The O-RAN ALLIANCE Security Working Group Continues to Advance O-RAN Security

PDF version of the O-RAN ALLIANCE web announcement
Published on February 9, 2024

O-RAN ALLIANCE e.V., Buschkauler Weg 27, 53347 Alfter, Germany
Register of Associations, Bonn VR 11238, VAT ID DE321720189

The O-RAN ALLIANCE Security Working Group Continues to Advance O-RAN Security

This is the fourth annual O-RAN security blogpost from the O-RAN ALLIANCE's Security Working Group, also referred to as WG11, describing the current state and plans for O-RAN security.

2023 was a successful year for the O-RAN ALLIANCE Security Working Group. O-RAN security specifications were enhanced with new requirements and controls that bring O-RAN closer to a zero trust architecture (ZTA). Updates to the security specifications enable mobile network operators to operate an Open RAN that meets and exceeds industry expectations for an open, interoperable, and secure system. 2023 also saw a significant increase in the number of security test cases in the security test specification used to verify compliance with the O-RAN security standards.

The O-RAN ALLIANCE Security Working Group is defining a secure O-RAN architecture that includes architectural elements, network functions, interfaces, and data, in collaboration with the other O-RAN ALLIANCE working groups. Figures 1 and 2 show the O-RAN detailed and abstract architecture views for the O-RAN defined interfaces (A1, O1, O2, E2, Y1 and Open Fronthaul) and architectural elements (SMO, Non-Real Time RIC, Near-Real Time RIC, O-CU-CP, O-CU-UP, O-DU, O-RU, O-eNB, and O-Cloud). New in these diagrams are the external interfaces for the SMO to import AI enrichment data and the Y1 interface used by the Near-Real Time RIC to communicate O-RAN analytics with consumers external to the O-RAN ecosystem.

