Evolving to a strong Cloud RAN security posture

ericsson.com
/en/ran/cloud

Minimizing threats to 5G Cloud RAN critical infrastructure

Abstract
5G deployments in the cloud bring the promise of greater efficiency, agility, and flexibility, however, the cloud expands the 5G attack surface and introduces new threats to critical infrastructure. Mobile network operators (MNOs) are accountable for the security posture of their cloud deployments. A strong Cloud Radio Access Network (RAN) security posture requires a defense-in-depth approach, with the goal of achieving secure critical infrastructure built upon the US National Institute of Standards and Technology's (NIST) zero-trust architecture (ZTA) to protect from internal and external threats. The Cloud RAN deployment model influences the risk assessment, and the responsibilities of stakeholders implementing each security control, including vendors, MNOs, and cloud service providers implementing each security control.

This paper builds upon the analysis from Ericsson's summer 2021 paper, "How to enable security in Cloud RAN", by considering new threat analysis from the US Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), the European Union Network and Information Security Agency's (ENISA) Network and Information Systems (NIS) Cooperative, and others, to provide recommendations for securing Cloud RAN deployments. It also provides an overview of the Ericsson Cloud RAN security posture, explaining the product security and features that enhance the overall security posture of the cloud deployment.

Introduction

Ericsson Cloud RAN will enable MNOs to evolve seamlessly toward cloud-native technologies and open-network architectures, with the goal that MNOs can deploy secure cloud-native networks anywhere, on any cloud and server platform.[1]

The Cloud RAN solution has built-in measures that provide a strong security posture, as provided by Ericsson's purpose-built RAN and Transport portfolios. This is important, since Cloud RAN and traditional RAN may be deployed in parallel by MNOs in so-called bluefield deployments.[2] The goal for securing RAN, whether Cloud RAN or purpose-built RAN, is to protect the availability and high performance of the network and communication services while also ensuring confidentiality, integrity and availability. Achieving these goals in Cloud RAN requires a defense-in-depth approach, in which security is enforced for all network communications and in each layer of the cloud stack, along with dependencies between cloud layers. The Cloud RAN security solution is built upon a ZTA to enable MNOs to mitigate external and internal threats. In addition, Cloud RAN applications will support security automation and intelligence through the Ericsson Security Manager (ESM) and the Ericsson Intelligent Automation Platform (EIAP), a service management and orchestration platform that can host security-specific rApps.

An overview of Open RAN

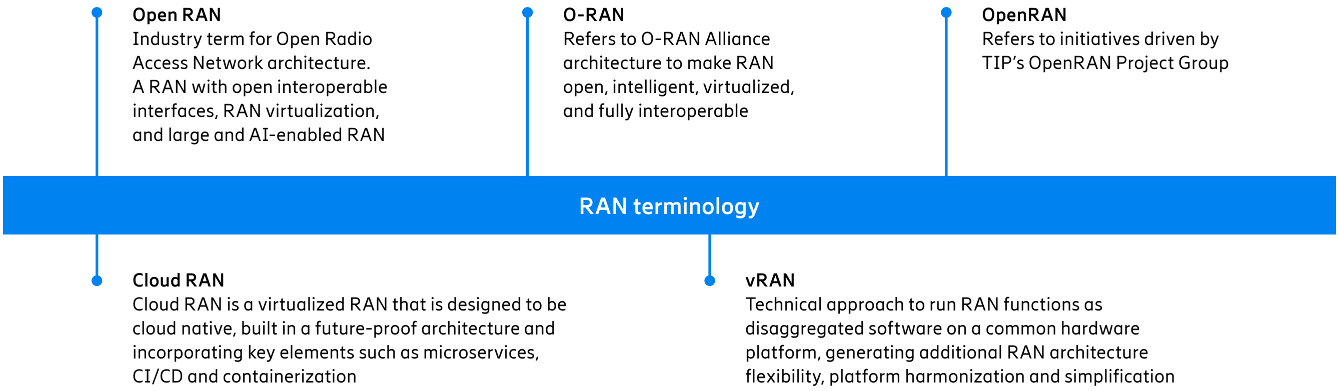
Open RAN, including Cloud RAN[3] and O-RAN,[4] has open and interoperable interfaces built upon 3rd Generation Partnership Project (3GPP) standards, enabling RAN intelligence through artificial intelligence/machine learning. Cloud RAN uses the 3GPP Release 15 (R15) higher layer split (HLS) with the RAN compute disaggregated into a central unit (CU) and distributed unit (DU), with open management and automation interfaces, and a non-real-time RAN intelligent controller (non-RT-RIC) that includes rApps.[5] O-RAN, as specified by the O-RAN Alliance, modifies the 3GPP RAN architecture with the addition of the lower layer split (LLS) and near-real-time-RAN intelligent controllers (Near-RT-RICs). These Open RAN terms are explained further in Figure 1. The benefits of Open RAN for the MNO are that it enables new deployments and capabilities, including:

- utilizing the same hardware for different applications
- high reliability and flexible scaling of compute resources provided by the cloud infrastructure
- improved network automation capabilities and optimized performance with the Non-RT RIC
- deployment of RAN equipment from different vendors in the same geographical area

