O-RAN.WG11.SMO-Security-Analysis-TR.0-R003-v03.00

*Technical Report*

# O-RAN Working Group 11 (Security Working Group)

# Study on Security for Service Management and Orchestration (SMO)

O-RAN ALLIANCE e.V., Buschkauler Weg 27, 53347 Alfter, Germany

# Contents

# 1 Scope

This technical report provides the threat model and risk assessment for the SMO. The report identifies threats and risks and recommends potential security controls to protect against those threats through safeguards or mitigation.

The steps of the threat modelling process are as follows:

1. Identify assets: Identify the assets of the SMO that must be protected.
2. Identify threats: Identify the threats that could adversely impact the SMO and threats that can use the SMO to adversely impact other components of the O-RAN system.
3. Identify the attack surface and attack vectors: Identify the points in the SMO where an attacker could
    a. gain entry to the SMO
    b. gain entry to another O-RAN system through the SMO
    c. exploit a vulnerability or misconfiguration
    d. compromise the system or its data.
4. Measure risk: The extent to which confidentiality, integrity, or availability is threatened, based upon a risk-based analysis considering the impact level resulting from an attack and the likelihood of occurrence.
5. Recommend controls: The management, operational, and technical controls for an information system to protect the confidentiality, integrity and availability of the SMO and its information.

This Technical Report makes the following considerations:

- The attack surface of the SMO includes its interfaces, functions, and data. Data-at-rest, Data-in-motion, and Data-in-use must be considered.
- O-RAN Alliance WG1 is in the process of defining an architecture for a decoupled SMO. This will influence the set assets to be protected.
- The O-RAN Alliance is pursuing a zero-trust architecture (ZTA) for its specifications based upon NIST SP 800-207 [8]. This will affect the risk scoring.
- Security controls are recommended for specifications of the SMO. The recommended controls provided in this report will be shared with the responsible O-RAN Alliance working group, such as WG1 and WG10, so that the appropriate specification relevant to the recommendation can be updated.
- Some of the identified SMO assets may already be in scope for separate ongoing SFG security work items. The SMO security Technical Report work item may inform those work items.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

[1] O-RAN ALLIANCE PD: "O-RAN Document Drafting Rules (ODR)".

[2] O-RAN ALLIANCE TS: "O-RAN Architecture Description (OAD)".

[3] O-RAN ALLIANCE TS: "O-RAN Non-Real-Time RAN Intelligent Controller".

[4] O-RAN ALLIANCE TS: "O-RAN Security Protocols Specifications".

[5] O-RAN ALLIANCE TS: "O-RAN Security Requirements and Controls Specifications".

[6] O-RAN ALLIANCE TR: "O-RAN Threat Modelling and Risk Assessment".

[7] O-RAN ALLIANCE TS: "O-RAN Security Test Specifications".

[8] Zero Trust Architecture, NIST SP 800-207, NIST, August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final.

[9] US National Security Agency (NSA) / Cybersecurity and Infrastructure Security Agency (CISA), Security Guidance for 5G Cloud Infrastructures, Part I, Oct 28, 2021, Part II, Nov 18, 2021, Part III, Dec 2, 2021, Part IV, Dec 16, 2021. https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/smdpage11747/2/ (as of Feb 28, 2022).

[10] Not used.

[11] Not used.

[12] OWASP Top 10 Web Application Security Risks, 2021, https://owasp.org/www-project-top-ten/.

[13] Cloud Security Alliance (CSA), Top Threats to Cloud Computing: Egregious Eleven, 2019, https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven.

[14] Cloud Security Alliance (CSA), Top Threats to Cloud Computing: Pandemic Eleven, 2022, https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven.

[15] OWASP Top 10 Proactive Controls, 2021, https://owasp.org/projects/spotlight/historical/2021.02.10/

[16] Center for Internet Security (CIS) Critical Security Controls, https://www.cisecurity.org/controls/cis-controls-list

[17] Cloud Security Alliance (CSA) Cloud Control Matrix (CCM), https://cloudsecurityalliance.org/research/cloud-controls-matrix/

[18] ISO/IEC 27001:2013 Information Security Management System (ISMS).

[19] NIST SP 800-53r5, Security and Privacy Controls for Information Systems and Organizations, 2020.

[20] Technical Report (TR), Study on Security for Non-RT-RIC, O-RAN.SFG.Non-RT-RIC-Security-TR-v01.00

# 3 Definitions of terms, symbols, and abbreviations

## 3.1 Terms

This document uses the verbal forms for the expression of provisions as defined in O-RAN.TSC.Drafting-Rules.0-v01.00.

This document uses the term Zero Trust Architecture (ZTA) as defined by US NIST in [8] and applied to 5G cloud deployments by US CISA in [9].

A ZTA provides protection from external and internal threats, assuming the following:

1. there is no implicit trust granted to an asset based upon ownership, physical location, or network location [8]
2. the adversary is already inside the network. Perimeter defenses are no longer sufficient to secure a network, and there should always be an assumption that a threat actor has established a foothold in the network [9]

This document uses the term "attack surface" defined by US NIST as

> *The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment* [https://csrc.nist.gov/glossary/term/attack_surface]

This document refers to "sensitive information" defined by US NIST as

> *information whose loss, misuse, or unauthorized access or modification could adversely affect security* [https://csrc.nist.gov/glossary/term/sensitive]

For the purposes of the present document, the terms and definitions provided in [2]apply:

**A1**: Interface between non-RT RIC and Near-RT RIC to enable policy-driven guidance of Near-RT RIC applications/functions, and support AI/ML workflow.

**Near-RT RIC:** O-RAN Near-Real-Time RAN Intelligent Controller: A logical function that enables near-real-time control and optimization of RAN elements and resources via fine-grained data collection and actions over E2 interface. It may include AI/ML (Artificial Intelligence / Machine Learning) workflow including model training, inference and updates.

**Non-RT RIC:** O-RAN Non-Real-Time RAN Intelligent Controller: A logical function within SMO that drives the content carried across the A1 interface. It is comprised of the Non-RT RIC Framework and the Non-RT RIC Applications (rApps) whose functions are defined below.

