WHITE PAPER

Open RAN security

NOKIA

Introduction

Open RAN is an emerging architecture and approach in the Radio Access Network (RAN) domain that aims to provide more flexibility, scalability, efficiency and innovation for communications service providers (CSP) and enterprises.

The Open RAN architecture expands the threat surface due to new open interfaces, functionalities, technologies and a potential multi-supplier environment. A combination of security procedures, techniques and technologies can mitigate the potential risks associated with an increased threat surface.

Nokia has taken a leading role in supporting the industry in addressing the Open RAN security concerns. In this paper, we examine the challenges and Nokia's approach to addressing them.

Nokia's commitment to Open RAN

Nokia develops its Cloud RAN and Open RAN solutions under the flexible anyRAN approach. Based on close collaboration with industry-leading technology partners, anyRAN provides the widest choice of strategic options for the RAN evolution of CSPs and enterprises.

Open RAN refers to the disaggregation and standardization of the RAN interfaces, particularly the Open Fronthaul interface between the Radio Unit (RU) and the Baseband. This is called horizontal disaggregation of RAN.

Standardized interfaces are critical for interoperability and seamless integration that enables supplier diversity. For more details on horizontal disaggregation and Open RAN, refer to Nokia Open RAN Industry and Solution Update[1].

Nokia has long been an industry advocate of Open RAN and was the first Tier 1 supplier to join the O-RAN Alliance in 2018. Nokia currently co-chairs three important technical work groups and two next-generation research groups. From 2021 to 2024, Nokia made more contributions to the work of the O-RAN Alliance than any other member.

In line with the Open RAN vision of enabling true multi-supplier deployments, Nokia is leading the industry in creating opportunities for the industry ecosystem and new developers to verify and launch Open RAN compliant solutions.

Nokia supports the O-RAN Alliance Open Testing and Integration Centers (OTIC) and has invested in its own collaboration and testing centers in Dallas, USA, and Ulm, Germany. Nokia also promotes the establishment of third-party application development, integration and testing environments as part of the i14y Lab consortium. As a key contributor to O-RAN PlugFests, Nokia is demonstrating real multi-supplier interoperability via open interfaces and supporting third-party applications.

At every step of Nokia's development and verification process, we ensure that security concerns will not be a factor limiting the operator or enterprise's selection of Open RAN.

Comprehensive approach to security intelligence

Nokia has been producing threat intelligence reports for many years and these reports are freely available on the web. Our latest edition is the most comprehensive report to date, including a greater emphasis on cybersecurity trends and emerging technologies that will impact the telecom industry.

According to the Nokia Threat Intelligence Report 2024[2], the main findings in attacks against mobile networks were:

- A more complex cyber threat landscape has emerged with advanced techniques such as ransomware, potentially state-sponsored, targeting data theft and service disruption.
- The number of Distributed Denial of Service (DDoS) attacks continues to grow, and carpet-bombings are becoming larger in scope. Botnets, which accounted for about 60% of DDoS traffic, continue to be a major driver.
- The use of AI, automation and residential proxies has become more prominent, reflecting a rise in attack sophistication.

Nokia's Cyber Security Center in France continuously enhances its cyber threat intelligence (CTI) capabilities and develops effective countermeasures. Nokia leverages data and numerous threat intelligence feeds from trusted industry sources, which provide real-time information about emerging threats and vulnerabilities to telecom networks.

The expert team at Nokia's Threat Intelligence Center in Canada plays a pivotal role in curating and analyzing relevant data, sifting through vast amounts of information to identify trends and provide actionable intelligence to CSPs.

Nokia is a member of the Telecommunications Information Sharing and Analysis Center (T-ISAC), a collaborative organization that allows us to tap into the collective knowledge of industry experts and gain new insights into emerging threats specific to the telecom industry.

Together, these diverse sources of information form a robust framework for gathering and analyzing cyber threat intelligence data. The data drives the requirements and controls related to the most significant threats as presented in the Nokia reports.

The data also enables Nokia to provide CSPs and enterprises with the knowledge they need to proactively defend against evolving threats in the era of 5G, the internet, IoT and open interfaces. In addition, Nokia supports customers with a broad offering of security services, such as advanced consulting services, implementation and managed services.

Investing in cybersecurity education and awareness programs will be vital for both suppliers and customers to defend against socially engineered attacks and inadvertent data exposures.

Open RAN security challenges

The telecom industry is gradually moving towards virtualization, cloudification and openness, which bring new functions, interfaces, technologies, multiple suppliers and more stakeholders into the processes.

This results in more complexity, which increases the potential attack surface and also the risk of internal vulnerabilities, as explained in the EU Network and Information Systems (NIS) Cooperation Group's Report on the cybersecurity of Open RAN[3].

Figure 1 illustrates key areas of security challenges that come with Open RAN.