Open RAN also provides benefits with regards to enhanced security, including:[6]

- use of open-source software enabling transparency and common control
- open interfaces ensuring transparency and use of standard, interoperable, and secure protocols
- disaggregation, enabling supply chain resilience through vendor diversity
- use of AI/ML enabling visibility and intelligence to achieve greater security

Figure 1: Open RAN Technologies



Open RAN
Industry term for Open Radio Access Network architecture. A RAN with open interoperable interfaces, RAN virtualization, and large and AI-enabled RAN

O-RAN
Refers to O-RAN Alliance architecture to make RAN open, intelligent, virtualized, and fully interoperable

OpenRAN
Refers to initiatives driven by TIP's OpenRAN Project Group

RAN terminology

Cloud RAN
Cloud RAN is a virtualized RAN that is designed to be cloud native, built in a future-proof architecture and incorporating key elements such as microservices, CI/CD and containerization

vRAN
Technical approach to run RAN functions as disaggregated software on a common hardware platform, generating additional RAN architecture flexibility, platform harmonization and simplification

[1] Cloud RAN - 5G RAN - Virtually everywhere – Ericsson
[2] Bluefield deployments in telecommunications – Ericsson
[3] Ericsson Cloud RAN | Networks | Main Catalog | Ericsson
[4] www.o-ran.org/
[5] "Intelligent security: How the SMO can enhance the security posture of Open RAN", Ericsson, June 2022
[6] O-RAN Alliance, Technical Paper, June 2021

Accountability for securing Open RAN

The key stakeholders in cloud deployments are the cloud service provider and its customer – the cloud consumer.

The MNO, as the cloud consumer, deploys 5G critical infrastructure in hybrid and public clouds. The MNO may also choose to deploy a private cloud to achieve the highest level of security gained from asset ownership, deployment control, and network visibility. The Cloud Shared Responsibility Model (CSRM) is a helpful cloud industry tool to determine which stakeholder has security responsibility at each layer of the cloud stack. Figure 2 shows the Ericsson version of the CSRM and similar versions from Microsoft Azure,[7] AWS[8] and GCP[9] are publicly available. The CSRM can be summarized by the following cloud industry phrase: "The cloud service provider is responsible for security of the cloud and the cloud consumer is responsible for security in the cloud". While the cloud service provider may be delegated responsibility by the MNO, it is the MNO who is accountable for the security posture of the 5G RAN and core deployment, as reported in US DHS CISA's "Security Guidance for 5G Cloud Infrastructures".[10]

The assignment of responsibility is further complicated in hybrid cloud environments. This is because the hybrid cloud may be a mix of private cloud and public cloud, a private cloud within a cloud service provider's public cloud infrastructure, or the cloud service provider infrastructure deployed on-premise of the MNO.

The Cloud Security Alliance (CSA) has identified the additional security risks with hybrid clouds and has formed the CSA Hybrid Cloud Security Working Group.[11] Security responsibilities must be clearly defined and specified in the cloud service agreement. The MNO is always responsible for protecting sensitive data and properly configuring security tools, network functions, interfaces and APIs. This Ericsson paper[12] provides considerations and recommendations for MNOs to securely deploy in hybrid and public clouds.

Figure 2: Cloud Shared Responsibility Model

Security within service delivery models

	Infrastructure as a service (IaaS)	Platform as a service (PaaS)	Software as a service (SaaS)
Human access	Cloud consumer	Cloud consumer	Cloud consumer
Data	Cloud consumer	Cloud consumer	Cloud consumer
Application	Cloud consumer	Cloud consumer	Cloud service provider
Operating system	Cloud consumer	Cloud service provider	Cloud service provider
Virtual networks	Cloud consumer	Cloud service provider	Cloud service provider
Hypervisors	Cloud service provider	Cloud service provider	Cloud service provider
Server and storage	Cloud service provider	Cloud service provider	Cloud service provider
Physical networks	Cloud service provider	Cloud service provider	Cloud service provider

[7] Shared responsibility in the cloud, October 2022
[8] AWS, Shared Responsibility Model
[9] Google Cloud Platform: Shared Responsibility Matrix, April 2019
[10] Security Guidance for 5G Cloud Infrastructures, US DHS CISA, October 2021
[11] Cloud Security Alliance, Hybrid Cloud Security, May 2021
[12] 5G security for public and hybrid clou deployments, S. Poretsky, H. Akhtar, and P. Linder, Ericsson, September 2022

Traditionally, RANs have been considered secure because the operator deploys their hardware at their facility and on their network, which they manage. This enabled MNOs to protect their RAN with perimeter security, as the greatest risks from threats were external to the network. Open RAN enables RAN migration to hybrid and public clouds where RAN will be running on third-party hardware, at a third-party facility, on a third-party network and managed by that third party. A foundation of trust must be established with secure storage of credentials, to build a trust chain up the layers of the cloud stack to the application and across interworking network functions.

