Indian Telecom Security Assurance Requirements (ITSAR)

भारतीय दूरसंचार सुरक्षा आश्वासन आवश्यकताएँ (भा.दू.सु.आ.आ.)

Open RAN (O-RAN) of 5G: RIC

Draft for comments

ITSAR Number: ITSAR30310YYMM
ITSAR Name: NCCS/ITSAR/Access Equipment/5G Access Equipment/Open RAN (O-RAN) of 5G - RIC-V1.0.0

Date of Release: DD.MM.YYYY
Date of Enforcement:

Version: 1.0.0

MTCTE के तहत जारी:
Issued under MTCTE by:

राष्ट्रीय संचार सुरक्षा केंद्र (रा.सं.सु.कें.)
दूरसंचार विभाग, संचार मंत्रालय
भारत सरकार
सिटी दूरभाष केंद्र, एसआर नगर, बैंगलोर-५६००२७, भारत
National Centre for Communication Security (NCCS)
Department of Telecommunications
Ministry of Communications
Government of India
City Telephone Exchange, SR Nagar, Bangalore-560027, India

About NCCS

National Centre for communication Security (NCCS), with headquarters at Bengaluru was set up in 2018 with the objective to establish and operationalize a framework of security testing and certification within the country. Security Assurance Standards (SAS) division of NCCS is mandated to prepare Telecom security requirements/standards called Indian Telecom Security Assurance Requirements (ITSAR) that addresses the country specific security needs in telecommunication landscape and notify the same.

Document History

Sr No.	Title	ITSAR No.	Version	Date of Release	Remark
1.	Open RAN (O-RAN) of 5G: RIC	**ITSAR30310YYMM**	1.0.0	DD.MM.YYYY	First Release

Table of Contents

A) Outline

Open RAN, or Open Radio Access Network is a cluster of 5G RAN as defined by O-RAN alliance. The O-RAN alliance defines split gNB network element as O-RU, O-DU and O-CU as part of O-RAN network. The objective of this document is to present a comprehensive, country-specific security requirements for deployment of O-RAN network elements resulting from exercising the suggested and supported functional split options for a gNB as specified in 3GPP and O-RAN alliance.

The specifications produced by various regional/international standardization bodies/organizations/ associations like 3GPP, O-RAN alliance, TSDSI along with the country-specific security requirements are the basis for this document.

This document commences with a brief description of various functional split options of O-RAN with emphasis on 3GPP and O-RAN alliance recommended, supported option and then proceeds to address the common security requirements and specific security requirements of O-RAN network elements.

B) Scope

This document targets on the security requirements of the 5G RAN Network Element i.e., O-RAN components as defined and explicitly supported by 3GPP/O-RAN alliance. The requirements specified here are binding on network equipment providers i.e OEMs (Original Equipment Manufacturers).

C) Conventions

1. Must or shall or required denotes the absolute requirement of a particular clause of ITSAR.
2. Must not or shall not denote absolute prohibition of a particular clause of ITSAR.
3. Should or Recommended denotes that the clause of ITSAR may be ignored under justifiable circumstances but after careful examination of its implications.
4. Should not or not Recommended denotes that that clause of ITSAR may not be ignored under justifiable circumstances but after careful examination of its implications.
5. In case of CSR, all the requirements are applicable to non-RT RIC, near RT RIC , SMO and O-Cloud unless otherwise stated. If only O-RAN is mentioned, then it refers to all O-RAN components.
6. The following protocol versions only shall be used:
    a. SSH – SSHv2;
    b. TLS – TLS 1.2 or higher;
    c. DTLS – DTLS 1.2;
    d. CMP – CMPv2;
    e. Oauth 2.0

Chapter 1: Overview

1.1 Introduction

The fifth generation of mobile technologies - 5G - is expected to connect people, things, data, applications, transport systems and cities in a smart networked communication environment. 5G is standardized by the 3rd Generation Partnership Project (3GPP) and the requirement framework for 5G are specified by ITU under IMT-2020. The usage scenario/use cases identified for 5G are i) enhanced Mobile BroadBand (eMBB) ii) massive Machine Type Communication (mMTC) and iii) Ultra Reliable and Low Latency Communications (URLLC).

The 5G deployment scenarios are better understood by a closer study of high-level RAN architectures and network topologies supported by 5G. Disaggregation of the base stations and separation of the control plane (CP) and user plane (UP) entities are the basic design principles of 5G RAN architecture. The basis of this could be tied to the evolving concepts of Disaggregated RAN or split gNB, C-RAN (Cloud RAN) and O-RAN. The Telecom Infra Project (TIP) and Small Cell Forum (SCF) are the other communities which focuses on the gNB split options and define the standards for the deployment and implementation. TIP is operator centric solutions. SCF drives the specification and standardisation of key elements of small cell technology including Iuh, FAPI, nFAPI, and the enhancement of X2 interface. These specification from SCF enable on open, multivendor platform and lower barrier to densification for all stakeholders.

The O-RAN inherits split option 7.2 mentioned in 3GPP 38.816 standards. Addition to that, O-RAN defines various deployment options for OAM architecture. This document discusses about O-RAN which defines following objective in the path of evolution.

- Leading the industry towards open, interoperable interfaces, RAN virtualization, Big Data and AI enabled RAN intelligence.
- Maximize the use of common-off-the-shelf hardware and minimizing the proprietary hardware.
- Specifying APIs and interfaces, driving standards to adopt them as open source wherever it is appropriate.
- The O-RAN architecture identifies the key functions and interfaces defined in O-RAN.
- Flexibility; multi vendor solutions enabling a diverse ecosystem for the operators to choose best of breed options for their 2G/3G/4G and 5G deployments.
- Innovation va adoption of New technologies (AI/ML etc.,)
- Supply Chain diversity.

The logical architecture of the O-RAN is shown below as per the specification Non-RT RIC Functional Architecture.

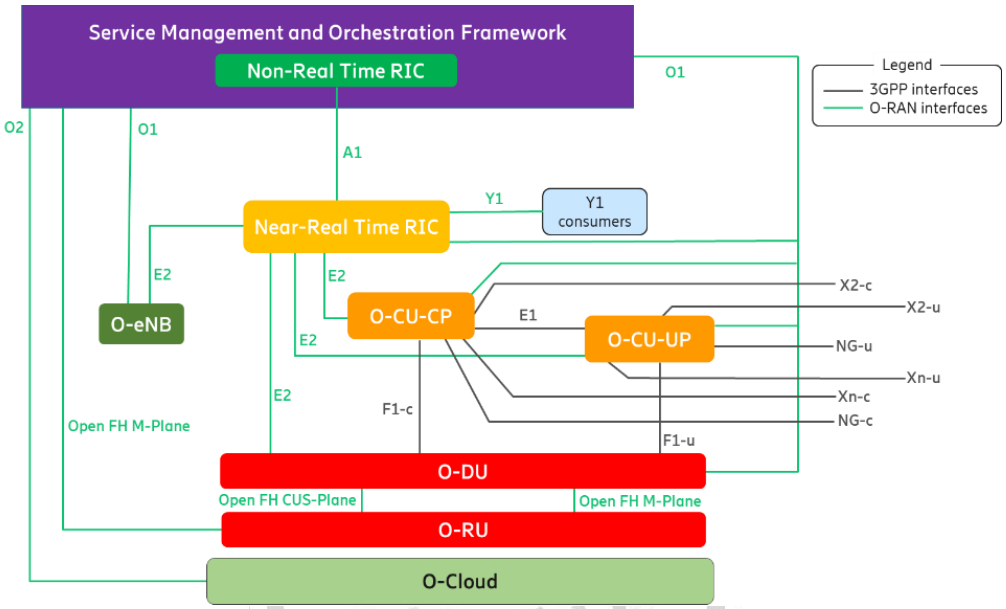

Figure 1: O-RAN Architecture and interfaces.
(Ref: O-RAN.WG2.Non-RT-RIC-ARCH-TR-v01.01, clause 2.1)

1.2 Security: As depicted in the above picture, it is important to secure every interface of the O-RAN Components and its interactions. This document will take an effort to identify all 3GPP and O-RAN interfaces specific to Service Management and Orchestration (SMO), non-real time RIC (rApps), Near Real Time RIC (xApps), Real Time RIC (between O-DU and O-RU) and O-Cloud (Cloud Computing Platform) and define security requirements for each component and interfaces. The Non-RT RIC architecture of the O-RAN is show below as per the specification Non-RT RIC Functional Architecture.

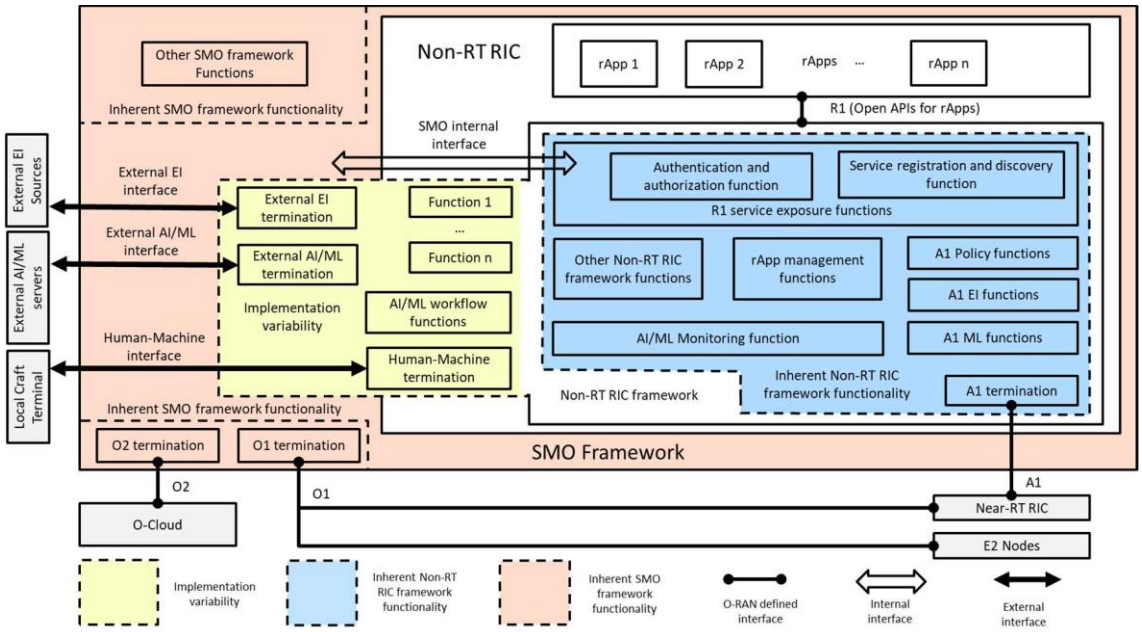

Figure 2: Non-RT RIC Architecture

(Ref: O-RAN.WG2.Non-RT-RIC-ARCH-TR-v01.01, clause 2.2)

The Near-RT RIC architecture of the O-RAN is show below as per the specification Near-RT RIC Architecture.

