders are defined. Those are the common stakeholders used among the use case definitions and the proposed scenarios described in section 4.

Figure 3-2 represents the interactions between the different stakeholders and a high-level description about how they can adopt the aforementioned roles in the 5GZORRO chain.

Customer or Service Consumer role will be typically played in 5GZORRO by **Verticals industries,** e.g. manufacturing sector, media sector/CDN provider acquiring 5G communication services. Vertical industries will consume services from the CSPs/M(V)NOs, deploying its vertical application components on top of communication service in order create the vertical service, arranging in the negotiation terms of the service for their exploitation reflected in a Service Level Agreement (SLA). The use cases described in section 4 cover different vertical business cases in which 5GZORRO solution will be relevant.

Communication Service Providers (CSPs), MNOs will be typically playing in 5GZORRO the role described for Service Providers. The 5GZORRO platform will run inside their domains, allowing them the full automated network, service and security management, discovering, brokering and trading with their resources. Every CSP may have limited resources, so it may want to extend their capabilities under certain needs, using resources from other entities, like third-party providers or other CSPs/MNOs that can publish in the 5GZORRO platform the excess of resources. Therefore, it may play the Resource Consumer and Resource Provider roles as well.

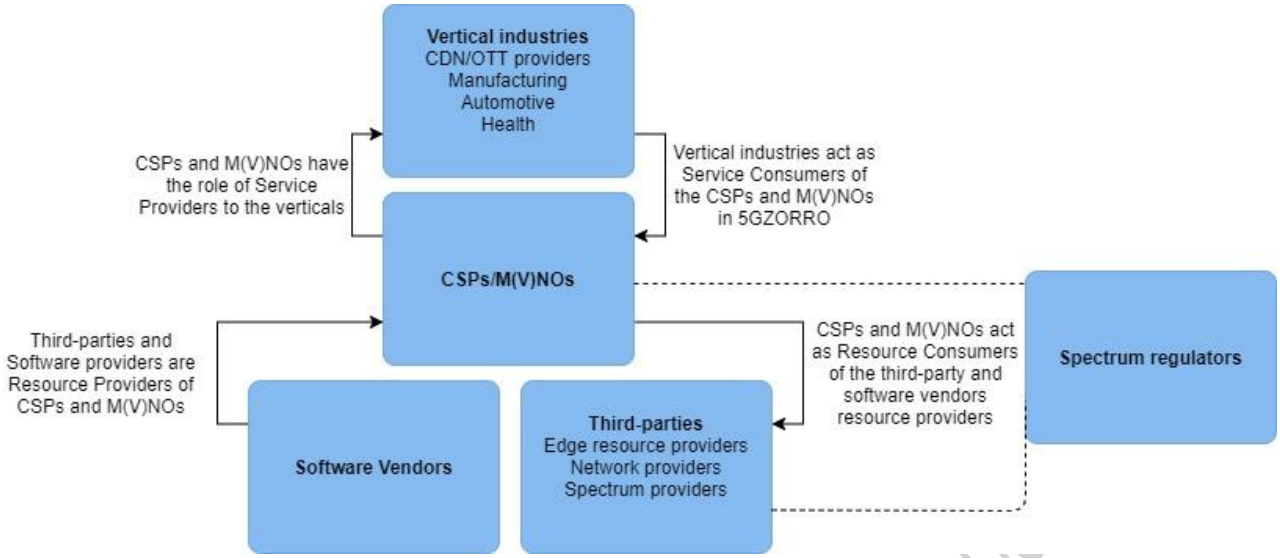


Figure 3-2 5GZORRO stakeholders

The **Third-Party Resource Provider** is the stakeholder that has a stock of free resources to offer to the platform as a Resource Provider. Third-party resource providers can be classified in:

- 3rd party edge resource provider, providing compute and storage capabilities inside large venues or other busy locations. They are usually deployed, maintained and operated by them, and will onboard their resource offer in the 5GZORRO platform.
- 3rd party network provider, that will share network infrastructure, including spectrum. It can be a dedicated entity that has deployed infrastructure to realize private communications but has no license to commercialize them to the public. Instead, part of its infrastructure resources can be offered and used by other stakeholders that play the resource provider's role (among other MNOs).

It is envisaged that Third-Party Resource Providers will perform a set of limited Resource management activities when compared to Resource Providers i.e. its Resource Control platform should comprise a sub-set of features supported by a standard 5GZORRO Resource Control platform.

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

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

4. Use cases

4.1. Use case analysis overview

This section details the description of the use cases, providing a specific review of the state of the art for each of them, the novelty that they introduce by interfacing with the 5GZORRO project and covering multiple scenarios in order to illustrate the expected behaviour and benefits using the 5GZORRO platform and how the stakeholders will interact with it.

Three Use Cases are proposed:

1. **Smart Contracts for Ubiquitous Computing/Connectivity**: It covers mechanisms for the implementation of DLT-anchored Smart Contracts and Oracles with the objective of enabling decentralized trust for multi-party interactions and SLA management.

2. **Dynamic spectrum allocation**: It envisions Blockchain enabled spectrum markets, where shared spectrum right holders can trade and lease spectrum rights for a given area and time, enhancing spectrum efficiency while maintaining the QoS at the required level.

3. **Pervasive virtual Content Distribution Network Services (vCDN)**: It covers the capacity for delivering scalable, pervasive vCDN services including HQ video streaming (live and/or VoD), in situations with significant variations in the context of flash crowd scenarios e.g., video sharing in stadiums or demonstrations, or sharing breaking news live feed, based on the concepts described in use cases 1 and 2.

Regarding the proposed use cases and their scope, the Smart contract (UC1) and Spectrum allocation (UC2) attend are more system and platform-oriented vision, lied to the technologies that will allow the resource sharing and the security and trust between multiple entities. The pervasive vCDN use case (UC3) is more oriented to a vertical application, besides of covering orchestration and licensing topics assuming that UC1 and UC2 are a base for it.

4.2. Smart Contracts for Ubiquitous Computing/Connectivity

4.2.1. Motivation and business rationale

Anywhere we currently see a traditional offline paper commercial/legal contractual relationship in the connectivity sector, a Smart Contract can potentially replace it. Current business processes in the telecoms sector are rigid, incur an inordinate amount of process friction owing to the manual nature of the initiation, oversight and management of bilateral and multilateral stakeholder relationships, and are generally temporally static i.e. once done, they can only be changed by specific manual interactions. This results in avoidable financial and non-financial cost to the sector, and arguably as a yet unquantified cost in terms of stifled innovation.

As an example, we consider a UK-based automotive manufacturing site that will be producing a 5G connected vehicle. The vehicle computer will expect to receive continuous over-the-air software updates to the various connected car services which will continue to evolve. This includes firmware updates to the vehicle operating system, previously updated via USB interface. In order to ensure type compliance, it will be necessary to demonstrate that the software update was completed and not subsequently rolled back unless authorised. This places significant handshake and crypto-signing requirements on the process at the time of the update. These issues would be magnified if firmware updates were to take place in ad hoc locations, for example,

once the vehicle is in the dealer distribution network. However, a significant number of vehicles will require updates after they leave the factory and before they enter the dealership network. Since the automotive manufacturer exports most of its production via a local UK seaport, this could mean the update might need to be accomplished in holding yards at the seaport or subsequently in one or more of several seaport storage yards in Europe before onwards distribution. The exit of the UK from the EU may impact this requirement as the automotive manufacturer may focus more sales effort in the UK and this could force a requirement for other more temporary requirement in UK storage areas e.g. seaport yards, mass vehicle storage sites, etc. This ongoing uncertainty as to the distribution of UK produced vehicles, therefore, poses a further challenge to the configuration of the connectivity to the expected vehicle storage areas. The firmware/hardware interface will likely require a handshake with a 5G core operating system and will probably expect this to be delivered over 5G Radio Access Network (RAN). However, given the complexity of the process, this might be best handled through Multi-Access Edge Compute (MEC) deployment at the gNode B. A 5G private network 'slice' could coordinate this function across multiple networks but the investment challenge required to provide 5G infrastructure at multiple temporary (greenfield) locations will be substantial and commercially unattractive to the automotive manufacturer. It is here, where 5GZORRO would allow the manufacturer to arrange a Smart Contract that reflect the agreements between the different parties, to request the use of the available 5G infrastructure, leasing the needed resources and services through the Marketplace and guaranteeing the connectivity in the mentioned areas avoiding infrastructure and management investments.

4.2.2. State of the Art/starting point

Whilst there are several industry consortia, and an increasing number of commercial actors participating in industry focused Proof of Concept ("PoC") projects that utilise DLT and Smart Contracts. These tend to be focused on intercarrier settlement and are still work in progress with no publicly disclosed enterprise production solutions currently commercially deployed.

TM Forum[11] is performing initial work with blockchain technology for different use cases based on its members' proposals, and following the *catalyst project* paradigm usually applied by the Forum.

First, the SLA Management use case explored in the Blockchain Unleashed catalyst project has implemented a smart-contract based solution (see Figure 4-1) that enables a new SLA monitoring process with many benefits when compared with currently used processes, namely: real time settlement and visibility, reduced settlement times and significant reduction in the cost of SLA monitoring due to reduced time to implement and manage SLAs.

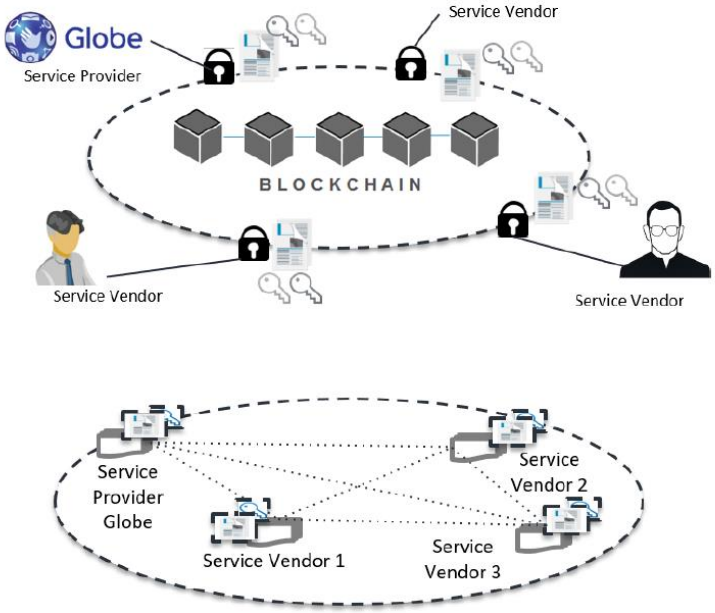


Figure 4-1 – TM Forum Blockchain Unleashed [11] catalyst project solution

A more recent catalyst project, the Telecom Infrastructure Marketplace [12], is exploring a blockchain-based marketplace for infrastructural assets to promote more agile, flexible and on-demand business and procurement models (e.g. under auction-based model) to perform 5G deployment scenarios. For example, to automatically discover, query and find in a "passive infra-structure" marketplace the frequency, the cell, the passive infrastructure and the backhaul for some dedicated purpose and need. In this case, smart contracts are used to automate and secure transactions and to provide traceability of the overall telco infrastructures among different partners.

In the telecoms sector specifically, there are several commercially-productive efforts implementing distributed ledger, smart contract and in some cases, tokenised technologies to solve various business problems. These include QLC Chain [13], Clear Blockchain [14], and more generally R3 Corda [15][16], through its work with the Carrier Business Automation Network (CBAN) and Enterprise Ethereum Alliance. The CBAN is focussed on supporting development of applications addressing wholesale voice settlement, fraud protection/mitigation, mobile roaming settlement and data on demand amongst other objectives; DLT/Blockchain is at its heart.

Outside of the telecom sector, but still in the broad utilities market, state of the art projects of note are Enerchain [17] and Powerledger [18], both involved with trust decentralisation of the sale of electricity, gas and water supply between wholesale and retail market participants.

There are enterprise production trials and PoCs employing smart-contract technologies deployed in other sectors including healthcare, insurance and banking.

These previous experiences are being leveraged by 5GZORRO in this use case, on the core tenets of standardisation, efficiency and transparency. Design, development and implementation of the systems architecture can be usefully and valuably informed by existing State of the Art ("state of the art ") examples of offline technologies and processes in this regard such as the Incoterms International Commercial Terms) which have been in use for decades as a standardised contractual model, comparable to Service Level Agreement criteria, which govern international trade, and/or the ISDA Master Agreement used by the financial markets sector to govern Over The Counter ("OTC") financial derivative instrument transactions.

4.2.3. 5GZORRO novelty

The 5GZORRO project is aware of the aforementioned adjacent industry business process customs; these adjacent industries have implemented elements of standardisation, transparency and efficiency to similarly global and densely populated competitive stakeholder market landscapes (trade and financial markets, for example). 5GZORRO will design, build and implement smart-contract oracles and smart-contract libraries that will facilitate multiparty resource discovery and allocation processes throughout the 5GZORRO platform.

Smart-contracts and smart-contract libraries will support a 5GZORRO decentralized catalogue which will hold the collection of 5GZORRO product offers available to be traded among providers and consumers. We distinguish two types of product offers:

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

In principle, the 5GZORRO Catalogue is more focused on Resource product offers and not on Service product offers. However, if we consider extreme situations where we could also tokenise resources from end-users (e.g. residential 5G routers) it will facilitate to have a single catalogue where end-customers simultaneously manage 5G Services consumption and 5G Resources offers.

It should also be noted that it is envisaged more than one type of 5GZORRO catalogue, each holding different types of services and resources depending on the market segments and verticals to be addressed. For

example, one catalogue type targeting end-users holding its third-party resources and one catalogue type targeting Service Providers holding carrier grade resources.

Deploying DLT solutions, including smart contracts, enables hitherto technically unavailable levels of business automation, transparency, trust in trust-less environments, and immutability of transactional information, and the establishment of commercial relationships between unknown and untrusted third-party market participants requiring zero-touch and trust instantiation of commercial contracts ad hoc.

4.2.4. Overall use case description

The implementation of a sector native DLT environment with Smart Contract functionality intrinsically allows for trust-less interactions between multiple parties. This is valuable versus current systems and processes that only allow for trusted interactions between two parties at any given time.

In addition to enabling decentralized trust for multi-party interactions and SLA management as above, the implementation of DLT-anchored smart contracts in 5GZORRO will also allow the implementation of oracles (elements in red in Figure 4-3).

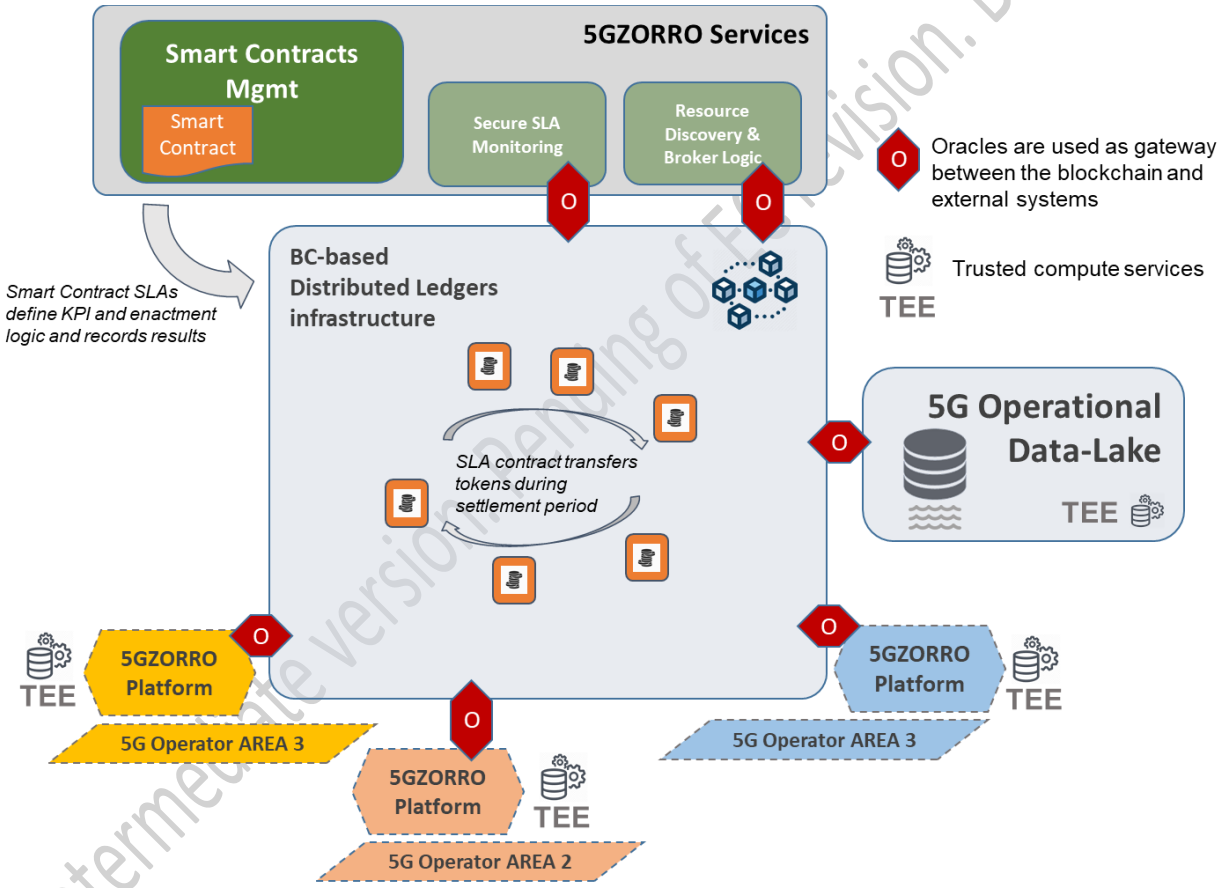


Figure 4-2 Overall UC1 environment graphical description

These oracles are agents that find and verify real-world occurrences and submit this information to a distributed ledger to be used by the 5GZORRO smart contracts. Oracles provide external data and trigger smart contract executions when predefined conditions are met. Due to the relevance of data contained in the oracle and the actions they trigger, it is essential to provide a trust and secure environment that enables smart contracts execution and oracle information management without compromising their integrity.

5GZORRO leverages the tokenization of assets concept, enabled by DLTs based Smart Contracts, to support trading operations with specific SLA required. Two or more 5GZORRO stakeholders will be able to trade, set-up and operate a new technical/commercial relationship via a Smart Contract for 3rd-party resource leasing

with SLA associated to the operation. The trade of these assets, is managed by smart contracts and requires a high level of trust among them. From the 5GZORRO stakeholders' perspective, the Distributed Ledgers will support a distributed catalogue of resources which can be used for the service deployment. For providing these functionalities we leverage the following approaches, also graphically explained in Figure 4-3:

- Develop Standardised Smart Contracts anchored in a shared DLT environment to enable parties to verify the identity of participating nodes (service provider-owned infrastructure) and the resource contribution of those nodes in relation to the end-to-end provision of services to the consumer and to other DSPs/CSPs
- Build new oracle-based smart contracts containing commercially relevant data such as unit pricing e.g. MB/ minute, RAM, CPU's, latency measure, etc. to provide a central point of reference for ad hoc multi-party commercial/SLA smart contracts among parties. An oracle-enabled smart contract containing standard pricing, FX data, etc. can provide a similar central reference source to inter-party commercial/SLA smart contracts. Commercial pricing terms can be periodically updated in the smart contracts between parties and can call out to oracles for reference data.
- Use of a private permissioned DLT to facilitate the aforementioned requirements in addition to addressing enterprise use cases such as performance (transaction throughput and consensus latency), identity (KYC/AML requirements) and transaction/data privacy that are not generally satisfied by a public DLT.
- To further supplement the increased levels of privacy achieved via a private permissioned DLT, a Trusted Execution Environment (TEE) could be used in 5GZORRO to ensure attestation of the trustworthiness of data being submitted to the DLT. For example, an aggregator of certain data (such as SLA metrics) could be executed in the TEE in order to establish a level of trust prior to it being submitted to the ledger.

This level of automation, coupled with the decentralized trust interactions enabled intrinsically by the cryptography-based foundation of the DLT environment, will result in 5GZORRO zero-touch multi-party interactions among all parties required to provide a seamless and ubiquitous computing and connectivity service and experience to the end users. Whilst one of the main goals of 5GZORRO is infrastructural resource sharing in a zero-touch environment, as analysed in this use case, Smart contract/DLT implementations are envisioned to be ubiquitously applicable throughout the industry, horizontally and vertically speaking i.e. the implementation will be simple yet effective, and therefore expected to be recursive throughout the architecture and infrastructure technical landscape.

4.2.4.1. Stakeholders involved

Existing and new potential stakeholders will be beneficially and potentially disruptively affected by a broad implementation and adoption of Smart Contract technologies in the context of 5GZORRO. These include:

- **Communication Service Providers (CSP) [***acting as Resource Providers***]**, including Tier One fixed and mobile network owners and operators.

  The standardization of offline manually initiated and managed contracts via a smart-contract library has the potential to bring substantial operational cost savings to Tier One network operators and owners. This will likely also include significant reduction in headcount which gives rise to non-technical and non-business considerations for the operator/owner, including internal political considerations. Further evolutionary considerations arising from smart contract implementation include the opening of a relatively closed current commercial infrastructure landscape which operates as a regulated monopoly vs. an open free market ad hoc landscape. This presents as yet undefined new revenue opportunities for existing infrastructure resource providers, but also brings new competitive actors into the current landscape.

- **Verticals consortia** [*acting as Service Consumers*]

The purchase and operational management and control of network infrastructure and services is financially expensive. With the implementation of 5GZORRO, new consumers may enter the market as a zero-touch automated TEE, in part enabled by smart contracts, allows previously excluded consumers into the markets. These may take the form of purchasing consortia seeking economies of scale through purchasing aggregation such as have emerged in the public sector in different areas and countries across Europe.

- **Mobile (Virtual) Network Operators (MVNO)** [*acting as Resource Consumers and Service Providers*]

  MVNOs, both as Service Providers and Resource Consumers of Tier One Network CSP's, may benefit from substantially increased commercial and technical dynamism enabled by smart contract implementation. Rather than being tied to a single MNO for network infrastructure and resources, smart contracts can give rise to a new and dynamic market landscape for ad hoc consumption from multiple different Tier One network resource owners, provided an appropriate evolution of the regulatory landscape takes place, to guarantee consumer rights and avoid hidden consolidation practices.

- **National Spectrum and Resource Regulators and Managers** [*acting as Regulator Authority*]

  The existing regulatory, oversight and enforcement roles of bodies such as OFCOM in the United Kingdom and the FCC in the US, as well as supranational bodies such as ICAAN, are able to be mapped into the 5GZORRO system architecture. Such mapping is implemented via Smart Contracts, again mapping the existing business and regulatory framework and hierarchies and automating execution of these roles and permissions into the 5GZORRO system. For example, the rights of mobile and virtual mobile network operators to create spectokens (this term is further described in section 4.3) based on the existing license rights of each as spectrum usage rights owners in a national jurisdiction. The terms of such usage mapping into the Smart Contract terms and being regulated and permissioned by the Regulator Authority, in this case the national spectrum regulator in the jurisdiction in question.

- **Software vendors**.

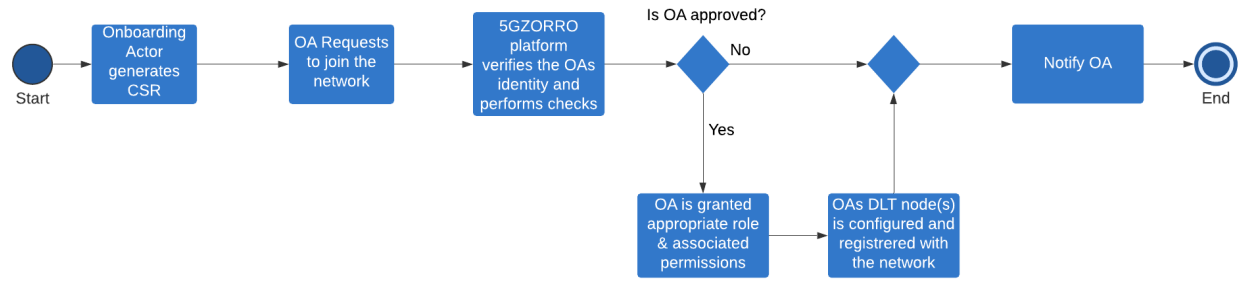
  Vendors will increase their commercial possibilities onboarding their products in the 5GZORRO platform in the form of virtual functions (VFs), that will be exposed in the 5GZORRO catalogue, allowing other stakeholders to use their products to compose customized services. Scenarios

4.2.4.2. Scenario 1: User and Organisation On-Boarding

Scenario Name	**User and Organization On-Boarding**
Rationale/ objective	To enable new Resource Providers and Service Providers to be enrolled into the 5GZORRO DLT system and begin advertising their resources (Resource Providers) or services (Service Providers) that combine one or more resource offers and can begin to consume services (Service Consumers). Once onboarded the party can begin advertising/consuming resources/services based on their assigned roles & permissions. A party requires a DLT based Marketplace node in order to partake in the decentralized governance and state changes associated with any resources/services that they wish to advertise or consume; interactions being immutable once committed to the ledger. Resource/service state changes are modelled in subsequent scenarios below.
Stakeholders involved	• 3rd Party Infrastructure Provider (Resource Providers) • CSPs & MVNOs (Resource Consumers/Service Providers) • Verticals (Service Consumers) Each of the above stakeholders will either already be registered with the 5GZORRO platform and operate one or more DLT nodes or be the stakeholder

	being onboarded. For the purposes of the remainder of this scenario they will be termed as follows: • Existing network participants (existing actor EA) • New entrant (onboarding actor: OA) • Marketplace Node Operator – each Resource Provider and Service Provider will operate at least one node to form part of the Marketplace network • Governance Administrator • Regulator Authorities (i.e. in case when regulated resource is involved such as frequencies)
Pre-conditions	• OA has discovered the 5GZORRO system (e.g. through a portal) • The network has been initialised and Governance administrators' peers exists with ability to grant all permissions to new actors joining the network • The OA has initiated a local peer operator node

Procedure/ workflow	A wide variety of mechanisms are available to achieve several elements of the following workflow (e.g. identifiers, approval, etc); the appropriate choice will become evident as other parts of the 5GZORRO's requirements are formulated, and the detailed design process commences.
	• OA requests to join the network.
	• OA's join request is handled by an approval mechanism; resulting in approval/rejection by the governance administrators
	  ○ A variety of implementation mechanisms available depending on requirements that emerge from other UCs.
	  ○ This may be accepted or rejected. For example, if the OA's identity cannot be verified.
	  ○ Workflow cannot proceed until approval is granted (consensus).
	• OA is granted permissions
	  ○ Permissions based upon business role and capabilities
	  ○ Determines which smart contracts the actor can execute, actions they can take on the network, permissions they can grant other actors, etc.

