National Telecommunications and Information Administration

5G Challenge Notice of Inquiry

Ericsson Response

Company

Company Name: Ericsson Inc.

Mailing Address: 6300 Legacy Drive, Plano TX, 75024

Point of Contact

Name: Patrik Ringqvist

Mailing Address: 6300 Legacy Drive, Plano TX 75024

Telephone: (214) 228-1880

Email: patrik.ringqvist@ericsson.com

Table of Contents

1 Executive Summary

Ericsson is a leading provider and trusted supplier of 5G and information and communications technologies to service providers around the globe. The United States is our largest market worldwide, and Ericsson has a longstanding and expanding commitment to the United States: our presence in the United States dates back 120 years, and we have 7,700 employees in the United States. Section 2 below has more details on this topic.

Ericsson is also an active contributor towards building an open ecosystem, including the 'open 5G stack'. We are one of the leading contributors in 3GPP (3rd Generation Partnership Project), O-RAN (Open Radio Access Network) Alliance, OSC (O-RAN Software Community), and ONAP (Open Network Automation Platform) initiatives. Please see Section 4.2 for additional information on Ericsson's participation in fostering open ecosystem.

Ericsson proposes the open 5G stack "Challenge" to be a lab managed by the DoD where all vendors can bring their components of the open 5G stack for functional and interoperability testing. We believe that a multi-vendor 'Open Ecosystem Plugfest' of 5G components will encourage the vendors – both new and incumbents – to contribute open 5G stack components within their areas of expertise and innovation. The results of this testing will also help define a current state-of-the-art open ecosystem. An 'Open Ecosystem Plugfest' of this magnitude and importance will typically motivate the vendors to take their products to the next level. This 'Open Ecosystem Plugfest' will also provide an opportunity for other markets—like the enterprise market—to understand the developments and progress that have taken place towards an open ecosystem, thereby fostering further innovations in the overall open 5G stack market. Please refer to Section 4.3 for more on our "Challenge" proposal.

Finally, Ericsson will bring in the following open 5G stack components to this proposed 'Open Ecosystem Plugfest':

- Cloud RAN functions
- Cloud infrastructure for RAN functions
- Cloud Native 5GC (5G Core) functions
- Cloud infrastructure for CN (Core Network) functions
- Service Management and Orchestration
- Security

Please refer to Section 4.4 to learn more about Ericsson's contribution to the proposed "Challenge'.

We look forward to having a follow up discussion with NTIA on our open 5G stack "Challenge" proposal and contributions to the open 5G stack.

2 Introduction

Ericsson is a global 5G leader. We were the first supplier with live commercial 5G networks on five continents. We now support the widest ecosystem of supported devices on 5G live networks, with 111+ commercial 5G agreements or contracts with unique operators. And, we led the way on 5G standards, with the highest share of 5G patent declarations (15.8 percent) of any organization in the world. We are the largest holder of standard-essential patents for mobile communications, with 54,000 patents. Finally, we participate in more than 100 industry organizations, standards bodies, and other technology alliance groups.

As this response demonstrates, we are committed to advancing the U.S. 5G marketplace, the U.S. 5G ecosystem, and U.S. global leadership in 5G with secure 5G networks and systems. The United States is our largest market worldwide, and Ericsson has a longstanding and expanding commitment to the United States: our presence in the United States dates back 120 years, and we have 7,700 employees in the United States. As a trusted supplier for all major domestic service providers and many regional carriers, Ericsson brings the following elements to our 5G operations in the United States:

- Our North American headquarters, located in Plano, Texas, is the site of key development operations, as well as product support, design, integration, verification, and release activities.
- Ericsson opened the first standalone 5G Smart manufacturing facility in the U.S. in Lewisville, Texas. The 300,000 square feet state-of-the-art factory is producing 5G and Advanced Antenna Systems to boost network capacity and coverage to meet the rapid demand for 5G as the next evolution mobile technology rolls out across the U.S. The factory puts Ericsson's 5G equipment supply chain close to our U.S. customers, and improves sustainability from an energy efficiency perspective. Ericsson has invested over $100 million in the facility.
- Our five Centers of Excellence (CoE) provide enhanced tower technician training facilities for best-in-class field services training and support for Ericsson as well as our partners' employees. Ericsson's five Centers of Excellence in the U.S. have trained and certified more than 3900 crew members since 2015. We support 65 percent of the 5G deployments across the United States, including efforts to close the digital divide in rural America.
- Our Austin, Texas, R&D center is a strategic investment in maintaining Ericsson's leadership position in 5G technology. Application-specific integrated circuits (ASICs) and software developed in Austin is instrumental in the global 5G mobile telecommunications infrastructure, which ushers in industrial digitalization and realization of IoT communications.
- D-15, our innovation hub at Ericsson's Silicon Valley facility in Santa Clara, California, allows our industry partners and customers to accelerate adoption of advances in artificial intelligence (AI) and machine learning.

3 Requested Information

NTIA (National Telecommunications and Information Administration) issued an inquiry on January 11, 2021, for all interested stakeholders to explore the creation of a 5G "Challenge" that would accelerate the development of the open 5G stack ecosystem in support of DoD (Department of Defense) missions. Ericsson's response to the key questions raised in the Notice of Inquiry (NOI) are provided below.

