ERICSSON

Zero Trust Architecture for evolving Radio Access Networks

November 2023

Contents

Executive overview

The year 2020 was a significant inflection point for Open Radio Access Networks (RAN) security with the achievement of three important milestones:

1. In March 2020, the O-RAN Alliance kicked off the Security Task Group (STG) that was part of the Working Group 1 (WG1) addressing Architecture [1].
2. In August 2020, Ericsson published "Security Considerations of Open RAN" [2] outlining security risks and recommending mitigations
3. In August 2020, NIST published SP 800-207, Zero Trust Architecture (ZTA) [3] to mature zero trust from a concept to an actionable plan.

ZTA is the evolution of the zero trust concept to a concrete plan based upon multi-layered security controls that provide confidentiality, integrity, availability, and authenticity protections from internal and external threats. In a ZTA, assets and resources are secured as micro-perimeters and no internal subject, whether human user or digital system, is assumed to be trusted for access to applications and data. ZTA is an important goal for securing critical infrastructure, including 5G Core networks and RAN, to protect against threat actors seeking to achieve internal presence for reconnaissance, network disruption, or data exfiltration.

As 5G critical infrastructure evolves to the cloud-native technologies and hybrid cloud deployments, it is increasingly necessary to implement a ZTA that provides protection from external and internal threats, with the assumption the adversary is already inside the network. The US Enduring Security Framework (ESF) has built upon NIST's work on ZTA to provide a playbook for ZTA in 5G cloud deployments with its four-volume publication "Security Guidance for 5G Cloud Infrastructures" [4]. A recent report from ATIS on 5G zero trust [5] concludes ZTA is needed across the entire end-to-end 5G System (5GS), including Core and RAN. ZTA for mobile networks is a journey that will take time and incur expense, so a risk-based approach should be used to guide a phased implementation. The US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) advises an incremental approach to implement a ZTA through four stages: Traditional, Initial, Advanced, and Optimal [6].

Over the past 3 years, the O-RAN Alliance evolved its WG1 STG to be a Security Focus Group (SFG) to serve all WG's and then promoted it to become WG11 for Security. Throughout this period, the O-RAN security working group, in all its forms, adopted many of the security risks identified in the 2020 Ericsson paper as official work items. The O-RAN Alliance also publicly announced its goal to pursue a ZTA in accordance with NIST and since then, WG11 has considered ZTA in its efforts to specify security requirements in Open RAN.

As Open RAN architecture continues to evolve, its specifications, product design, software development, implementation, and operations must continue to be secured with the target of a ZTA. WG11 has made significant progress to incrementally improve the Open RAN security posture and is continuing the ZTA journey with contributions from operators, vendors, government agencies, and academic institutions from around the globe. It is important that the security specifications of 5G, and future 6G, continue to progress through the ZTA maturity stages with network functions and interfaces secured to protect against external and internal threats. Further work is needed in the O-RAN Alliance, 3GPP, ATIS and other relevant industry bodies to ensure ZTA is strengthened in its specifications. Ericsson is committed to continue as a leader and major contributor to achieve this goal.

Ericsson has prioritized security for development and deployment of its software and hardware in critical infrastructure and has implemented it in Ericsson's RAN products. An Ericsson Open RAN solution, built upon its Cloud RAN [7] and Ericsson Intelligent Automation Platform (EIAP) [8] products, is secure-by-design using Ericsson's security assurance process and supporting 3GPP and O-RAN Alliance specified security controls that characterize a ZTA. Cloud RAN's security posture provides mobile network operators (MNOs) the confidence that their Open RAN deployments are secure, whether deployed on-premises or in a private, public, or hybrid cloud.

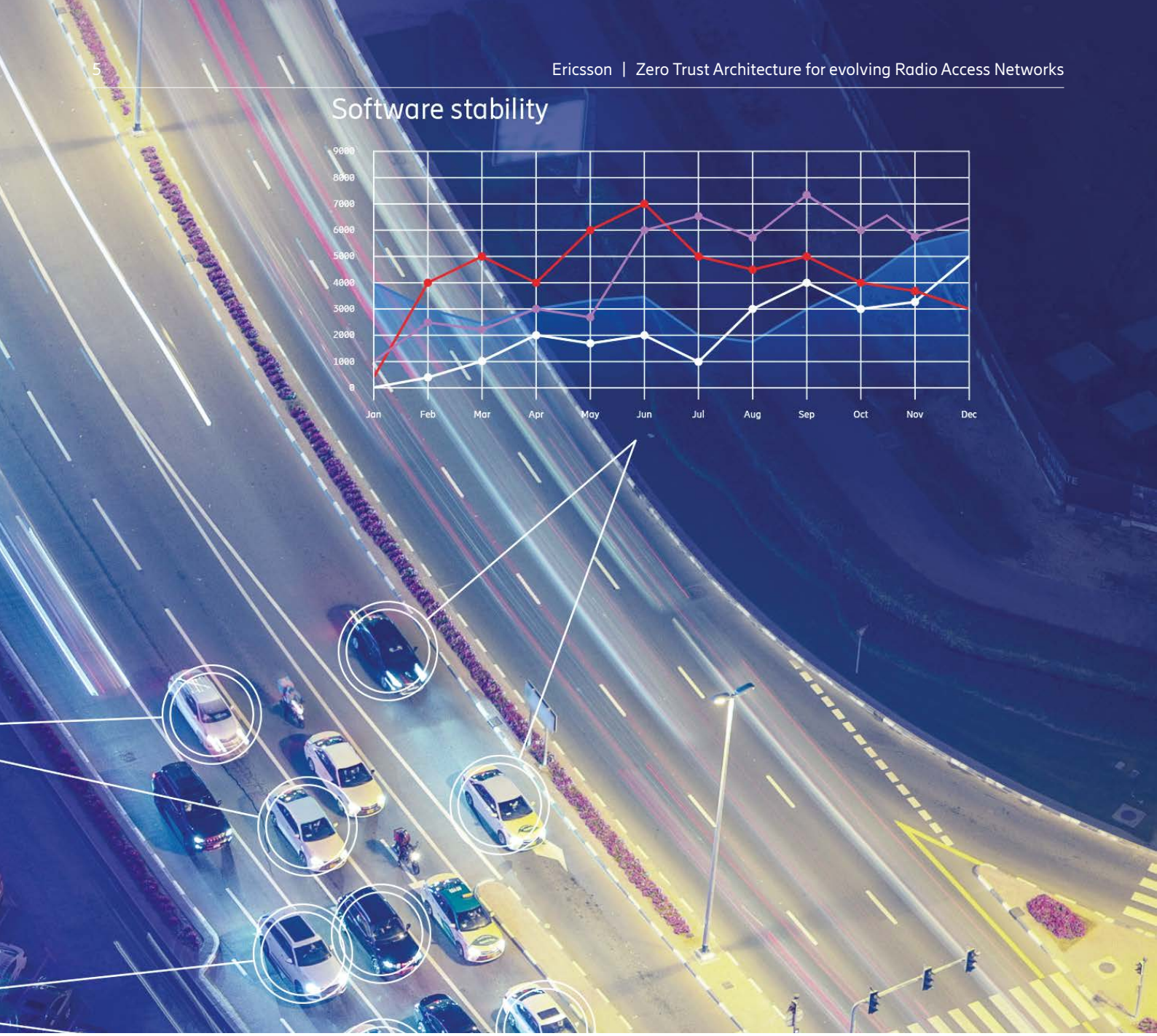
Introduction

The US National Cyber Security Strategy ("The Strategy") published by the White House Office of the National Cybersecurity Director (ONCD) on March 2, 2023 [9], stated the following:

- "Departments and agencies will direct R&D projects to advance cybersecurity and resilience in areas such as … cloud infrastructure, telecommunications … used in critical infrastructure."
- "This Administration is committed to improving Federal cybersecurity through long-term efforts to implement a zero trust architecture strategy and modernize IT and OT infrastructure."