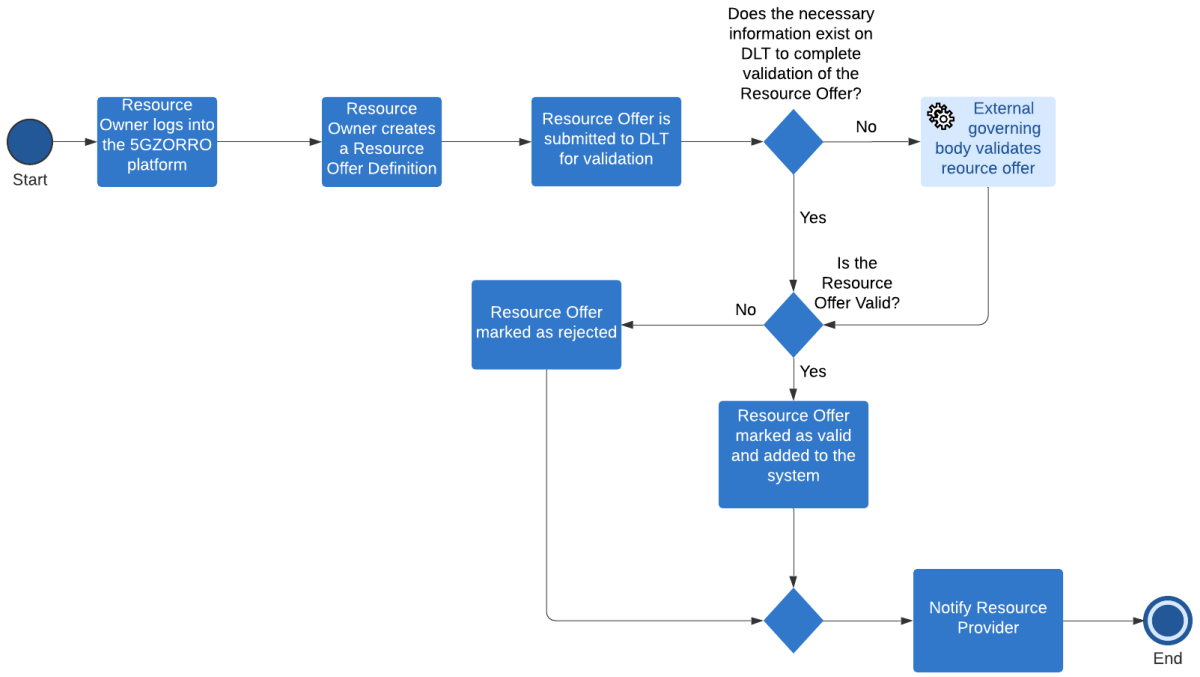
	
Envisioned architectural functionality	• Each actor is represented by a credential that allows parties to be uniquely identified and validated, whilst also ensuring secure private communications and non-repudiation where necessary. • Network of nodes comprising the distributed ledger based 5GZORRO Marketplace, with each Marketplace Node Operator (Resource Provider / Service Provider) having a copy of the world state (eventually consistent). ○ Permissions for new entrants is based upon distributed consensus. The specifics will be determined according to configuration (e.g. N Governance Administrators with administrator permission must approve a new party).

	• Oracles will be used for interacting outside of the blockchain. For example, when invoking external services, or when participants want to query the network from their business applications.
KPIs	• New Resource Providers, Resource Consumers, Service Providers are enrolled into the platform. • Each stakeholder participating in the 5GZORRO Marketplace is approved • Acceptance/rejection (consensus) when joining of a new node to the DLT network should be completed in less than 15 minutes. • 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. • 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.
Benefits of 5GZORRO approach	• Establishment of a private permissioned distributed portal for the purposes of trading resources underpinned by DLT • All actors can be tied to a legal identity, making underlying contracts that are entered enforceable • Allows potentially non-trusting parties to engage with one another when previously they would not have been able to without a trusted 3rd Party

Table 4-1 User and organization onboarding

4.2.4.3. Scenario 2: Resource Provider creating a Resource Offer

Scenario Name	**Resource provider creating a resource offer**
Rationale/ objective	Resource Provider creates a Resource Offer describing a capability on the 5GZORRO marketplace via a smart contract, so that Resource Consumers can discover and consume those resources. Software Resource Offers may have licensing agreements associated.
Storyboard	1. Resource Provider Operator logs into 5GZORRO system 2. Resource Provider Operator navigates to resource discovery and broker logic service. 3. Resource Provider Operator navigates to resource/provider portal 4. Resource Provider Operator uses the resource definition builder to create a new resource advertisement document using the resource document builder, including the resource offered, the terms of the resource and pricing. 5. Resource Provider Operator saves and publishes the resource advertisement document and is submitted (pending verification) 6. The system verifies that the resource is valid. For example, an external service may check that this operator is the owner of the Spectrum rights in the region claimed by the document using region governing body (Regulator Authority) 7. The Resource Offer is submitted to the ledger via a smart contract on the 5GZORRO platform at which point it becomes available in the resource catalogue
Stakeholders involved	• 3rd Party Infrastructure Provider (Resource Provider) • CSPs/M(V)NOs that publish resource offers (Resource Provider) • Software Vendors (Resource Provider) • Regulator Authority

Pre-conditions	• Resource Provider has been on-boarded onto the system • Resource Provider has been given resource publishing rights
Procedure/ workflow	Resource Provider Operator publishes resource definition via the resource definition portal. 1. Portal application translates the resource offer (RO) into the 5GZORRO resource offer Domain Specific Language (RO-DSL) and posts the document to the RO validation contract. 2. The RO validation service performs validation, using an Oracle service if necessary, to check the validity of the RO. For example, ensuring that the Resource Provider has the relevant spectrum rights by querying Regulator Authority. 3. If the RO is marked as valid, it is registered with the marketplace service and becomes available for negotiation/consumption via the catalogue 4. If the RO is marked as invalid, it is marked as rejected and a notification is returned to the user via the portal.
	
Envisioned architectural functionality	• A DSL for describing resource offers • Verification of resource offers • Decentralised catalogue application for recording resource offers • VNF licensing
KPIs	• 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). • DLT does not allow double spending of a registered resource • Resources are discoverable in the catalogue by all registered consumers within 5 minutes of being registered and verified. • DLT has an immutable record of current and historic rights over a resource
Benefits of 5GZORRO approach	• Resource providers can easily register their resources and any associated licence agreements • Resource offers are discoverable via distributed catalogue by all registered Resource Consumers

	• A Catalogue underpinned by DLT provides a singular view of resource availability • Automated verification of proposed resource offers e.g. checks on regulated resources

Table 4-2 Resource provider creating a resource offer

4.2.4.4. Scenario 3: Service Provider creating a Service Offer

Scenario Name	**Service provider creating a service offer**
Rationale/ objective	Services are formally represented as service offers in the 5GZORRO Marketplace via a smart contract, which embeds all the network characteristics in the form of SLA requirements that are expected to be fully satisfied by a suitable slice creation, potentially in a multi-party environment. 5GZORRO service offers are composed of one or several resources, that could be spectrum, software and/or hardware resources from different Resource Providers. In order to optimize the service offered and satisfy efficiently the agreed network requirements reflected in the contract, these services could be offered in several operational domains, i.e. different MNOs, CSPs or third-party providers. Service Consumers discover the services that fulfil their requirements and consume those services. This is the case of the private 5G network introduced in section 4.2.1, where it is a requirement to provide the 5G coverage in multiple temporary (greenfield) locations, but the MEC nodes and the gNodeBs may be owned by different operators in the area.
Storyboard	1. Service Provider Operator logs into 5GZORRO system 2. Service Provider Operator navigates to resource discovery and broker logic service. 3. Service Provider Operator uses the service definition builder to create a new service advertisement document using the service document builder, including the service offered, the terms of the service and pricing. 4. Service Provider Operator saves and publishes the service advertisement document 5. The system verifies that the service is valid. Any checks that cannot be carried out in a deterministic manner should be achieved via an oracle. 6. The service is published as a smart contract on the 5GZORRO platform at which point the service becomes available in the service catalogue.
Stakeholders involved	• CSPs / M(V)NOs (Resource Consumer & Service Provider)
Pre-conditions	• Service Provider has been on-boarded onto the system • Resource provider capabilities have been added and are discoverable • Service Provider has been given service publishing rights
Procedure/ workflow	1. Service Provider Operator publishes service definition comprising one or more Resource Offers via the service definition portal. Resource offers may have licensing agreements associated. 2. Portal application translates the service offer (SO) into the 5GZORRO service offer DSL (SO-DSL) and posts the document to the SO validation contract. 3. The SO validation services (implemented as on-chain smart contract) validates the service and if necessary, uses an Oracle service to check the validity of the SO.

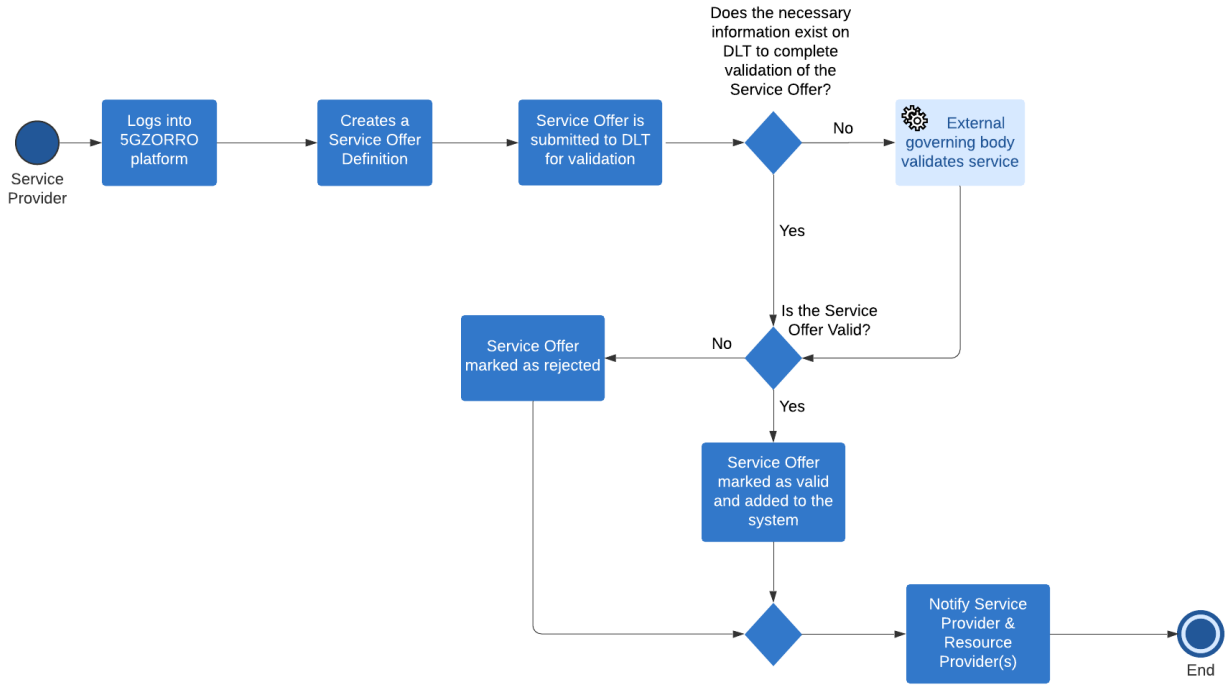
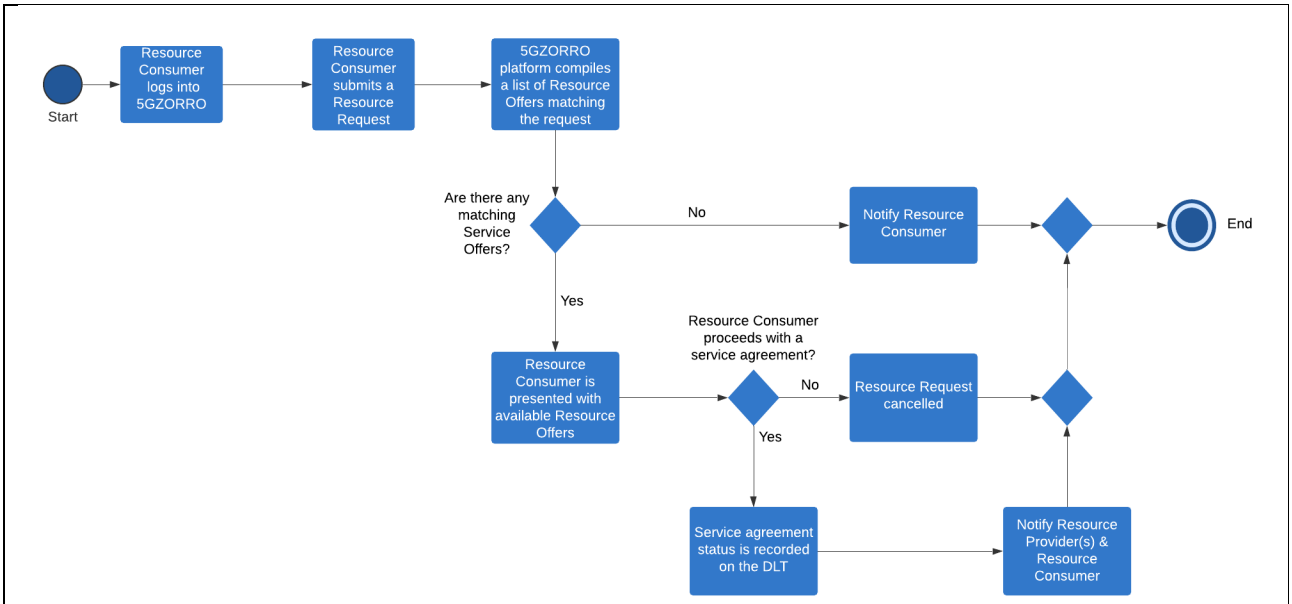
	4. If the SO is marked as valid, it is registered with the marketplace service (another smart contract implementation) and becomes available for negotiation/consumption. 5. If the SO is marked as invalid, it is marked as rejected and a notification is returned to the use via the SO portal.
	
Envisioned architectural functionality	• A Service Offer Builder Distributed Application (DApp) client. • A DSL for describing service offers • Oracle service for validating service offers • Marketplace application for recording service offers • Licensing application for software components
KPIs	• Resources are intelligently matched to a query and results are returned in less than 1 minute. • Only verified available resources are discoverable and should be discoverable within 5 minutes of being added to the catalogue. • Services can be composed of one or more resources and from one or more providers. • 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. • Establishment of smart contract (service agreement) should be completed within 5 minutes.
Benefits of 5GZORRO approach	• Ability to compose diverse service offers comprising resources potentially from a range of providers • A service catalogue underpinned by DLT provides a singular view of service availability

Table 4-3 Service Provider creating a Service Offer

4.2.4.5. Scenario 4: Resource Consumer Request

Scenario Name	Resource Consumer Request
Rationale/ objective	Resource Consumer (RC) requests resources by defining a resource consumption request, the request is realised in the 5GZORRO platform through a matching and brokering process, the result is a set of smart contracts capturing the legal agreements between all parties on the immutable ledger.
Storyboard	1. RC logs in and navigates the resource logic and brokering service portal 2. RC navigates to the resource request builder application 3. RC defines their resource requirements and requested terms such as service levels and pricing using the builder application. 4. RC saves and publishes the request. 5. The system matches the RC resource request with one or more resources for realising the request. 6. RC is notified of a match via the resource discovery portal. 7. RC confirms which resource is to be consumed from the available matches. 8. The system records the confirmation and creates smart contracts in a secure channel representing the service agreements between all parties. Current 'ownership' of any resources transfers to the consumer for the lifetime of the contract; automated state changes carried out by smart contracts according to defined workflow requirements. 9. Resource Provider and Resource Consumer are notified that the resource agreements are live.
Stakeholders involved	• CSPs/M(V)NOs • Third Party infrastructure providers
Pre-conditions	• RC has been on-boarded onto the system • There are enough Resource Offers registered with the system to realise the RC request
Procedure/ workflow	1. RC saves and publishes the request 2. A resource request document is generated by the builder application that describes the request using the resource request DSL (RR-DSL). 3. The RR-DSL document is posted to the matching service via API call. 4. The matching service uses models built by the machine learning, data lake component as well as a list of available resource offers to create a list of potential matches for the request. Each match may include several resources if the request requires it. 5. The matches response is retrieved by the discovery portal and displayed in the browser for the RC to either confirm or reject. 6. If the RC confirms a match, the portal sends a to the smart contract lifecycle manager to realise the contracts on the DLT



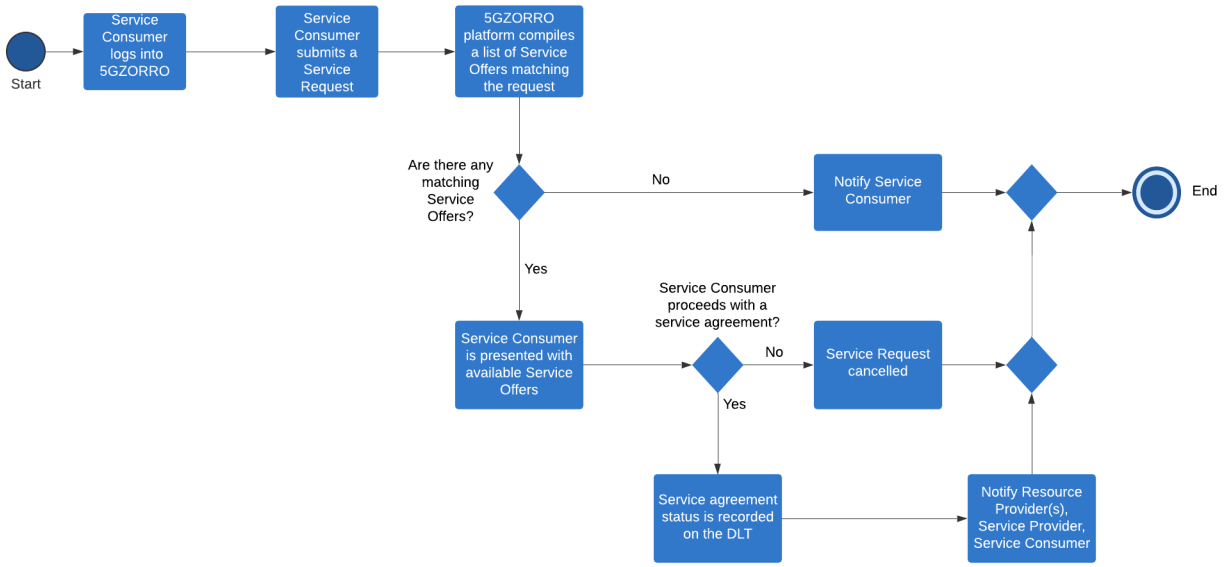
Envisioned architectural functionality	• A Resource Request Builder DApp • A DSL for describing resource requests • Resource matching application for mapping resource requests to resource offers
KPIs	• Resources are discoverable via the portal based on specified requirements. Time to compile resource matches should be less than 1 minute • Resource consumers can engage in a service with the underlying system automating contract agreements and resource provisioning. The process of contract negotiation and resource allocation should take < 5 minutes • Demonstrate a minimum of 3 providers/operators of virtualized resources or services for spectrum, radio/edge/core compute or networks to demonstrate distributed element
Benefits of 5GZORRO approach	• Smart resource discovery/matching for consumers • Zero-touch establishment of associated legal agreements between parties using smart contracts and associated legal prose • Zero-touch provisioning of resources

Table 4-4 Resource Consumer Request

4.2.4.6. Scenario 5: Service Consumer Request

Scenario Name	**Service Consumer Request**
Rationale/ objective	Service Consumer (SC) requests services by defining a service consumption request. This request is realised in the 5GZORRO platform through a matching and brokering process and its result is a set of smart contracts capturing the legal agreements between all parties on the immutable ledger. A service request could be composed of explicit segments to create and connect the private 5G network slice described in section 4.2.1, like a set of RUs to serve in certain areas, different edge capabilities to deploy concrete RAN components, like a vCU or a set of DUs (if far edge nodes), or the 5GC components to create the 5G network and keep updated the vehicle's firmware, with a set of latency or bandwidth requirements for each segment associated to the request.
Storyboard	1. SC logs in and navigates the resource logic and brokering service portal 2. SC navigates the service request builder application

	3. SC defines the overall network requirements and requested terms such as service levels and pricing using the builder application. 4. SC saves and publishes the request. 5. The system matches the SC service request with one or more services for realising the request. 6. SC is notified of a match via the service discovery portal. 7. SC confirms which service is to be consumed from the available matches. 8. The system records the confirmation and creates smart contracts in a secure channel representing the service agreements between all parties. Current 'ownership' of any resources comprising the service transfers to the consumer for the lifetime of the contract; automated state changes carried out by smart contracts according to defined workflow requirements. 9. Resource Provider, Service Provider and Service Consumer are notified that the service agreements are live.
Stakeholders involved	• CSPs/M(V)NOs • Verticals • Third Party infrastructure providers
Pre-conditions	• SC has been on-boarded onto the system • There are enough Service Offers registered with the system to realise the SC request
Procedure/ workflow	1. SC saves and publishes the request 2. A service request document is generated by the builder application that describes the request using the service request DSL (SR-DSL). 3. The SR-DSL document is posted to the matching service via API call. 4. The matching service uses models built by the machine learning, data lake component as well as a list of available service offers to create a list of potential matches for the request. Each match may include several resources if the request requires it. 5. The matches response is retrieved by the discovery portal and displayed in the browser for the SC to either confirm or reject. 6. If the SC confirms a match, the portal sends a to the smart contract lifecycle manager to realise the contracts on the DLT



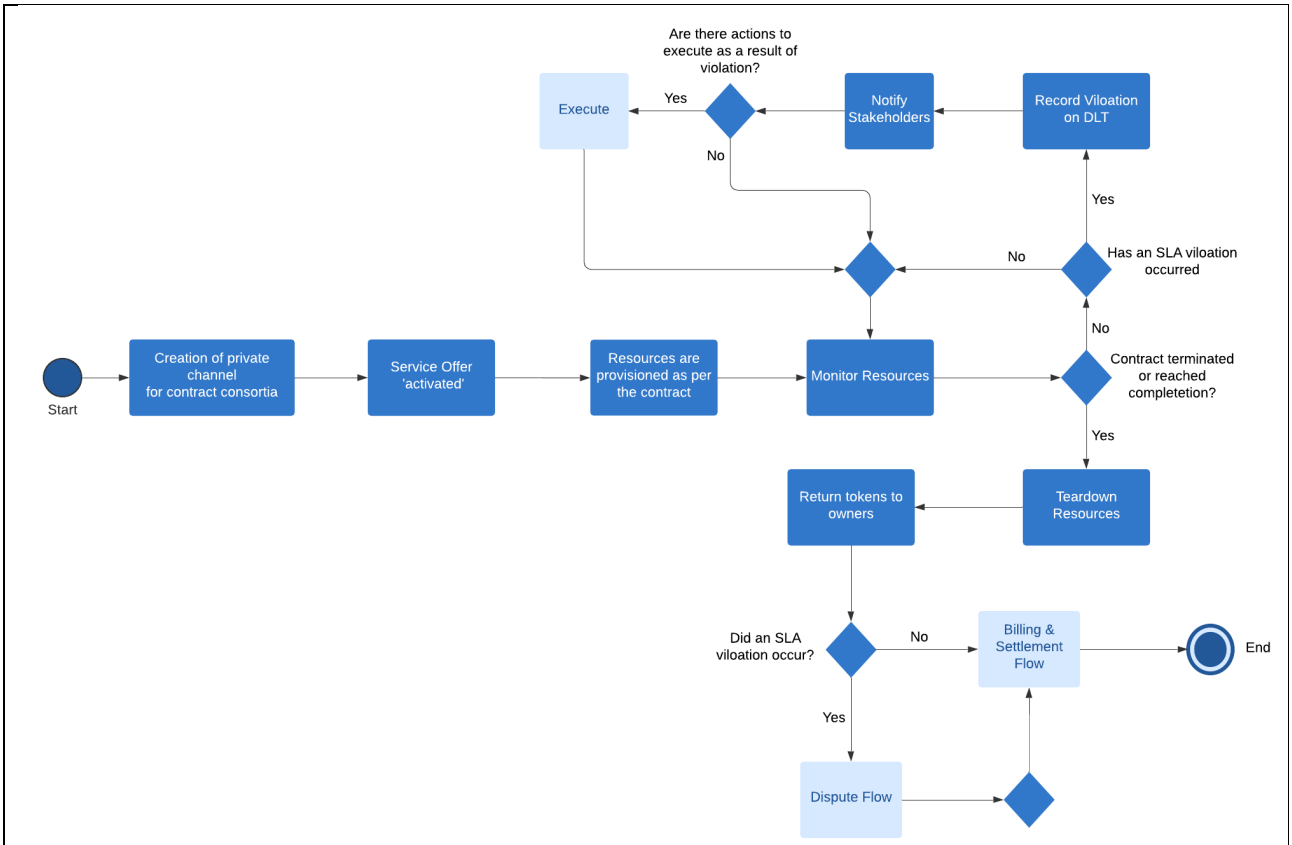
Envisioned architectural functionality	• A Service Request Builder DApp • A DSL for describing service requests • Service matching application for mapping service requests to service offers
KPIs	• Services are discoverable via the portal based on specified requirements. Time to compile service matches should be less than 1 minute • Service consumers are able to engage in a service with the underlying system automating contract agreements and resource allocation should take < 5 minutes • Demonstrate a minimum of 3 providers/operators of virtualized resources, services for spectrum, radio/edge/core compute or 5G network components to prove the distributed nature of the service
Benefits of 5GZORRO approach	• Smart service discovery/matching for consumers • Zero-touch establishment of associated legal agreements between parties using smart contracts and associated legal prose • Zero-touch provisioning of service resources

Table 4-5 Service Consumer Request

4.2.4.7. Scenario 6: Contract Lifecycle Management

Scenario Name	**Contract Lifecycle Management**
Rationale/ objective	Lifecycle management knits together the prior contract use-cases with state transitions that cause the business and technical events to be triggered. Zero-touch establishment and management of bilateral and multi-lateral agreements between Resource Providers and Resource Consumers, and Resource Providers, Service Providers and Service Consumers is at the heart of what the 5GZORRO platform will facilitate. Thus, the smart contract lifecycle management is the link with the inter-domain layer of 5GZORRO platform (see Figure 2-3). Once the establishment of an agreement is performed, the provisioning of resources is triggered in the Multi-domain Slice Orchestration and Management block, the resource and connectivity configuration provided by the Intelligent Cross-domain Service and Resource Management, the security and trust mechanisms provided by the Cross-domain Security and trust functionality are applied, and finally, the monitoring of the slice is performed in the Cross-domain Network Analytics module. Once the service is provided by the 5GZORRO platform, the Secure SLA Monitoring service enables retrieval of service and resource SLA and KPI related information between the parties. There are also conditional processes to deal with SLA violations, to resolve disputes, and to manage and notify parties of transitions between states.
Storyboard	1. Smart contract has already been established 2. System transitions to initialisation state 3. Resource/Service providers receives notification to provision resources/services and share technical data 4. Resource/Service providers mutually establish connections 5. Resource/Service consumer is notified that the system is ready and connects to relevant resource/service(s) 6. System transitions to monitoring state 7. System monitors resource/service providers for SLA violations, with participants informed of relevant events.