4 Ericsson Response

4.1 Introduction

As noted in the 5G Strategy Implementation Plan[1], "DoD has an opportunity to become an early adopter of 5G applications, which helps U.S. industry move more quickly in development and maturing those applications as well as the underlying 5G ecosystem." This effort will require a collaborative partnership with private industry where existing innovation and expertise continue to deliver leading edge networks and services. The foundation for this innovation is sustainable through an open and competitive marketplace where market forces determine technology solutions. This technology neutral approach will ensure that a secure and trusted 5G network will meet the existing demands of the DoD mission and evolve as the mission requirements expand. The following proposal seeks to demonstrate the existing interoperability across multiple vendors, sustainable through a technology neutral approach, and highlights the key impediments towards developing a fully open 5G stack.

4.2 Ericsson's contributions to the open ecosystem

Ericsson is committed to driving alliances that bring forward global scale with a strong ecosystem. Ericsson contributes to several alliances, including 3GPP, IEEE (Institute of Electrical and Electronics Engineers), IETF (Internet Engineering Task Force), O-RAN Alliance, OSC, and ONAP in order to enable global scale of economy, innovation, and inter-operable systems. The following are some of our contributions:

- The 3GPP has been the global standardization forum to lead the development of mobile communications by defining its protocols since 1998. Many of the 3GPP interfaces, such as the interface between the mobile device and the radio network (Uu), the interface between the radio and core networks (S1, NG) etc. are fully open and interoperable. Ericsson is an active contributor in 3GPP with the most input papers on the first releases of 4G and 5G and has invested tens of billions of dollars

[1] See Department of Defense 5G Strategy Implementation Plan: Advancing 5G Technology & Applications. Securing 5G Capabilities (December 15, 2020) https://www.cto.mil/wp-content/uploads/2020/12/DoD-5G-Strategy-Implementation-Plan.pdf

over more than three decades to create the world's 2G, 3G, 4G and 5G technology. We hold several 3GPP leadership positions and regularly collaborate with multiple US based eco-system players, such as Qualcomm, Apple, Intel, Facebook, and Google et al.

- Our work in the O-RAN Alliance builds on a foundation created by 3GPP, which has defined more than 100 open interfaces as of today. We are actively contributing to O-RAN specifications and focusing our efforts around open multidomain orchestration, automation and virtualization as a foundation for openness. Among the nine WGs (Working Groups), we are the co-chairs of WG2 (Non-RT RIC and A1 Interface) and WG5 (Open F1/W1/E1/X2/Xn Interfaces). We are also the editor of the following four specifications:
    - WG1: O-RAN Architecture Description
    - WG2: A1 Interface Specification
    - WG5: NR C-Plane Profile
    - WG6: O2 Interface Specification
- In OSC (O-RAN Software Community), Ericsson sits in its TOC (Technical Oversight Committee) and serves as the PTL (Project Technical Lead) for the 'Non-RT RIC (Non Real-Time RAN Intelligent Controller)' project.
- In ONAP, Ericsson has a seat in the TSC (Technical Steering Committee) and actively participates in more than 5 subcommittees with 50+ developers. We are the main code contributors in 7 projects and have been consistently among the top five companies with committers.

4.3 Challenge Structure & Goals

Ericsson proposes that a common lab is set up by the DoD where all vendors can bring their components of the open 5G stack for functional and interoperability testing. This multi-vendor 'Open Ecosystem Plugfest' of the open 5G stack components will achieve several goals:

- It will encourage vendors – both new and incumbents – to contribute open 5G stack components within their areas of expertise and innovation. The DoD, of course, needs to implement a framework around protecting the IPR (Intellectual Proprietary Rights), trade secret etc. of each vendor so that the vendors can freely participate in this 'Open Ecosystem Plugfest'.
- It will educate the ecosystem stakeholders on the status of innovation in open 5G stack components.
- The results of testing will help define the current state-of-the-art open ecosystem. It will also highlight the key impediments of developing an open ecosystem.

- A Plugfest of this magnitude and importance will typically motivate the vendors to take their products to the next level. That will drive further improvement and innovations in the overall open 5G stack market.
- The DoD, with the help of industry experts, will develop the metrics for evaluating each open 5G stack component to be tested at this 'Open Ecosystem Plugfest'. This evaluation will help to identify the maturity level of each contribution.
- The insights from this 'Open Ecosystem Plugfest' – i.e., what worked and what did not work – will enable DoD to make an informed understanding towards a more mature open 5G stack ecosystem.
- The interaction between the vendors in this open environment will foster better understanding and appreciation of each other. This will potentially create more partnership opportunities and further collaboration.

The following figure shows the O-RAN architecture with 5G components.

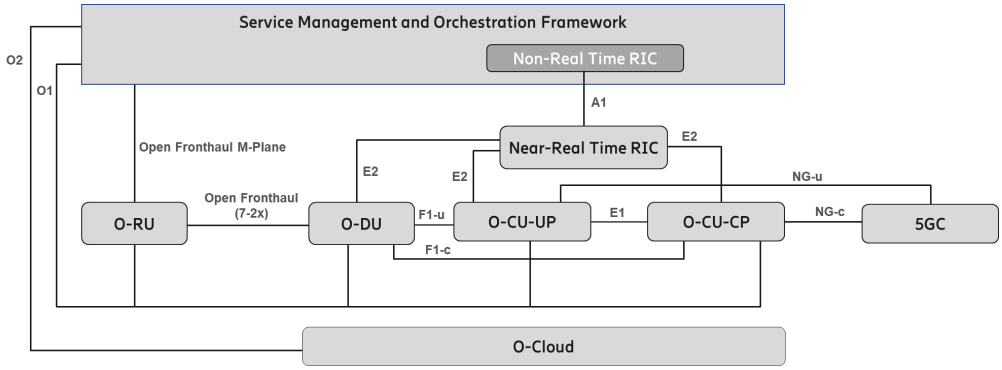


Figure 1: O-RAN architecture with 5G components

4.4 Incentives and scope

Ericsson proposes to contribute the following open 5G stack components to this 'Open Ecosystem Plugfest':

