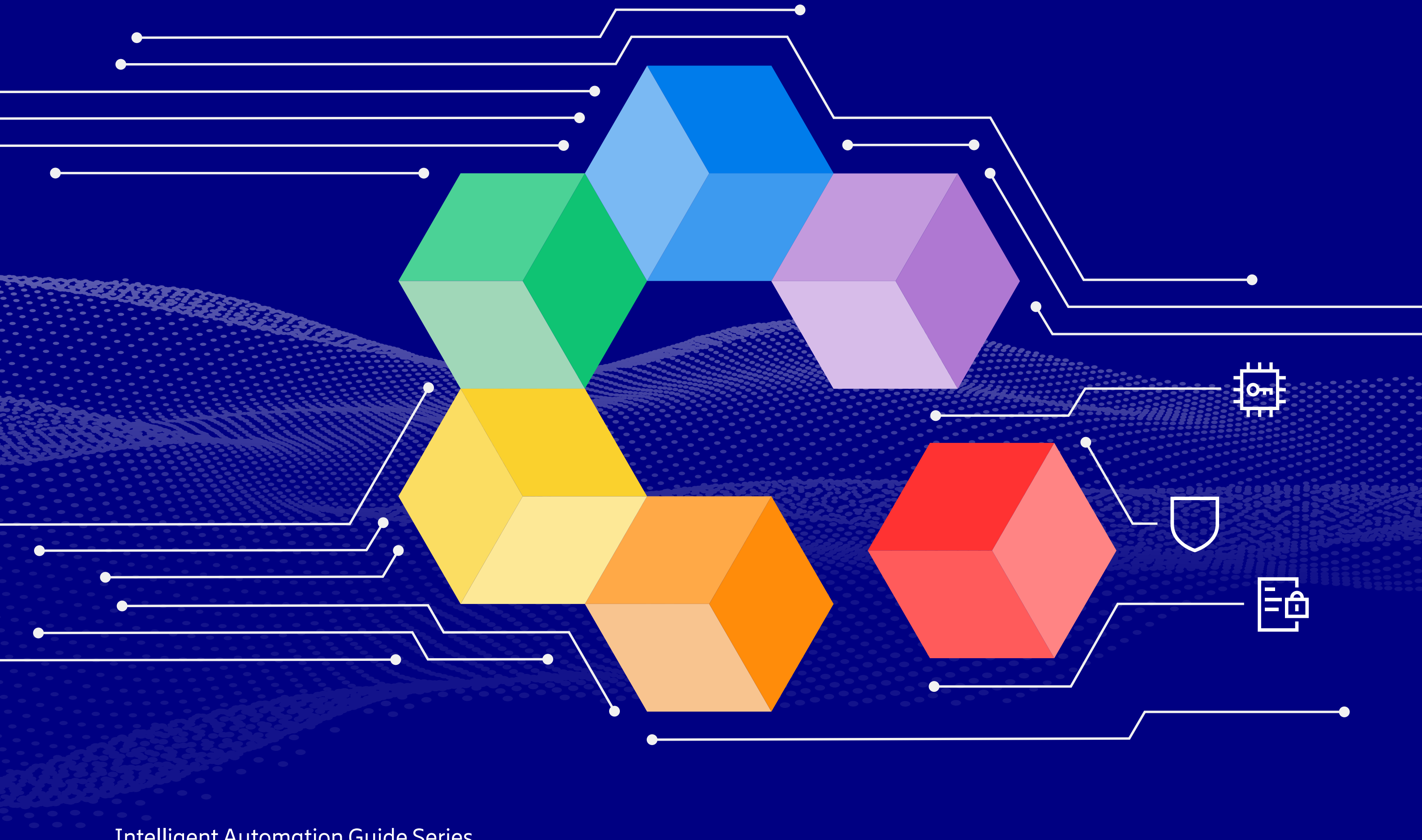
ericsson.com/
intelligent
automation
platform

Intelligent security



Intelligent Automation Guide Series
August 2023

How the SMO can enhance the security posture of Open RAN

Executive summary

As 5G deployments evolve to the cloud for Core and Open Radio Access Network (RAN), new security threats, risks, and controls must be considered. While the cloud introduces security advantages, it expands the 5G attack surface for external and internal threats. The 5G attack surface must be protected through a Zero Trust Architecture (ZTA) approach, built upon a secure-by-specification and design foundation.

The Service Management and Orchestration (SMO) framework supports a ZTA for its external interfaces and internal functions, applications, and interfaces.