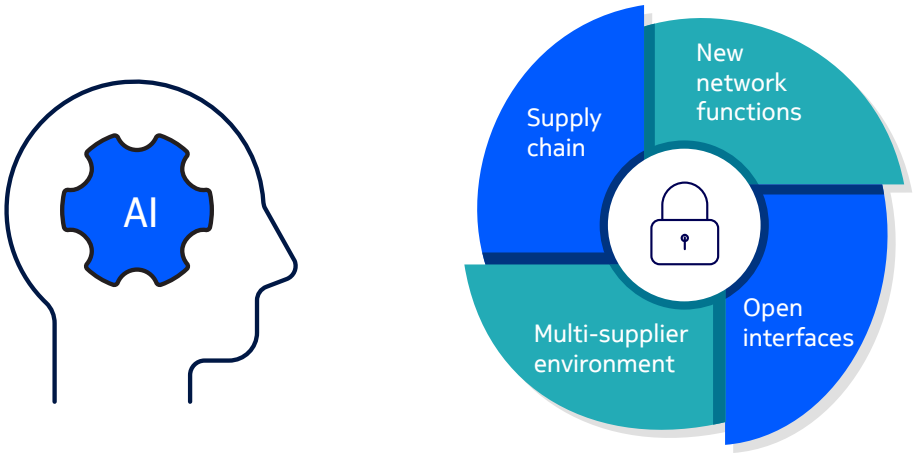

Figure 1. Key areas of Open RAN security challenges

New network functions

The Open RAN architecture introduces new functions such as non-real-time RAN Intelligent Controller (RIC). In addition, the O-RAN Alliance has defined the Service Management and Orchestration (SMO) framework as an open platform to manage a multi-supplier, multi-technology network. CSPs can pick and choose components for the SMO framework from different suppliers and integrate those together or select a comprehensive solution such as Nokia Service Management and Orchestration.

Multi-supplier environment

Open RAN architecture allows a diverse set of suppliers. Ensuring the integrity and authenticity of all the assets in the Open RAN system is critical. However, implementing components from different suppliers may lead to unintended vulnerabilities if not carefully managed. Nokia recommends that CSPs conduct thorough due diligence checks of all suppliers and implement strict security controls for all third-party network access to mitigate the risks posed by the involvement of multiple suppliers.

Supply chain

In a multi-supplier environment, ensuring the security of the entire supply chain becomes a challenge. Attacks on IT systems and communications networks are on the rise, fueled by geographical tensions and the rapid development of technologies. According to Nokia's threat intelligence analysis[2] and a report by the European Union Agency for Cybersecurity (ENISA)[4], supply chain attacks are also increasing rapidly.

Open interfaces

New open interfaces defined by the O-RAN Alliance support new functionalities. However, they also increase the attack surface and provide potential opportunities for threat actors to gain access to the system. The new interfaces include O1 and O2 related to the SMO framework, A1 and R1 related to the non-real-time RIC, and the Open Fronthaul between the radio unit and distributed unit. Nokia recommends enhanced security controls for RAN network management, such as multi-factor authentication and role-based access control.

Artificial intelligence

Open RAN supports the use of artificial intelligence (AI) in network optimization and programmability, which opens opportunities for new types of security threats.

As the attack surface expands in an Open RAN system and the threat landscape increases, the traditional perimeter-based security model has become obsolete. In a complex environment with new interfaces, new functionalities, more stakeholders and diverse trust domains, the perimeter simply cannot be trusted anymore. A novel approach to protecting the system is needed.

Nokia's Open RAN security approach

Nokia's Open RAN security approach consists of eight key pillars.

- Design for Security (DFSEC)
- Zero-trust architecture
- Supply chain security
- System integration of multi-supplier solutions
- Strong identity and access management
- Continuous threat monitoring and auditing processes
- Securing data both in transit and at rest
- Compliance with security standards

The following sections, also illustrated in Figure 2, go into more detail on each of these pillars.