	8. System transitions resources/services to terminated state based upon criteria in smart contract
Stakeholders involved	• Third Parties (Resource providers) • CSPs & M(V)NOs (Service Providers / Resource Consumers) • Verticals (Service Consumers)
Pre-conditions	• Valid smart contract has been established between parties, and it is ready for execution • All actors are operating normally (i.e. no technical issues) and are properly enrolled on the platform.
Procedure/ workflow	• Execution of a contract between 1 or more parties (see single and multi-party contracts) o Establishment of a private channel between contract participants to enable mutual communications. o Provisioning of resources defined in the contract. o Providing technical data to parties via the private channel to enable interconnections between Resource providers, Service providers and Service consumer. • Monitoring/SLAs of contract (see SLAs) o Transition from initialisation state to monitoring state o SLAs are monitored and enforced o Notifications to inform parties of SLA violations and any consequent actions o Execution of alternative actions workflow due to SLA failures (e.g. provision alternative service). • Teardown/deprovisioning o Termination of any resources involved in contracts that require explicit teardown. ▪ Termination conditions are contract-specific, but examples could be time-based or condition-based o Return of tokens representing any resources/services to respective Resource/Service providers. o Settlement of any outstanding bills to counterparties ▪ Potential dispute process when settlement not agreed



Envisioned architectural functionality	• Smart Contract lifecycle management • SLA management using notifications and transitions
KPIs	• Service offer activation should be completed within 5 minutes • SLA measurements and validation from at least 3 operators involved in a multi-party service chain • An SLA violation is recorded on the DLT for a given resource within 15 minutes of occurrence
Benefits of 5GZORRO approach	• Zero-touch monitoring & SLA enforcement • Automated life-cycle management of resources and services • Building trust through provider trust scoring based on previous SLA performance

Table 4-6 Contract lifecycle management

4.3. Dynamic Spectrum Allocation

4.3.1. Motivation and business rationale

Spectrum is a scarce asset in an 'everything-connected' eco-system, and a key for cellular networks that depend on its availability for operation. The entirety of spectrum used for radio communications can be split into two types: licensed and unlicensed spectrum. The majority of (commercial) cellular communications make use of the licensed bands, where the regulatory domain assigns specific frequencies to operators and/or verticals. This is the case for 5G, but also for previous generations of the cellular networks (2G, 3G, 4G). The unlicensed band, however, is accessible by anyone and used by essentially localized technologies such as Wi-Fi, Bluetooth or IEEE 802.15.4.

The *efficient* use of spectrum is of the utmost importance, given the fact that it is not only a limited resource but subject to very strict regulation. Achieving a high degree of efficiency in this context refers to maximizing the usage of the spectrum over time and space. One way to increase usage is to introduce the concept of dynamic spectrum sharing, where available (i.e. unused) spectrum is assigned over a limited duration of time and for a specific geographic location. This can be of interest for a variety of 5G actors that may require licensed spectrum in a very limited geographical area or a temporary increase of capacity under certain circumstances. Further examples are listed in a document provided by Dynamic Spectrum Alliance [19], who carries out technical studies for the European Commission. In the first case, we can think of Industry 4.0 factories or industry campuses, in the second of events requiring dedicated attention by a (group of) specific network service provider(s).

As an example for a case where the access to spectrum in a geographical is required, a smart factory that has come to an agreement with radio hardware providers to deploy some radio infrastructure within the premises of the factory is assumed. These radio installations are meant to provide connectivity to services for any user equipment or machines connected to them, relying on technologies such as 5GNR, LTE or Wi-Fi. In such a scenario, the use of unlicensed spectrum bands, e.g. with Wi-Fi, is one option. It can provide the basic means for user connectivity without considering any possible issues, such as interference or uncontrolled radio congestion, that go along with it. However, whenever radio technologies are used that operate in licensed bands or when a dedicated access, along with a certain QoS is desired (which can be key factors for the operation a smart factory), the smart factory needs to obtain the rights to use spectrum for its own purposes. Adjudged spectrum can be both licensed or unlicensed: licensed bands are commonly assigned to MNOs on a national level, requiring to reach an agreement with the regulator or the MNOs to be able to use a range of spectrum for the smart factory. But even the use of unlicensed bands requires to follow certain rules and guidelines imposed by the national laws. Examples for that are the limits of transmission power or even duty cycle limitations for certain radio technologies.

As such, there needs to be a way for the smart factory to obtain the rights to use spectrum in the geographical area that constitutes the factory and for (limited) periods of time. The fact that the use of spectrum is not only limited in space, but also in time is important, since the factory might not require the range of spectrum permanently and subsequently it also does not want to pay for unused capacities: only reduced capacities might be required during night time, when less users are connected or during bank holidays and weekends. 5GZORRO addresses this scenario by providing the means to the smart factory to arrange a Smart Contract with the Regulator or other owners of a range of spectrum that captures an agreement in which the use of spectrum in an area and over a timeframe is assigned to the smart factory, along with a set of SLAs. Validated and trusted radio monitoring and enforcement elements deployed in the infrastructure assure that the assigned spectrum is used correctly.

The Citizens Broadband Radio Services (CBRS), proposed by the Federal Communications Commission (FCC), applies spectrum sharing by assigning different priorities of access to specific users/verticals. Other specific uses of the spectrum can also be considered: A potential example could be the use of spectrum for high-capacity point to point connectivity within a certain area; the E-band (60-90 GHz) is particularly of interest to 5G operators and due to its high potential for reuse can be a good candidate for shared access. In 5GZORRO we plan to address these needs through a spectrum allocation solution capable to provide shared spectrum access service, with higher degree of flexibility by integrating various state-of-the-art (state of the art) technologies and solutions for implementation.

4.3.2. State of the Art/starting point

Moving from 4G to 5G introduces a series of key challenges from technical and business points of view. 5G deployments, with their massive number of small cells to be deployed, forces operators to look for new ways of managing spectrum allocation and its usage to achieve very small delays and high throughput while considering the interests of business stakeholders and end-users. On the one hand, for operators, a massive deployment of small cells and the required backhauling and networking infrastructure is a big investment

that can represent a challenge, but also a risk when considering the traditional roll-out models. On the other hand, for one of such users and actors operating in a constrained geographical area (such as an industry 4.0 factory, a stadium, or the automotive example presented in section 4.3.1), gaining the rights to use dedicated spectrum is a difficult and a slow process. Current business models loosely consider the requirements of localized and temporary use of spectrum, while initial efforts in this direction by some regulators (e.g. OFCOM in UK and BNetzA in Germany) still do not cover the expected automation service envisaged by the aforementioned example for automotive.

In in 5GZORRO, state of the art technologies and software solutions are integrated and enhanced to implement a dynamic spectrum allocation mechanism with associated marketplace. the 5GZORRO *spectrum market* will be a platform where stakeholders can buy and sell spectrum for a specific geographical area for a limited time duration.

By leveraging DLT/Blockchain technologies, the market platform can provide enhanced interoperability, automation, privacy and trust; key facets to a solution that spans opaque potentially distrusting organisations. Transactional immutability provided by smart contracts that backs the automated trading and monitoring of assets, is at the heart of giving rise to these properties of the solution whilst providing stakeholder privacy assurances and legally enforceability. As discussed in 4.2.2, there are already several projects and commercial solutions across the telecoms, energy and finance sectors that are relevant to the delivery of the 5GZORRO marketplace.

Using DLTs and a blockchain to track the assignment of the spectrum, the capability of controlling and configuring different Radio Access Technologies (RAT), monitoring the usage of spectrum, are key features required to implement the use case. The sharing and allocation of spectrum relying on blockchain has become a popular research topic lately and several approaches and aspects have been discussed in the literature. For example, blockchains can be used to enable and secure a database that determines which users can access the spectrum [20] in a competitive manner (first-come-first-served). While this work introduces several interesting concepts, such as primary users that generate the currency used to access the spectrum and the security associated to the virtual wallet holding this currency, the work misses a few important aspects required in 5GZORRO: a single licence is assumed under which the entirety of the spectrum falls, unlike what is planned for 5GZORRO, where the regulator determines when and where which spectrum can be used by other users. As such, the exclusive use or applying specific shares of the available spectrum are also missing, features that are required to be able to offer SLAs and formal contracts between 5GZORRO marketplace participants. The application of blockchain to implement CBRS has also been studied [21], mapping the basic CBRS functions to transaction that can be written to a blockchain. The big gain of this solution is the improved automatization of business-to-business workflows, an outcome which also expected from the 5GZORRO solution.

Further, in a more general approach, the benefits and drawbacks of using blockchain in comparison to traditional approaches (centralised databases, exclusive licensing, formal, written contracts about spectrum usage, etc.) is made and different approaches to spectrum sharing depending on the intended use of the spectrum are made [22]. This overview and the proposals of how blockchain can be used to achieve different ways to share spectrum. The concept of using smart contracts to store information about usage and usage rights is introduced here as well. Overall, this work provides useful technical and ideological inputs on how to use the blockchain technology for the project and how to integrate it the overall architecture.

As a matter of fact, the 5GZORRO consortium brings not only expertise in 5G architectures into the project, but it also contributes with a broad set of assets in forms of software and hardware solutions that can help to implement the dynamic spectrum allocation use case and to adopt approaches on the blockchain usage. The assets will be used to form a novel software framework to demonstrate this UC. In the following the current starting point in terms of available assets is presented.

In order to enforce the smart contracts that determine how acquired spectrum can be used by a stakeholder, a radio configuration and management framework is necessary. For a significant spectrum sharing and marketplace solution, it is needed to support multiple RATs, both from the licensed and unlicensed band.

Further, a spectrum monitoring and enforcement system will have to be implemented that will take care of contrasting the use of spectrum defined in smart contracts with the actual usage made in infrastructure.

The RAN controller developed by i2CAT, *RACOON*, features a set of slicing mechanisms for both Wi-Fi (IEEE 802.11) and LTE technologies that allow for the creation of virtual networks on top of physical devices. RACOON exposes an API that enables other instances to configure and control RAN devices. Currently, the controller supports and integrates small cells and Wi-Fi APs, which are interfaced via the NETCONF protocol[1]. With RACOON, it is possible to instantiate slices over Wi-Fi and LTE. A Wi-Fi slice consist of one or multiple virtual APs with their own SSID and a dedicated share of airtime in percentage instantiated on top of one or multiple Wi-Fi interfaces that can be distributed geographically. The Wi-Fi APs enable connectivity to the users with or without security. On the other hand, slices that can also include Small Cells (LTE): using MOCN, a per slice PLMNID is set up on top of a physical small cell and a dedicated tunnel is set up to the corresponding EPC. The EPC can be external or it can run as part of the slice (vEPC). Apart from setting up the RAN, services and applications for each radio slice can also be added to the slice when using i2CAT's NEUTROON [23] solution. This overall neutral hosting solution uses OSM and OpenStack to enable the creation of slices that include compute nodes where services can be deployed (such as vEPCs). Using VLANs, the traffic towards and from Wi-Fi APs or small cells is relayed to any services running in the compute slice. In 5GZORRO, RACOON's Wi-Fi slicing mechanism could be used to enforce a specific configuration of the RAN when setting up a smart contract for infrastructure that is managed by RACOON. As such, it could be demonstrated that RACOON is a useful asset for the 5GZORRO platform, as it reduces the risk of SLA breaches by setting up and controlling the RAN elements. Beyond this, new features will be evaluated to keep track of the spectrum usage of the RAN equipment and to enable the fulfilment of smart contracts issued by the 5GZORRO platform.

The *5G-EmPOWER controller* [24], developed by FBK, is a centralized software-defined RAN controller covering both LTE and Wi-Fi access networks. RAN slicing and multi-tenancy are two key features supported by 5G-EmPOWER. An LTE slice in 5G-EmPOWER is identified by a unique PLMN ID and it consists of a fixed number of Physical Resource Blocks (PRBs) from a physical/virtual base station and a dedicated MAC schedular that is responsible for scheduling these PRBs to users belonging to that particular slice. The base station is connected to the EPC through a dedicated transport link. A Wi-Fi slice is identified by a unique SSID and it involves access points sharing airtime between the slices. The high-level architecture of the 5G-EmPOWER platform is shown in Figure 4-4, which is composed of infrastructure, control, and vertical layers. The core of the system resides in the control layer enabled by the 5G-EmPOWER Operating System. The infrastructure layer includes LTE eNodeBs and Wi-Fi access points, both embedded with the 5G-EmPOWER Agent responsible for abstracting and exposing the radio resource/spectrum (e.g., PRBs, load, radio links) information to the control layer. The control layer is responsible for initiating the RAN slice creation, updating, and deletion process based on the radio resource capacity of the radio nodes and SLA requirements of the verticals. This communication takes place through the southbound interface implemented by the OpenEmpower protocol using a persistent TCP connection. Furthermore, it defines a set of high–level programming abstractions that are exposed to the verticals using a Python-based Software Development Kit (SDK). With such an approach, multiple tenants can be hosted on the same physical infrastructure. Conversely, each tenant can instantiate several RAN slices so that diverse SLA requirements of various verticals can be satisfied. Finally, the same RAN slice can also be shared among various user equipment (UEs), and a single UE can make use of several RAN slices simultaneously.

[1] It is to be evaluated whether further technologies will be integrated during the project.

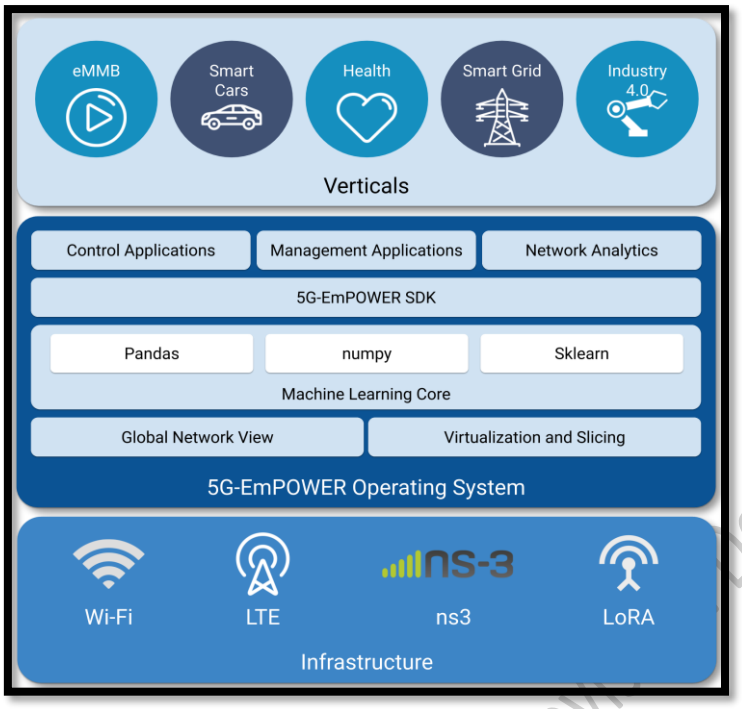


Figure 4-3: 5G-EmPOWER Architecture

The COHERENT project [25] designed and developed a control framework for 5G heterogeneous mobile networks, by leveraging the abstraction of physical and MAC layers states, behaviours and functions in the network, to enable a centralized network view of the underlying radio networks and to offer operators a powerful means to dynamically and efficiently control/share spectrum and radio network resources in the heterogeneous networks. The project addresses spectrum management in three separate contexts, which include Inter-operator spectrum sharing, Intra-operator spectrum sharing, and Micro-level spectrum sharing, by identifying key stakeholders and technical challenges involved in each context. However, the project does not address the problems involved in trust issues associated with spectrum sharing between different stakeholders and also lacks on-the-fly real-time SLA contract sealing/negotiations for spectrum sharing, which is one of the main goals in 5GZORRO.

A main outcome of the 5GCity project [26] is a 5G resources management platform that enables neutral hosts to allocate their radio and compute resources to different verticals. The platform, based on Open Source Mano, OpenStack and proprietary software solutions to handle RAN resources, gives neutral hosts a powerful tool to dedicate network slices on-demand. Such slices contain compute resources to host services and RAN elements to provide connectivity to end-users. The main principles of the slice resource allocation can be carried over to 5GZORRO, to set up and configure resources whenever a new smart contract is initiated.

The ElectroSense project [27], where University of Murcia is taking part, is aiming to create a network of radio sensors enabling the collection and later analysis of spectrum data. Following a crowd-sourcing approach and based on cheap commodity hardware, it offers aggregated spectrum information over an Interactive Web App and an open API. More than 170 sensors are currently registered around Europe and more can be added with an easy registration process. Based on a similar approach, but considering the specific nature and definition of this use case, some of the principles of the project can be considered in 5GZORRO, while extending the concept of active monitoring to the efficient use of licensed and unlicensed spectrum.

4.3.3. 5GZORRO novelty: spectokens and spectrum market

5GZORRO plans to innovate with a series of features that implement spectrum sharing and combines them into a novel solution that is more flexible and easier to manage comparable to CBRS or any other similar

approach. The 5GZORRO solution will offer a high degree of dynamism, by introducing the novel concept of *spectokens*. Spectokens are non-fungible tokens represent the rights to use spectrum in a location over a duration of time and will be available for sale and trading by appropriately permissioned 5GZORRO users. Each Smart Contract will contain the business terms of the resource being represented by the spectoken. This will not only allow for optimized use of the spectrum, but it will also enable near real-time, on-demand contracting with an optimal price for the resources being traded.

The implementation of a 5GZORRO distributed ledger provides for an archiving system to reflect the status and use of spectokens, shared amongst 5GZORRO users and which records transactions between 5GZORRO users. The computer code that is the foundation of each Smart Contract, representing the business logic of its offline counterpart document, is also written onto and stored in the shared ledger.

The 5GZORRO ledger is maintained by the employment of a consensus mechanism, with a hierarchy of users variably permissioned within the 5GZORRO environment to undertake certain actions (or not). This permissioned hierarchy will map closely to existing domain business structures, roles and permissions. In the case of regulated spectrum, for example, it is envisioned that in the initial deployment of 5GZORRO, national regulators (or similar state bodies responsible for national spectrum regulation) sit at the top of the hierarchy.

This hierarchy-based, business-level consensus will permit the creation of spectokens, by Resource Providers and will provide governance, transparency and oversight for 5GZORRO resource consumers as to the right to create non-fungible spectokens. A Smart Contract, recorded on the 5GZORRO ledger, will govern the issuance of such spectokens by Resource Providers.

The novelty of DLT and Smart Contracts and the non-fungible spectokens will be within the bounds and technical limitations of a private, permissioned consortium ledger environment, and the “If This, Then That” logic bounds of Smart Contract implementations. In this initial deployment, network consensus in the 5GZORRO ledger is based on hierarchical permissions set by the equivalent of Network Administrators of 5GZORRO, and is different initially from pure Network Consensus as might ordinarily be understood in the context of public, permission-less distributed ledger deployments such as Bitcoin[28] or Ethereum[3] public blockchains. Of course, several aspects will need to be evaluated, such as whether to rely on permissioned or permission-less blockchain. Such decisions will directly impact how the proof of trust is performed.

In order to enable the dynamic spectrum allocation in 5GZORRO, DLTs will be used to employ dynamicity, trust and transparency mechanisms between the host RAN provider, who allocates a portion of the radio resource/spectrum for a certain time, and the Resource Consumer, by agreeing on the terms and conditions of SLA in explicit detail using Smart Contracts.

Another novelty item that 5GZRORRO brings to this use case is the inclusion of AI-powered trading agents forming part of the 5GZORRO ecosystem that track the transactions of spectokens in the spectrum market, learning the spectrum leasing habits of the users. Based on its learning, the AI-powered trading agent could suggest optimal selling prices to stakeholders that own spectrum and are interested in selling unused spectrum at optimal prices. This can leverage a more efficient use of the spectrum, which is one of the goals a regulator pursues. Further, along the same line, the usage of RAN slices, i.e. the active usage of spectokens by different users, will be tracked and algorithms will support proactive and dynamic RAN slice adjustments to optimize the usage of spectrum while respecting the SLAs. The main metric to be tracked and which will serve to determine how the RAN slices are tuned will be the active usage (e.g. percentage over time of the airtime for Wi-Fi, resource blocks in LTE, etc.). Secondary metrics, such as the average or peak number of connected users.

4.3.4. Overall use case description

The 5GZORRO spectrum market will be the place where stakeholders can participate in trading of spectokens for different radio technologies. A variety of stakeholders from the public and private sector will benefit from the features of the 5GZORRO spectrum market. In the following, we provide a detailed description of the use case and the items that will be investigated during the project.

The dynamic spectrum allocation use case mainly deals with the creation, the trading and the use of spectokens which represent the right to use a certain radio bandwidth in a specific area for a limited amount of time. At the time of writing this document, some basic aspects of spectokens already are identified:

- Spectokens are created by the regulators of a country or region, who are responsible for approving their introduction into the spectrum market, and the trading rules among stakeholders.
- A spectoken is a unique, non-fungible token that represents the rights to use an atomic (non-divisible) range of frequency, e.g. 10 MHz in an area for a specific duration. The definition of the area associated with a spectoken needs to be evaluated during the project. It could refer to specific landmarks (e.g. a stadium, a city square, a factory building, etc.) or follow a more general approach, e.g. creating a grid of non-overlapping squares of 100x100m, 500x500m, or, in more general terms, a polygon forming a geographical area. For the pilots that will be performed in 5GZORRO project, an area will correspond to the lab in which the tests are performed. As a requirement, the RAN technologies deployed within such an area (e.g. small cells or Wi-Fi APs) need to be manageable by the RAN controllers that form part of the 5GZORRO platform. As such, spectokens are limited to areas that can be covered by this "integrated infrastructure".
- Apart from the association of spectrum bandwidth and location, a spectoken might also carry meta-data, such as the date of issuing, the last time the token was traded, the cost at which it is being traded, etc. It will be evaluated which information needs to form part of a spectoken and which information will form part of the smart contract that regulates how the spectokens are used.
- Spectokens can be traded among all stakeholders authorised to operate in the spectrum market. Each stakeholder can see which spectokens are owned by other stakeholders. Some information may not be transparent to all stakeholders (such as the original buy value of a spectoken may only be visible to the last buyer). Further, the trading needs to respect the constraints of the original spectoken, i.e. the bandwidth of a spectoken may not be further divided beyond its atomic
- Acquiring a spectoken gives the right to use the associated spectrum in the given area. The actual use of the spectrum is specified in a smart contract associated to one or several spectokens belonging to the same stakeholder. It is to be evaluated which information will be encoded in the spectoken and which information goes into the smart contract. The more is encoded into the spectoken, the less flexible the use of the spectoken will be. Any property that needs to be adaptable or easily modifiable needs to form part of a smart contract associated with one or several spectokens. The usage of spectokens determined by the smart contracts is then handed over to the enforcement and monitoring system of 5GZORRO, which implements the framework to configure the RAN elements and to apply the settings defined in the smart contract.

The regulator will be the one introducing spectokens into the spectrum market. Any stakeholder who wants to participate in the market, needs to go through an admission process. As an outcome of this admission process, the stakeholder has the means to establish a validated credential with the spectrum market, assuring its identity. Once spectokens are available in the market, a stakeholder may buy spectokens and agree on a smart contract that defines how the spectokens are used, e.g. which radio technology is to be used and the configuration of the physical layer of the radio technology. After that, the RAN controllers used in the spectrum apply the desired RAN configuration of the infrastructure.

The pilots and testing performed in this project will use a DLT-based permissioned blockchain environment instead of a public one. This ensures a controlled environment, where all stakeholders are aware of the market status and prices.

Implementing the terms of the spectrum related smart contract will be done by the monitoring and enforcement module envisioned in the 5GZORRO platform, which listens to specific events, such as smart contract creation or modifications. Using internal feedback from the RAN controllers and also feedbacks from external Oracles (trusted by other stakeholders and the 5GZORRO platform), the usage of the spectrum will be controlled and any deviation, i.e. violation of the smart contract's SLA, will be notified to the regulator.

This can trigger any subsequent actions, such as a sanction, which would be defined in the smart contract as well. The RAN controllers introduced in Section 4.3.2 can be used to force the RAN configuration determined in the smart contracts for infrastructure that is managed by the 5GZORRO platform. Apart from the enforcement of the SLAs from the smart contracts applied to the RAN, the RAN controllers will also implement monitoring features that can report to the 5GZORRO as a trusted component of the 5GZORRO platform. Any stakeholders with radio infrastructure who want to integrate their radio resources with the 5GZORRO platform to offer the resources on the spectrum market (e.g. like municipalities could do for a neutral hosting model), will require the deployment of a RAN controller as well, as explained in next section.

4.3.4.1. Stakeholders involved

We determine a set of stakeholders in addition to the basic ones present in all UCs (Governance Administrator, Marketplace Network Operator, etc.) Operator, etc.) who will have access to 5GZORRO's spectrum market and will be actively involved in the trading of spectokens:

- **Mobile (Virtual) Network Operators (MNOs) [***acting as Resource Provider / Service Provider/ Resource Consumer***]**: MNOs obtain licenses from the regulatory domain for certain ranges in the (licensed) spectrum. In 5GZORRO, MNOs will represent the key stakeholders who trade spectokens in the licensed spectrum. Mainly they are expected to acquire spectokens to be able to offer their services to users, but in some cases, they may resell their spectokens as well (e.g. to verticals, see below). M(V)NOs may also request spectrum, trading the tokens provided by other M(V)NOs. Additionally, M(V)NOs may own infrastructure that could be potentially integrated with the 5GZORRO platform to offer services on top. This depends on whether the necessary interfaces and management tools can be implemented in their hardware. If they do not have such infrastructure, they rely on third-party resource providers, such as the municipality. For the UC validations performed in 5GZORRO, we assume that M(V)NOs will deploy their services on top of third-party resources that are managed by the 5GZORRO platform.
- **Verticals from non-telco sectors (private venues) [***acting as Service Consumer***]**: They may require spectrum in a specific area over a certain time. The area can be restricted to a premise, e.g. a stadium where an event is hosted or a factory that uses 5G technologies to implement their services. Using 5GZORRO spectrum market will allow a vertical to acquire spectrum faster than with traditional approaches, making it possible to close contracts ad-hoc. Further, verticals will benefit from the increased granularity both for the area and duration when deciding where to request spectrum, enabling them to seal contracts that are tailored to their needs.
- **Municipalities (City Council) [***acting as Resource Providers / Service Provider/ Resource Consumers***]**: Public entities, like municipalities, play an important role in 5G deployments as they are owners of street furniture and public space in which compute and networking equipment can be installed. As such, apart from being enablers for deploying 5G infrastructures and services in specific areas (e.g. via neutral hosting as proposed in the 5GCITY project[26], they also can participate in the trading of spectokens to obtain rights of usage in specific areas, e.g. to host events that can last anything between a few hours or several days.
- **Regulator Authority**: All spectrum (licensed and unlicensed) carries legal obligations which are subject to the relevant competent authorities. From a spectrum management point of view, the competent authorities (regulator) oversee that the technical requirements attached to all spectrum are being respected, including ensuring non-interference. Licensed spectrum adds an additional process to ensure transparent and non-discriminatory grants for the rights of use to the market. So, one can view two distinct processes - managing spectrum for conformance and assigning rights for individual use. One is purely enforcement-related whereas the second one carries market-shaping and policy objectives. In 5GZORRO, the regulator will be introducing spectokens into the spectrum market.

It will be evaluated under which conditions a stakeholder can join the spectrum market (i.e. whether the Governance administrators manage the access or if it is automated) and under which conditions spectokens may be added to the market. This step will require the authentication and validation of stakeholders and their capacities. Once approved by the 5GZORRO platform, stakeholders that own spectrum licenses (regulator) will be able to add spectokens to the market when registering. The spectokens added by an authorized entity represent a specific share of the spectrum in a specific area. Both the definition of a share and the definition of an area, as well as how differently licensed and unlicensed bands are handled, are topics to be investigated later during the project. It is also up to be evaluated how the registration of spectokens is handled technically and legally. In this sense, the basic association of spectrum to a location and time could be further refined, by adding a certain flavour to spectokens, such as whether the sharing of the spectrum happens in the time or frequency domain (Time Division Duplex-TDD vs Frequency Division Duplex-FDD).

Once spectokens are added to the market, they become available to other spectrum market users, which can be bought by MNOs, municipalities and vertical industries to provide their services. Spectoken transactions are validated via the 5GZORRO platform and implemented via smart contracts. Spectrum monitoring and enforcement agents take care of assessing the use of LTE and Wi-Fi spectrum and the correct application of the smart contracts. The 5GZORRO platform will act as a hub between the spectrum market with its stakeholders and the agents that enforce the contracts on the hardware, hosting the spectrum database and the Access System (e.g. RAN controllers). Figure 4-4 depict the high-level interaction of the stakeholders with the 5GZORRO platform and how it interacts with different types of infrastructure.