The SMO – and rApps integrated within the SMO's Non-Real-Time RAN Intelligent Controller (Non-RT RIC) – can enhance the RAN security posture by implementing security use cases to protect against threats. This includes advanced persistent threats' (APTs) able to exploit Open RAN vulnerabilities through lateral movement and reconnaissance in cloud deployments. While the SMO can enhance RAN security, it must also be properly secured to prevent external and internal threat actors from gaining access and taking control of the RAN. Ericsson is leading within the O-RAN Alliance Security Working Group 11 (WG11) to ensure that the SMO and its SMO functions, Non-RT-RIC, rApps, and R1, A1, SMO internal, and external interfaces will be secure from external and internal threats.

The Ericsson Intelligent Automation Platform (EIAP) is Ericsson's implementation of the SMO components. It provides an open SMO platform that enables mobile network operators (MNOs) to optimize and secure their networks in a ZTA for delivery of enhanced customer experiences.

Introduction

The virtualization and automation of network functions have enabled cloud-based deployments of mobile core and RAN. Open RAN is a transformation of RAN built upon the pillars of automation, intelligence, cloudification, and open, interoperable interfaces providing a multivendor ecosystem. As stated by the US FCC CSRIC Report on Open RAN, "Open RAN is O-RAN, Cloud RAN, vRAN, and other technologies" [1]. For cloud-based deployments of critical infrastructure, a strong security posture based on the goal of a ZTA must be implemented to ensure confidentiality, integrity, availability, and authenticity protection of network functions, interfaces, and data from internal and external threats. As with any critical infrastructure, Open RAN networks need to be secured from external and internal threats with a Zero Trust Architecture (ZTA) [2].

While the cloud provides security advantages, it can introduce new RAN security risks due to the cloud's expanded attack surface. The migration of 5G critical infrastructure to private, hybrid, and public cloud deployments introduces new actors and stakeholders to a shared-responsibility model that further complicates the security posture of the deployment. The MNO, as a cloud consumer, can be accountable for the deployment security posture, which encourages proper due diligence when selecting a cloud service provider partner. However, the MNO can delegate some security responsibilities to the selected cloud service provider(s), as clearly specified in the cloud service agreement. The multiparty relationship between the vendor, MNO, cloud service provider and systems integrator require a clear definition of security roles and responsibilities to protect assets, including network functions, interfaces, and data.

Secure deployment of 5G critical infrastructure in the cloud requires additional considerations. A multi-cloud deployment requires security analysis of the selected cloud service provider to identify security gaps and controls. Changes to risk due to evolving threats, attack vectors and security control technologies must be periodically reassessed by all stakeholders. Information provided by artificial intelligence and machine learning (AI/ML) in Open RANs SMO has the potential to enhance security.

The SMOs Non-RT-RIC, with its rApps, can provide security awareness, threat intelligence and automated responses. However, as the SMO is responsible for all service management and orchestration, its components also introduce security risks. A security vulnerability within the SMO could be exploited by an adversary to serve as an entry point for reconnaissance, attacks against Open RAN components, and lateral movement across the RAN and 5G Core. The SMO must be protected with built-in security controls implemented with a zero-trust mindset, enhancing the Open RAN security posture. This paper outlines the threats to Open RAN deployments inherent in the cloud and recommendations for SMO security controls to achieve a ZTA, enhancing the security posture of the SMO and end-to-end Open RAN deployments.

Cloud threats and mitigations

5G cloudification for Core and RAN is built upon Cloud-native (or Cloudifed) Network Functions, which enable new use cases and business models through automation, elasticity, massive scale and interoperability in the cloud. The cloud increases the Open RAN attack surface due to dependency on cloud service providers, resource sharing with other tenants, security misconfiguration and use of open-source software [3]. 5G cloud deployments should be based upon a ZTA built on a foundation of continuous monitoring and logging following US government guidance that secures 5G cloud deployments with the following capabilities [4]:

- Prevent and detect lateral movement
- Secure isolation of network resources
- Data protection
- Ensure the integrity of cloud infrastructure