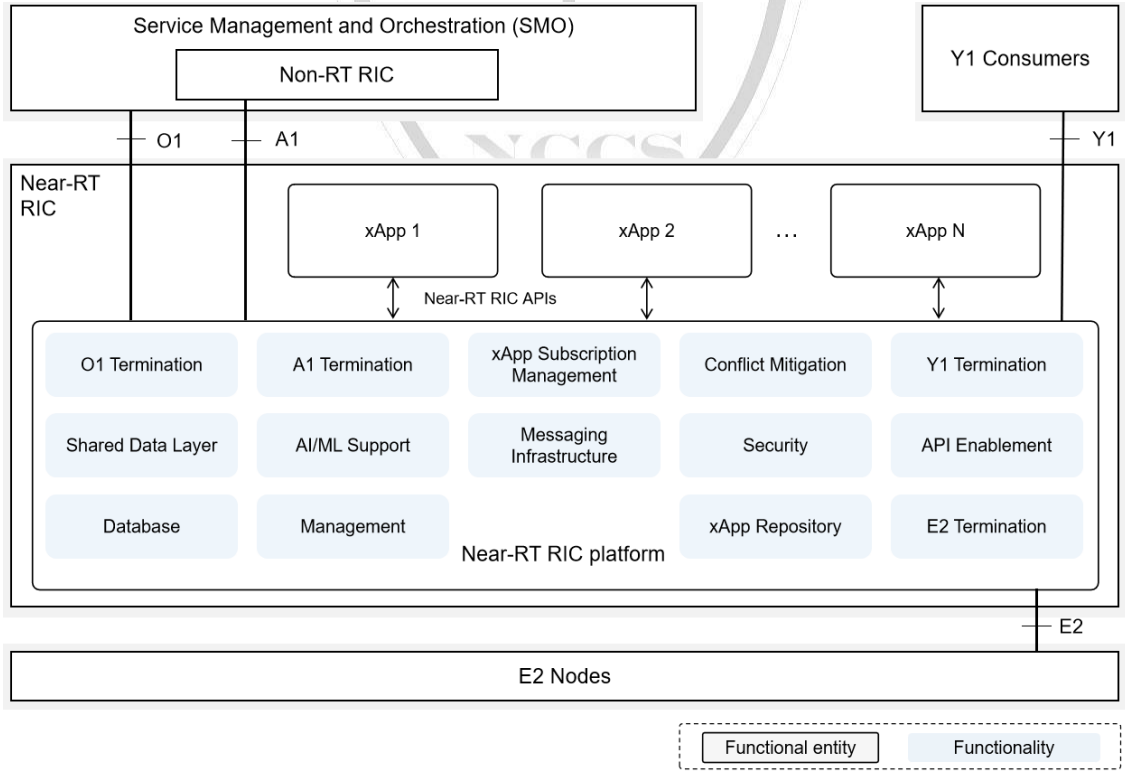

Figure 3: Near-RT RIC Architecture

(Ref: O-RAN.WG3.RICARCH-R003-v06.00, clause 6.1)

O-Cloud is the underlying cloud computing infrastructure that supports the virtualization and deployment of various O-RAN network functions. SMO is a critical component responsible for managing and Orchestrating the lifecyle of various services within an O-RAN network. RIC is a critical component that introduces a intelligence and automation into the management of O-RAN networks.

Interfaces defined by O-RAN besides the interfaces defined in 3GPP are:

- **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

Chapter 2: Common Security Requirements

Section 2.1: Access and Authorization

2.1.1 Management Protocols Mutual Authentication

Requirement:

The O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall support mutual authentication mechanisms, the mutual authentication mechanism can rely on the protocol used for the interface itself or other means.

Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" shall only be used for O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC management and maintenance.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section 4.2.3.4.4.1]

2.1.2 Management Traffic Protection

Requirement:

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC management traffic shall be protected strictly using secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section 4.2.3.2.4]

2.1.3 Role-based access control policy

Requirement:

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall support Role-Based Access Control (RBAC). A role-based access control system uses a set of controls that determines how users interact with domains and resources.

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). O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC supports RBAC with minimum of 3 user roles, in particular, for OAM privilege management for O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC Management and Maintenance, including authorization of the operation for configuration data and software via the network product console interface.

[Ref: TSDSI STD T1.3GPP 33.117- 17.2.0 V1.2.0. Section 4.2.3.4.6.2]

Note: The reference to Console interface may not be applicable here for Generalized Virtual Network Product (GVNP) Models of Type 1 & 2

2.1.4 User Authentication – Local/Remote

Requirement:

The various user and machine accounts on a O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall be protected from misuse. To this end, an authentication attribute is typically used, which, when combined with the username, 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 is not permitted. Exceptions are attributes that cannot be faked or spoofed by an attacker.

Minimum two of the above Authentication attributes shall be mandatorily combined for protecting all the accounts from misuse in public network environment. An exception to this requirement is local access and machine accounts where at least one authentication attribute shall be supported.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section 4.2.3.4.2.1]

2.1.5 Remote login restrictions for privileged users

Requirement:

Login to O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC as root or equivalent highest privileged user shall be limited to the system console only. Root user will not be allowed to login to O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC remotely.

This remote root user access restriction is also applicable to application software's / tools such as TeamViewer, desktop sharing which provide remote access to the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC.

[Reference TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section 4.3.2.6]

2.1.6 Authorization Policy

Requirement:

The authorizations for O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC 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.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section 4.2.3.4.6.1]

2.1.7 Unambiguous identification of the user & group accounts removal

Requirement:

Users shall be identified unambiguously by the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall support the assignment of individual accounts per user, where a user could be a person, or, for Machine Accounts, an application, or a system.

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall not enable the use of group accounts or group credentials or sharing of the same account between several users.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Sections 4.2.3.4.1.2]

Section 2.2: Authentication Attribute Management

2.2.1 Authentication Policy

Requirement:

In case of O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC the usage of a system function without successful authentication on basis of the user identity and at least two authentication attributes (e.g., password, certificate) in public network environment shall be prevented. For machine accounts and local access one authentication attribute will be sufficient. System functions comprise, for example network services (like SSHv2, 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.

Ref: TEC 25848:2022 TEC 25848:2022 TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section

4.2.3.4.1.1

2.2.2 Authentication Support – External

Requirement:

If the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC supports external authentication mechanism such as AAA server (for authentication, authorisation and accounting services), then the communication between O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC and the external authentication entity shall be protected using the authentication and related service protocols built strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

2.2.3 Protection against brute force and dictionary attacks

Requirement:

A protection against brute force and dictionary attacks that hinder authentication attribute guessing shall be implemented in O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC.

Brute force and dictionary attacks aim to use automated guessing to ascertain authentication attribute for user and machine accounts.

Various measures or a combination of the following measures can be taken to prevent this:

i. Using the timer delay (this delay could be the same or increased depending the operator's policy for each attempt) for each newly entered password input following an incorrect entry ("tar pit").
ii. Blocking an account following a specified number of incorrect attempts. 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.
iii. Using an authentication attribute blacklist to prevent vulnerable passwords.
iv. Using CAPTCHA to prevent automated attempts (often used for Web applications).

In order to achieve higher security, two or more of the measures indicated above shall be mandatorily supported by O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC.

An exception to this requirement is machine accounts.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section 4.2.3.4.3.3]

2.2.4 Enforce Strong Password

Requirement:

The configuration setting shall be such that a O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall only accept passwords that comply with the following complexity criteria:

i) Absolute minimum length of 8 characters (shorter lengths shall be rejected by the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC). It shall not be possible setting this absolute minimum length to a lower value by configuration.
ii) Password shall mandatorily comprise all the following four categories of characters:
    a. at least 1 uppercase character (A-Z)
    b. at least 1 lowercase character (a-z)
    c. at least 1 digit (0-9)
    d. at least 1 special character (e.g., @;!$.)
iii) The minimum length of characters in the passwords and the set of allowable special characters shall be configurable by the operator. The special characters may be categorized in sets according to their Unicode category.
iv) If a central system is used for user authentication password policy, then additional assurance shall be provided that the central system enforces the same password complexity rules as laid down for the local system in this sub-clause.
v) If a central system is not used for user authentication, the assurance on password complexity rules shall be performed on the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC.
vi) When a user is changing a password or entering a new password, O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC /central 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, etc.).

Password shall not be stored in clear text in the system; passwords shall be salted and hashed.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0 Section 4.2.3.4.3.1]

2.2.5 Inactive Session timeout

Requirement:

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.

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall monitor inactive sessions of administrative login users and initiate session locking mechanism based on user configurable timers. Unlocking the session shall be permissible only by authentication. If the inactivity period further continues for a defined period, Session /user ID time out must occur after this inactivity.

The timer values can be admin configurable as per requirement, normally set between 2 to 5 minutes.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section 4.2.3.5.2]

2.2.6 Password Changes

Requirement:

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 should be possible to implement this function on this system.

Password change shall be enforced after initial login.

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall enforce password change based on password management policy.

In particular, the system shall enforce password expiry. O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall support a configurable period for expiry of passwords.

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 minimum value shall be 3. This means that the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall store at least the three previously set passwords. The maximum number of passwords that the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC 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, etc.). An exception to this requirement is machine accounts.

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC to have in-built mechanism to support this requirement.

If a central system is used for user authentication password policy, then additional assurance shall be provided that the central system enforces the same password change policies as laid down for the local system in this subclause.

And if a central system is not used for user authentication, the assurance on password changes rules shall be performed on the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section 4.2.3.4.3.2]

2.2.7 Protected Authentication feedback

Requirement:

In case of O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC tThe Authentication attribute 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 "*".

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section 4.2.3.4.3.4]

2.2.8 Removal of predefined or default authentication attributes

Requirement:

In case of O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC Predefined or default authentication attributes shall be deleted or disabled.

Normally, authentication attributes such as password or cryptographic keys will be preconfigured from producer, OEM 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 OEM provides instructions on how to manually change it.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section 4.2.3.4.2.3]

2.2.9 Logout function

Requirement:

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 logout. The O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC 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.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section 4.2.3.5.1]

2.2.10 Policy regarding consecutive failed login attempts

Requirement:

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 the maximum number of failed user account login attempts shall be less than or equal to 8. 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 the capability to set the 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 the 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.

[Reference TSDSI STD T1.3GPP 33.117- 17.2.0 V1.2.0. Section 4.2.3.4.5]

2.2.11 Suspend accounts on non-use

Requirement:

It shall be possible for the system to automatically suspend an account after 'X' days without a valid login.

Note: X may be specified by operator. It can be implemented centrally also.

[Ref: CIS Password Policy Guide]

Section 2.3: Software Security

2.3.1 Source code security assurance

Requirement:

a) OEM shall follow best security practices including secure coding for software development. Source code shall be made available either at TSTL premises or at the mutually agreed location for source code review by the designated TSTL. It may be supported by furnishing the Software Test Document (STD).

b) Also, OEM shall submit the undertaking as below:
   i. Industry standard best practices of secure coding have been followed during the entire software development life cycle of the O-Cloud, SMO, Non-Real Time-RIC, and Near-Real Time RIC Software which includes OEM developed code, third party software and opensource code libraries used/embedded in the O-Cloud, SMO, Non-Real Time-RIC, and Near-Real Time RIC.
   ii. O-Cloud, SMO, Non-Real Time-RIC, and Near-Real Time RIC software shall be free from CWE top 25, OWASP top 10 and OWASP top10 API security weaknesses on the date of offer of product to designated TSTL for testing. For other security weaknesses, OEM shall give mitigation plan.

iii. The binaries for O-Cloud, SMO, Non-Real Time-RIC, and Near-Real Time RIC and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in bullet (ii) above.

Ref: 1. https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html

2. https://owasp.org/www-project-top-ten/

. https://owasp.org/www-project-api-security/]

2.3.2 Known Malware and backdoor Check

Requirement:

OEM shall submit an undertaking stating that O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC is free from all known malware and backdoors as on the date of offer of O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC to designated TSTL for testing and shall submit their internal Malware Test Document (MTD) of the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC to the designated TSTL.