**Non-RT RIC Applications (rApps):** Modular applications that leverage the functionality exposed via the Non-RT RIC Framework's R1 interface to provide added value services relative to RAN operation, such as driving the A1 interface, recommending values and actions that may be subsequently applied over the O1/O2 interface and generating "enrichment information" for the use of other rApps. The rApp functionality within the Non-RT RIC enables non-real-time control and optimization of RAN elements and resources and policy-based guidance to the applications/features in Near-RT RIC.

**Non-RT RIC Framework:** That functionality internal to the SMO that logically terminates the A1 interface to the Near-RT RIC and exposes to rApps, via its R1 interface, the set of internal SMO services needed for their runtime processing. The Non-RT RIC Framework functionality within the Non-RT RIC provides AI/ML workflow including model training, inference and updates needed for rApps.

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

**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.

**SMO:** Service Management and Orchestration system

## 3.2 Symbols

None

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 and the following apply:

| | |
|---|---|
| AI | Artificial Intelligence |
| CM | Configuration Management |
| DAR | Data at Rest |
| DIM | Data in Motion |
| DIU | Data in Use |
| DME | Data Management and Exposure |
| eNB | eNodeB (applies to LTE) |
| FM | Fault Management |
| FOCOM | Federated O-Cloud Orchestration and Management |
| FTP | File Transfer Protocol |
| FTPS | File Transfer Protocol Secure |
| gNB | gNodeB (applies to NR) |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| JSON | JavaScript Object Notation |
| KPI | Key Performance Indicator |
| KQI | Key Quality Indicator |
| ML | Machine Learning |
| MNO | Mobile Network Operator |
| NF | Network Function |
| NFO | Network Function Orchestrator |
| PII | Personally Identifiable Information |
| PKI | Public Key Infrastructure |
| PM | Performance Management |
| PTP | Precision Timing Protocol |
| RBAC | Role-based Access Control |

| | |
|---|---|
| REST | Representational State Transfer |
| RIC | RAN Intelligent Controller |
| RT | Real-Time |
| SBA | Service-Based Architecture |
| SME | Service Management and Exposure |
| SMO | Service Management and Orchestration |
| SMOF | SMO Functions |
| SMOS | SMO Services |
| SSH | Secure Shell |
| TCP | Transmission Control Protocol |
| TE&IE | Topology Exposure and Inventory Management |
| TLS | Transport Layer Security |
| ZTA | Zero Trust Architecture |

# 4 SMO Assets

## 4.1 Architecture

There are security risks with the SMO due to its internal functions and internal and external interfaces. Securing the SMO is imperative because it is responsible for all service management and orchestration. A security vulnerability within the SMO could be exploited to serve as an entry point for attacks against O-RAN components and lateral movement across O-RAN.

Figure 2.1-1 and Figure 2.1-2 show the service-based architectural view of the SMO including internal and external interfaces and the Non-RT-RIC. The Attack Surface of the SMO includes Functions, Interfaces, and Information, which each have assets that should be protected. Figure 2.1-3 is the SMO security architecture, based upon Figures 2.1-1 and 2.1-2. Figure 2.1-4 shows the evolution of the SMO to a Service-Based Architecture. and Figure 2.1-5 is the Decoupled SMO security architecture with support for RAN-Core Data Sharing. The following SMO assets need to be protected:

- SMO Framework
- SMO Functions (SMOF)
- Non-RT RIC
- SMO internal communications
- SMO Services (SMOS)
    - Service Management and Exposure (SME)
    - Data Management and Exposure (DME)
    - Topology Exposure and Inventory Management (TE&IM)
    - rApp Management
    - Network Function Orchestrator (NFO)
    - Federated O-Cloud Orchestration and Management (FOCOM)
    - RAN NF Fault Management (FM)
    - RAN NF Configuration Management (CM)
    - RAN NF Performance Management (PM)
    - A1 Enrichment Information Management
    - A1 Policy Management
    - SW Package Onboarding
    - Service Orchestration
    - Service Assurance
    - RAN Analytics

  - AI/ML Workflow

- SMOS Communications
- O1, O2, R1 and A1 interfaces
- Open Fronthaul M-Plane
- External interfaces
- User Management interfaces
- PKI
- Logging
- Data
- AI/ML models, algorithms, and methods

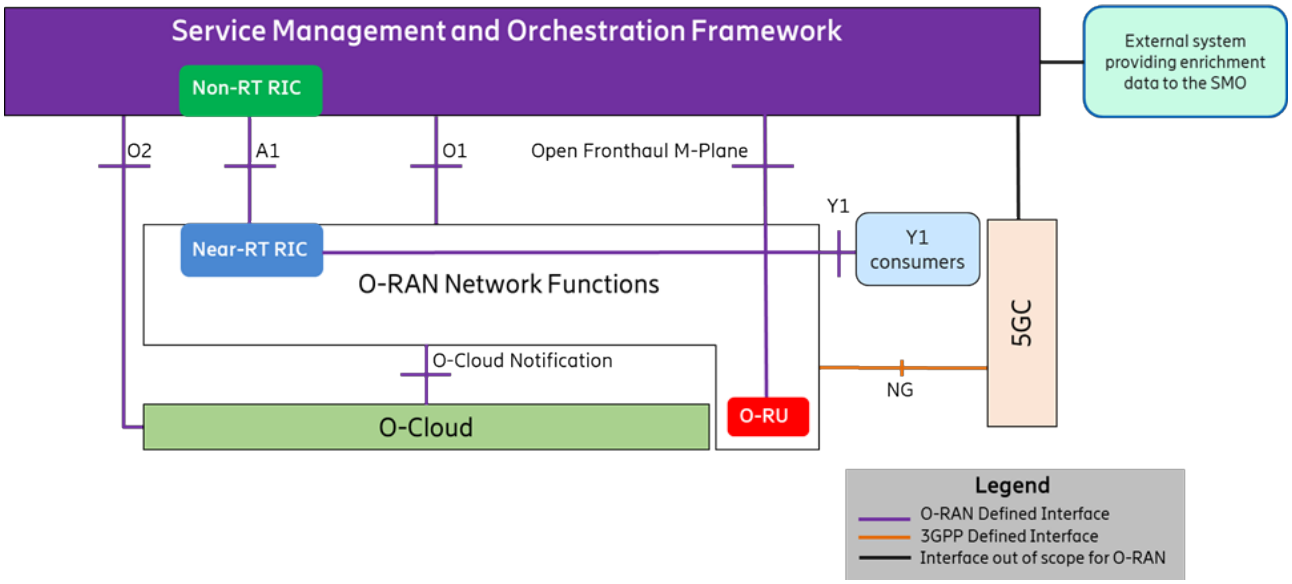


**Figure 2.1-1. High-Level Architecture of O-RAN [2]**

Figure 2.1-2 shows the Non-RT RIC architectural view with its SMO integration.