Cloud based critical infrastructure needs to be protected from external and internal threats with a Zero Trust Architecture (ZTA) that has the following features:

- Network functions and architectural elements are secured as micro-perimeters
- Trust is not assumed for subject, whether any human user or network asset. Authentication and access controls are implemented for external and internal subjects
- Confidentiality and Integrity protection is provided for data in-transit, at-rest, and in-use
- Continuous monitoring, logging, and alerting is implemented to detect security events



This paper dives deeper into ZTA for RAN, and specifically Open RAN, as the O-RAN Alliance is leading on the ZTA topic and has publicly stated it is pursuing a ZTA [10]. When developing a plan for ZTA in Open RAN, it is important to first identify the attack surface and assets, including network functions, applications, interfaces, and data, and then identify the potential external and internal threats to the attack surface. WG11 is pursuing a ZTA for Open RAN through external and internal threats analysis and specification of security requirements and controls across O-RAN's attack surface to mitigate those threats using guidance from NIST [11], ESF [12], and EU NIS [13].

This paper provides an overview of ZTA, terminology commonly used, and applicability to RAN. ZTA critical security controls to achieve a ZTA in Open RAN are identified with an example implementation plan based upon the stages defined in the CISA Zero Trust Maturity Model (ZTMM) [14]: Traditional, Initial, Advanced, and Optimal. This paper presents the progress that has been made in the O-RAN Alliance to enhance the security posture of O-RAN and its direction to incrementally align with a ZTA. The recommendations offered in this paper align with security specifications and globally recognized best security practices to achieve a ZTA for RAN, including Open RAN, in cloud-native environments.

The security posture of an Ericsson Open RAN solution, built upon its Cloud RAN and Ericsson Intelligent Automation Platform (EIAP) products, is secure by design and will have built-in security controls that meet O-RAN security specifications, 3GPP SA3 security standards, and ZTA guidance offered by NIST, ESF, and CISA.

The path forward to a ZTA

Principles of a ZTA

Zero trust is a concept in which digital systems cannot earn trust as humans do, and therefore no network user, packet, interface, or device can have assumed trust. The implementation of zero trust affects all subjects, including digital systems and human users. Zero trust has evolved from a concept to a Zero Trust Architecture (ZTA), defined by US NIST with the principle that "there is no implicit trust granted to an asset based upon its ownership, physical location, or network location" [15]. In a ZTA, perimeter security alone is insufficient as human and digital subjects inside the network cannot be assumed to be trusted, and each asset, such as an Open RAN architectural element or network function, needs to be secured as a micro-perimeter.

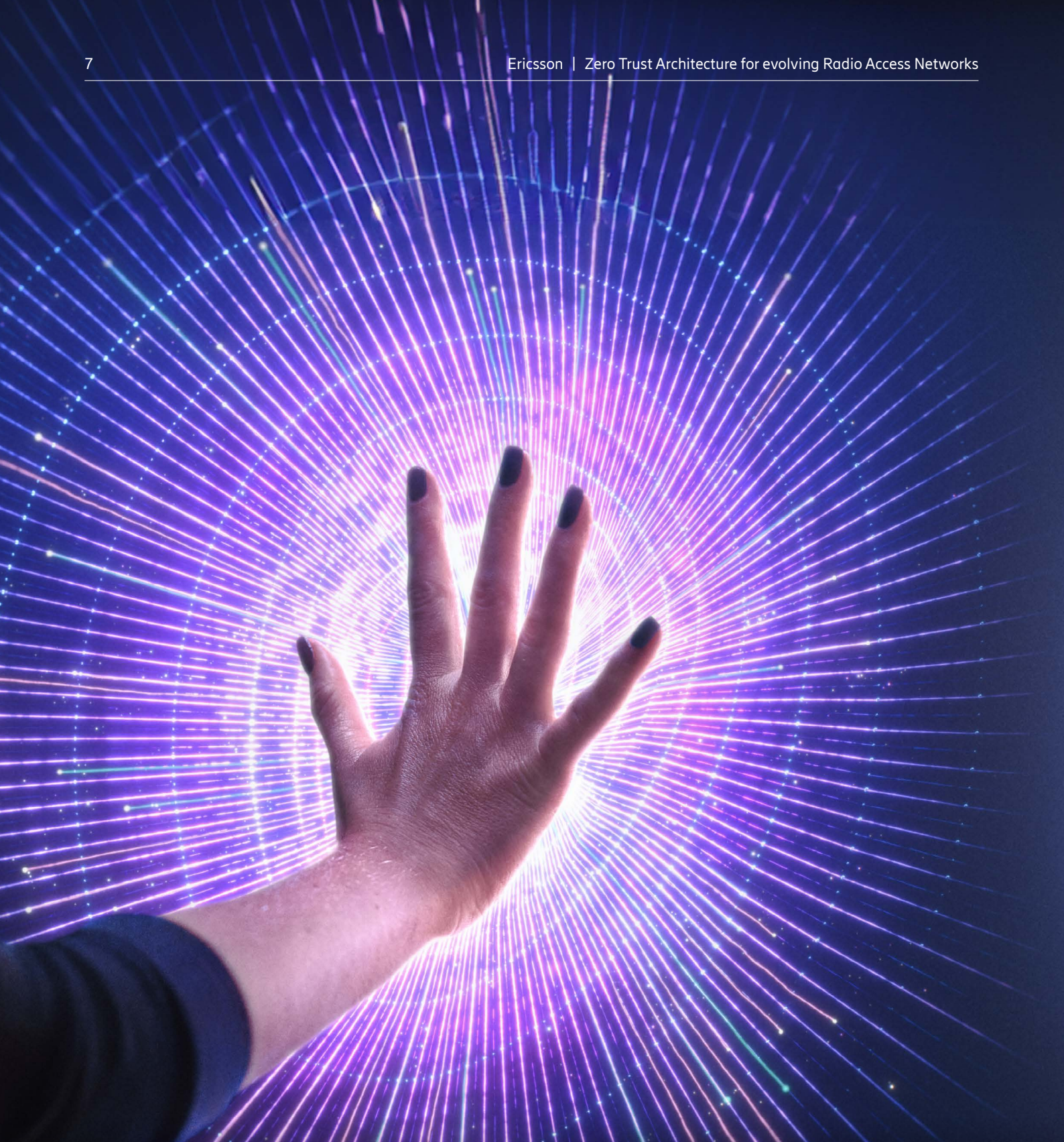
Guidance on ZTA for 5G

The migration of 5G critical infrastructure to cloud-native technologies and private, hybrid, and public cloud deployments introduces new actors and stakeholders to a shared-responsibility ecosystem. The security threats are also evolving, which requires additional security controls. RAN, as critical infrastructure, requires a ZTA security posture and the O-RAN Alliance plays a leading role to specify strong security requirements for a ZTA using an incremental, risk-based approach.