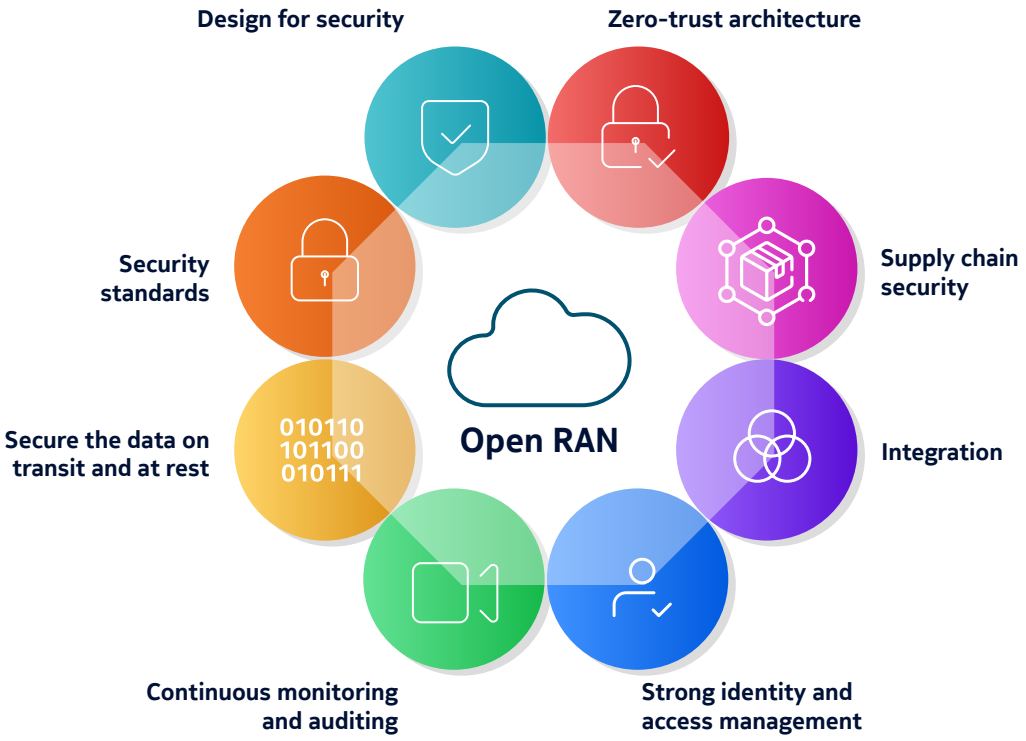

Figure 2. Key pillars of Nokia's Open RAN security solution

Design for security

Nokia's Design for Security (DFSEC) process[5] holistically addresses current and future security challenges. It supports new technologies and services and addresses emerging threats as well as customer and regulatory requirements.

At Nokia, security is an integral part of product quality. Security and privacy are built into all products from the start of the development process and maintained throughout the product life cycle. An example of product security design is the Trusted Platform Module (TPM) technology integrated into Nokia AirScale Baseband products and hardware accelerators. The TPM is a specialized chip that stores cryptographic keys for encryption, authentication and integrity verification. Compared to software-processed keys, hardware-processed keys make products more difficult to tamper with.

The key pillars of the framework include:

- Defined decision points and checks to ensure security controls have been completed throughout the development cycle.
- Maintaining a vulnerability database by gathering information from multiple sources, such as suppliers, media and the U.S. National Vulnerability Database (NVD) to identify emerging vulnerabilities.
- Careful management of patches and upgrades and working with customers to ensure these are applied as necessary.
- Using cloud security policies to ensure robust deployments.

Nokia uses the principle of shift left security, which means that security controls and policies are implemented as early in the development process as possible.

Zero-trust architecture

The Zero-Trust Architecture (ZTA) model[6], defined by the U.S. National Institute of Standards and Technology (NIST), is an optimum principle for ensuring a good security posture in complex environments. Zero trust shifts the paradigm by assuming that a breach has already happened and verifying every interaction. Together with strong identity and access management, ZTA aligns with the dynamic nature of Open RAN systems and provides a more robust security framework.

Zero-trust architecture is based on the principle of explicit trust. In this model, no asset in the system is trusted by default based on its location or ownership. It is designed for systems, where one of the assumptions is that the threat actor is already inside the system.

This architecture advocates continuous monitoring and analyzing of network traffic and user activity. When anomalies or suspicious activity are observed, alarms are triggered accordingly. This allows quickly detecting and responding to attacks and taking protective measures to mitigate the risk and recover the system.

In zero-trust architecture, the important **never trust, always verify** principle ensures that subjects can only access the data they are allowed to. Strong user authentication, together with strict access control, ensures the principle of **least privilege**, which significantly reduces the attack surface and prevents lateral movement. This makes it more difficult for threat actors to gain wide access to data.

Nokia's zero-trust architecture, illustrated in Figure 3, encompasses a strategic and holistic approach to cyber security. It helps secure the network by reducing the need to rely on implicit trust. It means that the security solution continuously validates every stage of digital interaction, addressing all threats.

The Nokia zero-trust architecture is based on IEEE, ITU-T, IETF and 3GPP standards on identification, authentication, ciphering and integrity protection and covers all radio access network elements. It follows a phased approach as outlined in the Zero-Trust Maturity Model[7] developed by the U.S. Government's Cybersecurity and Infrastructure Security Agency (CISA).

For end-to-end security, Nokia offers a comprehensive, real-time security operations and security monitoring management system, which covers radio access, transport, and core network domains.

