ETSI TS 104 104 V9.1.0 (2025-06)

Publicly Available Specification (PAS); O-RAN Security Requirements and Controls Specifications (O-RAN.WG11.SecReqSpecs-R003-v09.01)

CAUTION

The present document has been submitted to ETSI as a PAS produced by O-RAN Alliance and approved by the ETSI Technical Committee Mobile Standards Group (MSG).

Reference
DTS/MSG-001158

Keywords
control, O-RAN, PAS, requirements, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by O-RAN Alliance and approved by ETSI Technical Committee Mobile Standards Group (MSG).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document specifies the Security Requirements and appropriate Security Controls per O-RAN interface and per O-RAN component.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are necessary for the application of the present document.

[1] Void.

[2] ETSI TS 103 982: "Publicly Available Specification (PAS); O-RAN Architecture Description (O-RAN.WG1.OAD-R003-v08.00)".

[3] O-RAN ALLIANCE TS: "O-RAN Security Protocols Specification".

[4] O-RAN ALLIANCE TR: "O-RAN Security Threat Modeling and Risk Assessment".

[5] O-RAN ALLIANCE TS: "O-RAN A1 interface: Transport Protocol".

[6] O-RAN ALLIANCE TS: "O-RAN O2 General Aspects and Principles".

[7] O-RAN ALLIANCE TS: "O-RAN Near-Real-time RAN Intelligent Controller Architecture & E2 General Aspects and Principles".

[8] O-RAN ALLIANCE TS: "Cloud Platform Reference Designs".

[9] Void.

[10] IETF RFC 8341: "Network Configuration Access Control Model".

[11] IETF RFC 4513: "Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms".

[12] IEEE Std 802.1X™-2020: "IEEE Standard for Local and Metropolitan Area Networks -- Port-Based Network Access Control", (Revision of IEEE Std 802.1X™-2010 Incorporating IEEE Std 802.1Xbx™-2014 and IEEE Std 802.1Xck™-2018), pp. 1-289, 28 February 2020, doi: 10.1109/IEEESTD.2020.9018454.

[13] ETSI TS 103 859: "Publicly Available Specification (PAS); O-RAN Fronthaul Control, User and Synchronization Plane Specification v12.01; (O-RAN.WG4.CUS.0-R003-v12.01)".

[14] ETSI TS 104 023: "Publicly Available Specification (PAS); O-RAN Fronthaul Management Plane Specification v12.01; (O-RAN.WG4.MP.0-R003-v12.01)".

[15] "O-RAN Deployment Scenarios and Base Station Classes For White Box Hardware 2.0", July 2020 (ORAN-WG7.DSC.0-v02.00).

[16] O-RAN ALLIANCE TS: "O-RAN Operation and Maintenance Architecture".

[17] U.S. DoC and NTIA: "The Minimum Elements for a Software Bill of Materials (SBOM), Pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity", July 2021.

[18] The System Package Data Exchange™ (SPDX®).

[19] CycloneDX.

[20] NISTIR 8060: "Guidelines for the Creation of Interoperable Software Identification (SWID) Tags", David Waltermire et al., U.S. NIST, 2016.

[21] ISO/IEC 5962:2021: "Information technology — SPDX® Specification V2.2.1", August 2021.

[22] IETF RFC 2865: "Remote Authentication Dial In User Service (RADIUS)".

[23] IETF RFC 2866: "RADIUS accounting".

[24] IETF RFC 2869: "RADIUS Extensions".

[25] IETF RFC 4072: "Diameter Extensible Authentication Protocol (EAP) Application".

[26] O-RAN ALLIANCE TS: "Xhaul Packet Switched Architectures and Solutions".

[27] IEEE 1588™-2019: "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems".

[28] IETF RFC 7384: "Security Requirements of Time Protocols in Packet Switched Networks".

[29] ETSI TS 133 511: "5G; Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class (3GPP TS 33.511)".

[30] O-RAN ALLIANCE TS: "Synchronization Architecture and Solution Specification".

[31] O-RAN ALLIANCE TS: "O-RAN Control, User, and Synchronization Plane Specification".

[32] ETSI TS 138 323: "5G; NR; Packet Data Convergence Protocol (PDCP) specification (3GPP TS 38.323)".

[33] O-RAN ALLIANCE TS: "Near-RT RIC Architecture".

[34] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[35] Void.

[36] Void.

[37] O-RAN ALLIANCE TS: "Non-RT RIC Architecture".

[38] Void.

[39] O-RAN ALLIANCE TS: "R1 interface: General Aspects and Principles".

[40] Void.

[41] ETSI GS NFV-SEC 021: "Network Functions Virtualisation (NFV); Security; VNF Package Security Specification".

[42] ETSI GS NFV-SOL 004: "Network Functions Virtualisation (NFV); Protocols and Data Models; VNF Package and PNFD Archive specification".

[43] ETSI GS NFV-IFA 011: "Network Functions Virtualisation (NFV); Management and Orchestration; VNF Descriptor and Packaging Specification".

[44] 3GPP TR 33.848: "Study on Security Impacts of Virtualisation".

[45] 3GPP TR 33.818: "Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualised network products".

[46] US NSA ESF and US DHS CISA: "Security Guidance for 5G Cloud Infrastructures, Part I: Prevent and Detect Lateral Movement", page 5, October 2021.

[47] Void.

[48] Void.

[49] ETSI GR NFV-SEC 018 (V1.1.1): "Network Functions Virtualisation (NFV); Security; Report on NFV Remote Attestation Architecture".

[50] DoD 5220.22-M: "Data sanitization method".

[51] Kubernetes® Documentation: "Encrypting Confidential Data at Rest".

[52] Federal Information Processing Standards Publication (FIPS PUB) 140-3: "Security Requirements for Cryptographic Modules".

NOTE: "Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program".

[53] TPM 2.0 Library.

[54] ETSI GR NFV-SEC 003 (V12.1): "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".

[55] ETSI TS 133 501: "5G; Security architecture and procedures for 5G System (3GPP TS 33.501)".

[56] ETSI TS 133 401: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture (3GPP TS 33.401)".

[57] ISO/IEC 27000:2018: "Information technology — Security techniques — Information security management systems — Overview and vocabulary".

[58] NIST SP 800-92: "Guide to Computer Security Log Management".

[59] Void.

[60] IETF RFC 5905: "Network Time Protocol Version 4: Protocol and Algorithms Specification".

[61] IETF RFC 3339: "Date and Time on the Internet: Timestamps".

[62] ISO 86001: "Date and time — Representations for information interchange".

[63] IETF RFC 8915: "Network Time Security for the Network Time Protocol".

[64] IETF RFC 5424: "The Syslog Protocol".

[65] IETF RFC 5425: "Transport Layer Security (TLS) Transport Mapping for Syslog".

[66] O-RAN ALLIANCE TS: "Y1 interface: General Aspects and Principles".

[67] NIST SP800-162: "Guide to Attribute Based Access Control (ABAC) Definition and Considerations".

[68] NIST SP800-122: "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)".

[69] IETF RFC 8366: "A Voucher Artifact for Bootstrapping Protocols".

[70] IETF RFC 8995: "Bootstrapping Remote Secure Key Infrastructure (BRSKI)".

[71] IETF RFC 8572: "Secure Zero Touch Provisioning (SZTP)".

[72] ETSI TS 128 314: "5G; Management and orchestration; Plug and Connect; Concepts and requirements (3GPP TS 28.314)".

[73] ETSI TS 128 315: "5G; Management and orchestration; Plug and Connect; Procedure flows (3GPP TS 28.315)".

[74] ETSI TS 128 316: "5G; Management and orchestration; Plug and Connect; Data formats (3GPP TS 28.316)".

[75] NIST SP 800-88: "Guidelines for Media Sanitization".

[76] ETSI TS 133 117: "Universal Mobile Telecommunications System (UMTS); LTE; 5G; Catalogue of general security assurance requirements (3GPP TS 33.117)".

[77] IETF RFC 4122: "A Universally Unique IDentifier (UUID) URN Namespace".

[78] IETF RFC 4493: "The AES-CMAC Algorithm".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] NIST SP 800-190: "Application Container Security Guide".

[i.2] ENISA: "NFV Security in 5G-Challenges and Best Practices".

[i.3] Void.

[i.4] Void.

[i.5] Thales: "Kubernetes Secrets Encryption - Integration Guide".

[i.6] IBM: "Encrypting Kubernetes secrets with Key Management Service plug-in".

[i.7] NIST IR 8320: "Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases".

[i.8] "Recent trends in applying TPM to cloud computing".

[i.9] Open Worldwide Application Security Project (OWASP): "OWASP API Security Project".

[i.10] Void.

[i.11] O-RAN ALLIANCE TR: "Application Life Cycle Management (LCM) for Deployment Technical".

[i.12] ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Vocabulary for 3GPP Specifications (3GPP TR 21.905)".

[i.13] ETSI TS 133 210: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210)".

[i.14] ETSI TS 133 310: "Universal Mobile Telecommunications System (UMTS); LTE; 5G; Network Domain Security (NDS); Authentication Framework (AF) (3GPP TS 33.310)".

[i.15] IETF RFC 6083: "Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)".

[i.16] IETF RFC 3871: "Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure".

[i.17] ETSI GS NFV-SEC 012: "Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components".

[i.18] ETSI GR NFV-SEC 007: "Network Functions Virtualisation (NFV); Trust; Report on Attestation Technologies and Practices for Secure Deployments".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

A1: interface between Non-RT RIC and Near-RT RIC to enable policy-driven guidance of Near-RT RIC applications/functions, and support AI/ML workflow

A1 Enrichment Information (EI): information utilized by Near-RT RIC that is collected or derived at SMO/Non-RT RIC either from non-network data sources or from network functions themselves

A1 policy: type of declarative policies expressed using formal statements that enable the Non-RT RIC function in the SMO to guide the Near-RT RIC function, and hence the RAN, towards better fulfilment of the RAN intent

account and identity events: events generated by user identification and access control

application descriptor: template that defines the characteristics and requirements of the Application, allowing it to be deployed, managed, and orchestrated within the O-Cloud. It typically includes information such as the Application's functional behavior, deployment requirements, resource needs (such as CPU, memory, and storage), connectivity requirements, performance metrics, scalability options, and any dependencies or prerequisites. It also contains information related to security, including the service availability requirements and access rules for controlling the traffic direction to the Application.

application events: events generated by O-RAN Network Functions

application package: software package of xApps, rApps, and VNFs/CNFs (i.e. O-CU, O-DU, and Near-RT RIC)

audit records: "Audit records contain security event information such as successful and failed authentication attempts, file accesses, security policy changes, account changes (e.g. account creation and deletion, account privilege assignment), and use of privileges. OSs typically permit system administrators to specify which types of events should be audited and whether successful and/or failed attempts to perform certain actions should be logged." Defined in NIST SP 800-92 [58], clause 2.1.2.

data access event: events generated by any O-RAN component accessing, retrieving, modifying, or deleting data in files or databases

E2: interface connecting the Near-RT RIC and one or more O-CU-CPs, one or more O-CU-UPs, and one or more O-DUs

E2 Node: logical node terminating E2 interface. In this version of the specification, O-RAN nodes terminating E2 interface are:

- for NR access: O-CU-CP, O-CU-UP, O-DU or any combination.
- for E-UTRA access: O-eNB.

entity: individual (person), device, or process that interacts with an ORAN component

external interface: interface between the SMO and an External System

external system: data source outside the O-RAN domain that provides enrichment data to the SMO

general security event: events generated by the enabling, disabling or configuration of security features in O-RAN components

information security event: "Identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that can be security relevant." Defined in ISO/IEC 27000:2018 [57], clause 3.30.

information security incident: "Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security." Defined in ISO/IEC 27000:2018 [57], clause 3.31.

intents: declarative policy to steer or guide the behavior of RAN functions, allowing the RAN function to calculate the optimal result to achieve stated objective

isolation: security strategy that separates individual applications or software components from one another, ensuring that they run independently and do not interfere with each other's operations

log: "A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network." Defined in NIST SP 800-92 [58], clause 2.

log streaming: in information technology, log streaming refers to the near real-time transmission and analysis of log data generated by various software applications, systems, or devices

management and orchestration event: events generated by SMO operations

O-RAN near-real-time RAN Intelligent Controller (Near-RT RIC): logical function that enables real-time control and optimization of RAN elements and resources via fine-grained data collection and actions over E2 interface

network events: events generated by network activity from operating systems, hypervisors, or container engines

O-Cloud compute pool: cohesive set of computational resources within the O-Cloud infrastructure where multiple nodes work in harmony to provide a unified environment designed to host and manage O-RAN applications and services

O-Cloud instance ID: unique identifier assigned to components within the O-Cloud platform, including VMs, pods, containers, nodes, and compute pools (e.g. a cluster in Kubernetes). This ensures uniqueness across the entire O-Cloud environment, irrespective of the component type. For instance, a VM, a pod, a container, a node, and a cluster will each have a distinct O-Cloud instance ID within the platform, ensuring that there is no ambiguity in identification.

O-Cloud nodes: computational unit or entity within the O-Cloud infrastructure

O-Cloud platform software component: software module within the O-Cloud platform that provides essential functionalities and services to enable the deployment, management, and utilization of O-Cloud resources by O-RAN Network Functions

O-RAN Central Unit (O-CU): logical node hosting O-CU-CP and O-CU-UP

O-RAN Central Unit - Control Plane (O-CU-CP): logical node hosting the RRC and the control plane part of the PDCP protocol

O-RAN Central Unit - User Plane (O-CU-UP): logical node hosting the user plane part of the PDCP protocol and the SDAP protocol

O-RAN Distributed Unit (O-DU): logical node hosting RLC/MAC/High-PHY layers based on a lower layer functional split

O-RAN non-real-time RAN Intelligent Controller (Non-RT RIC): logical function that enables non-real-time control and optimization of RAN elements and resources, AI/ML workflow including model training and updates, and policy-based guidance of applications/features in Near-RT RIC

O-RAN Radio Unit (O-RU): logical node hosting Low-PHY layer and RF processing based on a lower layer functional split

O-RAN vendor: provider of any component of O-RAN

O1: interface between management entities (NMS/EMS/MANO) and O-RAN managed elements, for operation and management

O2: interface between SMO and the O-Cloud to provide cloud resources management and workload management for supporting O-RAN cloudified network functions

R1: interface between rApps and Non-RT RIC Framework via which R1 Services can be produced and consumed

R1 Services: collection of services including, but not limited to, service registration and discovery services, authentication and authorization services, AI/ML workflow services, and A1, O1 and O2 related services

non-RT RIC application (rApps): application designed to consume and/or produce R1 services

rApp instance: individual occurrence of an application running in the Non-RT RIC runtime environment

NOTE: As defined in [37].

rApp instance identifier: unique identifier for each rApp instance, assigned by the SMO/Non-RT RIC framework during rApp registration

NOTE: As defined in [37].

security controls: solution designed to meet a set of defined security requirements to protect the confidentiality, integrity, and availability of O-RAN elements

security log: log that contains audit records and security-related system events

Service Management and Orchestration (SMO): The O-RAN Service Management and Orchestration system as specified in the O-RAN Architecture Description (OAD) document [2], clause 5.3.1.

service provider: network provider who is planning to deploy applications into their network

NOTE: As defined in [16].

Shared Data Layer (SDL): API for accessing shared data storage

solution provider: application developer who delivers applications to Service Providers

NOTE: As defined in [16].

system events: "System events are operational actions performed by OS components, such as shutting down the system or starting a service. Typically, failed events and the most significant successful events are logged, but many OSs permit administrators to specify which types of events will be logged. The details logged for each event also vary widely; each event is usually timestamped, and other supporting information could include event, status, and error codes; service name; and user or system account associated with an event. "Defined in NIST SP 800-92 [58], clause 2.1.2.

Time of Day (ToD): precise hour, minute, and second of a day, serving as a unified time reference across the infrastructure to ensure that all nodes operate in synchronization

Y1: interface between Near-RT RIC and Y1 consumers, as defined in O-RAN Architecture Description [2], clause 5.4.18, that enables RAN analytics information exposure from Near-RT RIC

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 121 905 [i.12] and the following apply:

NOTE: An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in ETSI TR 121 905 [i.12].

AI/ML	Artificial Intelligence/Machine Learning
BMCA	Best Master Clock Algorithm
CNF	Cloud-native Network Function

DDoS	Distributed Denial of Service
DMS	Deployment Management Services (of O-Cloud)
DTLS	Datagram Transport Layer Security
eNB	eNodeB (applies to LTE)
FCAPS	Fault, Configuration, Accounting, Performance, SecurityFOCOM Federated O-Cloud Orchestration & Management
FOSS	Free and Open Source Software
FTPES	File Transfer Protocol Explicit Secure sockets layer
gNB	g NodeB (applies to NR)
IMS	Infrastructure Management Services (of O-Cloud)
IPSEC	Internet Protocol Security
LLS	Lower Layer Split
MFA	Multi-Factor Authentication
mTLS	mutual Transport Layer Security
NETCONF	Network Configuration Protocol
NF	Network Function
NFO	Network Function Orchestration
O-DU	O-RAN Distributed Unit
O-RU	O-RAN Radio Unit
OSC	O-RAN Software Community
PDCP	Packet Data Convergence Protocol
PNF	Physical Network Function
PTP	Precision Timing Protocol
RAN	Radio Access Network
RBAC	Role-Based Access Control
RIC	O-RAN RAN Intelligent Controller
SBOM	Software Bill of Materials
SDL	Shared Data Layer
SDLC	Software Development Life Cycle
SMO	Service Management and Orchestration
SPDX	Software Package Data eXchange
SRO	Shared Resource Operator
SSH	Secure Shell
SWID	Software Identification
TLS	Transport Layer Security
VM	Virtual Machine
VNF	Virtualised Network Function

4 Objectives and scope

4.1 Objectives

The present document specifies security requirements and security controls per O-RAN defined interface and O-RAN defined network function. It elaborates on O-RAN Threats and Risk Assessment [4] that identified assets to be protected, analysed the O-RAN components for vulnerabilities, examined potential threats associated with those vulnerabilities and provided security principles which stakeholders should address when building a secure end-to-end O-RAN system.

4.2 Perimeter

4.2.0 Introduction

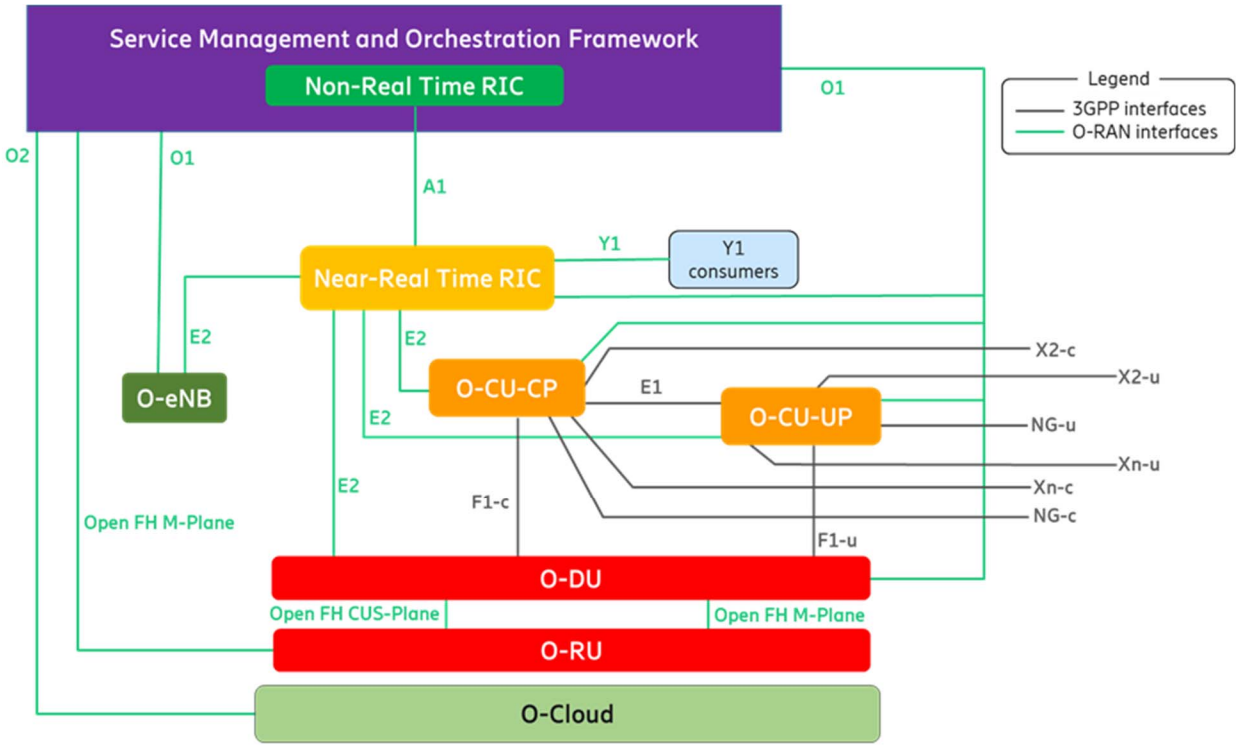

Figure 4.2.0-1: Logical Architecture of O-RAN system 2

As specified in [2] and illustrated in Figure 4.2.0-1, the logical architecture of O-RAN includes the following components, interfaces, and protocols.

4.2.1 O-RAN Architecture components

- Network functions and applications:
  - Service Management and Orchestration (SMO)
  - Non-RT RIC and rApps
  - Near-RT RIC and xApps
  - O-CU-CP/UP
  - O-DU
  - O-RU
  - O-eNB
- Cloud computing platform:
  - O-Cloud comprising physical infrastructure nodes to host the relevant O-RAN functions (such as Near-RT RIC, O-CU-CP, O-CU-UP, and O-DU) and, supporting software components (such as Operating System, Virtual Machine Monitor, Container Runtime) and the appropriate management and orchestration functions.

4.2.2 Interfaces defined by O-RAN

- A1 Interface between Non-RT RIC and Near-RT RIC to enable policy-driven guidance of Near-RT RIC applications/functions, and support AI/ML workflow.
- O1 Interface connecting the SMO to the Near-RT RIC, one or more O-CU-CPs, one or more O-CU-UPs, and one or more O-DUs.
- O2 Interface between the SMO and the O-Cloud.
- E2 Interface connecting the Near-RT RIC and one or more O-CU-CPs, one or more O-CU-UPs, one or more O-DUs, and one or more O-eNBs.
- Open Fronthaul CUS-Plane Interface between O-RU and O-DU.
- Open Fronthaul M-Plane Interface between O-RU and O-DU as well as between O-RU and SMO.

4.2.3 Interfaces not covered in the present document

- E1
- F1-c
- F1-u
- NG-c
- NG-u
- X2-c
- X2-u
- Xn-c
- Xn-u
- Uu

5 Security Requirements

5.0 Introduction

This clause describes the O-RAN Security Requirements per O-RAN maintained interfaces and network functions. Security Requirements specified in the present document are built upon Security Principles defined in [4] which intent to protect critical assets identified.

Protection levels of critical assets as defined in [4] - Confidentiality, Integrity, Replay, Authentication, Authorisation - are now specified as normative security requirements.

5.1 Network Functions and Applications maintained by O-RAN

5.1.1 Service Management and Orchestration (SMO)

5.1.1.1 Security Requirements

5.1.1.1.1 SMO

REQ-SEC-SMO-1: SMO shall support authentication of SMO functions.

REQ-SEC-SMO-2: SMO shall support authentication of External Systems.

REQ-SEC-SMO-3: SMO functions shall support authorization as a resource owner/server and client for internal requests.

REQ-SEC-SMO-4: SMO shall support authorization of the service requests received from External Systems.

REQ-SEC-SMO-5: SMO shall be able to recover, without catastrophic failure, from a volumetric DDoS attack across the O2 interface, due to anomalous behavior or malicious intent.

REQ-SEC-SMO-6: SMO shall be able to recover, without catastrophic failure, from a volumetric DDoS attack across an External Interface, due to anomalous behavior or malicious intent.

REQ-SEC-SMO-7: Each SMO function shall be able to recover, without catastrophic failure, from a volumetric DDoS attack during SMO Internal Communications, due to anomalous behavior or malicious intent.

5.1.1.1.2 SMO Internal Communications

REQ-SEC-SMO-Internal-1: SMO Internal Communications shall support confidentiality, integrity, and replay protection between SMO functions.

REQ-SEC-SMO-Internal-2: SMO Internal Communications shall support mutual authentication between SMO functions.

5.1.1.1.3 SMO External Interfaces

External Interfaces not specified by O-RAN that provide services to SMO, acting in a consumer role, shall meet security requirements specified in this clause.

REQ-SEC-SMO-External-1: SMO External Interfaces shall support confidentiality, integrity, and replay protection.

REQ-SEC-SMO-External-2: SMO External Interfaces shall support mutual authentication and authorization.

5.1.1.1.4 SMO Logging

The below mentioned requirements are referring to securing the event logs in SMO.

REQ-SEC-SMO-Log-1: SMO shall support forwarding of event logs to a mutually authenticated remote location.

REQ-SEC-SMO-Log-2: SMO shall provide confidentiality and integrity protection for event logs transferred to a remote server.

REQ-SEC-SMO-Log-3: SMO may support configuration settings that allow selection of remote servers to securely transfer the event logs.

REQ-SEC-SMO-Log-4: SMO shall be capable of logging the event logs locally on itself.

REQ-SEC-SMO-Log-5: SMO shall provide confidentiality protection for the locally stored event logs.

REQ-SEC-SMO-Log-6: SMO shall provide integrity protection for the locally stored event logs.

REQ-SEC-SMO-Log-7: SMO shall support access to event logs by authorized external services.

REQ-SEC-SMO-Log-8: SMO shall be capable of forwarding event logs to an authorized remote location.

REQ-SEC-SMO-Log-9: SMO shall be able to record all the security related log events.

REQ-SEC-SMO-Log-10: The security logs of SMO should be separate from other system logs.

REQ-SEC-SMO-Log-11: The SMO shall not permit configuration change to logging level(s) of any component on the SMO system without proper authorization.

REQ-SEC-SMO-Log-12: SMO shall support access to event logs by authorized internal services.

5.1.1.1.5 NFO and FOCOM

The below mentioned requirements are referring to securing the NFO and FOCOM in SMO.

REQ-SEC-NFO-FOCOM-1: NFO and FOCOM shall support confidentiality, integrity, and replay protection.

REQ-SEC-NFO-FOCOM-2: VOID.

REQ-SEC-NFO-FOCOM-3: NFO shall support mutual authentication with the O-Cloud on the O2dms interface.

REQ-SEC-NFO-FOCOM-4: FOCOM shall support mutual authentication with the O-Cloud on the O2ims interface.

REQ-SEC-NFO-FOCOM-5: NFO and FOCOM shall support authorization with the principle of least privilege for access attempts by O-Cloud service consumers, on a per-session basis.

REQ-SEC-NFO-FOCOM-6: NFO shall be able to recover, without catastrophic failure, from a volumetric DDoS attack due to anomalous behavior or malicious intent.

REQ-SEC-NFO-FOCOM-7: VOID.

REQ-SEC-NFO FOCOM-8: FOCOM shall be able to recover, without catastrophic failure, from a volumetric DDoS attack due to anomalous behavior or malicious intent.

5.1.1.2 Security Controls

5.1.1.2.1 SMO

SEC-CTL-SMO-1: SMO may support OAuth 2.0 authorization server and provide a token end-point, as specified in O-RAN Security Protocols Specifications [3], clause 4.7.

SEC-CTL-SMO-3: SMO shall support OAuth 2.0 resource owner/server, as specified in O-RAN Security Protocols Specifications [3], clause 4.7, for service requests received from other SMO functions.

SEC-CTL-SMO-4: SMO shall support OAuth 2.0 client functionality, as specified in O-RAN Security Protocols Specifications [3], clause 4.7, for service requests to other SMO functions.

SEC-CTL-SMO-5: SMO shall support mutual authentication of SMO functions using mTLS with PKI X.509v3 certificates as specified in O-RAN Security Protocols Specifications [3], clause 4.2.

SEC-CTL-SMO-6: SMO functions may support authentication of other SMO functions using TLS with pre-shared key (PSK) as specified in O-RAN Security Protocols Specifications [3], clause 4.2.

5.1.1.2.2 SMO Internal Communications

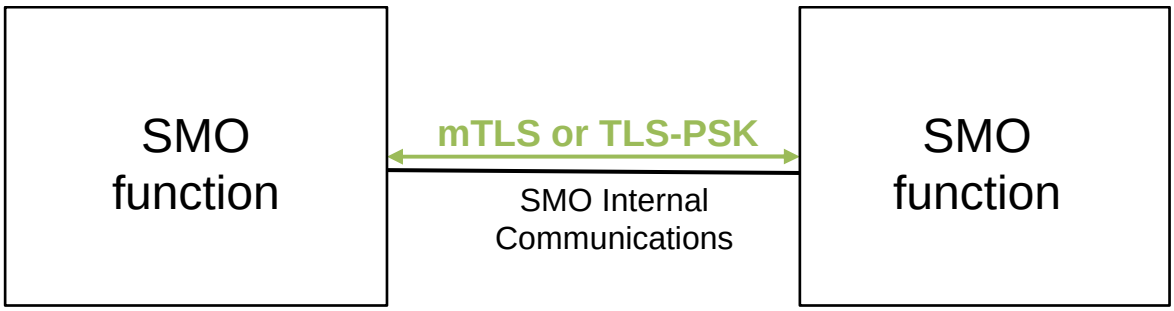

Figure 5.1.1.2.2-1: mTLS or TLS for SMO Internal Communications

SEC-CTL-SMO-Internal-1: For security protection at the transport layer, SMO Internal Communications shall support TLS as specified in O-RAN Security Protocols Specifications [3], clause 4.2.