US ONCD National Cybersecurity Strategy calls for a ZTA in 5G critical infrastructure [16] and US DHS CISA has produced Security Guidance for 5G Cloud Infrastructure calling for operators and suppliers to "strive to bring a zero trust mindset" [17] built upon NIST SP 800-207 [18]. An analysis of the guidance from US Federal agencies, and its applicability and impact to 5G deployments including Open RAN, is provided by ATIS in its report "Enhanced Zero Trust and 5G" [19], which reached the significant conclusion that the NIST ZTA and all seven of its tenets apply to the end-to-end 5GS, including 5G Core and RAN.

NIST Seven Tenets of Zero Trust [20]

T1	All data sources and computing services are considered resources
T2	All communication is secured regardless of network location
T3	Access to individual resources is granted on a per-session basis
T4	Access to resources is determined by dynamic policy
T5	The enterprise [operator] monitors and measures the integrity and security posture of all owned and associated assets
T6	All resource authentication and authorization are dynamic and strictly enforced before access is allowed
T7	The enterprise [operator] collects information about the current state of assets, network infrastructure and communications and uses it to improve its security posture



O-RAN Alliance WG11 has been pursuing a ZTA for Open RAN with consideration of all seven tenets for ZTA. 3GPP is currently studying the applicability of the NIST seven tenets to RAN, and 5G Core. Further work is needed in the O-RAN Alliance, 3GPP, ATIS, GSMA and other relevant industry bodies to ensure ZTA is strengthened in the specifications.

A ZTA for mobile networks should specify and implement the twelve critical security control groups shown in Figure 1, as identified by ATIS [21]. Areas of further opportunity in ZTA for mobile networks include continuous monitoring, data collection, dynamic security policy, and AI/ML security. 5G assurance schemes in the telecom industry, such as the 3GPP Security Assurance Specifications (SCAS), GSMA Network Equipment Security Assurance Scheme (NESAS), and European Union Agency for Cybersecurity (ENISA) best practices, will contribute to achieving a ZTA [22] [23]. Perimeter security will persist as a complement to an Open RAN ZTA, as it effectively mitigates external threats, such as Distributed Denial of Service attacks and Botnets.

ZTA critical controls for secure Open RAN

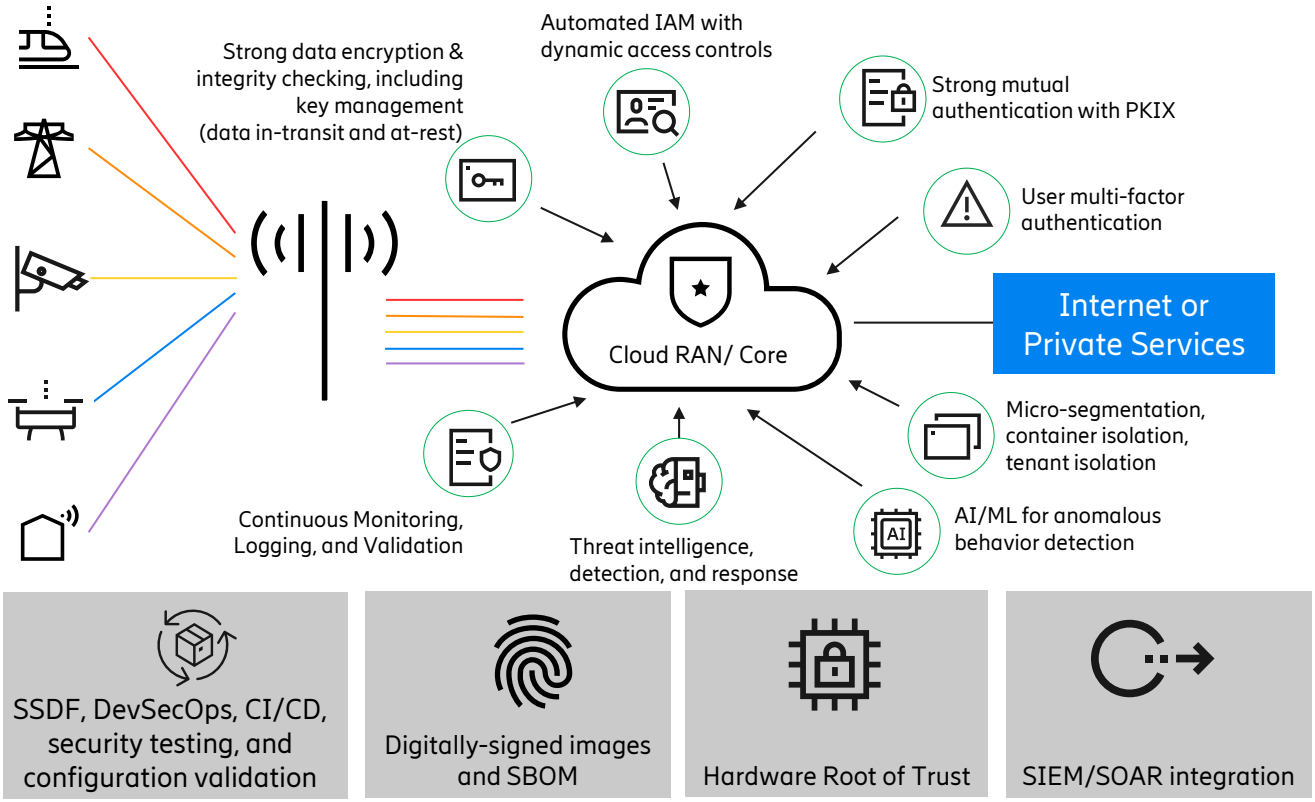


Figure 1. ZTA critical controls for secure Open RAN

Incremental phases to achieve 5G ZTA maturity

ZTA has substantial scope as each asset is a micro-perimeter that is secured with confidentiality, integrity, availability, and authenticity protection across multiple layers. This can add significant cost and an extended roadmap, which US DHS CISA acknowledges and states "the path to zero trust is an incremental process that may take years to implement" [24]. However, vendors and operators should not wait for perfect security, but instead incrementally strive towards a ZTA using a maturity model and a risk-based approach. A risk analysis helps to establish priorities for incremental improvements based on asset value, impact, and likelihood, while considering internal and external threats.

The CISA Zero Trust Maturity Model (ZTMM) [25] defines four maturity stages to incrementally achieve a ZTA, advancing from Traditional to Initial, then Advanced, and finally to the goal of Optimal. The CISA ZTMM also identifies 5 pillars for zero trust: Identity, Devices, Networks, Applications & Workloads, and Data. Each of these pillars has its unique Pillar-specific Functions, and share Cross-cutting Functions, that can evolve through the four stages. The three cross-cutting functions are Visibility and Analytics, Automation and Orchestration, and Governance.

ZTA critical controls for RAN can be implemented in an incremental approach by mapping the controls to the four CISA ZTMM stages. List 1 provides an example of how this can be done for evolving Open RAN security specifications where security risks from cloud-native technologies and cloud infrastructure need to be considered.