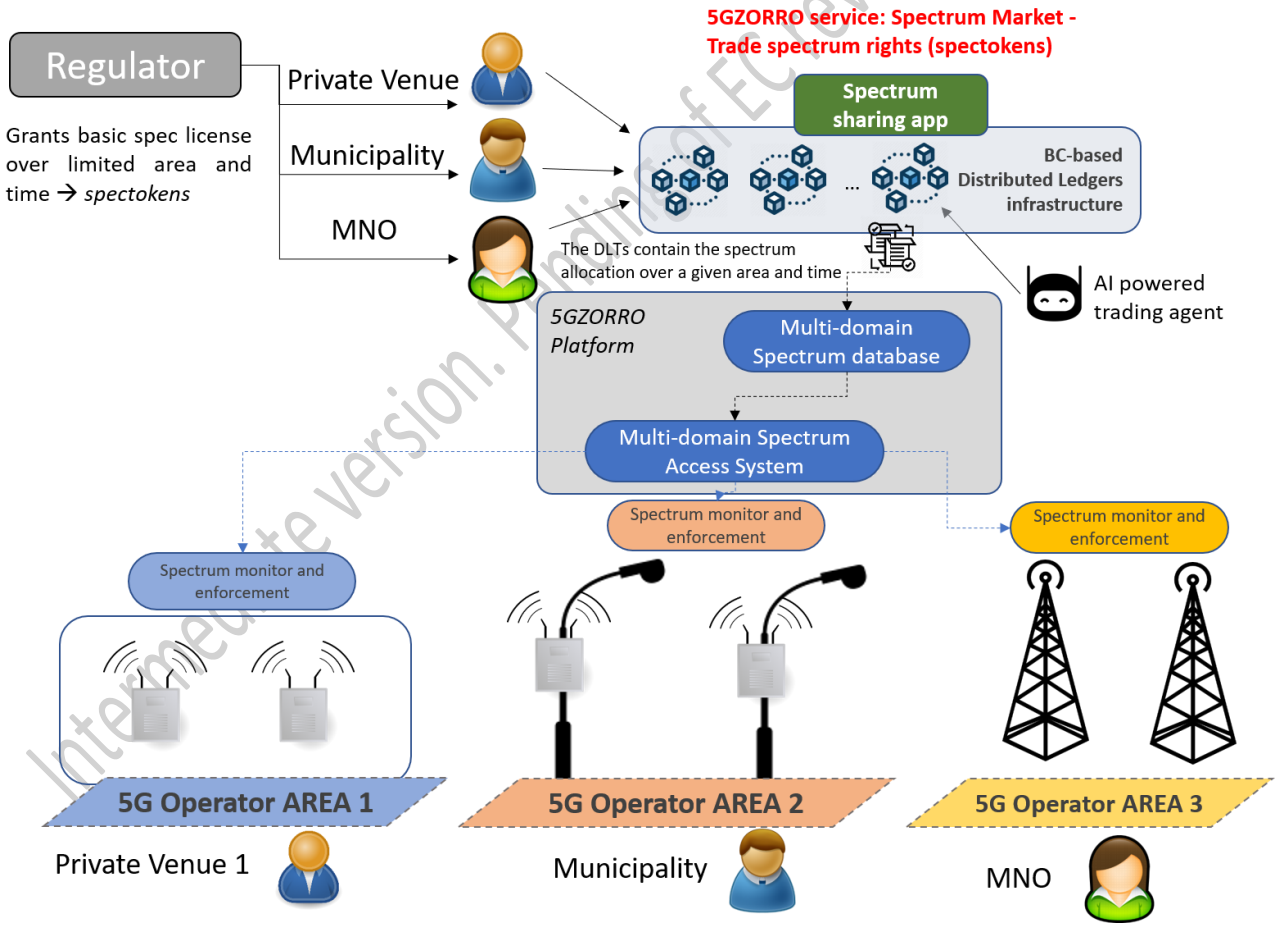


Figure 4-4 Actors and interactions in the 5GZORRO dynamic spectrum allocation UC

4.3.4.2. *Workflow*

The overall workflow for this use case is presented in Figure 4-5, including registration and spectrum trading among the stakeholders involved.

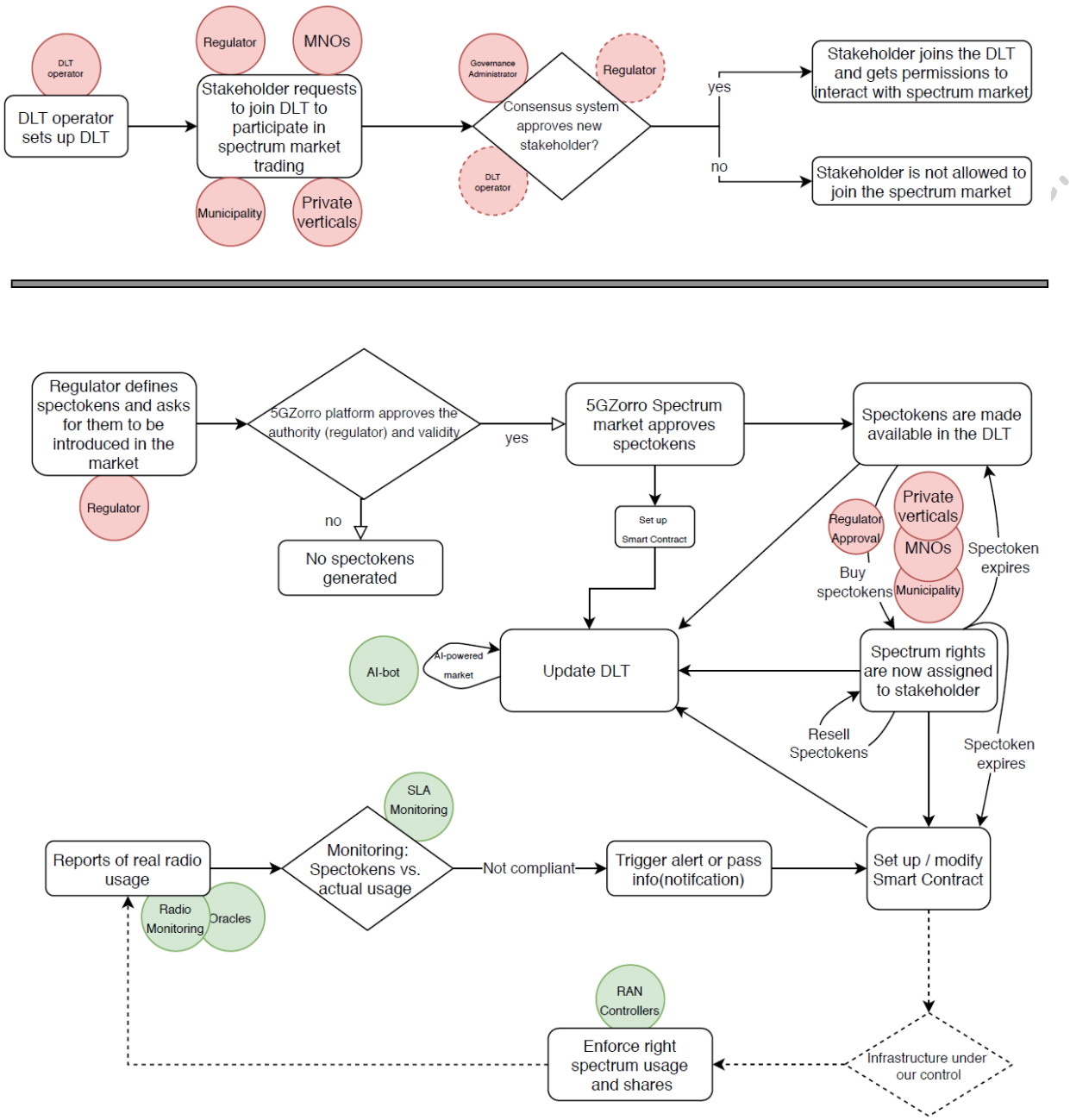


Figure 4-5 UC Workflow: Registration process (top) and spectrum trading (bottom)

4.3.5. Scenarios

This use case considers a total of 5 scenarios that demonstrate the main platform features that implement the dynamic spectrum allocation and how stakeholders interact with the system to participate in the spectrum market trading.

4.3.5.1. Scenario 1: DLT based Marketplace node setup and Stakeholder Registration

Scenario Name	**UC2_1: DLT based Marketplace node setup and Stakeholder Registration**
Rationale/ objective	A key element of the dynamic spectrum allocation use case is the DLT based Marketplace and the interaction of stakeholders with the DLT based Marketplace. This scenario covers the initial setup of the Marketplace node and the registration of users and the validation of different types of users (e.g. Service Providers).
Storyboard	• The Marketplace node operator initializes a DLT based Marketplace node and configures it, accepting new registrations from stakeholders that want to participate in the spectrum sharing. • The Regulator registers with the Marketplace (node is created and joins the Marketplace). • The Governance Administrators perform a governance check and identifies the Regulator as valid, assigning the Regulator entity a digital certificate with which interactions with the Marketplace are now possible. The Regulator obtains "Regulator permissions" that allow e.g. to create spectokens. • A Service Provider interested in trading spectrum registers with the Marketplace (node is created and joins the Marketplace). • Via consensus among the Governance Administrators, the Regulator (and if required from other relevant stakeholders with authority), the Service Provider is approved or rejected. In case of acceptance, the new stakeholder obtains a digital certificate with which interactions with the Marketplace are now possible. The Service provider joins with "Service Provider permissions", e.g. making it possible to buy a spectoken or reselling it.
Stakeholders involved	• Regulator Authority, Marketplace node operator, Governance Administrator, M(V)NO or Municipalities
Pre-conditions	• The Governance administrator has to have the means to perform governance checks to validate the identity of stakeholders joining the Marketplace.
Procedure/ workflow	• Stakeholder initializes Marketplace node, configuring it to work in a private (enterprise network) • The Regulator accesses the 5GZORRO app or web interface that allows him to join the spectrum sharing Marketplace. A node is created on the Regulator side and it joins the Marketplace. A certificate is assigned to the stakeholder. • Governance Administrators get notified about the new node having joined the Marketplace and performs a (manual) governance check. This check is done to determine the authenticity of the Regulator and to assign a certificate with which the Regulator will have the rights to perform specific transaction on the Marketplace. • The Regulator obtains the digital certificate and is now able to perform transactions on the Marketplace.

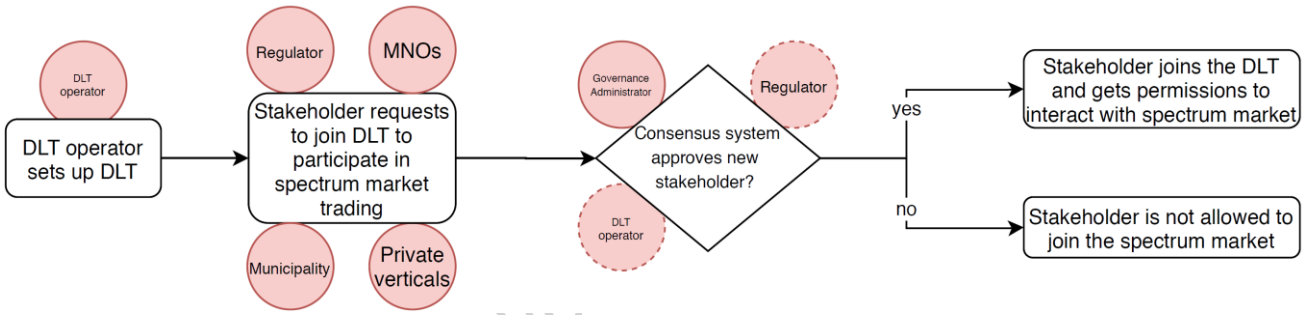
	• The Service Provider accesses the 5GZORRO app or web interface that allows him to join the spectrum sharing Marketplace. A node is created on the Service Provider side and it joins the Marketplace. A certificate is assigned to the user. • The Governance Administrator, the Regulator and any other entity with decision rights get notified about the new node having joined the Marketplace. A check about the validity of the joining stakeholder is performed. This check is done to determine the authenticity of the Service Provider and to assign a certificate with which the Service Provider will have the rights to perform specific transaction on the Marketplace or to be rejected in case no consensus is obtained. • With a positive outcome of the check, the Service Provider obtains the digital certificate and is now able to perform transaction on the Marketplace. • Whenever a new stakeholder registers, if this stakeholder has had any previous trust relationship with the 5GZORRO platform, the level of trust may be mapped to determine which rights for specific types of transactions are already available from the start. If no such trust relationship has existed before, only a set of minimal allowed transactions are available to the new stakeholder.
	
Business models	• Onboarding new users to join the Marketplace so they can participate in spectrum trading, essential for the UC.
Envisioned architectural functionality	• Spectrum App/Web interface • DLT based Marketplace for allowing for stakeholder to register and to perform spectoken transactions
KPIs	• The spectrum market allows different types of users to register, obtaining a digital certificate and the adequate set of permissions to perform transactions on the Marketplace. This registration can be done in less than 1h. • Safety: Only trusted stakeholders are allowed to interact with the system and stakeholder will have a different level of permissions. • Trust: Decisions of which stakeholders are allowed to join and whether they obtain certain rights needs to be decided in a consensus between relevant entities participating in the Marketplace (Governance Administrator, Regulator)
Benefits of 5GZORRO approach	• A trusted relationship between the Stakeholders and the 5GZORRO platform can be established via the DLT based Marketplace principles. • The Marketplace provides different levels of permissions for different stakeholders in a secure manner.

Table 4-7 Marketplace node setup and Stakeholder Registration

4.3.5.2. Scenario 2: Introducing spectokens into the spectrum market and trading of spectokens

Scenario Name	UC2_2: Introducing spectokens into the spectrum market and trading of spectokens
Rationale/ objective	Before trading of spectokens can happen in the spectrum market, the regulator authority has to introduce them. As such, this scenario deals with the introduction of spectokens into the spectrum market and it demonstrates how stakeholders can trade theses spectokens.
Storyboard	• Regulator approves the use of spectrum in different areas (defines spectokens) • The Marketplace validates the identity of the regulator and the permissions associated to the role of the Regulator. If the identity is validated and the spectokens aren't considered duplicates, the request to create spectokens is approved. • A smart contract running on the Marketplace DLT checks if the proposed spectokens can be added to the spectrum market. Valid spectokens are added to the Marketplace DLT. • MNO/Verticals/Municipalities access the spectrum market and can see the available spectokens. They now can buy or resell spectokens. • First time issuing of spectokens for a stakeholder requires Regulator's approval, whereas transferring spectokens can be done without Regulator approval. • After a successful transaction, be it generation or trading spectokens, the new status of spectoken distribution is kept in the Marketplace DLT. • The updated spectoken assignment and availability is displayed in the spectrum sharing App.
Stakeholders involved	• Regulator Authority, Industry Verticals, M(V)NO, Municipalities
Pre-conditions	• All stakeholders have to be registered in 5GZORRO and have to have their digital certificates in order to be able to interact with the Marketplace DLT.
Procedure/ workflow	• Regulator's identity as trusted stakeholder is confirmed (digital certificate) and access to the Marketplace is granted. • Regulator uses app or web interface to determine new availability of spectrum in a specific geographic location, i.e. a new set of spectokens is defined. • The new spectokens are approved in the Marketplace and the Marketplace DLT is updated. For that a transaction is performed on the Marketplace DLT. A smart contract is associated to the spectoken (that determines the price, for example). • The new spectoken distribution can now be consulted from the spectrum market app. • Stakeholders that play the role of Service Providers and Service Consumers (MNO/Industry vertical/municipalities) log into the spectrum market app to browse available spectokens.

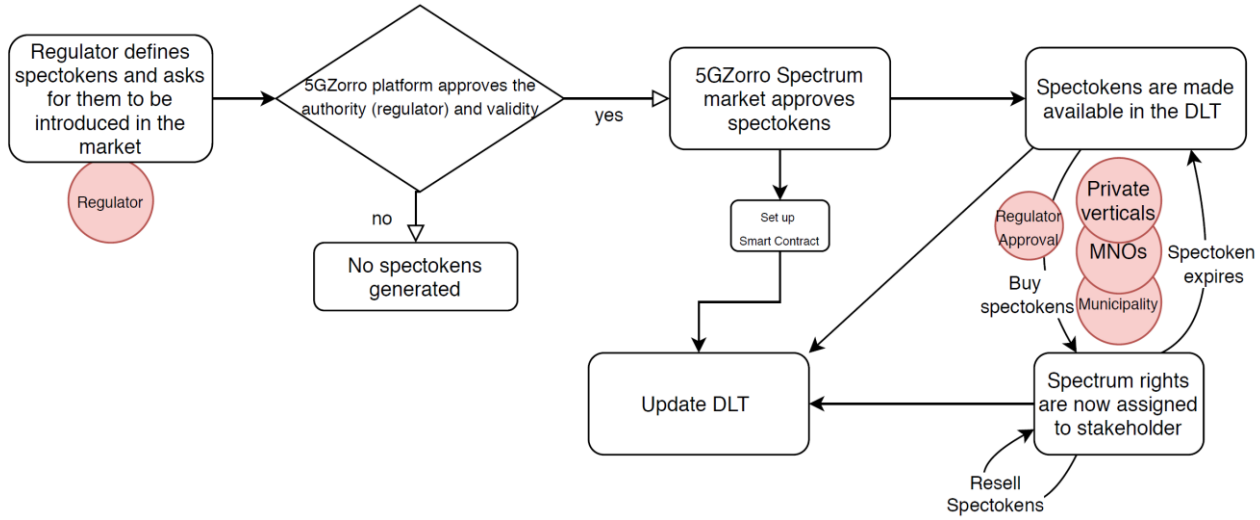
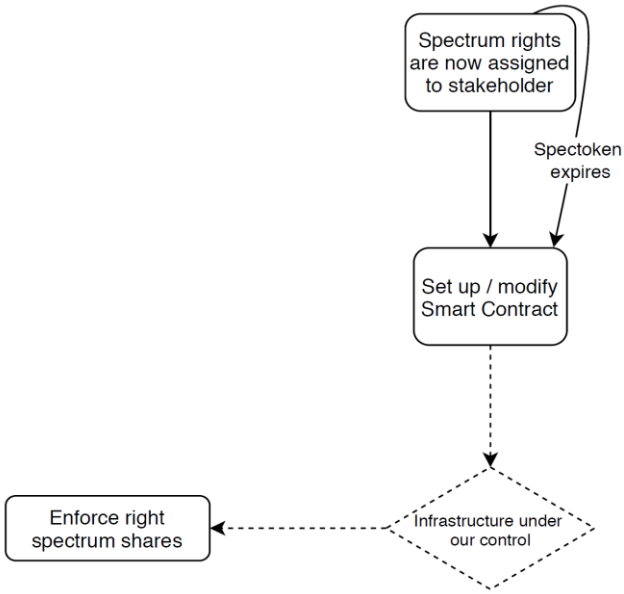
	• The stakeholder chooses one or more spectokens via the app to be bought. • For issuing spectrum the first time, the transaction needs to be approved by the Regulator. For reissuing, the process is automated. The transaction is validated and a smart contract is generated or the existing one is updated (in case of a reissue) for the future use of the spectrum. • The Marketplace DLT is now reflecting the new status of spectoken distribution and the smart contracts reflect the sealed deals.
	
Business models	• Regulator can create new spectokens, Stakeholder can trade these spectokens.
Envisioned architectural functionality	• Spectrum App • Marketplace DLTs for keeping track of spectoken distribution • Marketplace DLT transactions to generate spectokens and to buy them
KPIs	• Regulator can introduce spectokens within 5 minutes • Transaction of registering spectoken(s) can be completed within 1 minute • Transaction of buying spectoken(s) can be completed within 2 minutes
Benefits of 5GZORRO approach	• Faster and more flexible trading of spectrum usage rights • Secure transaction

Table 4-8 Introducing spectokens into the spectrum market and trading of spectokens

4.3.5.3. Scenario 3: Sealing smart contracts to use allocated spectrum

Scenario Name	UC2_3: Sealing smart contracts to use allocated spectrum
Rationale/ objective	Once a service provider or service consumer has obtained a spectoken, a smart contract is made which determines which technology will be used and other key parameters of the spectrum usage.
Storyboard	• The stakeholder (service provider/consumer) chooses how the assigned spectrum is to be used, e.g. which RAT is to be used and further details about the usage.

	• The Marketplace checks how the user wants to use the spectrum and creates one or several smart contracts that capture the different aspects of these settings. These smart contracts are bilateral and impose a set of regulations and SLAs. • The smart contracts are written to the Marketplace DLT and are "initiated". • The 5GZORRO monitoring and enforcement system applies the configuration to the radio infrastructure (since we assume that all infrastructure can be controlled by the 5GZORRO RAN controllers).
Stakeholders involved	• Industry Verticals / MNO / Municipalities
Pre-conditions	• Service Provider/Consumer has to have bought spectokens on top of which a service can be deployed
Procedure/ workflow	• The stakeholder owning spectokens accesses the 5GZORRO spectrum market app service t that allows to define a new "service" on how to use the bought spectrum. • The Marketplace is aware of the availability of spectokens of the stakeholder and allows to enable the usage of these spectokens (e.g. the choice of a radio technology according to the available spectokens and the availability of the infrastructure resources). • After determining all settings and rules for the usage that respects the requirements and restrictions from the regulatory side and the service provider/consumer side, a smart contract is generated. The smart contract also enables any necessary interfaces towards the service provider / service consumer. • The smart contract triggers the configuration of the infrastructure via the monitoring and enforcement component (dedicated API). • The stakeholder gets a notification that the service (smart contract) is now active and the requested spectrum is ready to be used.

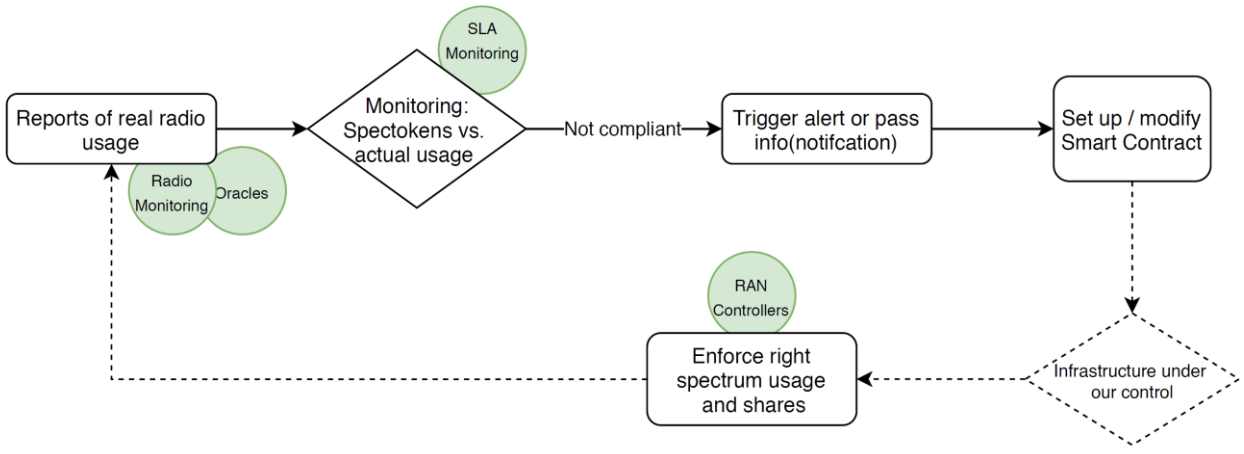


Business models	• Stakeholder will need to determine the type of service they want to be in place, this procedure determines the smart contract and the SLAs that will need to be respected by both sides (Stakeholder and 5GZORRO platform).
Envisioned architectural functionality	• The Marketplace DLT can be updated with smart contracts that determine the SLAs and the configuration of the services for the Stakeholders. • Monitoring and enforcement modules can communicate with smart contracts (RPCs). • RAN controller is capable to accept new service creations and to enable correct usage of RATs
KPIs	• The 5GZORRO infrastructure is able to apply the settings specified in the smart contract within 10 minutes
Benefits of 5GZORRO approach	• Desired use of spectrum and SLAs are converted to a secure smart-contract and the settings are directly implemented on the physical infrastructure, making it a very quick process to obtain requested spectrum • Shared use of spectrum on top of a same physical device (provided by the resource provider) is possible thanks to features implemented in the RAN controllers, i.e. multiple “slices” can run on top of it.

Table 4-9 Sealing smart contracts to use allocated spectrum

4.3.5.4. Scenario 4 Spectrum usage monitoring and SLA control

Scenario Name	**UC2_4: Spectrum usage monitoring and SLA control**
Rationale/ objective	Once smart contracts are in place and the infrastructure is configured, the monitoring system sends reports of the usage to the 5GZORRO platform. If an SLA is not met as per definition in the smart contracts an alert is triggered.

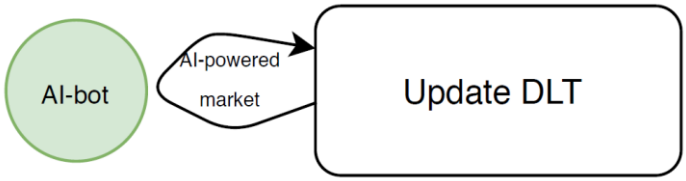
Storyboard	• Internal monitoring or external monitoring system gathers information about radio usage. • The information is passed to the 5GZORRO platform that checks if there are any inconsistencies between the SLAs defined in the smart contracts and the actual usage. • If any inconsistency is found, the 5GZORRO platform triggers an alert that is fed back to the smart contract and may trigger further actions (e.g. sanctions).
Stakeholders involved	• Industry Verticals / MNO / Municipalities
Pre-conditions	• Smart contract(s) are defining a certain usage of the spectrum • Monitoring system needs to be able to capture the key parameters of spectrum usage • If any external monitoring is applied and/or external inputs are introduced to the smart contracts
Procedure/ workflow	• The 5GZORRO monitoring elements gather information of spectrum usage. • The information is passed to the 5GZORRO platform. • The usage of the spectrum is compared to the existing smart contracts and fed back to them. • If an irregularity is detected, an action is triggered (sanction/notification/etc.).
	
Envisioned architectural functionality	• Monitoring and enforcement system (internal) • Oracles as “Gateways” into smart contracts
KPIs	• SLAs determined in a smart contract are respected: SLA breach is noticed within 2 minutes • Monitoring system provides status reports at least every 15 seconds

Benefits of 5GZORRO approach	• Feedback from monitoring system allows to keep track in real time of the spectrum usage. • SLA violations are detected immediately and can trigger reactions that affect the active smart contracts

Table 4-10 Spectrum usage monitoring and SLA control

4.3.5.5. Scenario 5: AI-powered Spectrum Market

Scenario Name	**UC2_5: AI-powered Spectrum Market**
Rationale/ objective	The Regulator introduces spectokens with a specific price into the spectrum market. Not always all spectokens will be bought, leaving some spectrum in certain geographical areas unused. This inefficiency from a business point of view can be addressed by implementing an AI-powered agent that can help to analyse the market behaviour and that can propose price alterations to the regulator to make unused spectrum more attractive during specific times or in specific regions.
Storyboard	• The AI-bot, another node participating in the DLT, pulls information about the trading habits in the spectrum market from the DLT. • The bot analyses if there is unused spectrum that is not bought or used by any stakeholder in certain regions or during certain periods of time. • The AI-bot proposes better offers for unused spectrum, by providing feedback to the smart contracts in place for spectokens that are still to be issued (not for spectokens already owned by stakeholders). • The Regulator can decide certain parameters, such as the maximum reduction of price of spectokens, and whether a specific permission by the regulator is necessary to apply the proposed price change.
Stakeholders involved	• Regulator, AI-trading bot
Pre-conditions	• Spectokens have to be for sale and the Regulator has to have configured the AI-bot.
Procedure/ workflow	• The Regulator configures the core AI-bot settings and enables it. • The AI-bot joins the Marketplace and gets permissions to read from the MArketplace and to operate on specific RPCs on the DLT that allow to propose new prices for the spectokens. • The AI-bot observers the market behaviour and releases new price proposals when adequate.