The cloud has an increased risk of internal threats from insiders, lateral movements, multiple tenants, and shared resources. An advanced persistent threat (APT) is a sophisticated, sustained cyberattack in which an external actor, typically a nation-state, establishes an undetected presence inside a network to steal sensitive data over a prolonged dwell time. Threats to Open RAN deployments in hybrid and public clouds must be assessed to ensure 5G critical infrastructure in the cloud is secure from internal and external threats. This is a new paradigm for securing the RAN and it requires a new risk analysis with the pursuit of a ZTA. As US DHS CISA advises for 5G-critical infrastructure deployments in the cloud – "Assume the adversary is already inside the network".[13]

[13] Security Guidance for 5G Cloud Infrastructures, US DHS CISA, October 2021

Cloud RAN Deployment models

Legacy baseband implemented as a purpose-built RAN provides layers 1 through 3 of the radio protocol stack.

The evolution of RAN to disaggregated, virtualized, cloud-native functions has enabled Open RAN to be deployed in private-, public-, and hybrid-cloud environments. These comprise:

- Layer 1, which includes Radio Frequency (RF) and physical layer (PHY).
- Layer 2, which includes Medium Access Control (MAC), Radio Link Control (RLC), and Packet Data Convergence Protocol (PDCP).
- Layer 3, which includes Service Data Adaptation Protocol (SDAP) and Radio Resource Control (RRC).

Open RAN, including Ericsson Cloud RAN, is based upon the virtualization and cloudification of RAN baseband functions. These functions evolved from purpose-built hardware deployed at cell sites to disaggregated functions that can be implemented in software to operate on commercial off-the-shelf server hardware, enabling RAN deployments at edge sites or central sites. 3GPP R15 HLS disaggregates baseband functions into the virtualized CU, with layer 2 PDCP and layer 3 protocols deployed in central locations, and virtualized DU with layer 1 and layer 2 MAC and RLC protocols deployed at the cell site. LLS provides further disaggregation as the DU is split into a DU and radio unit (RU). In the LLS configuration, the O-DU supports layer 2 MAC and RLC protocols and layer 1 PHY-high RAN functions including scrambling, modulation and precoding. The RU supports layer 1 PHY-low functions, including beamforming and RF.

Multi-access edge computing (MEC) provides computing and storage resources for networking functions and applications running on top of cloud infrastructure. Hybrid cloud facilitates MEC deployments of Cloud RAN with near-edge sites, locating the virtualized CU closer to the centralized hub data center and far-edge sites, locating the virtualized DU closer to the radio sites. Service management and orchestration (SMO) is deployed at a data center to provide visibility and intelligence for orchestration and automated policy control of RAN functions. The cloud service provider's infrastructure may be deployed on-site at the premisesof the MNO. Alternatively, the MNO may deploy its workloads on cloud infrastructure at the cloud service provider's data center and near-edge and far-edge data centers closer to the cell site, in various deployment options, as shown in Figure 3, and discussed further in a separate Ericsson paper.[14] The deployment of private networks for industrial use cases, another category in which Cloud RAN can be attractive, will be covered in a future paper.

Figure 3: RAN deployment configurations

	Cell site	Far-edge	Near-edge	Data center
Purpose-built RAN Cloud RAN option 1	Basedband RU, vDU, vCU			RAN management
3GPP R15 HLS Cloud RAN option 2	RU, vDU		vCU	RAN management
Cloud RAN option 3	RU	vDU vCU		SMO
Cloud RAN option 4	RU	vDU	vCU	SMO

[14] What's next for RAN, Ericsson, 2022

Cloud threats to Open RAN

As 5G Core and Open RAN migrate to the cloud, it is important to consider cloud threats when performing a risk analysis, particularly for the deployment of critical infrastructure in the cloud.

Open RAN has an expanded attack surface due to its additional functions, interfaces, and cloud deployment models.[15,16,17,18,19,20] Open RAN deployments in public and hybrid clouds also have an expanded threat surface due to increased risk from internal threats and APTs, as shown in Figure 4. ENISA's NIS Cooperative Report on Open RAN Cybersecurity[21] identified 5G Core and Open RAN as having increased risk of internal threats in the cloud due to:

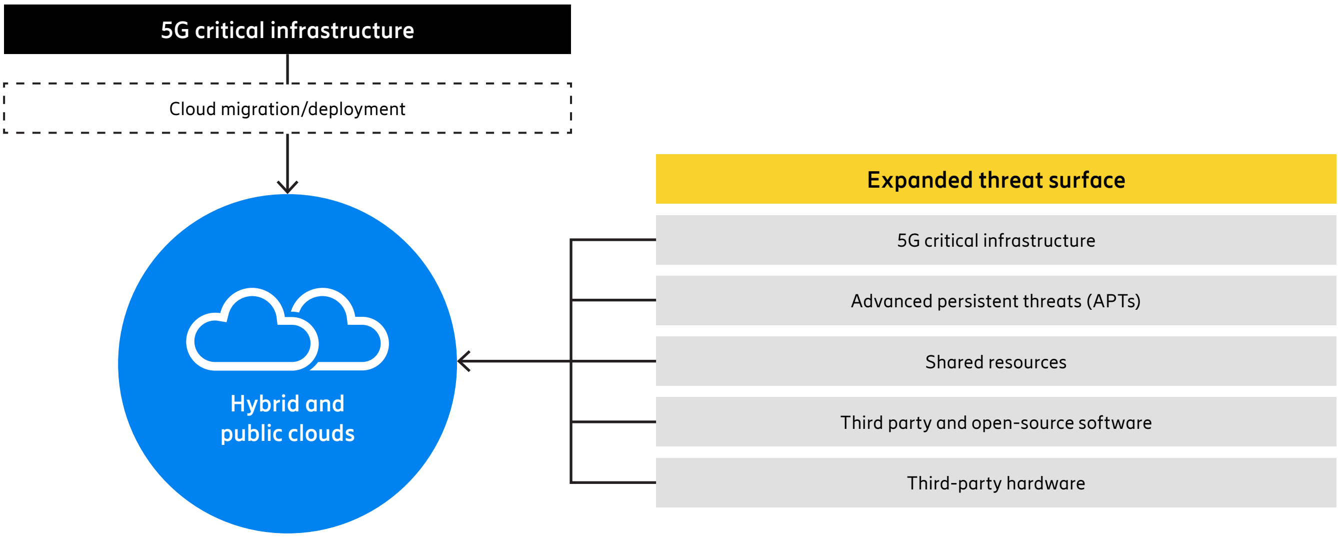
- greater dependency on cloud service providers
- lack of defined security roles across stakeholders
- resource sharing with other tenants
- broader use of open-source software
- use of insecure third-party hardware

Deployment in an MNO's on-premise private cloud can reduce risks from these threats.

The German Federal Office of Information Security (BSI) Open RAN Risk Analysis[22] identified high risks in O-RAN deployments due to optional use of critical security controls, specification of weak protocols and cipher suites, assumptions of internal trust, missing protections from denial of service attacks, and lack of cloud security controls for O-Cloud.

Karsten Nohl, an industry-recognized ethical attacker, demonstrated in his recent video[23] at the MCH Hackers Conference that exploits can be performed on an Open RAN system running in a cloud-native environment without properly secured configuration of the operating system, container run-time, and orchestration. The O-RAN Alliance's Working Group 11 (WG11) is evolving security specifications to address these risks[24] with Ericsson as a leading contributor.[25]

Figure 4: Expanded threat surface for 5G cloud deployments


5G critical infrastructure
Cloud migration/deployment
Hybrid and public clouds
Expanded threat surface
5G critical infrastructure
Advanced persistent threats (APTs)
Shared resources
Third party and open-source software
Third-party hardware

[15] Security Considerations of Open RAN, S. Poretsky and J. Boswell, Ericsson, August 2020
[16] Security Considerations of Cloud RAN, S. Poretsky and J. Jardal, Ericsson, September 2021
[17] O-RAN Alliance, June 2021
[18] Open RAN Risk Analysis, Germany BSI, Federal office of Information Security, English Translation, February 2022
[19] Report on Open RAN Cybersecurity, ENISA NIS Cooperative Group, May 2022
[20] Establishing a Strong Security Posture for Open RAN, Scott Poretsky, SCTE Cable-Tec Expo 2022, September 2022
[21] Report on Open RAN Cybersecurity, ENISA NIS Cooperative Group, May 2022
[22] Open RAN Risk Analysis, German Federal office of Information Security (BSI), November 2021. English version available February 2022
[23] "OpenRAN – 5G hacking just got a lot more interesting", Karsten Nohl, MCH (May Contain Hackers), July 2022
[24] O-RAN Alliance WG11, October 2022
[25] Ericsson – a leader in the O-RAN Alliance, Ericsson, September 2022

The importance of multi-layer security

Each layer of the cloud stack must be protected from external and internal threat actors who could exploit vulnerabilities.

The data, containers and applications, container run-time engine and orchestration, host operating system, and infrastructure layers share common vulnerabilities. Insecure APIs, weak encryption, security misconfigurations and exposed credentials may compromise confidentiality, integrity and availability of data and network functions. The software layers above the infrastructure can use open-source software with persistent vulnerabilities inherited from other projects. In a multi-tenant environment, there are known attacks such as container escape, host escape, and shared resource exhaustion, in addition to the risk of data exposure and data leakage to other tenants. Sensitive data with weak encryption can be exposed through unauthorized access to data-at-rest and man-in-the-middle (MitM) attacks on data-in-transit.