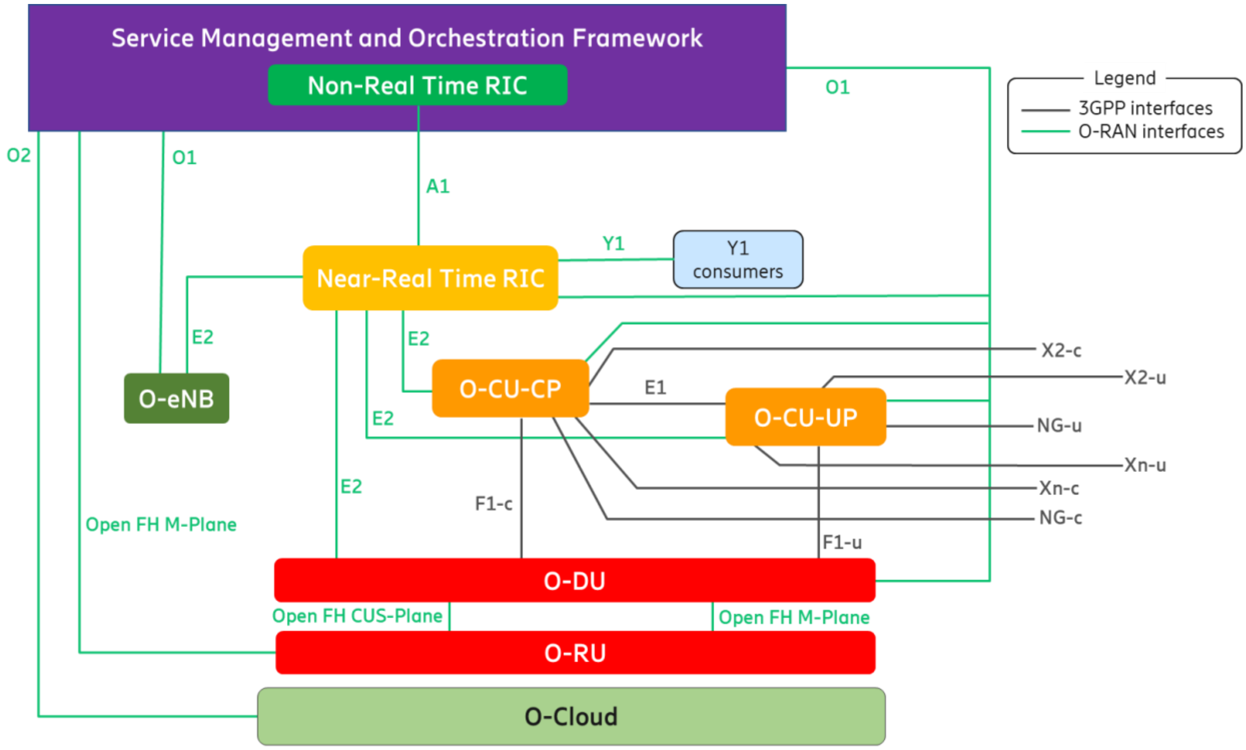

Figure 1 Logical Architecture of O-RAN [1]

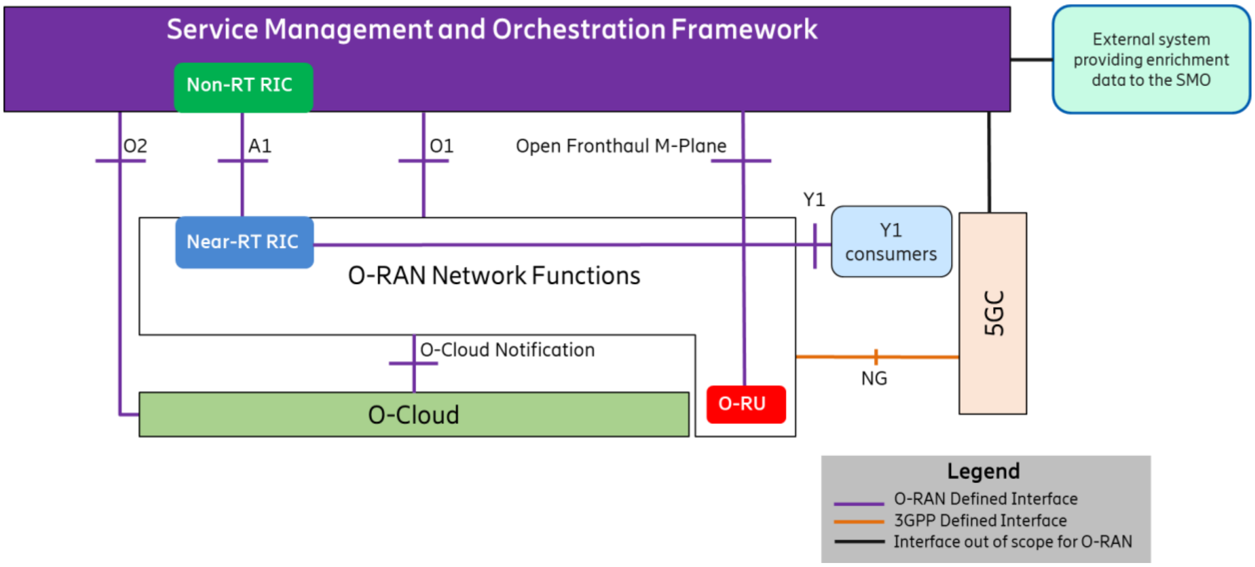

Figure 2 High Level Architecture of O-RAN [1]

O-RAN ALLIANCE is on the ZTA Journey

ZTA is a new security paradigm in which perimeter security alone is insufficient as human and digital subjects inside the perimeter cannot be assumed to be trusted. In a ZTA, each asset needs to be secured as a micro-perimeter. The O-RAN ALLIANCE is strengthening O-RAN's security posture by specifying security requirements and security controls that mitigate risk from external and internal threats in pursuit of a ZTA. The Security Working Group has kicked off an initiative to ensure that ZTA is built into O-RAN's security specifications. Each security work item team performs threat modeling and risk assessment with consideration of a ZTA, as defined in NIST SP 800-207 [2], using a risk-based approach to specify controls to protect against internal and external threats.