- Cloud RAN functions
- Cloud infrastructure for RAN functions
- Cloud Native 5GC (5G Core) functions
- Cloud infrastructure for CN functions
- Service Management and Orchestration
- Security

The following figure shows these open 5G stack components:

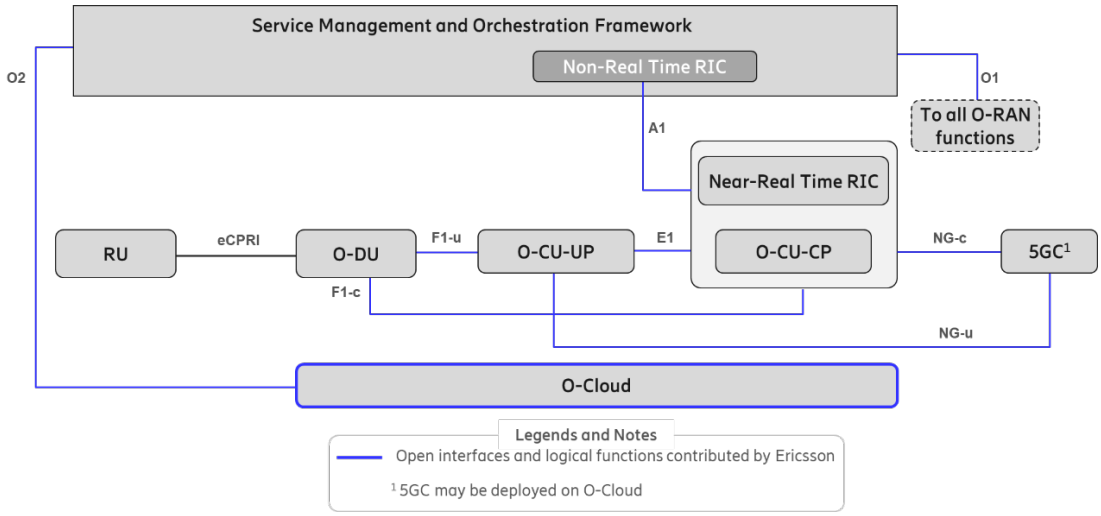


Figure 2: Ericsson components of open 5G stack

The following sections discuss each component.

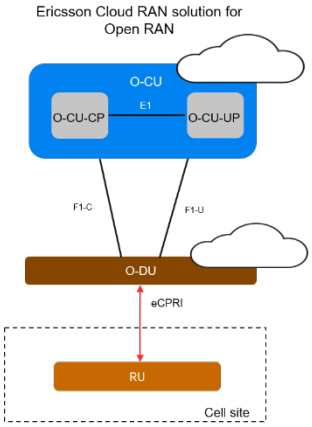
4.4.1 Cloud RAN functions

5G calls for new levels of flexibility in architecting, scaling and deploying telecom networks. Cloud technology provides interesting possibilities to complement the existing tried and trusted technologies in the RAN domain. Cloud RAN refers to realizing RAN functions over a generic compute platform instead of a purpose-built hardware platform.

Cloud RAN by Ericsson is a cloud-native software solution. As the telecom industry deploys 5G networks around the globe, technologies such as automation and virtualization, with Cloud RAN specifically, will play a key role in future network evolution. These technologies will be the catalyst for more openness in networks, with cloud technology offering new innovative alternatives for RAN deployment that complement existing tried and trusted solutions. Ericsson Cloud RAN will add more versatility to network buildouts to address a variety of 5G use cases.

5G RAN architecture consists of Centralized Unit (CU) and Distributed Unit (DU). Centralized Unit consists of the centralized unit control plane (CU-CP) and user plane (CU-UP) functions. CU-CP handles the Radio Resource control part of the CU function and scales with subscribers/connections. CU-UP handles the Packet Data Convergence Protocol and scales with the throughput. CU-CP and CU-UP have relatively low sensitivity to latency, so are suitable for virtualization using standard hardware platforms.

Distributed Unit covers the latency-stringent lower layers of the RAN stack namely, Physical Layer, Medium Access Control and Radio Link Control. Greater RAN workload as obtains in Massive MIMO beamforming radios will require greater processing power in the server hardware with hardware assist in the form of accelerators.



Function	Sub function	Main Processing function	Scales with
Centralized Unit CU	Control Plane (CU-CP)	Radio Resource Control	Subscribers/connections
	User Plane (CU-UP)	Packet Data Convergence Protocol	Throughput
Higher Layer Split (HLS)			
Distributed Unit DU	Digital Unit	Radio Link Control	TTI, bandwidth & branches
		Medium Access Control	TTI, bandwidth & branches
		Physical Layers	Branches & bandwidth
Lower Layer Split (LLS)			
	Radio Unit	Beamforming (if applicable)	Branches & bandwidth

Figure 3: Ericsson's Cloud RAN solution

Ericsson Cloud RAN solution for Open RAN consists of Virtualized O-DU and Virtualized O-CU as software applications. The O prefix here reflects the Openness of the RAN application to run on a third party, non-proprietary hardware and cloud platforms.