It is important that a higher level of security baseline is applied to operate 5G-critical infrastructure in the cloud. When selecting security controls using a risk-based analysis, it is essential to consider both external and internal threats. External threats to the cloud can be mitigated by using traditional perimeter-based security controls such as firewalls, web application firewalls (WAF), and by identity and access management (IAM) at the lower layers of the cloud stack. Internal threats to the cloud can be mitigated through a ZTA approach at the higher layers of the cloud stack with three main characteristics:

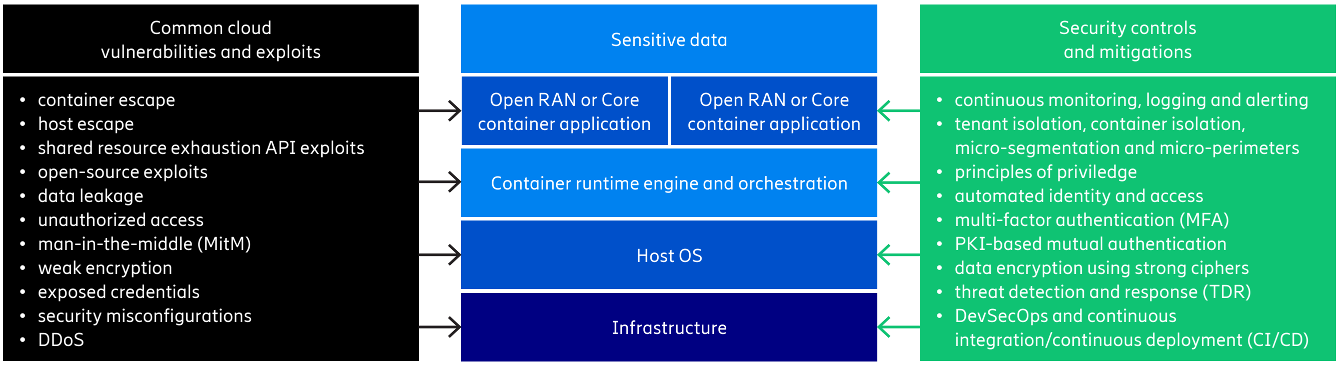
1. The protect surface is perimeter-less or narrowed to micro-perimeters, rather than relying upon traditional perimeter defenses that protect against only external threats.[26]
2. There is no implicit trust granted to an asset based upon ownership, physical location, or network location.[27]
3. The risk analysis assumes the adversary is already inside the network.[28]

An effective ZTA builds upon continuous monitoring, logging and alerting at all layers of the cloud stack. A network designed for a ZTA has micro-segmentation to separate traffic, micro-perimeters to have granular access based upon the principle of least privilege, container isolation to isolate attacks, and tenant isolation. Each layer of the cloud stack, as shown in Figure 5, should have secure access. Sensitive data at-rest and in-motion should be encrypted using strong cipher suites. Implementation of these security controls for a ZTA aligns with guidance from the US DHS CISA's "Security Guidance for 5G Cloud infrastructures",[29] which is built upon the following four pillars:

1. Prevent and detect lateral movement
2. Securely isolate network resources
3. Protect data-in-transit, in-use and at-rest
4. Ensure integrity of infrastructure

A secure 5G cloud deployment is built upon a foundation of secure software development processes. Development security and operations (DevSecOps) and continuous integration/continuous deployment (CI/CD) provide built-in security and rapid security updates. Industry best practices for cyber hygiene, such as security configuration validation and software updates for critical vulnerabilities, should be components of a strong security posture in the cloud. This approach helps to ensure that 5G cloud deployments meet the level of security expected for critical infrastructure. In addition, deployments should follow CIS Benchmarks for securing Kubernetes, Docker and Linux.[30]

Figure 5: Multi-layer cloud security


Common cloud vulnerabilities and exploits
• container escape
• host escape
• shared resource exhaustion API exploits
• open-source exploits
• data leakage
• unauthorized access
• man-in-the-middle (MitM)
• weak encryption
• exposed credentials
• security misconfigurations
• DDoS
Sensitive data
Open RAN or Core container application
Open RAN or Core container application
Container runtime engine and orchestration
Host OS
Infrastructure
Security controls and mitigations
• continuous monitoring, logging and alerting
• tenant isolation, container isolation, micro-segmentation and micro-perimeters
• principles of priviledge
• automated identity and access
• multi-factor authentication (MFA)
• PKI-based mutual authentication
• data encryption using strong ciphers
• threat detection and response (TDR)
• DevSecOps and continuous integration/continuous deployment (CI/CD)

[26, 27] NIST SP 800-207 Zero Trust Architecture (ZTA), US DoC NIST, September 2020

[28] Security Guidance for 5G Cloud Infrastructures, US DHS CISA, October 2021

[29] Security Gzuidance for 5G Cloud Infrastructures, Parts 1-4, US DHS CISA.

[30] CIS Kubernetes Benchmark, CIS Linux Benchmark, CIS Docker Benchmark

The benefits of Ericsson Cloud RAN Security

Ericsson's Cloud RAN solution is designed to be deployable on any cloud platform and will support 3GPP standard interfaces and O-RAN automation interfaces.

Cloud RAN will enable automation and intelligence together with the Ericsson SMO called the Ericsson Intelligent Automation Platform. Along with the Ericsson Security Manager, protect and detect security use cases can be enabled. Ericsson is working with ecosystem partners, including industry-leading IT infrastructure vendors, to enable secure cloudification.

This section describes the Ericsson Cloud RAN approach to security and how it enables MNOs to realize a ZTA that mitigates the new threats in cloud deployments. Achieving a strong network security posture requires security functions and a secure development process. As a starting point, Ericsson has been building the Cloud RAN security solution and security assurance processes, based on experiences from purpose-built RAN deployments of scale, applying DevSecOps best practices.