NIST defines seven tenets of zero trust that can be summarized with the following four principles guiding O-RAN security specifications:

- Network functions and architectural elements are resources secured as micro-perimeters.
- Trust is not assumed for any subject, whether human user or network asset, attempting to access a resource. Authentication and authorization are enforced on a per-session basis 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 and enforce dynamic security policies.

Achieving a ZTA is a journey. The United States Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has provided a Zero Trust Maturity Model (ZTMM) [3] with incremental stages to achieve a ZTA. The O-RAN ALLIANCE is continuing to pursue a ZTA in incremental stages as the O-RAN architecture, threats, and controls evolve. O-RAN security specifications are developed using a risk-based approach guided by Microsoft STRIDE threat modelling [4]. Significant progress has been made through 2023 and further work will progress through 2024 toward achieving the goal of a ZTA.

The Security Working Group will provide further analysis of ZTA for O-RAN in its forthcoming technical paper scheduled for publication at MWC Shanghai in June 2024. The paper will provide an analysis of the NIST 7 tenets of zero trust, the applicability of each tenet to O-RAN, and the security roadmap with a phased approach to achieve a ZTA.

O-RAN ALLIANCE Security Working Group

The Security Working Group's work is captured in three security specifications and a technical report that form the pillars of O-RAN security. These four pillar documents, as listed below, can be downloaded from the O-RAN ALLIANCE's public website at O-RAN Specifications [5].

- *O-RAN Security Threat Modeling and Risk Assessment 2.0* [6] – a risk-based threat model and analysis used for building an effective O-RAN security architecture that supports zero trust.
- *O-RAN Security Requirements and Controls Specifications 8.*0 [7] – security requirements for each O-RAN interface and component. Requirements address confidentiality, integrity, and availability by defining key controls such as authentication, authorization, replay protection, least privilege access control, and logging.
- *O-RAN Security Protocols Specifications 8.0* [8] – defines implementation requirements for security protocols used by O-RAN including SSH, IPSec, DTLS, TLS 1.2+, OAuth 2.0, SFTP, FTPES, and HTTPS.
- *O-RAN Security Tests Specifications 6.0* [9] – documents the security tests that validate O-RAN implementations of security functions, configurations, and security protocols requirements.

The Security Working Group has the following thirteen active security work items to ensure the evolving O-RAN architecture is secure:

- SMO Security
- Near-RT RIC Security
- O-Cloud Security
- AI/ML Security
- Open Fronthaul Security
- Shared O-RU Security
- O-RU Centralized User Management
- Certificate Management
- O-RAN OAuth 2.0 Framework
- Application Lifecycle Management
- Security Log Management
- Security Testing
- ZTA Framework

The accomplishments and future direction of each of the work items are discussed further below.

O-RAN Security Work Items

SMO Security

Service Management and Orchestration (SMO) is an O-RAN architectural element that includes SMO Services (SMOS), Non-Real-Time RIC, rApps, R1 interfaces, and internal SMOS Communications. The SMO is a high-risk target for attack because of its management role and interfaces across the entire O-RAN architecture. The work item team has produced security specifications consistent with a ZTA to protect internal and external SMO communications and the data-at-rest and in-transit. Security controls are specified to ensure confidentiality, integrity, availability, and authenticity protection. Further work will be performed in 2024 to specify security requirements and controls for the new SMO Service-Based Architecture and data exposure to external systems.

Near-RT RIC Security

The Near-Real Time RAN Intelligent Controller (Near-RT RIC) provides intelligence and optimization for the RAN by executing near-real time control functions. A security analysis of the Near-RT RIC is crucial for ensuring the overall security of an O-RAN system since it plays a key role in managing and optimizing network operations, which can have significant implications on user experience and data privacy.

