



5GZORRO

AI-driven Zero-touch Operations, Security and Trust in Multi-operator 5G Networks: Reference architecture

Alexios Lekidis, Intracom Telecom

Paulo Chainho, Altice Labs

Gino Carrozzo, NEXTWORKS

Zero-touch security and trust for ubiquitous computing and connectivity in 5G networks

5G PPP Phase 3 project (ICT-20, 5G Long Term Evolution)

- Project Start: **Nov/2019**
- Duration: **30 months**

13 organisations from 7 different countries

- **Telcos:** Telefónica [ES] and Altice Lab [PT]
- **Regulator:** Malta Communication Authority [MT]
- **Large ICT Industries:** Intracom Telecom [GR], ATOS [ES], IBM [IL]
- **SMEs:** Nextworks [IT], Bartr Holdings Limited [UK], Ubiwhere [PT]
- **Research centres / universities:** I2CAT [ES], FBK [IT], Univ. Murcia [ES]
- **Communication specialist:** Comunicare Digitale [IT]





Contents

- Challenges addressed by 5G ZORRO Arch
- The 5GZORRO approach
- Conclusions

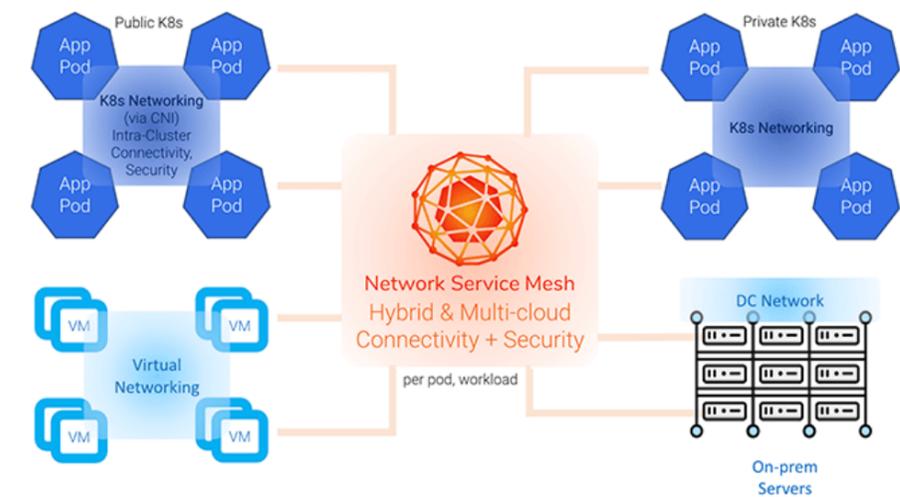
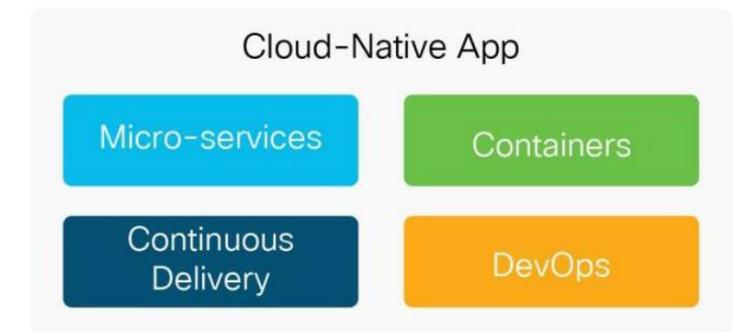
- **Challenges addressed by 5G ZORRO Arch**
- The 5GZORRO approach
- Conclusions

Challenges (1)

- 
Sharing heterogeneous types of resources (i.e. spectrum, virtualized radio access, virtualized edge/core, software defined WAN, etc.) **across multiple operators and infrastructure / resource providers** for truly pervasive 5G
 - Multi-party agreements to build on top of 3rd-party resources
 - e.g., micro-data centers at smart city IT infrastructures like edge computing at street cabinets or at lampposts

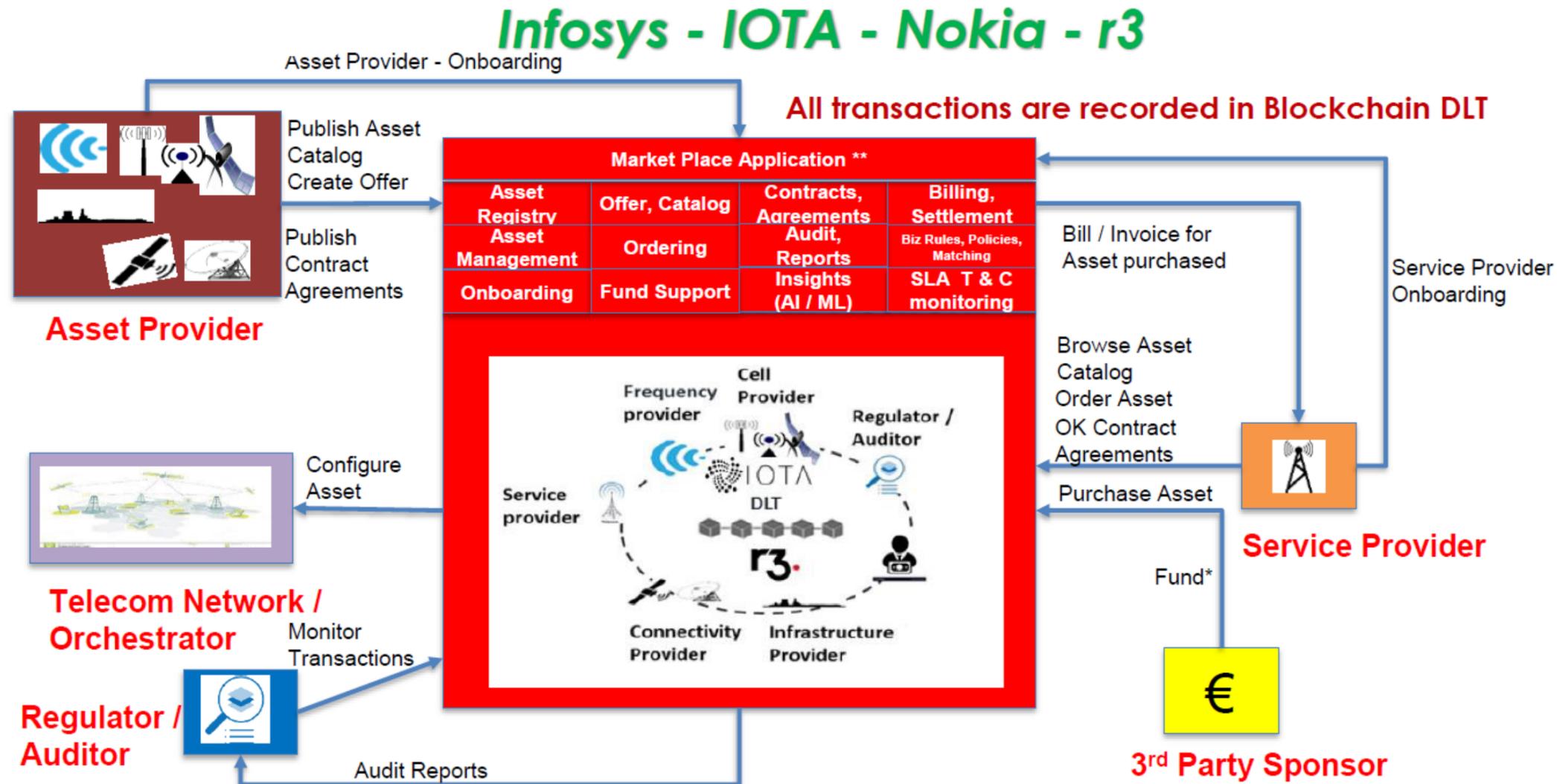
- 
Effective coexistence of Cloud-native vs more traditional IaaS network functions
 - Containers, service meshes, microservices, immutable infrastructure, and declarative APIs to make extremely flexible the service lifecycles