List 1. Example maturity levels for 5G ZTA

Traditional

- Perimeter-based approach with firewalls, IPS/IDS, and proxies
- Passwords
- Identity and Access Management (IAM) for management plane
- Syslog

Initial

- Strong encryption of sensitive data in transit and at rest using approved ciphers
- IAM including the principle of least privilege
- IEEE 802.1X for physical port access control
- mTLS 1.2 with PKI based X.509 certificates for mutual authentication of machine-to-machine communications
- Network micro-segmentation and isolation
- Continuous monitoring, logging, and alerting
- Security-by-design with secure software development and automated vulnerability testing
- Configuration validation
- Digitally signed images

Advanced

- Multi-Factor Authentication (MFA) for human users, , which may include password as one of the factors
- Network Access Control Model (NACM) support for authorization
- OAuth 2.0 for authorization between digital systems
- mTLS/TLS 1.3
- Threat Intelligence (TI)
- Automated Software Bill of Materials (SBOM)
- Key management service backed by a Hardware Security Module (HSM)
- Crypto-agility
- Security Information Event Management (SIEM)/Security Orchestration, Automation, and Response (SOAR) integration
- Container isolation
- Continuous integration/continuous deployment (CI/CD)

Optimal

- Strong sensitive Data Encryption for data-in-use using Trusted Execution Environment (TEE) and NIST approved ciphers
- IAM with dynamic access control policies
- Anomalous behavior detection, using artificial intelligence/machine learning (AI/ML)
- Threat and Endpoint Detection and Response (TDR/EDR)
- Secure software development based on NIST Secure Software Development Framework (SSDF)
- Secure software development based on DevSecOps

The next step would be to map each of the ZTA security controls, as shown in the example above, to the five pillars to assess coverage and gaps for CISA's Pillar-specific Functions and Cross-cutting Functions. An incremental, risk-based approach should be applied to each of the ZTMM stages.

ZTA considerations for Open RAN

RAN is evolving with cloud-native technologies, hybrid cloud deployments, application programming interfaces (APIs), and artificial intelligence/machine learning (AI/ML). While these technologies introduce attack vectors that are relevant for any cloud deployment, a higher level of due diligence is needed to achieve a ZTA in critical infrastructure, including RAN. ZTA ensures proper security controls for confidentiality, integrity, availability, and authenticity are specified, built, and implemented to protect cloud infrastructure, applications, and data against external and internal threats. These evolving attack vectors, associated risks, and mitigations are being addressed as security work items in O-RAN Alliance WG11 and are discussed further in the subsections below.

Secure AI/ML

While AI/ML will enable benefits such as RAN energy savings, network optimization, and device management, it also introduces security risks as adversaries can manipulate imported AI/ML data and models to corrupt or influence outcomes. While RAN can leverage AI/ML for faster and more accurate detection and response, it is important that AI/ML is securely implemented to achieve a ZTA. As stated by the US FCC, "Safe AI/ML also implies that its uses are ethical, trustworthy, and safe and provide adequate protection for privacy and security" [26].

AI/ML assets, including training data, testing data, models, and source code can be attacked during the training or deployment stages to effect availability, integrity, and privacy. AI/ML attacks can be classified as evasion attacks, poisoning attacks, API attacks, supply chain attacks, and privacy attacks [27], as described further below:

- Evasion attacks influence confidence scores and decision boundaries.
- Poisoning attacks corrupt training data sets, testing data sets, learning algorithms, or models to modify an outcome or cause a denial-of-service.
- API attacks exploit known API vulnerabilities using cross-site scripting, cross-site request forgery, and input validation failure.
- Supply chain attacks result from third parties maliciously or unknowingly providing poisoned training data or pretrained models.
- Privacy attacks include reconstruction, memorization, and membership inference attacks in which the adversary learns the content of a data set, which can result in the leakage of personal identifiable information (PII) or sensitive network information.

The OWASP Machine Learning Security Top Ten [28] provides additional information about AI/ML threats and mitigations.

Secure APIs

An API is a software-based interface that provides defined rules and message formatting for applications to communicate with each other. While APIs are fundamental to communication between digital systems, APIs have vulnerabilities that can be exploited by an adversary and therefore must have confidentiality, integrity, availability, and authenticity protection. The Cloud Security Alliance (CSA) ranked APIs as the number two threat vector in the cloud, after IAM at number one and ahead of security misconfigurations at number three [29].

APIs, such as Representational State Transfer (REST), must be secured using industry best practices. The Open Web Application Security Project (OWASP) maintains a list of the top 10 threats and risks to APIs with the purpose to provide awareness for developers to implement proper controls and mitigations [30] and a repository of API security tools [31]. The OWASP REST API's best security practices [32] include: using HTTPS, implementing access controls with authentication and authorization, and performing input validation. PKI X.509 certificates and OAuth 2.0 are preferred for strong authentication and authorization, respectively.

Security assurance for cloud-native environments

5G cloud deployments, whether private, public, or hybrid, will leverage cloud native technologies, which bring unique security challenges. Existing industry best security practices for cloud-native environments, as provided in List 2, need to be implemented where applicable to achieve a ZTA for critical infrastructure.

List 2. Industry best security practices for cloud-native RAN

- Enduring Security Framework (ESF)
  - Security guidance for 5G cloud infrastructure
- Center for Internet Security (CIS)
  - Top critical security controls
  - CIS Benchmarks
- US DHS Cybersecurity and Infrastructure Security Agency (CISA)
  - Kubernetes hardening guide
- Cloud Security Alliance (CSA)
  - Top threats to cloud computing
- US DoC National Institute of Standards and Technology (NIST)
  - NIST SP 800-204, Security strategies for microservices-based application systems
  - NIST SP 800-207, Zero Trust architecture
  - NIST SP 800-210, General access control guidance for cloud systems
  - NIST Cyber Security Framework (CSF)
  - NIST Secure Software Development Framework (SSDF)
  - NIST National Vulnerability Database (NVD)
- Open Web Application Security Project (OWASP)
  - Top 10 proactive controls
  - Top 10 web application security risks
  - Top 10 API security threats

However, relying upon industry best practices is not good enough, as it can result in an inconsistent security posture in a multi-vendor network deployment as security falls to the least common denominator in a multi-vendor environment. As stated by the US ONCD in [33]:

"Too many vendors ignore best practices for secure development, ship products with default configurations or known vulnerabilities, and integrate third-party software of unvetted or unknown provenance."

Industry best security practices can be considered for formal security requirements in security specifications and standards from 3GPP, O-RAN Alliance, and GSMA. Ericsson is a committed leader for security in Open RAN and traditional integrated RAN and will continue to work within industry bodies, to ensure security best practices mature from informal guidance to industry-specified requirements sufficient for critical infrastructure.

Cloud deployments

Cloud security is a new challenge for securing critical infrastructure, including RAN. In the cloud, critical infrastructure has new internal threats introduced due to network assets running on third-party infrastructure (including servers, network, and storage) in facilities and networks managed and operated by third parties. Assets in a mobile core and back-office IT systems, such as CRM, are often the primary targets for external attacks and are configured with security controls to mitigate these threats. However, vulnerabilities in cloud infrastructure can be exploited by an adversary to establish a beachhead and move laterally to reach the 5G Core and IT systems. In this case, the external threat actor transitions to become an internal threat actor that can perform reconnaissance and move laterally to gather information or cause disruption.