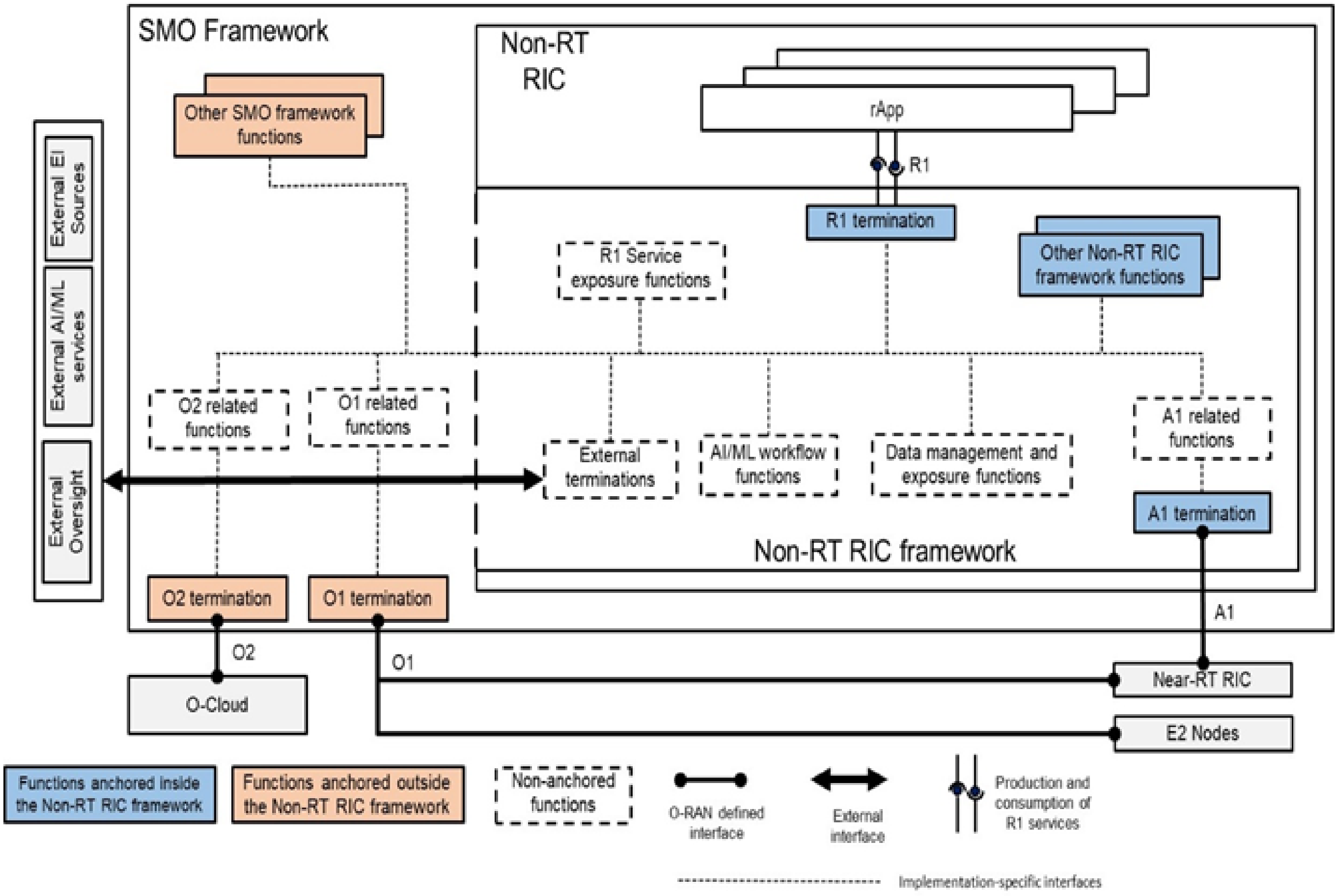


**Figure 2.1-2. Non-RT-RIC Reference Architecture [3]**

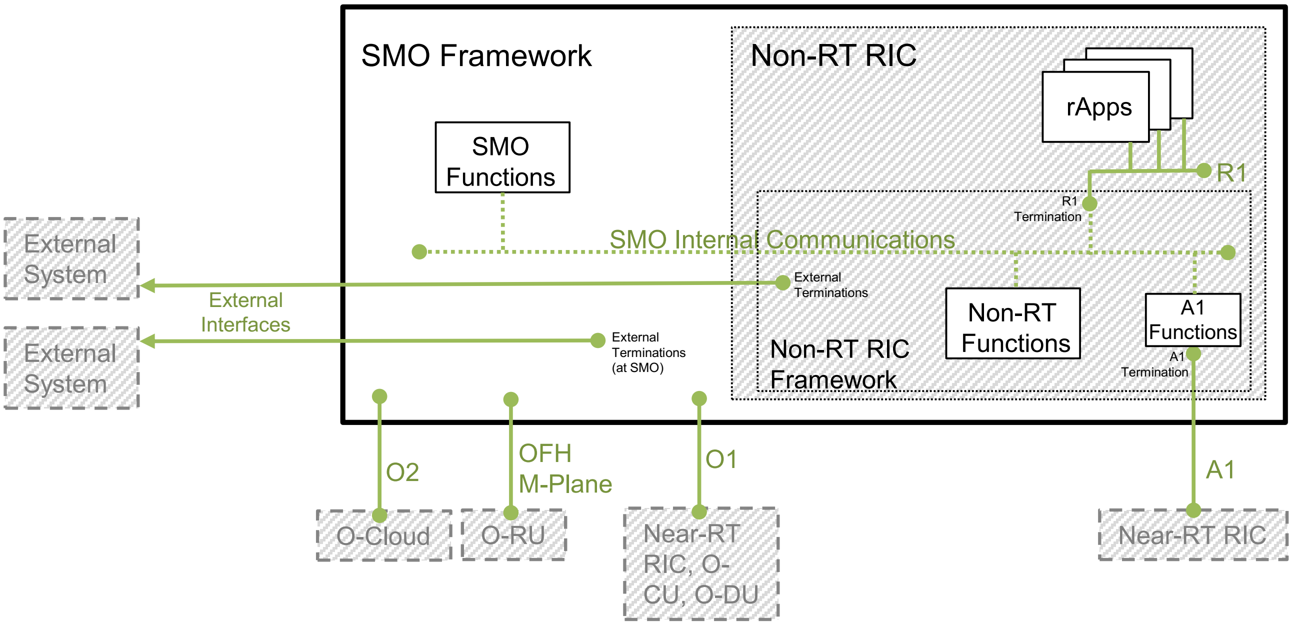