This work item has identified key issues and proposed solutions for the security of the Near-RT RIC. Based on this work security requirements and -controls for the Near-RT RIC internal APIs, external interfaces, the xApps, and the platform itself have been defined, and related test cases created. In the future the work item group will continue to support the ongoing work on the Near-RT RIC with further security analysis and related specification work.

O-Cloud Security

O-Cloud security is foundational to O-RAN security as O-RAN Cloud-Native Functions (CNFs) run on O-Cloud infrastructure specified by the O-RAN ALLIANCE. O-RAN made significant strides in O-Cloud security by defining new requirements for mandatory support of multi-factor authentication, workload isolation, ingress/egress restrictions, rate limiting, signature validation for secure updates, secure storage erasure, time synchronization across cloud components, and cloud instance identification that assigns unique, randomized identifiers to all cloud components such as VMs, pods, containers, and compute pools. Cloud instance identification is critical to MNO's managing their deployed O-RAN inventory. The work item team will continue to advance O-Cloud security requirements throughout 2024.

AI/ML Security

O-RAN strives to leverage artificial intelligence and machine learning (AI/ML) to operate network resources automatically and efficiently for diverse use cases such as performance optimization, sustainability, and anomaly detection. While AI/ML can provide great benefits to O-RAN, it is also an attack vector that can be exploited by adversaries. The goal of this work item is to secure AI/ML across the O-RAN architecture, including the SMO, Non-RT RIC, Near-RT RIC, rApps, and xApps. The work item team is in the process of completing threat modeling assessment and will then form security requirements to protect against potential AI/ML attacks in O-RAN.

Open Fronthaul Security

The Security Working Group added PKI-based mTLS to the M-Plane and will continue to work with other O-RAN Alliance working groups to secure the C-Plane with confidentiality and integrity protection and S-Plane with authenticity protection. MACsec is currently being studied for the C-Plane and IEEE 1588 Security TLV is being studied for the S-Plane.

Shared O-RU Security

Shared O-RU is an operational configuration in which an O-RAN operator can host enterprise customers, referred to as single operator, or other operators, referred to as multi-operator. This introduces a multi-tenant environment and new threats of unauthorized parties accessing architectural elements and data. The Security Working Group has added new requirements and controls to ensure Shared O-RU deployments are secure for confidentiality, integrity, availability, and authenticity. In 2024, WG11 will continue its security analysis of Shared O-RU use cases, in collaboration with other O-RAN Alliance working groups, and form normative security requirements for resiliency, resource partitioning, performance management, resets, software versioning, and other use cases.

O-RU Centralized User Management

This work addresses user management and role-based access control for management interfaces on the O-RU. The mapping from user to role can be made locally in each unit or centrally. O-RAN WG11 has earlier defined requirements on centralized user management for the O1 interface and is now working on the same for M-Plane.

Certificate Management

O-RAN WG11 is studying and specifying a certificate management framework to make security associations across the entire O-RAN system and to enable zero touch automation for O-RAN operations, administration, and maintenance. This framework supports security associations for TLS 1.2 and TLS 1.3 employed by O1, O2, A1, and other interfaces as well as IEEE 802.1X port-based network access control for point-to-point LAN segments in the Open Fronthaul. 3GPP specifies a certificate management framework based on IETF CMPv2 for creating security associations, the O-RAN certificate management framework supports CMPv2 as well. O-RAN is evaluating alternatives to CMPv2 as part of the industry evolution of certificate management that includes IETF ACME, IETF BRSKI, and IETF EST.