- 
Full automation of network and service management



Challenges (2)

- Cross-operator/cross-domain service chains with **security** and **trust**
 - across the **5G network sections**
 - among multiple parties



* Off chain process ** Application capabilities can be on-chain / off chain to demonstrate Blockchain Maturity Model

Src: TMForum Telecom Infrastructure Marketplace



Contents

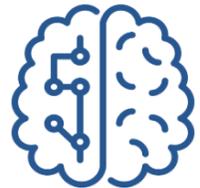
- Challenges addressed by 5G ZORRO Arch
- **The 5GZORRO approach**
- Conclusions

Building blocks for 5G consolidation/evolution



- **Operational Data Lakes**

- Logically centralized reservoirs of network operation data (e.g. resource monitoring, traffic captures, topology information, performance metrics, etc.) accessible via APIs for data access, processing, aggregation, filtering



- **Artificial Intelligence (AI)**

- To transform network orchestration and management into a cognitive process through which the network can self-adapt and self-react to changing conditions with minimal manual intervention



- **Distributed Ledger Technologies (DLT) / Blockchains (BC)**

- To implement distributed security and trust across the various parties involved in the 5G service chain

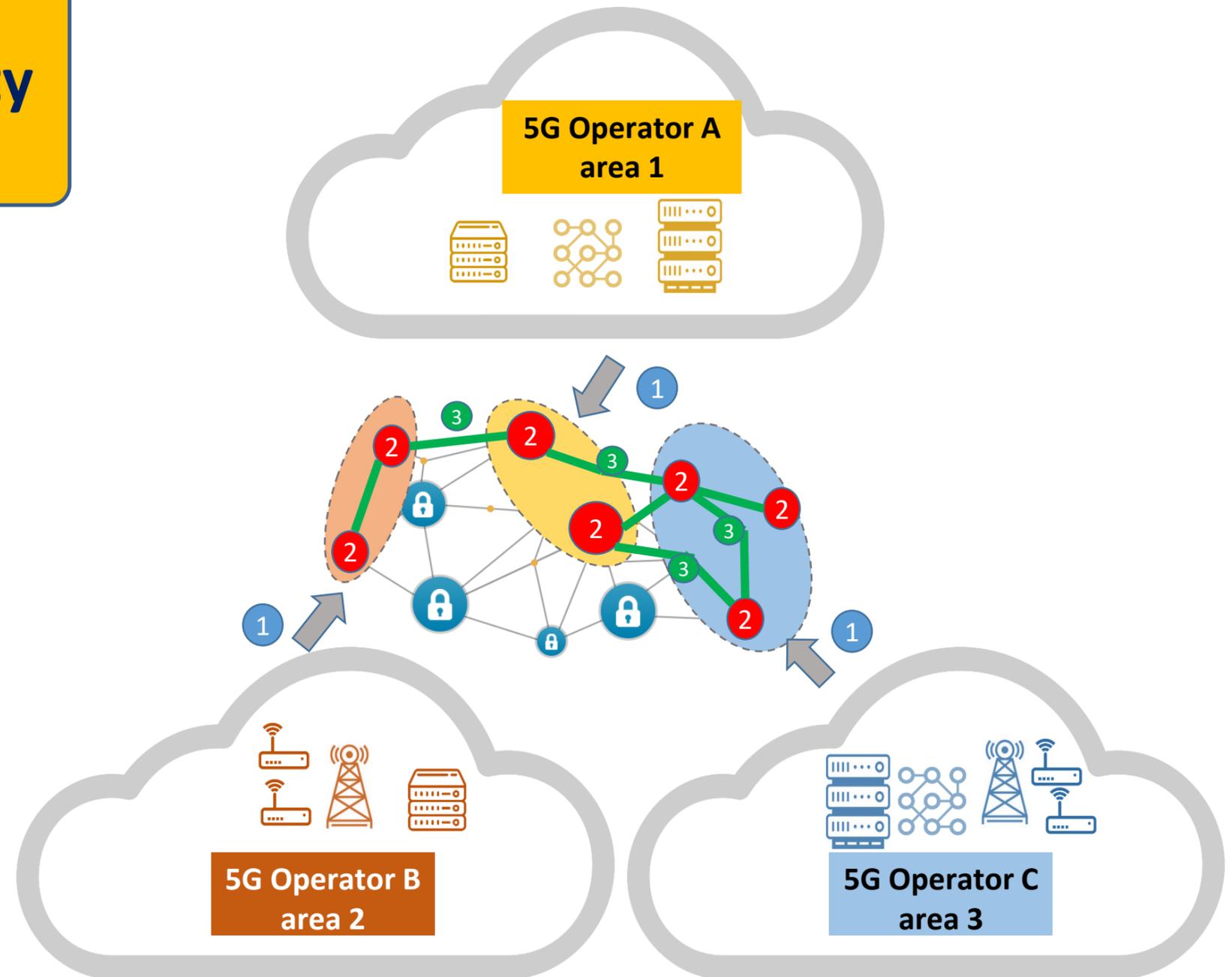


- **Cloud native technologies for SDN/NFV-based services for 5G**

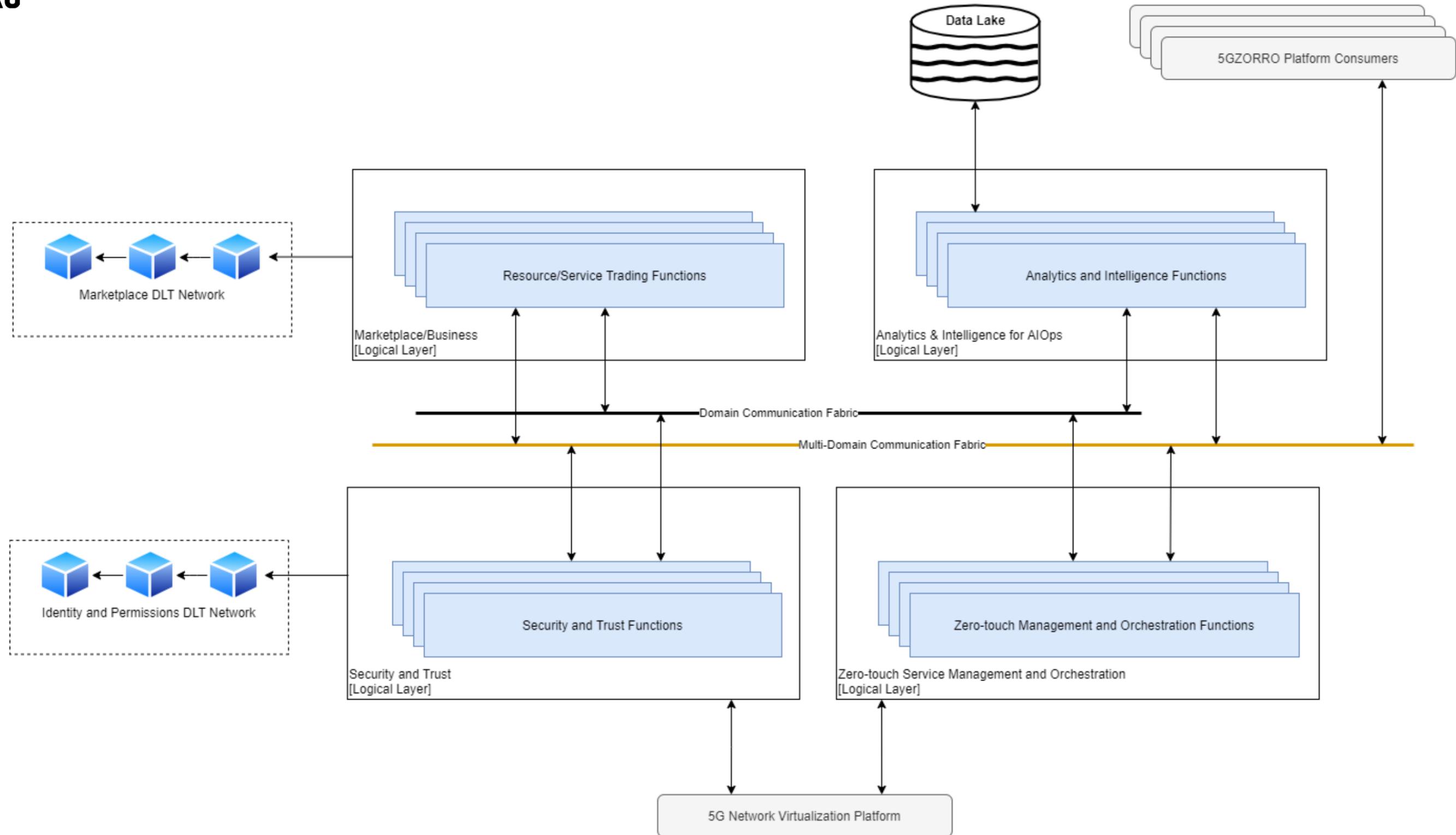
- To achieve the necessary flexibility, scalability and resilience of SDN/NFV-based services for 5G

Zero-touch security and trust for ubiquitous computing and connectivity in 5G networks

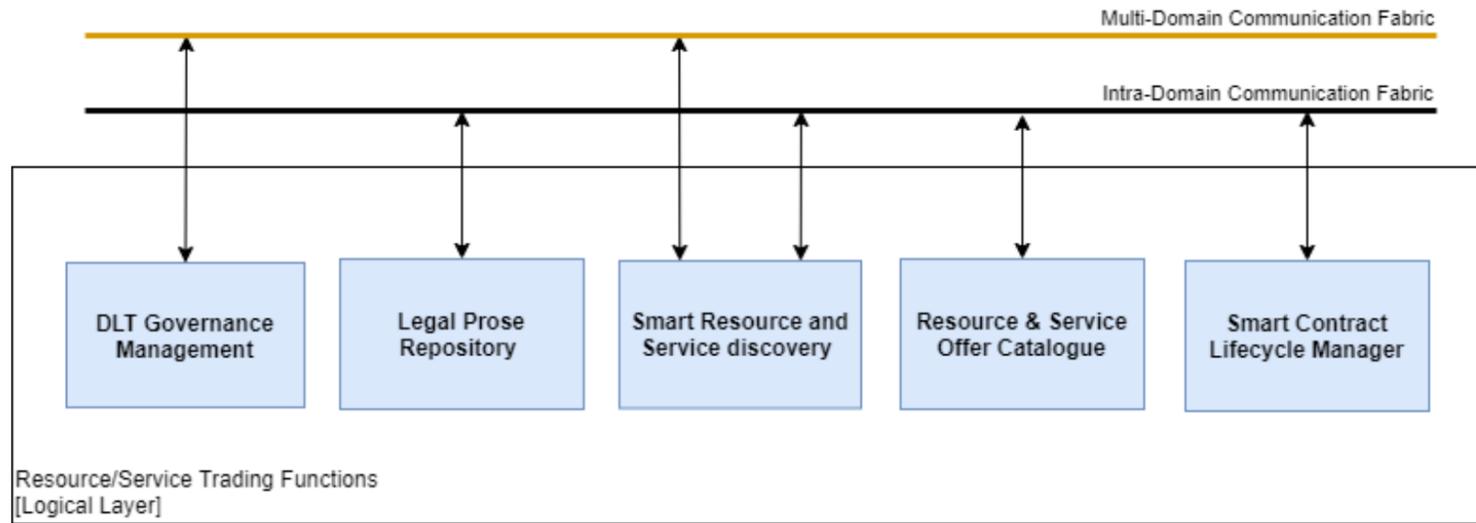
- 1** Zero Touch Resource Discovery using **DLTs** [for trust&security]
- 2** **Intelligent** 3rd party resource selection, request and access/use
- 3** **Trust establishment** among multi-parties



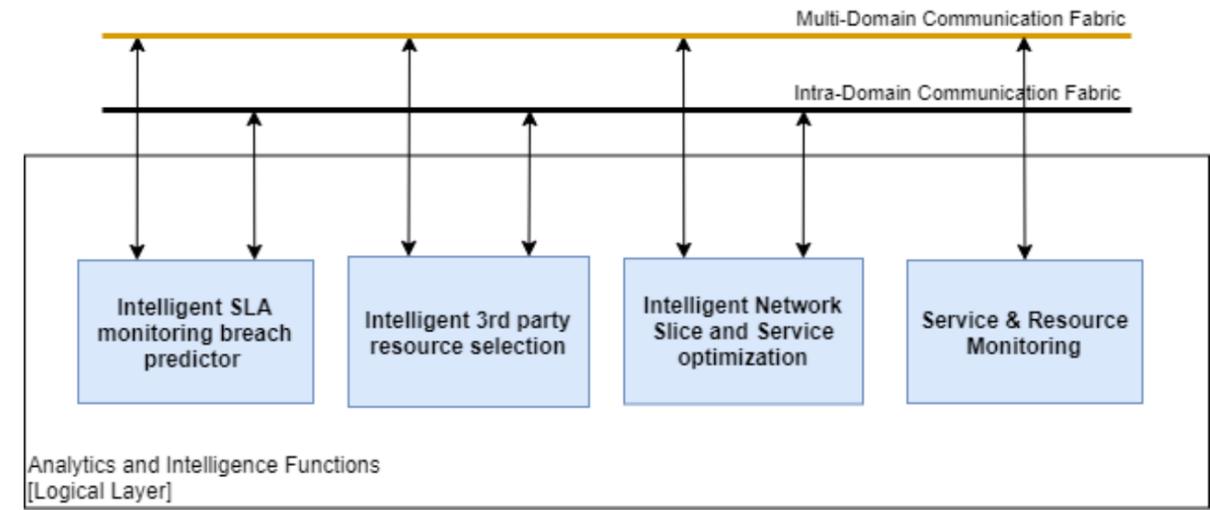
A new architecture for multi-operator 5G Networks