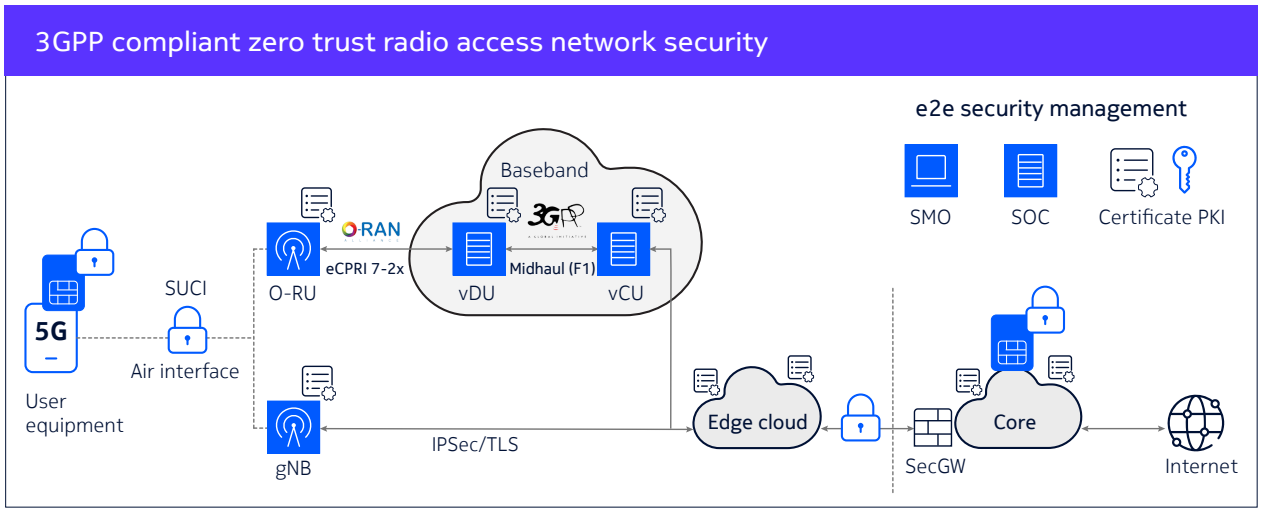

Figure 3. Nokia 5G radio access zero-trust architecture

Supply chain security

Nokia, like many other companies in the technology industry, builds solutions that leverage open source and components from other suppliers. These components may have further dependencies on other sources. This chain of software and hardware components and their use in our products forms a supply chain.

One of the drivers of Open RAN is to add more diversity to the supply chain. The communications infrastructure is critical for modern society, and a broad base of suppliers enhances its resilience. At the same time, it provides more opportunities for attackers to exploit the system and thus increases the attack surface. In a multi-supplier Open RAN system, both the technology solutions and the supply chain are more complex.

The supply chain represents an efficient route to gaining access to and control of target systems. Typical attack techniques that are used to compromise a supply chain include malware infection, social engineering, brute-force attacks, exploiting software vulnerabilities, exploiting configuration vulnerabilities, and leveraging open-source intelligence (OSINT).

Mitigating the risk of attacks requires efficient vendor coordination, as well as systematic and rigorous processes to ensure the end-to-end security of the entire supply chain, including development processes. When considering security from the perspective of a supply chain, it can be simplified into four steps as depicted in Figure 4.

Figure 4. Important steps for supply chain security

Nokia is adopting the Secure Supply Chain Consumption Framework (S2C2F)[8] from Open Source Security Foundation (OpenSSF) to assess the compliance of practices. The S2C2F suggests a set of practices to ensure that the open-source components of the supply chain are from a known source, built in a secure environment and shipped securely.

The OpenChain project defined the ISO/IEC 5230:2020 standard[9] for open-source compliance to ensure that different organizations of the supply chain follow a high-quality open-source compliance process. Nokia's process conforms to the requirements of ISO/IEC 5230:2020, and we have made an announcement about the adoption of this standard.

Identify what you have

Awareness of all the components in a product is critical in building security. A software bill of materials (SBOM)[10] is a key building block in software security and managing software supply chain risks. It is an inventory of the components and their ingredients that together make a product, providing the needed transparency.

SBOM helps identify and manage software supply chain related risks. When created in electronic form, SBOM allows automated vulnerability scanning. Nokia adopts the OpenChain Telco SBOM Guide Version 1.0[11] as the basis of SBOMs we provide to our customers. The OpenChain Telco SBOM Guide was created to ensure that the SBOMs used in the telecom industry are of high standard and that all actors follow the same quality principles.

Know where it comes from

Nokia's world-class supply chain process has been designed to guarantee the highest level of security to ensure business continuity in the short and long term. The process also helps ensure that our products and operations deliver high performance and quality.

Nokia's Third-party Security Risk Management process for suppliers ensures supply chain security and complies with legal and regulatory requirements.

Vendor selection with explicitly defined qualitative criteria is critical and forms the foundation for secure and resilient products and services. Nokia uses rigorous criteria for selecting both the vendors and the open-source software used in our products based on industry best practices and the criteria defined in the Open Source Security Foundation (OpenSSF) Scorecard[12].

The credibility and reliability of the selected sources are secured with automated security checkpoints throughout their life cycle.

Ensure it is shipped securely

Supply chain integrity is also protected during the build phase with stringent source code control and auditing. In its build environment, Nokia uses mirrored sources for open-source and third-party software. All mirrored sources are audited, and access to source repositories prevents man-in-the-middle attacks.

The software built in Nokia's development environment is digitally signed and when it is delivered to installation, its provenance and integrity can be ensured. Nokia's base station products only use signed software components.

Build in a secure environment

Nokia's development infrastructure is secured with stringent access controls and comprehensive audit trails to identify all access rights and any changes to tools in the development environment. All software builds are reproducible and auditable at the source code level, and Nokia conducts frequent audits to identify potential attacks on the supply chain to ensure integrity.