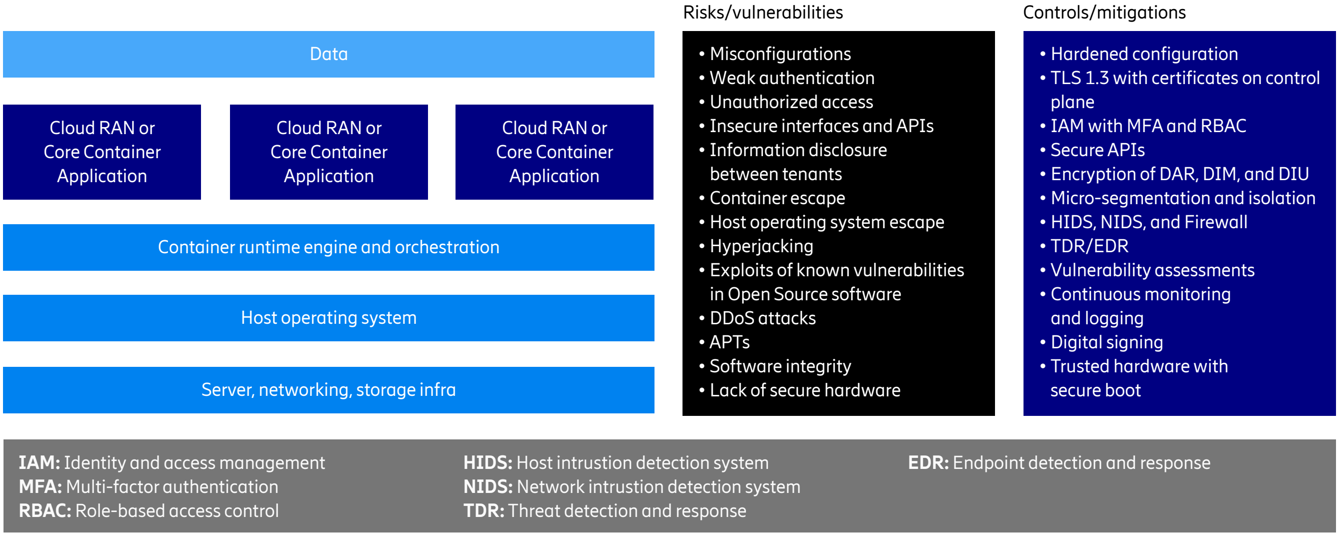
Each layer of the cloud stack must be secured to reduce risk from potential vulnerabilities being exploited by internal or external threat actors, as shown in Figure 1. Security controls must be provided to protect data, containers, container runtime engines and orchestration, operating systems and infrastructure – such as servers, networking and storage. Well-known attacks, including container escape, host escape and information disclosure between tenants can be mitigated with micro-segmentation, tenant isolation and container isolation. Common vulnerabilities, such as misconfigurations, weak authentication and authorization, and use of open-source software with known vulnerabilities can be prevented using industry best security practices.

The O-RAN ALLIANCE has specified the security architecture to include these security controls, consistent with a ZTA:

- IPsec and Transport Layer Security (TLS) 1.2 and 1.3 for confidentiality and integrity protection for data in transit
- Mutual TLS (mTLS) versions 1.2 and 1.3 with PKI-based X.509 certificates for mutual authentication
- Certificate Management Protocol version 2 (CMPv2) for certificate management
- OAuth 2.0 for authorization
- NETCONF Access Control Model (NACM) for authorization
- IEEE 802.1X port-based network access control on Open FH
- API security
- Network function robustness against volumetric DDoS attacks
- Life cycle management for network functions and applications
- Security event logging
- Signed and protected Software Bill of Materials (SBOM)

Additional security controls for a ZTA include:

- MFA
- Configuration hardening
- Confidentiality and integrity protection for data at rest and in use (DAR, DIU)
- Hardware root of trust


Data
Cloud RAN or Core Container Application
Cloud RAN or Core Container Application
Cloud RAN or Core Container Application
Container runtime engine and orchestration
Host operating system
Server, networking, storage infra

Risks/vulnerabilities

- Misconfigurations
- Weak authentication
- Unauthorized access
- Insecure interfaces and APIs
- Information disclosure between tenants
- Container escape
- Host operating system escape
- Hyperjacking
- Exploits of known vulnerabilities in Open Source software
- DDoS attacks
- APTs
- Software integrity
- Lack of secure hardware

Controls/mitigations

- Hardened configuration
- TLS 1.3 with certificates on control plane
- IAM with MFA and RBAC
- Secure APIs
- Encryption of DAR, DIM, and DIU
- Micro-segmentation and isolation
- HIDS, NIDS, and Firewall
- TDR/EDR
- Vulnerability assessments
- Continuous monitoring and logging
- Digital signing
- Trusted hardware with secure boot

IAM: Identity and access management
MFA: Multi-factor authentication
RBAC: Role-based access control
HIDS: Host intrusion detection system
NIDS: Network intrustion detection system
TDR: Threat detection and response
EDR: Endpoint detection and response

Figure 1: Exploring the cloud threats and mitigations

Shared responsibility model

The key stakeholders in cloud deployments are the cloud service provider and its customer – the cloud consumer. Examples of a cloud consumer include small and medium enterprises, government agencies, and critical infrastructure such as 5G networks [5]. The cloud consumer uses the cloud service provider's services with one of the three cloud service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [6].

The responsibilities of the cloud service provider and cloud consumer to provide security at each layer of the cloud varies with the three service models. The "cloud shared responsibility model", shown in Figure 2, provides guidance to determine the responsible stakeholder at each security layer of the cloud for each of these service models.

> The cloud service provider is responsible for security of the cloud and the cloud consumer is responsible for the security in the cloud, which always includes data, devices and people.