**Figure 2.1-3. SMO Security Architecture**

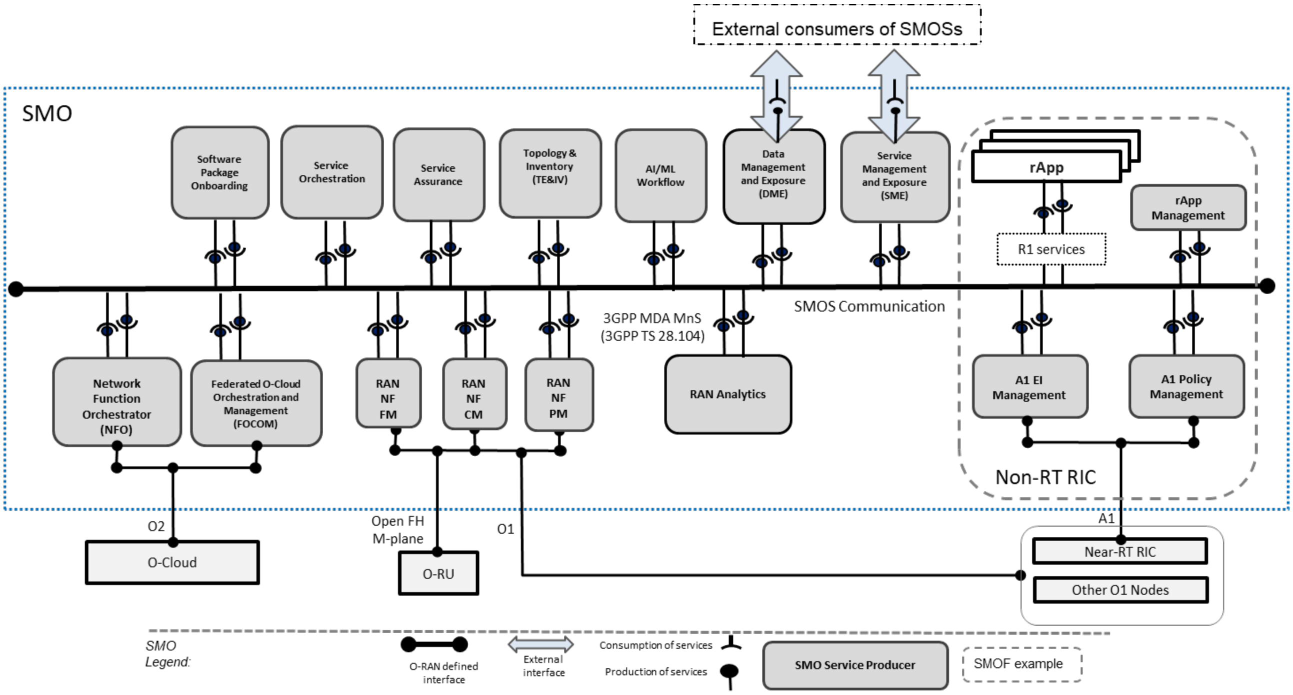
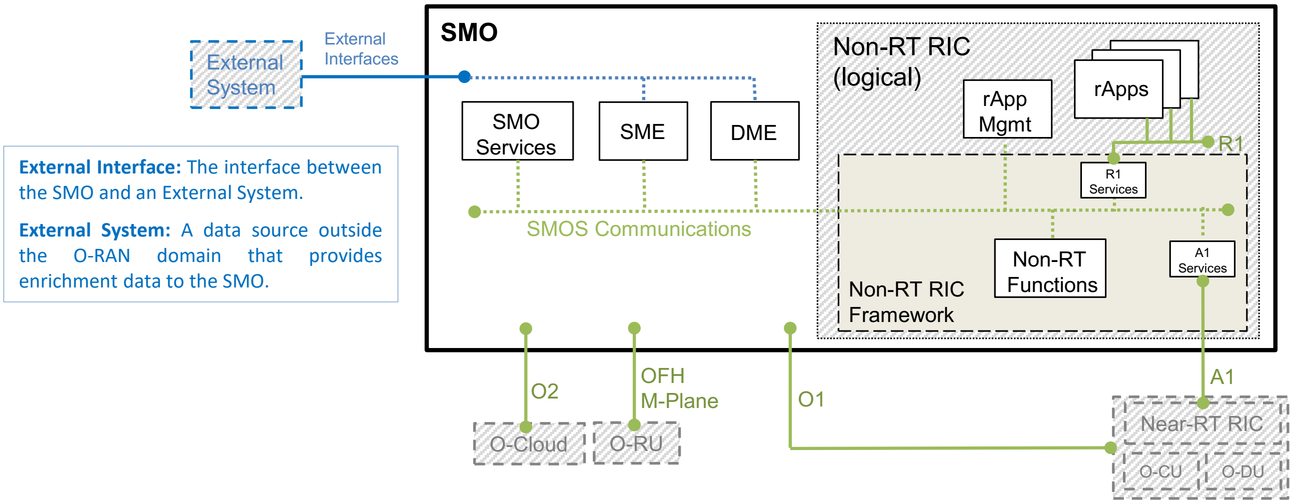