Nokia's products and solutions are secure, complying with industry standards for security and adhering to best industry practices. This helps ensure that the supply chain and all its components are reliable and trusted throughout their entire life cycle, from solution design to end-of-life.

Integrating solutions from multiple suppliers together

Nokia is committed to delivering open, secure, high-performing and interoperable networks. We have a long record of accomplishment in successfully integrating products from multiple suppliers together.

Nokia recognizes the importance of supplier diversity in the Open RAN ecosystem, which can help make the supply base more resilient. However, in an end-to-end solution comprising products from multiple suppliers, any mismatches in functionalities or differences in configurations may expose vulnerabilities and increase the attack surface. These vulnerabilities can be mitigated with a hardening approach where all unused services are disabled, configurations are verified, and access control is validated. This is where the importance of robust system integration comes into the picture.

System integration is a process where products from different suppliers are seamlessly integrated and verified to form a high-performing, resilient and secure end-to-end solution. This rigorous process includes extensive testing and validation, and it is critical in ensuring that the multi-supplier environment works as expected.

The system integration process ensures the quality of the solution and lays down the foundation for end-to-end security. Nokia's leading integration capabilities support customers in deploying and maintaining secure Open RAN networks. Nokia's best-in-class Open RAN Integration Centers in Dallas and Ulm have already demonstrated their excellent capabilities in integrating advanced, high-performance, secure multi-supplier Open RAN systems.

Strong identity and access management

Nokia recommends that CSPs and enterprises conduct thorough due diligence checks of all suppliers and implement strict security controls for all third-party network access to mitigate the risks posed by supply chain threats.

Important radio access network management access security controls include:

- **Multi-factor authentication**: Requiring users to provide two or more verification factors can help prevent unauthorized access to sensitive systems or data.
- **Role-based access control**: Limiting user access to only the resources needed to perform their jobs can help minimize the extent to which a threat actor can penetrate the network.
- **Privileged user monitoring**: Regularly reviewing privileged user activity can help detect and prevent unauthorized actions or data exfiltration.
- **Vulnerability assessments and penetration testing**: Regularly performing vulnerability assessments and penetration tests can help identify and address potential security weaknesses in networks before they can be exploited by threat actors.
- **Verifying parameter changes**: Pre-screening the parameters with a configuration and optimization tool before applying them to the network.

Open RAN Service Management and Orchestration (SMO)

The O-RAN Alliance has defined the SMO framework as an open platform to manage a multi-supplier, multi-technology network. The SMO framework aims to provide intelligent service agility, automation, and operational efficiency as networks are becoming increasingly complex and requirements for on-demand services are surging.

CSPs can pick and choose components for the SMO framework from different suppliers and integrate those together.