SEC-CTL-SMO-Internal-2: For mutual authentication between SMO functions, SMO Internal Communications shall support mTLS as shown in Figure 5.1.1.2.2-1 and specified in O-RAN Security Protocols Specifications [3], clause 4.2.

SEC-CTL-SMO-Internal-3: For authentication between SMO functions, SMO Internal Communications may support TLS with Pre-Shared Key (PSK), as specified in O-RAN Security Protocols Specifications [3], clause 4.2.

5.1.1.2.3 SMO External Interfaces

External Interfaces not specified by O-RAN that provide services to SMO, acting in a consumer role, shall meet security controls specified in this clause.

Figure 5.1.1.2.3-1: mTLS on SMO External interfaces

SEC-CTL-SMO-External-1: For confidentiality and integrity protection of data in transit, SMO External Interfaces shall support TLS as specified in O-RAN Security Protocols Specifications [3], clause 4.2.

SEC-CTL-SMO-External-2: For mutual authentication between the SMO and External Source, SMO External Interfaces shall support mTLS as shown in Figure 5.1.1.2.3-1 and specified in O-RAN Security Protocols Specifications [3], clause 4.2.

SEC-CTL-SMO-External-3: SMO External Interfaces shall support OAuth 2.0 resource owner/server, as specified in O-RAN Security Protocols Specifications [3], clause 4.7.

SEC-CTL-SMO-External-4: SMO External Interfaces shall support OAuth 2.0 client functionality, as specified in O-RAN Security Protocols Specifications [3], clause 4.7.

5.1.1.2.4 SMO Logging

SEC-CTL-SMO-Log-1: A SMO External Interface used for SMO log export shall support TLS as specified in O-RAN Security Protocols Specifications [3], clause 4.2, and FTPES.

SEC-CTL-SMO-Log-2: SMO log export may support SSH as specified in O-RAN Security Protocols Specifications [3], clause 4.1, and SFTP.

SEC-CTL-SMO-Log-3: SMO log export shall support mutual authentication using mTLS with public key infrastructure (PKI) and X.509v3 certificates as specified in O-RAN Security Protocols Specifications [3], clause 4.2.

SEC-CTL-SMO-Log-4: When SSH is supported for SMO log export, SSH shall support authentication using public and private keys in a Public Key Infrastructure (PKI).

SEC-CTL-SMO-Log-5: When SSH is supported for SMO log export, SSH may support authentication using PKI and X.509v3 certificates.

5.1.1.2.5 NFO and FOCOM

SEC-CTL-NFO-FOCOM-1: NFO shall support mutual authentication with O-Cloud DMS using mTLS with PKI X.509v3 certificates, as specified in O-RAN Security Protocols Specifications [3], clause 4.2.

SEC-CTL-NFO-FOCOM-2: FOCOM shall support mutual authentication with O-Cloud IMS using mTLS with PKI X.509v3 certificates, as specified in O-RAN Security Protocols Specifications [3], clause 4.2.

SEC-CTL-NFO-FOCOM-3: NFO shall support OAuth 2.0 resource owner/server as specified in O-RAN Security Protocols Specifications [3], clause 4.7, for service requests from O-Cloud resources.

SEC-CTL-NFO-FOCOM-4: FOCOM shall support OAuth 2.0 resource owner/server, as specified in O-RAN Security Protocols Specifications [3], clause 4.7, for service requests from O-Cloud resources.

SEC-CTL-NFO-FOCOM-5: NFO shall support OAuth 2.0 client functionality as specified in O-RAN Security Protocols Specifications [3], clause 4.7, for service requests to O-Cloud resources.

SEC-CTL-NFO-FOCOM-6: FOCOM shall support OAuth 2.0 client functionality, as specified in O-RAN Security Protocols Specifications [3], clause 4.7, for service requests to O-Cloud resources.

SEC-CTL-NFO-FOCOM-7: NFO shall support TLS, as specified in O-RAN Security Protocols Specifications [3], clause 4.2, on the O2 interface.

SEC-CTL-NFO-FOCOM-8: FOCOM shall support TLS, as specified in O-RAN Security Protocols Specifications [3], clause 4.2, on the O2 interface.

5.1.2 Non-RT RIC and rApps

5.1.2.1 Requirements

rApp packages shall follow the security requirements and controls in the Common App LCM clause 5.3.2.1 in the present document.

REQ-SEC-NonRTRIC-1: The Non-RT RIC shall support authorization as a resource owner/server and client.

REQ-SEC-NonRTRIC-2: The Non-RT RIC Framework, as a resource owner/server, shall provide authorization to requests from rApps as a client.

REQ-SEC-NonRTRIC-3: rApps shall provide client authorization requests to the Non-RT RIC Framework.

REQ-SEC-NonRTRIC-4: The Non-RT RIC shall be able to recover, without catastrophic failure, from a volumetric DDoS attack across the A1 interface, due to misbehavior or malicious intent.

REQ-SEC-NonRTRIC-5: The Non-RT RIC Framework shall be able to recover, without catastrophic failure, from a volumetric DDoS attack across the R1 interface, due to misbehavior or malicious intent.

REQ-SEC-NonRTRIC-6: rApps shall be able to recover, without catastrophic failure, from a volumetric DDoS attack across the R1 interface, due to misbehavior or malicious intent.

REQ-SEC-NonRTRIC-7: The SMO/Non-RT RIC Framework shall authenticate both API Producer and API Consumer across R1 interface using Kafka based protocol for data streaming.

REQ-SEC-NonRTRIC-8: The SMO/Non-RT RIC Framework shall support authorization mechanism for Kafka based protocol to provision access for data streaming by API Producer and API Consumer across R1 interface.

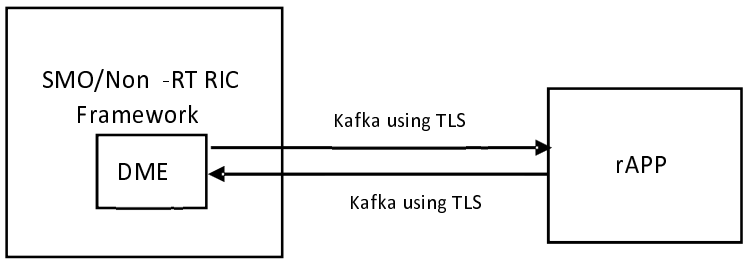

Figure 5.1.2.1-1: SMO/Non-RT RIC Framework supporting Kafka based protocol using TLS

REQ-SEC-NonRTRIC-9: rAppIDs shall be unique within the Non-RT RIC runtime environment.

REQ-SEC-NonRTRIC-10: rAppIDs shall be generated using strong randomization methods.

NOTE: Strong randomization methods can help resist brute force attacks.

5.1.2.2 Security Controls

SEC-CTL-NonRTRIC-1: For A1-EI, Non-RT RIC shall support OAuth 2.0 resource owner/server, as specified in O-RAN Security Protocols Specifications [3], clause 4.7, for service requests received from one or more Near-RT RICs.

SEC-CTL-NonRTRIC-2: For A1-P, Non-RT RIC shall support OAuth 2.0 client, as specified in O-RAN Security Protocols Specifications [3], clause 4.7.

SEC-CTL-NonRTRIC-3: For R1, SMO/Non-RT RIC Framework may support TLS, as specified in O-RAN Security Protocols Specifications [3], clause 4.2.

SEC-CTL-NonRTRIC-4: For R1, SMO/Non-RT RIC Framework shall support authorization using OAuth 2.0, as specified in O-RAN Security Protocols Specifications [3], clause 4.7.

SEC-CTL-NonRTRIC-5: For R1, Non-RT RIC Framework shall support OAuth 2.0 resource owner/server functionality, as specified in O-RAN Security Protocols Specifications [3], clause 4.7.

SEC-CTL-NonRTRIC-6: For R1, rApps shall support OAuth 2.0 client functionality, as specified in O-RAN Security Protocols Specifications [3], clause 4.7.

5.1.3 Near-RT RIC and xApps

5.1.3.1 Requirements

xApp packages shall follow the security requirements and controls in the Common App LCM clause 5.3.2.1 in the present document.

REQ-SEC-XAPP-1: VOID

REQ-SEC-XAPP-2: VOID

REQ-SEC-XAPP-3: During the xApp registration procedure the xApp identifier (xApp ID) shall be associated with xApp credentials used for authentication.

REQ-SEC-XAPP-4: xApp IDs shall be created ensuring uniqueness.

REQ-SEC-NEAR-RT-1: Near-RT RIC shall authenticate xApp access to the Near-RT RIC database(s) during SDL registration.

REQ-SEC-NEAR-RT-2: Near-RT RIC shall provide authorized access to Near-RT RIC database(s).

REQ-SEC-NEAR-RT-3: The communication between xApps and Near-RT RIC platform APIs shall be mutually authenticated.

REQ-SEC-NEAR-RT-4: Near-RT RIC architecture shall provide an authorization framework for the consumption of the services exposed in the platform APIs by the xApps, that takes operator policies into consideration. The framework should be used by the specified API procedures in [33].

REQ-SEC-NEAR-RT-5: The Near-RT RIC shall support authorization as a resource owner/server (A1-P) and client (A1-EI).

REQ-SEC-NEAR-RT-6: The Near-RT RIC shall be able to recover, without catastrophic failure, from a volumetric DDoS attack across the A1 interface, due to misbehavior or malicious intent.

REQ-SEC-NEAR-RT-7: The Near-RT RIC shall be able to detect and defend against content-related attacks across the A1 interface, due to misbehavior or malicious intent.

NOTE 1: In practice, injection attacks and buffer overflow attacks are the most common classes of content-related attacks.

REQ-SEC-NEAR-RT-8: The Near-RT RIC shall be able to detect and defend against content-related attacks across the Y1 interface.

NOTE 2: In practice, injection attacks and buffer overflow attacks are the most common classes of content-related attacks.

REQ-SEC-NEAR-RT-9: The Near-RT RIC shall be able to detect and defend against content-related attacks across the E2 interface, due to misbehavior or malicious intent.

NOTE 3: In practice, injection attacks and buffer overflow attacks are the most common classes of content-related attacks.

5.1.3.2 Security Controls

API Security - Authentication

SEC-CTL-NEAR-RT-1: Transactional APIs (REST and gRPC) shall support mutual TLS (mTLS) authentication via X.509v3 certificates as specified in the O-RAN Security Protocols Specification [3], clause 4.2.

SEC-CTL-NEAR-RT-2: Time critical APIs, not supported by TLS protocol, shall support IPsec with IKEv2 certificate-based authentication according to O-RAN security protocol specification [3].

EXAMPLE 1: E2 related APIs are considered time critical APIs.

API Security - Authorization

In the actual context of Near-RT RIC, the platform as API producer shall be responsible to specify those rights/privileges for the platform services as resources to the xApps as consumers. As a guideline, an xApp should only have the required set of permissions to perform the actions for which they are authorized, and no more.

Authorization mechanisms shall be enforced by the Near-RT RIC platform in the following key API procedures [33]:

- **Discovery of Near-RT RIC APIs:** The Near-RT RIC platform shall provide means to restrict xApps from discovery of some published APIs based on configuration policies.
- **E2 Subscription API procedure:** The subscription management shall be based on operator's policies. An xApp may be restricted to interface with only a subset of E2 Nodes by such policies. This procedure establishes a set of preconditions that assume authorization processes:
  - xApp has been authorized to issue E2 Subscription API requests.
  - xApp has been authorized to request guidance from Conflict mitigation.
  - xApp Subscription Management has been configured to permit E2 Subscription API requests only from specific list of xApps.
- **E2 Control API procedure:** Only authorized xApps may initiate RIC control request messages issued by the Near-RT RIC over the E2 interface to the E2 Nodes, for a specific scope.

EXAMPLE 2: E2Nodes include E2 Node list, RAN function.

- **E2 Guidance API procedure:** Ensure only authorized xApp obtain guidance from the conflict mitigation platform function prior to initiating an action.

- **SDL API procedures:** xApps shall have been successfully registered and authorized prior to consuming the services exposed by SDL API.

EXAMPLE 3: Services exposed by SDL API may be client registration, fetch data, notification, store.

SEC-CTL-NEAR-RT-3: Transactional APIs (REST and gRPC) in Near-RT RIC shall support OAuth 2.0 authorization framework as specified in in O-RAN Security Protocols Specifications [3], clause 4.7.

The roles defined in OAuth 2.0 are assigned as follows:

- Resource owner / Resource server (producer): Near-RT RIC platform modules providing services via APIs
- Client (consumer): xApp

Grants shall be of the type Client Credentials Grant, as described in clause 4.4. of IETF RFC 6749 [34]. Mutual authentication using mTLS as specified in the O-RAN Security Protocols Specification [3], clause 4.2 shall be used.

SEC-CTL-NEAR-RT-4: For A1-P, Near-RT RIC shall support OAuth 2.0 resource owner/server, as specified in O-RAN Security Protocols Specifications [3], clause 4.7, for service requests received from a Non-RT RIC.

SEC-CTL-NEAR-RT-5: For A1-EI, Near-RT RIC shall support OAuth 2.0 client, as specified in O-RAN Security Protocols Specifications [3], clause 4.7.

API Security - Confidentiality and Integrity

SEC-CTL-NEAR-RT-6: Transactional APIs (REST and gRPC) shall support TLS as specified in the O-RAN Security Protocols Specification [3], clause 4.2 to provide message confidentiality and integrity.

SEC-CTL-NEAR-RT-7: Time critical, not supported by TLS protocol, shall support IPsec as specified in the O-RAN Security Protocols Specification [3], clause 4.5 to provide message confidentiality and integrity.

Table 5.1.3.2-1 provides a summary of the security controls (SEC-CTL- NEAR-RT-1 to -7) and a mapping of those to the related interface/API transport protocols considered in Near-RT RIC platform.

Table 5.1.3.2-1: Summary of the Security Controls for Near-RT RIC APIs

API protocol	Authentication method	Authorization method	Confidentiality method	Integrity method
gRPC	mTLS	OAuth2	mTLS	mTLS
SCTP	IKEv2	-	IPsec	IPsec
REST/HTTP	mTLS	OAuth2	mTLS	mTLS

SEC-CTL- NEAR-RT-8: The Near-RT RIC shall verify policies received through the A1 interface as follows:

- The policies conform to a pre-defined schema.
- The policy values are valid.
- The policies are being received at or below a pre-defined rate.

The Near-RT RIC shall log security event(s) if any of the policy verification steps fail.

EXAMPLE 4: In practice, policy value validation verifies that values are within the predefined range.

Security controls for the Y1 interface protocol structure solution 1

The Y1 interface protocol structure solution 1 is defined in the O-RAN ALLIANCE TS: "Y1 interface: General Aspects and Principles" [66], clause 7.2.

SEC-CTL-NEAR-RT-9: The Y1 interface shall support mutual TLS (mTLS) authentication via X.509v3 certificates as specified in O-RAN Security Protocols Specifications [3], clause 4.2. Both the client (the Y1 consumer) and the server (the Y1 provider) require a certificate, and both sides authenticate each other using their public/private key pair.

SEC-CTL-NEAR-RT-10: The Y1 interface shall support the OAuth 2.0 authorization framework as specified in O-RAN Security Protocols Specifications [3], clause 4.7.

The roles defined in OAuth 2.0 shall be assigned as follows:

- Resource owner / Resource server (producer): Y1 provider
- Client (consumer): Y1 consumer

SEC-CTL-NEAR-RT-11: The Y1 interface shall support TLS as specified in O-RAN Security Protocols Specifications [3], clause 4.2 to provide data confidentiality, integrity, and replay-protection.

xApp Registration - Security procedure

As part of the xApp registration procedure to the Near-RT RIC platform, the platform assigns an identity (ID) to the xApp, so called xApp ID. This xApp ID is used in xApp's API request messages to the Near-RT RIC platform to facilitate the Near-RT RIC platform the identification of the xApp (API service consumer).

SEC-CTL-NEAR-RT-12: The xApp ID shall be embedded into the provided xApp X.509 certificate used for authentication (mTLS) according to the parametrization in [3], issued by operator RA/CA PKI infrastructure. The security procedure to become part of the existing xApp registration procedure, specified in O-RAN.WG3.RICARCH (clause 9.1.4) where xApp ID is assigned, is detailed in Figures 5.1.3.2-1 and 5.1.3.2-2:

```
@startuml
participant xapp as "xApp\n[API service consumer]"
participant nfo as "Provisioning system\n(NFO in SMO)"
participant pf as "Near-RT RIC platform \n(Operator RA functionality)\n[API service
producer]"
participant pki as "Operator PKI\nCA"
xapp <- nfo : 1. Registration information\n[Near-RT RIC Platform\n(Address,Root CA
Certificate),\n OAuth 2.0 Access token]
xapp -> pf : 2. TLS (Server side certificate based authentication)
rnote over xapp
     3. Generate the private/public key pair
        and CSR
endnote
xapp -> pf : 4. Registration request (by xApp instance)\n[OAuth 2.0 access token, xApp
Instance CSR]
rnote over pf
     5. Verify OAuth 2.0 access token
        Generate the xApp ID
        POP (Proof of Possession of Private Key)
        RA policy: Add xApp ID to the request to be in the SAN field of the certificate
endnote
pf -> pki : 6. Request of the certificate by the RA
pf <- pki : 7. Issued certificate \n(embedded xApp ID in SAN)
rnote over pf
     8. Generate xApp MOI
endnote
xapp <- pf : 9. Registration Response (for xApp instance)\n[xApp ID, xApp Certificate,
(service API authentication \nand Authorization information)]
@enduml
```

Figure 5.1.3.2-1: UML code for secure xApp registration

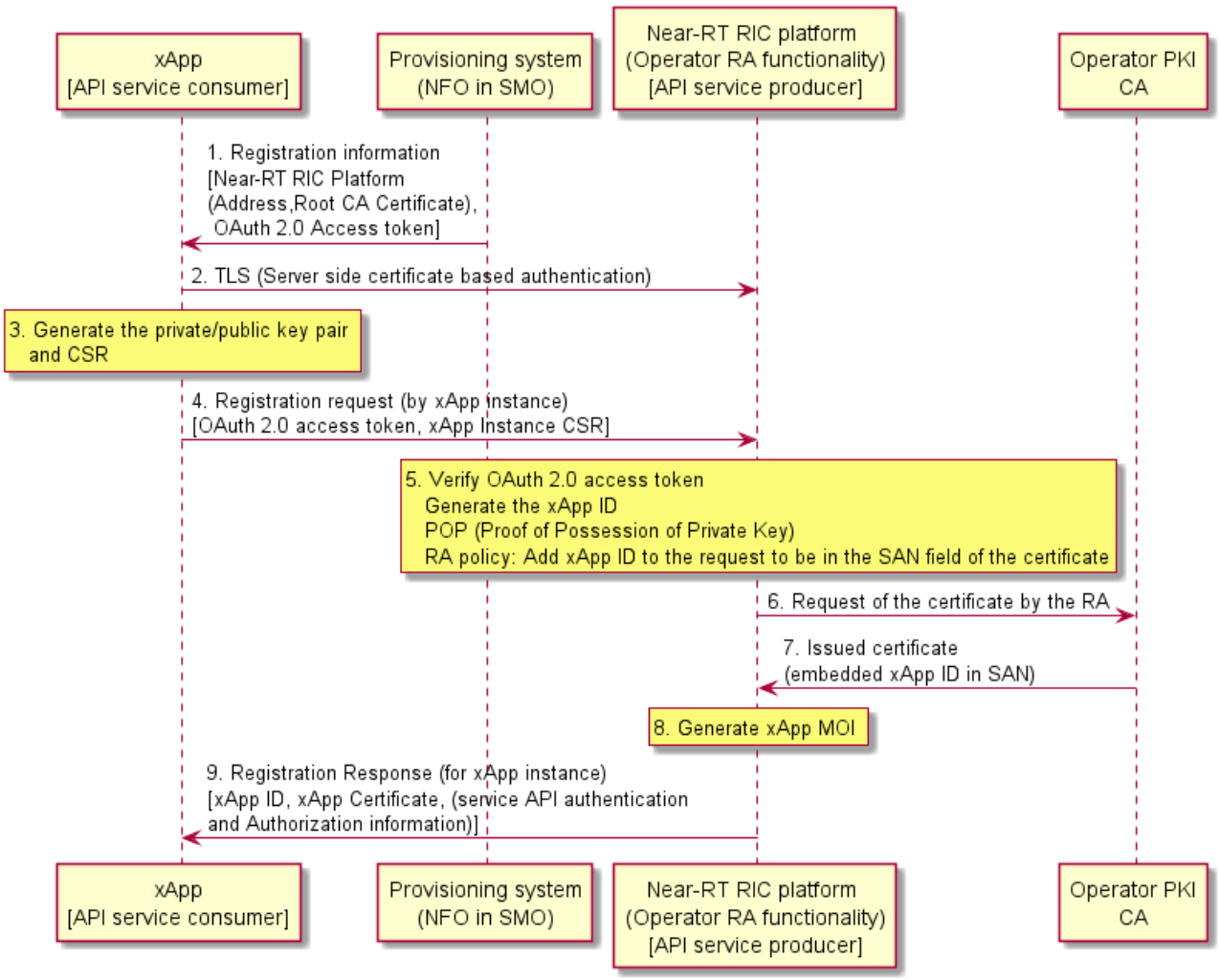

Figure 5.1.3.2-2: Security procedure for xApp registration

1. As a pre-requisite to the registration procedure, the xApp obtains information from a provisioning system (NFO in SMO) during the onboarding/deployment phase in the infrastructure. This information is used to authenticate and establish a secure TLS communication with the Near-RT RIC platform during the registration process. The information includes details of the Near-RT RIC platform (address, Root CA certificate) and includes an initial registration credential.

NOTE 1: An OAuth 2.0 access token is provided as initial registration credential in the example. Other types of credentials in the initial registration can be used.

2. The xApp and Near-RT RIC platform establish a TLS session (server-side certificate authentication) using the information obtained in step 1.

3. The xApp generates the private and public key pair, and CSR (Certificate Signing Request).

4. After successful establishment of the TLS session, the xApp instance sends a registration request message to the Near-RT RIC platform along with the pre-provisioned initial registration credential (OAuth 2.0 token), and the xApp instance CSR message.

5. The Near-RT RIC platform shall validate the initial registration credential, and the Management Function of the platform shall generate an xApp ID for that particular xApp instance. At the reception of the CSR message from the xApp, the Registration Authority (RA), implemented in the Near-RT RIC platform, shall prove that the xApp instance is in possession of the private key. If the proof of possession procedure is positive, the RA shall configure a policy to add the xApp ID in the Subject Alt Name (SAN) field of the certificate request message to be forwarded to the Operator CA to fetch the end entity certificate.

NOTE 2: The RA may use an enrolment protocol to fetch the certificate from the CA. The authentication mechanism between RA and CA are part of the operator PKI implementation.

6. The RA requests the certificate for the xApp instance.

7. Operator CA issues a certificate, embedding the xApp ID in SAN field of the certificate. The issued certificate by the operator CA will be used by the xApp for subsequent authentication and authorization procedures between the xApp and the Near-RT RIC platform when services/resources are consumed by xApps via APIs.

8. The Near-RT RIC platform (Management Function) generates an xApp Managed Object Instance (MOI) as specified in [33], which may contain the mechanism for authentication (mTLS) and authorization (OAuth 2.0) between the xApp and the corresponding module of the Near-RT RIC platform.

9. The Near-RT RIC platform (Management Function) responds with a xApp registration response message. The response shall include the assigned xApp ID, authentication, and authorization mechanism (if provided in step 8) and xApp certificate.

SEC-CTL-NEAR-RT-13: The data type of the xApp ID shall be a string that uniquely identifies the xApp instance. The format of this string shall be a Universally Unique Identifier (UUID) version 4 (as described in IETF RFC 4122 [77]).

SEC-CTL-NEAR-RT-14: subjectAltName in the xApp instance certificate shall contain a URI-ID with the URI for the xApp ID as an URN; this URI-ID shall contain the xApp ID of the xApp instance using the UUID format as described in IETF RFC 4122 [77].

EXAMPLE 5: urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6

SEC-CTL- NEAR-RT-15: The Near-RT RIC shall verify data received through the Y1 interface as follows:

- The data values are valid.
- The data is being received at or below a pre-defined message rate.

EXAMPLE 6: In practice, data value validation verifies that values are within the predefined ranges.

SEC-CTL- NEAR-RT-16: The Near-RT RIC shall log a security event each time an input validation step fails for data received through the Y1 interface.

SEC-CTL- NEAR-RT-17: The Near-RT RIC shall verify data received through the E2 interface as follows:

- The data values are valid.
- The data is being received at or below a pre-defined rate.
- The Near-RT RIC shall log security event(s) if any of the verification steps fail.

EXAMPLE 7: In practice, data value validation verifies that values are within the predefined ranges.

5.1.4 O-CU-CP/UP

5.1.4.1 Requirements

REQ-SEC-OCU-1: O-CU-CP and O-CU-UP shall meet the security requirements for gNB-CU-CP and gNB-CU-UP respectively, as specified in ETSI TS 133 501 [55].

5.1.4.2 Security Controls

SEC-CTL-OCU-1: O-CU-CP and O-CU-UP shall support the security controls for gNB-CU-CP and gNB-CU-UP respectively, as specified in ETSI TS 133 501 [55].

5.1.5 O-DU

5.1.5.1 Requirements

REQ-SEC-ODU-1: O-DU shall meet the security requirements for gNB-DU as specified in ETSI TS 133 501 [55].

The security requirements for the Open Fronthaul Interface are specified in clause 5.2.5 of the present document.

5.1.5.2 Security Controls

SEC-CTL-ODU-1: O-DU shall support the security controls for gNB-DU as specified in ETSI TS 133 501 [55]. The security controls for the Open Fronthaul Interface are specified in clause 5.2.5 of the present document.

5.1.6 O-RU

5.1.6.1 Requirements

REQ-SEC-ORU-1: O-RU shall meet the security requirements for gNB setup and configuration as specified in ETSI TS 133 501 [55].

REQ-SEC-ORU-2: O-RU shall meet the security requirements for gNB secure environment as specified in ETSI TS 133 501 [55].

The security requirements for the Open Fronthaul Interface are specified in clause 5.2.5 of the present document.

5.1.6.2 Security Controls

The security controls for the Open Fronthaul Interface are specified in clause 5.2.5 of the present document.

5.1.7 O-eNB

5.1.7.1 Requirements

REQ-SEC-OeNB-1: O-eNB shall meet the security requirements for eNB as specified in ETSI TS 133 401 [56].

5.1.7.2 Security Controls

SEC-CTL-OeNB-1: O-eNB shall support the security controls for eNB as specified in ETSI TS 133 401 [56].

5.1.8 O-Cloud

5.1.8.0 Introduction

NOTE 1: In the following requirements and controls, 'App' is intended to include both xApp and rApp.

NOTE 2: In the following requirements and controls, the actor 'Service Provider' is used to refer to the Telco Operator and/or the O-Cloud Provider since the Application package verification may be performed by both or by one or the other, depending upon the O-Cloud deployment models. The Telco Operator may act as the O-Cloud Provider (in case of private cloud model), or they may be two different entities (in case of hybrid or public cloud models).

5.1.8.1 Generic requirements

Generic requirements for Cloud Platform Management are specified in [8].

5.1.8.1.1 User Management Requirements for Cloud Platform Management

REQ-SEC-OCLOUD-1: Users shall be authenticated.

REQ-SEC-OCLOUD-2: Users shall be authorized. O-Cloud platform shall use an authorization mechanism to control the access rights of users.

REQ-SEC-OCLOUD-3: Means of isolation of control and resources among different users shall be implemented.

5.1.8.1.2 Security Controls

SEC-CTL-OCLOUD-1: O-Cloud platform should support access management to O-Cloud resources based on RBAC (Role-based access control) policies.

SEC-CTL-OCLOUD-2: O-Cloud platform shall support Multi-Factor Authentication (MFA) [46] to ensure secure access.

5.1.8.2 Software Package Protection at the O-Cloud Network Functions and Applications Layer

5.1.8.2.1 Requirements

REQ-SEC-OCLOUD-IMG-1 to 18: VOID.

REQ-SEC-OCLOUD-PKG-1: The Application package shall be successfully authenticated and verified by the O-Cloud Platform during instantiation from the trust images repository using signatures from both Application Provider and Service Provider.

REQ-SEC-OCLOUD-PKG-2: O-Cloud Platform shall verify the integrity of Application package during instantiation to determine if any unauthorized modification, deletion, or insertion has occurred.

REQ-SEC-OCLOUD-PKG-3: SMO and O-Cloud Platform shall support algorithms for the code signing and encryption/decryption processes and protection of keys.

5.1.8.2.2 Security Controls

SEC-CTL-OCLOUD-IMG-1 to 4: VOID.

5.1.8.3 O-Cloud Software Images Protection

5.1.8.3.0 Introduction

The identified requirements and controls in this clause are enforcing the protection of O-Cloud software images during both initial deployment and subsequent updates.

EXAMPLE: O-Cloud software includes AAL drivers, IMS, DMS, Host OS, Hypervisor/Container Engine.

5.1.8.3.1 Requirements

REQ-SEC-OCLOUD-SW-1: All O-Cloud software images shall be protected to ensure their integrity and authenticity.

REQ-SEC-OCLOUD-SW-2: The O-Cloud shall support the capability to perform vulnerability scanning on O-Cloud software images. The activation and enforcement of this vulnerability scanning prior to the deployment or updating of software images in the O-Cloud shall be configurable.

NOTE: This flexibility allows service providers to decide on the application of vulnerability scanning based on a comprehensive risk assessment, taking into account specific operational needs, deployment scenarios, or time constraints.

5.1.8.3.2 Security Controls

SEC-CTL-OCLOUD-SW-1: For all deployments and updates, the O-Cloud shall verify the digital signature associated with the new O-Cloud software image before installing the software package. The algorithms, key sizes, and standards used for signature generation and verification shall adhere to the 'O-RAN Security Protocol Specification' [3], clause 5.