The Cloud RAN DU and CU are the Cloud RAN application software that can run on third-party hardware and cloud infrastructure, thus providing a platform for multivendor innovation in 5G.

1. **Fully cloud-native realization of both CU-CP and CU-UP**. This provides independent scaling for centralized control and user planes and creates locational flexibility in deployments
2. **Cloud-native realization of the DU function**. This brings challenges around server and accelerator selection, cloud infrastructure and OAM, capacity dimensioning, power efficiency planning and security planning.

Ericsson Cloud RAN is fully compatible with standard-based eCPRI interface towards the radio units for both 5G standalone and non-standalone deployment models. Virtualization and multi-domain orchestration will also create a foundation for future RAN openness. Cloud RAN by Ericsson is designed to support Service Management and Orchestration architecture including Non-Real Time RAN Intelligent Controller (Non-RT RIC), in line with O-RAN interfaces.

4.4.1.1 Cloud Infrastructure for RAN Functions

Cloud RAN by Ericsson is a cloud-native software solution handling compute functionality in the RAN. Ericsson cloud RAN is cloud agnostic to underlaying (Container as a Service) CaaS layer and x86 HW.

Apart from the cloud RAN application software, the cloud infrastructure has its own processing demands on the server hardware infrastructure. The processing needed for a fully loaded, low-band (i.e., FR1-FDD) cell on a commercial-off-the-shelf (COTS) server, excluding processing for operating system and common functions, is roughly 1 core. Comparing to a fully loaded, mid-band (i.e., FR1-

TDD) cell without any accelerator this would be about 16 cores. The difference in processing volume comes from the amount of data produced and consumed in the mid-band system, differences in bandwidth, layers and traffic models. It is roughly 20 times larger in downlink compared to a low-band cell.

The figure below shows a rough calculation.

	Bandwidth	Layers in DL	Layers in UL	Total DL bandwidth (Bandwidth x Layers)	Total UL bandwidth (Bandwidth x Layers)
Low-band	20MHz	4	1	80MHz	20MHz
Mid-band	100MHz	16	8	1600MHz	800MHz
				~ 20x processing need	~ 40x processing need

Figure 4: Cloud infrastructure processing requirements for low-band and mid-band RAN

Low band workloads can be realized over a pure software-based implementation on x.86 servers; however, mid band over x86 based implementation will require offloading processing of certain layer 1 functions to more specialized hardware, called accelerators.

As indicated above, mid-band offers higher bandwidth and larger number of MIMO (Multi-Input Multi-Output) layers compared to the low-band. These mid-band features present the possibility to render extremely high capacity and speed promised by the 5G technology.

Ericsson is actively contributing to O-RAN Alliance´s working group 6 (WG6) with the ambition to allow for specification of many accelerator profiles and open capability negotiation between hardware and software. In selection of the cloud infrastructure, the virtualization approach itself could allow for optimized lower footprint. Virtual machines, where a hypervisor layer is needed to virtualize the infrastructure for software applications, typically require a greater number of compute cores. Thus, to further reduce hardware footprint, increase processing efficiency, operational flexibility and achieve lower TCO, the current best approach is using Kubernetes containers on bare metal. This essentially removes the virtualization layer (see the figure below) paving the way for a light weight, cloud-agnostic, efficient implementation of VDU and VCU workloads. Network Interface Cards (NIC) need to be selected for the right sync requirements and I/O throughput for user plane heavy functions such as CU-UP and DU.

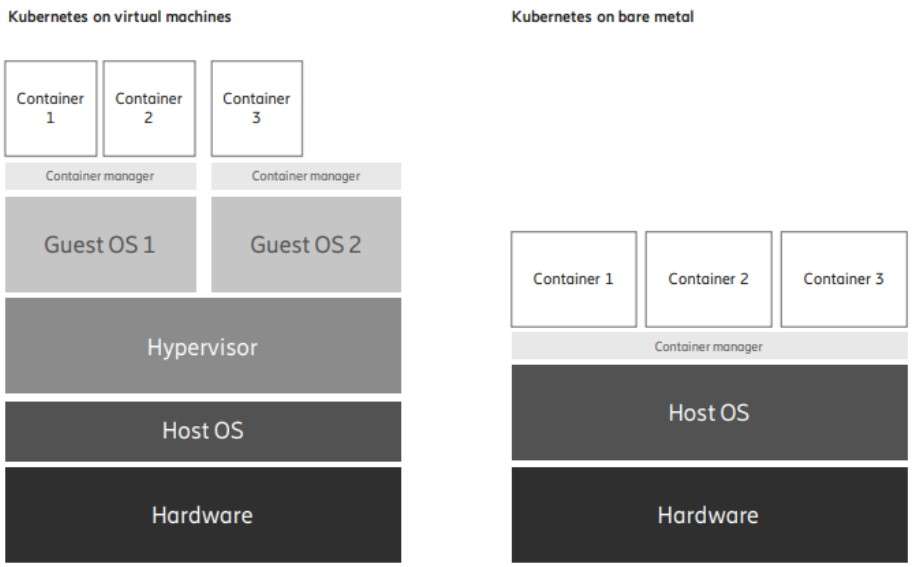


Figure 5: Kubernetes on virtual machines vs. bare metals

Cloud native implementation allows introduction of micro services-based architecture and distribution of network functions over different cloud infrastructures across multiple data centers and far edges of the networks very close to where the services are being consumed. From an operational perspective, there are three main benefits. Firstly, the software upgrades are faster and simplified, as virtual machine layer and associated upgrade complexities are eliminated. Secondly, there is a unified competence across applications, since the system is less diversified. Finally, the life-cycle management of the system is simplified, as the application onboarding is unified.