The cloud consumer must ensure that data is protected from unauthorized access that can result in internal or external threats viewing, modifying, or transferring data. As the data owner/controller, the cloud consumer is always accountable for the security posture of cloud deployment, including the configuration of selected controls. The cloud consumer must clearly articulate the security responsibilities delegated to each stakeholder.

Cloud service providers vary in terms of their security offerings and pricing models. Cloud consumers, as the accountable stakeholder should practice due diligence when selecting their cloud service provider partner to ensure governance and regulatory security requirements are met. The delegation of security responsibilities to the cloud service provider should consider risk-based selection of appropriate security controls and compliance with the applicable regulations. When the security control is provided by the cloud service provider, the MNO, as a cloud consumer, retains accountability and is responsible for security configuration and scheduling and implementation of software patches and upgrades. The security best practices to be followed by the cloud consumer include the items in this partial list:

- Avoid the use of weak or default passwords
- Use multi-factor authentication for human access
- Deprecate unused or invalid accounts
- Configure access controls with the principle of least privilege
- Secure Application Programming Interfaces (APIs), following guidance from OWASP [7]
- Use Public-Key Infrastructure (PKI) certificates for automated Machine-to-Machine mutual authentication
- Close unused ports and block unused protocols
- Maintain software patches and upgrades

In addition, the cloud consumer should follow CIS Benchmarks [8] for secure Open RAN deployments in the cloud.

Security within service delivery models

	IaaS	PaaS	Human access
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
Servers and storage	Cloud service provider	Cloud service provider	Cloud service provider
Physical networks	Cloud service provider	Cloud service provider	Cloud service provider

Figure 2: The shared responsibility model for the cloud

Hybrid cloud security

The US National Institute of Standards and Technology (NIST) defines the hybrid cloud as "infrastructure in a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability"[9]. This definition includes multiple deployment models, in which the Hyperscale Cloud Provider (HCP) can deploy on-premises at the MNO's facility, the MNO can deploy at the HCP's data center and cloud bursting is supported as the MNO requires additional resources on-demand. MNOs partner with HCPs to deploy the hybrid cloud, on-premise or in the HCP data center, for mobile edge computing to deliver Ultra-Reliable Low-Latency Communications use cases.

CISA advises that "cloud service providers and mobile network operators may share security responsibilities in a manner that requires the operators to take responsibility to secure their tenancy in the cloud"[10].

Three advantages of a hybrid cloud for the MNO, who has the stakeholder role of the cloud consumer, include:

1. The cloud consumer has better control and understanding of how various government rules, laws, and regulations apply to them.
2. The cloud consumer can architect the hybrid cloud deployment to ensure regulatory compliance of sensitive data on-premises, while less sensitive data is accessed, stored, and processed in the public cloud.
3. The cloud consumer can transfer part of the cloud operation to the cloud service provider, which already has the necessary cloud expertise, infrastructure, and systems.

However, there is a tradeoff of increased security risk in the hybrid cloud due to the lack of clear definition of security roles and responsibilities. The cloud consumer must practice due diligence to assess the regulatory compliance of the cloud service provider's environment.

The Cloud Security Alliance (CSA) has acknowledged the increased risk from hybrid cloud deployments and its Hybrid Cloud Security Working Group bases its activities on the security challenges for which "special attention needs to be paid to areas such as compliance and data security, which area of concern due to the interconnection between the public and private clouds"[11]. Further discussion of the Cloud Shared Responsibility Model, accountability, and delegation of responsibility for 5G cloud deployments is available in this Ericsson document [12].

Cloud security risks are applicable to any cloud deployment, including Open RAN deployments based on the O-RAN architecture with its O-Cloud, on top of which O-RAN network functions operate. The cloud threats and recommended controls must be considered for securing Open RAN deployments in the O-Cloud. At the O-RAN Alliance WG11, Ericsson is participating in the O-Cloud Security work item [13] to ensure that the O-Cloud is specified to be secure.