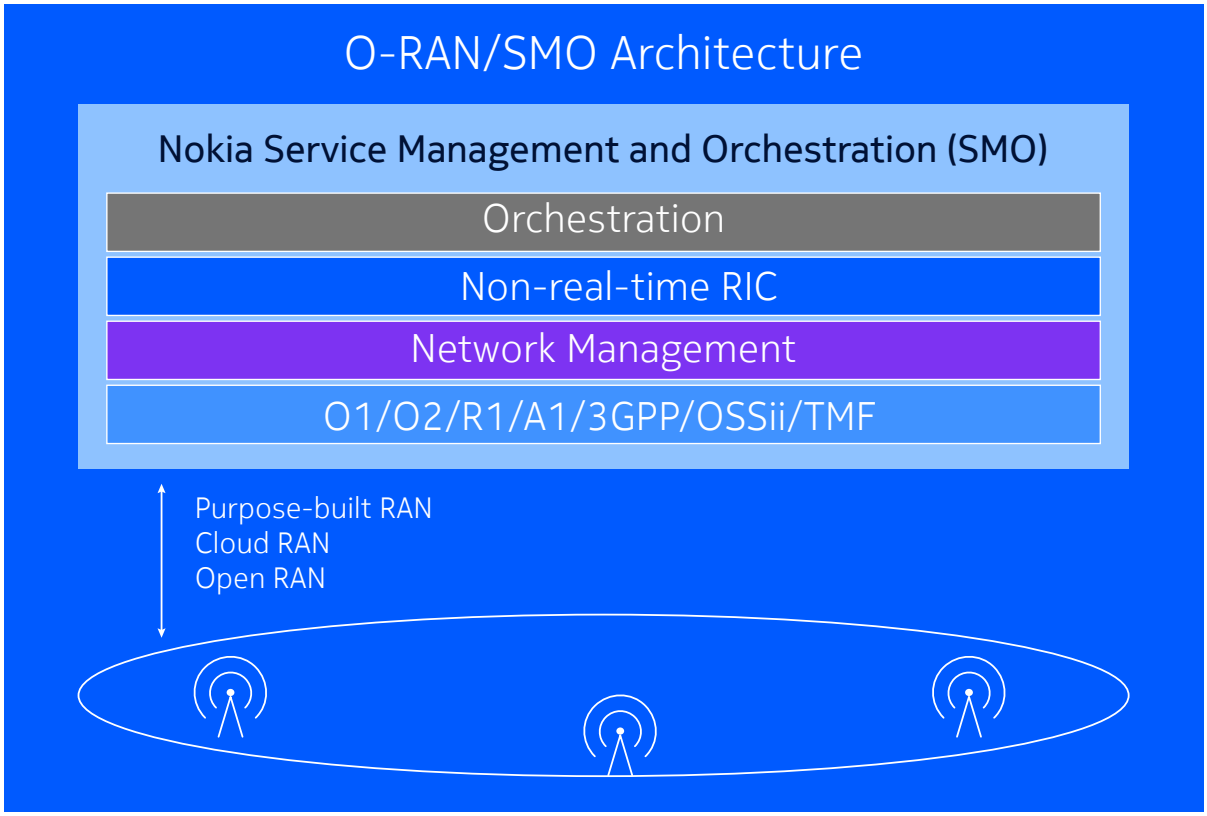

Figure 5. Open RAN Service Management and Orchestration architecture

The Nokia MantaRay solution portfolio includes MantaRay NM for network management, which will be extended with the non-real-time RIC and orchestration capabilities to create the SMO solution.

The functionality and architecture of MantaRay NM are continuously evolving to support the management and optimization of today's networks while seamlessly enabling Open RAN capabilities. Over time, MantaRay NM will include SMO O1, O2 and A1 protocols and security standards.

Besides support for the SMO and O1 interface, Nokia will continue to support the interface from RAN network functions towards MantaRay NM. This enables a low-cost introduction of Open RAN and provides support for any business logic and services that are not yet supported in an Open RAN SMO solution.

MantaRay NM provides a strong identity and access control aligned with the principles of **least privilege** and **never trust**, **always verify**. It is depicted in Figure 6.

MantaRay NM can be seamlessly integrated with third-party identity and access management services and LDAP server. When centralized Network Element User Management is activated on a RAN element, the user authorization and authentication can be managed centrally.

Nokia also supports segmentation with role-based access control, which is key in protecting the system against internal attacks and preventing lateral movement.

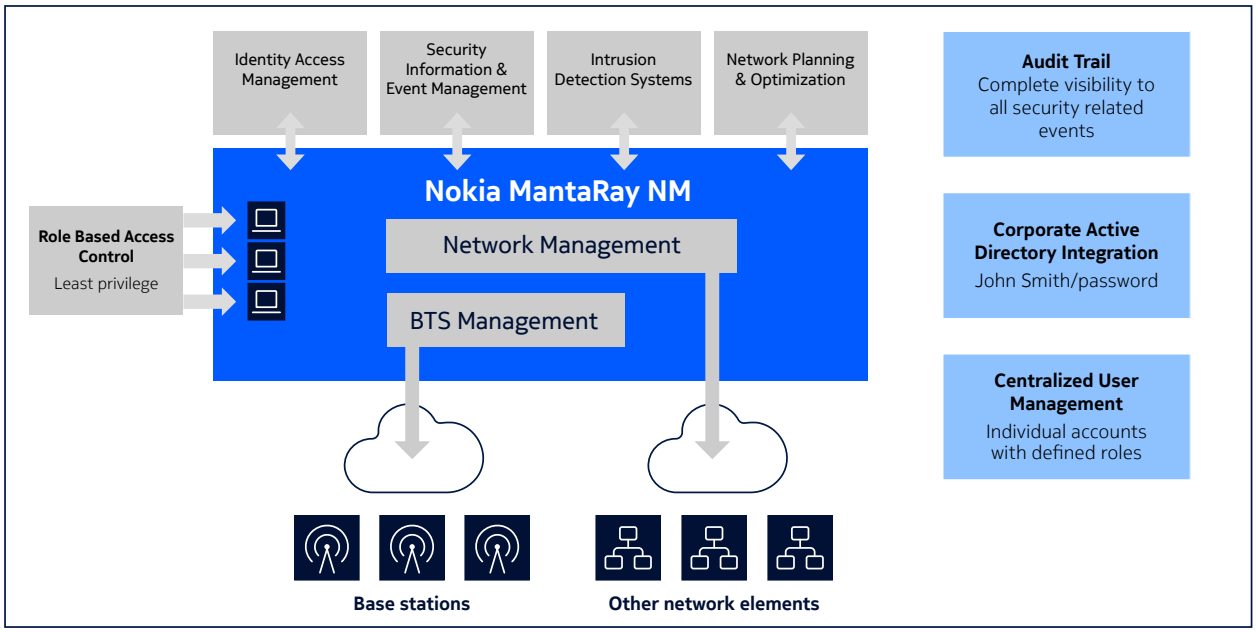

Figure 6. Strong Open RAN identity and access management with Nokia MantaRay NM

Continuous monitoring and auditing

A key principle of the zero-trust architecture is continuous monitoring and auditing.