Ericsson can deliver a pre-verified Cloud RAN solution comprising COTS hardware (and accelerators where needed), O-cloud infrastructure, 5G RAN that includes Radio Unit, Cloud RAN CU software, Cloud RAN DU software, and Radio gateways where needed for optimized transport performance.

Finally, Open RAN/ Cloud RAN comes with its own security requirements. Ericsson is leading with contributions in this area in SDOs in order to help realize a robust, secure, trusted solution. This is addressed in Section 4.4.4 below.

4.4.2 Cloud Native 5GC functions

4.4.2.1 5G Cloud Packet Core Overview

Building on market leading virtual Evolved Packet Core (EPC) applications, Ericsson is dedicated to supporting our customers on a smooth evolution from EPC to dual mode core operations, 5G EPC and 5GC. We ensure flexibility, fast time to market and efficiency in operations.

Ericsson's packet core solution is currently deployed in more than 300 commercial customer networks supporting a variety of use cases. Some of these use cases are brand-new and enabled by this new technology, while others are currently evolving use cases with a new level of automation and speed. Here are some examples:

- Mobile broadband (MBB) to modernize and manage capacity growth, addition of sites, and migration to datacenters. Our solution scales from a single COTS server for thousands of users to more traditional large-scale MBB operations with more than 10 million subscribers.
- Introduction of network slices to support massive IoT with decoupled lifecycle from consumer MBB service. This enables new IoT devices network connectivity for Cat-M and NB-IoT.
- Use enterprise slices at oil rigs, medical manufacturing sites, and steel plants etc. to realize the Industry 4.0 requirements.
- Bring new communication services such as VoLTE and Wi-Fi calling with fast rollout supported by full virtual EPC and IMS applications.
- Smooth network evolution from EPC to 5GC to enable faster time to market, higher performance and lower total cost of ownership.

4.4.2.2 5G Core Network Solution

Ericsson's dual-mode 5G Core solution delivers cloud native applications that supports EPC and 5G Core 3GPP architectures. The decomposition of software into microservices facilitates a fast, low-cost method of introducing new services at any scale. It supports easy and effective scaling of services from hundreds of users to hundreds of millions of users.

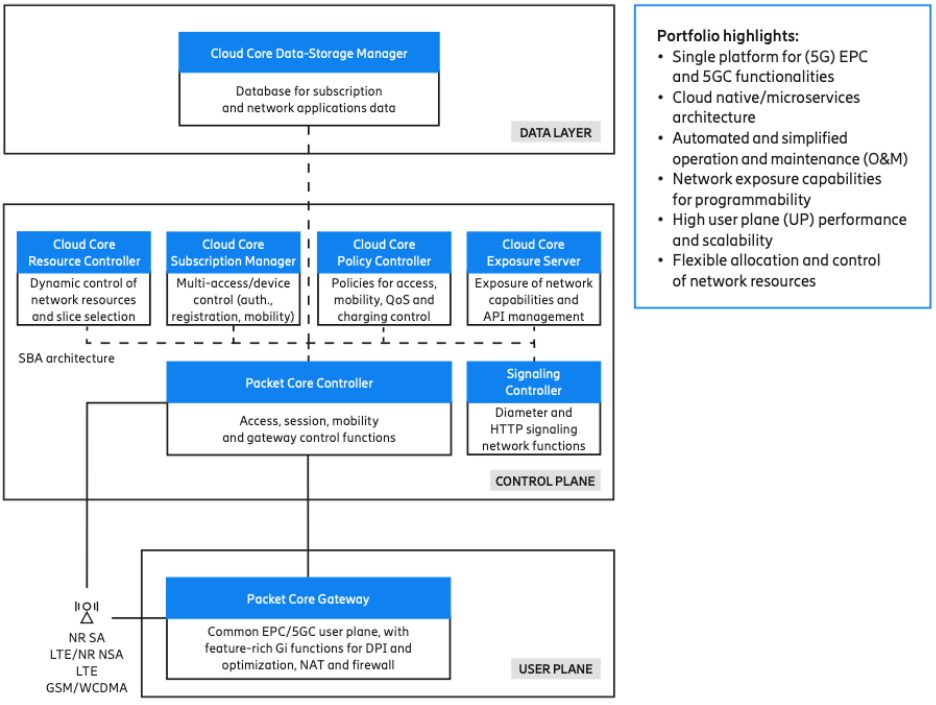


Figure 6: Dual-mode 5G Core

4.4.2.2.1 5GC with Service Based Architecture

Ericsson has implemented SBA based 5GC, which is the new standard from 3GPP introduced in Release 15 allowing, among other things, the 5G New Radio (NR) in a standalone (SA) fashion to be connected to the Core. With SBA, a new software architecture based on IT principles is introduced, allowing for faster service creation. This architecture is also the base for the evolution of all future 3GPP core standards.