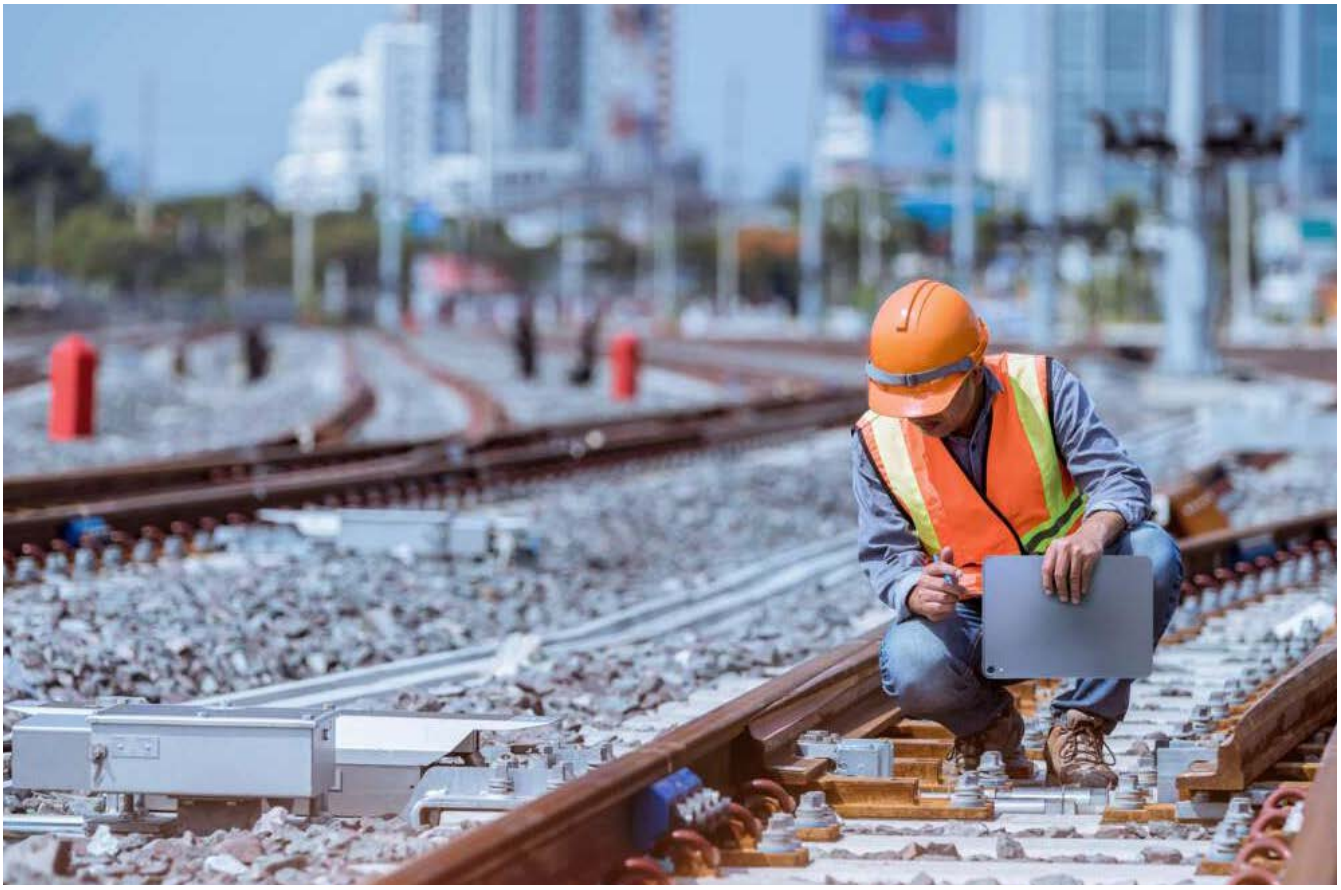
5G Core and RAN deployments in the cloud should be protected from internal threats using guidance from ESF by implementing the following security capabilities [34]:

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.

5G critical infrastructure can be deployed by the MNO in private, public, and hybrid clouds. Hybrid clouds can be a cloud service provider (CSP) infrastructure deployed on the MNO premises or MNO workloads deployed in the CSP data center. The primary challenge with securing 5G critical infrastructure in hybrid and public cloud deployments is the application of the Cloud Shared Responsibility Model, a security model used by CSPs [35] [36] [37].

Cloud deployment of critical infrastructure has multiple stakeholders who share security responsibilities, including the MNO, CSP, cloud-native network function vendors, and infrastructure vendors. The MNO can be accountable for the security posture of 5G deployments, including RAN, in private, public, or hybrid clouds. The MNO must clearly specify security requirements and any delegation of responsibilities to the CSP in the cloud service agreement. The MNO is always responsible for the protection of its customer's data and periodic validation of security configurations, including the configuration of security tools the CSP has provided per the cloud service agreement. Software vendors in the 5G ecosystem should follow US Government recommendations published in [38] to ensure security is built-in. Further discussion of the Cloud Shared Responsibility Model, accountability, and delegation of responsibility for 5G cloud deployments is available in [39].

ZTA in Open RAN



Open RAN is the evolution of traditional RAN by providing disaggregation, automation, intelligence, and open interfaces. This requires new open interfaces and architectural elements specified by the O-RAN Alliance and 3GPP. Intelligent automation in Open RAN is realized using AI/ML. As stated by the US FCC CSRIC Report on Open RAN, "Open RAN is O-RAN, Cloud RAN, vRAN, and other technologies" [40].

To achieve a ZTA in Open RAN, a goal of the O-RAN Alliance, the architectural elements must be secured as micro-perimeters and interfaces must be secured with the assumption the adversary is already inside the network to perform reconnaissance, proliferate data or information, or cause disruption. O-RAN Alliance WG11 considers this in its threat modeling and builds security requirements to provide confidentiality, integrity, availability, authentication, and authorization protections for internal and external threats across the architecture. New technologies used in Open RAN, such as AI/ML, APIs, cloud native technologies, and cloud infrastructure must also be properly secured for a ZTA in critical infrastructure.

Over the past two years, the O-RAN Alliance WG11 has addressed many security risks with the addition of enhanced security specifications to strengthen the O-RAN security posture toward a ZTA [41]. The O-RAN Alliance specified security controls, as shown in List 3 below, align with the "Initial" stage of the CISA ZTMM toward incrementally achieving an "Optimal" ZTA for Open RAN.

List 3. O-RAN specified security controls aligned with Initial Stage of ZTA

- Transport Layer Security (TLS) 1.2 and 1.3.
  - TLS and mutual TLS (mTLS) versions 1.2 and 1.3 have been specified across O-RAN interfaces.
- Certificate-based mutual authentication
  - mTLS with PKI X.509 certificates on O-RAN internal and external interfaces.
- Certificate Management Protocol version 2 (CMPv2) for consistent PKI certificate management across O-RAN.
- NACM for authorization
- IEEE 802.1X port-based network access control on OFH
  - Robustness against volumetric DDoS attacks
  - Supported by all NFs terminating all network interfaces
- Life cycle management for NFs and applications
- Security event logging
- Signed and protected Software Bill of Materials (SBOM)
- Secure credentials
  - Encrypted key storage, hardware root of trust, chain of trust, and remote attestation

Collaborative work in the O-RAN Alliance WG11 is ensuring that security specifications continue to evolve toward an Advanced, and eventually Optimal, ZTA for O-RAN. The top external and internal threats, shown in Figure 2, continue to be addressed by current WG11 security work item teams with contributions from operators, vendors, government agencies, and academic institutions from around the globe. As the O-RAN architecture continues to evolve, its new features, functions, and interfaces, also shown in Figure 2, will be secured for a ZTA.