5.1.8.4 O-Cloud Virtualization and Isolation

5.1.8.4.1 Introduction

This clause contains security requirements and controls to mitigate threats to O-Cloud Virtualization layer (Host OS-Hypervisor/Container engine/Cloud platform software components) and provide isolation to the Applications hosted on the O-Cloud.

5.1.8.4.2 Requirements

REQ-SEC-OCLOUD-ISO-1: O-Cloud shall implement means of preventing privilege escalation by Applications.

REQ-SEC-OCLOUD-ISO-2: The communication between the different Applications shall be mutually authenticated and authorized.

REQ-SEC-OCLOUD-ISO-3: The O-Cloud consumer and provider shall together ensure that the Applications have only the minimum required capabilities and privileges as well as minimum required access to the O-Cloud resources.

REQ-SEC-OCLOUD-ISO-4: The O-Cloud platform shall ensure that there is strict isolation between Applications in terms of data in transit, data in use and data at rest.

REQ-SEC-OCLOUD-ISO-5: Communication between O-Cloud platform software components shall be protected in terms of authenticity, confidentiality, integrity, and replay.

REQ-SEC-OCLOUD-ISO-6: The O-Cloud platform shall provide the capability to define network policies that restrict ingress and egress traffic and configure rate limiting between Applications.

REQ-SEC-OCloud-ISO-7: The O-Cloud platform shall not permit configuration change of any component on the O-Cloud platform without proper authorization.

5.1.8.4.3 Security Controls

SEC-CTL-O-CLOUD-ISO-1: For mutual authentication between O-Cloud platform software components, mTLS shall be supported as specified in O-RAN Security Protocols Specifications [3], clause 4.2.

SEC-CTL-O-CLOUD-ISO-2: For confidentiality and integrity protection of data in transit, O-Cloud platform software components shall support TLS as specified in O-RAN Security Protocols Specifications [3], clause 4.2.

SEC-CTL-O-CLOUD-ISO-3: The O-Cloud platform shall support an access control system to enforce access control policies that align with the principle of least privilege, ensuring that O-Cloud platform components or Applications have the necessary permissions to perform their tasks while preventing unauthorized access to sensitive resources.

5.1.8.5 Secure update

5.1.8.5.0 Introduction

The identified requirements and controls in this clause are enforcing the secure update of O-Cloud software.

EXAMPLE: O-Cloud software includes AAL drivers, IMS, DMS, Host OS, Hypervisor/Container Engine.

5.1.8.5.1 Requirements

REQ-SEC-OCLOUD-SU-1: All software within the O-Cloud platform shall be kept up to date with the last security updates for adding additional security protections and correcting vulnerabilities [i.1].

REQ-SEC-OCLOUD-SU-2: VOID.

REQ-SEC-OCLOUD-SU-3: VOID.

REQ-SEC-OCLOUD-SU-4: VOID.

REQ-SEC-OCLOUD-SU-5: In case of an incomplete update, or incident during the installation process, the O-Cloud platform shall remain in its initial working state.

REQ-SEC-OCLOUD-SU-6: The O-Cloud platform shall prevent the unauthorized rollback of its software to an earlier vulnerable version.

REQ-SEC-OCLOUD-SU-7: The update of O-Cloud software should be completed with minimal disruption and downtime.

5.1.8.5.2 Security Controls

SEC-CTL-OCLOUD-SU-1: VOID.

SEC-CTL-OCLOUD-SU-2: VOID.

SEC-CTL-OCLOUD-SU-3: VOID.

SEC-CTL-OCLOUD-SU-4: The O-Cloud shall possess the capability to detect and retrieve the latest security updates of the O-Cloud software images.

NOTE: This ensures that all O-Cloud software components can be consistently updated with the latest security patches for enhanced protection and vulnerability mitigation. The operation of this system should be automated.

SEC-CTL-OCLOUD-SU-5: The O-Cloud shall possess the capability to securely log and control software versions, thereby preventing unauthorized rollbacks to older, less secure software versions.

SEC-CTL-OCLOUD-SU-6: The O-Cloud should possess the capability to revert an O-Cloud software component to its previous stable version in the event of an incomplete update or installation incident, ensuring operational continuity.

SEC-CTL-OCLOUD-SU-7: The O-Cloud should be designed for redundancy and high availability, to maintain uninterrupted service during both the update process and in scenarios of unexpected update failures.

5.1.8.6 Secure Protection of cryptographic keys and sensitive data

5.1.8.6.1 Requirements

REQ-SEC-OCLOUD-SS-1: Sensitive data within the O-Cloud platform shall be protected in terms of integrity and confidentiality at rest, in use and in transit.

REQ-SEC-OCLOUD-SS-2: The O-Cloud platform shall support a secure deletion method from both active and backup storage medias.

REQ-SEC-OCLOUD-SS-3: The O-Cloud platform shall ensure that any data contained in a resource is not available when the resource is de-allocated from one VM/Container and reallocated to a different VM/Container. This requirement requires protection for any data contained in a resource that has been logically deleted or released but may still be present within the resource which in turn may be re-allocated to another VM/Container.

REQ-SEC-OCLOUD-SS-4: The O-Cloud platform shall have the capability that allows an Application to securely erase sensitive data owned by the Application.

EXAMPLE: Sensitive data includes, but is not limited to, cryptographic keys, Personally Identifiable Information (PII), credentials, tokens, and configuration data.

REQ-SEC-OCLOUD-SS-5: The secure deletion method should activate automatically during the boot process after a power outage to prevent unauthorized access to any residual data from all volatile memories, including RAM and cache.

NOTE: Data may linger in volatile memory for a short period after power is lost, potentially allowing for data recovery through cold boot attacks if the system is quickly powered back on.

See Annex C for the guidance to implement REQ-SEC-OCLOUD-SS-5.

5.1.8.6.2 Security Controls

SEC-CTL-OCLOUD-SS-1: The O-Cloud shall support the capability for encryption of all sensitive data, including cryptographic keys, credentials, tokens, and configuration data.

SEC-CTL-OCLOUD-SS-2: The O-Cloud shall support the capability for secure deletion of data in addressable memory locations that are no longer in use due to reallocation. This includes the ability to overwrite these locations with specific binary patterns, such as zeroes, ones, or a random bit pattern.

SEC-CTL-OCLOUD-SS-3: Medias containing sensitive information shall be sanitized using media-specific techniques.

See Annex C for the guidance to implement these controls.

5.1.8.7 Chain of Trust

5.1.8.7.1 Requirements

REQ-SEC-OCLOUD-COT-1: The O-Cloud platform shall support a root of trust that verifies the integrity of every relevant component in the O-Cloud platform [i.1], [i.2].

REQ-SEC-OCLOUD-COT-2: It shall be possible to attest an O-RAN Application through the full attestation chain from the hardware layer through the virtualization layer to the O-RAN Application layer [44], [49].

5.1.8.7.2 Security Controls

SEC-CTL-OCLOUD-COT-1: The chain of trust shall be built from measurements stored in a hardware root of trust.

SEC-CTL-OCLOUD-COT-2: The chain of trust shall be built from measurements stored in a software root of trust for scenarios where a hardware root of trust is not feasible or available.

SEC-CTL-OCLOUD-COT-3: A remote Attestation Service (AS) should be supported for providing additional benefits beside verifying O-Cloud platform integrity by CoT. The remote AS should collect O-Cloud platform configurations and integrity measurements from data center servers at a O-Cloud service provider via a trust agent service running on the O-Cloud platform servers [i.7]. The O-Cloud service provider is responsible for defining allowlisted trust policies. These policies should include information and expected measurements for desired platform CoT technologies. The collected data is compared and verified against the policies, and a report is generated to record the relevant trust information in the AS database [i.7].The remote AS should be extended to include O-RAN Applications integrity.

See Annex C for the guidance to implement these controls.

5.1.8.8 AAL

5.1.8.8.0 Introduction

There are two different scenarios of deployment of the hardware accelerator manager:

- Scenario 1: the hardware accelerator manager is a SW component part of the O-Cloud platform and outside the hardware accelerator device. It is linked to the hardware accelerator device via a vendor specific interface.
- Scenario 2: The hardware accelerator manager is part of the hardware accelerator device. In this scenario, the vendor specific interface does not exist.

For both scenarios, AALI-C-Mgmt interface is the same between the hardware accelerator manager and the O-Cloud IMS/DMS.

AAL components are parts of the O-Cloud platform, therefore the O-Cloud security requirements and controls on image protection, secure update, isolation, secure storage, and chain of trust shall apply to AAL components (see clause 5.1.8).

5.1.8.8.1 Requirements and Security Controls on AAL interfaces

5.1.8.8.1.1 AALI-C-Mgmt

5.1.8.8.1.1.1 Requirements

REQ-SEC-AALI-C-Mgmt-1: The hardware accelerator manager shall authenticate O-Cloud IMS/DMS when O-Cloud IMS/DMS initiates a communication to the hardware accelerator manager over AALI-C-Mgmt interface.

REQ-SEC-AALI-C-Mgmt-2: The hardware accelerator manager shall check whether O-Cloud IMS/DMS is authorized when O-Cloud IMS/DMS accesses the hardware accelerator manager.

REQ-SEC-AALI-C-Mgmt-3: AALI-C-Mgmt interface shall support confidentiality, integrity, and replay protection between the hardware accelerator manager and O-Cloud IMS/DMS.

5.1.8.8.1.1.2 Security Controls

SEC-CTL-AALI-C-Mgmt-1: AALI-C-Mgmt interface shall support TLS as specified in O-RAN Security Protocols Specifications [3], clause 4.2.

SEC-CTL-AALI-C-Mgmt-2: For mutual authentication between the hardware accelerator manager and O-Cloud IMS/DMS, AALI-C-Mgmt interface shall support mTLS as specified in O-RAN Security Protocols Specifications [3], clause 4.2.

SEC-CTL-AALI-C-Mgmt-3: AALI-C-Mgmt interface shall support authorization using OAuth 2.0, as specified in O-RAN Security Protocols Specifications [3], clause 4.7.

5.1.8.8.1.2 Vendor specific interface

5.1.8.8.1.2.1 Requirements

The following requirements apply only for Scenario 1.

REQ-SEC-AAL-VS-1: The hardware accelerator device shall authenticate the hardware accelerator manager when the hardware accelerator manager initiates a communication to the hardware accelerator device over the vendor specific interface.

REQ-SEC-AAL-VS-2: The hardware accelerator manager shall check whether the hardware accelerator device is authorized when the hardware accelerator manager accesses the hardware accelerator device.

REQ-SEC-AAL-VS-3: The vendor specific interface shall support integrity between the hardware accelerator manager and the hardware accelerator device.

REQ-SEC-AAL-VS-4: The vendor specific interface may support confidentiality and replay protection between the hardware accelerator manager and the hardware accelerator device.

NOTE: The implementation of confidentiality and replay protection over the vendor specific interface depends on the capacity/capability of the hardware accelerator device.

5.1.8.8.2 Specific Requirements and Security Controls on AAL components

5.1.8.8.2.1 Requirements

REQ-SEC-AAL-1: The hardware accelerator device shall provide the capability for memory to be cleared securely prior to allocation or when indicated by the AAL Application on returning the memory.

REQ-SEC-AAL-2: The AAL Implementation shall clear memory prior to allocation or when indicated by the AAL Application on returning the memory.

REQ-SEC-AAL-3: The hardware accelerator device shall have a unique identity for a proper identification and tracking of the hardware accelerator device by the hardware acceleration manager.

NOTE: This requirement allows the O-Cloud platform for proper identification and tracking of the accelerator, as well as ensuring that it is not tampered with or replaced without proper authorization.

REQ-SEC-AAL-4: Hardware accelerators should be procured from vendors who can demonstrate the security of their supply chain and manufacturing processes (supply chain security).

REQ-SEC-AAL-5: The hardware accelerator device shall provide the capability for fine grained memory access control. An AAL Application or AAL Profile Instance access shall be restricted to only given buffer(s), and access requests outside that buffer(s) shall fail.

REQ-SEC-AAL-6: The Hardware accelerator manager shall log security events to track and monitor any potential security incidents and to ensure accountability. Such security events include:

- Hardware accelerator failures.
- Hardware accelerator configuration changes.
- Hardware accelerator software update and boot process.
- Hardware accelerator access attempts by unauthorized users/systems, network connectivity issues, successful authentication/authorization events.
- Hardware accelerator performance issues or degradation.

5.1.8.8.2.2 Security Controls

SEC-CTL-AAL-1: The clear memory mechanism should involve overwriting data that was previously stored in the memory with a known pattern, such as all zeros or a random value, to memory buffers.

SEC-CTL-AAL-2: Supply chain audit of hardware accelerator vendors should be performed for establishing trust in vendor's supply chain management based on evidence presented.

NOTE: The evidence can be of different forms and some of them are described below:

- Process to identify and map the hardware accelerator components of each hardware accelerator to the sourcing information.
- A repeatable process of procuring components for building hardware accelerator.
- Ability and procedures to detect counterfeit hardware components.
- Procedures with strict access control measures for hardware accelerator inventory storage, transport, and distribution.

5.1.8.9 O2dms/O2ims/O-Cloud Notification APIs

5.1.8.9.1 Requirements

5.1.8.9.1.1 O2dms

REQ-SEC-OCLOUD-O2dms-1: O-Cloud DMS shall authenticate SMO (NFO or any other entity using O2dms) when SMO initiates a communication to O-Cloud for the deployment and management of Applications over O2dms interface.

REQ-SEC-OCLOUD-O2dms-2: O-Cloud DMS shall be able to establish securely protected connection in terms of confidentiality, integrity, and replay with the SMO (NFO or any other entity using O2dms) over the O2dms interface.

REQ-SEC-OCLOUD-O2dms-3: O-Cloud DMS shall check whether SMO (NFO or any other entity using O2dms) has been authorized when SMO access O-Cloud for the deployment and management of Applications.

REQ-SEC-OCLOUD-O2dms-4: O-Cloud DMS shall log SMO's management operations for auditing.

5.1.8.9.1.2 O2ims

REQ-SEC-OCLOUD-O2ims-1: O-Cloud IMS shall authenticate SMO (FOCOM or any other entity using O2ims) when SMO initiates a communication to O-Cloud for the management of infrastructure over O2ims interface.

REQ-SEC-OCLOUD-O2ims-2: O-Cloud IMS shall be able to establish securely protected connection in terms of confidentiality, integrity, and replay with the SMO (FOCOM or any other entity using O2ims) over the O2ims interface.

REQ-SEC-OCLOUD-O2ims-3: O-Cloud IMS shall check whether SMO (FOCOM or any other entity using O2ims) has been authorized when SMO access the O-Cloud infrastructure.

REQ-SEC-OCLOUD-O2ims-4: O-Cloud IMS shall log SMO's management operations for auditing.

5.1.8.9.1.3 O-Cloud Notification API

REQ-SEC-O-CLOUD-NotifAPI-1: The communication between Applications and the O-Cloud platform through the O-Cloud Notification API shall be mutually authenticated.

REQ-SEC-O-CLOUD-NotifAPI-2: The O-Cloud platform shall provide an authorization framework for the consumption of the services exposed in the O-Cloud Notification API by Applications.

5.1.8.9.2 Security Controls

SEC-CTL-O-CLOUD-INTERFACE-1: For the security protection at the transport layer on O2 interface, TLS shall be supported as specified in O-RAN Security Protocols Specifications [3], clause 4.2.

SEC-CTL-O-CLOUD-INTERFACE-2: For the authorization of O2 RESTful and O-Cloud Notification APIs requests and notifications, OAuth 2.0 shall be supported as specified in O-RAN Security Protocols Specifications [3], clause 4.7.

NOTE: In the actual context of O-Cloud, the platform as API producer shall be responsible to specify those rights/privileges for the platform services as resources to Applications as consumers. As a guideline, an Application should only have the required set of permissions to perform the actions for which they are authorized, and no more.

Authorization mechanisms shall be enforced by the O-Cloud platform in the following procedures:

- Subscription to events/status from the O-Cloud.

SEC-CTL-O-CLOUD-INTERFACE-3: For the mutual authentication between O-Cloud platform and Applications , and between O-Cloud platform and SMO, O2 interface and O-Cloud Notification APIs shall support mutual TLS (mTLS) authentication via X.509v3 certificates as specified in O-RAN Security Protocols Specifications [3], clause 4.2.

5.1.8.10 O-Cloud hardware

5.1.8.10.1 Introduction

This clause contains security requirements and controls on the O-Cloud hardware to protect sensitive data.

5.1.8.10.2 Requirements

REQ-SEC-O-CLOUD-HW-1: O-Cloud hardware deployment shall be protected against unauthorized extraction or inference of sensitive information using physical methods.

NOTE: O-Cloud hardware deployment refers to the hardware used to build the operator's O-Cloud infrastructure.

5.1.8.10.3 Security Controls

SEC-CTL-O-CLOUD-HW-1: O-Cloud hardware deployment should implement physical access restrictions to deny unauthorized access.

NOTE: O-Cloud hardware deployment refers to the hardware used to build the operator's O-Cloud infrastructure.

5.1.8.11 O-Cloud instance ID

5.1.8.11.0 Introduction

The following set of requirements and controls outlines the essential criteria concerning the O-Cloud instance ID. This ID is a cornerstone for uniquely identifying and managing various components, including VMs, pods, containers, nodes, and compute pools within the O-Cloud platform. Safeguarding its global uniqueness, preserving its confidentiality and integrity, and controlling its accessibility are crucial to prevent conflicts, unauthorized access, and potential system compromises.

5.1.8.11.1 Requirements

REQ-SEC-OCLOUD-INST-ID-1: The O-Cloud instance ID shall be unique within the O-Cloud platform to prevent conflicts and ensure accurate identification.

REQ-SEC-OCLOUD-INST-ID-2: The O-Cloud instance ID shall not be exposed in public-facing interfaces, APIs, or logs without proper authentication and authorization mechanisms in place.

REQ-SEC-OCLOUD-INST-ID-3: The O-Cloud instance ID shall be protected to ensure confidentiality and integrity, both during storage (at rest) and while being transmitted (in transit).

REQ-SEC-OCLOUD-INST-ID-4: The O-Cloud instance ID shall be subject to auditing and monitoring, with detailed logs maintained to track activities related to the instance's creation, usage, modification, and deletion.

REQ-SEC-OCLOUD-INST-ID-5: The O-Cloud instance ID shall be associated with a single component, be it a VM, container, pod, node, or compute pool, to ensure clear resource ownership, traceability, and accountability.

5.1.8.11.2 Security Controls

SEC-CTL-OCLOUD-INST-ID-1: O-Cloud instance IDs shall be generated using strong randomization methods to ensure a high degree of uniqueness and minimize the likelihood of collisions.

EXAMPLE: Implementation (Kubernetes-specific):

- Kubernetes generates unique instance IDs, called Pod names, by combining factors like pseudorandom number generators (PRNGs) and contextual information. PRNGs use an initial seed and deterministic algorithms to produce random-like numbers. These numbers, along with contextual elements like timestamps and namespace identifiers, form the basis of the Pod names. This approach ensures that generated names are non-guessable, unpredictable, and unlikely to collide within the Kubernetes cluster. The combination of PRNGs, randomization, and context guarantees that instance IDs are secure, unique, and suitable for identifying pods within the system.

SEC-CTL-OCLOUD-INST-ID-2: O-Cloud should validate newly generated instance IDs against existing IDs to guarantee uniqueness before finalizing instance creation.

5.1.8.12 Time Synchronization and Consistency Requirements for O-Cloud

5.1.8.12.0 Introduction

The requirements listed below highlight the O-Cloud's focus on creating a secure time synchronization framework with NTP as the focus. The requirement and security controls below in this clause are not applicable to PTP. By ensuring each node of the O-Cloud connects to a trusted and authenticated time source, O-Cloud aims to enhance its defences against threats such as clock manipulation, data inconsistencies and operational disruptions.

5.1.8.12.1 Requirements

REQ-SEC-OCLOUD-TS-1: All O-Cloud nodes shall be configured to connect to a secure and authenticated time synchronization server for ToD synchronization.

REQ-SEC-OCLOUD-TS-2: The O-Cloud shall be configured such that ToD synchronization is maintained across all nodes in an O-Cloud compute pool, there by guaranteeing uniform time references for all applications hosted on these nodes.

REQ-SEC-OCLOUD-TS-3: The O-Cloud shall guarantee that the timestamp consistency is preserved even when applications are relocated across different nodes of the O-Cloud infrastructure.

NOTE 1: Timestamp refers to:

1. **Log/event timestamps:** These are associated with each log entry generated. Examples include application start/stop, application relocation, node failures, network events, change in applications and O-Cloud configuration, resource allocation, deallocation, etc.
2. **Data Transaction timestamps:** For applications that rely on time-sensitive data within O-Cloud, consistent timestamps are crucial. Whenever data is read, written, or modified, a timestamp is generated to ensure both data integrity and consistency across nodes.

REQ-SEC-OCLOUD-TS-4: The O-Cloud shall guarantee that various instances of an identical application, irrespective of their location, generate logs with consistent timestamps.

NOTE 2: Within the O-Cloud infrastructure, a "consistent timestamp" denotes the synchronized and uniform chronological markers generated by various instances of an identical application, irrespective of their location. This uniformity ensures that aggregated or analysed logs from different instances present a coherent chronological sequence, aiding in precise event correlation and analysis. To achieve and maintain this consistency, it is recommended for O-Cloud to synchronize its internal clocks with trusted time sources, such as NTP servers, guaranteeing both the accuracy and trustworthiness of these timestamps.

REQ-SEC-OCLOUD-TS-5: All O-Cloud nodes within a compute pool, especially those serving a specific geographic region or co-located, shall be configured to operate using a consistent time reference, preferably UTC with a Time Zone (TZ) modifier.

NOTE 3: This requirement ensures:

1. **Uniformity in Time-Related Operations:** Simplifies the process of correlating logs, events, and time-sensitive operations across nodes, aiding in quicker identification of anomalies or malicious activities.
2. **Operational Consistency:** Ensures that scheduled tasks, backups, updates, or maintenance activities are executed consistently across the compute pool.
3. **Data Integrity:** Provides consistency for applications and databases that rely on timestamps for transactions, ensuring no discrepancies due to time differences.

5.1.8.12.2 Security Controls

SEC-CTL-OCLOUD-TS-1: The O-Cloud shall ensure that all nodes are configured to exclusively connect to a secure and authenticated time synchronization server for Time of Day (ToD) synchronization.

EXAMPLE 1:

- **NTP Usage:** The O-Cloud should primarily use the Network Time Protocol (NTP) for general time synchronization needs, ensuring consistent timestamps for operations such as logging security events. This connection should prioritize the use of NTP with authentication mechanisms in place to ensure the integrity and authenticity of the time data. The authentication mechanisms provided by NTPv4 should be employed for NTP. This includes the use of symmetric key cryptography to authenticate the time server. Additionally, consideration will be given to implementing NTP over MACsec to enhance security, ensuring the confidentiality and integrity of the time synchronization data.

SEC-CTL-OCLOUD-TS-2: All O-Cloud nodes shall be configured to synchronize their clocks exclusively with centralized time servers at regular intervals to ensure uniformity in time-related operations and data across the O-Cloud infrastructure.

EXAMPLE 2: Time synchronization protocol such as NTP can be used to achieve this consistency.

- **NTP:** While NTP provides millisecond-level accuracy, it is widely adopted and can be sufficient for many applications in the O-Cloud. The reference points here would be the stratum 1-time servers or atomic clocks that NTP servers synchronize with.

SEC-CTL-OCLOUD-TS-3: The O-Cloud should establish multiple time servers for redundancy. This ensures that nodes can switch to an alternative trusted server if the primary server becomes unavailable, thereby maintaining consistent time synchronization.

EXAMPLE 3:

- **NTP Redundancy:** By configuring nodes to have a list of NTP servers, they can automatically switch to a secondary or tertiary server if the primary server fails. This ensures continuous time synchronization and mitigates the risk of a single point of failure.

NOTE: See clause 5.3.8.9.2 for additional security controls.

5.1.9 Shared O-RU

5.1.9.1 Security Requirements

REQ-SEC-SharedORU-1: The Shared O-RU shall mutually authenticate with an O-RU Controller.

REQ-SEC-SharedORU-2: The Shared O-RU shall provide least privilege access to each SRO based upon its sro-id.

REQ-SEC-SharedORU-3: The Shared O-RU shall provide separate confidentiality and integrity protection of data-at-rest for the Host MNO and each SRO.

REQ-SEC-SharedORU-4: The Shared O-RU shall provide separate confidentiality, integrity, and replay protection for data-in-transit for the Host MNO and each SRO.

REQ-SEC-SharedORU-5: The Shared O-RU shall support Multi-Factor Authentication (MFA) for human user login.

REQ-SEC-SharedORU-6: The Shared O-RU shall support access controls for human users to access data.

REQ-SEC-SharedORU-7: The Shared O-RU shall be able to recover, without catastrophic failure, from a volumetric DDoS attack due to misbehavior or malicious intent.

REQ-SEC-SharedORU-8: The Shared O-RU shall support event logging with tenant-awareness.

5.1.9.2 Security Controls

SEC-CTL-SharedORU-1: The Shared O-RU shall support mTLS 1.2, or higher, as specified in O-RAN Security Protocols Specifications [3], clause 4.2 for mutual authentication on the M-Plane interface with an O-RU Controller.

SEC-CTL-SharedORU-2: The Shared O-RU should not use password-based authentication with an O-RU Controller.

SEC-CTL-SharedORU-3: The Shared O-RU shall support NACM for permitting or denying access to an SRO.

SEC-CTL- SharedORU-4: The Shared O-RU shall support TLS 1.2, or higher, as specified in O-RAN Security Protocols Specifications [3], clause 4.2, for confidentiality and integrity protection of data-in-transit on the M-Plane interface with an O-RU Controller.

5.2 Interfaces maintained by O-RAN

5.2.1 A1 Interface

5.2.1.0 Introduction

The A1 Interface is defined in the A1 specifications [5].

5.2.1.1 Requirements

REQ-SEC-A1-1: A1 interface shall support confidentiality, integrity, replay protection.

REQ-SEC-A1-2: A1 interface shall support mutual authentication and authorization.

5.2.1.2 Security Controls

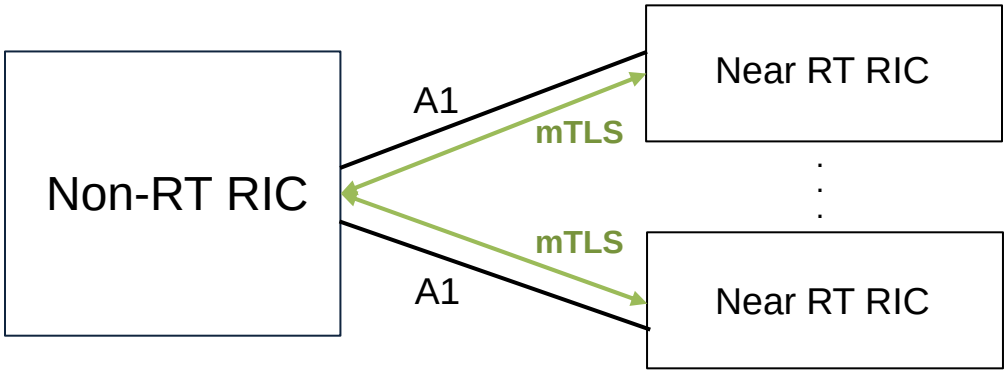

Figure 5.2.1.2-1: mTLS on A1 interface

SEC-CTL-A1-1: For the security protection at the transport layer on A1 interface, TLS shall be supported as specified in O-RAN Security Protocols Specifications [3], clause 4.2.

SEC-CTL-A1-2: For the mutual authentication of the Non-RT RIC and one or more Near-RT RICs, the A1 interface shall support mTLS as shown in Figure 5.2.1.2-1 and specified in O-RAN Security Protocols Specifications [3], clause 4.2.

SEC-CTL-A1-3: The A1 interface shall support authorization using OAuth 2.0, as specified in O-RAN Security Protocols Specifications [3], clause 4.7.

5.2.2 O1 Interface

5.2.2.0 Introduction

O1 Interface connecting the SMO to the Near-RT RIC, may have one or more O-CU-CPs, one or more O-CU-UPs, and one or more O-DUs.

5.2.2.1 Requirements

5.2.2.1.1 Summary

This clause specifies the requirements for O1 NACM support post function initialization when the function is in operation. NACM requirements related to network function initialization and when repairing broken access control configuration will be addressed in a future release of the present document.

5.2.2.1.2 Confidentiality, Integrity and Authenticity

REQ-TLS-FUN-1: O1 interface implementations that support TLS for confidentiality and integrity protection shall support TLS as specified in O-RAN Security Protocols Specification [3], clause 4.2.

REQ-TLS-FUN-2: O1 interface implementations that support mTLS for mutual authentication shall support mTLS 1.2, or higher, as specified in O-RAN Security Protocols Specification [3], clause 4.2.

REQ-TLS-FUN-3: The O1 interface in a Shared O-RU configuration shall support mTLS 1.2, or higher, as specified in O-RAN Security Protocols Specifications [3], clause 4.2, for mutual authentication.

REQ-TLS-FUN-4: The O1 interface in a Shared O-RU configuration shall support TLS 1.2, or higher, as specified in O-RAN Security Protocols Specifications [3], clause 4.2, for confidentiality and integrity protection of data-in-transit.

5.2.2.1.3 Least Privilege Access Control

REQ-NAC-FUN-1: Management Service providers and consumers that use NETCONF shall support the Network Configuration Access Control Model (NACM) as specified in IETF RFC 8341 [10] to restrict NETCONF protocol access for users to a preconfigured subset of available NETCONF protocol operations and content.