Establishing trust in 5G cloud deployments

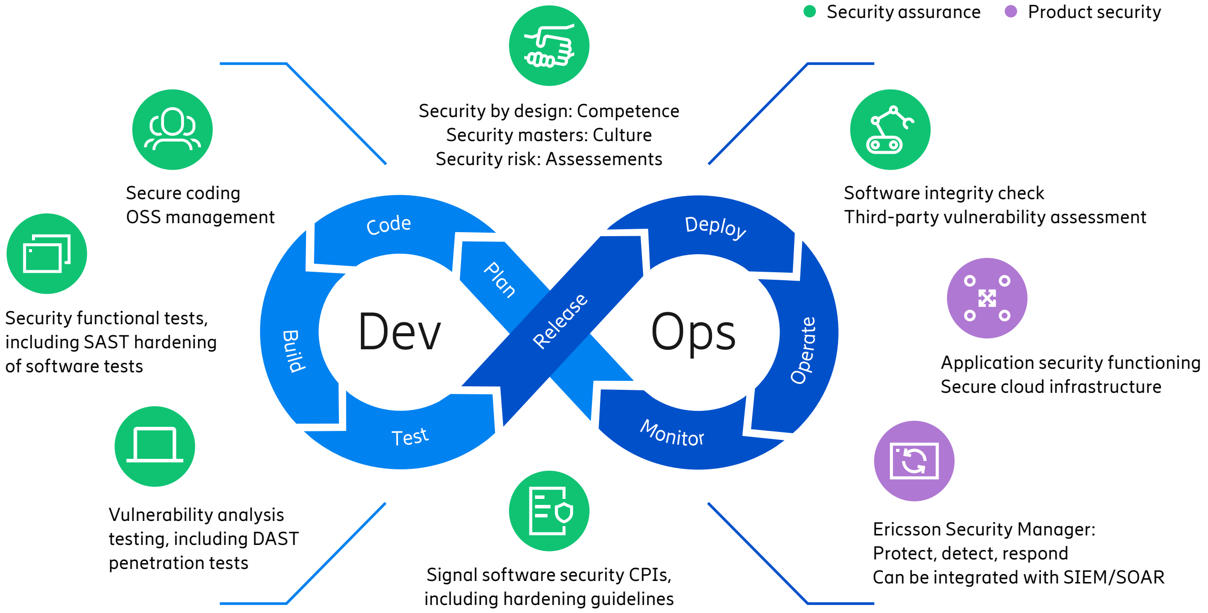
The zero trust principles described previously imply that validation needs to be undertaken before an entity, both human and virtual network function, can be trusted.

A 5G cloud deployment introduces more stakeholders and administrators, including third parties, that are involved in managing infrastructure, which increases the risks from malicious insiders, creating the need for a ZTA. A network built with a ZTA includes micro-perimeters with strong authentication and authorization to enforce trusted access network entities and data.

In Cloud RAN, the node management interface is protected to prevent data from being viewed, modified, or deleted by unauthorized third parties. The protection is ensured with functions such as MFA and role-based access control, enforcing the "least privilege" principle. Strong authentication and authorization are enforced using certificates. This applies to both human users accessing management interfaces, and automated machine-to-machine communications between network elements, such as communication through the F1 interface between the CU and DU.

Trust also needs to be established between the different layers in the cloud stack, as previously shown in Figure 5. In the cloud, hardware and software can be sourced from different vendors, creating the need to establish a trust chain anchored on a root of trust (RoT). This is different from purpose-built RAN where dedicated Ericsson hardware is used as RoT. The trust chain is built in the cloud stack and between network functions using certificate-based

Figure 6: Ericsson DevSecOps practices for a strong security posture


● Security assurance
● Product security
Security by design: Competence
Security masters: Culture
Security risk: Assessments
Secure coding
OSS management
Security functional tests, including SAST hardening of software tests
Vulnerability analysis testing, including DAST penetration tests
Signal software security CPIs, including hardening guidelines
Software integrity check
Third-party vulnerability assessment
Application security functioning
Secure cloud infrastructure
Ericsson Security Manager: Protect, detect, respond
Can be integrated with SIEM/SOAR
Dev
Ops
Code
Build
Test
Plan
Release
Deploy
Operate
Monitor

authentication. For Cloud RAN, the trust chain relies on a secure cloud infrastructure that utilizes secure boot operations and secure instantiation of cloud-native functions (CNFs) that have validated digital signatures.

Ericsson Cloud RAN software is signed digitally in the Ericsson CI/CD flow according to ETSI SOL 004 after passing quality checkpoints, as described in Figure 6, such as open source SW scans, static application security testing (SAST), dynamic security testing (DAST). It can be validated during on-boarding and at the instantiation by a trust-anchor file from Ericsson, containing the signing root certificate that has been pre-loaded in the infrastructure. This ensures that the software originates from Ericsson and is not manipulated or changed.

Data protection in the cloud

The assumption that an attacker is already inside the network implies that data in transit needs to be protected on all interfaces and data-at-rest needs to be protected in storage on all network functions.

