CLOUD NATIVE MANIFESTO

An Operator View

v1.0

www.ngmn.org

WE MAKE BETTER CONNECTIONS

CLOUD NATIVE MANIFESTO

An operator view by NGMN Alliance

Version:	1.0
Date:	06.09.2023
Document Type:	Final Deliverable (approved)
Confidentiality Class:	P - Public
Leadership:	Carlos Fernandes (Deutsche Telekom) Javan Erfanian (Bell Canada)
Programme Office:	Chris Hogg (representing NGMN)
Approved by / Date:	NGMN Board, 6th September 2023

EXECUTIVE SUMMARY

The term “Cloud Native” refers to a way of designing and operating applications, network functions, and services, in an open and flexible environment. Containers are used with Kubernetes, a de-facto orchestrator, in a micro-service architecture, as a fundamental design pattern. This approach leverages scalability, reliability, and automation and has successfully worked for large or very large deployments (for example by hyper-scaler cloud providers). The intention is to be efficient and cost effective, allowing fast time to market and providing the best customer experience.

As part of the key strategic pillars of NGMN strategy, namely Mastering the Route to Disaggregation, the cloud native debate stands as a high priority. Given the strategic impact of this paradigm shift, the foreseen implications to the operators in their adoption, and the multiple options and paths provided by industry players, it is the belief of NGMN Board members that a clear position on cloud native is required, so that the overall ecosystem can benefit and work towards better and more efficient telco services.

The community behind this manifesto document believes that both the telecommunications industry and its end-customers can benefit from adoption of a cloud native approach. This is not a simple copy exercise, but an effort to abstract the relevant cloud native principles and apply them in the telecom context which requires huge effort and changes to the network, and to the organisation as a whole. This manifesto document, therefore, touches on the application software architecture as well as the infrastructure and processes.

A declarative approach is needed for the cloud native infrastructure, to serve all the telecom scenarios through different topologies (core, edge distributed, RAN, FAN, transport, etc.) and technology (VM, bare metal) keeping a consistent deployment model everywhere.

This will allow operators to be consistent in their exposure of the available infrastructure capabilities, which can then be requested by an application; and which can verify and dynamically enforce the provider-consumer agreement.

The intrinsic dynamic nature of cloud native applications and infrastructure will demand a substantial shift in process supervision, which will enable greater multi-level granular service assurance based on a control loop and declarative target.

A reliable and solid source of truth repository is a central component of a cloud native architecture. This repository will ensure that the desired state is traceable, understood, and replicable – especially in the production environment – using fully automated digital pipelines.

Building a cloud native architecture calls for a joint effort among telecom operators, suppliers, and partners. This is described in this document by stating a few principal requirements and by outlining the area of focus for this journey from an operator point of view.

On our journey to highly flexible, sustainable, and resilient networks for the future, we believe in applying the following cloud native principles to all layers of network infrastructure, applications, and services*:

1. Decoupled infrastructure and application lifecycles over vertical monoliths;

2. 'API first' over manual provisioning of network resources;

3. Declarative and intent-based automation over imperative workflows;

4. GitOps** principles over traditional network operations practices;

5. Unified Kubernetes (or the like) resource consumption patterns over domain-specific resource controllers;

6. Unified Kubernetes (or the like) closed-loop reconciliation patterns over vendor-specific element management practices; and

7. Interoperability by well-defined certification processes over vendor-specific optimisation.

We also believe that openness and compatibility principles need to be key drivers of future Telecom and network services implementations to ensure we leverage Cloud Native principles to encourage software – orchestration – and hardware disaggregation.

---

* Does not imply order of priority
** Everything as code, single point of truth, immutable source of trust.

CONTENTS

01 A CLOUD NATIVE ABSTRACTION

Cloud native technology and architecture refers to an approach that enables the development and deployment of applications in the cloud and open environment using containerization, microservices architectures, and orchestration tools like Kubernetes. Special focus in this approach is put on scalability, resilience, and flexibility. Cloud native applications are typically built as a collection of loosely coupled services. Each service performs a specific function and can be developed, deployed, and scaled independently as well as on board any infrastructure (telco, private or public) and container platform. This approach promotes modularity and makes it easier to maintain and update individual components without affecting the entire system.