4.4.2.2.2 Dual Mode Platform

Ericsson's implementation of cloud native and SBA means one operational platform for both EPC and the new 5GC.This makes things much more streamlined by enabling migration toward 5GC either at the pace that the market demands, or according to a chosen strategy, or both.

4.4.2.2.3 Cloud Infrastructure for 5GC Functions

Cloud native applications (CNA) need to be agnostic to the underlying infrastructure. As we evolve the cloud infrastructure towards supporting container as a service (CaaS), the requirement for agnosticism remains, but the challenges become different. The CNA requires a container infrastructure and must be deployable either on CaaS or infrastructure as a service (IaaS) platforms.

The next natural step is to deploy the CaaS environment directly on the hardware, via bare metal deployments. However, VM (Virtual Machine) based applications will remain for the foreseeable future. To avoid fragmentation and multiple operational models, we foresee an extended CaaS layer, which would be capable of managing both VM and container workloads. For telco applications, the CaaS layer provides the most cost-efficient multivendor integration point with strong de-facto realizations like Kubernetes and Helm.

Ericsson's 5GC solution consists of the cloud native applications (CNAs) that are built following a set of design principles to allow deployment in cloud environments that meet the needs of the telecommunications industry. These principles are:

- agnosticity
- decomposed software
- application resilience
- state-optimized design
- orchestration and automation

These principles enable the deployment of Ericsson's 5GC CNAs on fully open cloud infrastructure, either private (e.g., OpenStack, Kubernetes etc.) or public (AWS, Azure, Google etc.).

4.4.3 Service Management and Orchestration

O-RAN Alliance defines Service Management & Orchestration (SMO) as a critical component to manage the RAN domain. Ericsson's SMO product is based on O-RAN Alliance's guidelines and uses open source ONAP as the foundation, with added features to bring values to service provider's multi-vendor RAN. The values of Ericsson's SMO can be summarized as follows:

RAN optimization:

- Extend RAN automation with AI (artificial intelligence) based fast loop by being close to the node at the edge.
- Improve RAN performance with data enrichment from local, regional, or centralized geographical domains, as defined by the customer.
- Drive innovation and time to market features with cloud native multi-vendor software applications that are managed on an open platform.

Integrated ecosystem:

- Facilitate FCAPS operations with tools including application SDK, cataloging, orchestration, inventory, data collection, policy administration & runtime, etc.
- Provide open APIs to integrate with customer's existing BSS/OSS to achieve interworking in a cohesive fashion.

Operation efficiency:

- Support multi-vendor, multi-tenant, and multi-domain scenarios.
- Manage services and slices dynamically with other physical and virtual network functions.
- Automate provisioning, optimization, healing and assurance for complex RAN domain.

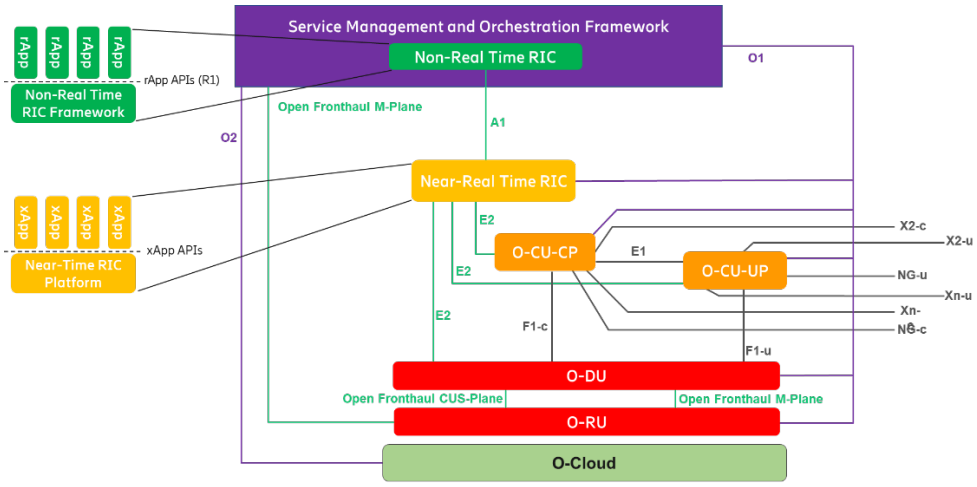


Figure 7: SMO and its relationship to RAN components

Ericsson's SMO provides both **design** and **runtime** environment for the network automation and optimization applications. These intelligent applications, called "rApps," (Non-RT RIC Applications) are cloud native microservices deployed to control the RAN network elements. To support advance service assurance and

automation, they can be artificial intelligence/machine learning (AI/ML) applications that are trained and fine-tuned on domain specific data for localized or end-to-end network analytics and optimization.

The design and orchestration environment of the SMO allows for rapid development, onboarding, deployment, and life cycle management of the applications (e.g., rApps and xApps).

The runtime environment of the rApps in SMO is aligned with Non-RT RIC. It provides standard based open R1 interfaces to allow execution of rApps developed by various sources (e.g., Ericsson, customer's own applications, and 3rd party applications).

The underlying SMO platform provides applications with common utilities to access network data. The mediation layer of the SMO provides open O1, O2, and A1 interfaces between the control applications and the network functions.

The SMO software uses cloud native technology that can be deployed into customer's choice of public or private cloud. Ericsson is developing an open standard based solution with flexible packaging options to meet our customers' operational needs.