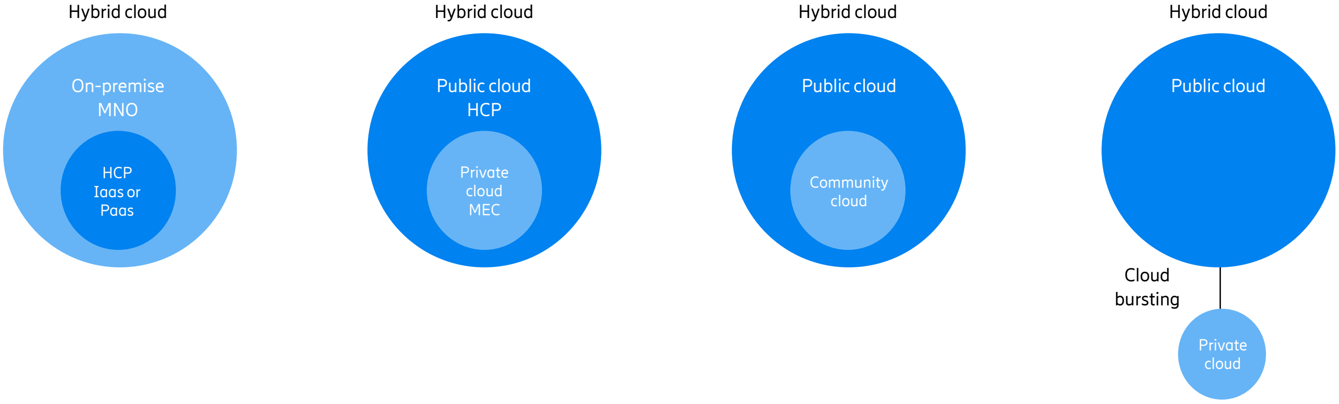


Figure 3: Hybrid cloud deployment models

Secure Open RAN intelligence

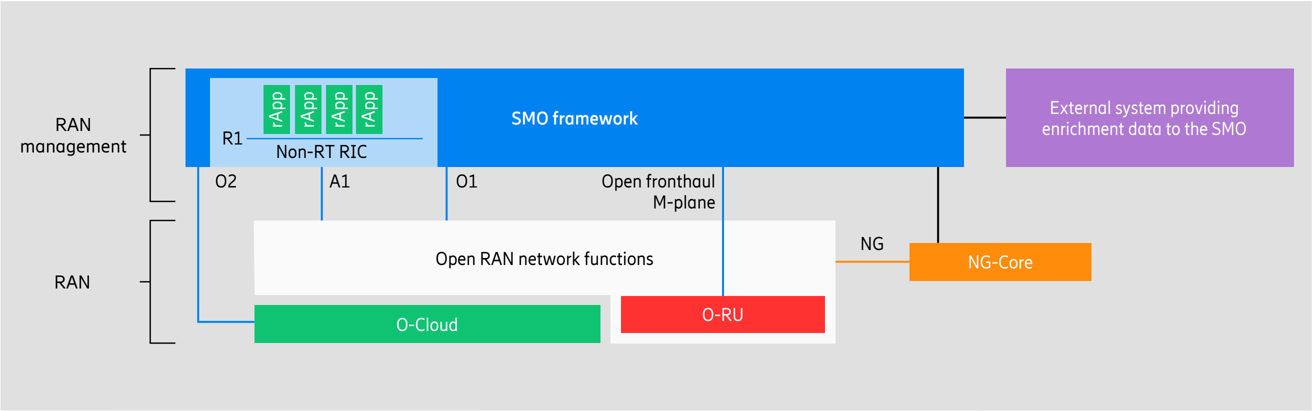
The SMO, through its Non-RT RIC provides policy-based guidance and enrichment information to the Near-RT RIC. SMO is responsible for Open RAN domain management, optimization, and orchestration. The Non-RT RIC is an automation platform that provides higher layer automation policies through direct connection to the RAN nodes with a control loop greater than one second using rApps orchestrating the Near-RT RIC. The O2 interface between the SMO and O-Cloud enables the SMO to manage the platform resources and workloads in the O-Cloud.

rApps are intended to provide RAN optimization, with the potential to extend to other RAN functions such as capacity planning or security. rApps are used in conjunction with artificial intelligence (AI) and machine learning (ML) models leveraging data sets from other functions in the Open RAN and external sources. rApps can be created by the SMO or Non-RT RIC platform vendor, network operator, or a third party. The Non-RT RIC is an automation platform through which third-party rApps offer an opportunity to create innovative automation use cases.

rApps will run on the underlying SMO and Non-RT RIC framework to provide RAN functions such as capacity planning and neighbor relations, and potentially, security functions for RAN anomaly detection, O-Cloud anomaly detection, secure configuration validation, and security compliance monitoring. As the SMO has network-wide visibility from internal and external data sources, its rApps can be purpose-built to provide RAN protecting security functions. Attacks such as APTs with lateral movement across the Open RAN cloud deployment can be detected and automatically mitigated.

The SMO will also be capable of providing RAN-specific security use cases built upon automated monitoring, detection and response to security events. External systems can provide enrichment data to the SMO to further enhance RAN security use cases. These security use cases can leverage fault, configuration, accounting, performance and security (FCAPS) data, including performance management (PM) and configuration management (CM) events, made available to the rApp from the RAN function via SMO services. The result is an SMO that is a valuable security tool for the RAN as it provides a security threat detection and response capability.

When deploying rApps that support RAN security use cases, additional requirements to adequately protect the SMO components and interfaces need to be considered to ensure secure operations. These security requirements are being addressed in O-RAN Alliance WG11 and are discussed in a later section. At the O-RAN Alliance WG11, Ericsson is leading the work items to secure the SMO and its Non-RT RIC, rApps, and its interfaces [14].