2.3.3 No unused software

Requirement:

Software components or parts of software which are not needed for operation or functionality of the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall not be present/configured

Orphaned software components /packages shall not be present in O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC.

OEM shall provide the list of software that are necessary for O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC's operation.

In addition, OEM shall furnish an undertaking as "O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC does not contain Software that is not used in the functionality of O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC"

[Ref: TSDSI STD T1.3GPP 33.117 -17.2.0 V1.2.0, Section 4.3.2.3]

2.3.4 Unnecessary Services Removal

Requirement:

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall only run protocol handlers and services which are needed for its operation, and which do not have any known security vulnerabilities. By default, all other ports and services will be permanently disabled. O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC Shall not support following services

- FTP
- TFTP
- Telnet
- rlogin, RCP, RSH
- HTTP
- SNMPv1 and v2
- SSHv1 and v2
- TCP/UDP Small Servers (Echo, Chargen, Discard and Daytime)
- Finger
- BOOTP server
- Discovery protocols (CDP, LLDP)
- IP Identification Service (Identd)
- PAD
- MOP

Any other protocols, services that are vulnerable are also to be permanently disabled.

Full documentation of required protocols and services (communication matrix) of the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC and their purpose needs to be provided by the OEM as prerequisite for the test case.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section 4.3.2.1]

2.3.5 Restricting System Boot Source

Requirement:

The O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall boot only from the memory devices intended for this purpose.

[Reference– TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section- 4.2.3.3.2]

2.3.6 Secure Time Synchronization

Requirement:

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall use reliable time and date information provided through NTP/PTP server.O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall establish a secure communication channel through standard interface with the Network Time Protocol (NTP) / Precision Time Protocol (PTP) server as per appropriate TEC ER (essential requirement) document.

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall establish a secure communication channel strictly using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" with NTP/PTP server. O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall generate audit logs for all changes to time settings.

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall support NTPv4 or later version to ensure secure time synchronization.

Note: RFC 8915 which proposes Network Time Security (NTS) as an extension field for the NTP version 4 is also permitted.

2.3.7 Restricted reachability of services

Requirement:

The O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall restrict the reachability of services such that they can be reached only on interfaces meant for the purpose. On interfaces where services are active, the reachability should be limited to legitimate communication peers.

Administrative services (e.g. SSHv2, HTTPS, RDP) shall be restricted to interfaces in the management plane for separation of management traffic from user traffic.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0 Section 4.3.2.2]

2.3.8 Self Testing

Requirement:

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC's cryptographic module shall perform power-up self-tests and conditional self- tests to ensure that the module is functioning properly. Power-up self-tests shall be performed when the cryptographic module is powered up during System bootup/restart. Conditional self-tests shall be performed when an applicable security function or operation is invoked (i.e. security functions for which self-tests are required). If a cryptographic module fails a self-test, the module shall enter an error state and output an error indicator via the status output interface. The cryptographic module shall not perform any cryptographic operations while in an error state.

2.3.9 Common application lifecycle management – Package Protection

Requirement:

1. The Application package shall be certified by the Application Provider.
   Example: Software testing suites for certification include vulnerability scanning, static and dynamic testing, and penetration testing etc.
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.
3. The Application package shall include minimally the following artifacts: the Application software image, the signing certificate, and signature(s) of Application Provider.
4. Each Application package artifact shall be digitally signed individually by the Application Provider.

5. The SMO shall verify all Application package artifacts upon reception using the signatures generated and provided by the Application Provider.
6. The Application package shall be validated by SMO upon its reception using the signature generated and provided by the Application Provider
7. The Application package shall be tested by the Service Provider for known security vulnerabilities. All discovered vulnerabilities shall be reported to the Application Provider.
8. The Application Provider shall have a vulnerability management process in place allowing the Service Provider to report discovered vulnerabilities.
9. Vulnerabilities discovered in Application packages during testing by Service Provider shall be remediated by the Application Provider.
10. The Application package shall be cryptographically bound to one Service Provider before its onboarding to the images repository. This prevents an unauthorized package to be instantiated even if it has valid Application certificate.
11. Application packages stored within the images repository shall be protected in terms of integrity and confidentiality.
12. Application packages stored within the images repository shall be accessible to only authorized entities and over networks that enforce authentication, integrity, and confidentiality.
13. Images repository shall be clear of vulnerable Application packages and of packages with missing certificates.
14. Sensitive information used during the lifecycle of the Application shall be protected in terms of confidentiality at rest and in transit.
    Example: Sensitive information includes LI Applications, keys, PII, passwords and other critical configuration data.
15. 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
16. Application packages shall have a Change Log. All the changes in the Application package shall be versioned, tracked, and inventoried in the Change Log.
17. Application packages 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 and ETSI GS NFV-SOL004. *Option one;* 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. *Optoin two:* The complete Application package is signed with the Application Provider private key.
18. Algorithms, key sizes and standards to be used for signature generation/verification shall follow the "O-RAN Security Protocol Specification.
19. Sensitive artifacts shall be encrypted for confidentiality protection.

20. Algorithms, key sizes and standards to be used for encryption/decryption shall follow the "O-RAN Security Protocol Specification"
21. Application packages shall be compliant with ETSI NFV specifications, ETSI GS NFV-SOL004, ETSI GS NFV-IFA 011 and ETSI GS NFV-SEC 021 for package formats and signing/verification procedures
22. Encryption shall be used to secure cryptographic keys used by the cryptographic operations using Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.2.1]

2.3.10 Common application lifecycle management – Secure Update

Requirement:

- Application updates shall follow the same security requirements as Application packages.
- Applications should be updated with their latest security updates.
- Applications should be protected from downgrade attacks to older, possibly vulnerable, software versions.

Security updates for Application vulnerabilities should be available in a timely mannerfter discovery of known vulnerability or vulnerabilities for an Application.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.2.2]

2.3.11 Common application lifecycle management – Security descriptor

Requirement:

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
2. The Application descriptor shall support a description of the Service Availability Level (SAL) requirements for virtual resources on the underlying O-Cloud platform.
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.
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.
5. The Application shall support the ability to compare the current owned resource consumption with the defined resource quotas from the Application descriptor.

6. The Application shall send an alarm to the SMO if the current owned resource consumption and the defined resource quotas are inconsistent.
7. The comparing process between the current owned resource consumption and the defined resource quotas should be triggered periodically by the Application.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.2.3]

2.3.12 Common application lifecycle management – Secure deletion

Requirement:

1. Unwanted Application data shall be securely sanitized from all storage media devices.
2. Sensitive application data shall be securely sanitized using clearing as defined in NIST SP 800-88
3. Highly sensitive Application data shall be securely sanitized using purging as defined in NIST SP 800-88

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.2.4]

2.3.13 Common application lifecycle management – decommissioning of applications

Requirement:

- A complete post-decommission report documenting the performed tasks shall be generated.
- Legacy data and software should be archived.
- All trust artifact associated with an application shall be revoked at the time of decommissioning.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.2.5]

Section 2.4: System Secure Execution Environment

2.4.1 No unused functions

Requirement:

Unused functions i.e., the software and hardware functions which are not needed for operation or functionality of the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall be permanently deactivated in the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC's software and/or hardware.

The list of hardware and software functions installed in the system shall match with the ones that have been mentioned and deemed necessary for the operation of the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section 4.3.2.4]

2.4.2 No unsupported components

Requirement:

OEM to ensure that the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall not contain software and hardware components that are no longer supported by them or their 3rd Parties including the opensource communities, such as components that have reached end-of-life or end-of-support. An undertaking in this regard shall be given by OEM.[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section 4.3.2.5]

2.4.3 Avoidance of Unspecified mode of Access

Requirement:

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall not contain any wireless access mechanism which is unspecified or not declared.

An undertaking shall be given by the OEM as follows:

"The O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel"

Section 2.5: User Audit

2.5.1 Log management – Generic requirement

Requirement:

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

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.2]

2.5.2 Log management – security log data storage

Requirement:

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.
2. Any anomalies detected in log settings, configurations, and processes shall be logged.
3. The O-RAN Network Function(s), the O-cloud platform and infrastructure, and the SMO Framework shall create Security Log data.
4. Security Log data shall be created and maintained per App, per xApp, or per rApp.
5. The created and stored Security Log data shall provide all necessary information to deduce the root cause of a system behavior.

6. The Security Log data access management shall be protected with the help of the micro perimeter.
7. The access to Security Log data shall be authenticated and authorized.
8. Any change of access rights to Security Log data shall be logged.
9. Changing the access rights of security log data is only possible with privileged access rights.
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.
11. The Security Log data rotation process shall be configurable at regular time and when the maximum log size is reached.
12. The Security Log data process shall log any log rotation reconfiguration.
13. The system shall be capable of creating, processing, transmitting, and always storing all required security log events.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.3.1]

2.5.3 Log management – security log data in motion

Requirement:

1. The Security Log data in motion shall be protected with the help of the micro perimeter.
2. The Security Log data in motion shall be confidentiality, integrity and replay protected if this is going to leave the micro perimeter.
3. A mutual authentication shall be performed for any setup of a secure communication channel between at least two micro perimeters.
4. If a Security Log data integrity verification has failed, the Security Log data and a related failure notification shall be logged.
5. If a Security Log data appears outside of its expected receiving window, the Security Log data and the related notification shall be logged.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.3.2]

2.5.4 Log management – setup of a micro perimeter

Requirement:

- The Micro Perimeter shall support the secure storage of sensitive data.
- The Micro Perimeter shall support the execution of Security Log data sensitive functions, which are hosting the Log-Agent(s) and the Log-Collector.
- The Micro Perimeter shall support the execution of instantiated Application VNF's and Platform/Operating System level software.
- The Micro Perimeter's integrity shall be assured.
- 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.

- The Micro Perimeter shall support the deployment of software and the booting-up and execution of a single software instance or multiple software instances.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.3.3]

2.5.5 Log management – storage in log data repository

Requirement:

1. The Security Log data stored in the repository shall be protected with the help of the micro perimeter.
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.
3. Security Log data from different cluster node(s) shall be stored isolated from each other.
4. The Security Log data repository shall grant write only operation to cluster node(s).
5. Security Log data which are stored in the repository shall be confidentiality and integrity protected.
6. The Security Log data repository shall support attribute-based (ABAC) access management according to NIST SP800-162.
7. The Security Log data access management shall support operations for read, write, edit, delete, copy, execute and modify.
8. The access management ABAC mechanisms shall include the Subject Attributes, the Resource Objects Attributes, the Access Control Rules (policy), and the environmental conditions.
9. The Log data repository shall create and store Security Log data in a non-volatile memory.
10. Security Log data in use shall be protected with the help of the micro perimeter.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.4]

2.5.6 Log management – secure storage of security log data

Requirement:

1. Security log data shall be stored in a centralized location for easy management and analysis.
2. Security log data shall be stored in a tamper-proof manner to ensure their integrity and authenticity.
3. Retention policies for security log data shall be established to determine how long logs shall be kept.
4. Access to the log storage shall be restricted to authorized personnel only.
5. Access to the log storage shall be logged.
6. Backup of the log storage shall be performed regularly.