REQ-NAC-FUN-2: The NETCONF implementation for O1 shall set the default values of the NACM Global Enforcement Controls as follows:

- enable-nacm = true
- read-default = permit
- write-default = deny
- exec-default = deny
- enable-external-groups = true

REQ-NAC-FUN-3: Management Service providers that support NETCONF shall support the following pre-defined groups in NACM to restrict NETCONF protocol access for users:

- O1_nacm_management: Allows changes to the /nacm objects which includes the NACM Global Enforcement Controls.
- O1_user_management: Allows assignment and deletion of users and assignment of users to roles on the O1 node.
  - **Mandatory** if the network device supports a local user store.
  - **Not provided** if the network device does not support a local user store and requires all user/role information to be provided by an external authentication/authorization service.
- O1_network_management: Allows read, write, and execute operations on the datastores. All operations on the /nacm objects are prohibited.
- O1_ network_monitoring: Allows read operations on configuration data in the datastore, except for the /nacm objects.
- O1_software_management: Allows installation of new software including new software versions for a PNF.

REQ-NAC-FUN-4: Users assigned to the O1_nacm_management group shall have read and write permission for the /nacm objects and attributes.

REQ-NAC-FUN-5: Users assigned to the O1_user_management group shall have read and write permissions for the locally defined user store objects and attributes.

REQ-NAC-FUN-6: Users assigned to the O1_network_management group shall have read, write, and execute permissions for the datastores. Users assigned to the O1_network_management group shall not have any permissions for the /nacm objects.

REQ-NAC-FUN-7: Users assigned to the O1_network_monitoring group shall have read permissions for the datastores. Users assigned to the O1_network_monitoring group shall not have read permissions for the /nacm objects.

REQ-NAC-FUN-8: Users assigned to the O1_software_management group shall have permissions to install new software on the PNF.

REQ-NAC-FUN-9: NETCONF endpoints shall support external user-to-group mapping via at least one of the following protocols: LDAP with StartTLS [11], OAuth 2.0, RADIUS with EAP, and TACACS/TACACS+.

REQ-NAC-FUN-10: Management Service providers may allow the definition of users in the <groups> NACM object.

5.2.2.2 Security Controls

As defined in the previous clause 5.2.2.1.2, the O1 will use TLS 1.2 or higher to enforce confidentiality, integrity, and authenticity; and will use NACM [10] to enforce least privileged access.

5.2.3 O2 Interface

5.2.3.0 Introduction

General Aspects and Principles of O2 Interface between the SMO and the O-Cloud are defined in [6].

5.2.3.1 Requirements

REQ-SEC-O2-1: O2 interface shall support confidentiality, integrity, replay protection and data origin authentication.

5.2.3.2 Security Controls

SEC-CTL-O2-1: Management Service providers and consumers that use TLS shall support TLS as specified in O-RAN Security Protocols Specifications [3], clause 4.2.

5.2.4 E2 Interface

5.2.4.0 Introduction

General Aspects and Principles of E2 Interface connecting the Near-RT RIC and one or more O-CU-CPs, one or more O-CU-UPs, one or more O-DUs, and one or more O-eNBs are defined in [7].

5.2.4.1 Requirements

REQ-SEC-E2-1: E2 interface shall support confidentiality, integrity, replay protection and data origin authentication.

5.2.4.2 Security Controls

SEC-CTL-E2-1: For the security protection at the IP layer on E2 interface, IPsec shall be supported as specified in O-RAN Security Protocols Specifications [3], clause 4.5.

5.2.5 Open Fronthaul Interface

5.2.5.1 C-plane

5.2.5.1.1 Introduction

The O-DU sends UL C-plane messages and DL C-plane messages to O-RU to trigger transmission and reception of RF signals. The DL C-plane message describing multiple symbols must arrive at O-RU within a certain time window for the O-RU to successfully receive DL I/Q data in U-plane messages from O-DU. Likewise, the UL C-plane message describing multiple symbols must arrive within a certain time window for the O-RU to successfully receive RF signal and send UL I/Q data in U-plane messages to O-DU. Any delay of these messages would cause the O-RU to drop/discard U-plane traffic from O-DU and the UE [31].

An adversary can inject its own DL C-plane or UL C-plane messages by spoofing the associated O-DU. As a result, it would block the O-RU from processing the corresponding U-Plane packets received from the O-DU and O-RU respectively, leading to temporary DoS and, limited cell performance on cells served by the O-RU [4].

5.2.5.1.2 Requirements

REQ-SEC-OFCP-1: The C-Plane shall support authentication and authorization of O-DUs that exchange C-plane messages with O-RUs.

REQ-SEC-OFCP-2: The O-DU shall be able to detect and defend against application level attacks across the C-Plane messages with O-RUs, due to misbehavior or malicious intent.

5.2.5.1.3 Security Controls

5.2.5.1.3.1 Authentication and Authorization of network elements supporting the C-Plane

This clause addresses requirements REQ-SEC-OFCP-1 based on the use of IEEE 802.1X-2020 Port-based Network Access Control [12] for authentication and subsequent authorization of nodes that exchange C-Plane messages.

Clause 5.2.5.5 of the present document provides requirements and security controls for the authentication and authorization of an O-DU and other network elements supporting the C-Plane within Open Fronthaul point-to-point LAN segments.

5.2.5.2 U-plane

5.2.5.2.1 Requirements

Open Fronthaul U-plane transports 5G System Control Plane and User Plane messages between O-CU-CP and UE, and O-CU-UP and UE. The Packet Data Convergence Protocol (PDCP) [32] is an optional feature that may provide confidentiality and integrity protection of 5G System Control Plane and User Plane between O-CU-CP and UE, and O-CU-UP and UE.

5.2.5.2.2 Security Controls

5.2.5.3 S-plane

5.2.5.3.1 Introduction

The Precision Time Protocol (PTP) is a protocol used to synchronize clocks within a PTP network. Within a PTP domain [27], the grandmaster clock is the source of time to which all other PTP clocks in the domain are synchronized.

The IEEE 1588 standard specifies the Best Master Clock Algorithm (BMCA) for electing the best clock from PTP Network and Local PTP Clock. The BMCA runs on PTP instances in the network continuously and is adjusting to changes in that network. PTP ANNOUNCE messages are used to build a timing distribution hierarchy with grandmaster at the top. There can be many grandmasters in PTP Network, but PTP Domain can have only one. The chosen grandmaster clock is responsible for providing timing to the PTP slave nodes.

Following the selection of the new grandmaster, the grandmaster begins transmitting the current time within the SYNC message and FOLLOW_UP messages if applicable. This allows the other clocks to synchronize their time to the grandmaster.

S-Plane attacks include an attacker masquerading as a grandmaster or manipulating PTP to degrade synchronization. Details are covered in clause 5.4.1.2 of [4].

The two most common deployment models for O-DU in O-RAN are:

- O-DU at the cell site deployment model: the O-DU is collocated with the O-RU with a direct connection between the two (LLS-C1) through a cell site gateway router.
- O-DU at the Data Centre deployment model: the O-DU is at a Data Centre. The O-RU's at the cell site connect to the O-DU via a direct connection between O-RU and O-DU (LLS-C1) or intermediary Ethernet switches (LLS-C2 or LLS-C3).

5.2.5.3.2 Requirements

REQ-SEC-OFSP-1: The S-Plane shall support authentication and authorization of PTP nodes that communicate with other PTP nodes within Configuration LLS-C1, Configuration LLS-C2, or Configuration LLS-C3.

NOTE 1: This ensures least privilege access to the S-Plane where authenticated and authorized PTP nodes communicate over the Open Fronthaul network.

NOTE 2: There is no specific requirement for authentication and authorization mechanism of S-plane PTP messages.

REQ-SEC-OFSP-2: The S-Plane should provide a means to prevent spoofing of master clocks.

REQ-SEC-OFSP-3: For the O-DU at the Data Centre deployment model the S-Plane should protect against MITM attacks that degrade the clock accuracy due to packet delay attacks or selective interception and removal attacks [28].

REQ-SEC-OFSP-4: The O-DU shall be able to detect and defend against application level attacks across the S-Plane interface, due to misbehavior or malicious intent.

5.2.5.3.3 Security Controls

5.2.5.3.3.1 Synchronization Architecture Redundancy

This clause addresses requirement REQ-SEC-OFSP-3 by providing an architectural recommendation to S-plane security based on redundancy in the Open Fronthaul Synchronization architecture.

The following architectural recommendations for security controls build S-Plane redundancy into to the Open Fronthaul for increased robustness against security breaches.

SEC-CTL-OFSP-1: The Open Fronthaul Synchronization architecture should support simultaneous Grandmasters.

SEC-CTL-OFSP-2: The Open Fronthaul Synchronization architecture should support the assignment of GMs to physically separated PTP ports. Multiple masters could be connected to offer topology resilience.

O-RAN Synchronization Architecture and Solution Specification [30], clause 8.2.3 Timing/Synchronization Redundancy & Resiliency provides additional details on redundancy for the Open Fronthaul Synchronization architecture.

5.2.5.3.3.2 Authentication and Authorization of PTP nodes

This clause addresses requirements REQ-SEC-OFSP-1 and REQ-SEC-OFSP-2 based on the use of IEEE 802.1X-2020 [12] Port-based Network Access Control for authentication and subsequent authorization of PTP nodes.

Clause 5.2.5.5 of the present document provides requirements and security controls for the authentication and authorization of S-Plane PTP nodes within Open Fronthaul point-to-point LAN segments.

5.2.5.4 M-plane

5.2.5.4.1 Requirements

The security requirements for M-Plane are defined in [14].

5.2.5.4.2 Security Controls

The security controls for M-plane are defined in [14].

5.2.5.5 Open Fronthaul Point-to-Point LAN Segment

5.2.5.5.0 Introduction

The Open Fronthaul Ethernet L1 physical interface comprises one or more coaxial cables, twisted pairs, or optical fibers. These are also known as point-to-point LAN segments [12]. Each end of the Open Fronthaul point-to-point LAN segment comprises a physical connection (colloquially known as an Ethernet Port) to physical O-RAN network elements, as described in [13] and [14].

EXAMPLE: Physical O-RAN network elements includes O-DU, O-RU.

An Open Fronthaul network element is an entity in a point-to-point LAN segment. Xhaul Transport Network Elements that share a point-to-point LAN segment with Open Fronthaul network elements are also Open Fronthaul network elements. Examples of O-RAN Alliance defined Open Fronthaul network elements include, but are not limited to, O-DU, O-RU, switches, FHM, FHGW, TNE and PRTC-T/GM [13], [14], [15], [26].

5.2.5.5.1 Requirements

REQ-SEC-OFHPLS-1: The Open Fronthaul shall provide a means to authenticate and authorize point-to-point LAN segments between Open Fronthaul network elements.

REQ-SEC-OFHPLS-2: The Open Fronthaul shall provide a means to detect and report when an authorized point-to-point LAN segment is made or broken.

REQ-SEC-OFHPLS-3: The Open Fronthaul shall provide a means to block access to unused Ethernet ports in an Open Fronthaul network element.

Open Fronthaul implementations may support IEEE 802.1X-2020 [12] to satisfy the requirements listed above. Implementations that support optional 802.1X shall provide the security controls as specified in clause 5.2.5.5.2.

5.2.5.5.2 Security Controls

5.2.5.5.2.1 Solution #1: Authentication and Authorization based on 802.1x Port based Network Access Control

IEEE 802.1X-2020 is optional to support.

NOTE 1: Further security requirements for IEEE 802.1X-2020 [12] will continue to be studied. It is intended to evolve IEEE 802.1X-2020 [12] to a mandatory requirement for the Open Fronthaul interface after completion of the study.

IEEE 802.1X-2020 Port-based Network Access Control [12] provides the means to control network access in point-to-point LAN segments within the Open Fronthaul network. Port-based network access control in the O-RAN Alliance Open Fronthaul comprises supplicant, authenticator, and authentication server entities described in IEEE 802.1X-2020 [12] and as further described in this clause. All other entities and functionality described in IEEE 802.1X are out of scope of this O-RAN Alliance specification and are determined by vendor implementation in agreement with operator-specific requirements.

SEC-CTL-OFHPLS-1: Operator implementation of IEEE 802.1X-2020 [12] for Open Fronthaul port-based network access control is optional to use for each point-to-point LAN segment.

Supplicants in the Open Fronthaul Network

SEC-CTL-OFHPLS-2: Open Fronthaul network elements shall support IEEE 802.1X-2020 [12] supplicant functionality for each port connection in the Open Fronthaul network element.

Authenticators in the Open Fronthaul Network

In IEEE 802.1X-2020 [12] a supplicant mutually authenticates with an authenticator.

SEC-CTL-OFHPLS-3: Any Open Fronthaul network element may be an authenticator in the Open Fronthaul network.

SEC-CTL-OFHPLS-4: An authenticator in an Open Fronthaul network shall perform port-based network access control on each point-to-point LAN segment as defined in IEEE 802.1X-2020 [12].

SEC-CTL-OFHPLS-5: Port-based network access control between a supplicant and authenticator in an Open Fronthaul network shall use EAP-TLS authentication as defined in IEEE 802.1X-2020 [12].

O-DU as an Authenticator

Configuration LLS-C1 [13] and Cascade Mode in the Shared Cell Concept [12] are cases where an O-DU and O-RU are Open Fronthaul network elements in a point-to-point LAN segment.

SEC-CTL-OFHPLS-6: In the case of Configuration LLS-C1, the O-DU shall support the authenticator functionality as defined in IEEE 802.1X-2020 [12].

Authenticator interface to an Authentication Server in the Open Fronthaul Network

IEEE 802.1X [12] describes an EAP-TLS exchange which includes an interface between an authenticator and authentication server.

SEC-CTL-OFHPLS-7: The interface between an authenticator and authentication server shall support IETF RADIUS standards, IETF RFC 2865 [22], IETF RFC 2866 [23], IETF RFC 3579 [24], and successor standards.

SEC-CTL-OFHPLS-8: The interface between an authenticator and authentication server should support IETF Diameter standards, IETF RFC 4072 [25] and successor standards.

NOTE 2: Mechanisms to secure the interface between the authenticator and authentication server are out of scope of the O-RAN Alliance.

5.2.5.5.2.2 Authentication and authorization procedure for 802.1x Port based Network Access Control

General requirements

Only those Open Fronthaul network elements acting as a supplicant that have mutually authenticated with an authenticator are authorized to participate in the Open Fronthaul network. If an authenticator port is to be activated in the Open Fronthaul, then the authenticator places the port into an unauthorized state that allows EAP over LAN (EAPOL) packets for EAP authentication and blocks all other traffic. If the mutual authentication has been successful and the operator authorizes operation for the network element port, then the port is switched to the authorized state whereby non-EAPOL packets can be sent and received.

SEC-CTL-OFHPLS-9: Open Fronthaul network elements acting as an authenticator shall place each of its unauthorized ports into a state that allows EAPOL traffic and block all other Ethernet traffic.

SEC-CTL-OFHPLS-10: Open Fronthaul network elements acting as an authenticator should be able to implement authorization policies that apply to its authorized ports. Authorization policies may include tagging authorized traffic with a particular VLAN-ID as it egresses the Open Fronthaul network element and/or enforcing access control policies that restrict the type of traffic able to be forwarded by the Open Fronthaul network element.

Manufacturer Install Certificates

This clause applies to the Extensible Authentication Protocol as defined in IEEE 802.1X [12] where such an approach is used. A supplicant implements an EAP method according to its supported credentials. Prior to a supplicant enrolling in an operator's PKI, a manufacturer installed certificate shall be used together with an EAP-TLS dialogue to enable certificate-based mutual authentication to be performed between an authenticator and a supplicant.

SEC-CTL-OFHPLS-11: The O-RU shall have installed a Manufacturer Installed X.509 Certificate.

Security Procedure

The following procedure describes the authentication and authorization, based on IEEE 802.1 Port based Network Access Control, of point-to-point LAN segments between a supplicant and another Open Fronthaul network element acting as an authenticator.

SEC-CTL-OFHPLS-12: The normal operation procedure defined in IEEE 802.1X [12] shown in Figure 5.2.5.5.2.2-1 and Figure 5.2.5.5.2.2-2 shall be performed to authenticate and authorize an O-RU within an Open Fronthaul network.

```
@startuml
!pragma teoz true
skinparam defaultTextAlignment center

participant "Authentication\nServer" as AAA
participant "IEEE 802.1x\nAuthenticator" as AUT
participant "IEEE 802.1x \nSupplicant" as SUP


note over AAA
  Manufacturer Trust
  Root Installed
end note
```

```
&note over SUP
  Manufacturer Installed
  X.509 Certificate
end note


&note over AUT
  Port in unauthorized
  state - blocks all
  traffic other than
  EAPOL traffic
end note

group Initial limited-access when authenticated using manufacturer certificate
    SUP->AUT: EAPoL Start
    AUT->SUP: EAP-Request/Identity
    SUP->AUT: EAP-Response/Identity (from Manufacturer Installed X.509 Certificate
Subject DN)

    AUT->AAA: RADIUS-Access-Request or Diameter-EAP-Request (EAP-Response)
    AAA->AUT: RADIUS-Access-Challenge or Diameter-EAP-Answer (EAP-Request)
    AUT->SUP: EAPoL (EAP-Request)
    note over AAA, SUP
      EAP Dialogue Continues using Manufacturer Installed X.509 Certificate
    end note
    AAA->AAA: Select Security Policy \nfor Manufacturer Installed X.509 Certificate
    AAA->AUT: RADIUS-Access-Accept or Diameter-EAP-Answer (EAP-Success) \nIncluding
security policy, e.g. Provisioning/Enrollment VLAN
    AUT->SUP: EAP-Success

    AUT->AUT: Set port to authorized state.\nAssign port to provided security policy,
\ne.g., Provisioning/Enrollment VLAN
end

group Enrollment into operator PKI
    note over AUT, SUP
      Certificate Enrollment Completes & Provision of Operator X.509 Certificate
    end note

    SUP->SUP: Install\nOperator X.509\nCertificate
end


group Subsequent full operational access when authenticated using operator installed
certificate


    note over SUP
      re-start of Supplicant
      triggers interface
      re-initialization
    end note

    note over AUT
      Interface re-initialization:
      resets port to unauthorized
      state - blocks all traffic
      other than EAPOL traffic
    end note

    SUP->AUT: EAPoL Start
    AUT->SUP: EAP-Request/Identity
    SUP->AUT: EAP-Response/Identity (from Operator X.509 Certificate Subject DN)

    AUT->AAA: RADIUS-Access-Request or Diameter-EAP-Request (EAP-Response)
    AAA->AUT: RADIUS-Access-Challenge or Diameter-EAP-Answer (EAP-Request)
    AUT->SUP: EAPoL (EAP-Request)
    note over AAA, SUP
      EAP Dialogue Continues using Operator Installed X.509 Certificate
```

```
    end note
    AAA->AAA: Select Security Policy\nfor Operator Installed X.509 Cert
    AAA->AUT: RADIUS-Access-Accept or Diameter-EAP-Answer (EAP-Success) \nIncluding
security policy, e.g. Operational VLAN
    AUT->SUP: EAP-Success

    AUT->AUT: Set port to authorized state.\nAssign port to provided security policy,
\ne.g., Operational VLAN


    note over SUP
      Normal Supplicant
      start up continues
    end note

end

@enduml
```

Figure 5.2.5.5.2.2-1: UML code for 802.1X Port Based Authentication in the O-RAN Fronthaul architecture

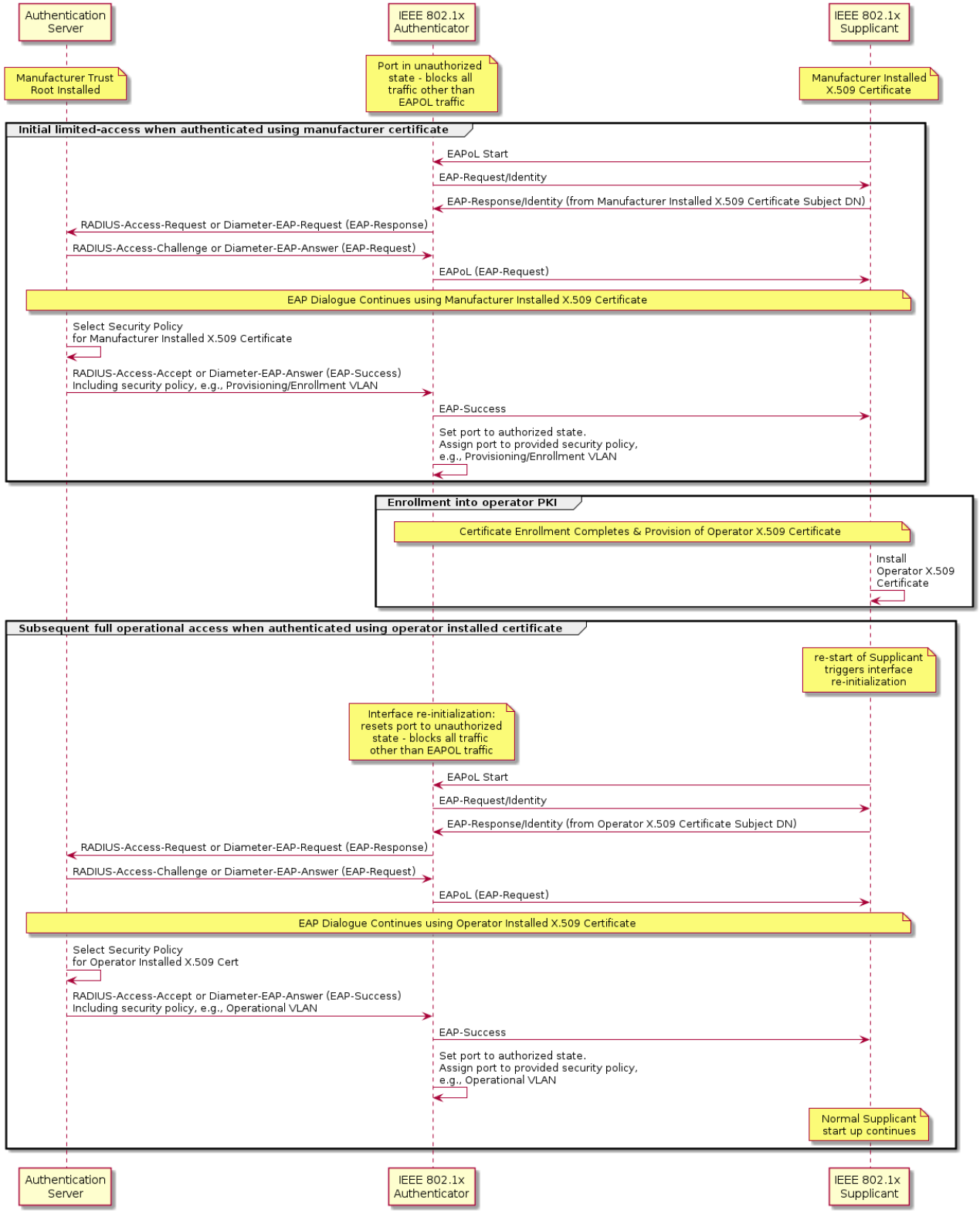

Figure 5.2.5.5.2.2-2: Operation of 802.1X Port Based Authentication in the O-RAN Fronthaul architecture

The authentication and authorization procedure may fail at any moment, for example because of no response from the supplicant after a network request. In that case, the operation procedure as specified in Figure 5.2.5.5.2.2-1 will be terminated as specified in IEEE 802.1X-2020 [12].

5.2.6 R1 Interface

5.2.6.0 Introduction

R1 is the interface between rApps and Non-RT RIC Framework via which R1 Services can be produced and consumed. See R1 specification [39].

5.2.6.1 Requirements

REQ-SEC-R1-1: R1 interface shall support confidentiality, integrity, and replay protection.

REQ-SEC-R1-2: R1 interface shall support mutual authentication and authorization.

5.2.6.2 Security Controls

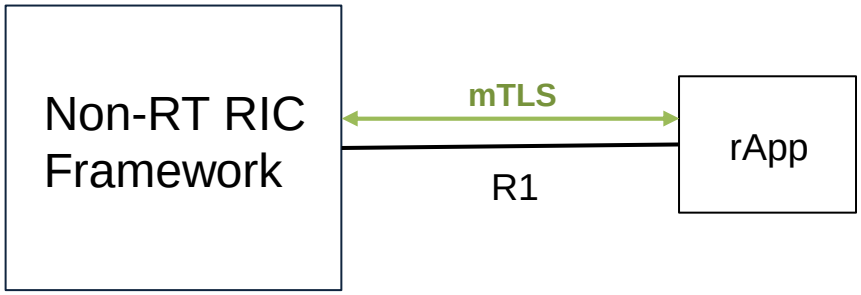

Figure 5.2.6.2-1: mTLS on R1 interface

SEC-CTL-R1-1: For the security protection at the transport layer on R1 interface, TLS shall be supported as specified in O-RAN Security Protocols Specifications [3], clause 4.2.

SEC-CTL-R1-2: For the mutual authentication of the Non-RT RIC Framework and rApps, the R1 interface shall support mTLS as shown in Figure 5.2.6.2-1 and specified in O-RAN Security Protocols Specifications [3], clause 4.2.

SEC-CTL-R1-3: The R1 interface shall support authorization using OAuth 2.0, as specified in O-RAN Security Protocols Specifications [3], clause 4.7.

5.2.7 Y1 Interface

5.2.7.1 Introduction

The Near-RT RIC provides RAN analytics information services via Y1 service interface. These services can be consumed by Y1 consumers by subscribing to or requesting the RAN analytics information via the Y1 service interface. Y1 consumers may be Application Functions (AFs). The Near-RT RIC serves as Y1 provider.

5.2.7.2 Requirements

REQ-SEC-Y1-1: The Y1 provider shall provide mechanisms to authenticate the Y1 consumer and allow for the Y1 consumer to authenticate the Y1 provider (mutual authentication).

REQ-SEC-Y1-2: The Y1 provider shall authorize the Y1 consumer before allowing access to any service over the Y1 interface.

REQ-SEC-Y1-3: The Y1 interface shall provide confidentiality and integrity protection for all data exchanged.

REQ-SEC-Y1-4: The Y1 interface shall provide replay-protection for all data exchanged.

REQ-SEC-Y1-5: The Y1 interface shall enforce the result of the authentication for the duration of communications.

REQ-SEC-Y1-6: The Near-RT RIC shall hide its topology from the Y1 consumers accessing the Y1 interface.

5.3 Transversal requirements

5.3.1 Software Bill of Materials

Void.

5.3.1.1 Requirements

Void.

5.3.2 Common Application Lifecycle Management

5.3.2.1 Package Protection

5.3.2.1.1 Requirements

REQ-SEC-ALM-FUN2-1: VOID.

REQ-SEC-ALM-FUN3-1: VOID.

REQ-SEC-ALM-PKG-1: The Application package shall be certified by the Application Provider.

EXAMPLE 1: Software testing suites for certification include vulnerability scanning, static and dynamic testing, and penetration testing. Refer to clause C.2.1 for additional information.

REQ-SEC-ALM-PKG-2: The Application package shall be signed by the Application Provider prior to its delivery to the Service Provider to ensure its authenticity and integrity.

REQ-SEC-ALM-PKG-3: The Application package shall include minimally the following artifacts according to [41], [42]: the Application software image, the signing certificate, and signature(s) of Application Provider.

REQ-SEC-ALM-PKG-4: Each Application package artifact shall be digitally signed individually by the Application Provider [41], [42].

REQ-SEC-ALM-PKG-5: The SMO shall verify all Application package artifacts upon reception using the signatures generated and provided by the Application Provider.

REQ-SEC-ALM-PKG-6: The Application package shall be validated by SMO upon its reception using the signature generated and provided by the Application Provider.

REQ-SEC-ALM-PKG-7a: The Application package shall be tested by the Service Provider for known security vulnerabilities. All discovered vulnerabilities shall be reported to the Application Provider.

REQ-SEC-ALM-PKG-7b: The Application Provider shall have a vulnerability management process in place allowing the Service Provider to report discovered vulnerabilities.

REQ-SEC-ALM-PKG-7c: Vulnerabilities discovered in Application packages during testing by Service Provider shall be remediated by the Application Provider.

REQ-SEC-ALM-PKG-8: The Application package shall be cryptographically bound to one Service Provider before its onboarding to the catalogue [i.11] and [16]. This prevents an unauthorized package to be instantiated even if it has valid Application certificate [41], [44] and [45].

REQ-SEC-ALM-PKG-9: Signatures shall be renewed before the certificate reaches the end of its validity period (signatures provided by the Application Provider may be ignored if the signature of the Service Provider is valid).

REQ-SEC-ALM-PKG-10: Application packages stored within the catalogue [i.11] and [16] shall be protected in terms of integrity and confidentiality.

REQ-SEC-ALM-PKG-11: Application packages stored within the catalogue [i.11] and [16] shall be accessible to only authorized entities and over networks that enforce authentication, integrity, and confidentiality.

REQ-SEC-ALM-PKG-12: Catalogue [i.11] and [16] shall be clear of vulnerable Application packages and of packages with missing certificates.

REQ-SEC-ALM-PKG-13: Sensitive information used during the lifecycle of the Application shall be protected in terms of confidentiality at rest and in transit [46], [41] and [42].

EXAMPLE 2: Sensitive information includes LI Applications, keys, PII, passwords and other critical configuration data.

REQ-SEC-ALM-PKG-14: SMO shall contain a pre-installed root certificate of trusted CA (trusted by the Service Provider) before the onboarding of the Application package for verifying its authenticity and integrity. Root certificate shall be delivered via a trusted channel separately from an Application package [42].

REQ-SEC-ALM-PKG-15: Application packages shall have a Change Log. All the changes in the Application package shall be versioned, tracked, and inventoried in the Change Log [43].