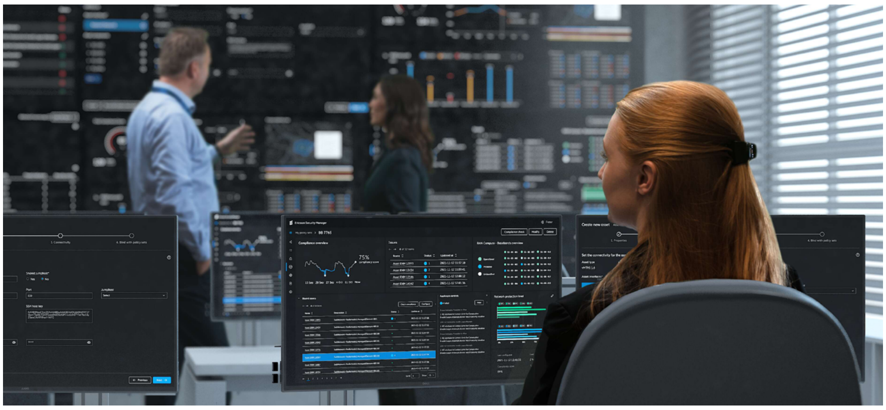


O1 and M-plane – SMO FCAPS interfaces to RAN
O2 – SMO cloud-native deployment interface
A1 – Non-RT-RIC to near-RT-RIC interface
R1 – rApps interface to Non-RT-RIC and/or SMO services

Legend
— Open RAN defined interface
— 3GPP defined interface
— Interface out of scope

Figure 4: O-RAN Architecture [15]

A secure, standardized R1 interface enables any rApp to work with other rApps. Insights from one rApp may serve as input to another, across the standardized R1 interface, to build more complex automation functions leading to more complex decisions. A group of rApps can compose larger security use cases, as insights are shared between rApps to form complex security insights and decisions.



SMOs, such as the Ericsson Intelligent Automation Platform (EIAP), play an important role in the Open RAN security posture. The EIAP supports third-party rApps [16], enabling a growing ecosystem of security use cases. An example of a security automation use case is RAN compliance monitoring to detect misconfigurations and recommend secure configurations. The SMO can provide the flexibility to build-in rApps with Security Information and Event Management (SIEM) and Security Orchestration Automation and Response (SOAR) functionality, plus the ability to integrate with external SOAR or SIEM in the Security Operations Center (SOC)

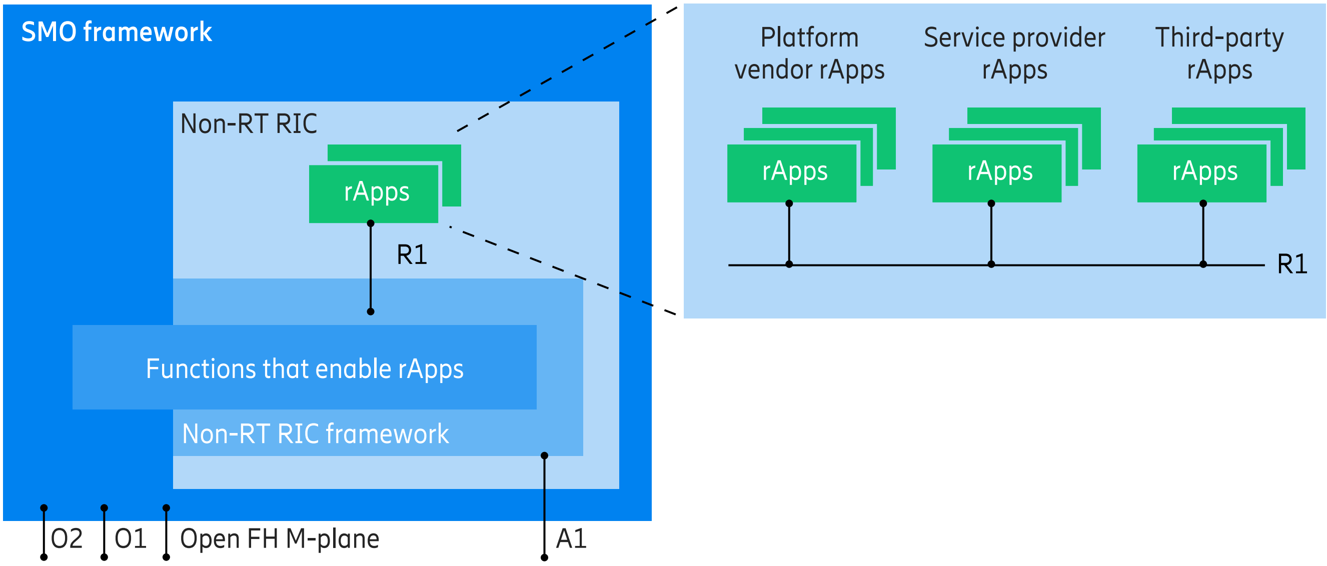


Figure 5: Exposure of SMO and Non-RT RIC framework [17] services

Securing the SMO

Securing the SMO is critical because a security vulnerability within the SMO could be exploited to serve as a beachhead for attacks against Open RAN components and lateral movement across Open RAN.