O-RAN Threat Taxonomy

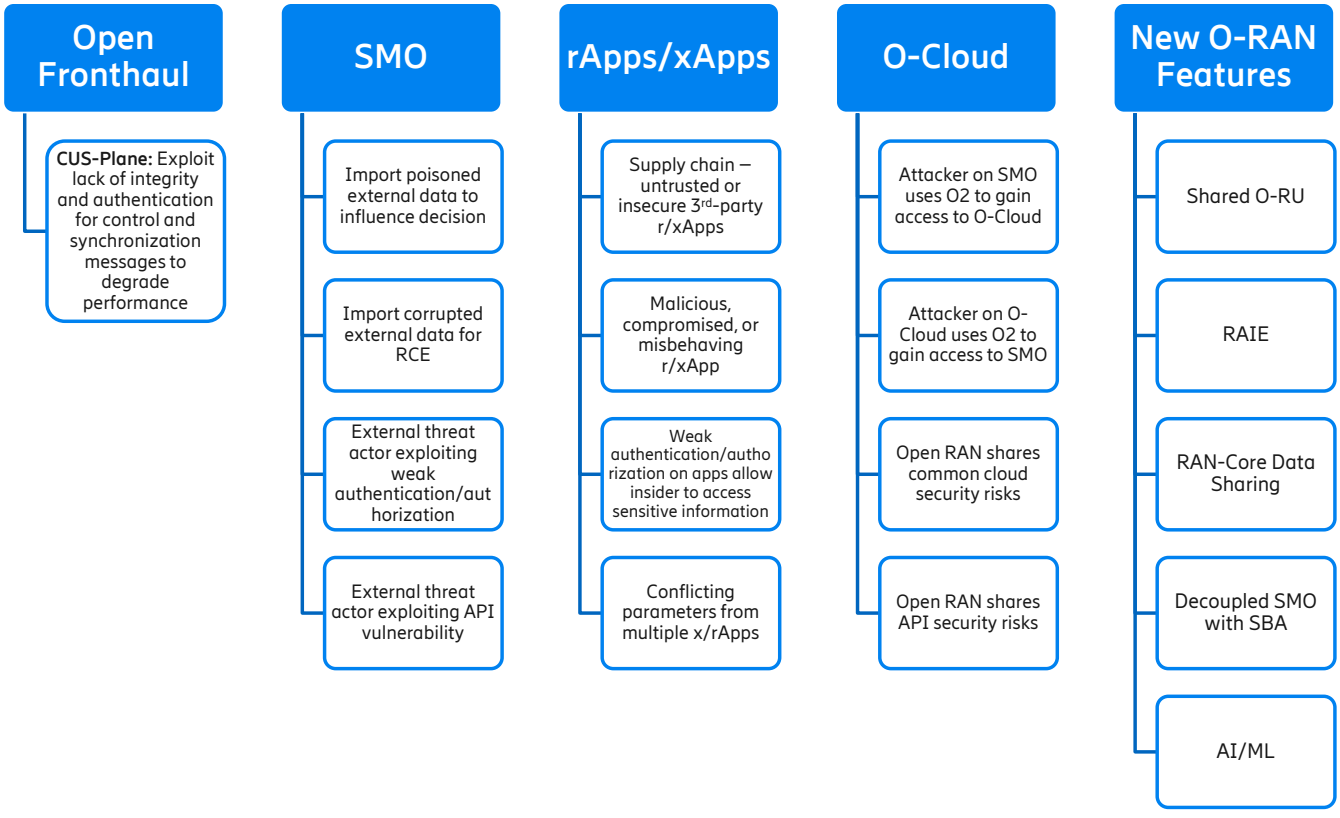


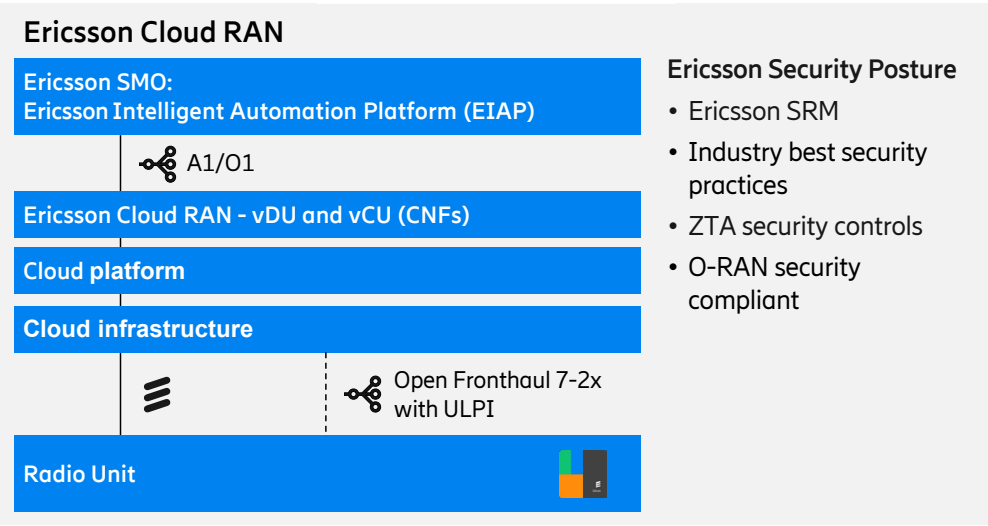
Figure 2. O-RAN Threat Taxonomy – current view

Cloud RAN: An Ericsson secure Open RAN solution

Ericsson Cloud RAN software and Ericsson Intelligent Automation Platform (EIAP), as shown in Figure 3, is part of Ericsson's Open RAN solution that implements the Open RAN goals of cloudification, intelligence/automation, and open internal RAN interfaces, as described in [42] and [43]. These products support disaggregation of hardware and software, cloud native architecture, SMO/Non-RT-RIC/rApps, O-RAN automation interfaces (A1, O1), and later also the OFH 7-2x with uplink performance improvement (ULPI), which is pending technical specification work in the O-RAN Alliance.

Ericsson's Security Reliability Model (SRM) [44], launched 10 years ago, is built upon industry best practices and provides governance that ensures security is built into Ericsson's Cloud RAN, EIAP, and other products. Ericsson SRM includes many of the ZTA recommended controls and DevSecsOps process, as shown in Figure 4. Ericsson SRM covers internal SW development, consumption of upstream third-party software, including open source software, secure coding practices, vulnerability scanning, vulnerability testing, penetration tests, and operations. Ericsson SRM also mandates addressing OWASP's top 10 risks [45] and producing a signed software bill of materials (SBOM) [46] and [47].