NOTE: Change log can also be provided separately as an external artifact.

5.3.2.1.2 Security Controls

SEC-CTL-ALM-PKG-1: Application package shall be signed and verified for integrity and authenticity protection.

To provide the authenticity and integrity protection for the Application package, one of the two following options shall be followed as defined in ETSI GS NFV-SEC 021 [41] and ETSI GS NFV-SOL 004 [42]:

- Option 1: The Application package contains a Digest (a.k.a. hash) for each of the artifacts of the Application package. The table of hashes is signed with the Application Provider private key.
- Option 2: The complete Application package is signed with the Application Provider private key.

The signature verification process comprises the following steps:

Responsible: Application Provider, Service Provider

1) A signed Application package shall be delivered to the Service Provider containing the Application package, the signing X.509v3 certificate, and the signature (signed hash value) of Application Provider.
2) The root CA certificate shall be pre-installed within the NFO for the validation of the Application Provider signing certificate.
3) Upon reception of the signed Application package from Application Provider by the Service Provider.
4) New hash(es) of the received Application package shall be calculated and verified by the Service Provider against the hash(es) in the signature using the Application Provider certificate retrieved from the received Application package.
5) Service Provider shall sign the verified Application package prior to its onboarding.
6) Service Provider shall compute the hash value of the Application package and the signature of the Application Provider.
7) The hash value shall be signed with the private key(s) of the Service Provider.
8) A signed Application package shall be onboarded containing the Application package, certificate(s), and signature(s) (signed hash value) of the Application Provider and Service Provider.
9) During instantiation, the Application package shall be authenticated and verified using signatures from both Application Provider and Service Provider.

SEC-CTL-ALM-PKG-1A: Algorithms, key sizes, and standards to be used for signature generation/verification shall follow the "O-RAN Security Protocol Specification" [3], clause 5.

SEC-CTL-ALM-PKG-2: Sensitive artifacts shall be encrypted for confidentiality protection.

SEC-CTL-ALM-PKG-2A: Algorithms, key sizes, and standards to be used for encryption/decryption shall follow the "O-RAN Security Protocol Specification" [3], clause 5.

SEC-CTL-ALM-PKG-3: Application packages shall be compliant with ETSI NFV specifications, ETSI GS NFV-SOL 004 [42], ETSI GS NFV-IFA 011 [43] and ETSI GS NFV-SEC 021 [39] for package formats and signing/verification procedures.

SEC-CTL-ALM-PKG-4: Encryption shall be used to secure cryptographic keys used by the cryptographic operations.

EXAMPLE: Cryptographic operations include signature generation/verification, encryption/decryption, and hashing.

5.3.2.2 Secure Update

5.3.2.2.1 Requirements

REQ-SEC-ALM-SU-1: Application updates shall follow the same security requirements as Application packages.

REQ-SEC-ALM-SU-2: Applications should be updated with their latest security updates.

REQ-SEC-ALM-SU-3: Applications should be protected from downgrade attacks to older, possibly vulnerable, software versions.

REQ-SEC-ALM-SU-4: Security updates for Application vulnerabilities should be available in a timely manner after discovery of known vulnerability or vulnerabilities for an Application.

5.3.2.3 Security Descriptor

5.3.2.3.1 Requirements

REQ-SEC-LCM-SD-1: The Application descriptor shall support a description of the security group rules. Those rules shall be associated to the relevant Application interfaces.

EXAMPLE: Security group rules include permissions, access control and filtering rules

REQ-SEC-LCM-SD-2: The Application descriptor shall support a description of the Service Availability Level (SAL) requirements for virtual resources on the underlying O-Cloud platform.

REQ-SEC-LCM-SD-3: The O-Cloud platform shall use the security group rules in the application descriptor for controlling the traffic direction, who can access the Application, what actions they can perform, and what level of access they have.

REQ-SEC-LCM-SD-4: The SMO shall use the Service Availability Level (SAL) in the Application descriptor for governing the status (availability, deployment, and operation) of Applications and reacting whenever a SAL requirement is being breached.

REQ-SEC-LCM-SD-5: The Application shall support the ability to compare the current owned resource consumption with the defined resource quotas from the Application descriptor.

REQ-SEC-LCM-SD-6: The Application shall send an alarm to the SMO if the current owned resource consumption and the defined resource quotas are inconsistent.

REQ-SEC-LCM-SD-7: The comparing process between the current owned resource consumption and the defined resource quotas should be triggered periodically by the Application.

5.3.2.4 Secure Deletion of Sensitive Data

5.3.2.4.1 Introduction

Support for secure deletion of data owned by the Application is included in clause 5.1.8.6 for O-Cloud secure storage requirements and controls. NIST SP 800-88 [75] can provide additional guidance for data sanitization.

5.3.2.4.2 Requirements

REQ-SEC-DEL-1: VOID.

5.3.2.4.3 Security Controls

SEC-CTL-DEL-1: VOID.

SEC-CTL-DEL-2: VOID.

5.3.2.5 Decommissioning of Applications

5.3.2.5.0 Introduction

NOTE: When an application is decommissioned, it is important to document the entire process. Another crucial task is to archive the legacy data and software for historical purposes.

5.3.2.5.1 Requirements

REQ-SEC-ALM-DECOM-1: A complete post-decommission report documenting the performed tasks shall be generated.

REQ-SEC-ALM-DECOM-2: Legacy data and software should be archived.

REQ-SEC-ALM-DECOM-3: All trust artifacts associated with an application shall be revoked at the time of decommissioning.

EXAMPLE: Trust artifacts include digital certificates, OAuth tokens, and application identifiers, etc.

5.3.3 Network Protocols and Services

5.3.3.0 Introduction

Each O-RAN component serves important network function(s) based on a list of its necessary network protocols and services supported through its network interface(s). Proper, transparent, and secure network protocols and services enabled on each O-RAN component is essential for its overall security posture with the reduced risk.

5.3.3.1 Requirements

REQ-SEC-NET-1: A list of network protocols and services supported on the O-RAN component shall be clearly documented by its vendor. Unused protocols shall be disabled.

5.3.4 Robustness of Common Transport Protocols

5.3.4.0 Introduction

IP, UDP, TCP, SCTP, SSH, HTTP and HTTP2 are the common transport protocols widely used by any O-RAN components for network communications and services. Robust implementation of those common transport protocols can significantly improve the security of each O-RAN component and system overall.

5.3.4.1 Requirements

REQ-SEC-TRAN-1: Common transport protocols (IP, UDP, TCP, SCTP, SSH, HTTP and HTTP2) used in O-RAN system should be able to handle unexpected inputs (not in-line with protocol specification) without functional compromise. The unexpected inputs include random mutations of the protocol headers and payloads, as well as targeted fuzzing with state awareness.

5.3.5 Robustness against Volumetric DDoS Attack

5.3.5.0 Introduction

Distributed Denial of Service (DDoS) attack is one of the most common security risks for any O-RAN component. DDoS attack often results in service interruption and even worse system crash and prolonged network outage. A volumetric DDoS attack can come from a bad actor or adversary, or a misconfiguration by the operator.

5.3.5.1 Requirements

REQ-SEC-DOS-1: An O-RAN element with external network interface shall be able to withstand network transport protocol based volumetric DDoS attack without system crash and returning to its normal service level after the attack subsides.

5.3.5.2 Security Controls

SEC-CTL-DOS-1: An O-RAN element should be designed to incorporate redundant elements to achieve High Availability (HA).

NOTE: The redundant High Availability (HA) elements play a crucial role in scalability of the O-RAN element to address the requirements of legitimate users when facing a volumetric Distributed Denial of Service (DDoS) attack. Vendors should provide robust support for these HA features. Operators, in turn, should evaluate deployment scenarios in order to make an informed decision about deploying these HA features, aiming to enhance network performance and resilience.

5.3.6 Robustness of OS and Applications

5.3.6.0 Introduction

The robustness of the O-RAN component in the OS and application(s) installed is fundamental to the overall security posture of the O-RAN system.

5.3.6.1 Requirements

REQ-SEC-SYS-1: Known vulnerabilities in the OS and applications of an O-RAN component shall be clearly identified.

5.3.7 Password-Based Authentication

5.3.7.0 Introduction

Weak, stolen, and mis-used passwords are some of the common and leading causes of data breaches and methods of gaining access to systems, services, and applications. Password policy and management are applicable to both remote and Web UI login interfaces for user and automated machine password-based authentication on O-RAN components.

5.3.7.1 Requirements

REQ-SEC-PASS-1: If password is used as an authentication attribute, O-RAN component vendors should follow security best practices to mitigate risks resulting from different password-based authentication attacks such as brute-forcing, unauthorized password resets, man-in-the-middle, and dictionary attacks.

5.3.7.2 Security Controls

SEC-CTL-PASS-1: Default passwords should be changed upon installation. Configured passwords should follow the organization's policies for strong passwords.

SEC-CTL-PASS-2: O-RAN components shall support account lock-out for repeated failed login attempts. The number of failed login attempts shall be configurable. The number of attempts may be guided by the organization's policy.

SEC-CTL-PASS-3: Passwords shall be encrypted when stored and transmitted.

5.3.8 Security Log Management

5.3.8.1 Introduction

Security log management is "the process for generating, transmitting, storing, analyzing, and disposing of computer security log data. Log management is essential to ensuring that computer security records are stored in sufficient detail for an appropriate period of time. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Logs are also useful when performing auditing and forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends and long-term problems." Defined in NIST SP 800-92 [58], executive summary.

5.3.8.2 Generic Requirements

REQ-SEC-SLM-1: An O-RAN component shall support the generation and transmission of security log data.

5.3.8.3 Micro Perimeter for Cluster Node

5.3.8.3.1 Requirements on Security Log Data Storage

REQ-SEC-SLM-TESS-1: The Security Log data which have been created within a micro perimeter shall be persistently stored in a non-volatile memory. This refers to Security Log data at rest. This applies to back-up Security Log data as well.

REQ-SEC-SLM-TESS-2: Any anomalies detected in log settings, configurations, and processes shall be logged.

REQ-SEC-SLM-TESS-3: The O-RAN Network Function(s), the O-Cloud platform and infrastructure, and the SMO Framework shall create Security Log data.

REQ-SEC-SLM-TESS-4: Security Log data shall be created and maintained per App, per xApp, or per rApp.

REQ-SEC-SLM-TESS-5: The created and stored Security Log data shall provide all necessary information to deduce the root cause of a system behaviour.

REQ-SEC-SLM-TESS-6: The Security Log data access management shall be protected with the help of the micro perimeter.

REQ-SEC-SLM-TESS-7: The access to Security Log data shall be authenticated and authorized.

REQ-SEC-SLM-TESS-8: Any change of access rights to Security Log data shall be logged.

REQ-SEC-SLM-TESS-9: Changing the access rights of security log data is only possible with privileged access rights.

REQ- SEC-SLM-TESS-10: The Security Log data process shall support Log data rotation. Log data rotation in this context refers to a closing of a Log-storage and opening a new Log-storage when the first Log-storage is complete.

REQ- SEC-SLM-TESS-11: The Security Log data rotation process shall be configurable at regular time and when the maximum log size is reached.

REQ- SEC-SLM-TESS-12: The Security Log data process shall log any log rotation reconfiguration.

REQ- SEC-SLM-TESS-13: The system shall be capable of creating, processing, transmitting, and always storing all required security log events.

5.3.8.3.2 Requirements on Security Log-data in Motion

REQ-SEC-SLM-TESM-1: The Security Log data in motion shall be protected with the help of the micro perimeter.

REQ-SEC-SLM-TESM-2: The Security Log data in motion shall be confidentiality, integrity and replay protected if this is going to leave the micro perimeter.

REQ-SEC-SLM-TESM-3: A mutual authentication shall be performed for any setup of a secure communication channel between at least two micro perimeters.

REQ-SEC-SLM-TESM-4: If a Security Log data integrity verification has failed, the Security Log data and a related failure notification shall be logged.

REQ-SEC-SLM-TESM-5: If a Security Log data appears outside of its expected receiving window, the Security Log data and the related notification shall be logged.

5.3.8.3.3 Requirements for Setup of a Micro Perimeter

REQ-SEC-SLM-TE-1: The Micro Perimeter shall support the secure storage of sensitive data.

REQ-SEC-SLM-TE-2: The Micro Perimeter shall support the execution of Security Log data sensitive functions, which are hosting the Log-Agent(s) and the Log-Collector.

REQ-SEC-SLM-TE-3: The Micro Perimeter shall support the execution of instantiated Application VNF's and Platform/Operating System level software.

REQ-SEC-SLM-TE-4: The Micro Perimeter's integrity shall be assured.

REQ-SEC-SLM-TE-5: Only authorized access shall be granted to the Micro Perimeter, i.e. access to Security Log data stored and used within it, and to instantiated functions within it.

REQ-SEC-SLM-TE-6: The Micro Perimeter shall support the deployment of software and the booting-up and execution of a single software instance or multiple software instances.

5.3.8.4 Micro Perimeter for Log data Repository

5.3.8.4.1 Requirements on Storage in Log data Repository

REQ-SEC-TESR-1: The Security Log data stored in the repository shall be protected with the help of the micro perimeter.

REQ-SEC-TESR-2: The Security Log data which have been created inside the trusted environment of the repository shall be persistently stored in a non-volatile memory. This refers to Log data at rest. This applies to back-up Log data.

REQ-SEC-TESR-4: Security Log data from different cluster node(s) shall be stored isolated from each other.

REQ-SEC-TESR-5: The Security Log data repository shall grant write only operation to cluster node(s).

REQ-SEC-TESR-6: Security Log data which are stored in the repository shall be confidentiality and integrity protected.

REQ-SEC-TESR-7: The Security Log data repository shall support attribute-based (ABAC) access management according to NIST SP 800-162 [67].

REQ-SEC-TESR-8: The Security Log data access management shall support operations for read, write, edit, delete, copy, execute and modify.

REQ-SEC-TESR-9: The access management ABAC mechanisms shall include the Subject Attributes, the Resource Objects Attributes, the Access Control Rules (policy), and the environmental conditions.

REQ-SEC-TESR-10: The Log data repository shall create and store Security Log data in a non-volatile memory.

REQ-SEC-TESR-11: Security Log data in use shall be protected with the help of the micro perimeter.

5.3.8.5 Secure storage of security log data

5.3.8.5.1 Introduction

Security log data storage involves the safekeeping and retention of security log data for a certain period of time. Security log data storage should ensure that all data of security events is retained reliably for a certain time so that no data is lost or altered, and access to the data is restricted to authorized personnel only.

5.3.8.5.2 Requirements

REQ-SEC-SLM-SST-1: Security log data shall be stored in a centralized location for easy management and analysis.

REQ-SEC-SLM-SST-2: Security log data shall be stored in a tamper-proof manner to ensure their integrity and authenticity.

REQ-SEC-SLM-SST-3: Retention policies for security log data shall be established to determine how long logs shall be kept.

REQ-SEC-SLM-SST-4: Access to the log storage shall be restricted to authorized personnel only.

REQ-SEC-SLM-SST-5: Access to the log storage shall be logged.

REQ-SEC-SLM-SST-6: Backup of the log storage shall be performed regularly.

REQ-SEC-SLM-SST-7: O-RAN elements shall be authorized to only send security log data to centralized log storage.

5.3.8.5.3 Security Controls

SEC-CTL-SLM-SST-1: Centralized storage for security log data should be realized using centralized logging servers or cloud-based services.

SEC-CTL-SLM-SST-2: Tamper-proof storage of security log data may be achieved through digital signature, encryption, and hashing techniques.

SEC-CTL-SLM-SST-3: The retention period should be based on legal, regulatory, and compliance requirements, as well as the organization's own policies.

5.3.8.6 Secure Transfer of security log data

5.3.8.6.1 Introduction

Security log transfer involves the movement of security log data from one location to another, such as from a local device to a centralized logging server.

5.3.8.6.2 Requirements

REQ-SEC-SLM-STR-1: Security log data shall be confidentiality- and integrity- protected during transfer to protect them from unauthorized access or tampering.

REQ-SEC-SLM-STR-2: The parties involved in the security log transfer shall mutually authenticate each other to ensure that the logs are coming from a trusted source and going to a trusted destination. Failures detected during the authentication shall be logged.

REQ-SEC-SLM-STR-3: Mechanisms shall be in place to ensure the integrity of the security log data during transfer.

REQ-SEC-SLM-STR-4: The log transfer process shall be auditable to enable the tracking and identification of any unauthorized or suspicious log transfers.

REQ-SEC-SLM-STR-5: An O-RAN component may support log streaming for security log events.

5.3.8.6.3 Security Controls

SEC-CTL-SLM-STR-1: Digital signatures or Hash-based Message Authentication Codes (HMACs) may be used to provide integrity protection of security log data.

SEC-CTL-SLM-STR-2: An O-RAN component may support the transport of Syslog as defined in IETF RFC 5424 [64] over TLS as defined in IETF RFC 5425 [65] for log streaming of security log events.

5.3.8.7 Log Format

5.3.8.7.1 Introduction

Each O-RAN component produces logs in various formats. The logs are collected at a central and trusted location where the logs are unified.

5.3.8.7.2 Requirements

REQ-SEC-SLM-FMT-1: Security logs shall be formatted in a consistent, standard, and machine-readable format that maintains backward compatibility with previous log format versions.

5.3.8.8 Log Fields

5.3.8.8.1 Introduction

To enable effective security analytics, it is important to include additional details in the security logs of the security event. These details help to identify adversarial operations within the O-RAN environment. A typical security log entry consists of two main parts: the log fields and the log message. The log fields provide metadata about the security log entry, while the log message contains the actual content and details of the security event being logged. The requirements specified in this clause pertain to the log fields.

5.3.8.8.2 Requirements

REQ-SEC-SLM-FLD-1: Security logs shall include the date and time of the security event for each log entry, using a consistent and standardized format that logs time to at least the second.

REQ-SEC-SLM-FLD-2: Security logs shall record the location of the security event for each log entry. For network transactions, the location shall incorporate both the source and destination IP addresses. In cases where security events transpire within a single component, the location field shall only contain the source IP address.

REQ-SEC-SLM-FLD-3: Security logs shall include the entity that is the cause of the security event for each log entry.

5.3.8.8.3 Security Controls

SEC-CTL-SLM-FLD-1: Security logs should use the ISO 8601 [62] date and time format.

SEC-CTL-SLM-FLD-2: Security logs shall use IP addresses for the location field.

5.3.8.9 Authenticated Time Stamping and Missing Time Source

5.3.8.9.1 Requirements

REQ-SEC-SLM-ATS-1: All network functions shall be synchronised to a common and authenticated time source.

REQ-SEC-SLM-ATS-2: Any successful as well as the unsuccessful synchronization to the common time source shall be logged.

REQ-SEC-SLM-ATS-3: The Security Log-data shall be time-stamped with the system time in case of unsuccessful synchronisation to a common time source.

REQ-SEC-SLM-ATS-4: The Security Log-data recording shall take place in the order in which the (security) log events occur.

REQ-SEC-SLM-ATS-5: The Security Log data shall contain a timestamp that includes a timezone.

5.3.8.9.2 Security Controls

5.3.8.9.2.1 Authenticated Time Stamping

SEC-CTL-SLM-ATS-1: The Network Time Protocol (NTP) version 4 should be supported as specified by IETF RFC 5905 [60] for the support of authenticated time stamping.

SEC-CTL-SLM-ATS-2: If NTPv4 authentication is in use, then AES-CMAC as specified by IETF RFC 4493 [78] shall be supported. In this use case the NTP client can verify the integrity of the received NTP-packet.

SEC-CTL-SLM-ATS-3: If NTP security (as specified by IETF RFC 5905 [60]) is in use for the integrity and replay protection of NTP-packets, then NTS (IETF RFC 8915 [63]) shall be supported. In this use case the NTP client can verify the authenticity of the NTP packets by use of X.509 PKI infrastructure.

5.3.8.9.2.2 Common Time Source

SEC-CTL-SLM-CTS-1: The Time Stamp representation should be in a standardized format, and the format in use should be logged. For reference to the formatting, refer to IETF RFC 3339 [61] and ISO 8601 [62].

5.3.8.10 Security Log Management Due Diligence and Auditing

5.3.8.10.1 Requirements

REQ-SEC-SLM-DDA-1: The organization should define a policy and procedure for security logging. The security log management policy shall define periodic audits to confirm that logging standards and guidelines are being followed throughout the organization.

REQ-SEC-SLM-DDA-2: The organization should ensure that the policies and procedures in the log management process are being performed properly.

REQ-SEC-SLM-DDA-3: The security log management should be prioritized appropriate throughout the organisation.

REQ-SEC-SLM-DDA-4: The organization should prioritize its goals based on balancing the organization's reduction of risk with the time and resources needed to perform security log management functions.

REQ-SEC-SLM-DDA-5: The organization should create and maintain a secure log management infrastructure.

REQ-SEC-SLM-DDA-6: The organization should create an infrastructure that is robust enough to handle not only expected volumes of log data, but also peak-data volumes during extreme situations.

REQ-SEC-SLM-DDA-7: The organization should provide adequate support for all staff with log management responsibilities.

REQ-SEC-SLM-DDA-8: As part of the log management planning process, the organization should define the roles and responsibilities of individuals and teams who are expected to be involved in log management.

REQ-SEC-SLM-DDA-9: The security log management policy should define how to provide confidentiality, integrity, and availability of the results of log analysis which are to be protected while at rest, in use and in motion.

REQ-SEC-SLM-DDA-10: The security log management policy should provide a definition of how to handle inadvertent disclosures of sensitive information that is recorded in logs.

REQ-SEC-SLM-DDA-11: The security log management policy should provide a definition of which type of log-data to be analyzed and how often.

5.3.8.10.2 Security Controls

SEC-CTL-SLM-DDA-1: Testing and validation should be used to ensure that the policies and procedures in the log management process are being performed properly.

SEC-CTL-SLM-DDA-2: While defining the log management scheme, organizations should ensure that they provide the necessary training to relevant staff regarding their log management responsibilities as well as skill instruction for the needed resources to support log management. The support also includes the provision of log management tools and tool documentation, the provision of technical guidance on log management activities, and the disseminating information to log management staff.

SEC-CTL-SLM-DDA-3: The organisations should assign team and individual roles which are often involved in log management as follows:

- ***System and network administrators***, who are usually responsible for configuring logging on individual systems and network devices, analyzing those logs periodically, reporting on the results of log management activities, and performing regular maintenance of the logs and logging software.
- ***Security administrators***, who are usually responsible for managing and monitoring the log management infrastructures, configuring logging on security devices (e.g. firewalls, network-based intrusion detection systems, antivirus servers), reporting on the results of log management activities, and assisting others with configuring logging and performing log analysis.
- ***Computer security incident response teams***, who use log data when handling some incidents.
- ***Application developers***, who may need to design or customize applications so that they perform logging in accordance with the logging requirements and recommendations.
- ***Information security officers***, who may oversee the log management infrastructures.
- ***Chief information officers (CIO)***, who oversee the IT resources that generate, transmit, and store the logs.
- ***Auditors***, who may use log data when performing audits. Individuals involved in the procurement of software that should or can generate computer security log data.

5.3.8.11 Security Events to be Logged

5.3.8.11.1 Introduction

During O-RAN operations, components generate many events. Some of these events have security utility and are thus termed security events. Logging these security events is critical to maintaining a secure O-RAN environment. For convenience, security event log requirements are organized by high-level categories. These categories are mapped against the following O-RAN architectural elements: SMO, O-RAN Network Functions (NF), and O-Cloud (see Table 5.3.8.11.1-1).

- The SMO has security events related to management and orchestration.
- O-RAN Network Functions have application security events.
- O-Cloud has both network security events and system security events related to operating systems, hypervisors, and container runtimes.
- The following security event types occur in all O-RAN components (SMO, O-RAN NF, and O-Cloud): account and identity event, data access events, and general security events.

Table 5.3.8.11.1-1: Types of Security Events by O-RAN Component

	O-RAN Architectural Component		
Types of Security Events	**SMO**	**O-RAN NF**	**O-Cloud**
Management and Orchestration Events	X		
Application Events		X	
Network Events			X
System Events			X
Data Access Events	X	X	X
Account and Identity Events	X	X	X
General Security Events	X	X	X

5.3.8.11.2 Network Security Event Log Requirements

REQ-SEC-SLM-NET-EVT-1: O-Cloud shall log all physical and virtual network events related to creating and modifying network configurations, enabling, and disabling ports, network connections, and packets over limit from the firewalls from all host operating systems, hypervisors, and container engines.

5.3.8.11.3 System Security Event Log Requirements

5.3.8.11.3.1 General O-Cloud Security Events

5.3.8.11.3.1.1 Requirements

REQ-SEC-SLM-GEN-EVT-1: O-Cloud shall log the following resource-related events: shortages, system crashes, reboots, shutdowns, resource creation, and deletion from all host operating systems, hypervisors, and container engines.

REQ-SEC-SLM-GEN-EVT-2: O-Cloud shall log when maintenance activity is undertaken for host operating systems, hypervisors, and container engines.

REQ-SEC-SLM-GEN-EVT-3: O-Cloud shall log the creation of scheduled jobs and the particular time the job will run for all host operating systems, hypervisors, and container engines.

REQ-SEC-SLM-GEN-EVT-4: O-Cloud shall log a security event when driver tampering is detected. This includes but is not limited to modifications made to the main driver executable and any associated files, libraries, dependencies, or configuration files.

REQ-SEC-SLM-GEN-EVT-5: O-Cloud shall log a security event when it detects unauthorized changes to the O-Cloud hardware resource configuration.

REQ-SEC-SLM-GEN-EVT-6: O-Cloud shall log a security event when it detects unauthorized changes to the Application configuration.

5.3.8.11.3.1.2 Security Controls

SEC-CTL-SLM-GEN-EVT-1: O-Cloud shall log a security event if driver signature verification fails.

SEC-CTL-SLM-GEN-EVT-2: O-Cloud shall implement a robust File Integrity Monitoring (FIM) system that continuously monitors the integrity of all driver-related files, including executables, libraries, configuration files, and dependencies. The FIM system shall be configured to calculate cryptographic hashes of these files as baseline values and regularly compare the current cryptographic hashes with their baseline hashes stored in the FIM system.

SEC-CTL-SLM-GEN-EVT-3: O-Cloud shall log a security event if any hashes of driver files do not match their baseline values.

SEC-CTL-SLM-GEN-EVT-4: Baseline configurations for the hardware resource shall be established by the SMO, and regularly compared to the current state.

SEC-CTL-SLM-GEN-EVT-5: O-Cloud shall log a security event when it detects unauthorized deviation from the O-Cloud hardware resource configuration baseline.

SEC-CTL-SLM-GEN-EVT-6: Baseline configurations for each Application shall be established by the SMO, and regularly compared to the current state.

SEC-CTL-SLM-GEN-EVT-7: O-Cloud shall log a security event when it detects unauthorized deviation from the Application configuration baseline.

NOTE: Log management systems, such as SIEM, fall beyond the purview of O-RAN and are considered external entities. In the context of O-Cloud, it is recommended to set up these log management systems to dispatch notifications to the administrator when any of the following security events take place:

- Driver signature verification fails.
- Driver file hash verification fails.
- Unauthorized deviations from the O-Cloud hardware resource configuration baseline are detected.

- Unauthorized deviations from the application configuration baseline are detected.

5.3.8.11.3.2 Hypervisor Specific System Security Events

REQ-SEC-SLM-HYP-EVT-1: O-Cloud shall log all changes to operating system configurations, hypervisor configurations, changes to virtualization settings, and changes to resource allocations.

REQ-SEC-SLM-HYP-EVT-2: O-Cloud shall log all hypervisor events related to attaching or detaching virtual disks.

REQ-SEC-SLM-HYP-EVT-3: O-Cloud shall log all hypervisor events related to creating, starting, stopping, restarting, and deleting virtual machines.

5.3.8.11.3.3 Container Engine Specific System Events

REQ-SEC-SLM-CON-EVT-1: O-Cloud shall log all image repository events related to additions, modifications, and removal of images.

REQ-SEC-SLM-CON-EVT-2: O-Cloud shall log all container engine events related to volume creation, deletion, and mounting.

REQ-SEC-SLM-CON-EVT-3: O-Cloud shall log all container engine events related to creating, starting, stopping, restarting, and deleting containers.

5.3.8.11.4 Application Security Event Log Requirements

REQ-SEC-SLM-APP-EVT-1: O-RAN Network Functions shall log any errors or exceptions generated.

REQ-SEC-SLM-APP-EVT-2: O-RAN Network Functions shall log the use of any dynamically loaded libraries, including the name and version information of the library being loaded.

5.3.8.11.5 Data Access Security Event Log Requirements

REQ-SEC-SLM-DAT-EVT-1: O-RAN components shall log successful file additions, deletions, and unsuccessful attempts due to errors and authorization issues.

REQ-SEC-SLM-DAT-EVT-2: O-RAN components should log successful file reads and writes.

REQ-SEC-SLM-DAT-EVT-3: O-RAN components shall log unsuccessful attempts of file reads and writes due to errors and authorization issues.

REQ-SEC-SLM-DAT-EVT-4: O-RAN components shall log successful directory additions, deletions, and unsuccessful attempts due to errors and authorization issues.

REQ-SEC-SLM-DAT-EVT-5: O-RAN components shall log successful database or data store additions, deletions, and unsuccessful attempts due to errors and authorization issues.

REQ-SEC-SLM-DAT-EVT-6: O-RAN components should log successful database or data store reads and writes.

REQ-SEC-SLM-DAT-EVT-7: O-RAN components shall log unsuccessful attempts of database and data store reads and writes.

REQ-SEC-SLM-DAT-EVT-8: O-RAN components shall log permission changes to files, directories, databases, or data stores.