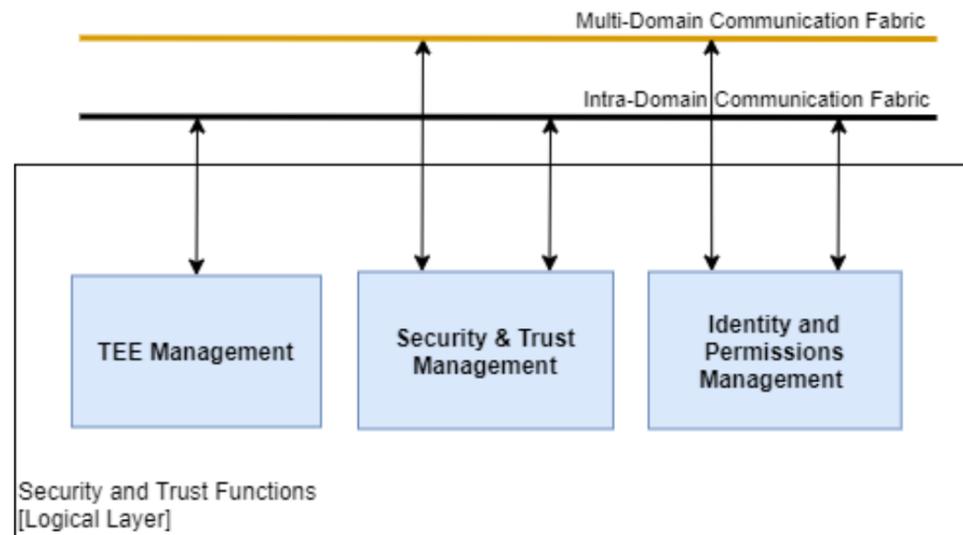
5GZORRO functional breakdown across the 4 layers



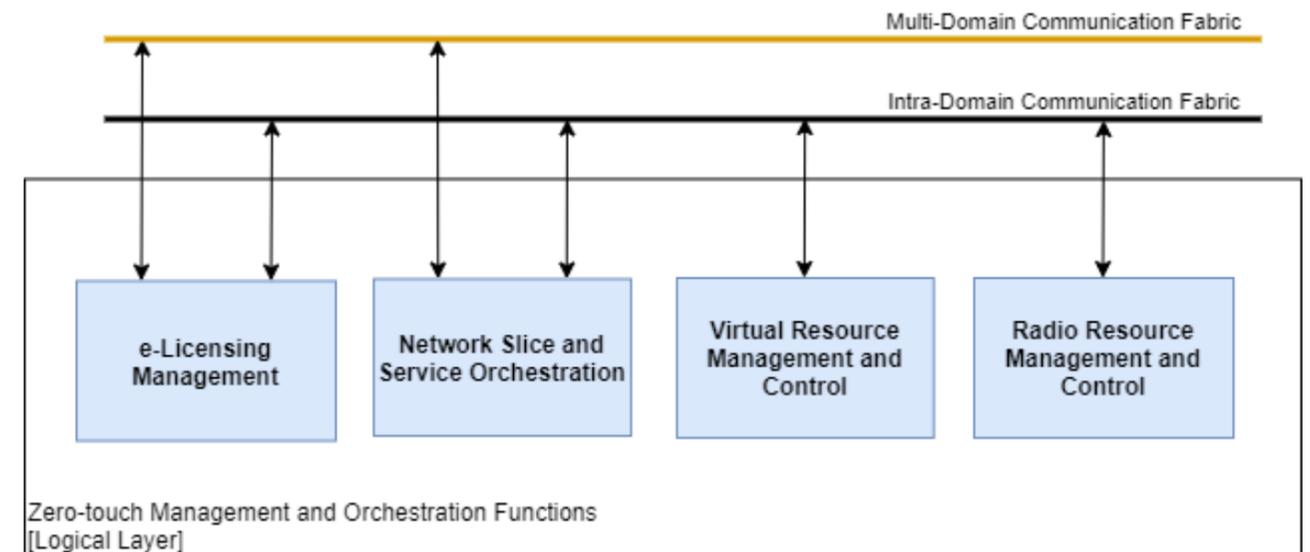
- Run decentralized catalogues for 5G Resource and 5G Service offers + legal proses
- Run life-cycle management for Smart Contracts among providers and consumers



- Trigger proactive scaling mechanism to increase/decrease resources for services
- Predict SLA breaches and discover the most appropriated resources in marketplace



- Manage global (cross-domain) distributed Identifiers
- Evaluate confidence/reputation of infrastructures and activities of other stakeholders when deciding which commercial relationships to establish



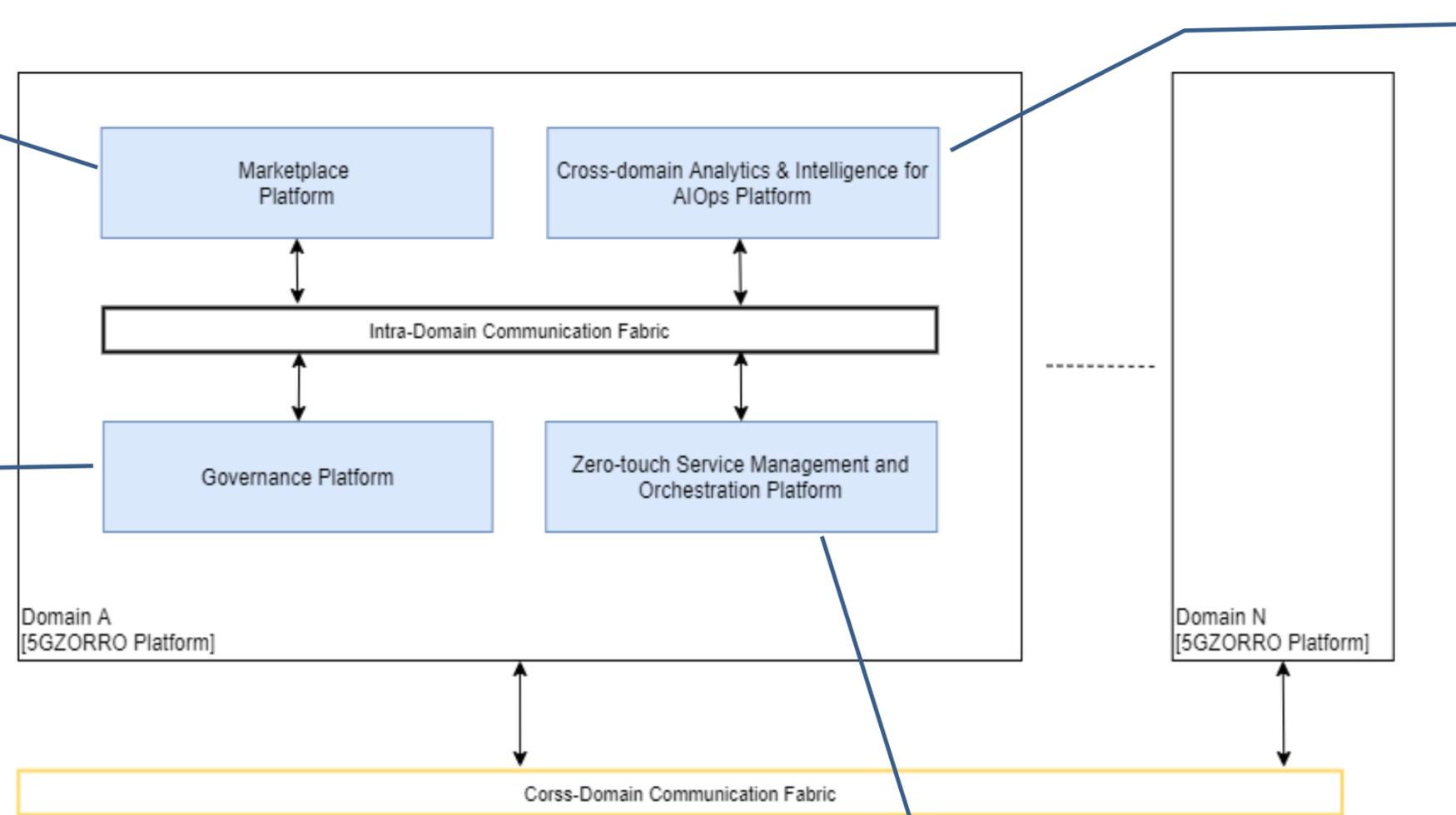
- Zero-touch automated management of 5G NetSlices & Services
- E-License Management for VNFs