Ericsson Cloud RAN's security posture



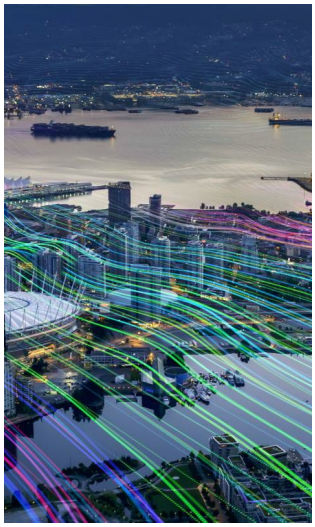


Figure 3. Ericsson Cloud RAN security posture

Secure product development

Leveraging company-wide security by design principles (Ericsson SRM) and experiences from Integrated RAN

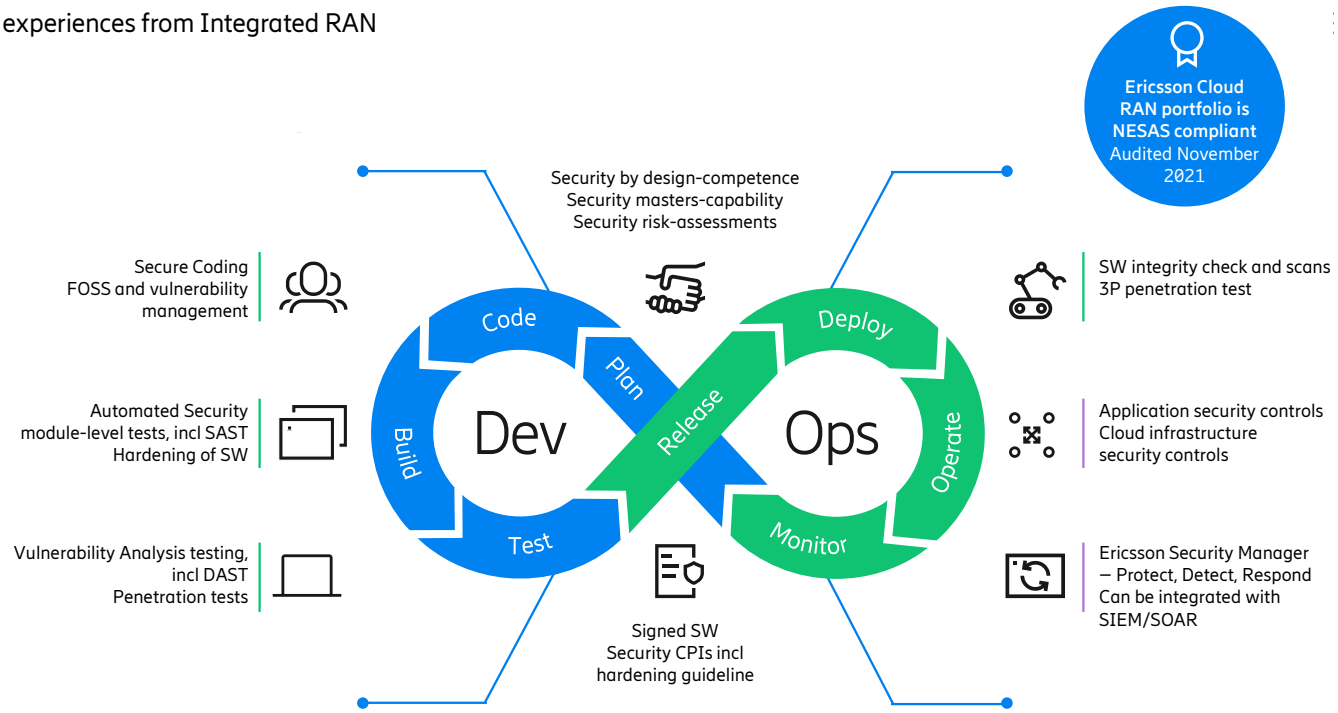


Figure 4. Secure product development

Ericsson Cloud RAN will have built-in support for the ZTA security controls that are relevant to the application software and follow industry best security practices. Product security will evolve to be consistent with the CISA ZTMM, starting from the Initial level, targeting the Advanced controls, and striving toward the Optimal level.

For transactional APIs, Cloud RAN will implement confidentiality and integrity protection using mTLS with PKI-based X.509 certificates, including the internal interfaces between the pods in the application. The open fronthaul compliant O-RU will support the supplicant function for port-based authentication following IEEE 802.1X. Continuous monitoring and logging will be supported in Ericsson Cloud RAN software and can be streamed to a SMO, such as the EIAP, or other centralized monitoring nodes, such as the Ericsson Security Manager (ESM). This will allow the realization of security use cases such as the detection of breaches and lateral movement through the disaggregated cloud stack and allow for the introduction of AI/ML providing security capabilities.

These are a few examples of application security controls consistent with a ZTA, which also requires underlying hardware and cloud infrastructure to be secure from external and internal threats.

EIAP provides the SMO, the Non-RT RIC, and rApps, each with AI/ML capabilities. The EIAP is built using the same secure-by-design principles as Cloud RAN and will include the security controls needed to achieve the ZTA to protect new interfaces and functions introduced in the SMO architecture. The SMO can enhance the RAN security posture by implementing new security use cases. rApps deployed in an SMO framework must be provided by trustworthy suppliers using SBOM and digitally signed software, along with support for strong authentication and authorization and a secure, standardized R1 interface.

Ericsson products are GSMA NESAS certified. Ericsson advocates that O-RAN Alliance, GSMA, continue its collaboration to specify an equivalent industry security certification program for O-RAN building upon NESAS.

Conclusions

5G networks, as critical infrastructure, are evolving to a Zero Trust Architecture (ZTA), as defined by US NIST, to protect against external and internal threats. Traditional perimeter-based security is insufficient with the emergence of new threat vectors that have already been exploited by sophisticated threat actors. A ZTA provides micro-perimeters and secure interfaces with security controls including authentication and authorization for external and internal subjects to access resources, confidentiality and integrity protection of data-in-transit, at-rest, and in-use, and continuous monitoring and logging. The path to a ZTA can take time and incur costs. It is important to take an incremental, risk-based approach to evolve ZTA through maturity stages defined by US CISA. This enables vendors and MNOs to embrace ZTA at an acceptable pace to achieve the wanted security posture.

The O-RAN Alliance is pursuing a ZTA with consideration of external and internal threats in its security analysis. With the leadership of Ericsson and other contributors, O-RAN Alliance WG11 continues to enhance the O-RAN security posture for each of its assets, including architectural elements, network functions, interfaces, and data. New O-RAN features, such as Decoupled SMO, Shared O-RU, RAN-Core Data Sharing, and AI/ML will have security built-in to its specifications. WG11 is also in the process of formalizing relevant industry best practices into O-RAN security specifications, including O-Cloud. The work items in WG11 address many of the findings and recommendations made in [48], [49], and [50].

The foundation of ZTA is secure products built upon secure specifications, security-by design principles, secure software development frameworks, and product security assurance. Vendors should implement O-RAN Alliance security specifications and Ericsson's integrated RAN, Cloud RAN and EIAP, are secure-by-design using Ericsson's SRM security assurance process and support of security controls that align with a ZTA. Ericsson's RAN solutions implement the wanted security posture and Ericsson will continue to lead at relevant industry bodies, including the O-RAN Alliance and 3GPP, to ensure ZTA is built-in. Cloud RAN's security posture provides MNOs the confidence that their Open RAN deployments are secure whether deployed on-premises or in a private, public, or hybrid cloud.