Business models	• Unused spectrum is wasted spectrum and the Regulator always aims for a maximum efficiency in spectrum usage. The AI-bot is a tool that can help to adjust market prices in case that spectrum is left unused.
Envisioned architectural functionality	• AI-bot that interacts with the DLT
KPIs	• Unused spectokens are recognized and alternative pricing is proposed by the AI-bot to increase chances of spectrum to be sold.
Benefits of 5GZORRO approach	• With the AI-based trading assistance, unused shares of the spectrum are detected automatically and suggestions are made on how to modify the pricing of spectrum to sell it more easily and to increase spectrum efficiency

Table 4-11 AI-powered Spectrum Market

4.4. Pervasive vCDN Services

4.4.1. Motivation and business rationale

Content Delivery Networks (CDNs) are geographically distributed networks of computation and storage resources used to offer high-availability and high-performance services to content consumers. Broad spatial distribution allows CDN providers to reach their clients with the desired service quality, whether it is serving web content, application data, live or on-demand streaming media. The latter case, that of video content delivery, is especially interesting since video streaming has strict requirements with respect to viewing quality. User mobility introduces extra requirements, not only from the network perspective (serving bandwidth and delay/jitter) but also from the content perspective (streaming servers' resources, content availability, etc).

Uneven popularity of certain content and/or density of content requests in space and time pose additional challenges to the overall quality of the offered services, stressing the usage of the CDN resources in certain geographic areas and/or at certain times. For example, during flash-crowd events like sports or music events, the viewing or video streaming content increases dramatically in a given geographical area, exceeding the average consumption which a specific CDN has been dimensioned for. In the case of Communication Service Providers (CSPs), there is the possibility that the dynamic reallocation of available (CSP-owned) resources in the specific geographical area may address the issue. But, most of the times, this is not possible. Things become more difficult in the case of Over-The-Top (OTT) service providers who rent resources from CSPs to serve their clients. In such cases, the leasing of new resources in near real-time becomes an issue. Especially if the serving CSP at a specific area has no more resources to allocate.

To address the aforementioned challenges, CSPs need to avoid relying on their own resources only and to be able to dynamically form agreements with third-party resource providers so as to enhance either their own CDN services or the quality of service offered to CDN/OTT providers. For this to happen, mechanisms for on-demand discovery and integration of 3rd party resources and for intelligent real-time scaling out of critical

service components need to be in place. Security and trust are crucial as different stakeholders (CSPs, OTTs, infrastructure providers, content providers) that do not necessarily have pre-established trust relationships are involved.

4.4.2. State of the Art/starting point

5G services are envisioned to be deployed over logically segmented and geographically distributed virtualized infrastructure resources. Logical resources and related network functions are grouped into network slice instances to meet certain network characteristics required by the Service Instance. At any particular point, the operator may need to increase or reduce on demand the amount of virtual resources deployed at a given place, according to per traffic or user-generated requirements, always addressing the performance requirements, typically agreed in an SLA between the operator and its clients (i.e., the service providers). This is particularly expected in cases of high fluctuations in the resource demands, which are typically associated with user mobility and/or the dynamics of the applications. Simply offloading the excessive workload to centralized cloud computing locations presents limited applicability when having edge computing related KPIs such as low-latency support, as it essentially corresponds to SLA violation.

Emerging solutions for resolving such situations are CDNs which use cloud resources, such as storage and compute. These cloud-based CDNs benefit from the geographical availability and the pay-as-you-go model of cloud platforms, reducing the requirements for infrastructure investments. Popular cloud based CDNs are Rackspace Cloud Files [29], Akamai CDN [30], Amazon CloudFront [31], MetaCDN [32] and Limelight Orchestrate Platform [33]. However, most of the current cloud CDN providers chiefly depend on a single cloud provider. Thus, the services lack consideration for cost models when taking advantage of cloud content storage spanning on multiple cloud providers [34]. Moreover, the use of cloud infrastructure for supporting a CDN network entails predefined specialized legal agreements and technical relationships among content, CDN and cloud providers. This binds the CDN and/or the content provider with a chosen cloud provider for a specific time period.

A similar approach to cloud based CDN is to leverage upon resources of 3rd party infrastructures, for example from Neutral Host operators, for managing flash crowd events. In other words, the infrastructure hosting the CDN application may dynamically form agreements with 3rd parties, based on traffic demand. In this case, resource allocation, as represented by the corresponding network slice instance, can be flexibly extended to various locations/areas, composing radio as well as edge, metro and core virtualized assets from various providers into a single end-to-end network slice. In principle, this approach targets the secure and trusted integration of any suitable resource in the vicinity of end users, thus, facilitating the seamless provisioning of computing and physical resources anytime and anywhere. Therefore, the proposed solution gets 5G closer to the pervasive computing paradigm, that is an environment where the devices are unobtrusively connected and always available. 5GZORRO will build upon the mechanisms of slicing and MANO as starting point, in order to allow for the seamless but secure integration of 3rd party resources to the existing 5G resources.

Regarding CDN technologies, 5GZORRO will build upon ICOM's commercial offering of a CDN solution, entitled fs|cdn™ Anywhere [35], and adapt it to fit the purposes of the project. The fs|cdn™ Anywhere is an end-to-end CDN solution that allows to seamlessly integrate IPTV and value-added interactive services into the operator's back-office OSS / BSS and external Over-The-Top (OTT) content systems, through a rich set of available APIs. Moreover, it includes components/features for the encryption, transcoding, distribution, caching & reception of content, with support for Set-Top-Boxes (STBs) as well as Smart TV, Smart Phone and Tablet devices (iOS and Android). In the figure below, we present ICOM's CDN solution, and its high-level architecture. For the purposes of 5GZORRO, the content distribution edge network components will be virtualized to be offered as Virtal Network Functions (VNFs), hence leading to a virtual CDN (vCDN) solution. Especially for the case of mobile clients (smartphones and SIM-enabled tablets), fs|cdn™ Anywhere adopts the HTTP Live Streaming (HLS) and Dynamic Adaptive Streaming over HTTP (MPEG-DASH) protocols approaches and creates a hierarchical (tree-like) topology of HTTP servers (video streamers and content caches) to emulate a multicast delivery tree (multicast is not supported by HTTP; this part of the solution is

not depicted in the above diagram). These video streamers and content caches are placed in key locations of the CSP's network and allow for reaching all the CSP's CDN subscribers. As mentioned before, the functionality of the streaming servers and content caches are currently hosted in CSP's infrastructure. The aim of this use case is to allow for the dynamic introduction of leaf nodes in the aforementioned tree-like structure, that will be hosted on 3rd party infrastructure. To be more precise, video streamers and/or cache servers (offered as VNFs) will be scaled-out using 3rd party resources and will provide additional serving capabilities to the same geographic area as before. There is a licensing scheme accompanying the deployment of fs|cdn™ Anywhere solution, which binds a particular CDN deployment to a maximum number of end-users that can be served by the CSP provider. This licensing verification and corresponding security-related policies are managed by the centralized CDN components (i.e., the CDN backend at the core/cloud). This licensing covers the case of the instantiation of an arbitrary number of edge components, such as the ones that will be deployed on the CSP edge and the 3rd party, for scalability and performance optimizations, as long as the number of end-users remains bounded according to the licensing agreement.

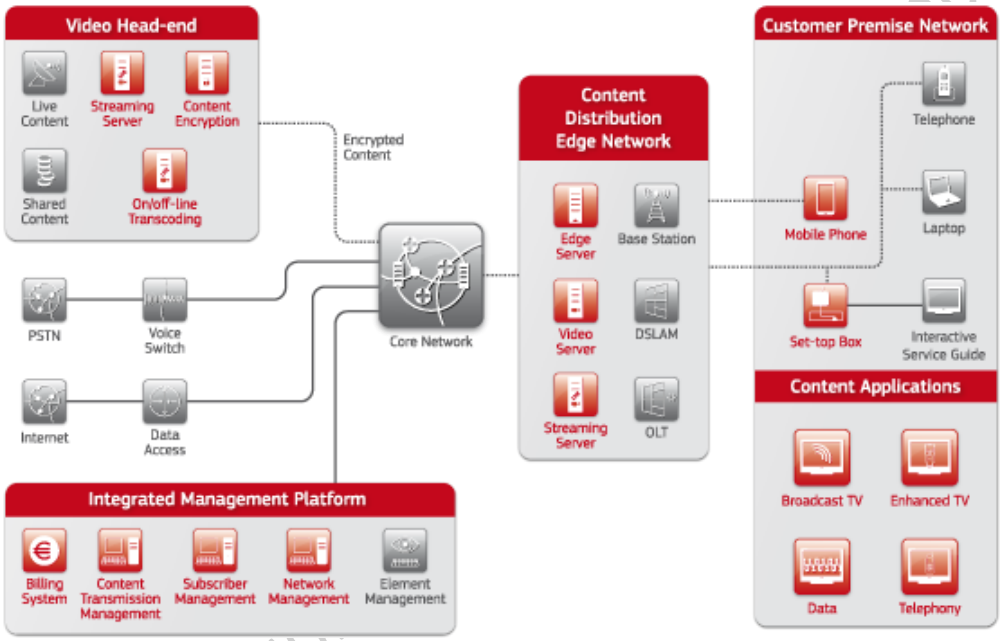


Figure 4-6: ICOM's fs|cdn™ Anywhere solution

4.4.3. 5GZORRO novelty

Several 5GZORRO's novelties will be demonstrated in this use case, built on top of the previously described two use cases. In other words, the vCDN use case can be considered as an all-encompassing use case that inherits novelties from the previous two use cases and further presents some additional ones. The novelties introduced here are summarized as follows.

Zero-touch resource discovery. All infrastructure owners, including 5G and Edge/Cloud operators, will advertise their resources (compute, storage and network) to the underlying DLT, based on the innovations introduced by UC1 (see Section 4.2). The information stored in the DLT instance is utilized by CSP providers in order to discover/identify potential usable resources nearby the intended point of interest *(Resource Discovery & Broker Logic*). Unlike centralised databases, distributed ledgers store information on synchronised independent computers controlled by the individual participants in the network, which increases security and interoperability. The security aspects related to DLT are: data encryption, access control, tamper-resistant data, identity management and fault tolerance. DLT is perceived as a trusted and transparent shared resource that contributes to the automation and decentralization of processes, minimizing the trust necessary in a manual or centralized solution. In this way, DLT provides a tool of trust that minimizes (or eliminates) the need of an auditing intermediary as it enables real-time auditing. Therefore, it is especially beneficial for this use case, where untrusted stakeholders seek to build a trusted infrastructure

for sharing data in a secure and accountable manner. DLT offers further competitive advantages through reduction in the cost of networking, which represents the efforts required to bootstrap and operate a multi-stakeholder platform without need of an intermediary. In contrast to operations relied on centralized intermediation entities, a DLT enables the stakeholders to create a common interchange and enforcement mechanism without a trusted third party. Information exchange and visibility can be easily managed and anonymity can be preserved where required.

The decentralised 5GZORRO catalogue, which is based on DLT, will be responsible for maintaining up to date records of available resources. The introduction of a resource and each subsequent state change in the resource's lifecycle is managed by a smart contract, ensuring valid state changes. Moreover, the resource requests will be also communicated to the DLT infrastructure, by translating the availability and demand, reports from Domain Monitoring & Analytics components into discoverable resources. These include not only resource utilization, but also trusted information regarding achievable KPIs e.g., reported latency or throughput values.

3rd-party resource selection and request. AI techniques will be employed to select the most appropriate required 3rd party resource from the available ones. The decision, performed by the Intelligent 3rd party Virtual Resource Selection 5GZORRO service, is based on historical information linking previous choices to respective performance as represented by KPIs (e.g. service migration time, service downtime, end-to-end service response times, etc.). The selection will trigger the setup request for accessing the specified 3rd party resources. As soon as the trading parties, that is the resource provider and consumer, sign the change of a selected resource's state, the new state is committed to the distributed ledger as a valid transaction.

Security and trust establishment among multi-parties. The required trust will be established on the business layer through the Smart Contracts Management (see UC1, Section 4.2) and Secure SLA Monitoring services which are appropriately configured for the newly established SLA.

Network slice adaptation and service instantiation. Streaming servers, like streaming proxy for video delivery based on HLS and/or MPEG-DASH protocols and content storage components will be virtualized and offered as VNFs and their performance will be exposed to the 5GZORRO operational Data Lake. In addition, mechanisms for fast deployment and integration of new VNFs will be employed to allow for a smooth extension of the CDN network providing proper APIs in order to interact with the Management and Orchestration (MANO) platform (e.g. ETSI OSM [36]) of the underlying 5G infrastructure and allow the instantiation of the VNFs and the appropriate Day-0/1/2 configurations composing the slice. The initial network slice provider will manage the network slice extension to the chosen 3rd party resource provider infrastructure. For the inclusion of the external resources to the new slice, a secure communication must be built between the two parties. More precisely, after the selection of the 3rd party resources, a VPN service will be triggered for the automatic establishment of a VPN connection, in order to securely transmit the host application components, i.e., the vCDN components. Afterwards, the 3rd party resources will be configured to host the components for the particular service, including on-boarding and instantiation of the corresponding VNFs, and the potential transfer of contextual information and content. Traffic/DNS reconfiguration will be performed so as to smoothly divert traffic to new serving nodes. Load balancer instantiation and configuration may also be used for this purpose.

In addition, the existing network slice assigned to the vCDN service and which was initially serving the end users, now has to be extended so as to include the new participating node. Based on the load balancing decisions, certain users have to be reassigned to a different network slice so as to be connected to the new vCDN edge server. As expected, the new and the old network slices will include some common network entities (RAN, edge servers) and some different, depending on the scenario in place (see Section 4.4.5). The extension of the operational boundaries of the current network slice instance is performed by the Inter-domain Slice Orchestration & Management.

VNF licensing. Fs|cdn™ Anywhere solution has a licensing scheme accompanying the service deployment, so the license verification and corresponding security-related policies will be carried by the eLicensing service offered in 5GZORRO. Besides, other software resources could be added to the CDN solution, in order to offer

a more complete set of functionalities, and thus deploying a service composed from different software providers, in which case, the license terms of each provider must be considered. The 5GZORRO eLicensing functionality will provide the ability of keeping the trace of the resource usage independently of the deployment premises owner, providing the ability to manage the licenses in the slice extension cases in a fully automated way.

4.4.4. Overall use case description

Through this use case, scalable and pervasive vCDN services including HQ video streaming (live and/or VoD) will be investigated. Content popularity dynamics present significant variations in the context of flash crowd scenarios e.g., video sharing in stadiums or demonstrations, or sharing breaking news live feed. It therefore offers a realistic context for the evaluation of the 5GZORRO solutions.

4.4.4.1. Stakeholders involved

The stakeholders involved in this use case are:

- The **CSP [***acting as Service Provider / Resource Provider / Resource Consumer***]** is the operator of the 5G network (and typically the owner of the 5G infrastructure) who also provides network slices to the verticals service providers (CDN service provider in this case). Intrinsically, the CSP contains the 5GZORRO platform in order to securely interact with the resource providers, for example to create and update slices involving other parties. It has a dual role. On the one side, it is a Service and Resource Provider, as it offers infrastructure resources and slice services to the CDN/OTT provider. On the other hand, the CSP is also a Resource Consumer as it leases resources from 3rd party providers.
- The **3rd party infrastructure provider [***acting as Resource Provider***]** has deployed infrastructure (network, edge), operates it independently of the CSP(s), and can offer (part of its) ad-hoc infrastructure resources to CSPs, if requested by the latter (e.g., in situations of increased workload and/or saturated resources). Thus, this stakeholder plays the Resource Provider may offer both compute and network resources, or only one of these resource types. A compute resource can be a quantity of GPU's and some RAM deployed in the edge, while a network resource can be a portion of a Base Station's infrastructure.
- The **CDN service provider [***acting as Service Provider / Resource Consumer / Service Consumer***]** is the operator of the content delivery network, on top of the leased CSP's infrastructure. Thus, it is a Service Provider which also plays the role of the Resource and Service Consumer from the CSP perspective. In the 5G environment, the CDN provider leases network slices from the CSP and may deploy its own vCDN components at CSP's MEC (Multi-access Edge Computing) infrastructure, including performance guarantees related to throughput and low latency in certain areas of the network, so as to optimize the content delivery. However, most of the times, especially in the cases of (on-demand or broadcasted) video content, the CSP may also play the role of the CDN provider towards the End Users (i.e., offering its own IPTV service).
- The **OTT service provider [***acting as Service Provider / Resource Consumer / Service Consumer***]** is a specialized Service Provider that operates across an IP network. Therefore, it has no formal business relationship with Resource Providers, but it exploits the services of Internet Service providers instead. In practice, the OTT service provider may form its own CDN over the network/computation/storage infrastructure of (multiple) CSPs. Thus, like a CDN, the OTT provider has three roles. It is a Service Provider for the End Users and a Resource and Service Consumer for the CSP. Moreover, the OTT provider may use the services of a CDN provider in order distribute its content. In this case, the OTT provider is also a Service Consumer for the CDN.
- The **Content provider [***acting as Service Consumer / Service Provider***]** offers the content to be distributed over the CDN/OTT service. In other words, the CDN/OTT service provider offers the mechanism(s) and platform to distribute the content, while the Content provider offer the content

itself. In this respect, content providers are Service Consumers of the content distribution services provided by CDNs and OTTs. In addition, the End Users may be customers of the Content Provider, instead of the CDN/OTT provider. Consequently, for the End User perspective, the Content Provider may have the role of the Service Provider as well. Nowadays, there are often cases where the CDN/OTT providers also create their own content, hence having both roles. In this case however, it is still possible that their platforms offer content from other content providers as well.

- The **End User [***acting as Service Consumer***]** is the final Content Consumer that makes the request to the content provider. Therefore, the end users are the Service Consumers of the Content Provider or CDN/OTT providers when they provide their own content, according to the specific business relationship. In our context, they have user equipment (UEs) that is 5G capable.

4.4.4.2. Workflow

In our scenarios, a CDN/OTT service provider will utilize virtualized content distribution network (vCDN) technology to deliver (ultra) high definition video services to its subscribers. The CDN/OTT service provider leases a network slice instance from a CSP including performance guarantees related to throughput and low latency in certain areas of the network, based on a profiling of the service workload. For the case of OTTs, more than one network domains, and thus more than one CSPs, may be involved. During high workload situations (popular content, music/sports events), the CSP's edge infrastructure cannot satisfy the demand. As a result, the CSP's advanced auto-scaling policy results in the (pro-/re-active) AI-based resource discovery process aimed to identify potential usable 3rd-party (spare) resources e.g., stadium compute infrastructure, nearby smart building or even smart city IT infrastructure, etc. The discovery process identifies the candidate 3rd party infrastructure. The matching is based on trusted information about current resource availability, as exposed and shared by infrastructure providers, as well as profile information related to latency guarantees. The reliability of this information derives from the trust models applied in the DLT infrastructure and 5GZORRO platform. Specifically, even though the CSP cannot be sure that a 3rd party has the capacity it declares it has, it can calculate the trust towards this party according to its policies and experiences. The final selection of the 3rd party resources is based on an intelligent process taking into account resource availability, past and current KPI measurements, security/trust properties, pricing, etc, and results in a resource request for the establishment of a network slice extension reaching the 3rd party infrastructure. During the final stage the network slice extension is realized. This includes the establishment of a secure connection between the CSP edge server and the new infrastructure site (potentially over 5G-NR), the instantiation and/or potential migration of service components (application level) e.g., video transcoder, and the necessary load balancing adaptation e.g., DNS server updates.

The above description is illustrated in Figure 4-8, where the actions that follow the resource saturation prediction are depicted. In this diagram we demonstrate the key difference between CDN and OTT providers, which is that, contrary to CDNs, OTT services can be served by multiple CSPs (dotted lines). Although we focus on the case when the bottleneck is detected at the virtual resources of the CDN service, the process for the OTT service is similar. Moreover, both CDN and OTT providers receive content from the same Content Provider and deliver it to their subscribers (UEs). The red-coloured user equipment is connected to the 1st network operator (CSP #1) and logins to the CDN provider. In the figure we mark with light blue colours the actions where envisioned architectural components are involved, with green communication messages between CSP and CDN providers, with dark blue actions related to physical connectivity and with orange the service provisioning to end users.

In this example, the imminent resource saturation is detected at the virtual resources of the CDN service located at CSP #1 edge server. Colour characterization. Light blue: processes related to envisioned architectural components, Green: message exchange between CSP and CDN providers, Dark blue: connectivity related actions, Orange: UE service consumption.

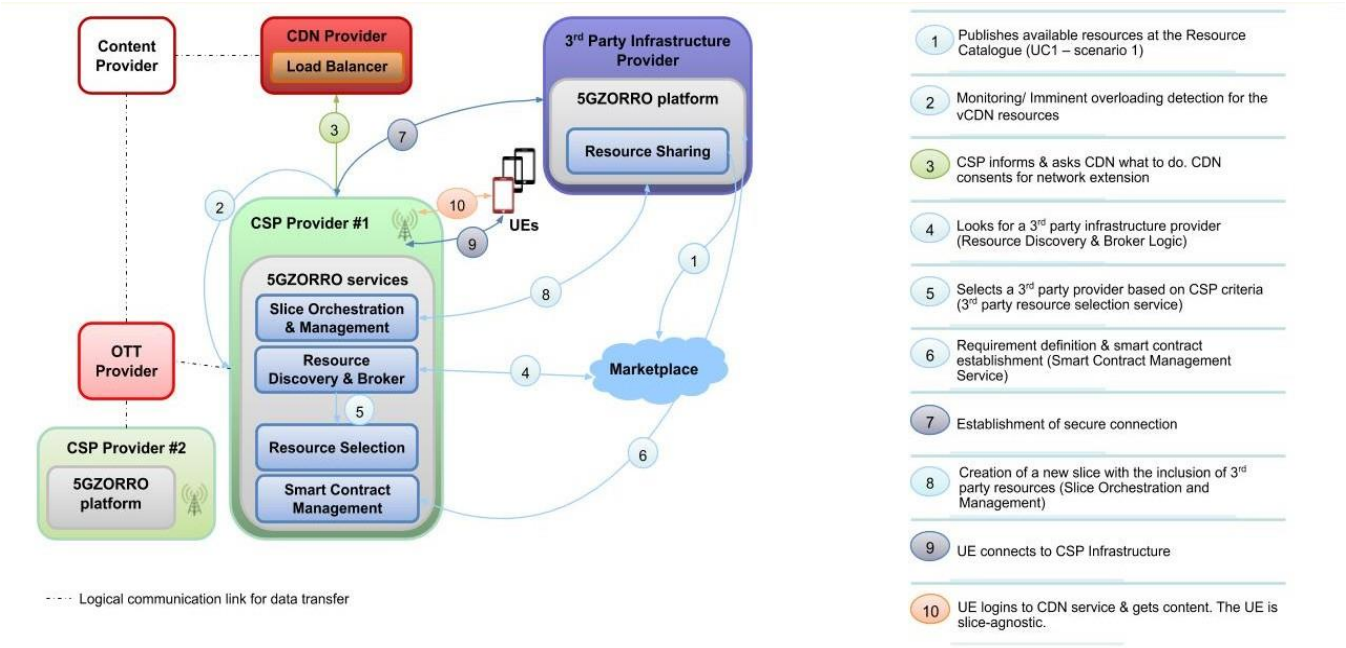
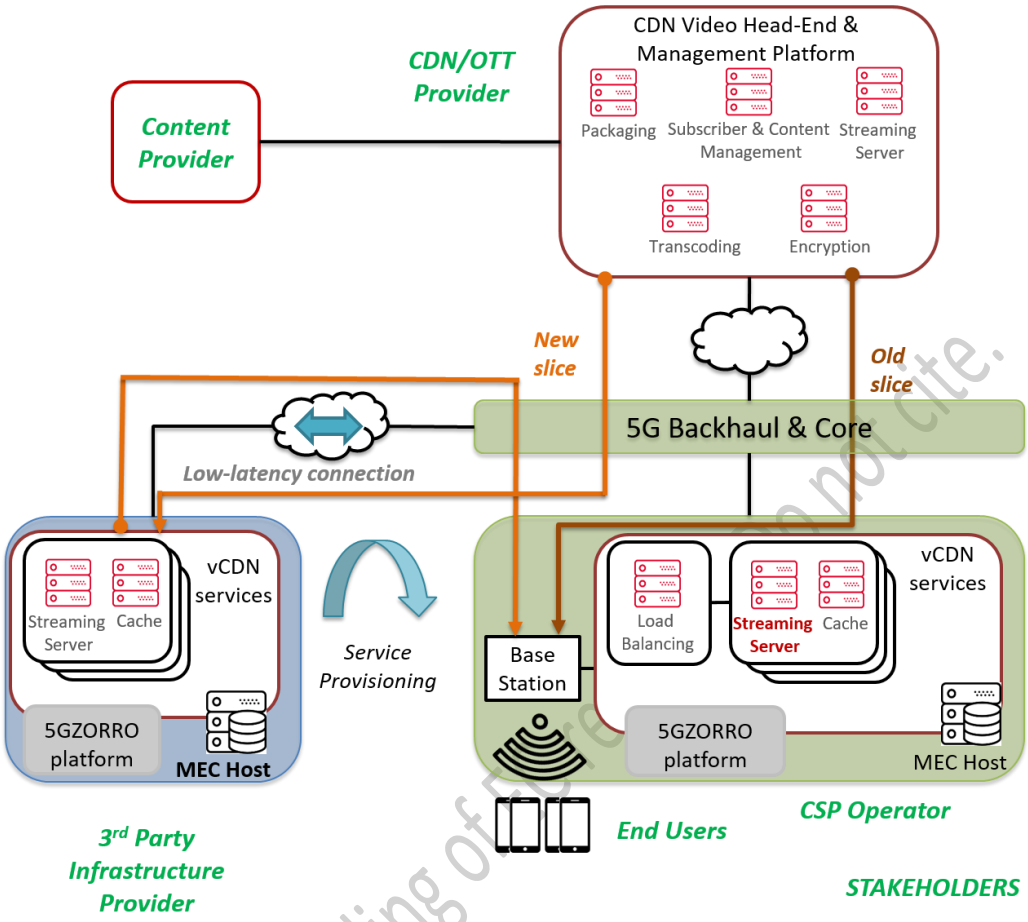


Figure 4-7: High-level workflow.