Software Architecture Overview

Marketplace Platform leverages DLT technologies including Smart Contracts technologies to enable the trade of 5G resources managed by the zero-touch Service Management and Orchestration

Governance Platform is operated by stakeholders with permissions to take decisions according to the Marketplace Governance Model, featuring the decentralized management of DIDs and Verifiable Credentials by leveraging DLT technologies.

Intra-Domain Communication Fabric and **Cross-Domain Communication Fabric** are the two different types of Communication Fabrics in the 5GZORRO Platform; the former allows modules to communicate with other modules inside the same domain, and the latter allows modules to communicate with modules in other domains



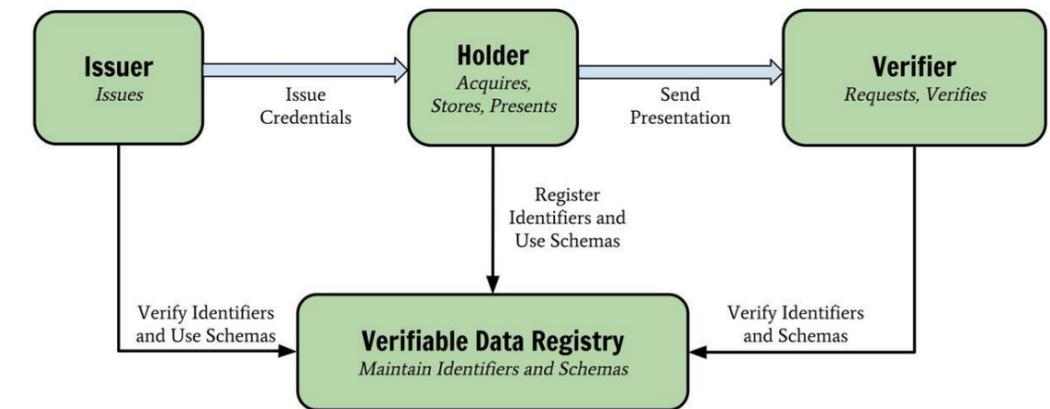
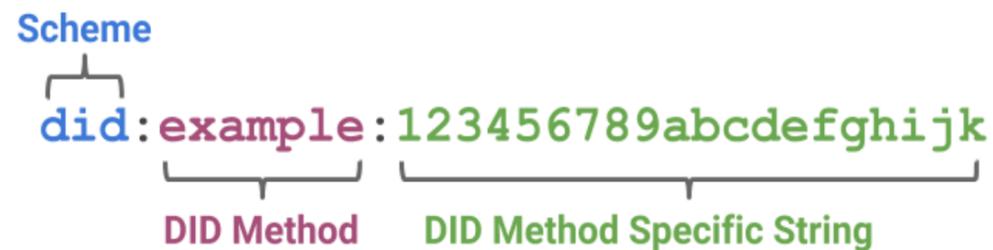
Cross-Domain Analytics & Intelligence for AIOps platform mainly comprises the cross-domain Functionalities from the Analytics & Intelligence for AIOps logical layer. It leverages distributed data lake and AI technologies to provide data persistence, data share and data analytics across domains

Zero-touch Service Management and Orchestration Platform Mainly responsible to control 5G Resources including Radio Spectrum resources, Transport Networking Resources and Computing resources (at data centers and at edge computing nodes) as well as existing legacy resource controllers from previous 5G deployments

Decentralized Identity management

Decentralized Identifiers (DIDs) to identify providers, consumers, services, resources, organizations, etc.

- Proposed by W3C to associate any owner (e.g. stakeholders, resources, services, organizations, entities) with a digital identity (DID document)
- Portable URL-based identifier generated as a string