OAuth 2.0

OAuth2.0 plays an important role for O-RAN by providing a common authorization framework for all the O-RAN architecture elements and REST-based interfaces such as R1, O1, O2, A1, Y1. The OAuth2.0 security work item will specify the procedure flow for token registration, token request, token verification, and token authorization. In 2024, the work item will complete a detailed study of existing industry standards and O-RAN specifications that will be used to form requirements for O-RAN’s use of authorization with authenticated access token mechanisms.

Application Lifecycle Management

Application lifecycle management security is an important part of O-RAN security and essential to achieve a ZTA. This work item has identified threats and solutions for the security of applications and added normative security requirements for areas such as application packages, updates, decommissioning, identifiers, and security descriptors. In 2024, the work item will continue to advance application security and add security test cases for the application lifecycle management security requirements.

Security Log Management

Security event logging and secure log management are pillars of security, forming the backbone of audit and zero trust monitoring. Secure logs enable an operator to respond to anomalous behavior in near-real-time, analyze log data for expected as well as unexpected behavior, and perform forensic analysis. In 2023, the Security Working Group published security event and secure log management requirements, controls, and tests.

Security Testing

This work item is responsible for maintaining the *O-RAN Security Tests Specifications 6.0* [9]. The O-RAN ALLIANCE has set the goal for the security test specification to serve as the basis for O-RAN security certifications to be performed on O-RAN architectural elements by OTICs and authorized certification organizations. WG11 is currently engaged with GSMA to establish an O-RAN NESAS. The security test specification will serve in a role like the 3GPP SCAS documents.

The remainder of this post provides a synopsis of the current state of O-RAN security requirements, controls, and tests with 2023 updates **bolded**. The plan for 2024 concludes the blog.

Interface Security Controls

Table 1 is a snapshot of the interface security controls enforcing authenticity, confidentiality, integrity, authorization, data origination, and replay prevention. The notable 2023 addition is optional IEEE 802.1X [10] support for the Open Fronthaul. The other protocols listed in Table 1 are mandatory for the vendor to support and optional for the operator to use, as regional regulatory requirements may differ. Detailed requirements can be found in [7] and [8].

Security Control	Non-Fronthaul					Open Fronthaul			
	A1	O1	O2	E2	**Y1**	C-plane	U-plane	S-plane	M-plane
Authenticity	mTLS	mTLS	mTLS	IPsec	mTLS	**802.1X**	**802.1X**	**802.1X**	mTLS/SSH/**802.1X**
Confidentiality	TLS	TLS	TLS	IPsec	TLS		PDCP		TLS/SSH
Integrity	TLS	TLS	TLS	IPsec	TLS		PDCP		TLS/SSH
Authorization	OAuth	NACM	OAuth		OAuth	**802.1X**	**802.1X**	**802.1X**	NACM/**802.1X**
Data Origination	mTLS	mTLS	mTLS	IPsec	mTLS				TLS/SSH
Replay Prevention	TLS	TLS	TLS	IPsec	TLS		PDCP		TLS/SSH

Table 1 Mandatory O-RAN interface security controls

Authorization for the E2 interface is being developed in collaboration with the Near-Real Time RIC and E2 interface work group. Confidentiality and integrity protection on the Open Fronthaul C-Plane and authenticity protection on the Open Fronthaul S-Plane are being developed in collaboration with the

Open Fronthaul and Transport working groups. PDCP requirements are specified by the 3GPP in TS 33.501.

Cross-Platform or Transversal Requirements

Cross-platform or transversal requirements apply to all O-RAN architectural elements and interfaces. 2023 introduced security requirements for secure deletion of data, application decommissioning, security log management, certificate management, application security, and trust anchor provisioning. Table 2 lists the mandatory O-RAN requirements for each category of transversal requirements, with details provided in [2].