**Figure 2.1-4. Decoupled SMO with SBA [ref: WG1]**



**External Interface:** The interface between the SMO and an External System.

**External System:** A data source outside the O-RAN domain that provides enrichment data to the SMO.

**Figure 2.1-5. Decoupled SMO Security Architecture**

## 4.2 Functions

The following SMO functions should be considered in a risk analysis:

- ASSET-C-01: SMO Framework
- ASSET-C-11: Non-RT RIC
- SMO Functions
- Non-RT Functions, including:
    - ASSET-C-12: AI/ML Functions
    - R1 Service Exposure Functions
    - Data Management and Exposure Functions
- A1 Functions

Note that inclusion of an asset identifier (ASSET-X-yy) indicates that the asset has been identified in the O-RAN Threat Modelling and Remediation Analysis document [6].

## 4.3 Applications

The following SMO applications should be considered in a risk analysis:

- ASSET-C-10: rApps

Note that inclusion of an asset identifier (ASSET-X-yy) indicates that the asset has been identified in the O-RAN Threat Modelling and Remediation Analysis document [6].

## 4.4 Interfaces

The following SMO interfaces should be considered in a risk analysis:

- ASSET-C-14: A1
- ASSET-C-16: R1
- ASSET-C-17: External Interfaces
- SMO Internal Communications
- O1
- O2
- OFH M-Plane

Note that inclusion of an asset identifier (ASSET-X-yy) indicates that the asset has been identified in the O-RAN Threat Modelling and Remediation Analysis document [6].

## 4.5 Information

The following SMO information and data should be considered in a risk analysis:

- O1 Data
  - ASSET-D-03: O1 Critical management plane data
  - ASSET-D-09: O1 informational data
- O2 Data
  - ASSET-D-12: O2-IMS and O2-DMS data
  - ASSET-D-13: O2 Telemetry data
  - ASSET-D-14: O2 cloud provisioning data
- Secret Stores
  - ASSET-D-16: X.509 certificates
  - ASSET-D-17: Private keys
  - ASSET-D-20: Administrator credentials (passwords and tokens)
- AI/ML Data
  - ASSET-D-25: Training or test data: data sets collected externally or internally from the Near-RT RIC, O-CU and O-DU and passed to the ML training hosts in a ML system.
  - ASSET-D-26: The trained ML model which includes intellectual property, numerous configured hyperparameters and millions of learned parameters.

    - ASSET-D-27: The ML prediction results built into the model (e.g. expected outcomes)
    - ASSET-D-28: The behavior of the ML system including tasks for data collection, data wrangling, pipeline management, model retraining, and model deployment.
- PII
    - ASSET-D-30: O-RAN specific UE IDs
- Event logs

Note that inclusion of an asset identifier (ASSET-X-yy) indicates that the asset has been identified in the O-RAN Threat Modelling and Remediation Analysis document [6].

# 5 Threats

## 5.1 Threat Model

For identifying threats, we are using STRIDE:

1. S - Spoofing identity. An application or program can masquerade as another to gain advantages not typically allowed for that program.
2. T - Tampering with data. This involves the malicious modification of data, including making unauthorized changes to a database and alteration of data as it flows between computers.
3. R - Repudiation. A user or program refuses the authenticity of a good or reasonable command or action.
4. I - Information disclosure. This involves the exposure of information to individuals with unauthorized access to it. For example, users gain the ability to read a file that they normally would not have been granted access to, or an intruder can read data in transit between computers.
5. D - Denial of service. These attacks deny service to valid users, such as making a website unavailable or unusable by flooding it with illegitimate requests to keep legitimate users without access.
6. E - Elevation of privileges. An unauthorized user gains privileged rights to access previously no granted to compromise or destroy the system, such as a change in membership.

| **Threat types** | **Impact types** |
|---|---|
| Spoofing | Authenticity |
| Tampering | Integrity |
| Repudiation | Non-repudiation |
| Information disclosure | Confidentiality |
| Denial of Service | Availability |
| Elevation of Privilege | Authorization |

## 5.2 Threat Template

Template to present the threat characteristics:

| | |
|---|---|
| **Threat ID** | |
| **Threat title** | |
| **Threat description** | |
| **Threat type** | Spoofing<br>Tampering<br>Repudiation<br>Information disclosure<br>Denial of Service<br>Elevation of Privilege |
| **Vulnerabilities** | |
| **Impact type** | Authenticity<br>Integrity<br>Non-repudiation<br>Confidentiality<br>Availability<br>Authorization |
| **Affected Assets** | |

## 5.3 Potential Threats and Exploits

A threat analysis is facilitated by an understanding of potential threats, as identified by the Cloud Security Alliance (CSA) and the Open Web Application Security Project (OWASP).

The OWASP Top 10 Web Application Security Risks [12] was updated in 2021 to include the following:

A01:2021 Broken Access Control
A02:2021 Cryptographic Failure
A03:2021 Injection (including Cross-Site Scripting)
A04:2021 Insecure Design
A05:2021 Security Misconfiguration
A06:2021 Vulnerable and Outdated Components
A07:2021 Identification and Authentication Failures
A08:2021 Software and Data Integrity Failures (including Insecure Deserialization)
A09:2021 Security Logging and Monitoring Failures
A10:2021 Server-Side Request Forgery

The CSA Top Threats to Cloud in 2019 was labelled the “Egregious Eleven” [13], as listed below:

1. Data Breaches
2. Misconfiguration and Inadequate Change Control
3. Lack of Cloud Security Architecture and Strategy
4. Insufficient Identity, Credential, Access, and Key Management
5. Account Hijacking
6. Insider Threat
7. Insecure Interfaces and APIs
8. Weak Control plane
9. Metastructure and Applistructure Failures
10. Limited Cloud Usage Visibility
11. Abuse and Nefarious Uses of Cloud Services

The CSA updated its list of top threats to cloud in 2022 and renamed it the “Pandemic Eleven” [14], as listed below:

1. Insufficient Identity, Credential, Access and Key Management, Privileged Accounts
2. Insecure Interfaces and APIs
3. Misconfiguration and Inadequate Change Control
4. Lack of Cloud Security Architecture and Strategy
5. Insecure Software Development
6. Unsecure Third-Party Resources
7. System Vulnerabilities
8. Accidental Cloud Data Disclosure
9. Misconfiguration and Exploitation of Serverless and Container Workloads
10. Organized Crime, Hackers & APT
11. Cloud Storage Data Exfiltration

## 5.4 SMO Threats

The threats listed in section 3.3 relevant to O-RAN and SMO are considered in the SMO threat analysis.  The following threats to SMO have been identified and are analyzed in in section 4 – Threat Analysis.