In addition, the cloud native approach brings in another appealing set of characteristics:

- **Closed-loop intent-based execution environment.** For the most part, Kubernetes has become the selected de-facto environment for a cloud native deployment (though not the only one and others might be developed in the future). This environment comes with the concept of "controllers" which can understand a desired state and always enforce it.

- **Separation and abstraction.** The Kubernetes framework maintains control of a specific set of capabilities while specifying a clean interface toward the infrastructure (e.g. CNI, CSI). This feature enables abstraction from the type of infrastructure the Kubernetes cluster runs on as long as the interfaces remain respected.

- **API driven.** Kubernetes is built upon API-first as a concept laying the foundation for a thorough 'as-a-code' approach and allowing a clean and scalable separation between the product coding and strictly controlled and fully automated deployment.

- **Enabling applications built for scale and maintainability.** Container-based applications with micro-services as design patterns potentially allow for larger scalability and simpler lifecycle.

The above 'characteristics' can be leveraged and extrapolated to inject in the telecom space a radical and positive change in the overall operational model, from the application to the infrastructure and laying the foundation for introducing sophisticated control mechanisms (e.g. AI-like) to reach the advanced concepts of the autonomous network.

In the next chapter, we will provide a view of what the cloud native target will look like for the applications, the infrastructure, and the operations.

02 CLOUD NATIVE IN THE TELCO SPACE

2.1 CLOUD NATIVE APPLICATIONS

On the application side, Cloud Native facilitates the deployment of advanced services (e.g. slicing, Non Public Network (NPN), Network As A Service (NaaS), etc.) and the interworking with cloud native enterprise applications. A number of game-changing attributes are expected:

a. **Natural Scalability** as virtually no constraints are placed from the Kubernetes infrastructure to horizontally scale in and out, leaving then the focus to build applications that can exploit this capability (also in the network integration).

b. **Improved Resilience:** Redundancy and auto-healing are naturally embraced, thus enhancing network reliability, and minimising downtime and manual restoring. This also includes the cases in which the underlying equipment has upgrades or fixes on a regular basis, without impact to the running applications.

c. **Faster Deployment and Simpler Lifecycle:** because of the model-based approach, organisations can rapidly deploy and update network services (e.g. inline upgrade and canary test), reducing time-to-market and risk for the currently complex lifecycle operations.

d. **Granular Security:** Cloud native networking incorporates modern security practices, such as micro-segmentation, enabling finer-grained control and isolation of network traffic, thus strengthening overall security posture. Moreover, with fast and reliable upgrades and updates, security patching will be better managed natively.

The capability set opens for a number of use cases such as:

- Scale in and out of the application in pursuit of energy efficiency, sustainability targets and cost efficiency;
- Modernise and make more efficient existing service assurance, with corrective actions being taken close to the root causes;
- Circuit breaker logic to isolate a security compromised portion of an application; and
- Creation of a more natural integration with the ecosystem of the Enterprise applications (where cloud native is a growing trend).

2.2 CLOUD NATIVE INFRASTRUCTURE

The intrinsic separation and abstraction brought in by the Kubernetes environment favour the following infrastructure development.

a. **Different types of infrastructure** (VM, Bare metal, smart NIC and HW accelerators - Telco/Private Cloud or Public Cloud) are abstracted in a consistent and predictable way and made consumable by the applications, as required.

b. **Shared Infrastructure** can be used by the network domain, including Core, Transport, RAN and fixed access, as well as IT (OSS, BSS, product catalogue, customer interface, etc.).

c. **Exposing the Opens APIs** of virtualized and containerized infrastructure assets. (CISM, VIM, etc.).

d. **A unique control plane** for the cloud infrastructure from the Core to the Edge, therefore, enabling a uniform deployment approach across the whole estate. This leads to a more uniform infrastructure (as proposed by Sylva) to simplify CNF integration with the infrastructure.

e. **Building a sophisticated orchestration and control layer** on top of the infrastructure control plane; open to introducing the latest technology evolution (for example leveraging AI type of approach).