The foundation of Cloud RAN security is provided by 3GPP security specifications. External interfaces between the network elements, such as CU and DU, use 3GPP-required security protocols for encryption and integrity protection with strong cipher suites.[31] Cloud RAN will also provide protection between the interfaces inside the application, with encryption and integrity protection of the communication between pods. The pod, which is the smallest execution unit in Kubernetes, is the smallest trust zone, establishing the ZTA micro perimeter. The Cloud RAN application has built-in automated internal certificates and key management to support the protection of the pods anchored on an RoT.

Cloud RAN will support the following security protocols for confidentiality and integrity protection of data in transit on external and internal interfaces:

- Control plane (F1, E1, N2): DTLS v1.2
- User plane (N3, F1, Xn): IPsec
- Air interface (CU to UE): PDCP, RRC, 802.1x authentication
- O&M interfaces CM/PM/FM/file transfer: TLS v1.3, FTPES, LDAPS, SNMPv3
- Internal interfaces inside application (pod-pod): TLS v1.3 using built-in certificates and key vault

Applications store data, such as keys, credentials and configuration files in the infrastructure's run-time persistent volume. Kubernetes supports encryption at rest for this data, but the encryption key requires protection from malicious insiders. It is recommended for the MNO to use a Bring Your Own Key (BYOK) approach to improve key management and control to maintain provenance and assurance.[32]

Cloud RAN offers the possibility to keep this encryption key to the storage service inside the application's built-in key vault. The Cloud RAN CNF can be integrated with a centralized key management service (KMS) from the infrastructure to manage encryption keys. The centralized KMS enables use of an external hardware security module to provide additional protection for cryptographic keys and operations. Backup and restore functionality ensure that it is possible to restore the running Cloud RAN application to the previous state by creating a protected backup file containing keys and configuration data. Access control and monitoring of data access and usage are other essential functions for protecting data that needs to be configured in the cloud platform.

Ensuring high availability on a shared platform

Even though a cluster is completely disconnected from the internet, it may share the underlying cloud infrastructure with other tenants.

Shared resources introduce new attack vectors in 5G cloud deployments. To mitigate these risks, micro-segmentation techniques should be configured to provide isolation between the host and Cloud RAN network functions, and between network functions to prevent one compromised container from impacting other containers running on the shared platform. Micro-segmentation implies security controls and policies are implemented to logically divide the deployment into distinct security segments down to the individual workload level. Cloud RAN applications provide separation between different traffic types (control/user/management plane) as well as separation of fronthaul, midhaul, and backhaul interfaces. Having several isolation layers adds protection and provides security in depth.

To better withstand overload and potential overload attacks, such as distributed denial of service attacks, Cloud RAN products can be deployed with high availability and redundancy. Redundant instances can be deployed in the same data center or the second instance may be deployed in a geographically separate data center, ready to take over, minimizing the impact on availability whether a single instance or an entire data center goes down. Given that security functions are in place, another key to secure deployments is for the MNO to use and maintain a consistent and secure configuration. Ericsson Cloud RAN pods are delivered with a secure-by-default configuration and tested on a hardened infrastructure. An example of pod hardening is to have maximum limits defined for CPU and RAM to avoid starvation of other pods in the same cluster and to ensure that no keys or secrets are part of the pod/container images. The Cloud RAN software is verified with SELinux and comes with default settings for pod security, name spaces, and network policies. Ericsson recommends hardening the cloud platform based on the CIS benchmarks.[33]

In the more complex and dynamic cloud deployment, the risk of security misconfiguration increases. This increases the need for automation that ensures both the cloud platform and the telco application follow the intended security baseline and policies. The MNO security operation center (SOC) can use a security information and event manager (SIEM) or security orchestration, automation and response (SOAR) to efficiently collect and analyze log data from their digital assets in one place, in order to ensure compliance with the baseline. The Ericsson Cloud RAN applications will support security automation and intelligence through the ESM and the EIAP, which as a SMO can host security-specific rApps.[34] The ESM and EIAP can interwork with an external SOAR or SIEM in the MNO SOC to also allow visualization of the Cloud RAN data there.

For compliance monitoring,the security baseline automation functionality provides a repeatable process for:

- systematic selection of technical security and privacy policies and controls
- automatic enforcement toward the network context
- continuous compliance monitoring after initialization

[31] 3GPP TS 33.501
[32] Options for Key Management in the Cloud | CSA (cloudsecurityalliance.org)
[33] CIS Kubernetes Benchmark, CIS Linux Benchmark, CIS Docker Benchmark
[34] Why SMO provides an ideal platform for intelligent Open RAN security, S. Poretsky and J. Jardal, Ericsson, June 2022