7. O-RAN elements shall be authorized to only send security log data to centralized log storage.
8. Centralized storage for security log data should be realized using centralized logging servers.
9. Tamper proof storage of security log data may be achieved through digital signature, encryption and hashing techniques.
10. The retention period should be based on legal, regulatory, and compliance requirements, as well as the organization's own policies.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.5]

2.5.7 Log management – secure transfer of security log data

Requirement:

1. Security log data shall be confidentiality- and integrity- protected during transfer to protect them from unauthorized access or tampering.
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.
3. Mechanisms shall be in place to ensure the integrity of the security log data during transfer.
4. The log transfer process shall be auditable to enable the tracking and identification of any unauthorized or suspicious log transfers.
5. An O-RAN component may support log streaming for security log events.
6. Digital signatures or hash based message authentication codes (HMAC) may be used to provide integrity protection of security log data.
7. O-RAN component may support the transport of Syslog over TLS1.2 for log streaming of security log events.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.6]

2.5.8 Log management – log format

Requirement:

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

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.7]

2.5.9 Log management – log fields

Requirement:

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.

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.
3. Security logs shall include the entity that is the cause of the security event for each log entry.
4. Security log should use the ISO 8601 date and time format.
5. Security log shall use IP addresses for the location field.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.8]

2.5.10 Log management – authenticated time stamping and missing time source

Requirement:

1. All network functions shall be synchronised to a common and authenticated time source.
2. Any successful as well as the unsuccessful synchronization to the common time source shall be logged.
3. The Security Log-data shall be time-stamped with the system time in case of unsuccessful synchronisation to a common time source.
4. The Security Log-data recording shall take place in the order in which the (security) log events occur.
5. The Security Log data shall contain a timestamp that includes a timezone.
6. The Network Time protocol version 4 shall be supported for the support of authenticated time stamping.
7. If NTPv4 authentication is in use, then AES-CMAC as specified by RFC4493 shall be supported. In this use case the NTP client can verify the integrity of the received NTP-packet.
8. If NTP security as specified by RFC5905 is in use for the integrity and replay protection of NTP-packets, then NTS as per RFC8915 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.
9. The Time Stamp representation should be in a standardized format, and the format in use should be logged. For reference to the formatting please refer to RFC 3339 and ISO 8601

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.9]

2.5.11 Log management – application system security event log

Requirement:

1. O-RAN Network Functions shall log any errors or exceptions generated.
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.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.11.4]

2.5.12 Log management – Data access security event log

Requirement:

1. O-RAN components shall log successful file additions, deletions, and unsuccessful attempts due to errors and authorization issues.
2. O-RAN components should log successful file reads and writes.
3. O-RAN components shall log unsuccessful attempts of file reads and writes due to errors and authorization issues.
4. O-RAN components shall log successful directory additions, deletions, and unsuccessful attempts due to errors and authorization issues.
5. O-RAN components shall log successful database or data store additions, deletions, and unsuccessful attempts due to errors and authorization issues.
6. O-RAN components should log successful database or data store reads and writes.
7. O-RAN components shall log unsuccessful attempts of database and data store reads and writes.
8. O-RAN components shall log permission changes to files, directories, databases, or data stores.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.11.5]

2.5.13 Log management –account and identity security event log

Requirement:

1. O-RAN components shall log account creation, modification, deletion, and unsuccessful attempts.
2. O-RAN components shall log changes to account privilege levels and unsuccessful attempts.
3. O-RAN components shall log successful group membership changes for accounts and unsuccessful change attempts.
4. O-RAN components shall log successful and unsuccessful authentication attempts for accounts.
5. O-RAN components shall log successful and unsuccessful authorization attempts to create a session or initiate a transaction.
6. O-RAN components shall log the termination of sessions or transactions.
7. O-RAN components shall log the occurrence of downgraded privileges or elevation of privileges for accounts.
8. O-RAN components shall log the termination of sessions.
9. O-RAN components shall log transactions successfully executed by accounts and unsuccessful attempts.
10. O-RAN components shall log requests that do not require an authenticated account.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.11.6]

2.5.14 Log management – general security event log

Requirement:

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).
2. O-RAN components shall log the use of administrative privileges.
3. O-RAN components shall log any change to a security-related configuration item, including a description of the configuration change.
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.
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.
6. O-RAN components shall log security patches submitted but not applied.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.11.7]

2.5.15 Log management – log data life cycle management

Requirement:

1. 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.
2. The Security Log data rotation process shall be configurable at regular time and when the maximum log size is reached.
3. The Security Log data process shall log any log rotation reconfiguration.
4. The system shall be capable of creating, processing, transmitting, and always storing all required security log events.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.12]

2.5.16 Log management – security log data policy

Requirement:

1. The archived Security Log data and their storage media shall be checked periodically to determine whether the Security Log data is accessible.
2. The archived Log data and their media shall be physically protected.
3. The personally identifiable information (PII) shall be removed from archived Security Log data.

4. The archived Security Log data shall be integrity and confidentiality protected.
5. 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 must not be filtered out.
6. The log policy shall include requirements for log generation, log transmission, store and disposal, and log analysis.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.13]

2.5.17 Log management – DDoS to Security Log Data.

Requirement:

1. The log management infrastructure should be designed to support typical and peak volume of log data to be processed per hour and day.
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.
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.
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.
5. The log management infrastructure should support mechanisms for log data redundancy.
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.
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.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.14]

2.5.18 Log management – Preventing Tampering of Log Data

Requirement:

1. The log management infrastructure should support access management for log data.
2. The log management infrastructure should support real time logging (log data streaming).
3. The log management infrastructure should support replication of log data.
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.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.15]

Section 2.6: Data Protection

2.6.1 Cryptographic Based Secure Communication

Requirements:

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall Communicate with the connected entities strictly using the secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

OEM shall submit to TSTL, the list of the connected entities with O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC and the method of secure communication with each entity with details of interface, protocol stack implemented, configuration, detailed procedure of establishing the communication with each entity and any other details required for verifying this requirement.

2.6.2 Cryptographic Module Security Assurance

Requirement:

Cryptographic module embedded inside the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-3 or later as prescribed by NIST standards.

Till further instructions, this clause will be considered 'complied' by submission of an undertaking by the OEM in specified format along with self-certified test reports.

An undertaking is to be submitted by the OEM mentioning that "Cryptographic module embedded inside the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-3 or later as prescribed by NIST standards".

[Ref: 1. ENISA Recommendation "Standardization in support of the cybersecurity certification", Dec 2019
2. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf]

2.6.3 Cryptographic Algorithms implementation Security Assurance

Requirement:

Cryptographic algorithm implemented inside the Crypto module of O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall be in compliance with the respective FIPS standards (for the specific crypto algorithm).

Till further instructions, this clause will be considered 'complied' by submission of an undertaking by the OEM in specified format along with self-certified test reports.
An undertaking is to be submitted by the OEM mentioning that "Cryptographic algorithm implemented inside the Crypto module of O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC is in compliance with the respective FIPS standards (for the specific crypto algorithm embedded inside the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC)"

[Ref: 1. ENISA Recommendation "Standardization in support of the cybersecurity certification", Dec 2019
2. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf]

2.6.4 Protecting data and information – Confidential System Internal Data

Requirement:

a) When O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC is in normal operational mode (i.e., not in maintenance mode) there shall be no system function that reveals confidential system internal data in the clear text to users and administrators.
b) Access to maintenance mode shall be restricted only to authorised privileged user.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section 4.2.3.2.2.]

2.6.5 Protecting data and information in storage

Requirement:

a) For sensitive data (persistent or temporary) in storage, read access rights shall be restricted. Sensitive files of O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC system that are needed for the functionality shall be protected against manipulation strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" with appropriate non-repudiation controls.
b) In addition, the following rules apply for:
   (i) Systems that need access to identification and authentication data in the clear/readable form e.g., in order to perform an activity/operation. Such systems shall not store this data in the clear/readable form, but scramble or encrypt it by implementation-specific means.
   (ii) Systems that do not need access to sensitive data in the clear. Such systems shall hash this sensitive data strictly using the cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.
   (iii) Stored files in the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC: Shall be protected against manipulation strictly using the NCCS approved Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0 Section 4.2.3.2.3]

2.6.6 Protection against Copy of Data

Requirement:

a) Without authentication, O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall not create a copy of data in use or data in transit.
b) Protective measures should exist against use of available system functions/software residing in O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC to create copyof data for illegal transmission.
c) The software functions, components in the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

2.6.7 Protection against Data Exfiltration - Overt Channel

Requirement**:**

a) O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit.
b) Establishment of outbound overt channels such as, HTTPS, IM, P2P, Email etc. are to be forbidden if they are auto-initiated by / auto-originated from the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC.
c) Session logs shall be generated for establishment of any session initiated by either user or O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC.

2.6.8 Protection against Data Exfiltration - Covert Channel

Requirement:

a) O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit.
b) Establishment of outbound covert channels and tunnels such as DNS Tunnel, HTTPS Tunnel, ICMP Tunnel, TLS1.2, SSL, SSHv2, IPSEC VPN, RTP Encapsulation etc. are to be forbidden if they are auto-initiated by / auto-originated from the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC.
c) Session logs shall be generated for establishment of any session initiated by either user or O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC system.

Section 2.7: Network Services

2.7.1 Traffic Filtering – Network Level

Requirement:

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall provide a mechanism to filter incoming IP packets on any IP interface(Refer to RFC 3871)
In particular the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall provide a mechanism:

To filter incoming IP packets on any IP interface at Network Layer and Transport Layer of the stack ISO/OSI.

(i) To allow specified actions to be taken when a filter rule matches. In particular at least the following actions should be supported:
   - Discard/Drop: the matching message is discarded; no subsequent rules are applied, and no answer is sent back.
   - 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.

(ii) To enable/disable for each rule the logging for Dropped packets, i.e., details on messages matching the rule for troubleshooting.

(iii) To filter on the basis of the value(s) of source IP, destination IP and port addresses of protocol header.

(iv) To reset the accounting.

(v) The O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall provide a mechanism to disable/enable each defined rule.

[Reference– 1. TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0 Section 4.2.6.2.1
2. RFC 3871 – Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure]

2.7.2 Traffic Separation

Requirement:

The O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall support the 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.

[Ref: 1. TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. section 4.3.5.1
2. RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure].

2.7.3 Traffic Protection –Anti-Spoofing:

Requirement:

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC 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.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. section 4.3.3.1.1]

Section 2.8: Attack Prevention Mechanisms

2.8.1 Network Level and application-level DDoS

Requirement:

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall have protection mechanism against Network level and Application-level DDoS attacks.

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC 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. In particular, partial or complete impairment of system availability shall be avoided. The O-RAN network element shall be able to return to its normal service level after the attack subsides.

Potential protective measures include:

- Restricting of available RAM per application
- Restricting of maximum sessions for a Web application
- Defining the maximum size of a dataset
- Restricting CPU resources per process
- Prioritizing processes
- Limiting of amount or size of transactions of a user or from an IP address in a specific time range
- Limiting of amount or size of transactions to an IP address/Port Address in a specific time range

The O-RAN element should be designed to incorporate redundant elements to achieve high availability. The vendors should provide robust support for these high availability features.

[Ref: 1. TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section 4.2.3.3.1,
2. ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.5]

2.8.2 Excessive Overload Protection

Requirement:

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall act in a predictable way if an overload situation cannot be prevented. O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC 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 O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC cannot reach an undefined and thus potentially insecure, state.