5.3.8.11.6 Account and Identity Security Event Log Requirements

REQ-SEC-SLM-AAI-EVT-1: O-RAN components shall log account creation, modification, deletion, and unsuccessful attempts.

REQ-SEC-SLM-AAI-EVT-2: O-RAN components shall log changes to account privilege levels and unsuccessful attempts.

REQ-SEC-SLM-AAI-EVT-3: O-RAN components shall log successful group membership changes for accounts and unsuccessful change attempts.

REQ-SEC-SLM-AAI-EVT-4: O-RAN components shall log successful and unsuccessful authentication attempts for accounts.

REQ-SEC-SLM-AAI-EVT-5: O-RAN components shall log successful and unsuccessful authorization attempts to create a session or initiate a transaction.

REQ-SEC-SLM-AAI-EVT-6: O-RAN components shall log the termination of sessions or transactions.

REQ-SEC-SLM-AAI-EVT-7: O-RAN components shall log the occurrence of downgraded privileges or elevation of privileges for accounts.

REQ-SEC-SLM-AAI-EVT-8: VOID.

REQ-SEC-SLM-AAI-EVT-9: O-RAN components shall log transactions successfully executed by accounts and unsuccessful attempts.

REQ-SEC-SLM-AAI-EVT-10: O-RAN components shall log requests that do not require an authenticated account.

5.3.8.11.7 General Security Event Log Requirements

REQ-SEC-SLM-GSE-1: O-RAN components shall log the activation and deactivation of security software related to security logging, firewalls, malware protection, Data Loss Prevention (DLP), and Intrusion Detection Systems (IDS).

REQ-SEC-SLM-GSE-2: O-RAN components shall log the use of administrative privileges.

REQ-SEC-SLM-GSE-3: O-RAN components shall log any change to a security-related configuration item, including a description of the configuration change.

REQ-SEC-SLM-GSE-4: O-RAN components shall log the occurrence of viewing, renewing, exporting, importing, modifying, and deleting of certificates and keys. The logged data for these events shall not include any sensitive information related to the certificates or the keys.

REQ-SEC-SLM-GSE-5: O-RAN components shall log the occurrence of cryptographic operations on resources involved in signatures, encryption, decryption, hashing, key generation, and key destruction. The logged data for these events shall not include any sensitive information related to the cryptographic operations.

REQ-SEC-SLM-GSE-6: O-RAN components shall log security patches submitted but not applied.

5.3.8.12 Log data Lifecycle Management

REQ-SEC-LCSS-2: The Security Log data process shall support Log data rotation. Log data rotation in this context refers to a closing of a Log-storage and opening a new Log-storage when the first Log-storage is complete.

REQ-SEC-LCSS-3: The Security Log data rotation process shall be configurable at regular time intervals and when the maximum log size is reached.

REQ-SEC-LCSS-4: The Security Log data process shall log any log rotation reconfiguration.

REQ-SEC-LCSS-5: The system shall be capable of creating, processing, transmitting, and always storing all required security log events.

5.3.8.13 Requirements on Security Log data Policy

REQ-SEC-POL-5: The archived Security Log data and their storage media shall be checked periodically to determine whether the Security Log data is accessible.

REQ-SEC-POL-6: The archived Log data and their media shall be physically protected.

REQ-SEC-POL-7: The Personally Identifiable Information (PII) shall be removed from archived Security Log data. For details on PII, refer to [68].

REQ-SEC-POL-8: The archived Security Log data shall be integrity and confidentiality protected.

REQ-SEC-POL-9: For the Security Log data lifecycle a policy shall be supported for log retention and log preservation. If this provides filter options, then security Log data shall not be filtered out.

REQ-SEC-POL-10: The log policy shall include requirements for log generation, log transmission, storage and disposal, and log analysis.

5.3.8.14 Preventing (D)DoS to Security Log Data

5.3.8.14.1 General

The Requirements below are applicable to the vendors of the log management infrastructure.

5.3.8.14.2 Requirements

REQ-SEC-SLM-DoS-1: The log management infrastructure should be designed to support typical and peak volume of log data to be processed per hour and day [58].

REQ-SEC-SLM-DoS-2: The log management infrastructure should support the handling of peak situations for extreme situations. Extreme situations in this context refer to widespread malware incidents, vulnerability scanning, and penetration tests that may cause unusual large number of log entries [58].

REQ-SEC-SLM-DoS-3: The log management infrastructure should provide notifications at different log data volumes. This refers to the introduction of escalation levels at different log data volumes.

REQ-SEC-SLM-DoS-4: The log management infrastructure should provide notifications at different log data event rates. This refers to the introduction of escalation levels at different log data event rates.

REQ-SEC-SLM-DoS-5: The log management infrastructure should support mechanisms for log data redundancy.

REQ-SEC-SLM-DoS-6: The log management infrastructure should trigger the archiving of log data based on the level of escalation achieved. The escalation level may be triggered by increased log data volume or log data event rates.

REQ-SEC-SLM-DoS-7: The log management infrastructure should trigger the retention of log data based on the level of escalation achieved. The escalation level may be triggered by increased log data volume or log data event rates.

5.3.8.15 Preventing Tampering of Log Data

5.3.8.15.1 General

The Requirements below are applicable to the vendors of the log management infrastructure.

5.3.8.15.2 Requirements

REQ-SEC-SLM-TLD-1: The log management infrastructure should support access management for log data.

REQ-SEC-SLM-TLD-2: The log management infrastructure should support real time logging (log data streaming).

REQ-SEC-SLM-TLD-3: The log management infrastructure should support replication of log data.

REQ-SEC-SLM-TLD-4: The log management infrastructure should support the derivation of digests of log-data to existing and preceding digests with the aim to keep the cryptographic chain and to attest the completeness and the integrity of the security events.

5.3.9 Certificate Management Framework

5.3.9.1 Requirements

5.3.9.1.1 PNFs

REQ-SEC-CMF-PNF-1: An O-RAN PNF requiring a PKI certificate shall support certificate management protocol.

REQ-SEC-CMF-PNF-2: In order to facilitate vendor certificate-based initial enrolment of PNFs, vendors shall pre-install vendor-signed certificates in PNFs.

REQ-SEC-CMF-PNF-3: In order to facilitate vendor certificate-based initial enrolment of PNFs, operators shall pre-provision the FQDN/IP address of RA/CA to PNFs.

EXAMPLE 1: Pre-configurations before deployment.

EXAMPLE 2: Startup installation procedure as defined in [14], clause 6.1.

REQ-SEC-CMF-PNF-4: PNFs which use vendor-signed certificates for initial certificate enrolment should monitor the expiry of the vendor root CA certificate or any of the sub-CA certificates in the trust chain used to sign the certificate.

REQ-SEC-CMF-PNF-5: When the expiry of the vendor root CA certificate or any of the sub-CA certificates in the trust chain is approaching, PNFs should raise notifications (alarms) with increasing levels of severity as the expiry date gets closer.

5.3.9.1.2 VNFs/CNFs

REQ-SEC-CMF-VNF_CNF-1: The O-Cloud shall support a certificate management protocol for use by O-RAN VNFs/CNFs that require a PKI certificate.

REQ-SEC-CMF-VNF_CNF-2: An O-RAN VNF/CNF requiring a PKI certificate directly from a CA/RA, without O-Cloud involvement, shall support a certificate management protocol.

5.3.9.1.3 Any NF (PNF/VNF/CNF)

REQ-SEC-CMF-ANYNF-1: Any offline or out-of-band (automated or manual) PSK/Refnum generation, distribution and provisioning systems shall provide PSK/Refnum values only to an authorized PNF/CNF/VNF.

REQ-SEC-CMF-ANYNF-2: NFs shall raise alarms/notifications and/or security events to SMO or certificate management systems alerting about the certificates about to expire in the near future with increasing severity levels as the expiry date approaches.

REQ-SEC-CMF-ANYNF-3: SMO or certificate management systems should instruct NFs to trigger certificate renewal procedures according to operator's policies.

EXAMPLE 1: Policy 1 instruct NFs to trigger certificate renewals in a staggered manner.

EXAMPLE 2: Policy 2 instruct NFs to trigger certificate renewals according to resource availability.

REQ-SEC-CMF-ANYNF-4: NFs shall provide interfaces to allow configuration of the advance alarms/notifications/security events interval prior to certificate expiry for different severity levels.

EXAMPLE 3: Configuration Minor alarm N1 days before expiry, Major alarm, and security event N2 days before expiry, Critical alarm, and security events N3 days before expiry of certificates, Critical alarm, and security event every day after expiry.

REQ-SEC-CMF-ANYNF-5: NFs shall trigger certificate renewal procedure before the certificate expiry using policies provided by the operator.

EXAMPLE 4: Policy 1Trigger renewal N1/N2/N3 days before expiry.

EXAMPLE 5: Policy 2Trigger renewal when instructed by SMO or certificate management.

REQ-SEC-CMF-ANYNF-6: NFs shall provide interfaces to enable certificate management systems to trigger certificate renewal before the expiry.

REQ-SEC-CMF-ANYNF-7: NFs shall send a notification to the SMO indicating the success or failure state after the certificate renewal completion.

REQ-SEC-CMF-ANYNF-8: NFs should raise a critical alarm as well as log security events if the certificate for NF(s) has expired.

REQ-SEC-CMF-ANYNF-9: NFs should raise a critical alarm as well as log security events if the certificate renewal has failed.

REQ-SEC-CMF-ANYNF-10: In the event if the newly installed/renewed certificate fails, NFs shall continue to use its previous certificate until that certificate expires.

5.3.9.2 Security Controls

5.3.9.2.1 PNFs

SEC-CTL-CMF-PNF-1: An O-RAN PNF requiring a PKI certificate shall support CMPv2 as specified in O-RAN Security Protocols Specification [3], clause 4.6.

5.3.9.2.2 VNFs/CNFs

SEC-CTL-CMF-VNF_CNF-1: The O-Cloud shall support CMPv2 as specified in O-RAN Security Protocols Specification [3], clause 4.6.

SEC-CTL-CMF-VNF_CNF-2: An O-RAN VNF/CNF requiring a PKI certificate directly from a CA/RA, without O-Cloud involvement, shall support CMPv2 as specified in O-RAN Security Protocols Specification [3], clause 4.6.

5.3.9.2.3 Any NF (PNF/VNF/CNF)

SEC-CTL-CMF-ANYNF-1: NFs may establish TLS connection using renewed certificates before terminating existing TLS connections.

SEC-CTL-CMF-ANYNF-2: NFs may terminate any established TLS connection after the renewed certificates are validated and re-establish TLS connection with new certificate.

SEC-CTL-CMF-ANYNF-3: NFs may wait for already established TLS connections to close before applying the renewed certificate for new TLS connections.

5.3.10 Application Programming Interfaces (APIs)

5.3.10.1 Introduction

The security requirements in this clause provide protections against the vulnerabilities and security risks identified in the OWASP API Security Project Top 10 2023 vulnerabilities and security risks of Application Programming Interfaces (APIs) [i.9]. APIs as referred to in this clause are transactional APIs based on REST or gRPC. The terms client, resource owner, and resource server are defined in IETF RFC 6749 [34].

5.3.10.2 Security Requirements

REQ-SEC-API-1: APIs used in O-RAN to access an internal or external data source should perform object-level authorization checks.

REQ-SEC-API-2: O-RAN endpoints using APIs shall support certificate-based authentication.

REQ-SEC-API-3: O-RAN endpoints using APIs may support password-based authentication that is a factor used in multi-factor authentication (MFA). Password-based single-factor authentication should not be used.

REQ-SEC-API-4: O-RAN endpoints using APIs should provide strong authorization.

REQ-SEC-API-5: O-RAN endpoints using APIs shall validate the authenticity of tokens. Unsigned JWT tokens shall not be accepted.

REQ-SEC-API-6: O-RAN endpoints shall validate API client requests to return sensitive data.

REQ-SEC-API-7: APIs used in O-RAN shall have confidentiality and integrity protection for data-in-transit.

REQ-SEC-API-8: APIs used in O-RAN shall implement a schema-based validation mechanism to enforce returned data.

REQ-SEC-API-9: APIs used in O-RAN shall impose a restriction on the size and number of resources that a client requests.

REQ-SEC-API-10: APIs used in O-RAN shall support authorization that denies all access by default and requires explicit grants to specific roles for access to every function.

REQ-SEC-API-11: APIs used in O-RAN shall default-deny properties that should not be accessed by clients.

REQ-SEC-API-12: APIs used in O-RAN shall only be accessed by valid HTTP verbs. All other HTTP verbs should be disabled.

REQ-SEC-API-13: APIs used in O-RAN shall validate, filter, and sanitize client-provided data and other data coming from integrated systems. Data validation shall be performed using a single, trustworthy, and actively maintained library. Special characters shall be escaped using the specific syntax for the target interpreter.

REQ-SEC-API-14: APIs used in O-RAN shall limit the number of returned records to prevent mass disclosure in case of injection.

REQ-SEC-API-15: APIs used in O-RAN shall log all failed authentication attempts, denied access, and input validation errors.

5.3.10.3 Security Controls

SEC-CTL-API-01: API client and server shall support mTLS 1.2, or higher, as specified in O-RAN Security Protocols Specifications [3], clause 4.2 for mutual authentication.

SEC-CTL-API-02: API server shall support OAuth 2.0 resource server functionality, as specified in O-RAN Security Protocols Specifications [3], clause 4.7, for service requests received from API clients.

SEC-CTL-API-03: API server shall support OAuth 2.0 resource owner functionality, as specified in O-RAN Security Protocols Specifications [3], clause 4.7, for service requests received from API clients.

SEC-CTL-API-04: API client shall support OAuth 2.0 client functionality, as specified in O-RAN Security Protocols Specifications [3], clause 4.7 for each service request.

SEC-CTL-API-05: API client and server shall support TLS 1.2, or higher, as specified in O-RAN Security Protocols Specifications [3], clause 4.2, for protection of data-in-transit.

5.3.11 Trust Anchor Provisioning

5.3.11.0 Introduction

Before an O-RAN component can establish a mutual TLS connection with a signalling peer, the O-RAN component needs to be able to trace the peer's certificate path to a valid trust anchor.

5.3.11.1 Requirements

REQ-SEC-TAP-1: An O-RAN PNF using PKIX certificates shall be shipped with one or more pre-provisioned Trust Anchors, which may be a vendor-signed certificate or operator-signed certificate.

REQ-SEC-TAP-2: An O-RAN PNF shall support the secure storage of the trust anchors in a secure element or a secure enclave such that they cannot be tampered with or modified.

REQ-SEC-TAP-3: An O-RAN PNF using PKIX certificates shall enable an authorized function to recover the list of provisioned trust anchors and associated public keys.

REQ-SEC-TAP-4: An O-RAN PNF shall be able to be securely provisioned with new trust anchors and have an existing trust anchor replaced, for events such as expiration.

REQ-SEC-TAP-5: An O-RAN PNF shall log an event for each trust anchor provisioning operation.

5.3.11.2 Security Controls

SEC-CTL-TAP-1: An O-RAN PNF shall support CMPv2, as specified in O-RAN Security Protocols Specification [3], clause 4.6, for trust anchor provisioning.

SEC-CTL-TAP-2: An O-RAN PNF may support voucher-based protocols [69] to enable an O-RAN function to be securely provisioned with a new trust anchor.

SEC-CTL-TAP-3: An O-RAN PNF may support BRSKI [70] for trust anchor provisioning.

SEC-CTL-TAP-4: An O-RAN PNF may support SZTP [71] for trust anchor provisioning.

SEC-CTL-TAP-5: An O-RAN PNF may support 3GPP SCS [72], [73], [74] for download of initial security configuration.

6 SBOM Guidelines for O-RAN

6.1 SBOM Overview

This clause provides guidance for generation, delivery, and use of a Software Bill Of Materials (SBOM).

SBOM is a fundamental component of a mature Software Development Lifecycle (SDLC) process. SBOM is an industry best practice part of secure software development that enhances the understanding of the upstream software supply chain so that vulnerability notifications and updates can be properly and safely handled across the installed customer base. The U.S. Department of Commerce (DoC) and the National Telecommunications and Information Administration (NTIA) define SBOM as "a formal record containing the details and supply chain relationships of various components used in building software." The DoC, in coordination with NTIA, published a report "The Minimum Elements for a Software Bill of Materials (SBOM)" [17] that provides guidance on the data fields, automation, and processes to be used by suppliers and customers. The SBOM documents proprietary and third-party software, including commercial and Free and Open-Source Software (FOSS), used in software products. The SBOM is maintained and used by the software supplier and stored and viewed by the network operator.

6.2 Void

[Intentionally blank]

6.3 SBOM Requirements for O-RAN

6.3.0 Introduction

The SBOM delivery should be made under contractual agreement with specific terms that include the following requirements and controls.

6.3.1 Requirements

REQ-SBOM-001: The O-RAN vendor shall provide the SBOM with every O-RAN software delivery package, including patches.

REQ-SBOM-002: The minimum set of data fields shall include Supplier Name, Component Name, Version of the Component, Other Unique Identifiers as available, Dependency Relationship, Author of the SBOM data, and Timestamp [17].

REQ-SBOM-003: Vulnerabilities shall not be included as an additional data field because it would represent a static view from a specific point in time, while vulnerabilities are constantly evolving.

NOTE 1: The SBOM should be used by vendors and operators to periodically check against known vulnerability databases to identify potential risk.

NOTE 2: The level of risk for a vulnerability should be determined by the software vendor and operator with consideration of the software product, use case, and network environment.

NOTE 3: The SBOM provides visibility into the use of open-source and third-party provided software having known vulnerabilities or contributions from individuals or companies in adversarial nations, but it does not protect against zero-day vulnerabilities that were unintentionally or maliciously inserted, exploited, or discovered and not reported.

REQ-SBOM-004: SBOM depth shall be provided at top-level.

REQ-SBOM-005: SBOM depth shall be provided to a second-level for O-RAN Software Community (OSC) sourced software to indicate which OSC modules are used and which individual and/or company contributed the software for that module.

REQ-SBOM-006: SBOM depth shall be provided to second-level for any used open source software.

REQ-SBOM-007: SBOM shall be authenticity and integrity protected when in transit and at rest.

REQ-SBOM-008: Commercial software vendors using software from the O-RAN Software Community (OSC) shall provide an SBOM that includes the components used from the OSC.

REQ-SBOM-009: SBOM for commercial software shall be access controlled.

REQ-SBOM-010: The consumer of an SBOM shall maintain confidentiality protection on the SBOM delivered from the SBOM producer.

REQ-SBOM-011: The SBOM shall be provided in Software Package Data eXchange (SPDX) [17], CycloneDX [18], or Software Identification (SWID) [19] format.

NOTE 4: ISO/IEC 5962:2021 [21] specifies SPDX as a standard data format for communicating the component and metadata information associated with SBOM.

6.3.2 Security Controls

SEC-CTL-SBOM-001: For integrity, a hash shall be generated for the SBOM, as specified in O-RAN Security Protocols Specification [3], clause 5.

SEC-CTL-SBOM-002: For authenticity, a digital signature shall be provided for the SBOM, as specified in O-RAN Security Protocols Specification [3], clause 5.

Annex A (informative): Security Principles mapping to Security Requirements

Table A.1: Security Principles mapping to Security Requirements defined in [4]

	Components							Interfaces					
SP	**O-RU**	**O-DU**	**O-CU**	**O-CLOUD**	**Near RT RIC**	**Non RT RIC**	**SMO**	**FH M-Plane**	**FH S-Plane**	**FH CU-Plane**	**E2**	**O1**	**A1**
SP-AUTH				REQ-SEC-OCLOUD-1									
SP-ACC													
SP-CRYPTO													
SP-TCOMM											REQ-SEC-O2-1		REQ-SEC-A1-1
SP-SS													
SP-SB													
SP-UPDT													
SP-RECO													
SP-OPNS													
SP-ASSU													
SP-PRV													
SP-SLC													
SP-ISO				REQ-SEC-OCLOUD-2									
SP-PHY													
SP-CLD													
SP-ROB													
SP-AUTH				REQ-SEC-OCLOUD-1									
SP-ACC													
SP-CRYPTO													
SP-TCOMM											REQ-SEC-O2-1		REQ-SEC-A1-1
SP-SS													
SP-SB													
SP-UPDT													
SP-RECO													
SP-OPNS													
SP-ASSU													
SP-PRV													
SP-SLC													
SP-ISO				REQ-SEC-OCLOUD-2									
SP-PHY													
SP-CLD													
SP-ROB													

Annex B (informative): Security: List of 3GPP security requirements

Table B.1: References for 3GPP Security requirements

Reference	Title
ETSI TS 133 501	Security architecture and procedures for 5G system
ETSI TS 133 511	Security Assurance Specification (SCAS) for the next generation - Node B (gNodeB) network product class
TS 33.117	Catalogue of general security assurance requirements
TR 33.818	Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualized network products
TR 33.848	Study on security impacts of virtualisation

Table B.2: 3GPP Security requirements

Item	Title	3GPP Security requirements	3GPP specifications	NESAS/SCAS
gNodeB-specific security functional requirements				
#1	Mitigation of bidding down attacks in Xn handovers	An attacker could attempt a bidding down attack by making the UE and the network entities respectively believe that the other side does not support a security feature, even when both sides in fact support that security feature. It shall be ensured that a bidding down attack, in the above sense, can be prevented. In the Path-Switch message, the target gNB shall send the UE's 5G security capabilities, UP security policy with corresponding PDU session ID received from the source gNB to the AMF.	ETSI TS 133 501 clauses 5.1.1 & 6.7.3.1	ETSI TS 133 511 clause 4.2.2.1.14
#2	Authentication and Authorization	Access network authorization: Assurance shall be provided to the UE that it is connected to an access network that is authorized by the serving network to provide services to the UE. This authorization is 'implicit' in the sense that it is implied by a successful establishment of access network security. This access network authorization applies to all types of access networks.	ETSI TS 133 501 clause 5.1.2	
#3	Requirements on gNB related to keys	The gNB shall allow for use of encryption and integrity protection algorithms for AS (Access Stratum) and NAS (Non Access Stratum) protection having keys of length 128 bits. The network interfaces shall support the transport of 256-bit keys. The keys used for UP (User Plane), NAS and AS protection shall be dependent on the algorithm with which they are used.	ETSI TS 133 501 clause 5.1.3	
#4	Subscriber privacy	The SUPI should not be transferred in clear text over gNB except routing information, e.g. Mobile Country Code (MCC) and Mobile Network Code (MNC).	ETSI TS 133 501 clause 5.2.5	

Item	Title	3GPP Security requirements	3GPP specifications	NESAS/SCAS
gNodeB-specific security functional requirements				
#5	User data and signalling data confidentiality	The gNB shall support ciphering of user data between the UE and the gNB. The gNB shall activate ciphering of user data based on the security policy sent by the SMF. The gNB shall support ciphering of RRC-signalling. The gNB shall implement the following ciphering algorithms: - NEA0, 128-NEA1, 128-NEA2 as defined in Annex D of ETSI TS 133 501. The gNB may implement the following ciphering algorithm: - 128-NEA3 as defined in Annex D of ETSI TS 133 501. Confidentiality protection of user data between the UE and the gNB is optional to use. Confidentiality protection of the RRC-signalling is optional to use. Confidentiality protection should be used whenever regulations permit. The PDCP protocol, as specified in ETSI TS 138 323 between the UE and the NG-RAN, shall be responsible for user plane data confidentiality protection.	ETSI TS 133 501 clause 5.3.2	ETSI TS 133 511 clauses 4.2.2.1.6 & 4.2.2.1.7 & 4.2.2.1.10 & 4.2.2.1.11
#6	User data and signalling data integrity	The gNB shall support integrity protection and replay protection of user data between the UE and the gNB. The gNB shall activate integrity protection of user data based on the security policy sent by the SMF. The gNB shall support integrity protection and replay protection of RRC-signalling. The gNB shall support the following integrity protection algorithms: - NIA0, 128-NIA1, 128-NIA2 as defined in Annex D of ETSI TS 133 501. The gNB may support the following integrity protection algorithm: - 128-NIA3 as defined in Annex D of ETSI TS 133 501. Integrity protection of the user data between the UE and the gNB is optional to use, and shall not use NIA0. All RRC signalling messages except those explicitly listed in TS 38.331 as exceptions shall be integrity-protected with an integrity protection algorithm different from NIA0, except for unauthenticated emergency calls. NIA0 shall be disabled in gNB in the deployments where support of unauthenticated emergency session is not a regulatory requirement. The PDCP protocol, as specified in ETSI TS 138 323 between the UE and the NG-RAN, shall be responsible for user plane data integrity protection.	ETSI TS 133 501 clause 5.3.3	ETSI TS 133 511 clauses 4.2.2.1.1 & 4.2.2.1.2 & 4.2.2.1.8 & 4.2.2.1.9
#7	RRC integrity check failure	The RRC integrity checks shall be performed both in the ME and the gNB. In case failed integrity check (i.e. faulty or missing MAC-I) is detected after the start of integrity protection, the concerned message shall be discarded. This can happen on the gNB side or on the ME side.	ETSI TS 133 501 clause 6.5.1	
#8	UP integrity check failure	If the gNB or the UE receives a PDCP PDU which fails integrity check with faulty or missing MAC-I after the start of integrity protection, the PDU shall be discarded.	ETSI TS 133 501 clause 6.6.4	

Item	Title	3GPP Security requirements	3GPP specifications	NESAS/SCAS
gNodeB-specific security functional requirements				
#9	Requirements for the gNB setup and configuration	Setting up and configuring gNBs by O&M systems shall be authenticated and authorized by gNB so that attackers shall not be able to modify the gNB settings and software configurations via local or remote access. - The certificate enrolment mechanism specified in 3GPP TS 33.310 for base station should be supported for gNBs. The decision on whether to use the enrolment mechanism is left to operators. - Communication between the O&M systems and the gNB shall be confidentiality, integrity and replay protected from unauthorized parties. The security associations between the gNB and an entity in the 5G Core or in an O&M domain trusted by the operator shall be supported. These security association establishments shall be mutually authenticated. The security associations shall be realized according to ETSI TS 133 210 and 3GPP TS 33.310. - The gNB shall be able to ensure that software/data change attempts are authorized. - The gNB shall use authorized data/software. - Sensitive parts of the boot-up process shall be executed with the help of the secure environment. - Confidentiality of software transfer towards the gNB shall be ensured. - Integrity protection of software transfer towards the gNB shall be ensured. - The gNB software update shall be verified before its installation (see clause 4.2.3.3.5 of 3GPP TS 33.117).	ETSI TS 133 501 clause 5.3.4	
#10	Requirements for key management inside the gNB	Any part of a gNB deployment that stores or processes keys in cleartext shall be protected from physical attacks. If not, the whole entity is placed in a physically secure location, then keys in cleartext shall be stored and processed in a secure environment. Keys stored inside a secure environment in any part of the gNB shall never leave the secure environment except when done in accordance with 3GPP specifications.	ETSI TS 133 501 clause 5.3.5	
#11	Requirements for handling user plane data for the gNB	Any part of a gNB deployment that stores or processes user plane data in cleartext shall be protected from physical attacks. If not, the whole entity is placed in a physically secure location, then user plane data in cleartext shall be stored and processed in a secure environment.	ETSI TS 133 501 clause 5.3.6	
#12	Requirements for handling control plane data for the gNB	Any part of a gNB deployment that stores or processes control plane data in cleartext shall be protected from physical attacks. If not, the whole entity is placed in a physically secure location, then control plane data in cleartext shall be stored and processed in a secure environment.	ETSI TS 133 501 clause 5.3.7	
#13	Requirements for secure environment of the gNB	The secure environment shall support secure storage of sensitive data, e.g. long-term cryptographic secrets and vital configuration data. The secure environment shall support the execution of sensitive functions, e.g. en-/decryption of user data and the basic steps within protocols which use long term secrets (e.g. in authentication protocols). The secure environment shall support the execution of sensitive parts of the boot process. The secure environment's integrity shall be assured. Only authorised access shall be granted to the secure environment, i.e. to data stored and used within it, and to functions executed within it.	ETSI TS 133 501 clause 5.3.8	

Item	Title	3GPP Security requirements	3GPP specifications	NESAS/SCAS
gNodeB-specific security functional requirements				
#14	Requirements for the gNB F1 interfaces	F1-C interface shall support confidentiality, integrity, and replay protection. All management traffic carried over the CU-DU link shall be integrity, confidentiality and replay protected. The gNB shall support confidentiality, integrity and replay protection on the gNB DU-CU F1-U interface for user plane. F1-C and management traffic carried over the CU-DU link shall be protected independently from F1-U traffic. **Security mechanisms** In order to protect the traffic on the F1-U interface, IPsec ESP and IKEv2 certificates-based authentication shall be supported as specified in sub-clause 9.1.2 of ETSI TS 133 501 with confidentiality, integrity and replay protection. In order to protect the traffic on the F1-C interface, IPsec ESP and IKEv2 certificates-based authentication shall be supported as specified in sub-clause 9.1.2 of ETSI TS 133 501 with confidentiality, integrity, and replay protection. IPsec is mandatory to implement on the gNB-DU and on the gNB-CU. On the gNB-CU side, a SEG may be used to terminate the IPsec tunnel. In addition to IPsec, for the F1-C interface, DTLS shall be supported as specified in IETF RFC 6083 to provide integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the provisions given in clause 6.2 of ETSI TS 133 210.	ETSI TS 133 501 clauses 5.3.9 & 9.8.2	
#15	Requirements for the gNB E1 interfaces	The E1 interface between CU-CP and CU-UP shall be confidentiality, integrity and replay protected. **Security mechanisms** In order to protect the traffic on the E1 interface, IPsec ESP and IKEv2 certificates-based authentication shall be supported as specified in sub-clause 9.1.2 of of ETSI TS 133 501 with confidentiality, integrity, and replay protection. In addition to IPsec, DTLS shall be supported as specified in RFC 6083 to provide integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the provisions given in clause 6.2 of ETSI TS 133 210. IPsec is mandatory to support on the gNB-CU-UP and the gNB-CU-CP. Observe that on both the gNB-CU-CP and the gNB-CU-UP sides, a SEG may be used to terminate the IPsec tunnel.	ETSI TS 133 501 clauses 5.3.10 & 9.8.3	