Cloud Native infrastructure capabilities favour the following:

- To gain network agility and automate innovative new network applications efficiently, offering the network as a service.
- Smart workload placement matched to the infrastructure capabilities and capacity which then can be deployed where they are truly needed in a way to find the optimal balance for the investments required and scaling down whenever resources are unused.
- Dynamic assignment of resources keeping their level even with changed conditions such as required for true implementation of network slicing.
- Possibility to react quickly and efficiently to abnormal situations like disasters or other planned or unplanned events.

2.3 CLOUD NATIVE OPERATING MODEL

The operating model builds on the following pillars:

a. **Digital pipeline fully automated** and interconnected with suppliers' and developers' pipelines will take care of the lifecycle of both infrastructure and applications.

b. **A unique immutable source of truth** is used to drive deployments; once the common and harmonised artefacts are placed into the source of trust repository then further changes are not possible (similar to the GitOps approach). Operators must build this source of truth interconnected with various inventories.

c. **The desired deployment target is modelled through defined rules and artefacts** which can then be deployed and enforced in many ways.

d. **Automatic correction of anomalies is always the default approach** which requires critical attention to management and processing of the relevant information.

This operating model allows to:

- Create a clear and unique definition of what is the state of the production environment, and to have the possibility of increasing levels of traceability and audit to drastically reduce the configuration drift that is a major source of entropy and errors.
- Encourage harmonisation of tools and manual procedures.

03 PRINCIPLES AND REQUIREMENTS FOR CLOUD NATIVE TELECOM

1. Kubernetes or a similar same performant system must be the running environment for cloud native application

2. Independence between the infrastructure layer and application layer

a. Infrastructure exposes in a standard way the current and future capabilities to the Kubernetes layer (like HW accelerator or smart NIC).

b. The application can consume the abstracted capabilities without creating an implicit dependency outside of the explicit consumption model.

c. Application must limit dependency from a specific Kubernetes version or specific Infra version. The industry needs a more uniform infrastructure and to set up the integration capabilities.

d. Software, network functions and applications are enabled to be on boarded by any hardware, container platform or public domain.

3. The cloud native application is built:

a. Embracing the microservices architecture.

b. For horizontal scalability.

c. To allow auto-healing.

d. To allow configuration through the Kubernetes construct without manual intervention.

e. To be deployed through a fully automatic process.

f. To enable a rolling update from one version to the next.

g. Compatible to any infrastructure and container platform.

4. Intent-based description for the cloud native application and service

a. This application descriptor shall be based on standards.

b. It shall be possible to describe what type of abstracted resources are exposed by infrastructure.

c. It shall be possible to define services in a declarative way and expose them via API to customers.

5. Application lifecycle management is entirely automated through a digital pipeline process

a. Production deployment artifacts are all contained in a source of truth repository that drives an automatic deployment. The approach is the same as the code.

b. Only a change in the source of truth causes a change in the production environment, which otherwise cannot be changed.

c. Pipelines must be interoperable, through Gitops repositories and integration labs.

d. Ensure to employ DevOps techniques that actively make cloud native continuous deployment efficient.

6. A well-defined certification process for cloud native applications shall be available in the industry

a. To ensure high confidence in the integration leaving only a smaller verification effort to the telecom operator.

b. Tests shall be developed to cover the most important cases for network integration.

c. To cover security aspects.

d. To ensure compatibility and interoperation between software/function/CNF and hardware/infrastructure with container platform.

7. From monitoring to observability

a. Infrastructure and cloud native application shall provide a rich set of information to be able to understand the overall status in a simple and fast way.

b. Information shall be used as close as possible to solve anomalies and conditions locally.

c. This move is also essential towards the development of fully autonomous networks. This is a major transformation for brownfield operators.

d. To offer an open-source monitoring toolkit designed especially for microservices, from metrics to insight, and supports integration with third-party exporters.