OEM shall provide a technical description of the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC's Overload Control mechanisms (especially whether these mechanisms rely on cooperation of other network elements e.g., RAN)

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section 4.2.3.3.3]

2.8.3 Interface robustness requirements

Requirement:

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall not be affected in its availability or robustness by incoming packets from other network elements 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 O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC. 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 ckets 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 to packets (i.e., packets which cannot be correlated to any request).
-
- [Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. section 4.2.6.2.2]

Section 2.9: Vulnerability Testing Requirements

2.9.1 Fuzzing – Network and Application Level

Requirement:

It shall be ensured that externally reachable services of O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC are reasonably robust when receiving unexpected input.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0 section 4.4.4]

2.9.2 Port Scanning

Requirement:

It shall be ensured that on all network interfaces of O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC, only documented ports on the transport layer respond to requests from outside the system.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. section 4.4.2]

2.9.3 Vulnerability Scanning

Requirement:

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.

The vulnerabilities found during the Vulnerability Scanning/Assessment process shall be remediated as below. For other than critical vulnerabilities, OEM shall provide a remediation plan.

Sr. No.	CVSS Score	Severity	Remediation
1	9.0 - 10.0	Critical	To be patched immediately
2	7.0 - 8.9	High	To be patched within a month
3	4.0 - 6.9	Medium	To be patched within three months
4	0.1 - 3.9	Low	To be patched within a year

Zero-day vulnerabilities shall be remediated immediately or as soon as possible.

[Ref: 1. https://nvd.nist.gov/vuln-metrics/cvss]
2. GSMA NG 133 Cloud Infrastructure Reference Architecture]
3. TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0 section 4.4.3]

Section 2.10: Operating System

2.10.1 Growing Content Handling

Requirement:

a) Growing or dynamic content shall not influence system functions.

b) A file system that reaches its maximum capacity shall lead to an event getting logged with appropriate message parameters and shall not stop O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC from operating properly. Therefore, countermeasures shall be taken to ensure that this scenario is avoided.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section 4.2.4.1.1.1]

2.10.2 Handling of ICMP

Requirement:

Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the O-Cloud, SMO, and Near-Real Time RIC.

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall not send certain ICMP types by default but it may support the option to enable utilization of these types which are marked as "Optional" in below table:

Type (IPv4)	Type (IPv6)	Description	Send	Respond to
0	128	Echo Reply	Permitted	N/A
3	1	Destination Unreachable	Permitted	N/A
8	129	Echo Request	Permitted	Optional
11	3	Time Exceeded	Optional	N/A
12	4	Parameter Problem	Permitted	N/A
N/A	2	Packet too Big	Permitted	N/A
N/A	135	Neighbor Solicitation	Permitted	Permitted
N/A	136	Neighbor Advertisement	Permitted	N/A

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall not respond to, or process (i.e., do changes to configuration) under any circumstances certain ICMP message types as marked in the below table.

Type (IPv4)	Type (IPv6)	Description	Send	Respond to	Process (i.e., do changes to configuration)
5	137	Redirect	N/A	N/A	Not Permitted
13	N/A	Timestamp	N/A	Not Permitted	N/A
14	N/A	Timestamp Reply	Not Permitted (i.e., as automatic reply to "Timestamp")	N/A	N/A
N/A	133	Router Solicitation	N/A	Not Permitted	Not Permitted
N/A	134	Router	N/A	N/A	Permitted

		Advertisement			

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section 4.2.4.1.1.2]

2.10.3 Authenticated Privilege Escalation only

Requirement:

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall not support a privilege escalation method in interactive sessions (both CLI and GUI) which allows a user to gain administrator/root privileges from another user account without re-authentication.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section 4.2.4.1.2.1]

2.10.4 System account identification

Requirement:

Each system account in O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall have a unique identification with appropriate non-repudiation controls.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V.1.2.0. Section 4.2.4.2.2]

2.10.5 OS Hardening - Minimized kernel network functions

Requirement:

In case of O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC 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:

1. IP Packet Forwarding between different interfaces of the network product.
2. Proxy ARP
3. Directed broadcast
4. IPv4 Multicast handling
5. Gratuitous ARP messages

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0 Section - 4.3.3.1.2]

2.10.6 No automatic launch of removable media

Requirement:

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall not automatically launch any application when a removable media device is connected.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section - 4.3.3.1.3]

2.10.7 Protection from buffer overflows

Requirement:

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC 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 by OEM.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0 Section - 4.3.3.1.5]

2.10.8 External file system mount restrictions

Requirement:

If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.

OS-level restrictions shall apply to normal users against mount / use of removable media devices (e.g., USB drive, CD ROM etc.) for data transfer.

[Reference– TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0 Section - 4.3. 3.1.6]

2.10.9 File-system Authorization privileges

Requirement:

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC 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.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0 Section - 4.3.2.7]

2.10.10 SYN Flood Prevention

Requirement:

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall support a mechanism to prevent Syn Flood attacks. This feature shall be enabled by default.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section - 4.3.3.1.4]

2.10.11 Handling of IP options and extensions

Requirement:

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.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. Section - 4.2.4.1.1.3]

2.10.12 Restrictions on running Scripts / Batch-processes

Requirement:

Scheduled tasks for carrying out the activities such as taking the backups, monitoring disk space and system maintenance activities shall be executed by the privileged user such as administrator only. Similarly, O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall have feature to restrict Scripts / Batch-processes / Macros usage among various users. It shall be possible to administratively configure scheduled tasks usage i.e. Cron-Job usage (permit / deny) among various users like Normal users, privileged users.

2.10.13 Restrictions on Soft-Restart

Requirement:

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall restrict software-based system restart options usage among various users. The software reset / restart either through command or use of key-combinations like CTRL+ALT+DEL is not available to normal users for prevention of unintended / malicious trigger of system reset / restart.

2.10.14 Robustness of OS and applications

Requirement:

Known vulnerabilities in the OS and applications of an O-RAN component shall be clearly identified

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.6]

Section 2.11: Web Servers

This entire section of the security requirements is applicable if the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC supports **web management interface.**

2.11.1 HTTPS

Requirement:

The communication between Web client and Web server shall be protected strictly using the Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)” only

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. section 4.2.5.1]

2.11.2 Webserver logging

Requirement:

Access to the O-RAN Components webserver (for both successful as well as failed attempts) shall be logged by O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC.

The web server log shall contain the following information:

- Access timestamp
- Source (IP address)
- Account (if known)
- 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

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. section 4.2.5.2]

2.11.3 HTTPS input validation

Requirement:

The O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks.

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC 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.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. section 4.2.5.4]

2.11.4 No system privileges

Requirement:

No O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC web server processes shall run with system privileges.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. section 4.3.4.2]

2.11.5 No unused HTTPS methods

Requirement:

HTTPS methods that are not required for O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC operation shall be deactivated.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0 section 4.3.4.3]

2.11.6 No unused add-ons

Requirement:

All optional add-ons and components of the web server shall be deactivated if they are not required for O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC operation.

In particular, CGI or other scripting components, Server Side Includes (SSI), and WebDAV shall be deactivated if they are not required.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. section 4.3.4.4]

2.11.7 No compiler, interpreter, or shell via CGI or other server-side scripting

Requirement:

If CGI (Common Gateway Interface) or other scripting technology is used, the CGI directory or other corresponding scripting directory shall not include compilers or interpreters.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. section 4.3.4.5]

2.11.8 No CGI or other scripting for uploads

Requirement:

If CGI or other scripting technology is used, the associated CGI/script directory shall not be used for uploads.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. section 4.3.4.6]

2.11.9 No execution of system commands with SSI

Requirement:

If Server Side Includes (SSI) is active, the execution of system commands shall be deactivated.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. section 4.3.4.7]

2.11.10 Access rights for web server configuration

Requirement:

Access rights for O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0 section 4.3.4.8]

2.11.11 No default content

Requirement:

Default content that is provided with the standard installation of the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC web server shall be removed.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. section 4.3.4.9]

2.11.12 No directory listings

Requirement:

Directory listings (indexing) / "Directory browsing" shall be deactivated.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. section 4.3.4.10]

2.11.13 Web server information in HTTPS headers

Requirement:

The HTTPS header shall not include information on the version of the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC web server and the modules/add-ons used.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. section 4.3.4.11]

2.11.14 Web server information in error pages

Requirement:

User-defined error pages and Error messages shall not include version information and other internal information about the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC web server, and the modules/add-ons used.

Default error pages of the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC web server shall be replaced by error pages defined by the OEM.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. section 4.3.4.12]

2.11.15 Minimized file type mappings

Requirement:

File type or script-mappings that are not required for O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC operation shall be deleted.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. section 4.3.4.13]

2.11.16 Restricted file access

Requirement:

Restrictive access rights shall be assigned to all files which are directly or indirectly reside in the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC web server's document directory.

In particular, the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC web server shall not be able to access files which are not meant to be delivered.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0 section 4.3.4.14]

2.11.17 Execute rights exclusive for CGI/Scripting directory

Requirement:

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.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. section 4.3.4.15]

2.11.18 HTTP User session

Requirement:

To protect user sessions, O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC 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, etc.).
4. In addition to the Session Idle Timeout, O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC 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 IDs shall be regenerated for each new session (e.g., each time a user logs in).
6. The O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC 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.
7. Where session cookies are used the attribute 'HTTP Only' shall be set to true.
8. Where session cookies are used the 'domain' attribute shall be set to ensure that the cookie can only be sent to the specified domain.
9. 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.
10. The O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall not accept session identifiers from GET/POST variables.
11. The O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall be configured to only accept server generated session ID.

[Ref: TSDSI STD T1.3GPP 33.117-17.2.0 V1.2.0. section 4.2.5.3]

2.11.19 Application Programming Interfaces

Requirement:

1. APIs used in O-RAN to access an internal or external data source shall perform object-level authorization checks.

2. O-RAN endpoints using APIs shall support certificate-based authentication.
3. O-RAN endpoints using APIs shall support password-based authentication that is a factor used in multi-factor authentication (MFA). Password-based single-factor authentication should not be used.
4. O-RAN endpoints using APIs should provide strong authorization.
5. O-RAN endpoints using APIs shall validate the authenticity of tokens. Unsigned JWT tokens shall not be accepted.
6. O-RAN endpoints shall validate API client requests to return sensitive data.
7. APIs used in O-RAN shall have confidentiality and integrity protection for data-in-transit.
8. APIs used in O-RAN shall implement a schema-based validation mechanism to enforce returned data.
9. APIs used in O-RAN shall impose a restriction on the size and number of resources that a client requests.
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.
11. APIs used in O-RAN shall default-deny properties that should not be accessed by clients.
12. APIs used in O-RAN shall only be accessed by valid HTTP verbs. All other HTTP verbs should be disabled.
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.
14. APIs used in O-RAN shall limit the number of returned records to prevent mass disclosure in case of injection.
15. APIs used in O-RAN shall log all failed authentication attempts, denied access, and input validation errors.
16. API client and server shall support mTLS 1.2, or higher, for mutual authentication.
17. API server shall support OAuth 2.0 resource server functionality, for service requests received from API clients.
18. API server shall support OAuth 2.0 resource owner functionality, for service requests received from API clients.
19. API client shall support OAuth 2.0 client functionality, for each service request.
20. API client and server shall support TLS 1.2, or higher, for protection of data-in-transit.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.10.2]

Section 2.12: Other Security requirements

2.12.1 Remote Diagnostic Procedure – Verification

Requirement:

If the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC is providing remote access for troubleshooting purposes/alarm maintenance then it shall be allowed only for authorized users, other than the root user.