Table 3.4 – SMO Threats

| Threat-Id | Threat Description (Brief) |
|---|---|
| **General SMO Threats** | |
| T-SMO-01 | External attacker exploits authentication weakness on SMO |
| T-SMO-02 | External attacker exploits authorization weakness on SMO |
| T-SMO-03 | External Overload DoS attack targeted at SMO |
| T-SMO-04 | Internal attacker exploits authentication weakness on a SMO function |
| T-SMO-05 | Internal attacker exploits authorization weakness on SMO |
| T-SMO-06 | Internal Overload DoS attack targeted at SMO functions |
| T-SMO-07 | Internal DoS attack disables internal SMO function(s) or process(es) |
| T-SMO-08 | Attacker exploits insecure API to gain access to SMO |
| T-SMO-09 | Sensitive data in motion is exposed to an internal attacker |
| T-SMO-10 | Sensitive data at rest is exposed to an internal attacker |
| T-SMO-11 | AI/ML poisoning by internal attacker |
| T-SMO-12 | AI/ML exposure on external entity |
| T-SMO-13 | Malicious actor views local logs |
| T-SMO-14 | Malicious actor modifies local log entries |
| T-SMO-15 | Malicious actor deletes local logs |
| T-SMO-16 | Malicious actor intercepts exports of local logs |
| T-SMO-17 | Malicious external actor gains unauthorized access to logs |
| T-SMO-18 | Malicious internal actor gains authorized access to logs |
| **Threats at O2 interface** | |
| T-SMO-19 | Internal attacker exploits O2 interface to view data in transit between SMO and O-Cloud |
| T-SMO-20 | Internal attacker exploits O2 interface to modify data in transit between SMO and O-Cloud |
| T-SMO-21 | Internal attacker uses O2 interface via SMO to exploit API vulnerability to gain access to O-Cloud infrastructure |
| T-SMO-22 | Internal attacker floods O2 interface via SMO to cause DDoS on O-Cloud infrastructure |
| T-SMO-23 | External attacker uses O2 interface via O-Cloud to exploit API vulnerability to gain access to SMO |
| T-SMO-24 | External attacker floods O2 interface via O-Cloud to cause DDoS on SMO |
| T-SMO-25 | External attacker uses O2 interface via O-Cloud to gain authorized access to sensitive data-at-rest at the SMO |
| **Threats at External interfaces** | |
| T-SMO-26 | External attacker exploits External interface to view data in transit between SMO and external service |
| T-SMO-27 | External attacker exploits External interface to modify data in transit between SMO and external service |
| T-SMO-28 | External attacker uses External interface to exploit API vulnerability to gain access to SMO |
| T-SMO-29 | External attacker floods External interface to cause DDoS at SMO |
| T-SMO-30 | External attacker uses External interface to gain access to sensitive data-at-rest at the SMO |
| T-SMO-31 | External attacker poisons External AI/ML data to corrupt SMO |
| T-SMO-32 | External attacker poisons External Enrichment Information data sources to corrupt SMO |

# 6 Threat Analysis

SMO threats are identified in the tables below. External and internal threats are from the perspective of the SMO. External Threats are external to the SMO and Internal Threats are internal the SMO. This section provides threat analysis of three types of SMO threats:

- General SMO Threats
- Threats at O2 interface
- Threats at External interfaces

Additional SMO threats may be added for Decoupled SMO and Shared O-RU.

## 6.1 General SMO Threats

| | |
|---|---|
| **Threat ID** | T-SMO-01 |
| **Threat title** | External attacker exploits authentication weakness on SMO |
| **Threat description** | An external attacker can exploit the improper/missing authentication weakness on SMO functions. If the authentication of O-RAN subjects on A1, O1, O2, and External interfaces on SMO is not supported or not properly implemented, those interfaces without proper credentials could be exploited to gain access to the SMO. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-02 |
| **Threat title** | External attacker exploits authorization weakness on SMO |
| **Threat description** | An external attacker can exploit the improper/missing authorization weakness on SMO functions.  A malicious external entity on A1, O1, O2, and External interfaces without authorization or with an incorrect access token may invoke the SMO functions. The data at rest related to that function will be leaked to the attacker. In addition, an attacker can be able to perform certain actions, e.g.  disclose O-RAN sensitive information or alter O-RAN components. |
| **Threat type** | Elevation of Privilege, Information Disclosure |
| **Impact type** | Authorization. Confidentiality |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-03 |
| **Threat title** | External Overload DoS attack targeted at SMO |
| **Threat description** | Overload situation could appear in the case of DoS attack or increased traffic on externally facing interfaces. Inability to mitigate traffic volumetric attacks on an external interface affects availability of SMO data and functions. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-04 |
| **Threat title** | Internal attacker exploits authentication weakness on a SMO function |
| **Threat description** | An internal attacker can exploit the improper/missing authentication weakness on SMO functions.  If the authentication of internal interfaces (e.g. Internal Message Bus and R1) on SMO is not supported or not properly implemented, those interfaces without credentials could exploited to gain access to the SMO. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-05 |
| **Threat title** | Internal attacker exploits authorization weakness on SMO |
| **Threat description** | An internal attacker can exploit the improper/missing authorization weakness on SMO functions.  Malicious internal entities without authorization or with an incorrect access token may invoke the SMO functions. The data at rest related to these functions will be leaked to the attacker. In addition, an attacker can be able to perform certain actions, e.g.  disclose O-RAN sensitive information or alter O-RAN components. |
| **Threat type** | Elevation of Privilege, Information Disclosure |
| **Impact type** | Authorization |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-06 |
| **Threat title** | Internal Overload DoS attack targeted at SMO functions |
| **Threat description** | Overload situation could appear in the case of DoS attack or increased traffic on internal SMO interfaces. Inability to mitigate traffic volumetric attacks on an external interface affects availability of SMO data and functions. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-07 |
| **Threat title** | Internal DoS attack disables internal SMO function(s) or process(es) |
| **Threat description** | Internal malicious actor exploits a vulnerability or escalates privilege to execute a DoS attack by disabling one or more SMO processes or functions. Inability to detect and report such events affects availability of SMO functions. |
| **Threat type** | Denial of Service, Escalation of Privilege |
| **Impact type** | Availability |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-08 |