Category	Mandatory Requirements
Application Lifecycle Management	• Application signing by vendor • Signature validation by SMO • **Secure deletion of sensitive data** • **Secure decommissioning of applications**
Network Protocols and Services	• **Provider documentation of all required network protocols/services** • **Default disabling of unused network protocols/services**
Robust Protocol Implementation	• Handle unexpected inputs without functional compromise
Robustness of OS and Applications	• Known vulnerabilities in the OS and applications be documented by their providers
Password based Authentication	• Mitigate risks from password authentication attacks where password authentication is implemented
Software Supply Chain Security	• Vendor signed, NTIA compliant SBOM with every O-RAN software delivery.
Security Log Management	• **Identification of security events to log** • **Collection of security logs by all O-RAN elements** • **Least privileged access controls on security logs** • **Logging of anomalous events** • **Confidentiality and integrity protection of log data at rest and in transit** • **Rotation of logs to prevent data loss** • **Use of Micro-perimeters to protect logs** • **Time stamping of all logged events** • **Inclusion of identity of O-RAN element generating event**
Certificate Management Framework	• **Support of CMPv2**
API Security	• **Support of OWASP API Project security** • **Support of certificate-based authentication using mTLS 1.2+** • **Confidentiality and integrity protection of data in transit with TLS 1.2+** • **Least privileged authorization using OAuth 2.0** • **Input validation**
Trust Anchor Provisioning	• **Pre-provisioning of certificates that chain back to a vendor or operator CA in PNFs**

Table 2 O-RAN Cross-Platform Security Requirements

Security Tests

2023 saw the addition of tests for NACM, 802.1X, eCPRI, SCTP, REST, input validation, secure configuration, logging, open fronthaul, O1, O2, E2, Y1, SMO internal communications, SMO external communications, and O-Cloud.

O-RAN Component	Tests
Security Protocols	• SSH • TLS 1.2, TLS 1.3 • DTLS 1.2 • IPSec • OAuth 2.0 • **NACM** • **802.1X** • **X.509 Digital Certificates** • **eCPRI** • **SCTP**
RESTful APIs	• **Authentication** • **Authorization** • **Input Validation** • **Logging**
Common Network Security	• Network Protocol and Service Enumeration • Password Guessing, Unauthorized Password Reset, Password Policy Enforcement • Network Protocol Fuzzing • **Robustness against Volumetric DDoS: O-CU-CP, O-CU-UP, O-DU, O-RU, Near-Real-Time RIC** • **Input Validation and Error Handling: O-CU-CP, O-CU-UP, O-DU, Near-Real-Time RIC** • **Secure configuration verification: O-CU-CP, O-CU-UP, O-DU, O-RU, Near-Real-Time RIC** • **Logging and monitoring: O-CU-CP, O-CU-UP, O-DU, O-RU, Near-Real-Time RIC**
System Security evaluation	• System Vulnerability Scanning • **System logging: Log Format and Fields, Authenticated Time Stamping, System Security Events, Application Security Events, Data Access Security Events, Account and Identity Security Events, General Security Events, Log Storage**
Software Security Evaluation	• SBOM: Signature, Data Fields, Format, Depth, **Completeness, Version, Vulnerability Cross Check, Delivery, O-RAN Software Community (OSC)** • Software Image Signing: Software Image/Application Package Signing, Software Signature Verification
ML security validation	
O-RAN interfaces	• Open Fronthaul Point-to-Point LAN Segment

	• **Y1: Authenticity, Confidentiality, Integrity, Anti-replay, Authorization** • **O1, O2, OFH M-Plane: Authenticity, Confidentiality, Integrity, Anti-replay, Authorization** • **OFH C/U/S/M-Plane: 802.1X Authenticity, Authorization** • **E2: Authenticity, Confidentiality, Integrity, Anti-replay** • **OFH S-Plane: Master clock DoS protection, Spoofing Prevention for Master Clock, Clock Accuracy Protection Against MITM Attacks**
x/rApp	• Signing • rApp Authorization
SMO	• **Internal Communication** • **External Interfaces** • **Logging**
O-Cloud	• Virtualization Layer: Authenticity, Authorization • Network Connections Allowed/Blocked by Network Policies • Exploitation of O-Cloud Component Vulnerabilities • **O-Cloud Privilege Escalation Prevention** • **Application instantiation by O-Cloud: Signature Verification** • **Resource Management and enforcement in O-Cloud: Resource Consumption Limits, Storage Volume Limits, CPU Overcommit Prevention, Memory Overcommit Prevention, Network Overcommit Prevention, Storage Overcommit Prevention** • **Secure Update: Infrastructure Software Package Integrity, Secure Update procedure, Secure Update failure**
VNF/CNF	• **Executive Environment Protection** • **Signature Validation** • **Application Image Deployment Security**
Common Application Lifecycle Management	• Application package signature verification