All activities performed by the remote user are to be logged with the following parameters:

1. User id
2. Time stamp
3. Interface type
4. Event level (e.g., CRITICAL, MAJOR, MINOR)
5. Command/activity performed and
6. Result type (e.g., SUCCESS, FAILURE).
7. IP Address of remote machine

2.12.2 No System Password Recovery

Requirement:

No provision shall exist for O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC System / Root password recovery.

[Ref: GSMA NG 133: GSM Association Non-confidential Official Document NG.133 - Cloud Infrastructure Reference Architecture managed by OpenStack section 2.2.7.7]

2.12.3 Secure System Software Revocation

Requirement:

Once the O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC software image is legally updated/upgraded with New Software Image, it should not be possible to roll back to a previous software image.

In case roll back is essential, it shall be done only by the administrator with appropriate non-repudiation controls.

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall support a well-established control mechanism for rolling back to previous software image.

2.12.4 Software Integrity Check –Installation

Requirement:

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall validate the software package integrity before the installation/upgrade stage strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for ITSAR" only.

Tampered software shall not be executed or installed if integrity check fails.
[Ref: TSDSI STD T1. TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.3.5]

2.12.5 Software Integrity Check – Boot

Requirement:

The O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall verify the integrity of a software component by comparing the result of a measurement of the component, typically a standard cryptographic hash generated strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for ITSAR" to the expected reference value.

2.12.6 Unused Physical and Logical Interfaces Disabling

Requirement:

O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall support the mechanism to verify both the physical and logical interfaces exist in the product.

Physical and logical accessible interfaces (except console interface) which are not under use shall be disabled so that they remain inactive even in the event of reboot.

2.12.7 No Default ProfileRequirement:

Predefined or default user accounts (other than Admin/Root) in O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC shall be deleted or disabled.

2.12.8 Certification management

Requirement:

An O-RAN PNF requiring a PKI certificate shall support CMPv2 as specified in O-RAN Security Protocols Specification

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.9.1]

2.12.9 Trust anchor provisioning

Requirement:

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.

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.
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.
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.
5. An O-RAN PNF must log an event for each trust anchor provisioning operation.
6. An O-RAN PNF shall support CMPv2, for trust anchor provisioning.
7. An O-RAN PNF may support voucher-based protocols to enable an O-RAN function to be securely provisioned with a new trust anchor.
8. An O-RAN PNF may support BRSKI for trust anchor provisioning.
9. An O-RAN PNF may support SZTP for trust anchor provisioning.
10. An O-RAN PNF may support 3GPP SCS for download of initial security configuration.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.11.1]

2.12.10 SBOM

Requirement:

1. 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.
2. SBOM depth shall be provided to second-level for any used open source software.
3. The SBOM shall be provided in Software Package Data eXchange (SPDX), CycloneDX, or Software Identification (SWID) format.
4. For integrity, a hash shall be generated for the SBOM, as specified in O-RAN Security Protocols Specification-R003-v08.00, clause 5.
5. For authenticity, a digital signature shall be provided for the SBOM, as specified in O-RAN Security Protocols Specification-R003-v08.00, clause 5.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 6.3]

Chapter 3: Specific Security Requirements

Section 3.1: O-Cloud

3.1.1 O-Cloud generic requirements.

Requirement:

1. Users shall be authenticated.
2. Users shall be authorized. O-Cloud platform shall use an authorization mechanism to control the access rights of users.
3. Means of isolation of control and resources among different users shall be implemented.
4. O-Cloud platform should support access management to O-Cloud resources based on RBAC (Role-based access control) policies.
5. O-Cloud platform shall support Multi-Factor Authentication (MFA) to ensure secure access.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.8.1]

3.1.2 O-Cloud software package protection for network functions and application layer

Requirement:

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.
2. O-Cloud Platform shall verify the integrity of Application package during instantiation to determine if any unauthorized modification, deletion, or insertion has occurred.
3. SMO and O-Cloud Platform shall support algorithms for the code signing and encryption/decryption processes and protection of keys.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.8.2]

3.1.3 O-Cloud virtualization and isolation.

Requirement:

1. O-Cloud shall implement means of preventing privilege escalation by Applications.
2. The communication between the different Applications shall be mutually authenticated and authorized.
3. 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.
4. Communication between O-Cloud platform software components shall be protected in terms of authenticity, confidentiality, integrity, and anti-replay.

5. The O-Cloud platform shall provide the capability to define network policies that restrict ingress and egress traffic and configure rate limiting between Applications.
6. The O-Cloud platform shall not permit configuration change of any component on the O-Cloud platform without proper authorization.
7. For mutual authentication between O-Cloud platform software components, mTLS 1.2 shall be supported as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2.
8. For confidentiality and integrity protection of data in transit, O-Cloud platform software components shall support TLS 1.2 as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2.
9. 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.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.8.4]

3.1.4 O-Cloud Secure Update

Requirement:

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.
2. All O-Cloud software images shall be protected to ensure their integrity and authenticity.
3. In case of an incomplete update, or incident during the installation process, the O-Cloud platform shall remain in its initial working state.
4. The O-Cloud platform shall prevent the unauthorized rollback of its software to an earlier vulnerable version.
5. The update of O-Cloud software should be completed with minimal disruption and downtime.
6. Algorithms, key sizes and standards to be used for signature generation/verification of the O-Cloud software images during the update process shall follow the O-RAN Security Protocol Specification-R003-v08.00 clause 5.
7. Before updating O-Cloud, all O-Cloud software images shall be validated by SMO upon their reception using signatures generated and provided by O-Cloud Software Providers.
8. The O-Cloud platform shall verify prior to the update process, the digital signature contained in the new O-Cloud software image.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.8.5]

3.1.5 O-Cloud Secure storage of cryptographic keys and sensitive data

Requirement:

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

2. The O-Cloud platform shall support a secure deletion method from both active and backup storage medias.
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.
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.
5. The O-Cloud shall support the capability for encryption of all sensitive data, including cryptographic keys, credentials, tokens, and configuration data.
6. 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.
7. Medias containing sensitive information shall be sanitized using media-specific techniques.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.8.6]

3.1.6 O-Cloud Chain of Trust

Requirement:

1. The O-Cloud platform shall support a root of trust that verifies the integrity of every relevant component in the O-Cloud platform.
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.
3. The chain of trust shall be built from measurements stored in a hardware root of trust.
4. 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.
5. 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. 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. The remote AS should be extended to include O-RAN Applications integrity.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.8.7]

3.1.7 O-Cloud hardware accelerator manager interface

Requirement:

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.
2. The hardware accelerator manager shall check whether O-Cloud IMS/DMS is authorized when O-Cloud IMS/DMS accesses the hardware accelerator manager.
3. AALI-C-Mgmt interface shall support confidentiality, integrity, and replay protection between the hardware accelerator manager and O-Cloud IMS/DMS.
4. AALI-C-Mgmt interface shall support TLS 1.2 as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2.
5. For mutual authentication between the hardware accelerator manager and O-Cloud IMS/DMS, AALI-C-Mgmt interface shall support mTLS 1.2 as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2.
6. AALI-C-Mgmt interface shall support authorization using OAuth 2.0, as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.7.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.8.8.1.1]

3.1.8 O-Cloud hardware accelerator manager vendor specific interface

Requirement:

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.
2. The hardware accelerator manager shall check whether the hardware accelerator device is authorized when the hardware accelerator manager accesses the hardware accelerator device.
3. The vendor specific interface shall support integrity between the hardware accelerator manager and the hardware accelerator device.
4. The vendor specific interface may support confidentiality and replay protection between the hardware accelerator manager and the hardware accelerator device.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.8.8.1.2]

3.1.9 O-Cloud hardware accelerator component

Requirement:

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.

2. The AAL Implementation shall clear memory prior to allocation or when indicated by the AAL Application on returning the memory.
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.
4. Hardware accelerators should be procured from vendors who can demonstrate the security of their supply chain and manufacturing processes (supply chain security).
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.
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
7. The clear memory mechanism shall 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.
8. Supply chain audit of hardware accelerator vendors shall be performed for establishing trust in vendor's supply chain management based on evidence presented

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.8.8.2]

3.1.10 O-Cloud notification API – DMS

Requirement:

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.
2. O-Cloud DMS shall be able to establish securely protected connection in terms of confidentiality, integrity and anti-replay with the SMO (NFO or any other entity using O2dms) over the O2dms interface.
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.
4. O-Cloud DMS shall log SMO's management operations for auditing.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.8.9.1.1]

3.1.11 O-Cloud notification API - IMS

Requirement:

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.
2. O-Cloud IMS shall be able to establish securely protected connection in terms of confidentiality, integrity and anti-replay with the SMO (FOCOM or any other entity using O2ims) over the O2ims interface.
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.
4. O-Cloud IMS shall log SMO's management operations for auditing.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.8.9.1.2]

3.1.12 O-Cloud notification API

Requirement:

1. The communication between Applications and the O-Cloud platform through the O-Cloud Notification API shall be mutually authenticated.
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.
3. For the security protection at the transport layer on O2 interface, TLS 1.2 shall be supported as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2.
4. 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-R003-v08.00, clause 4.7.
5. 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) 1.2 authentication via X.509v3 certificates as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.8.9.1.3, 5.1.8.9.2]

3.1.13 O-Cloud Hardware

Requirement:

O-Cloud hardware deployment shall be protected against unauthorized extraction or inference of sensitive information using physical methods.

O-Cloud hardware deployment refers to the hardware used to build the operator’s O-Cloud infrastructure.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.8.10.2]

3.1.14 O-Cloud Instance ID

Requirement:

1. The O-Cloud instance ID shall be globally unique within the O-Cloud platform to prevent conflicts and ensure accurate identification.
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.
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).
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.
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.
6. O-Cloud instance IDs shall be generated using strong randomization methods to ensure a high degree of uniqueness and minimize the likelihood of collisions.
7. O-Cloud should validate newly generated instance IDs against existing IDs to guarantee uniqueness before finalizing instance creation.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.8.10.2]

3.1.15 O-Cloud Time Synchronization

Requirement:

1. All O-Cloud nodes shall be configured to connect to a secure and authenticated time synchronization server for ToD synchronization.
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.
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.
   Timestamp refers to:
   a) **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.
   b) **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.
4. The O-Cloud shall guarantee that various instances of an identical application, irrespective of their location, generate logs with consistent timestamps.

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.
   This requirement ensures:
   a) **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.
   b) **Operational Consistency:** Ensures that scheduled tasks, backups, updates, or maintenance activities are executed consistently across the compute pool.
   c) **Data Integrity:** Provides consistency for applications and databases that rely on timestamps for transactions, ensuring no discrepancies due to time differences.
6. 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.
7. 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.
8. 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.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.8.10.2]

3.1.16 Network security event log

Requirement:

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.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.11.2]

3.1.17 General O-Cloud security event log

Requirement:

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.
2. O-Cloud shall log when maintenance activity is undertaken for host operating systems, hypervisors, and container engines.
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.