8. Sustainability by design

a. With more reliable operations and greater confidence in the fact that deployment can be modified without compromising stability will drive to better environmental efficiency.

b. Turning servers on/off and taking advantage of horizontal scaling will pave the way for more energy efficiency.

c. Standardised mechanisms for carrying out energy consumption measurement and orchestration strategy elements that are sensitive to energy consumption need to be integrated by design.

04 INDUSTRY FOCUS TO DELIVER CLOUD NATIVE

a. **Skills Gap and Mindset** not only to bridge the technology gaps but also to embrace a radically different silo-less approach in telecom development and related operational process (e.g. introducing a more holistic perspective with SRE and NRE). New culture towards software centricity is needed to become agile and adopt to this new architecture.

b. **Network applications Interoperability:** the effort required to develop a solid and strong certification process for network applications and functions going cloud native and to harmonise their release management ensuring interoperability and openness.

c. **Legacy Management and work in standards bodies and open source** This is not only related to managing the transition from legacy infrastructure but also working in standard bodies to bring procedure and protocol improvements to make the transition to cloud native more efficient and less costly.

d. Ownership and understanding of the relevant integration problems through the cloud native journey (e.g. among inventory systems and source of truth repository).

e. **Tools sprawling limitation:** Up to now, Telco and network services implementation are led by multiple fragmented teams mainly working in silos with limited synchronisation at their organisation borders. As a result, there is no convergence in terms of tooling, and there is overlap with mainly prescriptive practices limiting the automation capability.

f. **Data focus for observability and AI focus for extended automation:** We know that AI will be a game changer in how we operate at scale the new generation of cloud native telco infrastructure to gain more autonomous operations. However, the way observability, traffic, and usage data are designed, will have a critical impact on our ability to have AI-enabled operations and real automation. It will be key to proposing a coherent and consistent data strategy to leverage traditional monitoring practices toward observability and to enable AI to reach its true potential for our business cases.

g. **Commercial Model:** Commercial models should be introduced to animate vendors to deliver open documentation, and open APIs as opposed to closed systems where professional services were offered for service providers to create new services. With the adoption of cloud and DevOps, it's important to create some agility and ownership within service providers as well for innovation in services while vendors could continue to build revenue by providing high-quality software with open APIs for service providers' consumption. New commercial models will bring a new equilibrium on win-win between operators and vendors for the benefit of end-customers with a value chain that helps technology vision thrive on cloud native, open ideology and practices.

h. **Deliver/identify a common, standardised, industry-wide model for Cloud Native infrastructure:** As an entry point to a declarative, automated, API-driven, dynamic telco cloud infrastructure, the industry should agree on a, standard abstraction model to represent Telco Cloud infrastructure; this will enable native portability of cloud native applications across sites, platforms, vendors, and operators. There are multiple options for the implementation of the automation backing the API: each operator may develop its own internal pipelines or may collaborate with others in open-source cloud platform implementation projects, or rely on commercial solutions by cloud vendors that comply with the aforementioned standard API model.

05 CONCLUSIONS

By embracing Cloud Native, telecom operators can unlock the full potential of the open and interoperable system of infrastructure, container platform and functions / applications leading towards achieving greater agility and scalability, enhanced operational efficiency, cost effectiveness and deliver innovative services for the benefit of their customers.

For telecom operators, none of this can lead to a clou native transformation without sharing requirements and expectations with vendors and partners in order to provide seamless services and journey. That is why a framework of requirements and a reference implementation model from an operator point of view need to be used to ensure validation of our new disaggregated telco stack, where Open Source Telco Stack project Sylva could be a catalyst.

There are clearly aspects that will require focus such as certification and network integration, and to tackle them the operators recommend a concerted effort is needed across the different initiatives and standard bodies (like LFN, CNCF, ETSI and 3GPP).