Nokia MantaRay NM supports continuous monitoring with the Audit Trail Log (ATL) functionality. It provides end-to-end traceability for RAN system events and KPIs in all RAN elements, including radio units, distributed units and centralized units, as well as in the SMO framework.

Incorrect configurations are one of the top causes of system vulnerabilities. MantaRay NM allows monitoring of all security-related configuration changes. Each individual configuration change and the related user identification are reported to the audit trail log, effectively mitigating unintentional configuration drift and unauthorized changes.

The audit trail data can be exposed via the northbound interface (NBI) to the security information and event management solution in the customer environment for longer-term audit trail storage and analysis.

In addition, MantaRay NM monitors system performance to determine if the system is healthy and if there are any anomalies in the network. The rich set of performance data from MantaRay NM can also be transferred to the customer's own system.

Securing data both in transit and at rest

Data confidentiality and integrity are important for both data in transit and data at rest.

Encrypting data at rest ensures that sensitive information remains protected when stored in customer databases or other storage solutions. In the Nokia Open RAN solution, all sensitive data stored in a system is protected according to 3GPP requirements.

Nokia Open RAN complies with the requirements of a secure environment described in 3GPP Technical Specification # 33.501[13]:

- The secure environment shall support secure storage of sensitive data such as long-term cryptographic secrets and vital configuration data.
- The secure environment shall support the execution of sensitive functions such as encryption/decryption of user data and the basic steps within protocols that use long-term secrets (for example, authentication protocols).

- The secure environment shall support the execution of sensitive parts of the boot process.
- The integrity of the secure environment shall be assured.
- Only authorized access shall be granted to the secure environment. This includes the data stored and used within the system and the functions executed within the system.

Encrypting data in transit means protecting the communication between two endpoints. In Nokia Open RAN, all the interfaces are encrypted.

Digital certificates are the key functionality behind authentication and encryption. Nokia PKI certificate authority (CA), based on X.509 provides a reliable and efficient automated solution for managing the certificates throughout their lifetime. Nokia PKI CA uses Certificate Management Protocol version 2 (CMPv2) for consistent and reliable certificate management across the system.

Nokia also protects the confidentiality and integrity of the management-plane interfaces, which use the TLS1.3 or TLS1.2 protocol, with PKI CA and by using mutual TLS (mTLS). Mutual TLS is an enhancement of TLS in which both parties authenticate each other by verifying that both can trust each other.

The O-RAN Alliance has specified TLS as the security solution O1 interface, with endpoints to be authenticated by certificates.

Compliance with security standards

The Nokia Open RAN solution complies with the security standards developed by several standardization bodies, such as 3GPP, the Internet Engineering Task Force (IETF), the European Telecommunications Standards Institute (ETSI), NIST, ISO/IEC and the O-RAN Alliance.

Nokia is the O-RAN Alliance's number one contributor to Open RAN standardization and Open RAN security standardization and a key contributor to the work of 3GPP:

- As an active member of the O-RAN Alliance, Nokia made 17 percent of all the contributions during 2021-2024, more than any other contributor.
- Nokia co-chairs two O-RAN Alliance Next Generation Research Groups, which are addressing Architecture towards 6G O-RAN (RS02) and Native Security (RS04).
- Nokia drove the adoption of the evolved Common Public Radio Interface (eCPRI) based 7-2x fronthaul interface between the open radio units and the open distributed unit as a basis for connecting radio and baseband units of different suppliers.
- Nokia continues to co-chair the O-RAN Alliance's technical work group 4 (WG4), which focuses on creating the specifications for Open Fronthaul interfaces.
- Nokia also co-chairs WG10, which covers the Open RAN specifications related to operations and maintenance.
- Nokia chairs 3GPP's technical work group 3 for Service and System Aspects (SA WG3), which concentrates on security work. The group is responsible for defining 5G security and privacy requirements and specifying the related technology architecture and protocols, including which cryptographic algorithms to use and how.

Nokia also contributes actively to the work of other standardization bodies.

We have adopted 5G security-related technologies, processes, and tools defined in GSMA's Network Equipment Security Assurance Scheme (NESAS). In addition, we have adopted the industry best practices defined by leading security organizations such as the Alliance for Telecommunications Industry Solutions (ATIS), ENISA and the U.S. National Telecommunications and Information Administration (NTIA).

Read more about Nokia's contribution to Open RAN standardization on our webpage.

Conclusion

Most CSPs are expected to gradually evolve their networks towards hybrid deployments with the coexistence of purpose-built RAN, Cloud RAN and Open RAN based on their business strategy. Open RAN needs a robust and comprehensive security architecture and processes that encompass all traffic across signaling, data and application layers also in a multi-supplier environment.

Nokia is committed to making the Open RAN vision a commercial reality, and we are committed to Open RAN security. Nokia Open RAN complies with the 3GPP and O-RAN Alliance standards and industry best practices defined by leading security companies.

The unique Nokia 5G zero-trust architecture is designed to ensure the privacy, security and integrity of any RAN flavor, including Open RAN. It follows the Zero-Trust Architecture (ZTA) model to protect the system from external and internal vulnerabilities.