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.
5. O-Cloud shall log a security event when it detects unauthorized changes to the O-Cloud hardware resource configuration.
6. O-Cloud shall log a security event when it detects unauthorized changes to the Application configuration.
7. O-Cloud shall log a security event if driver signature verification fails.
8. 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.
9. O-Cloud shall log a security event if any hashes of driver files do not match their baseline values.
10. Baseline configurations for the hardware resource shall be established by the SMO, and regularly compared to the current state.
11. O-Cloud shall log a security event when it detects unauthorized deviation from the O-Cloud hardware resource configuration baseline.
12. Baseline configurations for each Application shall be established by the SMO, and regularly compared to the current state.
13. O-Cloud shall log a security event when it detects unauthorized deviation from the Application configuration baseline.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.11.3.1]

3.1.18 Hypervisor specific system security event log

Requirement:

1. O-Cloud shall log all changes to operating system configurations, hypervisor configurations, changes to virtualization settings, and changes to resource allocations.
2. O-Cloud shall log all hypervisor events related to attaching or detaching virtual disks.
3. O-Cloud shall log all hypervisor events related to creating, starting, stopping, restarting and deleting virtual machines.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.11.2]

3.1.19 Container engine specific system security event log

Requirement:

1. O-Cloud shall log all image repository events related to additions, modifications, and removal of images.

2. O-Cloud shall log all container engine events related to volume creation, deletion, and mounting.
3. O-Cloud shall log all container engine events related to creating, starting, stopping, restarting and deleting containers.

[Ref: O-RAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.3.8.11.3]

Section 3.2: SMO

3.2.1 SMO generic security requirements

Requirement:

1. SMO shall support authentication of SMO functions.
2. SMO shall support authentication of External Systems.
3. SMO functions shall support authorization as a resource owner/server and client for internal requests.
4. SMO shall support authorization of the service requests received from External Systems.
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.
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.
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
8. SMO shall support OAuth 2.0 authorization server and provide a token end-point, as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.7.
9. SMO shall support OAuth 2.0 resource owner/server, as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.7, for service requests received from other SMO functions.
10. SMO shall support OAuth 2.0 client functionality, as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.7, for service requests to other SMO functions.
11. SMO shall support mutual authentication of SMO functions using mTLS 1.2 with PKI X.509v3 certificates as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2.
12. SMO functions may support authentication of other SMO functions using TLS 1.2 with pre-shared key (PSK) as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.1.1.1, 5.1.1.2.1]

3.2.2 SMO Internal communications.

Requirement:

1. SMO internal communications shall support confidentiality, integrity and replay protection between SMO functions.
2. SMO internal communications shall support mutual authentication between between SMO functions.
3. For security protection at the transport layer, SMO Internal Communications shall support TLS 1.2 as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2.
4. For mutual authentication between SMO functions, SMO Internal Communications shall support mTLS 1.2 and specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2.
5. For authentication between SMO functions, SMO Internal Communications may support TLS 1.2 with pre-shared key (PSK), as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.1.1.2, 5.1.1.2.2]

3.2.3 SMO external interfaces

Requirement:

1. SMO external interfaces shall support integrity, confidentiality and replay protection over external interfaces.
2. SMO external interfaces shall support mutual authentication and authorization.
3. For confidentiality and integrity protection of data in transit, SMO External Interfaces shall support TLS 1.2 as specified in O-RAN Security Protocols Specifications, clause 4.2.
4. For mutual authentication between the SMO and External Source, SMO External Interfaces shall support mTLS 1.2 and specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2.
5. SMO External Interfaces shall support OAuth 2.0 resource owner/server, as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.7.
6. SMO External Interfaces shall support OAuth 2.0 client functionality, as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.7.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.1.1.3, 5.1.1.2.3]

3.2.4 SMO Logging

Requirement:

1. SMO shall support forwarding of event logs to a mutually authenticated remote location.
2. SMO shall support confidentiality and integrity protection over event logs transferred to a remote server
3. SMO shall support configuration settings that allow selection of remote servers to securely transfer the event logs.
4. SMO shall be capable of logging the event logs locally on itself.

5. SMO shall support confidentiality protection over event logs transferred to a remote server.
6. SMO shall support integrity protection over event logs transferred to a remote server.
7. SMO shall support access to event logs by authorized external services.
8. SMO shall be capable of forwarding event logs to an authorized remote location.
9. SMO shall be able to record all the security related log events.
10. SMO should be able to separate security logs from the system logs.
11. SMO shall not permit configuration change to logging levels of any component on the SMO system without appropriate authorization.
12. SMO shall support access to event logs by authorized internal services.
13. SMO External Interface used for SMO log export shall support TLS 1.2 as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2, and FTPES.
14. SMO log export may support SSHv2 as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.1, and SFTP.
15. SMO log export shall support mutual authentication using mTLS 1.2 with public key infrastructure (PKI) and X.509v3 certificates as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2.
16. When SSHv2 is supported for SMO log export, SSHv2 shall support authentication using public and private keys in a public key infrastructure (PKI).
17. When SSHv2 is supported for SMO log export, SSHv2 may support authentication using PKI and X.509v3 certificates.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.1.1.4, 5.1.1.2.4]

3.2.5 SMO NFO and FOCOM

Requirement:

1. User access to NFO and FOCOM shall provide authenticity, confidentiality, integrity, availability, and anti-replay.
2. NFO and FOCOM communication with other SMO components (such as OAM, Non-RT RIC components) shall provide authenticity, confidentiality, integrity, availability, and anti-replay.
3. NFO shall allow access to its services and O2dms interface to only authenticated and authorized service consumers.
4. FOCOM shall allow access to its services and O2ims interface to only authenticated and authorized service consumers.
5. NFO and FOCOM shall implement principle of least privileges for their service consumers.
6. NFO and FOCOM shall define the minimum and maximum resource limits for its micro services. The limits shall be specified for CPU, memory, and storage resources.
7. NFO and FOCOM shall define auto scaling thresholds for its micro services.

8. SMO may support OAuth 2.0 authorization server and provide a token end-point, as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.7.
9. SMO shall support OAuth 2.0 resource owner/server, as specified in O-RAN Security Protocols Specifications-R003-v08.00,clause 4.7, for service requests received from other SMO functions.
10. SMO shall support OAuth 2.0 client functionality, as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.7, for service requests to other SMO functions.
11. SMO shall support mutual authentication of SMO functions using mTLS with PKI X.509v3 certificates as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2.
12. SMO functions may support authentication of other SMO functions using TLS with pre-shared key (PSK) as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.1.1.5, 5.1.1.2.5]

3.2.6 O1 interface

Requirement:

1. ORAN O1 interface needs to be confidentiality, integrity and authenticity protected. Management service providers and consumers shall use TLS 1.2 specified in O-RAN security protocol specification R003-v08.00.
2. Management Service providers and consumers that use NETCONF SHALL support the Network Configuration Access Control Model (NACM) as specified in RFC 8341 to restrict NETCONF protocol access for users to a preconfigured subset of available NETCONF protocol operations and content.
3. 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
4. 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.

       a. **Mandatory** if the network device supports a local user store.

b. **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

5. Users assigned to the O1_nacm_management group SHALL have read and write permission for the /nacm objects and attributes.
6. Users assigned to the O1_user_management group SHALL have read and write permissions for the locally defined user store objects and attributes.
7. 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.
8. Users assigned to the O1_network_monitoring group SHALL have read permissions for the datastore. Users assigned to the O1_network_monitoring group SHALL NOT have read permissions for the /nacm objects.
9. Users assigned to the O1_software_management group SHALL have permissions to install new software on the PNF.
10. NETCONF endpoints SHALL support external user to group mapping via at least one of the following protocols: LDAP with Start TLS 1.2, OAuth 2.0, RADIUS with EAP, and TACACS/TACACS+.
11. Management Service providers MAY allow the definition of users in the <groups> NACM object.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.2.2]

3.2.7 O2 interface

Requirement:

1. O2 interface shall support confidentiality, integrity, replay protection and data origin authentication.
2. Management Service providers and consumers that use TLS 1.2 shall support TLS 1.2 as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.2.3]

Section 3.3: Non Real Time - RIC

3.3.1 Non RT-RIC and rApps

Requirement:

1. The Non-RT RIC shall support authorization as a resource owner/server and client.
2. The Non-RT RIC framework, as a resource owner/server, shall provide authorization to requests from rApps as a client.
3. rApps shall provide client authorization request to the Non-RT RIC framework
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.
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.
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.
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.
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.
9. rAppIDs shall be unique within the Non-RT RIC runtime environment.
10. rAppIDs shall be generated using strong randomization methods.
11. For A1-EI, Non-RT RIC shall support OAuth 2.0 resource owner/server, as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.7, for service requests received from one or more Near-RT RICs.
12. For A1-P, Non-RT RIC shall support OAuth 2.0 client, as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.7.
13. For R1, SMO/Non-RT RIC Framework may support TLS 1.2, as specified in O-RAN Security Protocols Specifications-R003-v08.00.
14. For R1, SMO/Non-RT RIC Framework shall support authorization using OAuth 2.0, as specified in O-RAN Security Protocols Specifications.
15. For R1, Non-RT RIC Framework shall support OAuth 2.0 resource owner/server functionality, as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.7.
16. For R1, rApps shall support OAuth 2.0 client functionality, as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.7.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.2.1, 5.1.2.2]

3.3.2 A1 interface

Requirement:

1. A1 interface shall support confidentiality, integrity, replay protection.
2. A1 interface shall support mutual authentication and authorization.

3. For the security protection at the transport layer on A1 interface, TLS 1.2 shall be supported as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2.
4. For the mutual authentication of the Non-RT RIC and one or more Near-RT RICs, the A1 interface shall support mTLS 1.2 and specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2.
5. The A1 interface shall support authorization using OAuth 2.0, as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.7.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.2.1]

3.3.3 R1 interface

Requirement:

1. R1 interface shall support confidentiality, integrity, and replay protection.
2. R1 interface shall support mutual authentication and authorization.
3. For the security protection at the transport layer on R1 interface, TLS 1.2 shall be supported as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2.
4. For the mutual authentication of the Non-RT RIC Framework and rApps, the R1 interface shall support mTLS 1.2 and specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2.
5. The R1 interface shall support authorization using OAuth 2.0, as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.7

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.2.6]

Section 3.4: Near RT RIC

3.4.1 Near-RT RIC and xApps

Requirement:

1. Near-RT RIC shall authenticate xApp access to the Near-RT RIC database(s) during SDL registration.
2. Near-RT RIC shall provide authorized access to Near-RT RIC database(s).
3. The communication between xApps and Near-RT RIC platform APIs shall be mutually authenticated.
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.
5. The Near-RT RIC shall support authorization as a resource owner/server (A1-P) and client (A1-EI).

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.
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
8. The Near-RT RIC shall be able to detect and defend against content-related attacks across the Y1 interface.
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.
10. During the xApp registration procedure the xApp identifier (xApp ID) shall be associated with xApp credentials used for authentication.
11. xApp IDs shall be created ensuring uniqueness.
12. Transactional APIs (REST and gRPC) shall support mutual TLS (mTLS) 1.2 authentication via X.509v3 certificates as specified in the O-RAN Security Protocols Specification-R003-v08.00, clause 4.2.
13. Time critical APIs, not supported by TLS 1.2 protocol, shall support IPsec with IKEv2 certificate-based authentication according to O-RAN security protocol specification-R003-v08.00.
14. 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-R003-v08.00, clause 4.7
15. For A1-P, Near-RT RIC shall support OAuth 2.0 resource owner/server, as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.7, for service requests received from a Non-RT RIC.
16. For A1-EI, Near-RT RIC shall support OAuth 2.0 client, as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.7
17. Transactional APIs (REST and gRPC) shall support TLS 1.2 as specified in the O-RAN Security Protocols Specification-R003-v08.00, clause 4.2 to provide message confidentiality and integrity
18. Time critical, not supported by TLS 1.2 protocol, shall support IPsec as specified in the O-RAN Security Protocols Specification-R003-v08.00, clause 4.5 to provide message confidentiality and integrity.
19. The Near-RT RIC shall verify policies received through the A1 interface as follows:
    a. The policies conform to a pre-defined schema.
    b. The policy values are valid.
    c. The policies are being received at or below a pre-defined rate.
20. The Near-RT RIC shall log security event(s) if any of the policy verification steps fail.
21. The Y1 interface shall support mutual TLS (mTLS) 1.2 authentication via X.509v3 certificates as specified in O-RAN Security Protocols Specifications-R003-v08.00, 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.