4.4.4 Security

The NTIA 5G Challenge can evaluate the 5G threat surface, including 3GPP Releases 15 and 16 security improvements for 5G, O-RAN's expanded threat surface introduced by new interfaces and functions, open source software threats and vulnerabilities, and the trust stack in 5G cloud networks. Each of these is shown in the figure and described further below.

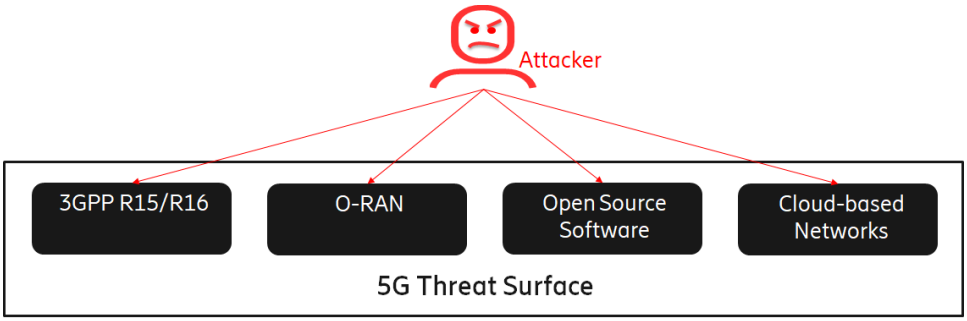


Figure 8: 5G threat surface as defined by Ericsson

4.4.4.1 3GPP security considerations

3GPP releases 15 and 16 standardize 5G and include security improvements over 4G to ensure confidentiality, integrity, and availability (C, I, A) of the networks, devices, and data-in-transit. 3GPP Release 15 introduces security improvements for subscriber authentication, subscriber privacy, secure session-based architecture and interconnects, integrity protection on the user plane, protection

of the transport interfaces between the RAN and 5G Core (5GC), and end-to-end Network Slicing.

Improved subscriber authentication includes more secure mutual authentication using 5G-AKA, EAP-AKA, and EAP-TLS, Home Control of authentication for roaming devices, and non-SIM card based authentication, which is useful for IoT devices. Improved subscriber privacy includes the use of the SUPI/SUCI for encrypted long-term subscriber identifiers and stronger False Base Station (FBS) protection. SBA security is provided with TLS and OAuth 2.0 on all mandatory functions.

Interconnect security between operators is provided at the application layer with the introduction of the (SEPP). Support for user plane integrity protection is mandatory on the UE and gNB and IPSec support is mandatory on the gNB.

End-to-end Network Slicing, including RAN Slicing and Transport Slicing, provides inherent security through traffic separation and 3GPP Release 16 adds Network Slice Specific Authentication and Authorization (NSSAA) for separate authentication and authorization per network slice.

4.4.4.2 O-RAN security considerations

The O-RAN Alliance is standardizing an Open RAN architecture built upon 3GPP standards, as shown in the figure below. This Open RAN Architecture introduces new security risks with an expanded attack surface, vulnerabilities in the Near-RT RIC (Near Real-Time RAN Intelligent Controller) and xApps that could be exploited, and non-secure management interfaces that do not follow industry best practices for attacks on C, I, and A.

The O-RAN architecture adds new functions: SMO, Near-RT RIC, and Non-RT-RIC. The O-RAN architecture adds new interfaces: A1, E2, O1, O2, and Open Fronthaul, which is used for the architectural modification called the Lower Layer Split (LLS) 7-2x. The Fronthaul interface includes the M-Plane for management and the CUS-Plane for control, user traffic, and synchronization. The M-Plane should be secured with certificate-based mutual authentication using TLS, X.509, and PKI. Currently the M-Plane used SSHv2 with password-based authentication. Open Fronthaul control plane messages should be protected to prevent man-in-the-middle-attacks for sniffing and spoofing. Currently the Open Fronthaul control messages are in the clear and unauthenticated.

The Near-RT RIC, and its xApps, can configure direct and indirect conflicts of parameters at the gNB that cause degradation in service or denial service for an attack on availability. This attack vector is exacerbated with third-party xApps from multiple vendors setting the same parameters at the gNodeB. xApps have access to sensitive personal identifiable information such as device-id and device location. It is possible for malicious attacker to gain access to the xApps to track a user or an authorized user to exploit the sensitive information.