Nokia's recommendations for communications service providers are based on security practices, which will help our customers enhance their Open RAN security posture and protect their valuable data:

- Trust through verification: we ensure that trust is established explicitly through stringent verification processes.
- Principle of least privilege: we adopt strong identity and account management practices, along with strict role-based access control, to minimize access to only what is necessary.
- Data protection: we safeguard data both in transit and at rest to maintain its confidentiality and integrity.
- Continuous monitoring: we offer tools such as MantaRay NM to enable continuous monitoring and achieve full visibility of the system and data, logging all security-related events.
- Preventing lateral movement: we implement strong, dynamic access control and network segmentation to prevent unauthorized lateral movement within the network.

Nokia's world-class supply chain process has been designed to guarantee the security and integrity of all the Open RAN solution components. Through our stringent development and verification processes, we ensure the highest performance, robustness, energy efficiency, security and resiliency for an Open RAN system.

Glossary

AI	Artificial Intelligence
APT	Advanced Persistent Threat
ATIS	Alliance for Telecommunications Industry Solutions
ATL	Audit Trail Log
CA	Certificate Authority
CISA	Cybersecurity and Infrastructure Security Agency
CMP	Certificate Management Protocol
CSP	Communications Service Provider
CTI	Cyber Threat Intelligence
DDoS	Distributed Denial of Service
DFSEC	Design for Security
GSMA	GSM Association
GTP	GPRS Tunnelling Protocol
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
IETF	Internet Engineering Task Force
IEC	International Electrotechnical Commission
IoT	Internet of Things
IPsec	IP Security Architecture
ISO	International Organization for Standardization
LTE	Long Term Evolution
mTLS	Mutual Transport Layer Security
NBI	Northbound Interface
NESAS	Network Equipment Security Assurance Scheme
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
NVD	National Vulnerability Database
OpenSSF	Open Source Security Foundation
OSINT	Open-Source Intelligence
OTIC	Open Testing and Integration Center
PKI	Public Key Infrastructure
RAN	Radio Access Network
RIC	RAN Intelligent Controller
RS	Research Group
RU	Radio Unit
S2C2F	Secure Supply Chain Consumption Framework
SBOM	Software Bill of Materials
SMO	Service Management and Orchestration
SOC	Security Operations Center
SQL	Structured Query Language
SSH	Secure Shell Protocol
SUCI	Subscriber Concealed Identifier
3GPP	Third Generation Partnership Project
T-ISAC	Telecommunication Information Sharing and Analysis Center
TLS	Transport Layer Security
UMTS	Universal Mobile Telecommunications System
VES	Virtual Function Event Streaming
WG	Working Group
ZTA	Zero-Trust Architecture
ZTMM	Zero-Trust Maturity Model

References

1. Nokia (2024). White Paper: Nokia Open RAN Industry and Solution Update.
   https://onestore.nokia.com/asset/213914
2. Nokia (2024). Threat Intelligence Report 2024.
   https://onestore.nokia.com/asset/214202
3. NIS Cooperation Group (2022). Report on the cybersecurity of Open RAN.
   https://ec.europa.eu/newsroom/dae/redirection/document/86603
4. ENISA (2021). Threat Landscape for Supply Chain Attacks.
   https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
5. Nokia (2023). Design for Security (DFSEC).
   https://www.nokia.com/sites/default/files/2023-04/dfsec_introduction.pdf
6. NIST (2020). SP 800-207 Zero Trust Architecture.
   https://csrc.nist.gov/pubs/sp/800/207/final
7. CISA (2023). Zero Trust Maturity Model.
   https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model
8. Open Source Security Foundation (2022-2024). Secure Supply Chain Consumption Framework (S2C2F) Simplified Requirements.
   https://github.com/ossf/s2c2f/blob/main/specification/framework.md
9. OpenChain (2020). ISO/IEC 5230:2020 standard specification.
   https://www.iso.org/standard/81039.html
10. CISA. Software Bill of Materials.
    https://www.cisa.gov/sbom
11. OpenChain (2024). OpenChain Telco SBOM Guide Version 1.0.
    https://github.com/OpenChain-Project/Reference-Material/blob/master/SBOM-Quality/Version-1/OpenChain-Telco-SBOM-Guide_EN.md
12. OpenSSF. OpenSSF Scorecard - Security health metrics for Open Source.
    https://github.com/ossf/scorecard
13. 3GPP (2018). Technical Specification 33.501.
    https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

Further reading

- Report: Open RAN Security Report, NTIA
- Webpage: ATIS Standards and Specifications
- Webpage: EU 5G Toolbox
- Webpage: O-RAN Alliance Security Focus Group
- Nokia White Paper: 5G mobile radio network security challenges and opportunities
- Nokia White Paper: Security in the quantum era: Evaluating post-quantum solutions

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID: 214354

nokia.com

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs, which is celebrating 100 years of innovation.

With truly open architectures that seamlessly integrate into any ecosystem, our high-performance networks create new opportunities for monetization and scale. Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.