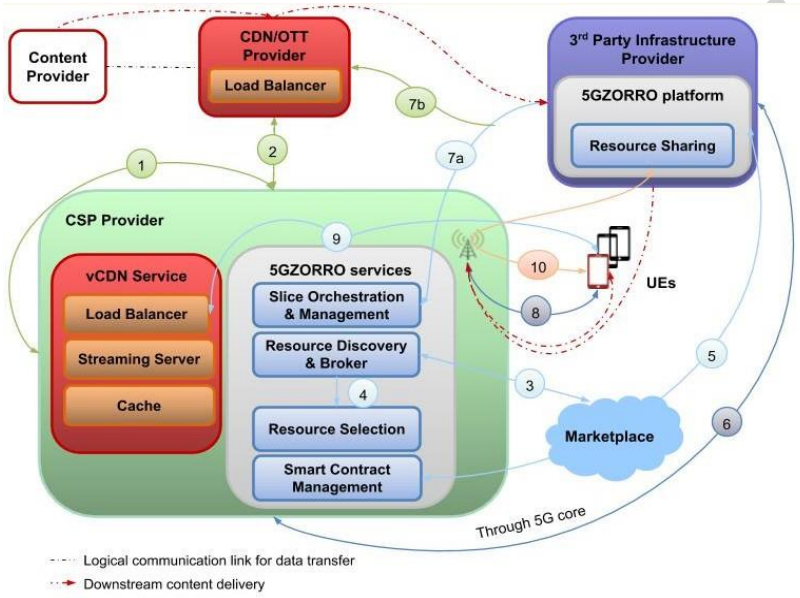
4.4.5. Scenarios

4.4.5.1. Scenario 1: Low latency 3rd party Edge resources

Scenario Name	Low latency 3rd party Edge resources
Rationale/ objective	The need for the slice extension derives from the upcoming overloading of the streaming server that is located at the CSP Edge Server of an instantiated slice. This scenario considers the case of 3rd party Edge resources with low latency connectivity to the network operator infrastructure (the 5G Core) through, e.g., direct optical. Therefore, the downstream traffic of the vCDN service can pass from the core network to the 3rd party edge server and from there to the CSP edge infrastructure with a minimum delay, provided that the latency of the CSP edge server and CSP backhaul connection is also low in order to comply with the SLA requirements. In this scenario, the End Users continue to connect to the initial Base Station of the CSP, since there is not any bottleneck on the wireless access. The key advantage in this concept is that the effect of the extended slice to the End User data delivery bitrate is negligible and thus there will be no SLA violation. Based on the above discussion, the 3rd party that will lease its resources may be a corporation, such as Amazon, Google or Intracom, which has deployed its own cloud services and maintains low-latency connections with the 5G Backhaul for its service provisioning. A business like that is prompted to dynamically rent its unexploited resources in order to increase their revenues.

Deployment	
Storyboard	While the vCDN service is running, it is monitoring the edge servers' performance and the service quality delivered to the end users. In order to prevent hazardous conditions, the CDN services running on the CSP edge servers are configured to provide notifications as soon as their load exceeds certain predefined thresholds. For example, if the number of users connected to a specific CDN Edge Server exceeds a threshold value, the CDN provider will request additional resources from the CSP in order to avoid reaching a saturation point. In addition to this request, the CDN/OTT may define a set of rules and configurations by which it approves the inclusion of 3rd party resources to the CSP scaling mechanism. Therefore, it will facilitate the CSP to take actions before the actual resource saturation takes place. When the CSP receives a request for extra resources it initially tries to satisfy this through its own infrastructure. If these resources are not sufficient and the CSP has the CDN's consent, it will search for 3rd party infrastructure resources (Resource Discovery & Broker Logic), selects the 3rd party infrastructure provider (3rd party resource selection service) and establish a secure (probably VPN) connection with the 3rd party provider. Moreover, the requirements of the CSP infrastructure towards the 3rd party provider are defined and a smart contract between these two parties is established (Smart Contract Management Service). In the meantime, the CDN/OTT temporarily shares its VNFs to a specified registry, allowing the CSP to modify the slice and set up these VNFs in the 3rd party. The extension of the current network slice (Slice Orchestration and Management) takes place over this connection which leads to the inclusion to the allocated 3rd party resources in the eventual setup. Particularly, the 5GZORRO slice management service will pull the VNFs from the registry to the 3rd party and, once this is completed, the VNFs will be removed from the registry.

	Furthermore, the Load Balancer is in charge of traffic splitting decisions and can redirect the user requests to the new slice. Therefore, the new UEs will be served through the same wireless network interface but from a different proxy server. In other words, the new slice will be similar to the older one until it exits the 5G Backhaul and Core Network. From that point, the new slice, taking advantage of the low-latency connectivity, will extend to the edge server of the 3rd party infrastructure. From the content delivery perspective, the 3rd party edge infrastructure will host a streaming and a cache server. For instance, the content that is associated with the new slice instance will be cached on the third-party infrastructure. Next, the content will be delivered to the Base Station where the users are connected and the Base Station, in turn, will transmit the content to the UEs.
Stakeholders involved	• CSP (network operator) • 3rd party infrastructure provider • CDN/OTT service provider • End User
Pre-conditions	• Low latency connections of CSP and 3rd party Edge Servers to 5G Core • Radio resources are not the bottleneck • vCDN service runs at the CSP edge infrastructure
Procedure/ workflow	



1. Monitoring/ Imminent overloading detection
2. CSP informs & asks CDN what to do. CDN consents for network extension
3. Looks for a 3rd party infrastructure provider (Resource Discovery & Broker Logic)
4. Selects a 3rd party provider based on CSP criteria (3rd party resource selection service)
5. Requirement definition & smart contract establishment (Smart Contract Management Service)
6. Establishment of secure connection
7. a Creation of a new slice with the inclusion of 3rd party resources (Slice Orchestration and Management)
   b Inform the CDN about the new node
8. UE connects to CSP Infrastructure
9. Load Balancer corresponds the UE requests to a slice (e.g. the extended one)
10. UE logins to CDN service & gets content

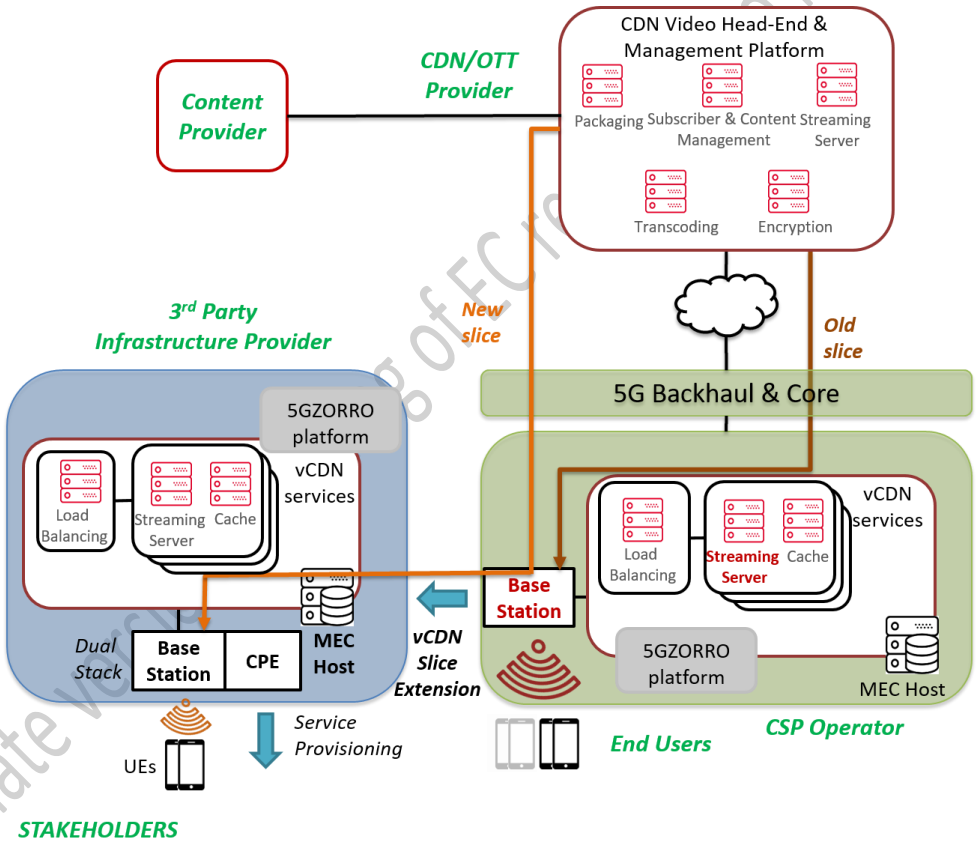
Business models	• For the CDN and OTT providers the allocation of 3rd party resources will look like an extension of its network infrastructure with new streaming servers. Moreover, since the end users will experience an enhanced performance, the CDN/OTT provider's user engagement will increase. Thus, its revenues will be increased with a minimum cost from its side, thanks to the use of dynamic, on demand resource allocation. • The CSP will improve the communication services it offers to CDN and OTT providers 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. 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.

	• 3rd party infrastructure providers will lease their unexploited resources, increasing in this way their profits. • All the processes described above are transparent to 5G connected end-user equipment, which need not be modified in order to be compatible with the 5GZORRO system.
Envisioned architectural functionality	• Resource Discovery and Brokerage Logic • Intelligent 3rd Party Resource Selection • Smart Contracts Management • Secure SLA Monitoring • Slice Orchestration and Management • Load Balancer
KPIs	• The distribution of resource updates as well as the resource discovery should take less than 10 minutes • Ability to create a Smart Contract for 3 or more untrusted parties in order to negotiate, set-up and operate new technical or commercial relationships for 3rd party resource leasing and allocation with associated SLA • Completion of end-to-end provisioning in less than 5 mins • At least 10 heterogeneous and diverse operational data sets streamed into 5G Operational Data Lake from various data sources, at least one per provider/operator).
Benefits of 5GZORRO approach	• The occurrences of user connection aborts or performance degradations due to rapidly increasing traffic will be eliminated. Thus, the CDN/OTT subscribers will enjoy an enhanced user experience. • The CDN/OTT provider will be capable of serving more subscribers than it has been dimensioned for a specific geographical area, paying only for the extra resources that will be used for that period of time. • The CSP provider, which actually leverages upon the 5GZORRO platform and realizes the resource allocation functions, will be able to offer advanced services to its CDN and OTT clients. Additionally, it may take advantage of the 5GZORRO services in order to optimize its own operation and resource exploitation. The communication provider will get automated selection of the most appropriate 3rd party resource provider based on AI learning capabilities, making a compromise between the QoS achieved with the network extension and the respective leasing cost.

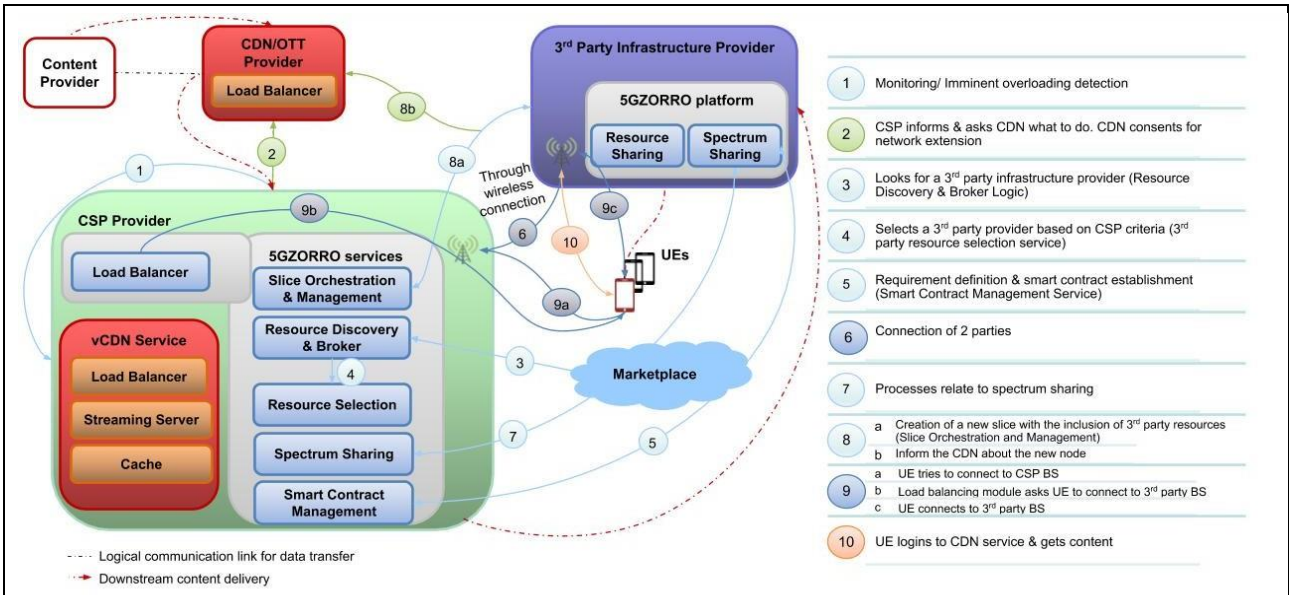
Table 4-12 Low latency 3rd party Edge resources

4.4.5.2. Scenario 2: 3rd party Edge acting as CPE

Scenario Name	3rd party Edge acting as CPE
Rationale/ objective	The second scenario refers to a more complicated setup, where third party resources are connected to the main (virtualized) infrastructure through a wireless connection, namely as ordinary terminal devices i.e., a CPE supports connectivity to the network operator. One reason for the slice extension is, as in the 1st scenario, the proper use of resources for maintaining the agreed performance for all users, despite the increased traffic. However, contrary to the 1st scenario, in this case there is an additional overloading of the CSP Base Station, which is the main saturation point.

	Thus, the CSP requests for an infrastructure provider that has a network interface and maintains a 5G wireless connection with the CSP edge infrastructure, in order to split the user traffic. Therefore, the downstream traffic of the new slice can travel through the CSP edge Base Station to the 3rd party edge infrastructure. This infrastructure provider can be a private 5G network, for example the network of a factory or a business corporation, for which an amount of resources is not utilized for an extended period of time. Thus, it is possible that the infrastructure provider 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. Moreover, as far as the performance perceived by the End User equipment is concerned, the increase of the data transmission delay for the new slice will be again negligible due to the 5G wireless connectivity between the CSP and the 3rd party infrastructure.
Deployment	
Storyboard	In addition to the CDN/OTT monitoring, the CSP edge server is also monitoring the traffic as well as the resource usage for the serving area. Thus, in the case of increasing traffic, the Monitoring Controller detects it and, based on the rate of the traffic increment, it predicts the probability of resource depletion. Particularly, in this scenario, the overloading occurs at the Base Station. Note that the CSP acts before the actual congestion takes place. When the CSP detects an excessive usage of resources, it informs the CDN/OTT service provider about the potential resource saturation and asks the CDN provider whether to extend the network. In order to avoid performance degradation and to keep on satisfying the SLA requirements, the CDN may accept the slice extension. This agreement between CDN/OTT and CSP providers can also have a proactive, rule-based character whereby the CDN provider has agreed beforehand upon the

	configurations of the inclusion of 3rd party resources. Once the CSP has the CDN's consent, it will search (Resource Discovery & Broker Logic) and selects (3rd party resource selection service) a 3rd party infrastructure resource provider as described in 4.4.5.1. Since the CSP and the 3rd party provider can have a wireless connection, this connection is employed for the instantiation of vCDN service components in the 3rd party infrastructure. This setup obviously includes aspects related to dynamic spectrum allocation, as the two Base Stations are located in nearby areas and, thus, they should avoid using the same spectrum portions for eliminating radio interference issues. Moreover, the 3rd party infrastructure provider may own a limited spectrum for its private network and there may be cases where this spectrum is not enough for supporting the new users that connect to its radio interface. Therefore, the 3rd party infrastructure should be able to borrow extra spectrum bandwidth. Service provisioning is supported through a local 5G-NR (or other) wireless interface, effectively extending the service coverage area of the network operator. Therefore, the new UEs will be served through the 3rd party wireless network interface. Generally, there should be a CSP Load Balancing module (instead of a CDN Load Balancer) responsible for choosing the wireless interface where each user will be connected to. In regard to the new slice, this will be similar to the older one until it reaches the CSP Base Station. From that point, the new slice will extend to the edge server of the 3rd party infrastructure. From the CDN perspective, the 3rd party edge server will look like a new server where it can provide its content. For example, the content that is associated with the new slice instance will be cached on the third-party infrastructure and will be delivered to the users that are connected to the 3rd party Base Station.
Stakeholders involved	• CSP (network operator) • 3rd party infrastructure provider • CDN/OTT service provider • End User
Pre-conditions	• Edge server has wireless access radio technology • Edge server is collocated with original MEC server • vCDN service runs at the CSP edge infrastructure
Procedure/ workflow	

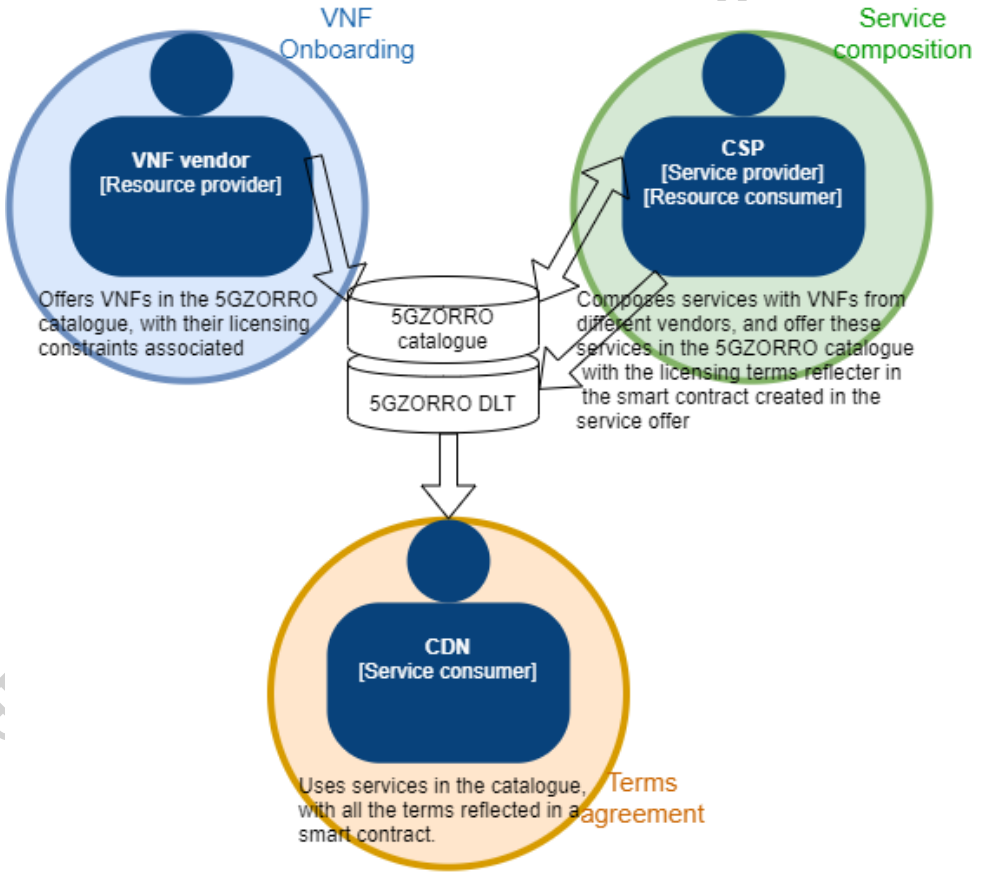


Business models	The business model for this scenario is similar to the business model of scenario 1, with some additional benefits for the 3rd party resource provider and the end user: The 3rd party infrastructure provider leases also its 5G network resources. Moreover, the network operation of the 3rd party provider will not be adversely affected by the allocation of the unexploited resources, as the provider has the option to decide which resources will be leased and for how long, based on its traffic and resource usage.
Envisioned architectural functionality	• Resource Discovery and Brokerage Logic • Intelligent 3rd Party Resource Selection • Spectrum sharing • Smart Contracts Management • Secure SLA Monitoring • Slice Orchestration and Management
KPIs	In addition to KPIs in scenario 1: • The system should be able to connect cell towers in proximity (i.e., within 100 ~ 250 metres distance from each other). • Time to process and enforce new spectrum transactions should be less than 10 minutes • Radio interference between the CSP and the 3rd party is minimum.
Benefits of 5GZORRO approach	In addition to the benefits of scenario 1, the end users will not be affected by the bottleneck at the CSP's Base Station, as some of the devices will be reconnected to 3rd parties' base stations

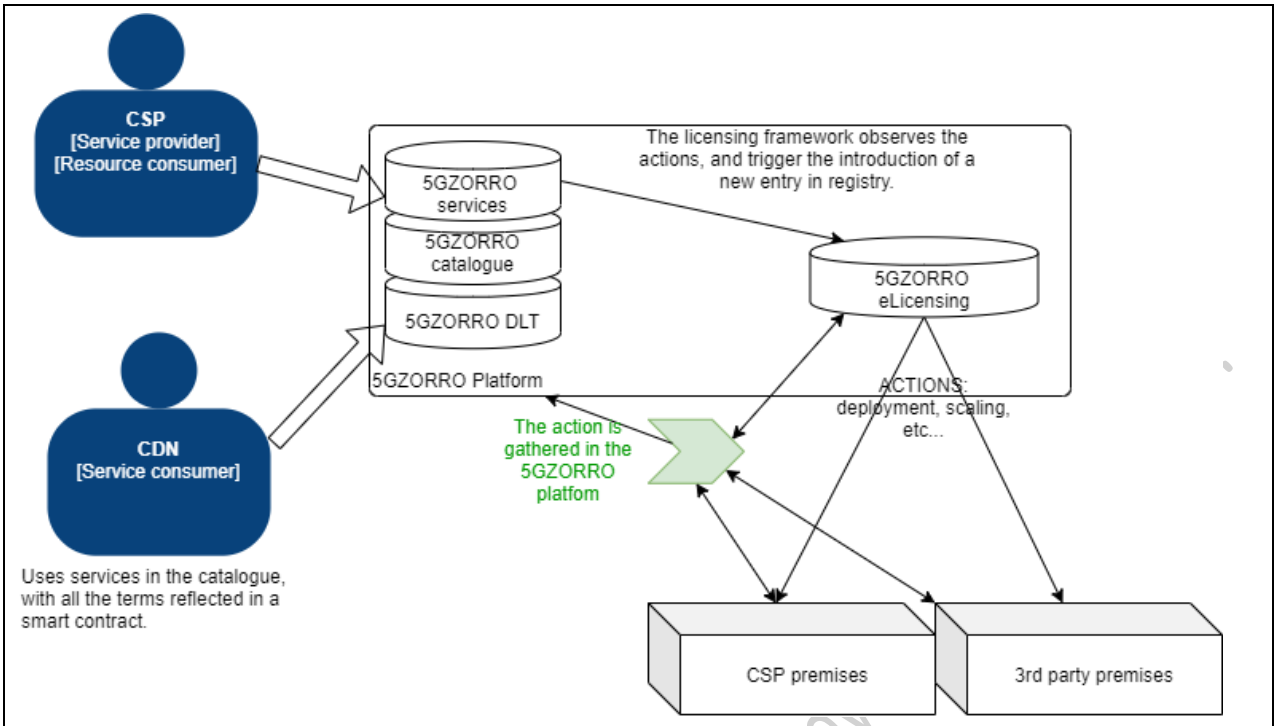
Table 4-13 3rd party Edge acting as CPE

4.4.5.3. Scenario 3: Licensing validation features

Scenario Name	**Licensing validation features**
Rationale/ objective	When applying zero-touch resource discovery, 3rd-party resource selection and request applying AI techniques and automated Network slice adaptation and service

	instantiation, there are licensing costs (i.e. activation of a VNF, scalability decision, etc) that need to be considered in the decision algorithm and enforced by NFV MANO. 5GZORRO should offer a platform that allows the trade of hardware and software resources from different entities, and also the software resource composition by a Service Provider, using the aforementioned services. Therefore, mechanisms to provide the trace of the software resources (e.g VNFs) usage for its subsequent processing for the billing are required. Vendor independent license templates need to be created and attached to the contract agreed for the use of this software resource. The 5GZORRO eLicensing functionality shall provide the ability of keeping the trace of the resource usage in all the entities that are proposed in the previous scenarios, like in Scenario 1, extending the slice in order to guarantee the latency using 3rd party resources.
Deployment	
Storyboard	In this scenario, the setup is similar to Scenario1 but from a multivendor service composition and a license control point of view. A service will be composed using the CDN Virtual Functions and also adding VNFs from different multiple VNF vendors. The functionalities of these new VNFs are providing specific monitoring data from application and infrastructure level to the data lake, in order to allow the analytics creation and update as part of the zero-touch service offered in the platform. The steps to follow for this scenario are:

	1. The Service Provider, that is the CSP in this scenario, composes the service with Virtual Functions (see Service provider creating a service offer, scenario 3 in UC1) that has the licensing schemes associated and this service is offered in the 5GZORRO catalogue to potential Service Consumers (SC). 2. When a SC, the CDN provider in this case, decides to use the service, both SC and SP sign the smart contract that includes the licensing terms of each VNF, as showed in the previous picture (related to scenario 4 of Use Case 1). 3. Once the smart contract is agreed and signed, the 5GZORRO services will create or modify the slice, deploying the slice in the CSP premises and in the 3rd-party premises, to cover the latency requirements mentioned in Scenario 1. 4. 5GZORRO platform through the eLicensing service should support the licensing capabilities, have the vision of the deployed VNFs, regardless of deployment location. 5. The licensing terms from added in the VNF onboarding should be monitored for each related VNF. 6. The licensing framework should keep the track of every action related to the licensing terms agreed of each VNF that composes the service in a secure and non repudiable way. 7. Actions traced are processed, in terms of time of usage, number of instances deployed, number of users that the VNF serves, and all the terms declared in the licensing schemes. 8. The processed information will be exposed to the involved stakeholders, providing them the request capabilities for consulting the usage of their resources.
Stakeholders involved	• CSP (network operator) • 3rd party infrastructure provider • VNF vendors
Pre-conditions	• VNFs from different providers onboarded in the 5GZORRO catalogue, with the licensing schemes declared. • Service composed by the CSP using different VNF providers.
Procedure/ workflow	



Business models	• External software vendors can enter 5GZORRO ecosystem and benefit from trusted provision of the resources to Service/Resource providers. • Software vendors have a non-repudiable mechanism for keeping full track of the proprietary resources that have been used.
Envisioned architectural functionality	• Resource Discovery and Brokerage Logic • Intelligent 3rd Party Resource Selection • Smart Contracts Management • VNF eLicensing • Slice Orchestration and Management
KPIs	• Enable the creation of license agreement templates associated to VNF/NS instances • Create templates attached to eContract detailing name, context, license conditions, negotiation goal and constraints • Generate vendor independent license token to manage location independent VNFs from 3rd party edge to core datacenter • License service creates generic tokens to latter run any vendor VNF across at least 2 network segments
Benefits of 5GZORRO approach	• A trusted relationship between the software vendors and the software Resource Consumers. • Automated and flexible licensing management for Resources and Services from different software vendors.

Table 4-14 Licensing validation features

5. Requirements

5.1. Requirements methodology elicitation and KPIs

Based on the use cases described in the previous section, a requirements elicitation process has been performed following the methodology in [37] in order to come up with an initial set of requirements which will be driving the overall 5GZORRO architecture design. This initial list of requirements is also expected to provide guidance to forthcoming stages of the 5GZORRO project in the further design of multiple components, and ultimately in the implementation and validation of the 5GZORRO system.

5.1.1. Requirements type

5GZORRO considers the following 3 types of requirements:

- **Business requirements (BR)**: which are also known as stakeholder requirements specifications (StRS), describe the business characteristics of a proposed system from the viewpoint of the system's stakeholders, i.e. business scope, business objectives, etc.
- **User requirements (UR)**: often referred to as user needs, describe what the user does with the system, such as what activities that users must be able to perform.
- **System requirements**, further split in
    - *Functional (SRF):* Functional requirements explain what has to be done by identifying the necessary task, action or activity that must be accomplished.
      Non-functional (SRNF): Non-functional requirements are requirements that specify criteria that can be used to judge the operation of a system, rather than specific behaviours. Non-functional requirements are often called "quality attributes" of a system

As depicted in Figure 5-1, the layering of these requirement types can be imagined as in a pyramid, with more generic and high level targets for business and user requirements, down to detailed functional terms defined through system requirements.