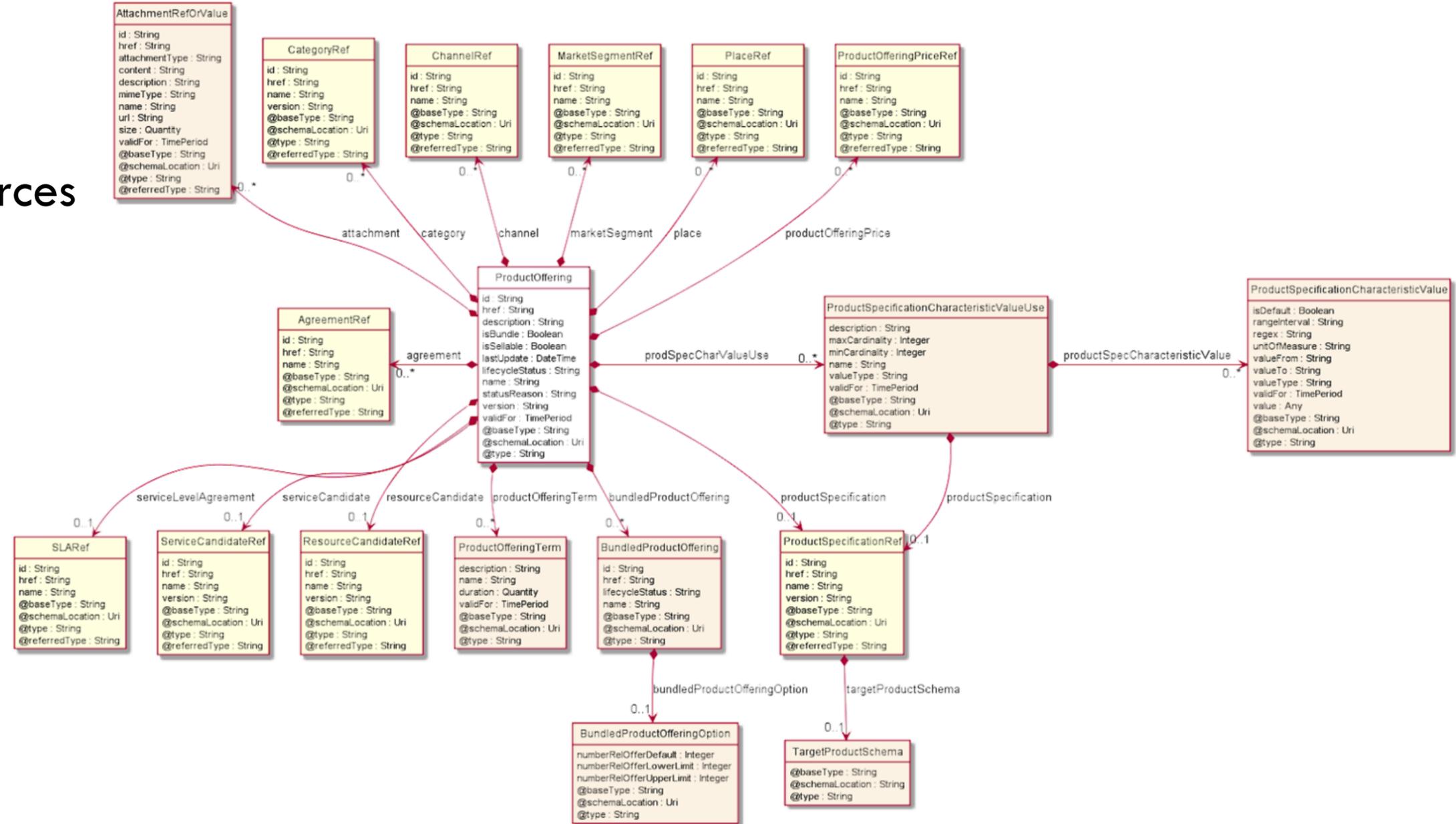


- Each DID resolves to a DID document
 - A DID document contains metadata to describe public keys, authentication protocols, and service endpoints necessary to bootstrap cryptographically-verifiable interactions with the identified entity

A Verifiable Credential (VC) is a tamper-evident and privacy-preserving credential (set of claims) that can be demonstrated through a cryptographic process

Use TMForum offering specs: Product-TMF620, Service-TMF633, Resource-TMF634

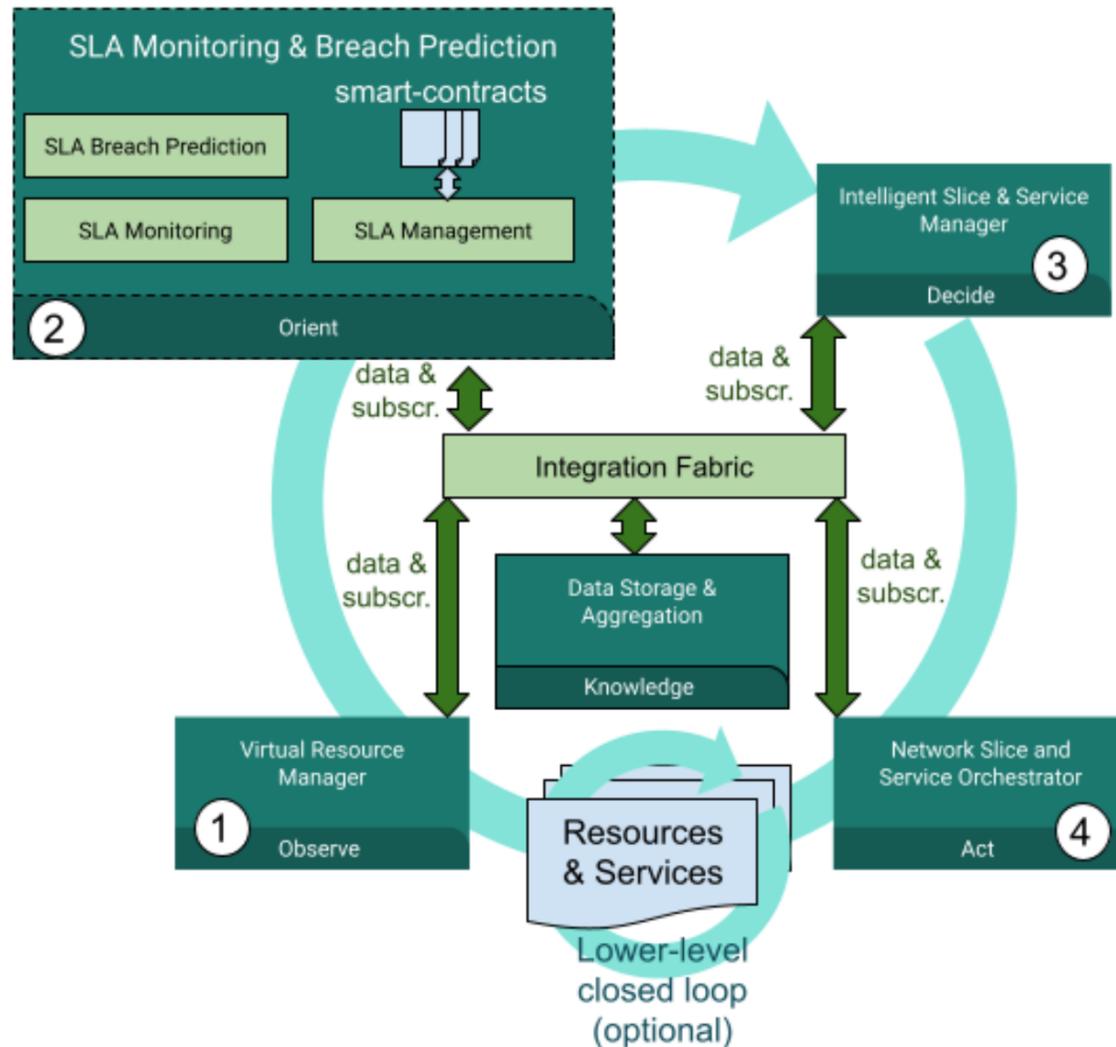
- Spectrum
- RAN elements (active & passive)
- Edge/Core Cloud resources (IaaS, PaaS)
- VNF/CNF
- Network Slice and Network Service