Internal and external threats require a ZTA [18] approach, in which we assume that the adversary is already inside the network. The SMO accesses internal and external data stores that must have securely implemented APIs. It is critical to implement proper mitigations to ensure the protection of confidentiality, integrity, availability and authenticity of SMO functions, interfaces, and data. Security considerations also need to be made for access, interworking, conflict mitigation, AI/ML, and the supply chain. The SMO and internal functions, applications and data must enforce secure access using mutual authentication with PKI-based certificates, multi-factor authentication, the principle of least privilege and access controls such as role-based access control or policy-based access control.

O-RAN Alliance WG11 has performed a security analysis of the SMO, with consideration of the goal to achieve a ZTA. WG11 has produced two technical reports [19] and [20], which have led to specifications of the following security requirements for SMO, SMO Functions, and Non-RT RIC [21]:

- Mutual authentication, with support for mTLS 1.2 or higher
- Authorization of service requests, with support for OAuth 2.0
- DDoS protection

These requirements must be supported for the SMO internal communications, R1 interface, A1 interface, and external interfaces used to import AI data from external AI data sources.

In addition, WG11 has specified the following security requirements for SMO logging [21]:

- Confidentiality and integrity protection of stored event logs
- Authorization to access stored security event logs
- Mutual authentication and protected export of event logs using mTLS 1.2 or 1.3, or SSHv2

A motivation for rApp creation is to provide greater vendor diversity in which best-of-breed vendors can contribute third-party applications with the goal of having a secure marketplace for RAN applications. However, this introduces the supply chain security risks that must be mitigated to enable a trustworthy ecosystem of rApps suppliers. A secure and trusted supply chain includes rApps from trustworthy suppliers, digitally signed software, validation that security requirements are implemented, vulnerability assessment, and Software Bill of Materials (SBOM). Security is a critical success factor for the integration of third-party rApps due to risks from malicious rApps, rApps with vulnerabilities, and conflicting rApps from multiple vendors.

As the number of rApp suppliers increases, so does the risk of conflicting policies and parameter settings. Conflict mitigation is important in a multi-vendor environment in which multiple apps from different vendors could be, unintentionally or maliciously, forming and pushing conflicting RAN policies and parameter settings.
Conflict mitigation prevents availability attacks, which cause RAN performance degradation and outages.

Secure peering between rApps, and between rApps and SMO functions, must be provided with certificate-based mutual authentication across the R1 interface. Confidentiality and integrity protection are essential on the R1 interface to protect against malicious neighbor rApps snooping, modifying, or injecting messages on the interface. Authentication between internal exposure functions and rApps should use mutual Transport Layer Security (mTLS) 1.3, with PKI X.509 certificates, which also provides confidentiality and integrity protection of data in motion across the SMO Service Communications and R1 interfaces. rApps must also be built with strong authorization functions using the principle of least privilege to limit exploits from malicious or rogue rApps. O-RAN Alliance WG11 has produced authentication and authorization requirements for rApps [21].

rApps are intended to perform RAN optimization functions, leveraging AI/ML, which, when used in critical infrastructure such as Open RAN, must be secure from adversaries that poison data, corrupt models, influence outcomes, exploit APIs, and reconstruct information. Security of AI/ML data and models is a recognized challenge across all industries that must be addressed to ensure AI/ML is securely used in Open RAN. rApps used in conjunction with AI/ML can leverage internal and external data sources and integration with these data sources is provided using open APIs that are interoperable and secure, with strong mutual authentication. O-RAN Alliance WG11 is currently developing security specifications for secure use of AI/ML in Open RAN and secure import of AI data from external sources to the SMO.

Suppliers of rApps should follow secure software development processes, such as defined in the NIST Secure Software Development Framework [22], and practice due diligence when using open-source software. Suppliers should also place security controls in continuous integration/continuous delivery pipelines and conduct vulnerability assessments.

The rApps ecosystem could evolve further with independent third-party security assessments that could provide audits and evaluations to enter the ecosystem or marketplace. This could model the Global System for Mobile Communications Association (GSMA) Network Equipment Security Assurance Scheme (NESAS), for secure development practices obtained by 5G vendors [23].