Cloud Native is also a cultural shift, which requires preparation and attention on aspects related to processes and people skill sets, re-factoring and modernisation of legacy applications, and commercial models that would allow vendors to provide open solutions that would support better service innovation.

In order for this new technology and architecture to be successful, it is the operators view that strong collaborations of players and stakeholders in the industry are needed to achieve the common goal together.

Finally, this journey will create the right and needed platform and systems to adopt and exploit the latest technologies of which we already see signs of today (for example the adoption of AI), finally landing into the domain of true Autonomous Networks, as TM Forum advocates.

NGMN continues to work towards shaping industry requirements that promote growth and technology leadership. The work done under the Operating Disaggregated Networks program (ODiN) has already delivered extensive insights and guidance in the field, in both Versions 1 and 2, with upcoming Version 3, scheduled for release in Q1 2024, aiming to detail the operating models recommended to the organisations willing to fully embrace the journey, including the cloud native principles included in this document.

On our journey to highly flexible, sustainable, and resilient networks for the future, we believe in applying the following cloud native principles to all layers of network infrastructure, applications, and services*:

1. Decoupled infrastructure and application lifecycles over vertical monoliths;

2. 'API first' over manual provisioning of network resources;

3. Declarative and intent-based automation over imperative workflows;

4. GitOps** principles over traditional network operations practices;

5. Unified Kubernetes (or the like) resource consumption patterns over domain-specific resource controllers;

6. Unified Kubernetes (or the like) closed-loop reconciliation patterns over vendor-specific element management practices; and

7. Interoperability by well-defined certification processes over vendor-specific optimisation

We also believe that openness and compatibility principles need to be key drivers of future Telecom and network services implementations to ensure we leverage Cloud Native principles to encourage software – orchestration – and hardware disaggregation.

---

* Does not imply order of priority
** Everything as code, single point of truth, immutable source of trust.

06 ABBREVIATIONS

CISM	Container Infrastructure Service Management
CNF	Cloud native Network Function
CNI	Container Network Interface
CSI	Container Storage Interface
FAN	Fixed Access Network
HW	Hardware
NaaS	Network As A Service
NIC	Network Interface Controller (also known as Network Interface Card)
NPN	Non Public Network
NRE	Network Reliability Engineering
SNPN	Standalone Non Public Network
SRE	Site Reliability Engineering
RAN	Radio Access Network
VM	Virtual Machine

07 ACKNOWLEDGEMENTS

Special acknowledgements go to the following Operator Members, who made significant contributions to the development of this publication:

Bell Canada
BT
Chunghwa Telecom
Deutsche Telekom
Orange
Smart/PLDT
Telia
TELUS
Turkcell
Vodafone

NEXT GENERATION MOBILE NETWORKS ALLIANCE E.V

NGMN, established in 2006, is a global, operator-led alliance of over 80 companies and organisation spanning operators, manufacturers, consultancies and academia.

VISION

The vision of the NGMN Alliance is to provide impactful industry guidance to achieve innovative, sustainable, and affordable mobile telecommunication services for the end user with a particular focus on Mastering the Route to Disaggregation / Operating Disaggregated Networks, Green Future Networks and 6G, whilst continuing to support 5G's full implementation.

MISSION

The mission of the NGMN Alliance is

- to evaluate and drive technology evolution towards 5G's full implementation and the three major priorities for 2021 and beyond:

  Route to Disaggregation: Leading in the development of open, disaggregated, virtualised and cloud native solutions with a focus on the end to end operating model.

  Green Future Networks: Building sustainable and environmentally conscious solutions.

  6G: Emergence of 6G highlighting key trends across technology and societal requirements plus use cases, requirements and design considerations to address.

- to establish clear functional and non-functional requirements for mobile networks of the next generation.
- to provide guidance to equipment developers, standardisation bodies and cooperation partners, leading to the implementation of a cost-effective network evolution.
- to provide an information exchange forum for the industry on critical and immediate concerns and to share experiences and lessons learnt for addressing technology challenges.
- to identify and remove barriers for enabling successful implementations of attractive mobile services.