Architectural design based on ETSI ZSM

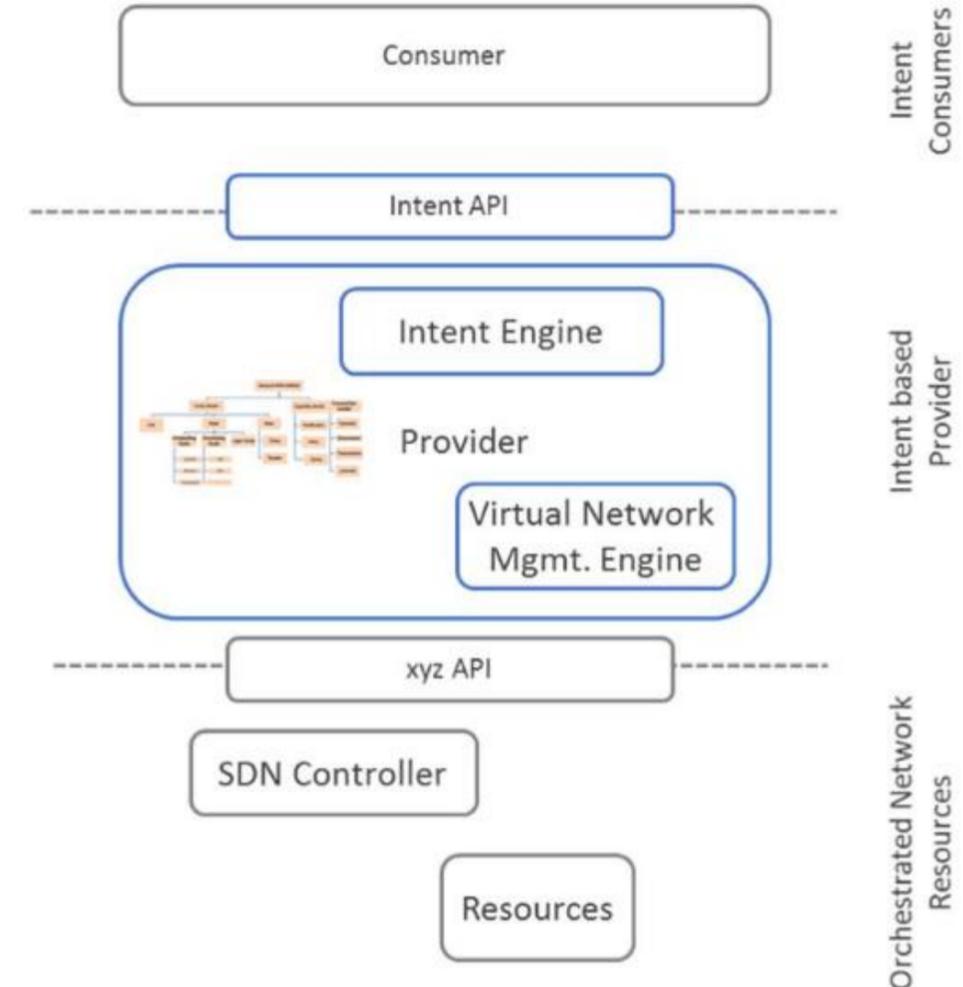
Closed-loop architecture

- Gathering of monitoring data about managed resources
- Data formalization into SLA monitoring metrics
- Issues and anomalies forecasting
- Mitigation actions



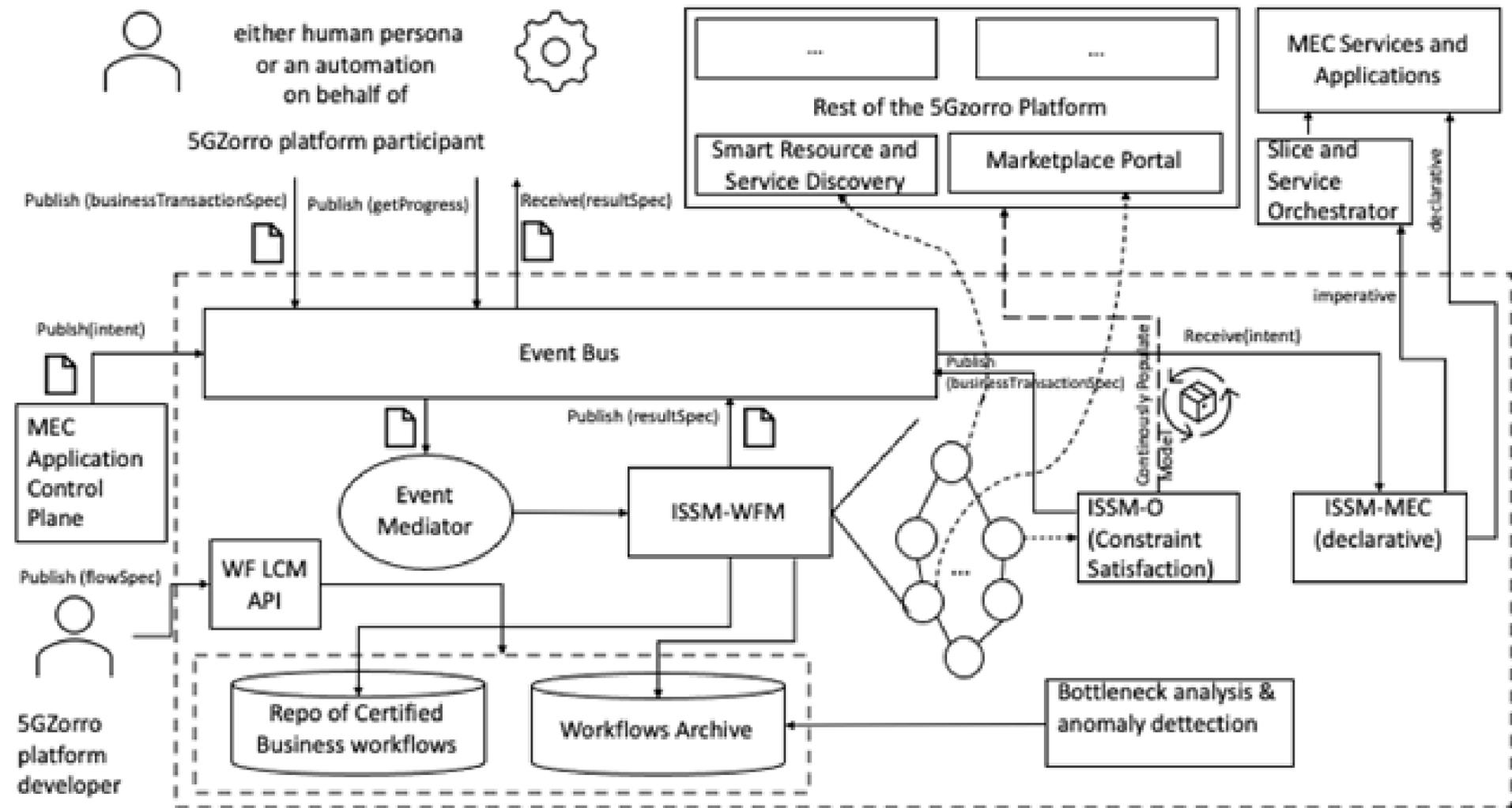
AI Resource/Service Discovery

- Intent-based discovery API
- Clustering of resource/service offers
- Ranking algorithms on resources based on intents