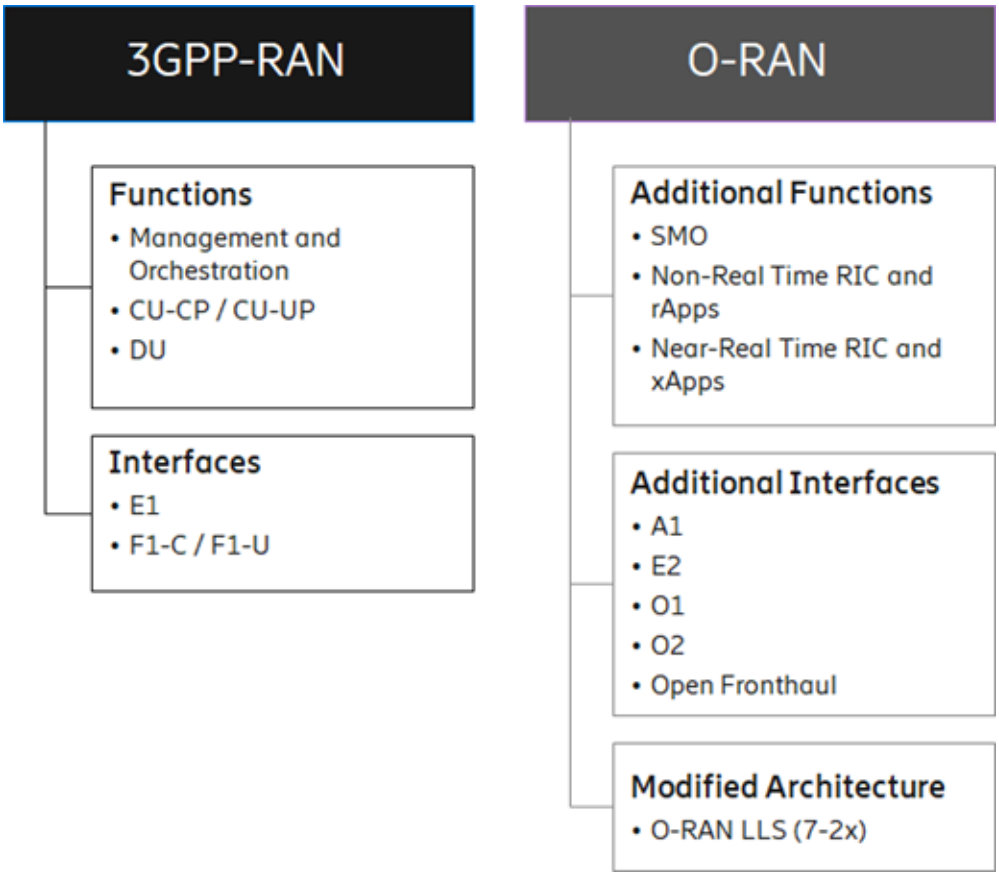


Figure 9: 3GPP and O-RAN functions and interfaces (source: Ericsson)

4.4.4.3 Open source software security considerations

Use of open source software (OSS) presents increased risks that require a higher level of due diligence. OSS is a powerful tool that can be used by organizations to accelerate innovation while reducing the development timeline, product time to market, and overall cost. OSS provides a platform for talented coders to openly collaborate and build software. The transparency of code reviewed by many expert eyeballs can reduce software complexity and the number of bugs. Open source works optimally when developers behave as "good citizens". It has been challenging for OSS to reach the level of security often required. OSS has many attack vectors, including intentional backdoors made by malicious developers, propagation of vulnerabilities through reuse, exploitation of publicly disclosed vulnerabilities, and human error.

It only takes a single third-party component from an upstream developer to unintentionally or maliciously slip in a vulnerability that has a cascade effect, introducing vulnerabilities that propagate and persist throughout the ecosystem, potentially for years. Use of OSS requires a higher level of due diligence which organizations can implement by applying industry best practices for supply chain security, secure software development, and secure software maintenance. When security is properly addressed, OSS can be an important contributor to the development of virtual, cloud-native 5G RAN, including O-RAN and Core functions.

Ericsson, as a regular contributor to the various OSS initiatives and projects, has a vast experience in developing open source platforms by securely integrating open source software into our products and solutions.

4.4.4.4 Cloud security considerations

Network security is built upon a trust stack of trusted hardware, trusted software, trusted deployment, trusted applications, and trusted operations. Cloud deployments have an expanded threat surface due to the decoupling of the software from the hardware, multiple organizations sharing the same hardware, a third-party organization managing the cloud infrastructure, and use of open source software components. The chain of trust between these disparate components is not standardized and is implementation dependent, making it challenging to determine the level of risk, such as defined by the NIST Risk Management Framework (RMF).

In a cloud environment an external attacker could gain access to a compromised container and from there gain access to services and infrastructure. Likewise, an attacker that gains access to a service can use it as platform to gain access to containers and infrastructure. 3GPP is in the process of developing cloud security standards. The NTIA 5G Challenge could be an opportunity to evaluate cloud security to provide input to the relevant standards bodies.

4.5 Timeframe & Infrastructure

Ericsson's solution to the proposed "Challenge" (i.e., the 'Open Ecosystem Plugfest' detailed in Section 4.3) has been described in Section 4.4. The timeframe for the readiness and availability of specific solution components may vary based on use cases and deployment scenarios which will define the scope of the final proposal.

Ericsson welcomes future discussions with the NTIA to work out the detailed timelines for participating in the open 5G stack "Challenge".

5 Conclusion

Ericsson is committed to DoD's aspiration of accelerating the open 5G stack ecosystem by promoting cooperation, collaboration, and interoperability across the industry. Our proposed 'Open Ecosystem Plugfest' – owned and managed by the DoD – where all vendors can bring their components of the open 5G stack to demonstrate functionality and interoperability is an effective "Challenge" to enhance the current open ecosystem. Finally, Ericsson's portfolio of open components – i.e., Cloud RAN, Cloud Native 5GC (5G Core), Service Management and Orchestration, and open cloud infrastructure – further demonstrates our commitment and continued leadership in the open 5G stack.

We are looking forward to subsequent engagement with the NTIA and other stakeholders to contribute and collaborate in the open 5G stack "Challenge".

Sincerely,

Patrik Ringqvist

Principal Solutions Consultant
Market Area North America
ERICSSON
6300 Legacy Dr.
Bldg. WildFlower
Plano, TX 75024
Telephone: (214) 228-1880 (M)

February 10, 2021