Table 3 Security Tests

2024 O-RAN Security Specifications Roadmap

In 2024 the Security Working Group will focus on completing security requirements for the decoupled SMO, Near Real-Time RIC, MACSec for the Open Fronthaul, certificate management for CNFs/VNFs, AI/ML, O-RU centralized user management and O-Cloud. Table 4 provides a quick reference of the new security work underway and how it will improve O-RAN security. This work will be performed with consideration of external and internal threats with the goal of achieving a ZTA.

Category	Description
SMO	• Develop security requirements for SMO Services in a Service-Based Architecture • Identify risks with external data consumers and specify additional security requirements for external interfaces

Near-RT RIC and xApps	• Specify authorization requirements for the E2 interface. • Identify risks to the Near-RT RIC platform via external interfaces for RAN analytics information exposure
Fronthaul C/U/S Planes	• Study MACSec requirements for improved security of the Open Fronthaul.
Automated Certificate Management Framework	• Specify a comprehensive framework for automated X.509v3 certificate management based on CMPv2 and ACME for CNFs/VNFs.
AI/ML Security	• Study the threats to AI/ML. • Develop controls to protect against attacks on AI/ML used in O-RAN architectural elements.
O-RU Centralized User Management	• Study centralized user management for O-RU's.
O-Cloud	• Define requirements for O-Cloud software deployment admission control mechanism. • Define requirements for the hardening of container orchestration environments.
Security Test Specifications	• Continue to close gaps in tests for security requirements and controls.
Risk Assessment	• Update the risk assessment to ensure that the security requirements and controls remain effective. • Demonstrate how the security requirements and controls effectively mitigate the O-RAN security risks.

Table 2 2024 Planned Security Specification Activities

Conclusion

WG11, O-RAN's Security Working Group, will continue to define practical, testable security requirements that support the O-RAN ALLIANCE's vision of a fully open, intelligent, and secure RAN that aligns with a ZTA. As the specifications mature, the journey to ETSI publication will also continue.

References

[1] O-RAN Architecture Description (OAD), version 11.0, O-RAN Alliance, February 2024.

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

[3] Zero Trust Maturity Model (ZTMM), version 2.0, US DHS CISA, April 2023.

[4] STRIDE Threat Model, Microsoft, Threats - Microsoft Threat Modeling Tool - Azure | Microsoft Learn, last visited January 3, 2024.

[5] O-RAN Specifications download website, O-RAN Alliance, O-RAN Specifications.

[6] O-RAN Security Threat Modeling and Risk Assessment, version 2.0, O-RAN Alliance, February 2024.

[7] O-RAN Security Requirements and Controls Specifications, version 8.0, O-RAN Alliance, February 2024.

[8] O-RAN Security Protocols Specifications, version 8.0, O-RAN Alliance, February 2024.

[9] O-RAN Security Tests Specifications, version 6.0, O-RAN Alliance, February 2024.

[10] "IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control," IEEE Std 802.1X-2020 (Revision of IEEE Std 802.1X-2010 Incorporating IEEE Std 802.1Xbx-2014 and IEEE Std 802.1Xck-2018), 28 Feb. 2020, doi: 10.1109/IEEESTD.2020.9018454.