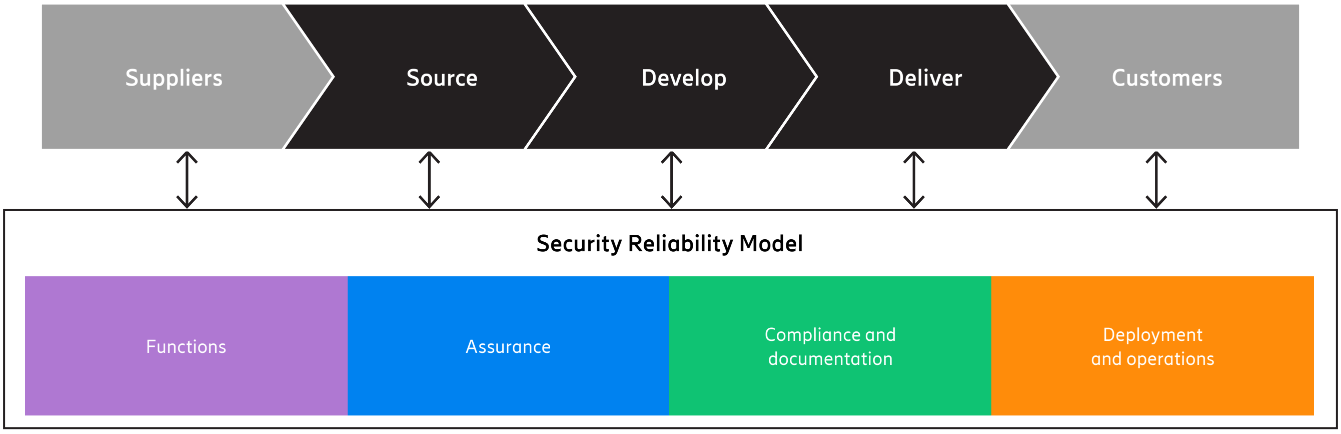
Enabling a secure supply chain

The increased use of open-source software in cloud deployments has many advantages but also requires proper handling to mitigate inherent risks in the supply chain.

Attack vectors may compromise a trusted manufacturer's software, hardware, or established open-source libraries. To prevent supply-chain attacks, Ericsson drives activities across all parts of the CI/CD flow, referred to as "Secure by Design" or DevSecOps, as shown in Figure 6. The security culture among the people at Ericsson is supported by our Security Master Model, which ensures security competence in all teams, from design to deployment and support. Ericsson has created its Security Reliability Model (SRM)[35] to ensure a common approach to product security and privacy cross-company, providing guidance and alignment with external demands.[36]

The SRM framework includes the management of open-source software. It starts with the selection of third-party sub-suppliers and open-source software forums, and stipulates requirements in the sourcing and inbound supply stage to ensure that the third-party products and sources are properly scrutinized before being included in the product. During the R&D product development phase, DevSecOps principles are applied, as described in Figure 6, including activities like source code checks, secure code analytics (SAST, DAST), and penetration tests by an in-house dedicated Ericsson red-team simulating attacks as carried out by hackers. Finally, in the MNO deployment and operation phase, mitigations, or software patches of newly found vulnerabilities existing in deployed software, are managed by a dedicated Ericsson Product Security Incident Response Team (PSIRT).[37] In November 2021, Ericsson Cloud RAN portfolio passed the Network Equipment Security Assurance Scheme (NESAS) certification.[38]

Figure 7. Ericsson Security Reliability Model


Suppliers
Source
Develop
Deliver
Customers
Security Reliability Model
Functions
Assurance
Compliance and documentation
Deployment and operations

[35, 36] The Ericsson Security Reliability Model
[37] Ericsson Product Security Incident Response Team (PSIRT)
[38] Ericsson Cloud RAN passes GSMA's NESAS security audit

Conclusion

Open RAN deployments, including Cloud RAN and O-RAN, in public and hybrid clouds, have an expanded threat surface due to increased risk from internal threats caused by the introduction of third parties in a multi-tenant environment. The CSRM is a helpful tool for stakeholders to determine who has security responsibility at each layer of the cloud stack. Each layerof the cloud stack must be protected from external and internal threat actors, who can exploit common vulnerabilities to compromise confidentiality, integrity and availability of data and networking functions.

The Ericsson Cloud RAN security solution will enable secure Open RAN deployments striving toward ZTA to mitigate external and internal threats. Significant investments across the development organization have been made to achieve strong network security. Ericsson is building Cloud RAN security solution and security assurance processes based on experiences from purpose-built RAN deployments of scale, and collaborating with leading IT infrastructure vendors.

Cloud RAN application software provides functionality to protect data on internal and external interfaces. Support is provided for establishing trust through mutual authentication, automating and securing configurations, and data streaming to enable threat detection and automated configuration compliance. In addition, Ericsson's Cloud RAN offering passed the independent NESAS audit, making it fully compliant with the security requirements defined by global standards organizations 3GPP and GSMA.

About Ericsson

Ericsson enables communications service providers and enterprises to capture the full value of connectivity. The company's portfolio spans the following business areas: Networks, Cloud Software and Services, Enterprise Wireless Solutions, Global Communications Platform, and Technologies and New Businesses. It is designed to help our customers go digital, increase efficiency and find new revenue streams. Ericsson's innovation investments have delivered the benefits of mobility and mobile broadband to billions of people globally. Ericsson stock is listed on Nasdaq Stockholm and on Nasdaq New York.
www.ericsson.com

Ericsson
SE-164 80 Stockholm, Sweden
Telephone +46 10 719 0000
www.ericsson.com

The content of this document is subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document

4/0341-FGB1010990