Conclusion

The SMO is a powerful framework for monitoring, orchestrating, and securing Open RAN. A secure SMO must be designed and built with a ZTA mindset to protect against external and internal threats, in which we assume that the adversary is already inside the network. The O-RAN Alliance WG11 has specified security requirements for the SMO, Non-RT RIC, and rApps.

The visibility and orchestration capabilities of the SMO make it an ideal platform to enhance the security of end-to-end Open RAN cloud deployments, aligning with the principles of a ZTA. The SMO's intelligence and rApp support enable an ecosystem of purpose-built security functions providing faster and deeper threat detection that protects against external and internal threats so malicious actors cannot gain access and move laterally to control the Open RAN deployment. Ericsson is leading within the O-RAN Alliance Security Working Group 11 (WG11) to ensure that the SMO and its SMO functions, Non-RT RIC, rApps, and interfaces will achieve a ZTA.

The Ericsson Intelligent Automation Platform, as Ericsson's implementation of the SMO is an open service management and orchestration platform that enables MNOs to optimize and secure their networks for the delivery of enhanced customer experiences. EIAP supports third-party rApps, enabling a dynamic and collaborative ecosystem of security use cases.

References

1. https://www.fcc.gov/file/24520/download
2. Enhanced Zero Trust and 5G, ATIS, July 2023, https://www.atis.org/tops-council/enhanced-zero-trust-and-5g/
3. Report on the Cybersecurity of Open Radio Access Networks, EU NIS Cooperation Group, May 11, 2022 digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks
4. www.cisa.gov/news/2021/10/28/nsa-and-cisa-provide-cybersecurity-guidance-5g-cloud-infrastructures
5. www.cisa.gov/communications-sector
6. The NIST Definition of Cloud Computing, NIST SP 800-145, NIST, September 2011
7. OWASP API Security Project | OWASP Foundation
8. www.cisecurity.org/cis-benchmarks/
9. The NIST Definition of Cloud Computing, NIST SP 800-145, NIST, September 2011
10. Security Guidance for 5G Cloud Infrastructures, Volumes 1 thru 4, US DHS Cybersecurity and Infrastructure Security Agency (CISA), October 28, 2021, www.cisa.gov/news/2021/10/28/nsa-and-cisa-provide-cybersecurity-guidance-5g-cloud-infrastructures
11. Cloud Security Alliance, Hybrid Cloud Security, cloudsecurityalliance.org/research/topics/hybrid-cloud-security/#:~:text=For%20hybrid%20clouds%2C%20special%20attention,users%20identify%20and%20reduce%20risk.
12. 5G security for public and hybrid cloud deployments, S. Poretsky, H. Akhtar, and P. Linder, Ericsson, Sept 2022. https://www.ericsson.com/en/reports-and-papers/further-insights/5g-security-for-hybrid-cloud.
13. O-Cloud Security Analysis Technical Report, O-RAN Alliance Security Focus Group, O-RAN.SFG.O-CLOUD-Security-Analysis-TR-v01.00.docx, March 2022.
14. Study on Security for Non-RT-RIC, Technical Report, O-RAN Alliance Security Focus Group, O-RAN.SFG.Non-RT-RIC-Security-TR-v01.00, March 2022
15. O-RAN Architecture Description, O-RAN.WG1.O-RAN-Architecture-Description-v06.00, O-RAN Alliance, Nov 2021.
16. https://www.ericsson.com/en/blog/2023/6/how-to-build-automation-applications-using-a-vibrant-developer-ecosystem
17. Adapted from O-RAN Architecture Description, O-RAN.WG1.O-RAN-Architecture-Description-v06.00, O-RAN Alliance, Nov 2021.
18. Zero Trust Architecture, NIST SP 800-207, US DoC NIST, August 2020
19. Technical Report: Study on Security for Service Management and Orchestration (SMO), v2.0, O-RAN Alliance.
20. Technical Report: Study on Security for Non-RT-RIC, v1.0, O-RAN Alliance.
21. O-RAN Security Requirements Specifications, v6.0, O-RAN Alliance.
22. Secure Software Development Framework (SSDF): Recommendations for Mitigating the Risk of Software Vulnerabilities, Version 1.1, US NIST, csrc.nist.gov/publications/detail/sp/800-218/final
23. GSMA Network Equipment Security Assurance Scheme (NESAS) www.gsma.com/security/network-equipment-security-assurance-scheme/

About Ericsson

Ericsson enables communications service providers to capture the full value of connectivity. The company's portfolio spans Networks, Digital Services, Managed Services, and Emerging Business and is designed to help our customers go digital, increase efficiency and find new revenue streams. Ericsson's investments in innovation have delivered the benefits of telephony and mobile broadband to billions of people around the world. The Ericsson stock is listed on Nasdaq Stockholm and on Nasdaq New York.

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

15/22102-FGM101030