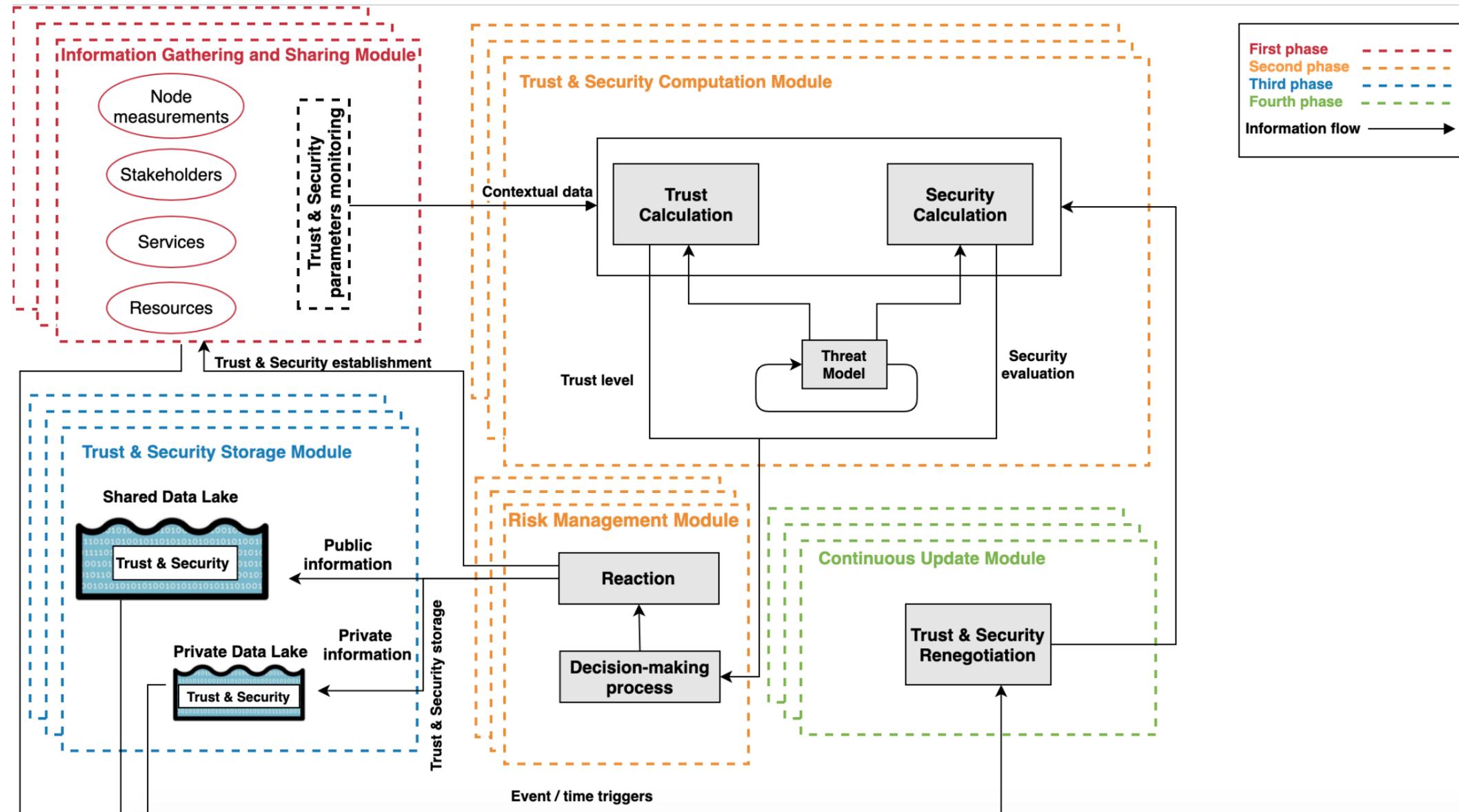
Slice automation through workflows

- Performs contextualized queries for available resources
- Extends the slice when it has run out of resources from the available offers
- Automates LCM for each slice
- Includes support for MEC-based applications
- Application development is also based on intents



Trust & Security computation among multiple operators

- Evaluate **reputation** to decide which commercial relationships can be better established
- Assess and **compute security and trust properties**
 - Use information from data lake
 - Check against Threat Models
 - Compute Risk and decide accordingly

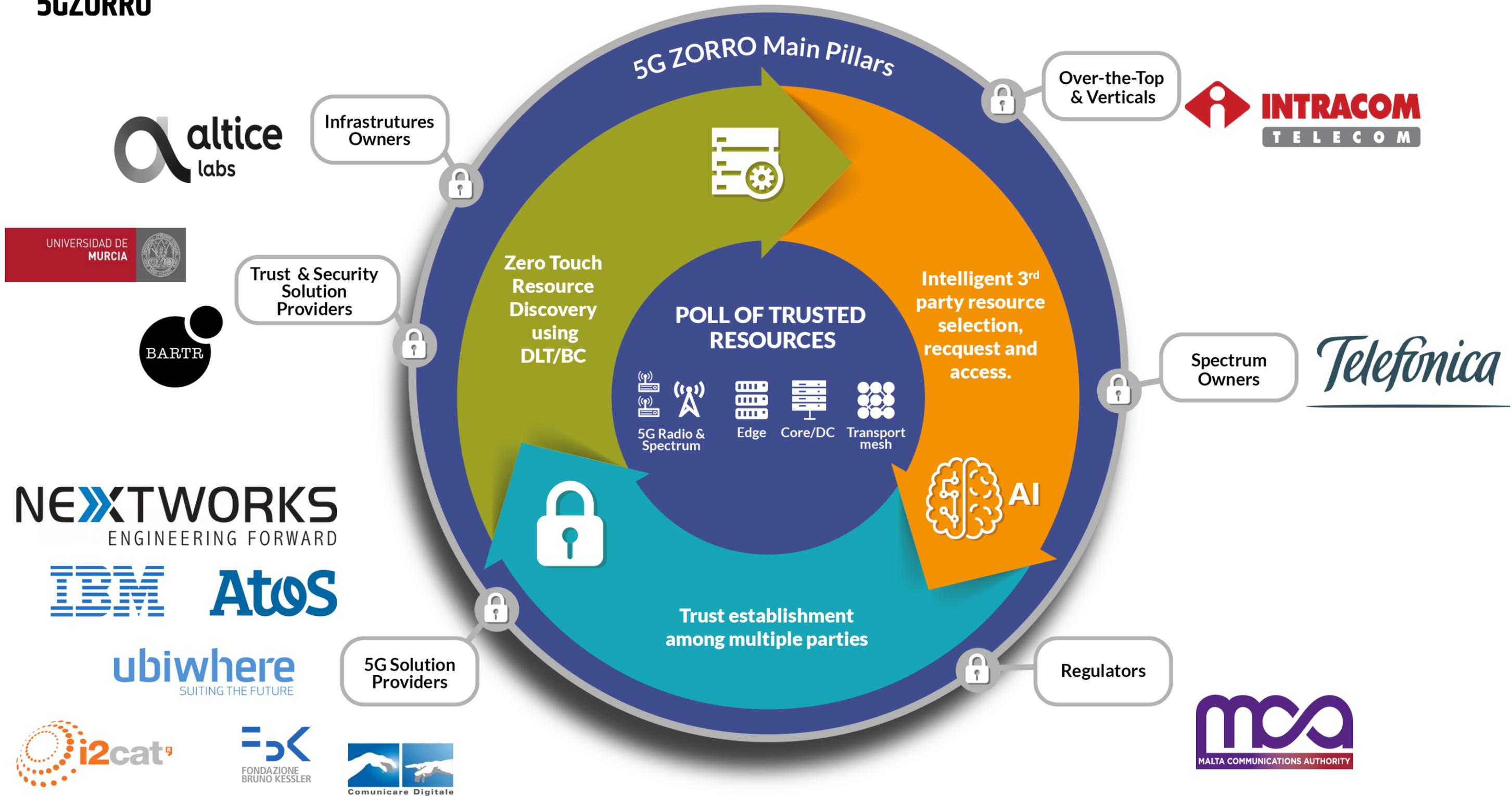




Contents

- Challenges addressed by 5G ZORRO Arch
- The 5GZORRO approach
- **Impact on evolution of 5G networks & future steps**

Addressing the needs of a structured ecosystem





5GZORRO architecture value propositions

Security and trust

→ *Increased network reliability and service scalability across domains*

Zero-touch automation

→ *Lower cost of development, maintenance and operation of network resources*

Spectrum market based on DLTs

→ *Best-practices in spectrum management and trading, reduced 5G spectrum capital expenditure*

Trusted environments and smart contracts

→ *New opportunities for cross-sector and open innovation from different parties*



Initial prototypes of **5GZORRO-core** components under development

Plans to start validations towards the end of Q2-2021 in



and



Thank You



Zero-touch security and trust for ubiquitous computing and connectivity in 5G networks



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871533