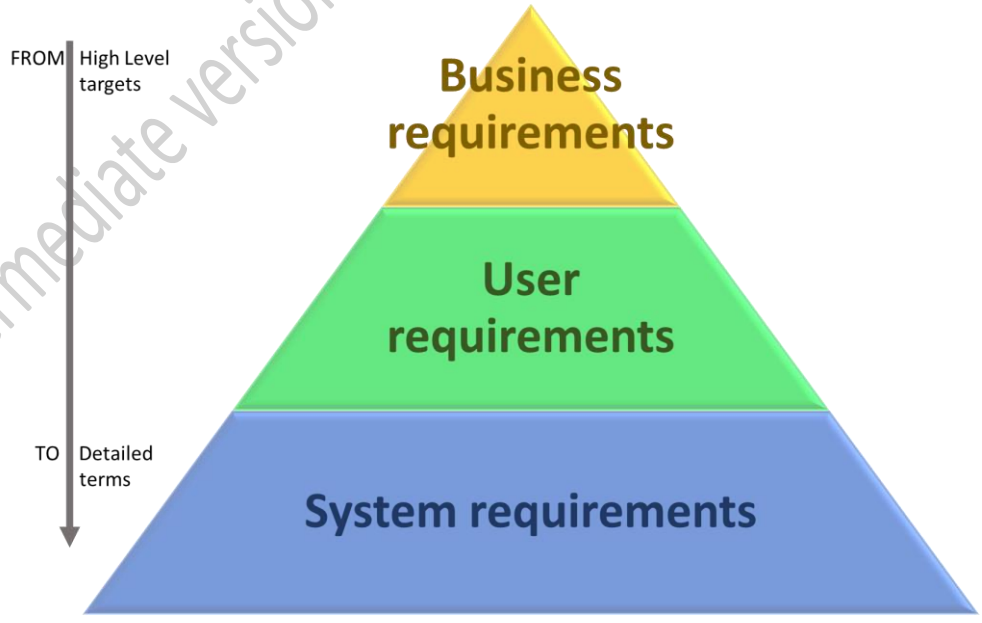


Figure 5-1: 5GZORRO requirements classification as per [37]

5.1.2. Applicable Domain

Based on the technical areas relevant to 5GZORRO the following technical domains have been considered to classify the different requirements:

- Spectrum
- Edge/Core cloud
- Security
- Orchestration
- Data Lakes
- Distributed Ledgers
- SLA management

5.1.3. Requirements prioritization

In order to achieve an incremental approach when designing and building the 5GZORRO system, a prioritization mechanism has been used based on the MoScoW Technique [38]. This method uses four priority groups: MUST have, SHOULD have, COULD have, and WON'T have, that represent the following level of priority:

- **MUST**: mandatory.
- **SHOULD**: of high priority
- **COULD**: preferred but not necessary
- **WOULD**: can be postponed and suggested for future execution

5.2. Requirements

In this section, the initial list of requirements gathered from the use cases specification is presented in the form of a table for each use case. Each requirement includes the motivation behind this requirement and the KPIs that will ensure that the requirement is correctly implemented in the core 5GZORRO platform or offered by the 5GZORRO services.

In order to facilitate the tracking of the use cases, in the following table is presented a summary of the requirements, ordered by prioritization and grouped by domain.

Requirement priority	Domain	Number of identified requirements	Requirement ID
MUST	**Spectrum**	**6**	*UC2.5, UC2.10, UC2.11, UC2.9, UC3.17, UC3.18*
	Edge/Core cloud	**5**	*UC3.1, UC3.4, UC3.5, UC3.6, UC3.16*
	Security	**7**	*UC2.18, UC2.19, UC2.24, UC2.16, UC2.17, UC2.3, UC2.1*
	Orchestration	**8**	*UC3.9, UC3.10, UC3.14, UC3.19, UC1.34, UC1.36, UC3.20, UC3.21*
	Data Lakes	**1**	*UC3.8*
	Distributed Ledgers	**32**	*UC1.1, UC1.2, UC1.3, UC1.5, UC1.16, UC1.37, UC1.8, UC1.10, UC1.11, UC1.14, UC1.18, UC1.20,*

			UC1.26, UC1.27, UC1.29, UC1.9, UC1.6, UC1.7, UC1.12, UC1.15, UC1.17, UC2.2, UC2.4, UC2.6, UC2.21, UC2.23, UC2.7, UC2.15, UC2.8, UC3.12, UC3.13, UC3.15
	SLA management	**3**	*UC1.31, UC1.32, UC2.12*
SHOULD	**Spectrum**	**1**	*UC2.13*
	Edge/Core cloud	**2**	*UC3.2, UC3.3*
	Security	**1**	*UC1.28*
	Data Lakes	**1**	*UC1.15*
	Distributed Ledgers	**7**	*UC1.4, UC1.19, UC1.23, UC1.21, UC1.22, UC2.20, UC2.22*
	SLA management	**2**	*UC1.33, UC1.30*
COULD	**Edge/Core cloud**	**1**	*UC3.7*
	Orchestration	**1**	*UC3.11*
	Data Lakes	**1**	*UC1.24*
	Distributed Ledgers	**2**	*UC1.13, UC1.35*
WOULD	**Data Lakes**	**1**	*UC2.14*

Table 5-1 Summary of use case requirements

Table 5-2: Use case 1 requirement's list

ID	Type	Unique name/title	Requirement Priority	Domain	Description	Rationale (justification)	Related KPIs
UC1.1	Business	Business Resource provider DLT management	MUST	Distributed Ledger	A Resource Provider must manage a 5GZORRO DLT node	Required to be part of the DLT network.	One or more nodes belonging to an approved resource provider have been deployed on the DLT network. All nodes can be verified as belonging to an identifiable legal entity. More than 3providers/operators of virtualized resources or services for spectrum, radio/edge/core compute & networks is required to demonstrate distributed multi-party element
UC1.2	Business	Business Resource provider onboarding	MUST	Distributed Ledger	A Resource Provider must describe resources to be provided	Resource Consumers need information about Products published in the catalogue	A resource provider is able to define the properties of a resource via the marketplace UI
UC1.3	Business	Marketplace Governance Model	MUST	Distributed Ledger	The 5GZORRO Ecosystem (or Marketplace) must be governed by a decentralized, transparent and auditable model.	Governance is required to provide rules on how the marketplace work	A permissioned DLT network has been deployed that underpins the marketplace. DLT does not allow double spending that would allow an agent to trade spectrum rights that it does not own
UC1.4	Business	Marketplace Governance neutrality	SHOULD	Distributed Ledger	The 5GZORRO technical implementation should be as much as possible agnostic of the Marketplace Governance Model since it is not in the scope of 5GZORRO.	The design of the Governance Model is outside of the 5GZORRO project scope	-
UC1.5	Business	Resource provider onboarding approval process	MUST	Distributed Ledger	The approval mechanism to be a resource provider in 5GZORRO must be handled according to 5GZORRO decentralized governance model (distributed consensus).	Approval of new members is one of the decisions to be ruled by the Marketplace governance model	Node(s) in the governance administrator role participate in the consensus around network admission approval
UC1.6	User	Resource Provider registration action	MUST	Distributed Ledger	The Resource Provider must be able to easily discover and use an Application to register as resource provider into 5GZORRO DLT system.	Required to support the entry of new Resource Providers in the Marketplace	New resource providers are able to register via an online form and be assigned the role of Resource Provider on approval
UC1.7	User	Notifications about Resource Provider registrations process	MUST	Distributed Ledger	The Resource Provider must be notified about all relevant information related to the registration process including approval or rejection decisions.	Required to support the entry of new Resource Providers in the Marketplace	Resource providers are notified via email of application events: - received - approved - rejected
UC1.8	System - Functional	Resource Provider registration information	MUST	Distributed Ledger	The Registration Application must collect and validate at least the following information from the Resource Provider: ● Description and formal classification of resources to be provided ● Required data (address/public key) to validate the candidate is running a 5GZORRO DLT node ● Any data as deemed necessary by the governance model pertaining to Know Your Customer (KYC) or Anti Money Laundering (AML) checks	Required to support the entry of new Resource Providers in the Marketplace	A registration form comprises of fields collecting the information deemed necessary to admit a new resource provider to the network

ID	Type	Unique name/title	Requirement Priority	Domain	Description	Rationale (justification)	Related KPIs
UC1.9	System - Non-functional	Identity Management	MUST	Distributed Ledger	Every stakeholder in the 5GZORRO ecosystem must have an Identity that is unique and non-repudiated that is managed by the 5GZORRO DLT system.	All members must have an identity that is trustworthy	All users of the system can be tied to a legal entity through PKI
UC1.10	System - Functional	User permissions	MUST	Distributed Ledger	As soon as Users are approved as members of 5GZORRO DLT system, a set of permissions must be granted based upon registered business role and capabilities. Examples of permissions are which smart contracts the actor can execute, actions they can take on the network, permissions they can grant other actors, etc	All members have defined what are granted permissions in the scope of the marketplace	The governance administrator is able to assign the following roles to a user as part of the onboarding process: Resource Provider, Service Provider, Regulator, DLT Operator / Governance Admin
UC1.11	System - Functional	Resources tokenization	MUST	Distributed Ledger	The DLT 5G System must support the Resource provider with the management of its resources according to applicable standards, by executing associated smart contracts that tokenises the resource capability.	To be aligned with Resources Tokenization concept	Resources can be created (issuance) on the DLT, encapsulating the properties of the resource (tokenisation) and any state changes validated through smart contracts
UC1.12	User	Resource registration action	MUST	Distributed Ledger	The Resource Provider must be able to register and update its tokenised Resources via the marketplace portal.	Required to support resources offers publish in the Marketplace catalogue	A resource provider can add resources using a form via the marketplace UI. A resource provider can update a resource via a marketplace UI form.
UC1.13	Business	Resources certification by regulators	COULD	Distributed Ledger	Depending on the resource type (e.g. radio frequencies), an external regulatory authority could be required to certify (sign) that the Resource Provider genuinely holds these rights, and they have permission to delegate them.	Certification of certain resources by regulators are required	Resources requiring certification do not become discoverable via the marketplace until they have been certified by the regulatory authority Resources type/class should be evident from its properties in order to ascertain special business rules (such as the need to certification in the case of spectrum)
UC1.14	System - Functional	Resource provisioning management	MUST	Distributed Ledger	Information about tokenized resources must be published in the 5GZORRO DLT system from where it can be discovered by potential consumers.	Required to support resources offers published in the Marketplace catalogue are discoverable by consumers	Parameterized queries can be run against the ledger to discover resources
UC1.15	User	Resource discovery action	MUST	Distributed Ledger	The Service Provider must be able to discover resources previously published by Resource Providers in the 5GZORRO DLT system.	Required to support Service Providers using the Marketplace catalogue when looking for resources to be used on their service offers	Users in the service provider role are able to search for advertised resources via the UI. KPI target: 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.
UC1.16	Business	Resource Consumers	MUST	Distributed Ledger	Service Providers are registered in the 5GZORRO DLT system to deliver their services.	Service Providers are Resource Consumers	One or more nodes belonging to an approved service provider have been deployed on the DLT network. All nodes can be verified as belonging to an identifiable legal entity. More than 3 providers/operators of virtualized resources or services for spectrum, radio/edge/core compute & networks is required to demonstrate distributed ledgers.

ID	Type	Unique name/title	Requirement Priority	Domain	Description	Rationale (justification)	Related KPIs
UC1.17	User	Service Offer Creation Action	MUST	Distributed Ledger	The Service Provider must be able to use the 5GZORRO Marketplace to create a Service Offer built on top of registered resources.	Required to support service offers publish in the Marketplace	There is a marketplace UI component that facilitates a parameterized search for resource offers. There is a marketplace UI component that allows multiple resource offers to be combined. Demonstrate a service offer comprising of 2 or more resource offers
UC1.18	System - Functional	Resources certification management	MUST	Distributed Ledger	Regulatory Authorities must have control over the life cycle of certified resources.	Required to ensure regulatory policies are enforced	The regulator is a mandatory participant in consensus for certified resources. Consensus model should reflect this
UC1.19	System - Functional	Resource Definition Language	SHOULD	Distributed Ledger	The 5GZORRO DLT system should support a Resource Definition Language DSL that is used to formally describe in the Smart Contract, the Resource Offer description from the description provided by the Resource Provider.	It would facilitate automated generation of smart contracts from offers description	A DSL has been developed/integrated that allows a user to formally define a resource offer through the marketplace UI
UC1.20	System - Functional	Resource Offer Approval	MUST	Distributed Ledger	The Resource Offer must be validated by the 5G ZORRO DLT system including rights over resources included in the offer. If the Resource Offer is marked as valid, it is registered with the marketplace by smart contract implementation and becomes available for negotiation/consumption. If the Resource Offer is marked as invalid, it is marked as rejected and a notification is returned to the user via the Marketplace portal.	Certification of certain resources by regulatory authorities are required	Resource offer creation and associated life-cycle state changes are governed by smart contract rules and consensus derived from the business model.
UC1.21	User	Resources request	SHOULD	Distributed Ledger	The Service Provider should be able to use the Marketplace portal to request resources according to a set of requirements	It would improve the resource discovery process	The marketplace UI has a component facilitating a parameterized search for resource offers. This UI is accessible to users in the Resource Consumers & Service Provider role
UC1.22	System - Functional	Resources request criteria	SHOULD	Distributed Ledger	The service provider should be able to use the Service Offer build tool to request resources according to the following criteria: - network requirements - service levels - prices - licensing - availability - Trust & Security	It would improve the resource discovery process	The marketplace UI described in the previous KPI should provide the ability to define these parameter categories: ● network requirements ● service levels ● prices ● licensing ● availability ● Trust & Security

ID	Type	Unique name/title	Requirement Priority	Domain	Description	Rationale (justification)	Related KPIs
UC1.23	System - Functional	Resources Match	SHOULD	Distributed Ledger	Resources requested by the Service Provider should be matched with resources available and published in the 5GZORRO DLT system. A service will return a list of available potential matches for a service request. Each match may include several services if the service request requires it. For example, RAN, Edge and Backhaul.	It would improve the resource discovery process	The marketplace UI has a component capable of presenting search results matching the provided parameterized query
UC1.24	System - Functional	Resources Match	COULD	Data-lake and analytics	A matching service could use models built by machine learning and data lake components & combine with available service offers to generate a list of matches	It would improve the resource discovery process	
UC1.25	System - Functional	Resources Match notification	SHOULD	Data-lake and analytics	The result of the Resources Match service should be notified to the Service Provider.	It would improve the resource discovery process	The marketplace UI alerts users to resource matches Email alert is sent to a user to notify them of a resources match including a link to review the match in the marketplace.
UC1.26	System - Functional	Service Offer Smart Contract	MUST	Distributed Ledger	The 5GZORRO DLT system must support a way to generate a service offer that is ready to be used in smart contracts, from the Service Offer description provided by the Service Provider in the Marketplace portal.	It would facilitate automated generation of smart contracts from offers description.	DLT supports the creation of service offers which are governed by smart contracts & consensus rules as defined by the business model.
UC1.27	System - Functional	Service Offer Approval	MUST	Distributed Ledger	The Service Offer must be validated by the 5G ZORRO DLT which is implemented as an on-chain smart contract. If the Service Offer is marked as valid, it is registered with the marketplace by smart contract implementation and becomes available for negotiation/consumption. If the Service Offer is marked as invalid, it is marked as rejected and a notification is returned to the user via the Marketplace portal.	Validation of services are required to minimise errors in the service delivery	Marketplace UI informs Service Providers of success/rejection of a newly created service offer. Validated service offers are listed in the available service offers in marketplace UI. Rejected service offers are not visible to consumers in the marketplace
UC1.28	System - Functional	Trusted Execution Environments	SHOULD	Distributed Ledger / Security	The 5GZORRO DLT system should support the Trusted Execution Environments (TEEs) to ensure that certain data to be added in the chain can be trusted. For example, aggregated SLA monitoring data.	It provides a secure execution environment where managed data is free from tampering	Support the integration of zero trust hardware platforms (TEE - Trusted Execution Environments) as a root of trust for the monitoring of information.
UC1.29	System - Functional	Service Agreement	MUST	Distributed Ledger	5GZORRO DLT should support the creation of a service agreement between Service Provider and Service Consumer	Provisioning of a business agreement between service provider and consumer	
UC1.30	User	Stakeholder notifications	SHOULD	SLA management	Each party involved in a service agreement should be notified of any events such as creation, SLA violations, end of service	It would improve the user experience	DLT events are captured by a software component and an email sent to involved parties

ID	Type	Unique name/title	Requirement Priority	Domain	Description	Rationale (justification)	Related KPIs
UC1.31	System - Functional	Smart Contract SLA monitoring	MUST	SLA management	Smart Contracts must support SLA monitoring functions where Services levels are monitored and SLA terms automatically enforced.	Required to support SLAs with Smart contracts	KPI target: SLA measurements and validation from at least 3 operators involved in a multi-party service chain KPI target: Oracle data layer accessed by 3 or more parties.
UC1.32	System - Functional	SLA breaches management	MUST	SLA management	SLA breaches must be recorded by the DLT and a notification is generated.	Required to ensure SLA breaches are auditable by all interested parties	An SLA violation is recorded on the DLT for a given resource. SLA violation prompts the DLT to issue an event to subscribing software components
UC1.33	System - Function	Stakeholder notifications	SHOULD	SLA management	The system should provide a notification mechanism for notifying all participating parties of all service and resource life cycle events.	It would improve the user experience	DLT issues events to subscribers for: ● service initiation ● SLA violation ● teardown
UC1.34	System - Function	Licensing monitoring	MUST	Orchestration	The 5GZORRO platform must provide a way to control the usage of the software resources, in a secure and non repudiable way from the different services in terms of their agreements in the resource offer.	It will provide the ability of tracing the usage of software resources	DLT has an immutable record of current and historic rights over a resource DLT validates state-transitions for a resource based on defined business model
UC1.35	Business	Pricing Updates	COULD	Distributed Ledger	Commercial pricing terms could be periodically updated in Smart Contracts between parties and call out to Oracles for reference data.		KPI target: Oracle data layer accessed by 3 or more parties
UC1.36	System - Functional	Resource Definition Language licensing capabilities	MUST	Orchestration	The DSL should support creation of license agreement templates associated with VNFs. The licensing agreements must be vendor independent.	It would facilitate automated licensing agreements in the offer description	Legal prose is associated with service agreements and linked to a resource/ smart contract
UC1.37	Business	Token life-cycle management	MUST	Distributed Ledger	The lifecycle of 5GZORRO marketplace tokens, including tokens creation, must be managed according to the Marketplace governance model	Required to ensure transparency on the way tokens are created and managed in general	

Table 5-3: Use case 2 requirement's list

ID	Type	Unique name/title	Requirement Priority	Domain	Description	Rationale (justification)	Related KPIs
UC2.1	User	Spectrum Market Authentication	MUST	Security / DLT	A user must be able to authenticate in order to access the spectrum market and begin trading. Only those passing an initial governance-check can do so, related to UC2.18 requirement. The authentication will happen against the user profiles stored in the DLT.	Access to the spectrum market	A user must be able to authenticate with the system with the unique credentials.
UC2.2	User	Spectrum Market App Access (App/Browser)	MUST	Application (App)	A user must be able to access the spectrum market app to be able to either register new available spectrum (generating spectokens) or to obtain spectrum for an area and time (buying spectokens). This can be a browser-based access or an App.	User interaction with the 5GZORRO spectrum market	A user is able to open the in with her account and to access the GUI.
UC2.3	User	Regulator Certification	MUST	Security	The regulator needs to have a certificate that allows its identification, necessary to apply the special rights to generate spectokens	Regulator authority has special rights, i.e. to generate spectokens. Its identity needs to be identifiable	Only with the certificate a certain set of actions are allowed, e.g. creating spectokens.
UC2.4	User	Visualize own Spectokens and Smart Contracts	MUST	Application (App) / DLT	A user must be able to visualize the spectokens she owns and the corresponding smart contracts. Further, the App needs to be able to notify/alert of SLA breaches in the spectrum usage as defined in the smart contract. For that, the user needs to have the necessary permissions on the DLT.	Browsing the spectoken assignments and smart contracts	The spectrum market app displays the information belonging to a user and if an SLA breach is detected, a notification needs to be visible.
UC2.5	System - Functional	Spectoken Creation	MUST	Spectrum / DLT	The system must be able to verify the regulator as the legal authority, who is able to generate spectokens. The spectoken generation then needs to be written to the DLT. For this, the regulator must have the necessary permissions.	Adding new spectokens to the market is necessary to enable dynamic spectrum allocation	A new spectoken can be generated, but only by the regulator.
UC2.6	System - Functional	Tracking DLTs	MUST	Distributed Ledgers	The DLTs keep track of the current status of the spectokens and associated smart contracts in the spectrum market.	Any transaction of spectokens needs to be validated and added to the blockchain	Spectoken trading will result in a transaction on the DLT that can be reviewed. If necessary, a smart contract is set up, which also can be reviewed.
UC2.7	System - Functional	Spectoken Trading	MUST	DLT / App	When a stakeholder issues to buy spectokens via the app, the current market status in the DLT needs to be checked and updated (a transaction needs to be added to the blockchain) and it needs to be reflected in the app. This requirement is bound to requirement UC2.9.	App needs to allow spectoken trading, any transaction needs to be reflected in the app.	If a user buys a spectoken via the app, the new status of the spectoken assignments are displayed correctly.

ID	Type	Unique name/title	Requirement Priority	Domain	Description	Rationale (justification)	Related KPIs
UC2.8	System - Functional	Smart Contracts	MUST	Smart contracts	As soon as spectokens are bought in order for the spectrum to be used, a smart contract "seals the deal" and determines how the acquired spectokens are to be used. Once the smart contract is established the smart contract settings are applied via the slice management modules (Requirement 2.10) and the spectrum monitoring/enforcement is initiated (Requirement UC2.11). In case of a smart contract breach, a reaction needs to be triggered (Requirement 2.12).	Beyond owning a spectoken, the use of the spectoken needs to be specified. This information goes into a smart contract.	Once the smart contract is set up, it appears on the DLT and it can be reviewed. The monitoring and enforcement system can pull the information stored there in order to set up the infrastructure.
UC2.9	System - Functional	5GZORRO NB API	MUST	Spectrum / Smart Contracts	The 5GZORRO platform needs to expose an API towards the DLT,, so that any configuration determined in the smart contract can be applied on the radio infrastructure and a "slice" can be generated (see requirement UC2.11).	Radio configuration and "spectrum enforcement" are necessary to apply the requested configuration of the spectrum	A set of API calls can be executed from the 5GZORRO platform towards the DLT to obtain information about active smart contracts.
UC2.10	System - Functional	Slice Management Modules	MUST	Spectrum / Edge / Main DC	The 5GZORRO platform needs to have orchestration/RAN control modules that can apply the configurations/settings determined by a smart contract for the intended use of the spectrum. The aggregate resources determined in the smart contract with regards to both compute resources and RAN resources need to be reservable and manageable in what can be called a "slice".	To enforce and monitor the spectrum usage determined in smart contracts, the platform needs a series of software modules.	Once the platform is running, a series of platform modules become operational and the platform owner can validate that they are operational.
UC2.11	System - Functional	Spectrum monitoring	MUST	Spectrum / SLA management	The spectrum has to be monitored; there are 2 ways to monitor the spectrum: 1.) The RAN controllers that take care of the enforcement of the desired radio settings of the infrastructure also include monitoring modules 2.) External monitoring tools report the spectrum usage (Oracles required to include these external readings)	In order to be able to contrast the actual usage of the spectrum with the allowed use (as per smart contract), the system needs monitoring tools	As part of the RAN controller module, a telemetry module is spun up, which gathers information about the spectrum usage. If external infrastructure is used, an Oracle is spun up and it starts reporting the spectrum usage.
UC2.12	Business	SLA checking	MUST	SLA Management	The spectrum usage reports are compared against the SLAs defined in the corresponding smart contract. As such, the spectrum usage measured needs to be fed back to the smart contract, where in case of a breach any other action should be triggered (sanction applied to Resource Consumers, etc.)	The spectrum monitoring and enforcement provides critical information that allows to check whether SLAs are maintained.	After obtaining a spectrum report that violates an SLA of a smart contract, a reaction is triggered.

ID	Type	Unique name/title	Requirement Priority	Domain	Description	Rationale (justification)	Related KPIs
UC2.13	System - Functional	Support for Oracles	SHOULD	Spectrum / SLA management	In case we need to gather spectrum usage reports from external reporting tools, Oracles need to be supported. The underlying programmable DLT to be deployed must allow for the deployment of Oracles, so off-chain data can be retrieved by different smart contracts,	Whenever the spectrum usage is monitored by external tools, we will need Oracles to be able to communicate the readings to our system Oracles may be required to support UC2.12 and 2.13 requirements related to spectrum usage and penalties enforcement, if such are not used correctly (transmission power above legal threshold and usage of such in unauthorised location)	An Oracle can be deployed to monitor the spectrum usage in the infrastructure of a third-party resource provider.
UC2.14	System - Functional	AI powered trading agents	WOULD	AI /Data Lakes	Based on user behaviour in the spectrum market, an AI could propose prices adjustments of spectokens to the regulator to maximize the spectrum usage, i.e. to maximize efficiency.	AI agents can analyse the behaviour in the market and can help the regulator to maximize the spectrum utilization.	An AI-powered trading agent is able to gather information about committed spectoken transactions and it can notify the regulator in case spectoken prices should be altered.
UC2.15	Business	Marketplace control	MUST	Marketplace	Only a Regulator (5GZORRO stakeholder), can control and issue tokens into the market, controlling the supply in circulation.	The regulator decides which tokens are available on the market.	Non-regulators don't have access to the spectoken creation.
UC2.16	Business	Marketplace control	MUST	Marketplace / Security	Only a Regulator (5GZORRO stakeholder), can define what the different tokens represent (bandwidth, location where such spectrum can be used, maximum allowed transmission power and period of time).	Each spectoken is defined by a set of parameters and these can only be set by the regulator.	Non-regulators don't have access to the spectoken management.
UC2.17	Business	Marketplace access control	MUST	Marketplace / Security	Resource Consumers (5GZORRO stakeholder) such as MNOs, Private Verticals and Municipalities must be authorised by the Regulator to access the marketplace. Only such stakeholders must be able to access the permissioned and private network and interact with the smart contracts.	Entering the spectrum market to trade requires a governance check.	Without authorization, a user can't access the permissioned network.
UC2.18	User	Marketplace access control (from app)	MUST	Application / Security	Users of the application (Marketplace GUI) must interact with the Smart Contracts using their own private key (from wallet).	Only authorised participants of the permissioned DLT may interact with the contracts; as such, the web application must be able to interact with the smart contracts, being properly invoked using the users' private keys.	Only the contracts associated with a user can be accessed by the user.
UC2.19	System Functional	Application interaction with the Smart Contracts	MUST	Application / Security / Smart Contracts	The web application providing the marketplace functionality must provide support for wallet creation. Only those authorised by the Regulator may have a wallet they can use to interact with the underlying smart contracts.	This is required to support UC2.19	Security
UC2.20	System Functional	DLT deployment	SHOULD	DLT	5GZORRO Platform should be able to facilitate the deployment of a programmable DLT such as a Blockchain where Smart Contracts will live.	The DLT is a basic element of UC2 and needs to be available.	The DLT can be deployed for 5GZORRO.