References

1. O-RAN Alliance, O-RAN ALLIANCE e.V.
2. Security Consideration of Open RAN, S, Poretsky and J. Boswell, August 2020.
3. Zero Trust Architecture (ZTA), NIST SP 800-207, S. Rose, O. Borchert, S. Mitchell, S. Connelly, US DoC NIST, August 2020.
4. Security Guidance for 5G Cloud Infrastructures, vols. I thru IV, US ESF, Oct/Nov 2021.
5. Enhanced Zero Trust and 5G, ATIS, July 2023.
6. Zero Trust Maturity Model, v2.0, US DHS CISA, April 2023.
7. Ericsson Cloud RAN, Cloud RAN - 5G RAN - Virtually everywhere - Ericsson.
8. Ericsson Intelligent Automation Platform (EIAP), Intelligent Automation Platform - Ericsson.
9. US National Cybersecurity Strategy ("The Strategy"), WH ONCD, March 2, 2023.
10. "O-RAN Minimum Viable Plan and Acceleration towards Commercialization", O-RAN Alliance technical paper, June 2021, O-RAN Minimum Viable Plan and the Acceleration towards Commercialization Whitepaper, June 2021 (websitefiles.com)
11. Zero Trust Architecture (ZTA), NIST SP 800-207, S. Rose, O. Borchert, S. Mitchell, S. Connelly, US DoC NIST, August 2020.
12. Security Guidance for 5G Cloud Infrastructures, vols. I thru IV, US ESF, Oct/Nov 2021
13. The NIS2 Directive, DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, December 2022.
14. Zero Trust Maturity Model, v2.0, US DHS CISA, April 2023.
15. Zero Trust Architecture (ZTA), NIST SP 800-207, S. Rose, O. Borchert, S. Mitchell, S. Connelly, US DoC NIST, August 2020.
16. US National Cybersecurity Strategy ("The Strategy"), WH ONCD, March 2, 2023.
17. Security Guidance for 5G Cloud Infrastructures, vols. I thru IV, US ESF, Oct/Nov 2021.
18. Zero Trust Architecture (ZTA), NIST SP 800-207, S. Rose, O. Borchert, S. Mitchell, S. Connelly, US DoC NIST, August 2020.
19. Enhanced Zero Trust and 5G, ATIS, July 2023.
20. Zero Trust Architecture (ZTA), NIST SP 800-207, S. Rose, O. Borchert, S. Mitchell, S. Connelly, US DoC NIST, August 2020.
21. Enhanced Zero Trust and 5G, ATIS, July 2023.
22. Evolving 5G security for the cloud, S. Poretsky, Ericsson, Jan 2022.
23. Cybersecurity of Open Radio Access Networks | Shaping Europe's digital future (europa.eu), EC NIS Cooperation Group, May 2022.
24. Zero Trust Maturity Model, v2.0, US DHS CISA, April 2023.
25. Zero Trust Maturity Model, v2.0, US DHS CISA, April 2023.
26. The Importance of Artificial Intelligence and Data for the Telecommunications Industry and the FCC, Jan 2021, fcc_aiwg_2020_whitepaper_final.pdf 17 Ericsson | Evolving Open RAN security .
27. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations (nist.gov), US DoC NIST, March 2023.
28. OWASP Machine Learning Security Top Ten | OWASP Foundation.
29. Top Threats to Cloud Computing: Pandemic Eleven, Cloud Security Alliance, June 2022.
30. OWASP API Security Project | OWASP Foundation.
31. API Security Tools | OWASP Foundation.
32. REST Security - OWASP Cheat Sheet Series.
33. US National Cybersecurity Strategy ("The Strategy"), WH ONCD, March 2, 2023.
34. Security Guidance for 5G Cloud Infrastructures, NSA ESF and DHS CISA, volumes I thru IV, Oct/Nov 2021.
35. MS Azure Shared Responsibility Model, Shared responsibility in the cloud - Microsoft Azure | Microsoft Learn.
36. AWS Shared Responsibility Model, Shared Responsibility Model - Amazon Web Services (AWS).
37. Google Shared Responsibility Model, Shared responsibilities and shared fate on Google Cloud | Architecture Framework.
38. Secure-by-Design, US NSA, US CISA, and US FBI, April 2023.
39. 5G security for public and hybrid cloud deployments, S. Poretsky, P. Linder, and H. Akhtar, Ericsson, September 2022.
40. Report on Promoting Security, Reliability, and Interoperability of Open Radio Access Network Equipment, US FCC CSRIC VIII WG2, Dec 2022.
41. O-RAN Specifications Downloads, O-RAN Downloads (orandownloadsweb.azurewebsites.net).
42. Evolving to a Strong Cloud RAN Security Posture, S. Poretsky and J. Jardal, Ericsson, Nov 2022.
43. Intelligent security: How the SMO can enhance the security posture of Open RAN, S. Poretsky and J. Jardal, Ericsson, August 2023.
44. Ericsson Security Reliability Model.
45. https://owasp.org/www-project-top-ten/.
46. https://ntia.gov/report/2021/minimum-elements-softwarebill-materials-sbom.
47. O-RAN Security Requirements Specification, O-RAN Alliance WG11.
48. Summary of the NCSC's security analysis for the UK telecoms sector, UK NCSC, January 2020.
49. Open RAN Risk Analysis (bund.de), English translation, BSI Germany, February 2022.
50. Cybersecurity of Open Radio Access Networks | Shaping Europe's digital future (europa.eu), EC NIS Cooperation Group, May 2022.

Author biographies

Scott Poretsky is Director of Security, Network Product Solutions, North America, Ericsson

Scott Poretsky is Ericsson North America's Director for Security, Network Product Solutions. He has over 25 years of industry experience in a variety of networking and security technologies. Scott is currently working in the areas of 5G security, Open RAN security, cloud security, and zero trust architectures. Scott currently serves as Co-Chair of the O-RAN Alliance's Security Working Group (WG11), Co-Chair of the ATIS 5G Zero Trust Study Group, and Advisory Board Member for the IEEE ComSoc technical committee for Communications Quality and Reliability (CQR). He has represented Ericsson in government-industry collaboratives including the FCC CSRIC and NSA/CISA sponsored Enduring Security Framework (ESF). Scott has one patent, numerous published papers, and numerous invited talks. Scott is a Certified Information Systems Security Professional (CISSP) and Certified Cloud Security Professional (CCSP). He earned an MSEE from the Worcester Polytechnic Institute (WPI) and BSEE from the University of Vermont.

Joakim Jardal is based in Stockholm, Sweden and is a Strategic Product Manager within Product Line Cloud RAN at Ericsson focusing on Security.

Joakim Jardal is a Strategic Product Manager within Ericsson product line Cloud RAN responsible for the functional area of security. He has over 18 years of industry experience from product development of 5G, LTE and WCDMA RAN. He has been holding many different roles within security and product quality assurance as well as system integration and customer first product introduction projects. Joakim received his M.Sc. degree in Applied Physics and Electrical Engineering from Linköping University, Sweden, in 2004 and also studied at University of Queensland in Brisbane, Australia. He is passionate about bringing new technologies to life in high quality products and to enable the teams that develop them.

Ericsson enables communications service providers to capture the full value of connectivity. The company's portfolio spans the business areas Networks, Cloud Software and Services, Enterprise Wireless Solutions, 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.

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

1/0341-FGD1011490