22. The Y1 interface shall support the OAuth 2.0 authorization framework as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.7. The roles defined in OAuth 2.0 shall be assigned as follows:
    a. Resource owner / Resource server (producer): Y1 provider
    b. Client (consumer): Y1 consumer
23. The Y1 interface shall support TLS 1.2 as specified in O-RAN Security Protocols Specifications-R003-v08.00, clause 4.2 to provide data confidentiality, integrity, and replay-protection.
24. The xApp ID shall be embedded into the provided xApp X.509 certificate used for authentication (mTLS 1.2) according to the parametrization in security protocol specification, issued by operator RA/CA PKI infrastructure.
25. 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).
26. 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.
27. The Near-RT RIC shall verify data received through the Y1 interface as follows:
    a. The data values are valid.
    b. The data is being received at or below a pre-defined message rate.

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

28. The Near-RT RIC shall log a security event each time an input validation step fails for data received through the Y1 interface. The Near-RT RIC shall verify data received through the E2 interface as follows:
    a. The data values are valid.
    b. The data is being received at or below a pre-defined rate.
    c. The Near-RT RIC shall log security event(s) if any of the verification steps fail.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.1.3.1, 5.1.3.2]

3.4.2 E2 interface

Requirement:

1. E2 interface shall support confidentiality, integrity, replay protection and data origin authentication.
2. For the security protection at the IP layer on E2 interface, IPsec shall be supported as specified in O-RAN Security Protocols Specifications clause 4.4.

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.2.4]

3.4.3 Y1 interface

Requirement:

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).
2. The Y1 provider shall authorize the Y1 consumer before allowing access to any service over the Y1 interface.
3. The Y1 interface shall provide mechanisms to provide confidentiality and integrity protection for all data exchanged.
4. The Y1 interface shall provide replay-protection for all data exchanged.
5. The Y1 interface shall enforce the result of the authentication for the duration of communications.
6. The Near-RT RIC shall hide its topology from the Y1 consumers accessing the Y1 interface

[Ref: ORAN.WG11.SeqReqSpecs.0-R003-v08.00, Section 5.2.7]

Annexure-I

Definitions

1. **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.
2. **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.
3. **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.
4. **Account and Identity Events:** Events generated by user identification and access control.
5. **Application descriptor:** A 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.
6. **Application Events:** Events generated by O-RAN Network Functions.
7. **Application package:** Software package of xApps, rApps, and VNFs/CNFs (i.e., O-CU, O-DU, and Near-RT RIC).
8. **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.
9. **Data Access Event:** Events generated by any O-RAN component accessing, retrieving, modifying or deleting data in files or databases.
10. **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.
11. **E2 Node:** a 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.
12. **Entity:** An individual (person), device, or process that interacts with an ORAN component.
13. **External Interface:** The interface between the SMO and an External System.
14. **External System:** A data source outside the O-RAN domain that provides enrichment data to the SMO.
15. **FCAPS:** Fault, Configuration, Accounting, Performance, Security.

16. **General Security Event:** Events generated by the enabling, disabling or configuration of security features in O-RAN components.
17. **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, clause 3.30.
18. **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, clause 3.31
19. **Intents:** A declarative policy to steer or guide the behavior of RAN functions, allowing the RAN function to calculate the optimal result to achieve stated objective.
20. **Isolation:** A 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.
21. **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.
22. **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.
23. **Management and Orchestration Event:** Events generated by SMO operations.
24. **Managed Element:** The definition of a Managed Element (ME) is given in 3GPP TS 28.622, Clause 4.3.3.
25. **Managed Function:** The definition of a Managed Function (MF) is given in 3GPP TS 28.622, Clause 4.3.4.
26. **Near-RT RIC:** O-RAN near-real-time RAN Intelligent Controller: a logical function that enables real-time control and optimization of RAN elements and resources via fine-grained data collection and actions over E2 interface.
27. **Near-RT RIC APIs:** A set of service-based interfaces that can be produced and consumed by the Near-RT RIC Platform and xApps.
28. **Near-RT RIC platform:** Platform supporting A1, E2, Y1 and O1 interfaces and providing a set of services via Near-RT RIC APIs needed for xApp functionality.
29. **Network Events:** Events generated by network activity from operating systems, hypervisors or container engines.
30. **Non-RT RIC:** O-RAN non-real-time RAN Intelligent Controller: a 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.
31. **Non-RT RIC Framework:** A functionality within the Non-RT RIC that logically terminates the A1 interface and provides support for rApps, including the R1 services through the R1 interface.
32. **NMS:** A Network Management System for the O-RU to support legacy Open Fronthaul M-Plane deployments

33. **O-CU:** O-RAN Central Unit: a logical node hosting O-CU-CP and O-CU-UP
34. **O-Cloud platform software component:** A 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. Some examples of O-Cloud platform software component include virtual machine managers, container orchestration frameworks (e.g., Kubernetes control plane) and database services.
35. **O-CU-CP: O-RAN Central Unit – Control Plane:** a logical node hosting the RRC and the control plane part of the PDCP protocol.
36. **O-CU-UP: O-RAN Central Unit – User Plane:** a logical node hosting the user plane part of the PDCP protocol and the SDAP protocol.
37. **O-DU: O-RAN Distributed Unit:** a logical node hosting RLC/MAC/High-PHY layers based on a lower layer functional split.
38. **O-RU: O-RAN Radio Unit:** a logical node hosting Low-PHY layer and RF processing based on a lower layer functional split.
39. **O2dms:** This interface is used for deploying and managing the O-Cloud.
40. **O2ims:** This interface is used for managing the infrastructure of the O-Cloud
41. **O-RAN vendor:** Provider of any component of O-RAN
42. **O1:** Interface between management entities (NMS/EMS/MANO) and O-RAN managed elements, for operation and management.
43. **O2:** Interface between SMO and the O-Cloud to provide cloud resources management and workload management for supporting O-RAN cloudified network functions.
44. **O-RAN vendor:** Provider of any component of O-RAN.
45. **Open Fronthaul M-Plane:** Management interface controlling the O-RU, generally driven from the O-DU but in the case of the hybrid topology also driven from the SMO.
46. **Personally Identifiable Information (PII):** is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.
47. **R1:** Interface between rApps and Non-RT RIC Framework via which R1 Services can be produced and consumed.
48. **R1 Services:** A 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.
49. **RAN:** Generally referred as Radio Access Network.
50. rApps: Non-RT RIC application: an application designed to consume and/or produce R1 services.
51. **Security Log:** A log that contains audit records and security-related system events.
52. **Service Management and Orchestration (SMO):** The O-RAN Service Management and Orchestration system as specified in the O-RAN Architecture Description (OAD) document, Clause 5.3.1.
53. **SMO External Interface:** The interface between the SMO and an SMO External System.
54. **SMO External System:** A data source outside the O-RAN domain that provides data to the SMO.
55. **SMO Functions (SMOFs):** Internal SMO entities which provide one or more SMO Services.

56. **SMO Service (SMOS):** Standardized cohesive set of management, orchestration and automation capabilities offered by an SMO Function.
57. **Shared Data Layer (SDL):** API for accessing shared data storage.Solution Provider: An application developer who delivers applications to Service Providers.
58. **Service Provider:** A network provider who is planning to deploy applications into their network.
59. **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.
60. **xApp:** An application consuming and/or producing Near-RT RIC services via the Near-RT RIC API to provide value added control of, or guidance to the E2 Nodes.
61. **Y1:** An interface between Near-RT RIC and Y1 consumers, as defined in O-RAN Architecture Description, clause 5.4.18. The interface enables RAN analytics information exposure from Near-RT RIC.
62. **Y1 consumers:** A role played by entities within or outside of the PLMN trust domain that consumes the Y1 services produced by the Near-RT RIC.

Annexure-II

Acronyms

AI/ML	-	Artificial Intelligence/Machine Learning
AAL	-	Acceleration Abstraction Layer
CNF	-	Cloud-native Network Function
DDoS	-	Distributed Denial of Service
DMS	-	Deployment Management Services
DTLS	-	Datagram Transport Layer Security
eNB	-	eNodeB (applies to LTE)
FOCOM	-	Front-Haul Control and Management
FOSS	-	Free and Open Source Software
FTP	-	File Transfer Protocol
FTPES	-	File Transfer Protocol Extension
gNB	-	gNodeB (applies to NR)
IMS	-	Infrastructure Management Services
IPSEC	-	Internet Protocol Security
MFA	-	Multi-Factor Authentication
mTLS	-	mutual Transport Layer Security
NETCONF	-	Network Configuration Protocol
NF	-	Network Function
NFO	-	Network Function Orchestration
O-CU	-	O-RAN Centralized Unit
O-DU	-	O-RAN Distributed Unit
O-RU	-	O-RAN Radio Unit
OSC	-	O-RAN Software Community
PDCP	-	Packet Data Convergence Protocol
PKI	-	Public Key Infrastructure
PNF	-	Physical Network Function
PSK	-	Pre-Shared Key
PTP	-	Precision Timing Protocol
RAN	-	Radio Access Network
RBAC	-	Role-based Access Control
REST	-	Representational State Transfer
RIC	-	RAN RAN Intelligent Controller
SBOM	-	Software Bill of Materials
SDL	-	Shared Data Layer
SFTP	-	Secure File Transfer Protocol
SMO	-	Service Management and Orchestration
SPDX	-	Software Package Data eXchange

	-	
SSH	-	Secure Shell
SWID	-	Software Identification
TLS	-	Transport Layer Security
VM	-	Virtual machine
VNF	-	Virtualised Network Function

Annexure-III

List of Submissions

List of Undertakings to be furnished by the OEM for O-Cloud, SMO, Non Real Time-RIC, and Near-Real Time RIC security Testing Submissions.

1. Source Code Security Assurance (against test case 2.3.1)
2. Known Malware and backdoor Check (against test case 2.3.2)
3. No unused Software (against test case 2.3.3)
4. No Unused Functions (against test case 2.4.1)
5. Avoidance of Unspecified mode of Access (against test case 2.4.3)
6. Cryptographic Module Security Assurance (against test case2.6.2)
7. Cryptographic Algorithms implementation Security Assurance (against test case 2.6.3)

Annexure-IV

References

1. 3GPP 33.117-17.2.0 V1.2.0: “Catalogue of General Security Assurance Requirements”.
2. O-RAN.WG11.SeqReqSpecs.0-R003-v08.00
3. O-RAN.WG11.SecProtSpecs-R003-v08.00
4. O-RAN.WG4.MP.0-R003-v13.00
5. O-RAN.WG2.Non-RT-RIC-ARCH-TR-v01.01
6. O-RAN.WG3.RICARCH-R003-v06.00
7. CIS_Benchmarks_Password_Policy_Guide_v21.12
8. https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html
9. https://owasp.org/www-project-top-ten/
10. https://owasp.org/www-project-api-security/
11. https://nvd.nist.gov/vuln-metrics/cvss
12. GSMA NG 133 Cloud Infrastructure Reference Architecture