Item	Title	3GPP Security requirements	3GPP specifications	NESAS/SCAS
gNodeB-specific security functional requirements				
#16	Security mechanisms for the N2/Xn interface	The transport of control plane data and user data over Xn/N2 shall be integrity, confidentiality and replay-protected. Security mechanisms In order to protect the traffic on the Xn reference point, it is required to implement IPsec ESP and IKEv2 certificate-based authentication as specified in sub-clause 9.1.2 of ETSI TS 133 501 with confidentiality, integrity, and replay protection. IPsec shall be supported on the gNB. In addition to IPsec, for the Xn-C interface, DTLS shall be supported as specified in IETF RFC 6083 to provide integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the provisions given in clause 6.2 of ETSI TS 133 210.	ETSI TS 133 501 clauses 9.2 & 9.4	ETSI TS 133 511 clauses 4.2.2.1.16 & 4.2.2.1.17
#17	AS algorithms selection	The serving network shall select the algorithms to use dependent on: the UE security capabilities of the UE, the configured allowed list of security capabilities of the currently serving network entity. Each gNB shall be configured via network management with lists of algorithms which are allowed for usage. There shall be one list for integrity algorithms, and one for ciphering algorithms. These lists shall be ordered according to a priority decided by the operator.	ETSI TS 133 501 clauses 6.7.3.0 & 5.11.2	ETSI TS 133 511 clause 4.2.2.1.12
#18	Key refresh at the gNB	Key refresh shall be possible for KgNB, KRRC-enc, KRRC-int, KUP-int, and KUP-enc and shall be initiated by the gNB when a PDCP COUNTs are about to be re-used with the same Radio Bearer identity and with the same KgNB. The network is responsible for avoiding reuse of the COUNT with the same RB identity and with the same key, e.g. due to the transfer of large volumes of data, release and establishment of new RBs, and multiple termination point changes for RLC-UM bearers. In order to avoid such re-use, the network may e.g. use different RB identities for RB establishments, change the AS security key, or an RRC_CONNECTED to RRC_IDLE/RRC_INACTIVE and then to RRC_CONNECTED transition." as specified in 3GPP TS 38.331, clause 5.3.1.2.	ETSI TS 133 501 clause 6.9.4.1 TS 38.331 clause 5.3.1.2	ETSI TS 133 511 clause 4.2.2.1.13
#19	AS protection algorithm selection in gNB change	The target gNB shall select the algorithm with highest priority from the UE's 5G security capabilities according to the locally configured prioritized list of algorithms (this applies for both integrity and ciphering algorithms). The chosen algorithms shall be indicated to the UE in the Handover Command message if the target gNB selects different algorithms compared to the source gNB.	ETSI TS 133 501 clauses 6.7.3.1 & 6.7.3.2	ETSI TS 133 511 clause 4.2.2.1.15
#20	Key update at the gNB on dual connectivity	When executing the procedure for adding subsequent radio bearer(s) to the same SN, the MN shall, for each new radio bearer, assign a radio bearer identity that has not previously been used since the last KSN change. If the MN cannot allocate an unused radio bearer identity for a new radio bearer in the SN, due to radio bearer identity space exhaustion, the MN shall increment the SN Counter and compute a fresh KSN, and then shall perform a SN Modification procedure to update the KSN. The SN shall request the Master Node to update the KSN over the Xn-C, when uplink and/or downlink PDCP COUNTs are about to wrap around for any of the SCG DRBs or SCG SRB.	ETSI TS 133 501 clauses 6.10.2.1 & 6.10.2.2.1	ETSI TS 133 511 clause 4.2.2.1.18

Item	Title	3GPP Security requirements	3GPP specifications	NESAS/SCAS
gNodeB-specific security functional requirements				
#21	Unauthorized Viewing	When the system is not under maintenance, there shall be no system function that reveals confidential system internal data in the clear to users and administrators. Such functions could be, for example, local or remote OAM CLI or GUI, logging messages, alarms, configuration file exports. Confidential system internal data contains authentication data (i.e. PINs, cryptographic keys, passwords, cookies) as well as system internal data that is not required for systems administration and could be of advantage to attackers (i.e. stack traces in error messages).		ETSI TS 133 511 clause 4.2.3.2.2 TS 33.117 clause 4.2.3.2.2
#22	Protecting data and information in storage	For sensitive data in (persistent or temporary) storage read access rights shall be restricted. Files of a system that are needed for the functionality shall be protected against manipulation. In addition, the following rules apply for: - Systems that need access to identification and authentication data in the clear, e.g. in order to perform an authentication. Such systems shall not store this data in the clear, but scramble or encrypt it by implementation-specific means. - Systems that do not need access to sensitive data (e.g. user passwords) in the clear. Such systems shall hash this sensitive data. - Stored files on the network product: examples for protection against manipulation are the use of checksum or cryptographic methods.		ETSI TS 133 511 clause 4.2.3.2.3 TS 33.117 clause 4.2.3.2.3
#23	Protecting data and information in transfer	Usage of cryptographically protected network protocols is required. The transmission of data with a need of protection shall use industry standard network protocols with sufficient security measures and industry accepted algorithms. In particular, a protocol version without known vulnerabilities or a secure alternative shall be used.		ETSI TS 133 511 clause 4.2.3.2.4 TS 33.117 clause 4.2.3.2.4
#24	System handling during overload situations	The system shall provide security measures to deal with overload situations which may occur as a result of a denial of service attack or during periods of increased traffic or reach the congestion threshold. In particular, partial, or complete impairment of system availability shall be avoided. Potential protective measures include: - Restricting available RAM per application. - Restricting maximum sessions for a Web application. - Defining the maximum size of a dataset. - Restricting CPU resources per process. - Prioritizing processes. - Overload control method, e.g. limiting amount or size of transactions of a user or from an IP address in a specific time range.		ETSI TS 133 511 clause 4.2.3.3 TS 33.117 clause 4.2.3.3.1
#25	Boot from intended memory devices only	The network product can boot only from the memory devices intended for this purpose.		ETSI TS 133 511 clause 4.2.3.3 TS 33.117 clause 4.2.3.3.2

Item	Title	3GPP Security requirements	3GPP specifications	NESAS/SCAS
gNodeB-specific security functional requirements				
#26	System handling during excessive overload situations	The system shall act in a predictable way if an overload situation cannot be prevented. A system shall be built in this way that it can react on an overload situation in a controlled way. However, it is possible that a situation happens where the security measures are no longer sufficient. In such case it shall be ensured that the system cannot reach an undefined and thus potentially insecure state. In an extreme case this means that a controlled system shutdown is preferable to uncontrolled failure of the security functions and thus loss of system protection. The vendor shall provide a technical description of the network product's Over Load Control mechanisms (especially whether these mechanisms rely on cooperation of other network elements e.g. eNode B) and the accompanying test case for this requirement will check that the description provides sufficient detail in order for an evaluator to understand how the mechanism is designed.		ETSI TS 133 511 clause 4.2.3.3 TS 33.117 clause 4.2.3.3.3
#27	System robustness against unexpected input	During transmission of data to a system it is necessary to validate input to the network product before processing. This includes all data which is sent to the system. Examples of this are user input, values in arrays and content in protocols. The following typical implementation error shall be avoided: - No validation on the lengths of transferred data - Incorrect assumptions about data formats - No validation that received data complies with the specification - Insufficient handling of protocol errors in received data - Insufficient restriction on recursion when parsing complex data formats - White listing or escaping for inputs outside the values margin		ETSI TS 133 511 clause 4.2.3.3 TS 33.117 clause 4.2.3.3.4
#28	Network product Software integrity validation	1) Software package integrity shall be validated in the installation/upgrade stage. 2) Network product shall support software package integrity validation via cryptographic means, e.g. digital signature. To this end, the network product has a list of public keys or certificates of authorised software sources, and uses the keys to verify that the software update is originated from only these sources. 3) Tampered software shall not be executed or installed if integrity check fails. 4) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software update, and modify the list mentioned in bullet 2.		ETSI TS 133 511 clause 4.2.3.3 TS 33.117 clause 4.2.3.3.5
#29	System functions shall not be used or accessed without successful authentication and authorization	The usage of a system function without successful authentication on basis of the user identity and at least one authentication attribute (e.g. password, certificate) shall be prevented. System functions comprise, for example network services (like SSH, SFTP, Web services), local access via a management console, local usage of operating system and applications. This requirement shall also be applied to accounts that are only used for communication between systems. An exception to the authentication and authorization requirement are functions for public use such as those for a Web server on the Internet, via which information is made available to the public.		3GPP TS 33.117 clause 4.2.3.4.1.1

Item	Title	3GPP Security requirements	3GPP specifications	NESAS/SCAS
gNodeB-specific security functional requirements				
#30	The network product shall use accounts that allow unambiguous identification of the user	Users shall be identified unambiguously by the network product. The network product shall support assignment of individual accounts per user, where a user could be a person, or, for Machine Accounts, an application, or a system. The network product shall not enable the use of group accounts or group credentials, or sharing of the same account between several users, by default. The network product shall support a minimum number of 50 individual accounts per user data base if not explicitly specified in a SCAS of a particular network product, so that accountability for each user is ensured even in large operator networks. The network product shall not support user access credentials unrelated to an account (see note 1).		3GPP TS 33.117 clause 4.2.3.4.1.2
#31	Account protection by at least one authentication attribute	The various user and machine accounts on a system shall be protected from misuse. To this end, an authentication attribute is typically used, which, when combined with the user name, enables unambiguous authentication and identification of the authorized user. Authentication attributes include: - Cryptographic keys - Token - Passwords This means that authentication based on a parameter that can be spoofed (e.g. phone numbers, public IP addresses or VPN membership) is not permitted. Exceptions are attributes that cannot be faked or spoofed by an attacker.		ETSI TS 133 511 clause 4.2.3.4.1 TS 33.117 clause 4.2.3.4.2.1
#32	Predefined accounts shall be deleted or disabled	All predefined or default accounts shall be deleted or disabled. Many systems have default accounts (e.g. guest, ctxsys), some of which are preconfigured with or without known passwords. These standard users shall be deleted or disabled. Should this measure not be possible the accounts shall be locked for remote login. In any case disabled or locked accounts shall be configured with a complex password as specified in clause 4.2.3.4.3.1 Password Structure of 3GPP TS 33.117. This is necessary to prevent unauthorized use of such an account in case of misconfiguration. Exceptions to this requirement to delete or disable accounts are accounts that are used only internally on the system involved and that are required for one or more applications on the system to function. Also, for these accounts remote access or local login shall be forbidden to prevent abusive use by users of the system.		ETSI TS 133 511 clause 4.2.3.4.1 3GPP TS 33.117 clause 4.2.3.4.2.2
#33	Predefined or default authentication attributes shall be deleted or disabled	Normally, authentication attributes such as password or cryptographic keys will be preconfigured from producer, vendor, or developer of a system. Such authentication attributes shall be changed by automatically forcing a user to change it on 1st time login to the system or the vendor provides instructions on how to manually change it.		ETSI TS 133 511 clause 4.2.3.4.1 3GPP TS 33.117 clause 4.2.3.4.2.3

Item	Title	3GPP Security requirements	3GPP specifications	NESAS/SCAS
gNodeB-specific security functional requirements				
#34	Password Complexity rule	The setting by the vendor shall be such that a network product shall only accept passwords that comply with the following complexity criteria: 1) Absolute minimum length of 8 characters (shorter lengths shall be rejected by the network product). It shall not be possible setting this absolute minimum length to a lower value by configuration. 2) Comprising at least three of the following categories: - at least 1 uppercase character (A-Z) - at least 1 lowercase character (a-z) - at least 1 digit (0-9) - at least 1 special character (e.g. @;!$.) The network product shall use a default minimum length of 10 characters. The minimum length of characters in the passwords shall be configurable by the operator. The default minimum length is the value configured by the vendor before any operator-specific configuration has been applied. The special characters may be categorized in sets according to their Unicode category. The network product shall at least support passwords of a length of 64 characters or a length greater than 64 characters. If a central system is used for user authentication, password policy is performed on the central system and additional assurance shall be provided that the central system enforces the same password complexity rules as laid down for the local system in this subclause. If a central system is not used for user authentication, the assurance on password complexity rules shall be performed on the Network Product. When a user is changing a password or entering a new password, the system checks and ensures that it meets the password requirements. Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level).		3GPP TS 33.117 clause 4.2.3.4.3.1
#35	Password changes	If a password is used as an authentication attribute, then the system shall offer a function that enables a user to change his password at any time. When an external centralized system for user authentication is used it is possible to redirect or implement this function on this system. Password change shall be enforced after initial login. The system shall enforce password change based on password management policy. In particular, the system shall enforce password expiry. Previously used passwords shall not be allowed up to a certain number (Password History). The number of disallowed previously used passwords shall be: - Configurable; - Greater than 0; - And its default value shall be 3. This means that the network product shall store at least the three previously set passwords. The maximum number of passwords that the network product can store for each user is up to the manufacturer. When a password is about to expire a password expiry notification shall be provided to the user. Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level.). An exception to this requirement is machine accounts.		3GPP TS 33.117 clause 4.2.3.4.3.2

Item	Title	3GPP Security requirements	3GPP specifications	NESAS/SCAS
gNodeB-specific security functional requirements				
#36	Protection against brute force and dictionary attacks	If a password is used as an authentication attribute, a protection against brute force and dictionary attacks that hinder password guessing shall be implemented. Brute force and dictionary attacks aim to use automated guessing to ascertain passwords for user and machine accounts. Various measures or a combination of these measures can be taken to prevent this. The most commonly used protection measures are: 1) Using the timer delay (this delay could be the same or increased depending the operator's policy for each attempt, e.g. double the delay, or 5 minutes delay, or 10 minutes delay) for each newly entered password input following an incorrect entry ("tar pit"). 2) Blocking an account following a specified number of incorrect attempts, refer to 4.2.3.4.5 of 3GPP TS 33.117. However, it has to be taken into account that this solution needs a process for unlocking and an attacker can force this to deactivate accounts and make them unusable. 3) Using CAPTCHA to prevent automated attempts (often used for Web applications). 4) Using a password blacklist to prevent vulnerable passwords. (see note 2) In order to achieve higher security, it is often meaningful to combine two or more of the measures named here. It is left to the vendor to select appropriate measures. Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level.). An exception to this requirement is machine accounts.		3GPP TS 33.117 clause 4.2.3.4.3.3
#37	Hiding password display	The password shall not be displayed in such a way that it could be seen and misused by a casual local observer. Typically, the individual characters of the password are replaced by a character such as "*". Under certain circumstances it may be permissible for an individual character to be displayed briefly during input. Such a function is used, for ex ample, on smartphones to make input easier. However, the entire password is never output to the display in plaintext. Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level.). An exception to this requirement is machine accounts.		3GPP TS 33.117 clause 4.2.3.4.3.4
#38	Network Product Management and Maintenance interfaces	The network product management shall support mutual authentication mechanisms, the mutual authentication mechanism can rely on the protocol used for the interface itself or other means.		3GPP TS 33.117 clause 4.2.3.4.4.1

Item	Title	3GPP Security requirements	3GPP specifications	NESAS/SCAS
gNodeB-specific security functional requirements				
#39	Policy regarding consecutive failed login attempts	a) The maximum permissible number of consecutive failed user account login attempts should be configurable by the operator. The definition of the default value set at manufacturing time for maximum number of failed user account login attempts shall be less than or equal to 8, typically 5. After the maximum permissible number of consecutive failed user account login attempts is exceeded by a user there shall be a block delay in allowing the user to attempt login again. This block delay and also the capability to set period of the block delay, e.g. double the delay, or 5 minutes delay, or 10 minutes delay, after each login failure should be configurable by the operator. The default value set at manufacturing time for this delay shall be greater than or equal to 5 sec. b) If supported, infinite (permanent) locking of an account that has exceeded maximum permissible number of consecutive failed user account login attempts should also be possible via configuration, with the exception of administrative accounts which shall get only temporarily locked.		3GPP TS 33.117 clause 4.2.3.4.5
#40	Authorization policy	The authorizations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform. Authorizations to a system shall be restricted to a level in which a user can only access data and use functions that he needs in the course of his work. Suitable authorizations shall also be assigned for access to files that are components of the operating system or of applications or that are generated by the same (e.g. configuration and logging files). Alongside access to data, execution of applications and components shall also take place with rights that are as low as possible. Applications should not be executed with administrator or system rights.		TS 33.117 clause 4.2.3.4.6.1
#41	Role-based access control	The network product shall support Role Based Access Control (RBAC). A role-based access control system uses a set of controls which determines how users interact with domains and resources. The domains could be Fault Management (FM), Performance Management (PM), System Admin. The RBAC system controls how users or groups of users are allowed access to the various domains and what type of operation they can perform, i.e. the specific operation command or command group (e.g. View, Modify, Execute). The network product supports RBAC, in particular, for OAM privilege management for network product Management and Maintenance, including authorization of the operation for configuration data and software via the network product console interface.		3GPP TS 33.117 clause 4.2.3.4.6.2
#42	Protecting sessions - logout function	The system shall have a function that allows a signed in user to logout at any time. All processes under the logged in user ID shall be terminated on log out. The network product shall be able to continue to operate without interactive sessions. Only for debugging purposes, processes under a logged in user ID may be allowed to continue to run after detaching the interactive session.		ETSI TS 133 511 clause 4.2.3.5 3GPP TS 33.117 clause 4.2.3.5.1
#43	Protecting sessions - inactivity timeout	An OAM user interactive session shall be terminated automatically after a specified period of inactivity. It shall be possible to configure an inactivity time-out period (see note 3).		ETSI TS 133 511 clause 4.2.3.5 3GPP TS 33.117 clause 4.2.3.5.2

Item	Title	3GPP Security requirements	3GPP specifications	NESAS/SCAS
gNodeB-specific security functional requirements				
#44	Security event logging	Security events shall be logged together with a unique system reference (e.g. host name, IP or MAC address) and the exact time the incident occurred. For each security event, the log entry shall include user name and/or timestamp and/or performed action and/or result and/or length of session and/or values exceeded and/or value reached. IETF RFC 3871, clause 2.11.10 specifies the minimum set of security events. Each vendor shall document what security events the product logs so that it can be verified by testing.		ETSI TS 133 511 clause .2.3.6 3GPP TS 33.117 clause 4.2.3.6.1
#45	Log transfer to centralized storage	a) The Network Product shall support forwarding of security event logging data to an external system. Secure transport protocols in accordance with clause 4.2.3.2.4 of 3GPP TS 33.117, shall be used. b) Log functions should support secure uploading of log files to a central location or to an external system for the Network Product that is logging.		ETSI TS 133 511 clause 4.2.3.6 3GPP TS 33.117 clause 4.2.3.6.2
#46	Protection of security event log files	The security event log shall be access controlled (file access rights) so only privileged users have access to the log files.		ETSI TS 133 511 clause 4.2.3.6 3GPP TS 33.117 clause 4.2.3.6.3
#47	Growing (dynamic) content shall not influence system functions	Growing or dynamic content (e.g. log files, uploads) shall not influence system functions. A file system that reaches its maximum capacity shall not stop a system from operating properly. Therefore, countermeasures shall be taken such as usage of dedicated filesystems, separated from main system functions, or quotas, or at least a file system monitoring to ensure that this scenario is avoided.		ETSI TS 133 511 clause 4.2.4 3GPP TS 33.117 clause 4.2.4.1.1.1
#48	Processing of ICMPv4 and ICMPv6 packets	Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the network product. In particular, there are certain types of ICMP4 and ICMPv6 that are not used in most networks, but represent a risk. ICMP message types which on receipt lead to responses or to configuration changes are not mentioned in this requirement, but they may be necessary to support relevant and specified networking features. Those must be documented. Certain ICMP types are generally permitted and do not need to be specifically documented. Those are marked as "Permitted" in this table below. The network product shall not send certain ICMP types by default, but it may support the option to enable utilization of these types (e.g. for debugging). Echo Reply can be sent by default. In case of remote base station auto deployment, Router Advertisement can be processed.		ETSI TS 133 511 clause 4.2.4 3GPP TS 33.117 clause 4.2.4.1.1.2
#49	IP packets with unnecessary options or extension headers shall not be processed	IP packets with unnecessary options or extension headers shall not be processed. IP options and extension headers (e.g. source routing) are only required in exceptional cases. So, all packets with enabled IP options or extension headers shall be filtered.		ETSI TS 133 511 clause 4.2.4 3GPP TS 33.117 clause 4.2.4.1.1.3
#50	Authenticated Privilege Escalation only	There shall not be a privilege escalation method in interactive sessions (CLI or GUI) which allows a user to gain administrator/root privileges from another user account without re-authentication. Implementation example: Disable insecure privilege escalation methods so that users are required to (re-)login directly into the account with the required permissions.		ETSI TS 133 511 clause 4.2.4 3GPP TS 33.117 clause 4.2.4.1.2.1

Item	Title	3GPP Security requirements	3GPP specifications	NESAS/SCAS
gNodeB-specific security functional requirements				
#51	System account identification	Each system account in UNIX® shall have a unique UID.		ETSI TS 133 511 clause 4.2.4 3GPP TS 33.117 clause 4.2.4.2.2
#52	HTTPS	The communication between Web client and Web server shall be protected using TLS. The TLS profile defined in Annex E of 3GPP TS 33.310 shall be followed with the following modifications: Cipher suites with NULL encryption shall not be supported		ETSI TS 133 511 clause 4.2.5 3GPP TS 33.117 clause 4.2.5.1
#53	Webserver logging	Access to the webserver shall be logged. The web server log shall contain the following information: - Access timestamp - Source (IP address) - (Optional) Account (if known) - (Optional) Attempted login name (if the associated account does not exist) - Relevant fields in http request. The URL should be included whenever possible. - Status code of web server response		ETSI TS 133 511 clause 4.2.5 3GPP TS 33.117 clause 4.2.5.2.1
#54	User sessions	To protect user sessions the Network Product shall support the following session ID and session cookie requirements: 1. The session ID shall uniquely identify the user and distinguish the session from all other active sessions. 2. The session ID shall be unpredictable. 3. The session ID shall not contain sensitive information in clear text (e.g. account number, social security.). 4. In addition to the Session Idle Timeout (see clause 4.2.3.5.2 Protecting sessions - Inactivity timeout of 3GPP TS 33.117), the Network Product shall automatically terminate sessions after a configurable maximum lifetime This maximum lifetime defines the maximum session span. When the maximum lifetime expires, the session shall be closed, the session ID shall be deleted, and the user shall be forced to (re)authenticate in the web application and to establish a new session. The default value for this maximum lifetime shall be set to 8 hours. 5. Session ID's shall be regenerated for each new session (e.g. each time a user log in). 6. The session ID shall not be reused or renewed in subsequent sessions. 7. The Network Product shall not use persistent cookies to manage sessions but only session cookies. This means that neither the "expire" nor the "max-age" attribute shall be set in the cookies. 8. Where session cookies are used the attribute 'HttpOnly' shall be set to true. 9. Where session cookies are used the 'domain' attribute shall be set to ensure that the cookie can only be sent to the specified domain. 10. Where session cookies are used the 'path' attribute shall be set to ensure that the cookie can only be sent to the specified directory or sub-directory. 11. The Network Product shall not accept session identifiers from GET/POST variables. 12. The Network Product shall be configured to only accept server generated session ID's.		ETSI TS 133 511 clause 4.2.5 3GPP TS 33.117 clause 4.2.5.3
#55	HTTP input validation	The Network Product shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks. The Network Product shall validate, filter, escape, and encode user-controllable input before it is placed in output that is used as a web page that is served to other users.		ETSI TS 133 511 clause 4.2.5 3GPP TS 33.117 clause 4.2.5.4

Item	Title	3GPP Security requirements	3GPP specifications	NESAS/SCAS
gNodeB-specific security functional requirements				
#56	Packet filtering	The Network Product shall provide a mechanism to filter incoming IP packets on any IP interface (see IETF RFC 3871 for further information). In particular the Network Product shall provide a mechanism: 1) To filter incoming IP packets on any IP interface at Network Layer .and Transport Layer of the stack ISO/OSI. 2) To allow specified actions to be taken when a filter rule matches. In particular at least the following actions should be supported: a. Discard/Drop: the matching message is discarded; no subsequent rules are applied and no answer is sent back. b. Accept: the matching message is accepted. c. Account: the matching message is accounted for i.e. a counter for the rule is incremented. This action can be combined with the previous ones. This feature is useful to monitor traffic before its blocking. 3) To enable/disable for each rule the logging for Dropped packets, i.e. details on messages matching the rule for troubleshooting. 4) To filter on the basis of the value(s) of any portion of the protocol header. 5) To reset the accounting. 6) The Network Product shall provide a mechanism to disable/enable each defined rule.		ETSI TS 133 511 clause 4.2.6.2.1 3GPP TS 33.117 clause 4.2.6.2.1
#57	Manipulated packets that are sent to an address of the network device shall not lead to an impairment of availability	A network device shall be not affected in its availability or robustness by incoming packets, from other network element, that are manipulated or differing the norm. This means that appropriate packets shall be detected as invalid and be discarded. The process shall not be affecting the performance of the network device. This robustness shall be just as effective for a great mass of invalid packets as for individual or a small number of packets. Examples of such packets are: - Mass-produced TCP packets with a set SYN flag to produce half-open TCP connections (SYN flooding attack). - Packets with the same IP sender address and IP recipient address (Land attack). - Mass-produced ICMP packets with the broadcast address of a network as target address (Smurf attack). - Fragmented IP packets with overlapping offset fields (Teardrop attack). - ICMP packets that are larger than the maximum permitted size (65 535 Bytes) of IPv4 packets (Ping-of-death attack). - Uncorrelated reply packets (i.e. packets which cannot be correlated to any request). Sometimes the relevant behaviour of the network device will be configured. In other cases, the behaviour of the network device may only be verified by the relevant tests.		ETSI TS 133 511 clause 4.2.6.2.2 3GPP TS 33.117 clause 4.2.6.2.2

Item	Title	3GPP Security requirements	3GPP specifications	NESAS/SCAS
gNodeB-specific security functional requirements				
#58	GTP-U Filtering	The following capability is conditionally required: - For each message of a GTP-U-based protocol, it shall be possible to check whether the sender of this message is authorized to send a message pertaining to this protocol (see note 4). - At least the following actions should be supported when the check is satisfied: - Discard: the matching message is discarded. - Accept: the matching message is accepted. - Account: the matching message is accounted for, i.e. a counter for the rule is incremented. This action can be combined with the previous ones. This feature is useful to monitor traffic before its blocking. This requirement is conditional in the following sense: It is required that at least one of the following two statements holds: - The Network Product supports the capability described above and this is stated in the product documentation. - The Network Product's product documentation states that the capability is not supported and that the Network Product needs to be deployed together with a separate entity which provides the capability described above. See notes 5, 6 and 7.		ETSI TS 133 511 clause 4.2.6.2.4 3GPP TS 33.117 clause 4.2.6.2.4
gNodeB-specific security hardening requirements				
Technical Baseline				
#59	No unnecessary or insecure services / protocols	The network product shall only run protocol handlers and services which are needed for its operation, and which do not have any known security vulnerabilities.		3GPP TS 33.117 clause 4.3.2.1
#60	Restricted reachability of services	The network product shall restrict the reachability of services so that they can only be reached on interfaces where their usage is required. On interfaces were services are active, the reachability should be limited to legitimate communication peers.		3GPP TS 33.117 clause 4.3.2.2
#61	No unused software	Unused software components or parts of software which are not needed for operation or functionality of the network product shall not be installed or shall be deleted after installation.		3GPP TS 33.117 clause 4.3.2.3
#62	No unused functions	During installation of software and hardware often functions will be activated that are not required for operation or function of the system. Also, hardware functions which are not required for operation or function of the system (e.g. unused interfaces) shall be permanently deactivated. Permanently means that they shall not be reactivated again after network product reboot. EXAMPLE: A debugging function in software which can be used for troubleshooting shall not be activated during normal operation of the network product.		3GPP TS 33.117 clause 4.3.2.4
#63	No unsupported components	The network product shall not contain software and hardware components that are no longer supported by their vendor, producer, or developer, such as components that have reached end-of-life or end-of-support. Excluded are components that have a special support contract. This contract shall guarantee the correction of vulnerabilities over components' lifetime.		3GPP TS 33.117 clause 4.3.2.5
#64	Remote login restrictions for privileged users	Direct login as root or equivalent highest privileged user shall be limited to the system console only. Root user will not be allowed to login to the system remotely.		3GPP TS 33.117 clause 4.3.2.6