ID	Type	Unique name/title	Requirement Priority	Domain	Description	Rationale (justification)	Related KPIs
UC2.21	User	DLT deployment	MUST	DLT	A DLT Operator must be able to deploy a programmable DLT, which shall form the basis of the spectoken marketplace	See above	The DLT operator can deploy the DLT.
UC2.22	User	Re-selling of spectrum	SHOULD	Marketplace	An authorised Resource Consumer (by a Regulator, UC2.18) who has acquired spectrum rights from the Regulator should be able to resell it to other Resource Consumers	This ensures business agility and a dynamic marketplace environment, providing the associated business terms (identified in UC2.17) associated to such trade are not altered.	Once spectokens have been bought by a user, there is the option to resell the spectokens.
UC2.23	User	Onboarding/ Request to register node	MUST	DLT	When a new stakeholder registers, a dedicated node has to be put in place which is registered with the DLT. This node will allow the stakeholder to participate in interacting with the spectrum market.	A core requirement of the DLT are nodes that form the permissioned/private network.	A node can be deployed for a new user and it can connect to the DLT.
UC2.24	User	Onboarding / Permissioning level	MUST	DLT / Trust	Once a new stakeholder is registered, a permissioning degree needs to be set for the stakeholder, allowing for different types of transaction on the DLT. Currently there are basically two levels of permissions planned: Regulator and Trader. The initial trust level should be always minimal, but should be increased as the stakeholder	Not every user has the same permissions, there are different levels of things that can be done.	Different types of users have different rights to perform actions on the DLT.

Table 5-4: Use case 3 requirement's list

ID	Type	Unique name/title	Requirement Priority	Domain	Description	Rationale (justification)	Related KPIs
UC3.1	Business	Network slice request	MUST	Edge/Core cloud	The CDN/OTT MUST be able to request a network slice from the network operator including performance guarantees in certain areas of the network, in order to maintain the agreed SLA with the service consumer	The business relationship between CDN/OTT provider and the CSP must be governed by certain rules that are defined in the Service Level Agreement (SLA). Through this SLA, the CSP guarantees an agreed performance towards the CDN/OTT service. To achieve this performance, the CSP takes advantage of the network slicing technology, which facilitates the end-to-end service delivery with assured performance.	A Communication Service Provider (CSP) offers network slices to Service Providers (e.g. CDN/OTT). The CSP is in position to guarantee a predefined performance level for the service.
UC3.2	System-functional	Discovery process launch	SHOULD	Edge/Core cloud	Provided that there is a network slice extension approval, when the network operator cannot meet the SLA and traffic requirements, the resource discovery process SHOULD be automatically launched	For the zero-touch objective, the processes of network extension and resource discovery should be automatically instantiated. For example, we should not require a network administrator to click a button to start the resource discovery or to access himself/herself the Marketplace in order to find a potential resource provider.	After a respective signal from the CSP, the Resource Discovery and Brokerage Process must be automatically (i.e. without human intervention) instantiated.
UC3.3	System-Functional	3rd party resource intelligent selection parameters	SHOULD	Edge/Core cloud	The 5GZORRO system SHOULD select 3rd party resources based on availability, expected performance (KPI measurements), security/trust properties and pricing	There must be a distinct 5GZORRO service, namely the Resource Selection service, which should apply AI techniques in order to pick the most suitable resource provider. This will be based on a number of parameters and criteria, such as leasing cost, calculated trust value and suitability with CSP's requirements.	(OBJ-4, Quantified target 3) Support intent-based API to guide the AI-driven resource discovery system KPI target: open 5GZORRO API specification for resource discovery. 5GZORRO platform implements accurate algorithms for resource selection.
UC3.4	System-functional	Service components migration	MUST	Edge/Core cloud Orchestration	Network slice extension MUST imply the migration of service components (application level) (e.g., video streamer, load balancer in the case of CDN)	The virtualized CDN services (vCDN) which are installed on the CSP edge server have to be copied and instantiated into the new allocated resources.	The CDN VNFs deployed at the CSP's edge servers with which the CDN already maintains an SLA agreement, must be able to get configured and instantiated at a 3rd party edge server as well. The software image that will be installed in the 3rd party must be accompanied by a license, different from that installed in the CSP, as the 3rd party permissions differ from the CSP's permissions.
UC3.5	System-functional	Register (CDN) resources	MUST	Edge/Core cloud Distributed Ledgers	The CDN/OTT providers MUST be able to register resources (VNFs) such as streaming servers and content storage	We need some kind of registry in 5GZORRO to share the VNFs between the different entities. The CDN needs to somehow share the VNFs that will compose the slice for the CDN delivery, to be spawned in the different resource providers. In other words, the VNFs must be exposed in the registry, allowing the CSP to modify the slice and set up these VNFs in the 3rd party.	A VNF registry will be deployed, allowing the Service Providers to share their VNFs between the different entities. Particularly, this is the place where the CDN/OTT temporarily stores its VNFs, so that the CSP may set them up into a selected 3rd party infrastructure provider. Once this is completed, the CSP must remove the VNFs from the registry.

ID	Type	Unique name/title	Requirement Priority	Domain	Description	Rationale (justification)	Related KPIs
UC3.6	System-functional	Instantiate/configure (CDN) resources	MUST	Edge/Core cloud Orchestration	Registered resources (VNFs) MUST be able to be configured after instantiation (e.g., to be managed by a MANO/OSS, including changes to slice when more resources are added)	The 5GZORRO slice management service pulls the services from the registry to the 3rd party.	MANO/OSS will be modified/extended to handle the network slice extension with additional VNF resources. These resources are extracted from the aforementioned registry.
UC3.7	System-functional	Fast resource deployment/migration	COULD	Edge/Core cloud Orchestration	The MANO/OSS MUST be able to deploy or migrate services fast enough so as to guarantee service continuity. (i.e., container-based implementation will have an edge over VM-based implementations)	The migration of CDN VNFs will be handled by the MANO/OSS. Also, the deployment of the VNFs into the 3rd party resource provider should be realized fast enough, so that the CSP must encounter no resource saturation before the new VNFs are ready to serve End Users.	Network Service instantiation time Network Service migration time
UC3.8	System-functional	Observable resource usage	MUST	Data Lakes	Traffic and resource usage MUST be observable (i.e., monitorable) at the edge server level	The CSP needs to monitor its resource usage in order to predict a potential resource saturation. Moreover, the CSP sends some monitoring data to the CDN core, which is required for monitoring from the CDN side.	(OBJ-1, Quantified target 1) Inject and process operational service data (configurations and runtime monitoring and logging) into a multi-party 5G Operational Data Lake KPI target: at least 10 heterogeneous and diverse operational data sets streamed into 5G Operational Data Lake from various data sources, at least one per provider/operator).
UC3.9	System-functional	Predictable resource overloading	MUST	Orchestration	The rate of the traffic increment MUST be used to calculate the probability of streaming proxy overloading Streaming proxy overloading probability MUST be predictable based on the rate of the traffic increment, allowing action to be taken before the actual resource saturation takes place	The rate with which the traffic increases is a good parameter for predicting the resource saturation. In this way, the CSP will be able to take actions before the traffic reaches a certain threshold, after which it may not have enough time to discover and allocate new resources and to set up the new VNFs without hindering the CDN service delivery.	By monitoring the total bits per second transmitted to end users on account of the CDN service, the CSP can perceive if the traffic has increased and, based on the way it increases, it can predict the need of additional resources.
UC3.10	System-functional	Excessive usage notification	MUST	Orchestration	Excessive usage of resources according to the current/valid SLA MUST trigger a notification to the CDN/OTT service provider about the potential resource saturation	The CDN must have the option to decide what may happen in case new resources seem to be needed. For instance, it may allow the CSP to expand only on its own resources and prohibit the exploitation of external resources. Or it may entrust the CSP to allocate the needed resources wherever they may be.	The CSP maintains an open communication channel with the CDN/OTT servers for data and notifications exchange. In case that the CSP has not any predefined rule or SLA requirement regarding what to do when additional resources are needed, it must notify the CDN and wait for its permission to proceed with the resource allocation, especially if it is about to expand on 3rd party resources.
UC3.11	System-functional	Rule-based scaling mechanisms	COULD	Orchestration Monitoring and Analytics	The CDN/OTT service provider COULD use rule-based mechanisms to be proactive and include 3rd party resources to the scaling mechanism	As mentioned on the above requirement, the CDN may fully trust upon the CSP for the resource allocation. However, the CDN/OTT should be allowed to set some requirements from its side regarding the expansion into external resources. For instance, some stakeholders of the 5GZORRO consortium may be competitors of the CDN/OTT service provider. Thus, the CSP must not include them in the potential resource providers.	The CDN/OTT provider knows in advance that the CSP offers the capability of expanding into external resources in order to support its services. Thus, through a proper API, the CDN/OTT must be able to define some rules towards the CSP in regard with the kind of the infrastructure providers it can rely on. For example, it may define a threshold value for the trust metric or a blacklist of known 5GZORRO stakeholders that it does not trust. Finally, through the same API, the CDN/OTT provider may prohibit the CSP to scale out to any external party.

ID	Type	Unique name/title	Requirement Priority	Domain	Description	Rationale (justification)	Related KPIs
UC3.12	System-functional	Search for infrastructure resources	MUST	Distributed Ledgers	The CSP MUST be able to search in the DLT catalogue for 3rd party infrastructure resources (Resource Discovery & Broker Logic)	The Resource Providers use the Marketplace APIs in order to publish their resources on the Catalogue. Thus, the CSP must access the Catalogue, via the Marketplace APIs, and find an infrastructure provider that can meet its requirements.	The CSP gets a list of available 3rd party infrastructure providers. Time needed for searching through the catalogue and retrieving the list of available resources.
UC3.13	System-functional	Intelligent selection of infrastructure resources	MUST	Distributed Ledgers	The CSP MUST be able to, select the 3rd party infrastructure provider (3rd party resource selection service)	The previous step, that is the Resource Discovery & Broker service, returns a list of available resources, which all satisfy the intended requirements. Then, it must be up to the Resource Selection Service to pick the best fitted resource, on behalf of the CSP.	(OBJ-4, Quantified target 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 KPI target: distribution of resource updates and discovery in less than 10 mins
UC3.14	System-functional	Secure connectivity between CSP and 3rd party	MUST	Orchestration Distributed Ledgers	The CSP MUST be able to establish a secure (probably VPN) connection with the 3rd party provider.	One of the requirements of the CDN/OTT service towards the CSP is to provide secure and reliable communication links.	Application of message encryption Connectivity interruptions.
UC3.15	System-functional	Define requirements in SmartContracts	MUST	Distributed Ledgers	The CSP MUST define requirements towards the 3rd party provider in a SmartContract	The best way to establish the final SLA agreement between the CSP and the 3rd party is through a Smart Contract. Smart Contracts are prefered for these kinds of agreements as they facilitate the automatic and secure transactions of DLT assets.	(OBJ-3, Quantified target 1) Ability for untrusted parties to negotiate, set-up and operate a new technical/commercial relationship via a Smart Contract for 3rd-party resource leasing/allocation with associated SLA KPI target: Smart Contract for 3 or more untrusted parties
UC3.16	System-functional	Notifications acceptance	MUST	Edge/Core cloud	The CDN/OTT service provider MUST be informed about the instantiation of the new virtual vCDN server, in order to update its HLS server hierarchy and perform DNS reconfigurations, which are needed for splitting the traffic among vCDN servers.	From the CDN perspective, a newly instantiated VNF is regarded as a new streaming server located at the edge of the network. Thus, it must be notified about any new vCDN server, in order to consider it in traffic spitting decisions. Otherwise, no traffic will ever reach the new vCDN server.	Delay time from the moment the new edge vCDN server is established until the core CDN is updated with the inclusion of this server.
UC3.17	System-functional	Dynamic spectrum allocation	MUST	Spectrum Edge/Core cloud	This setup MUST include aspects related to dynamic spectrum allocation, as the two Base Stations are located in nearby areas and, thus, they should avoid using the same spectrum portions for eliminating radio interference issues.	In the 2nd scenario of UC3, the traffic that was originally intended for a specific CSP edge node, is divided between two Base Stations. Thus, since the two colocated communication providers form an agreement, they can also agree upon the spectrum usage in order to eliminate radio interferences and to provide the best possible wireless communication performance.	(OBJ-5, Quantified target 4) Linkability between market agents and their associated radio access points, which will allow to provide the appropriate spectrum rights to each access point KPI target: <10M cell towers should be linkable by the system, which is a reasonable EU nation-wide deployment

ID	Type	Unique name/title	Requirement Priority	Domain	Description	Rationale (justification)	Related KPIs
UC3.18	System-functional	Extra spectrum bandwidth borrow	MUST	Spectrum Edge/Core cloud	The 3rd party infrastructure MUST be able to borrow extra spectrum bandwidth, in case it owns a limited and not sufficient (for supporting the new users that connect to its radio interface) spectrum for its private network.	This requirement is needed for the cases when the selected 3rd party has limited wireless communication resources. That can be, for example, the case of a private 5G network which has reserved only a small portion of the licensed spectrum bands.	(OBJ-5, Quantified target 1) Time to process and enforce new spectrum transactions (i.e. from the moment the transaction is settled until the spectrum becomes available) KPI target: complete new spectrum transactions in less than 10 minutes
UC3.19	System-functional	Licensing schemes	MUST	Orchestration	The licensing scheme of the CDN VNFs should be supported from the 5GZORRO platform, in terms of: ● Number of end users that can be served by the VNFs ● Number of components deployed at the cloud/edge (scalability) ● Time of usage	The CDN product manages the license in these terms. From the 5GZORRO platform we must support it.	(OBJ-6, Quantified target 1) Enable the creation of license agreement templates associated to VNF/NS instances KPI target: create templates attached to eContract detailing name, context, license conditions, negotiation goal and constraints
UC3.20	System-functional	Licensing attestation	MUST	Orchestration	VNF Attestation mechanisms should be placed.	Reliable license verification mechanisms are needed	
UC3.21	System-functional	Licensing system placement	MUST	Orchestration	The licensing system must be location and platform independent.	This will allow the licensing to work independently of the characteristics of the entity's premises	(OBJ-6, Quantified target 2) Generate vendor independent license token to manage location independent VNFs from 3rd party edge to core datacenter KPI target: license service creates generic tokens to latter run any vendor VNF across at least 2 network segments

5.3. Conclusions

This deliverable has set out in detail the candidate use cases for 5GZORRO and the corresponding requirements that further architecture work must fulfil. The work performed during this period had as main objective to introduce the first steps to demonstrate a zero-touch management approach ensuring trusted and secure execution across multiple domains, providing the foundation for sophisticated market-based structures based on Smart Contracts for network services and resources, as well as offering the possibility to several stakeholders an efficient and secure resource trading in a fully automated way.

In order to succeed in our commitment, we followed the strategy of elaborating different scenarios in the use cases with the purpose of describing concrete situations and iterations between vertical industries, CSPs, operators and third-party resource providers, leveraging the 5GZORRO capability offers. It is worth to notice that the pervasive vCDN use case is fully dependent on the other ones, since it is using the smart contract management presented in the first use case and also the dynamic spectrum allocation from use case two. Thus, the requirements analysis and collection has been produced taking in account this base; the Smart contract (UC1) and Spectrum allocation (UC2) requirements are more system and platform oriented. Both use cases are tied to the technologies that will allow the resource sharing, SLA monitoring and the security and trust between multiple entities, while the pervasive vCDN use case (UC3) is vertical application oriented, besides of covering orchestration and licensing topics. Concretely, in terms of future demonstration of the project, scenario 1 of the UC3 covers all the technical scenarios in UC1, with the resource discovering and selection using the 5GZORRO's catalogue, and scenario 2 of UC3 follows the steps defined in UC2, since it deals with spectrum trading.

The outputs of this deliverable will serve as input for the implementation work that will be performed in the WP2, WP3, WP4 and WP5. Additionally, the referenced requirements will be further discussed in tasks T2.2 and T2.3, and potentially improved or incremented in D2.3. The gathered use cases will be also developed in task WP5 and presented in the validation deliverables D5.1, D5.2 and D5.2.

6. References

[1] Zero Touch Network and Service Management. ETSI. Web [https://www.etsi.org/technologies/zero-touch-network-service-management]

[2] Experiential Networked Intelligence. ETSI. Web [https://www.etsi.org/technologies/experiential-networked-intelligence]

[3] Ethereum open-source platform for decentralized applications. Web [https://ethereum.org/]

[4] "Managing data lakes in big data era: What's a data lake and why has it became popular in data management ecosystem" Published in 2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 8-12 June 2015. Web-[https://ieeexplore.ieee.org/document/7288049]

[5] "AIOps for a Cloud Object Storage Service" Published in: 2019 IEEE International Congress on Big Data (BigDataCongress), 8-13 July 2019. Web [https://ieeexplore.ieee.org/document/8818188]

[6] Sabt, M., Achemlal, M., & Bouabdallah, A. (2015). Trusted execution environment: what it is, and what it is not. In 2015 IEEE Trustcom/BigDataSE/ISPA (Vol. 1, pp. 57-64).

[7] Ladjel, R., Anciaux, N., Pucheral, P., & Scerri, G. (2019). Trustworthy Distributed Computations on Personal Data Using Trusted Execution Environments. In 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing And Communications (pp. 381-388).

[8] Chang, R., Jiang, L., Chen, W., Xiang, Y., Cheng, Y., & Alelaiwi, A. (2017). MIPE: a practical memory integrity protection method in a trusted execution environment. Cluster Computing (Vol. 20, n. 2, pp. 1075-1087).

[9] Istio. Web [https://istio.io/]

[10] Hybrid/Multi-cloud IP Service Mesh. Web [https://networkservicemesh.io/]

[11] TM Forum TR279, CSP Use Cases Utilizing Blockchain, Version 3.1.1, August 2019

[12] TM Forum Blockchain-based Telecom Infrastructure Marketplace Blockchain-based Telecom Infrastructure Marketplace [https://www.tmforum.org/blockchain-based-telecom-infrastructure-marketplace/]

[13] Next generation public chain for Network-as-a-Service (NaaS). Web [https://qlcchain.org/project]

[14] Clear builds blockchain-based settlement and clearing networks for global industries. Web [https://www.clearx.io/]

[15] CORDA. Publicly available internet of Corda nodes operated by network participants. Web [https://corda.network/]

[16] R3 and CBAN. Web [https://www.r3.com/blog/r3-and-the-cban/]

[17] ENERCHAIN - DECENTRALLY TRADED DECENTRAL ENERGY. Web [https://enerchain.ponton.de/]

[18] Powerledger. Operating system for the new energy marketplace. Web [https://www.powerledger.io/]

[19] Dynamic Spectrum Alliance, Automated Frequency Coordination Web. [http://dynamicspectrumalliance.org/wp-content/uploads/2019/03/DSA_DB-Report_Final_03122019.pdf]

[20] K. Kotobi and S. G. Bilen, "Secure Blockchains for Dynamic Spectrum Access: A Decentralized Database in Moving Cognitive Radio Networks Enhances Security and User Access," in *IEEE Vehicular Technology Magazine*, vol. 13, no. 1, pp. 32-39, March 2018, doi: 10.1109/MVT.2017.2740458.

[21] Yrjola, Seppo. (2018). Analysis of Blockchain Use Cases in the Citizens Broadband Radio Service Spectrum Sharing Concept. 10.1007/978-3-319-76207-4_11.

[22] M. B. H. Weiss, K. Werbach, D. C. Sicker and C. E. C. Bastidas, "On the Application of Blockchains to Spectrum Management," in IEEE Transactions on Cognitive Communications and Networking, vol. 5, no. 2, pp. 193-205, June 2019, doi: 10.1109/TCCN.2019.2914052.

[23] NEUTROON solution. Web. [https://www.i2cat.net/projects/neutroon/]

[24] 5G-EmPOWER: A Software-Defined Networking Platform for 5G Networks [https://5g-empower.io/]

[25] COHERENT 5GPPP Project [http://www.ict-coherent.eu/]

[26] 5GCity 5GPPP project [https://www.5gcity.eu/]

[27] ElectroSense project: Collaborative Spectrum Monitoring [https://electrosense.org/]

[28] Bitcoin. Web [https://bitcoin.org/en/]

[29] Rackspace Cloud Files. Web [https://www.rackspace.com/en-au/openstack/public/files]

[30] Akamai CDN solutions. Web [https://www.akamai.com/uk/en/resources/cdn.jsp/]
[31] Amazon CloudFront. Web [http://aws.amazon.com/cloudfront/.]
[32] Broberg, J., Buyya, R., Tari, Z.: MetaCDN: Harnessing 'Storage Clouds' for high performance content delivery. J. Netw. Comput. Appl. 32(5), 1012–1022 (2009). ISSN:1084-8045. [http://dx.doi.org/10.1016/j.jnca.2009.03.004]
[33] Limelight Orchestrate CDN. [https://www.limelight.com/products/content-delivery-network/]
[34] M. Wang, P. P. Jayaraman, R. Ranjan, K. Mitra, M. Zhang, E. Li, S. Khan, M. Pathan, and D. Georgeakopoulos: An Overview of Cloud Based Content Delivery Networks: Research Dimensions and State-of-the-Art. Springer-Verlag Berlin Heidelberg (2015), DOI: 10.1007/978-3-662-46703-9_6
[35] fs|cdn™ Anywhere CDN solution. Web. [http://www.intracom-telecom.com/en/products/telco_software/iptv_multiplay/fs_cdn.htm]
[36] OSM - Open Source Mano. Web [https://osm.etsi.org/]
[37] Visual paradigm [https://www.visual-paradigm.com/project-management/different-types-of-requirements/]
[38] MoScoW Technique, available online at [https://www.agilebusiness.org/page/ProjectFramework_10_MoSCoWPrioritisation]

7. Abbreviations and Definitions

7.1. Definitions

AIOps	The term "*AIOps*" stands for "artificial intelligence for IT operations." Originally coined by Gartner in 2017, it refers to the way data and information from an application environment are used by an IT team to support and automate operations, using AI.
Decentralized catalogue	*5GZORRO decentralized catalogue* holds the collection of Product offers available to be traded among providers and consumers. In principle, 5GZORRO Catalogue is more focused on Resource product offers and not on Service product offers. However, if we consider extreme situations where we could also tokenise resources from end-users (e.g. residential 5G routers) it will facilitate to have a single catalogue where end-customers simultaneously manage 5G Services consumption and 5G Resources offers.
Distributed Ledgers Technology	*Distributed ledger technology* (DLT) refers to the technological infrastructure and protocols that allows recording the transaction of assets in which the transactions and their details are recorded in multiple places at the same time. Unlike traditional databases, distributed ledgers have no central data store or administration functionality. DLT provides simultaneous access, validation, and record updating in an immutable manner across a network spread across multiple entities or locations.
Network slice	*Network slicing* is the transform of the network it into a set of logical networks on top of a shared infrastructure. Each logical network is designed to serve a defined business purpose and comprises of all the required network resources, configured and connected end-to-end.
Operational data-lake	A *data-lake* is a centralized repository that allows you to store data originated from different sources, arranged in different formats, and having different attributes. Provides the ability of storing your data as-is, without having to first structure the data, and run different types of analytics, from dashboards and visualizations to big data processing, real-time analytics, and machine learning to guide better decisions.
Oracles	*Oracles* retrieve and verify external data for blockchains and smart contracts through methods such as web APIs or market data feeds. They feed the smart contract with external information that can trigger predefined actions of the smart contract. This external data stems either from so ware (Big-data application) or hardware (Internet-of-Things). Such a condition could be any data, like weather temperature, successful payment, or price fluctuations.
Service mesh	A *service mesh* is a networking pattern designed to simplify the communication between the modules building a modern Cloud-Native application. It offers a configurable, low-latency infrastructure layer designed to handle a high volume of network-based inter-process communication among application infrastructure services using application programming interfaces (APIs). A service mesh ensures that communication among containerized and often ephemeral application infrastructure services is fast, reliable, and secure.
Smart contracts	*Smart contracts* are programmable components of the DLT that encapsulate the agreed business model of parties wishing to interact with the ledger and cannot be tampered with; they represent an enforceable agreement.

Specktokens	*Spectokens* are non-fungible tokens represent the rights to use spectrum in a location over a duration of time and will be available for sale and trading by appropriately permissioned 5GZORRO users. Each Smart Contract will contain the business terms of the resource being represented by the spectoken. This will not only allow for optimized use of the spectrum, but it will also enable near real-time, on-demand contracting with an optimal price for the resources being traded.
Trusted Execution Environments	*Trusted Execution Environments (TEEs)* are isolated processing environments in which applications can be securely executed irrespective of the rest of the system, in particular on a separated kernel. It offers an execution space that provides a higher level of security for trusted applications than rich systems, guaranteeing code and data loaded inside to be protected with respect to confidentiality and integrity.
VNF e-licensing	The *5GZORRO VNF e-licensing* is a service that allows the establishment of vendor independent license agreements, using different license templates. When applying zero-touch resource discovery, 3rd-party resource selection and request applying AI techniques and automated Network slice adaptation and service instantiation, there are licensing costs (i.e. activation of a VNF, scalability decision, etc) that need to be considered in the decision algorithm and enforced by NFV-MANO in an automated way.

7.2. Abbreviations

5G IA	5G Infrastructure Association
AI	Artificial Intelligence
AML	Anti-Money Laundering
API	Application Programming Interface
BR	Business Requirement
CAPEX	Capital Expenditure
CBAN	Carrier Business Automation Network
CBRS	Citizens Broadband Radio Services
CF	Container Function
CPE	Customer Premises Equipment
CSP	Communication Service Provider
DApp	Distributed Application
DASH	Dynamic Adaptive Streaming over HTTP
DLT	Distributed Ledger Technology
DoA	Description of Action
DSL	Domain Specific Language
EA	Existing Actor
EC	European Commission
FCC	Federal Communications Commission
FDD	Frequency Division Duplex
GUI	Graphical User Interface
HLS	HTTP Live Streaming
HQ	High Quality
HTTP	Hypertext Transfer Protocol
IPR	Intellectual Property Rights
KPI	Key Performance Indicator
KYC	Know Your Customer
LTE	Long Term Evolution
MAC	Medium Access Control
MANO	Management and Orchestration
MEC	Multi-Access Edge Compute
ML	Machine Learning
M(V)NO	Mobile (Virtual) Network Operator
NFV	Networks Function Virtualization
NFVI	NFV Infrastructure
NR	New Radio
NS	Network Services
NSM	Network Service Mesh
OA	Onboarding Actor
OPEX	Operational Expenditure
OTC	Over The Counter
OTT	Over The Top
PKI	Public Key Infrastructure
PPP	Public Private partnership
PoC	Proof Of Concept
PRB	Physical Resource Blocks
QoS	Quality Of Service
RAN	Radio Access Network
RAT	Radio Access Technology
RO	Resource Offer
RPC	Rremote Procedure Call
SC	Service Consumer
SDO	Standard Developing Organization
SLA	Service Level Agreement
SO	Service Offer
SotA	State Of The Art
SR	Service Request
SRF	Service Requirement Functional
SRNF	Service Requirement Not Functional
STB	Set-Top-Box
TCP	Transmission Control Protocol
TDD	Time Division Duplex
TEE	Trusted Execution Environment
UC	Use Case
UE	User Equipment
UI	User Interface
UR	User Requirements
UTXO	Unspent Transaction Output
vCDN	Virtual Content Delivery Network
VF	Virtual Function
VM	Virtual Machine
VNF	Virtual Network Function
VoD	Video On Demand
WAN	Wide Area Network
WG	Working group
WP	Work Package

<END OF DOCUMENT>