Item	Title	3GPP Security requirements	3GPP specifications	NESAS/SCAS
gNodeB-specific security functional requirements				
#65	Filesystem Authorization privileges	The system shall be designed to ensure that only users that are authorized to modify files, data, directories, or file systems have the necessary privileges to do so. EXAMPLE: On unix® systems a 'sticky' bit may be set on all directories where all users have written permissions. This ensures that only the file's owner, the directory's owner, or root user can rename or delete the file. Without the sticky bit being set, any user that has write and execute permissions for the directory can rename or delete files within the directory, regardless of the file's owner.		3GPP TS 33.117 clause 4.3.2.7
Operating Systems				
#66	IP-Source address spoofing mitigation	Systems shall not process IP packets if their source address is not reachable via the incoming interface. Implementation example: Use of "Reverse Path Filter" (RPF) provides this function.		3GPP TS 33.117 clause 4.3.3.1.1
#67	Minimized kernel network functions	Kernel based network functions not needed for the operation of the network element shall be deactivated. In particular the following ones shall be disabled by default: - IP Packet Forwarding between different interfaces of the network product.		3GPP TS 33.117 clause 4.3.3.1.2
#68	No automatic launch of removable media	The network product shall not automatically launch any application when removable media device such as CD-, DVD-, USB-Sticks or USB-Storage drive is connected. If the operating system supports an automatic launch, it shall be deactivated unless it is required to support availability requirements.		3GPP TS 33.117 clause 4.3.3.1.3
#69	Syn Flood Prevention	The network product shall support a mechanism to prevent Syn Flood attacks (e.g. implement the TCP Syn Cookie technique in the TCP stack by setting net.ipv4.tcp_syncookies = 1 in the linux sysctl.conf file). This feature shall be enabled by default.		3GPP TS 33.117 clause 4.3.3.1.4
#70	Protection mechanisms against buffer overflows	The system shall support mechanisms for buffer overflow protection. Documentation which describes these buffer overflow mechanisms and also how to check that they have been enabled and/or implemented shall be provided.		3GPP TS 33.117 clause 4.3.3.1.5
#71	External file system mount restrictions	If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems. Implementation example: In Linux® systems, administrators shall set the options nodev and nosuid in the /etc/fstab for all filesystems, which also have the "user" option. See note 8.		3GPP TS 33.117 clause 4.3.3.1.6
Web Servers				
#72	No system privileges for web server	No web server processes shall run with system privileges. This is best achieved if the web server runs under an account that has minimum privileges. If a process is started by a user with system privileges, execution shall be transferred to a different user without system privileges after the start.		3GPP TS 33.117 clause 4.3.4.2
#73	Unused HTTP methods shall be deactivated	HTTP methods that are not required shall be deactivated. Standard requests to web servers only use GET, HEAD, and POST. If other methods are required, they shall not introduce security leaks such as TRACK or TRACE.		3GPP TS 33.117 clause 4.3.4.3
#74	Any add-ons and components that are not required shall be deactivated	All optional add-ons and components of the web server shall be deactivated if they are not required. In particular, CGI or other scripting components, Server Side Includes (SSI), and WebDAV shall be deactivated if they are not required.		3GPP TS 33.117 clause 4.3.4.4

Item	Title	3GPP Security requirements	3GPP specifications	NESAS/SCAS
gNodeB-specific security functional requirements				
#75	No compiler, interpreter, or shell via CGI or other server-side scripting	If Common Gateway Interface (CGI) or other scripting technology is used, the CGI directory - or other corresponding scripting directory - shall not include compilers or interpreters (e.g. PERL interpreter, PHP interpreter/compiler, Tcl interpreter/compiler or operating system shells).		3GPP TS 33.117 clause 4.3.4.5
#76	No CGI or other scripting for uploads	If CGI or other scripting technology is used, the associated CGI/script directory shall not be used for uploads.		3GPP TS 33.117 clause 4.3.4.6
#77	No execution of system commands with SSI	If Server Side Includes (SSI) is active, the execution of system commands shall be deactivated.		3GPP TS 33.117 clause 4.3.4.7
#78	Access rights for web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges	Access rights for web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges. Implementation example: Delete "read" and "write" access rights for "others." Only grant "write" access to the user who configures the web server.		3GPP TS 33.117 clause 4.3.4.8
#79	Default content shall be removed	Default content (examples, help files, documentation, aliases) that is provided with the standard installation of the web server shall be removed.		3GPP TS 33.117 clause 4.3.4.9
#80	No directory listings / Directory Browsing	Directory listings (indexing) / "Directory browsing" shall be deactivated.		3GPP TS 33.117 clause 4.3.4.10
#81	Information about the web server in HTTP headers shall be minimized	The HTTP header shall not include information on the version of the web server and the modules/add-ons used.		3GPP TS 33.117 clause 4.3.4.11
#82	Web server information in error pages shall be deleted	User-defined error pages shall not include version information about the web server and the modules/add-ons used. Error messages shall not include internal information such as internal server names, error codes. Default error pages of the web server shall be replaced by error pages defined by the vendor.		3GPP TS 33.117 clause 4.3.4.12
#83	File type- or script-mappings that are not required shall be deleted	File type- or script-mappings that are not required shall be deleted, e.g. php, phtml, js, sh, csh, bin, exe, pl, vbe, vbs.		3GPP TS 33.117 clause 4.3.4.13
#84	The web server shall only deliver files which are meant to be delivered	Restrictive access rights shall be assigned to all files which are directly or indirectly (e.g. via links or in virtual directories) in the web server's document directory. In particular, the web server shall not be able to access files which are not meant to be delivered.		3GPP TS 33.117 clause 4.3.4.14
#85	Only execute rights in CGI/Scripting directory	If CGI or other scripting technology is used, only the CGI/Scripting directory is configured with execute rights. Other directories used or meant for web content do not have execute rights.		3GPP TS 33.117 clause 4.3.4.15
Network Devices				
#86	Traffic Separation	The network product shall support physical or logical separation of traffic belonging to different network domains. For example, O&M traffic and control plane traffic belong to different network domains. See IETF RFC 3871 for further information.		3GPP TS 33.117 clause 4.3.5.1

Item	Title	3GPP Security requirements	3GPP specifications	NESAS/SCAS
gNodeB-specific security functional requirements				
Basic vulnerability testing requirements				
#87	Port scanning	It shall be ensured that on all network interfaces, only documented ports on the transport layer respond to requests from outside the system.		3GPP TS 33.117 clause 4.4.2
#88	Vulnerability scanning	The purpose of vulnerability scanning is to ensure that there are no known vulnerabilities (or that relevant vulnerabilities are identified and remediation plans in place to mitigate them) on the Network Product, both in the OS and in the applications installed, that can be detected by means of automatic testing tools via the Internet Protocol enabled network interfaces. Vulnerability scanning tools may also report false positives and they shall be investigated and documented in the test report.		3GPP TS 33.117 clause 4.4.3
#89	Robustness and fuzz testing	It shall be ensured that externally reachable services are reasonably robust when receiving unexpected input.		3GPP TS 33.117 clause 4.4.4
Virtualization				
#90	VNF package and VNF image integrity	1) VNF package and image shall contain integrity validation value (e.g. MAC). 2) VNF package shall be integrity protected during onboarding and its integrity shall be validated by the NFVO.		3GPP TR 33.818 clause 5.2.5.5.3.3.5.1 3GPP TR 33.848 clause 5.18.3
#91	GVNP lifecycle management security	1) VNF shall authenticate VNFM when VNFM initiates a communication to VNF. 2) VNF shall be able to establish securely protected connection with the VNFM. 3) VNF shall check whether VNFM has been authorized when VNFM access VNF's API. 4) VNF shall log VNFM's management operations for auditing.		3GPP TR 33.818 clause 5.2.5.5.7.1
#92	Secure executive environment provision	The VNF shall support to compare the owned resource state with the parsed resource state from VNFD (VNF Description) by the VNFM. The VNF can query the parsed resource state by the VNFM from the OAM. The VNF shall send an alarm to the OAM if the two resource states are inconsistent. This comparing process can be triggered periodically by the VNF, or the administrator can manually trigger the VNF to perform the comparing process.		3GPP TR 33.818 clause 5.2.5.5.7.2
#93	Traffic Separation	The virtualised network product shall support logical separation of traffic belonging to different network domains. For example, O&M traffic and control plane traffic belong to different network domains. See IETF RFC 3871 for further information.		3GPP TR 33.818 clause 5.2.5.5.8.5.1 3GPP TS 33.117 clause 4.3.5.1
#94	Inter-VNF and intra-VNF Traffic Separation	The network used for the communication between the VNFCs of a VNF (intra-VNF traffic) and the network used for the communication between VNFs (inter-VNF traffic) shall be separated to prevent the security threats from the different networks affect each other.		3GPP TR 33.818 clause 5.2.5.5.8.5.2
#95	Instantiating VNF from trusted VNF image	A VNF shall be initiated from a trusted VNF image which includes one or more than one images. The VNF image shall be signed by an authorized party. The authorized party is trusted by the operators.		3GPP TR 33.818 clause 5.2.5.6.6.1 3GPP TR 33.848 clause 5.18.3
#96	Secure virtualisation resource management	To prevent a compromised VIM from changing the assigned virtualised resource, the VNF shall alert to the OAM. For example, when an instantiated VNF is running, a compromised VIM can delete a VM which is running VNFCI, the VNF shall alert to the OAM when the VNF cannot detect a VNFC message. A VNF shall log the access from the VIM. See note 9.		3GPP TR 33.818 clause 5.2.5.6.7.1

Item	Title	3GPP Security requirements	3GPP specifications	NESAS/SCAS
gNodeB-specific security functional requirements				
#97	Secure executive environment creation	When an attacker tampers a driver which provided by the hardware and used to create the executive environment, the virtualisation layer shall alert the driver error to the administrator for checking the error and finding the attack at latter (see note 10).		3GPP TR 33.818 clause 5.2.5.6.7.2
#98	VM escape protection	To defence the attack that an attacker utilizes a vulnerability of a VNF to attack a virtualisation layer and then control the virtualisation layer, the virtualisation layer shall implement the following requirements: The virtualisation shall reject the abnormal access from the VNF (e.g. the VNF accesses the memory which is not allocated to the VNF) and log the attacks.		3GPP TR 33.818 clause 5.2.5.6.7.3
#99	Secure hardware resource management	The VIM manages the hardware resource configuration and state information exchange. When the VIM is compromised to change the hardware resource configuration, an alert shall be triggered by the hardware. The administrator can check the alert and find the attack at latter.		3GPP TR 33.818 clause 5.2.5.7.7.1
#100	Secure hardware resource management information	When a compromised Virtualisation layer tampers the hardware resource configuration which is received from the VIM to result in the configuration error of the hardware, the hardware shall trigger an alert. The administrator can check the alert and find the attack at latter (see note 11).		3GPP TR 33.818 clause 5.2.5.7.7.2
#101	Trusted platform	The host system shall implement a Hardware-Based Root of Trust (HBRT) ((e.g. TPM, HSM)) as Initial Root of Trust, see ETSI GS NFV-SEC 012. The trust state of the platform shall be measured and a trusted chain shall be built, see ETSI GR NFV-SEC 007.		3GPP TR 33.818 clause 5.2.5.7.7.3

NOTE 1: The network product may support independent user data bases for different access methods, e.g. one data base for command shell access on OS level and another data base for GUI access. User data bases may be stored locally on the network product or on a central AAA system that the network product accesses for user authentication.
NOTE 2: Password management and blacklist configuration may be done in a separate node that is different to the node under test, e.g. a SSO server or any other central credential manager.
NOTE 3: The kind of activity required to reset the timeout timer depends on the type of user session.
NOTE 4: The check could be performed e.g. against a whitelist or blacklist of permitted message type / sender identity combinations.
NOTE 5: Such a separate entity could e.g. be a GTP Firewall.
NOTE 6: Test cases for this separate entity are not provided in the present document, but are believed to be similar to them.
NOTE 7: The test cases are only applicable to all network product classes utilizing GTP-U based protocol.
NOTE 8: Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.
NOTE 9: The VIM manages the virtualisation resource assignment and synchronization of virtualised resource state information. In the implementation, the VIM and the virtualisation layer are coupled and provided by one vendor, they trust each other. Whether the VIM is trust or not is based on operator's decision.
NOTE 10: Whether the hardware is trust or not is based on operator's decision to ensure the virtualisation layer and the VNF to be run on the trusted hardware.
NOTE 11: Whether the virtualisation layer is trust or not is based on operator's decision.

Annex C (informative): Guidance on Security Requirements & Controls

C.1 O-Cloud

Controls given in this clause are designed as a guidance and non-normative. The implementation of those non-normative controls depends on the security policies within the O-Cloud Service Provider, O-RAN Application Provider and Service Provider.

C.1.1 Secure protection of cryptographic keys and sensitive data

Potential solutions for SEC-CTL-OCLOUD-SS-1

The following potential implementation options for encrypting cryptographic keys and sensitive data within the O-Cloud platform could be used. The appropriate option to be used depends on the sensitivity of the data to be protected and needs to be assessed/determined by the Service provider.

1. Software based:

    a. Software-based KMS vaults supporting management of keys, including creation, rotation, and revocation, as well as encrypting and decrypting sensitive data with managed keys [51].

    b. Use a vTPM: A virtual Trusted Platform Module (vTPM) is a software-based representation of a physical Trusted Platform Module 2.0 chip to provide secure storage of credentials or keys [54]. A vTPM acts as any other virtual device. It performs the same functions as a TPM, but it performs cryptographic coprocessor capabilities in software. It should comply with the TPM 2.0 specification [53].

2. Hardware based

    a. Hardware-based key vaults: The use of Key Management Service (KMS) based on an HSM [i.5], [i.6], [52]. The data is encrypted using a Data Encryption Key (DEK); a new DEK is generated for each encryption. The DEKs are encrypted with a Key Encryption Key (KEK) that is stored and managed in the HSM of the KMS provider.

    b. A hardware TPM [i.8], [53]. For data encryption, an encryption key is stored on disk but encrypted with the TPM master key (the Storage Root Key (SRK)). This encryption key can only be used after it was decrypted by an authenticated TPM. The actual data encryption/decryption is then done by the main CPU, only decryption/encryption of the encryption key is done inside the TPM.

Potential solutions for SEC-CTL-OCLOUD-SS-2

- Overwriting with zero (e.g. /dev/zero) or simple patterns.
- Overwriting with random data using:
    - True random data source (e.g. /dev/random). This solution takes too long to wait for the entropy generation.
    - Pseudorandom data source (e.g. /dev/urandom) can be used as a reasonable source of pseudorandom data.

Potential solutions for SEC-CTL-OCLOUD-SS-3

Each data center adheres to a strict disposal policy and uses the techniques described to achieve compliance with NIST SP 800-88 [75] and DoD 5220.22-M [50].

Potential solutions for REQ-SEC-OCLOUD-SS-5

Automatic memory scrubbing on boot:

- Implement a process that automatically clears all volatile memory as early as possible during the boot sequence. This can be achieved through BIOS settings or early-stage boot loader scripts that overwrite memory with zeros or random data to ensure no residual data is left accessible.

Watchdog timers:

- Use timers that watch for unexpected shutdowns or power losses. If something goes wrong, these timers help make sure memory is cleaned properly before the system starts up again.

Work with power backup systems:

- For systems with an Uninterruptible Power Supply (UPS), integrate the memory scrubbing mechanism with UPS software to initiate secure shutdown procedures that include clearing volatile memory when the UPS detects a power outage and is about to run out of battery.

C.1.2 Chain of Trust

Potential solutions for SEC-CTL-OCLOUD-COT-1

There are many ways to measure platform integrity. In many cases, a hardware security module is used to store measurement data such as a HSM and TPM. Various platform integrity technologies build their own CoTs [i.7] and listed here below:

- UEFI Secure Boot (SB)
- Intel Trusted Execution Technology (TXT)
- Intel Boot Guard
- Intel Platform Firmware Resilience (PFR)
- Intel Technology Example Summary
- AMD Platform Secure Boot (AMD PSB)
- Arm TrustZone Trusted Execution Environment (TEE) for Armv8-A
- Arm Secure Boot and the Chain of Trust (CoT)
- Cisco Platform Roots of Trust
- IBM Chain of Trust (CoT)

For more details, see [i.7], clause 3.2.

Potential solutions for SEC-CTL-OCLOUD-COT-2

A vTPM can be considered a software-based implementation of a root of trust. It emulates the behavior and functionalities of a physical TPM through software mechanisms and cryptographic libraries [53], [54]. A vTPM operates within a virtual machine or as a software module within an operating system, leveraging the underlying hardware and security features provided by the host system. It can perform key generation, storage, and cryptographic operations similar to a physical TPM. However, since it is implemented in software, its security relies on the host system's security measures and may be more vulnerable to compromise if the host system is compromised. Therefore, it is crucial to ensure the overall security of the O-Cloud where the vTPM is deployed and to consider additional security measures to protect the software root of trust.

Potential solutions for SEC-CTL-OCLOUD-COT-3

Refer to the following technology examples in [i.7], clause 6.1 for more information:

- Intel Security Libraries for the Data Center (ISecL-DC)

- Remote AS - Project Veraison (VERificAtIon of atteStatiON)
- IBM Platform Attestation Tooling

Relevant information on the Attestation Server is provided in [i.7], clause 6.1 and [44], clause 6.6.

Figure C.1.2-1 shows an example of remote AS:

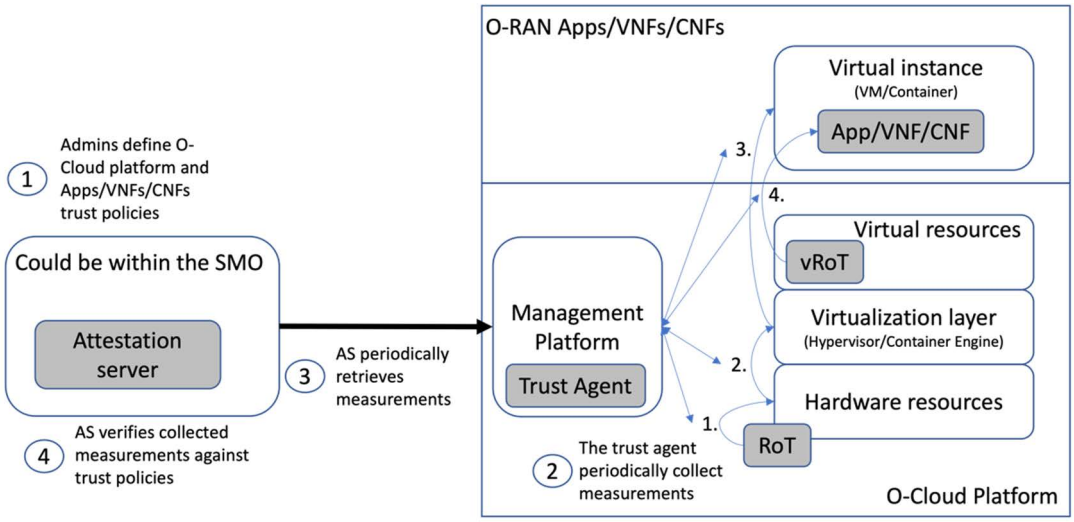

Figure C.1.2-1

The AS from the hardware layer to the O-RAN Application includes the following steps (see figure C.1.2-1):

Attestation of the O-Cloud platform

1. RoT measures and verifies hardware resources (server platform) including firmware/BIOS. It then launches the hardware resources.
2. The server act as the attester of the OS/virtualization layer. It measures, verifies, and launches the OS/virtualization layer.

The attestation results and corresponding measurements are maintained by the management platform (e.g. Kubernetes) acting as the trust agent.

Attestation of Application

The attestation process is initiated by the management platform requesting to instantiate a new Application:

1. The virtualization layer verifies the virtual instance.
2. Virtualized RoT (vRoT) measures the Application. The vRoT is a virtual instance associated to the hardware protected RoT. The virtualization layer provides this virtual resource to the virtual instance.

Corresponding measurements are reported to the trust agent. The trust agent exposes the attestation results to authorized attestation server (could be within the SMO) so that it verifies collected measurements against trust policies already defined by administrators.

C.2 Common Application Lifecycle Management

C.2.1 Software Package Protection

Potential controls on REQ-SEC-ALM-PKG-1 and REQ-SEC-ALM-PKG-4

Application packages need to be frequently tested throughout the lifecycle of the Application:

During Development	During on-boarding and during instantiation	During Runtime
Vulnerability scanning Static Application Security Testing (SAST) Dynamic Application Security Testing (DAST) Penetration testing Software composition analysis Testing to be performed frequently for vulnerability scanning or misconfiguration on Application packages. EXAMPLE: To check for malware or secrets stored in package. **Responsible:** Application Provider	Vulnerability scanning Dynamic Application Security testing (DAST) to be performed for: • Certifying the Application for functionality as well as authenticity, integrity, and packaging compliance. • Blocking deployments if the package does not comply with the Service Provider security policies • For scanning and detecting potential vulnerabilities • Checking for malware • Scanning for unnecessary system tools and libraries not required by Application • Software composition analysis **Responsible:** Application Provider, Service Provider	Perform continuous scanning/monitoring for known vulnerability or misconfiguration on runtime workloads, check for any open ports, VM/Container escape. **Responsible:** Service Provider

Tools used for static code and dynamic security analysis, analysis of code being released, and penetration test results must be shared with the Service Provider.

Annex D (informative): Change history

Date	Revision	Description
2024.03.20	09.00	AT&T.AO: Correct usages of "Must"
2024.03.20	09.00	Ericsson: Update NFO and FOCOM security requirements and controls
2024.03.20	09.00	Ericsson: Add Shared O-RU Security Requirements
2024.03.20	09.00	Keysight.AO: Added unexpected input management requirements for S-Plane and C-Plane
2024.03.20	09.00	MITRE: Resolve duplicate requirement reference IDs in SLM section
2024.03.20	09.00	MITRE: SRS Typos in SLM Reqs
2024.03.20	09.00	NEC.AO: Removal of Requirement REQ-SEC-DEL-1, REQ-CTL-DEL-1, REQ-CTL-DEL-2
2024.03.20	09.00	NOKIA.AO: Security requirements for PSK/Refnum based certificate enrolment
2024.03.20	09.00	NOKIA.AO: Security requirements for vendor root CA certificate renewal for PNFs
2024.03.20	09.00	NOKIA.AO: Security requirements for Certificate Renewal procedure for PNFs, CNFs and VNFs
2024.03.20	09.00	NOKIA.AO: Security requirements for vendor certificate based certificate initial enrolment for PNFs
2024.03.20	09.00	Rakuten Symphony: Correction to 802.1X security control clause
2024.03.20	09.00	WG11.AO: New requirement for the support of CMPv2 by VNF/CNF
2024.03.20	09.00	WG11.AO: Update of O-Cloud controls on secure storage
2024.03.20	09.00	WG11: New requirements focusing on O-Cloud SW images verification, vulnerability scanning and secure update
2023.11.06	08.00	Ericsson: Update the outdated reference of 3GPP references in Clause 2 and Annex B
2023.11.06	08.00	Ericsson: Editorial update in Clause 5.1.2.2 Security Controls
2023.11.06	08.00	Ericsson: Proposed changes in Clause 5.3.2 Common Application Lifecycle Management
2023.11.06	08.00	MITRE: New requirements on rAppIDs
2023.11.06	08.00	MITRE: New requirement on App decommissioning
2023.11.06	08.00	MITRE: Duplicate Account and Identity Security Event Log Requirement.
2023.11.06	08.00	NIST: SecRecSpec-O1-Interface-Modification
2023.11.06	08.00	NOKIA.AO: Near-RT RIC Secure mechanisms for Y1 interface
2023.11.06	08.00	NOKIA: Security requirements and controls for xApp registration procedure
2023.11.06	08.00	NOKIA: Security requirements for preventing tampering of log data
2023.11.06	08.00	NOKIA: security requirements for prevention of (D)DoS to Security Log Data management
2023.11.06	08.00	NOKIA: Security requirements for prevention of (D)DoS to Security Log Data management
2023.11.06	08.00	NOKIA: Security Log data one-way access
2023.11.06	08.00	NOKIA: Near-RT RIC Secure mechanisms for E2 interface
2023.11.06	08.00	Rakuten Symphony: New security requirements and controls for NFO/FOCOM
2023.11.06	08.00	Rakuten Symphony: New security controls for DoS / DDoS mitigation requirement REQ-SEC-DOS-1
2023.11.06	08.00	Rakuten Symphony: New security control covering REQ-SEC-AAL-4
2023.11.06	08.00	Rakuten Symphony: New Security Control for User Management Requirements for Cloud Platform Management
2023.11.06	08.00	WG11: New requirments on O-Cloud logging
2023.11.06	08.00	WG11: New requirements on O-Cloud instance ID
2023.11.06	08.00	WG11: New requirements on O-Cloud Time Synchronization
2023.07.12	07.00	AT&T.AO: Security Requirements specifications CMPv2
2023.07.12	07.00	AT&T.AO: Security Requirements specifications TA Provisoning
2023.07.12	07.00	Ericsson.AO: API Security Requirements
2023.07.12	07.00	Ericsson.AO: Update to informative SBOM statements
2023.07.12	07.00	Ericsson.AO: Revise Password requirements clause
2023.07.12	07.00	Ericsson: Shared O-RU Security Requirements and Security Controls
2023.07.12	07.00	Ericsson: Kafka Security Requirements
2023.07.12	07.00	Fujitsu.AO: Update Security requirements documents with secure deletion
2023.07.12	07.00	Fujitsu: Update Security requirements documents with secure decommissioning
2023.07.12	07.00	MITRE.AO: Common application package requirements
2023.07.12	07.00	MITRE: Security Log Management requirement for a standard security log format and security related log fields
2023.07.12	07.00	MITRE: Common application package security controls
2023.07.12	07.00	MITRE: Common application terminology
2023.07.12	07.00	MITRE: Security related activities and events to be logged
2023.07.12	07.00	MITRE: PART 2: Security related activities and events to be logged
2023.07.12	07.00	NOKIA: First security log management related requirements
2023.07.12	07.00	NOKIA: Near-RT RIC Secure mechanisms for A1 interface

Date	Revision	Description
2023.07.12	07.00	NOKIA: Security requirements for the Y1 interface
2023.07.12	07.00	NOKIA: Security requirements for storage and transfer of logs
2023.07.12	07.00	NOKIA: Security requirements on Trusted Environment for Cluster Node
2023.07.12	07.00	NOKIA: Security requirements on Trusted Environment for Log-data Repository
2023.07.12	07.00	NOKIA: Security Requirements for Log-data Lifecycle Management
2023.07.12	07.00	NOKIA: Security controls for the Y1 interface solution 1
2023.07.12	07.00	NOKIA: Security Requirements for Time stamps in Log-data
2023.07.12	07.00	NOKIA: Security requirements for Authenticated Time Stamping (Sol#5) and (Missing) Common Time Source (Sol#15)
2023.07.12	07.00	NOKIA: Security Requirements for Due Diligence and (Security) Log-Data Auditing (Sol#6)
2023.07.12	07.00	NOKIA: Security requirements for the support of syslog over tls
2023.07.12	07.00	Rakuten Symphony :Remove references to <running> and <candidate> datastores for NACM rules of O1 interface
2023.07.12	07.00	Rakuten Symphony: NACM group O1_software_management of O1 interface is applicable only for PNFs
2023.07.12	07.00	Rakuten Symphony.AO: New security requirements and controls for O-Cloud hardware
2023.07.12	07.00	Rakuten Symphony.AO: New security requirements and controls for O-Cloud Virtualization and Isolation
2023.07.12	07.00	Rakuten Symphony: ETSI PAS Adaption for O-RAN Security Requirement Specification
2023.07.12	07.00	Rakuten Symphony.AO: Rename the Security Requirement Specification document to include Security Controls
2023.07.12	07.00	Rakuten Symphony.AO: ETSI Adaptation and changes for the Near-RT RIC Section in the Security Requirement Specification
2023.07.12	07.00	Rakuten Symphony.AO: ETSI Adaptation and Changes for the Security Requirement Specification_Ocloud
2023.07.12	07.00	Rakuten Symphony: ETSI PAS Adaption for O-RAN Security Requirement Specification_Interfaces maintained by ORAN
2023.07.12	07.00	Rakuten Symphony: ETSI PAS Adaption for O-RAN Security Requirement Specification_Ph3_Section5.3_Transversal Requirements
2023.07.12	07.00	WG11: Update on the requirement REQ-SEC-DOS-1 against O-RAN DoS attacks
2023.07.12	07.00	WG11: Minor updates: VNF/CNF are replaced by Application, some reference have been updated
2023.03.21	06.00	Ericsson: Update format for references to O-RAN documents
2023.03.21	06.00	Ericsson: O-Cloud Management User Authentication and Authorization
2023.03.21	06.00	Ericsson: SMO Security Requirements and Security Controls
2023.03.21	06.00	Orange: New security requirements on AAL components
2023.03.21	06.00	Orange: New security requirements on security descriptor
2023.03.21	06.00	Qualcomm Incorporated: Security requirements and controls for O-CU-CP/UP, O-DU, O-RU and O-eNB
2023.03.21	06.00	Orange: New security requirements on AAL interfaces
2023.03.21	06.00	MITRE: New security requirements on secure update for apps/VNFs/CNF
2023.03.21	06.00	Orange: New security requirements on the protection of O2 interface and O-Cloud notification APIs
2023.03.21	06.00	MITRE: Update SBOM requirements from AppLCMSec TR recommendation
2022.11.10	05.00	Tbd.
2022.07.20	04.00	Added/updated requirements and controls for: • O-Cloud Image Security • Non-RT RIC, rApps, and A1 and R1 Interfaces • Near-RT RIC
2022.03.23	03.00	Added/updated requirements and controls for: • Near-RT RIC and xApps • Open Fronthaul Interface - C, S and U Planes • Open Fronthaul Point-to-Point LAN Segment
2021.11.09	02.00	Added requirements for: • Open Fronthaul Point-to-Point LAN Segment • SBOM • Network Protocols and Services • Robustness of Common Transport Protocols • Robustness against Volumetric DDoS Attack • Robustness of OS and Applications • Password-Based Authentication
2021.07.01	01.00	Final initial version 01.00

Date	Revision	Description
2024.03.20	09.00	Published as Final version 09.00
2023.11.06	08.00	Published as Final version 08.00
2023.07.14	07.00	Published as Final version 07.00
2023.03.22	06.00	Published as Final version 06.00
2022.11.18	05.00	Published as Final version 05.00
2022.07.20	04.00	Published as Final version 04.00
2022.03.23	03.00	Published as Final version 03.00
2021.11.09	02.00	Published as Final version 02.00
2021.07.01	01.00	Published as Final version 01.00

History

Document history		
V9.1.0	June 2025	Publication