| | |
|---|---|
| **Threat title** | Attacker exploits insecure API to gain access to SMO |
| **Threat description** | An insecure API may allow access to a system for an attacker to conduct remote code execution or an advanced persistent threat |
| **Threat type** | Tampering, Information Disclosure, Escalation of Privilege |
| **Impact type** | Integrity, Confidentiality, Authorization |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-09 |
| **Threat title** | Sensitive data in motion is exposed to an internal attacker |
| **Threat description** | Unprotected data transferred between internal SMO functions is disclosed to an internal threat actor |
| **Threat type** | Information Disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-10 |
| **Threat title** | Sensitive data at rest is exposed to an internal attacker |
| **Threat description** | 7 Unprotected data stored on the SMO is disclosed to an internal threat actor that has gain authorized access through privilege escalation |
| **Threat type** | Information Disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-11 |
| **Threat title** | AI/ML poisoning by internal attacker |
| **Threat description** | Internal attacker gains authorized access exploited to poison AI/ML training data,or the AI/ML models, stored in the SMO to influence insights. |
| **Threat type** | Tampering |
| **Impact type** | Integrity |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-12 |
| **Threat title** | AI/ML exposure on external entity |
| **Threat description** | An external attacker can gain access to external entities to view or modify sensitive data AI/ML data, or models, transferred between the external function and SMO via external interfaces(e.g., EI, Human-Machine, A1, O1) |
| **Threat type** | Information disclosure, Tampering |

| | |
|---|---|
| **Impact type** | Confidentiality, Integrity |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-13 |
| **Threat title** | Malicious actor views local logs |
| **Threat description** | Malicious actor accesses locally stored logs in the SMO to perform reconnaissance to collect sensitive or private information. |
| **Threat type** | Information disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-14 |
| **Threat title** | Malicious actor modifies local log entries |
| **Threat description** | Malicious actor accesses locally stored logs in the SMO to modify entries to hide presence or cause confusion. |
| **Threat type** | Tampering |
| **Impact type** | Integrity |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-15 |
| **Threat title** | Malicious actor deletes local log entries |
| **Threat description** | Malicious actor accesses locally stored logs in the SMO to delete entries to hide presence or cause confusion. |
| **Threat type** | Tampering |
| **Impact type** | Integrity |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-16 |
| **Threat title** | Malicious actor intercepts exports of local logs |
| **Threat description** | Malicious actor gains access to an external interface to intercept data in motion as logs are transferred from the SMO to a remote server/external entity. |
| **Threat type** | Information disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-17 |

| | |
|---|---|
| **Threat title** | Malicious external actor gains unauthorized access to logs |
| **Threat description** | Malicious external actor gains unauthorized access to stored logs to view, modify, and delete |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Confidentiality |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-18 |
| **Threat title** | Malicious internal actor gains authorized access to logs |
| **Threat description** | Malicious internal actor gains authorized access to stored logs to view, modify, and delete. |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization |
| **Affected Asset** | SMO |

## 4.2 Threats at O2 interface

| | |
|---|---|
| **Threat ID** | T-SMO-19 |
| **Threat title** | Internal attacker exploits O2 interface to view data in transit between SMO and O-Cloud |
| **Threat description** | If the O2 interface is not properly confidentiality protected, an internal attacker can perform a man-in-the-middle attack to view data in transit. |
| **Threat type** | Information disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | O2 interface |

| | |
|---|---|
| **Threat ID** | T-SMO-20 |
| **Threat title** | Internal attacker exploits O2 interface to modify data in transit between SMO and O-Cloud |
| **Threat description** | If the O2 interface is not properly integrity protected, an internal attacker can perform a man-in-the-middle attack to modify data in transit. |
| **Threat type** | Tampering |
| **Impact type** | Integrity |
| **Affected Asset** | O2 interface |

| | |
|---|---|
| **Threat ID** | T-SMO-21 |
| **Threat title** | Internal attacker uses O2 interface via SMO to exploit API vulnerability to gain access to O-Cloud infrastructure |

| | |
|---|---|
| **Threat description** | If the O2 interface uses an API with a known vulnerability that is not properly protected or patched, an attacker can exploit it to gain access to the O-Cloud infrastructure from the SMO. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-Cloud |

| | |
|---|---|
| **Threat ID** | T-SMO-22 |
| **Threat title** | Internal attacker floods O2 interface via SMO to cause DDoS on O-Cloud infrastructure |
| **Threat description** | If the O2 interface is not protected, an internal attacker on the SMO can flood the O2 interface to overload the O-Cloud.  This can prevent legitimate messages from reaching the O-Cloud or cause heavy processing at the O-Cloud, resulting in performance degradation. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | O-Cloud |

| | |
|---|---|
| **Threat ID** | T-SMO-23 |
| **Threat title** | External attacker uses O2 interface via O-Cloud to exploit API vulnerability to gain access to SMO |
| **Threat description** | If the O2 interface uses an API with a known vulnerability that is not properly protected or patched, an attacker can exploit it to gain access to the SMO from the O-Cloud infrastructure. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-24 |
| **Threat title** | External attacker floods O2 interface via O-Cloud to cause DDoS on SMO |
| **Threat description** | If the O2 interface is not protected, an external attacker in the O-Cloud can flood the O2 interface to overload the SMO.  This can prevent legitimate messages from reaching the SMO or cause heavy processing at the SMO, resulting in performance degradation or outage of the SMO. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-25 |
| **Threat title** | External attacker uses O2 interface via O-Cloud to gain authorized access to sensitive data-at-rest at the SMO |
| **Threat description** | If the SMO is not protected, an external attacker at the O-Cloud can use the O2 interface to gain authorized access to the SMO to view data-at-rest. |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization |

| | |
|---|---|
| **Affected Asset** | SMO |

## 4.3 Threats at External interfaces

| | |
|---|---|
| **Threat ID** | T-SMO-26 |
| **Threat title** | External attacker exploits External interface to view data in transit between SMO and external service |
| **Threat description** | If an External interface is not properly confidentiality protected, an external attacker can perform a man-in-the-middle attack to view data in transit. |
| **Threat type** | Information disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | External interface |

| | |
|---|---|
| **Threat ID** | T-SMO-27 |
| **Threat title** | External attacker exploits External interface to modify data in transit between SMO and external service |
| **Threat description** | If an External interface is not properly integrity protected, an external attacker can perform a man-in-the-middle attack to modify data in transit. |
| **Threat type** | Tampering |
| **Impact type** | Integrity |
| **Affected Asset** | External interface |

| | |
|---|---|
| **Threat ID** | T-SMO-28 |
| **Threat title** | External attacker uses External interface to exploit API vulnerability to gain access to SMO |
| **Threat description** | If an External interface uses an API with a known vulnerability that is not properly protected or patched, an attacker can exploit it to gain access to the SMO. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-29 |
| **Threat title** | External attacker floods External interface to cause DDoS at SMO |
| **Threat description** | If the External interface is not protected, an external attacker can flood an External interface to overload the SMO.  This can prevent legitimate messages and data from reaching the SMO or cause heavy processing at the SMO, resulting in performance degradation or outage of the SMO. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |

| | |
|---|---|
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-30 |
| **Threat title** | External attacker uses External interface to gain access to sensitive data-at-rest at the SMO |
| **Threat description** | If the SMO is not protected, an external attacker can use the External interface to gain authorized access to the SMO to view data-at-rest. |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-31 |
| **Threat title** | External attacker poisons External AI/ML data to corrupt SMO |
| **Threat description** | External data sources may be outside the control of the stakeholder(s) responsible for the O-RAN deployment. The stakeholder for an External data source could fail to provide proper security controls to protect data consumed by the SMO.  If an external attacker were to gain access to AI/ML data, it could be corrupted and then be used at the SMO. |
| **Threat type** | Tampering |
| **Impact type** | Integrity |
| **Affected Asset** | SMO |

| | |
|---|---|
| **Threat ID** | T-SMO-32 |
| **Threat title** | External attacker poisons External Enrichment Information data sources to corrupt SMO |
| **Threat description** | External data sources may be outside the control of the stakeholder(s) responsible for the O-RAN deployment. The stakeholder for an External data source could fail to provide proper security controls to protect data consumed by the SMO.  If an external attacker were to gain access to External Enrichment Information, it could be corrupted and then be used at the SMO. |
| **Threat type** | Tampering |
| **Impact type** | Integrity |
| **Affected Asset** | SMO |

## 4.4 Preliminary Threat Analysis for RAN-Core Data Sharing

RAN-Core Data Sharing is a new SMO feature to provide data export from the SMO to the 5G Core (5GC).  5 possible architectural options are being considered:

- Option 1: SMO/Non-RT RIC to 5GC Consumer with Facade of NWDAF
- Option 2: SMO/Non-RT RIC to 5GC DCCF/MFAF with Facade of NWDAF
- Option 3: SMO/Non-RT RIC to 5GC NWDAF with Facade of OA&M
- Option 4: SMO/Non-RT RIC to 5GC NWDAF with Facade of RAN NF
- Option 5: SMO/Non-RT RIC to 5GC NWDAF with MDAS through SME

WG11 performed a security analysis of the architectural options to provide recommendations for which should be considered for specification.  In summary, Option 1 is high security risk and should not be considered. Option 2, 3, 4, and 5 are lower risk and equivalent from a security perspective. However, those options have a major risk due to lack of certificate-based mutual authentication with NWDAF. Option 5, in addition, requires the 3GPP NWDAF add support for the O-RAN SME interface, which needs new 3GPP standardization.

# 5 Security Controls

Industry recommendations for strong security controls are provided from sources such as the OWASP Top 10 Proactive Controls [15], Center for Internet Security (CIS) Critical Security Controls [16], Cloud Security Alliance (CSA) Cloud Control Matrix (CCM) [17], ISO/IEC 27001:2013 Information Security Management System (ISMS) [18], NIST SP 800-53r5 Security and Privacy Controls for Information Systems and Organizations [19], and Cybersecurity and Infrastructure Security Agency (CISA) Security Guidance for 5G Cloud Infrastructures [9].

The OWASP Top 10 Proactive Controls are as follow:

C1: Define Security Requirements

C2: Leverage Security Frameworks and Libraries

C3: Secure Database Access

C4: Encode and Escape Data

C5: Validate All Inputs

C6: Implement Digital Identity

C7: Enforce Access Controls

C8: Protect Data Everywhere

C9: Implement Security Logging and Monitoring

C10: Handle All Errors and Exceptions

The CIS Critical Security Controls are as follow:

CIS Control 1: Inventory and Control of Enterprise Assets

CIS Control 2: Inventory and Control of Software Assets

CIS Control 3: Data Protection

CIS Control 4: Secure Configuration of Enterprise Assets and Software

CIS Control 5: Account Management

CIS Control 6: Access Control Management

CIS Control 7: Continuous Vulnerability Management

CIS Control 8: Audit Log Management

CIS Control 9: Email Web Browser and Protections

CIS Control 10: Malware Defenses

CIS Control 11: Data Recovery

CIS Control 12: Network Infrastructure Management

CIS Control 13: Network Monitoring and Defense

CIS Control 14: Security Awareness and Skills Training

CIS Control 15: Service Provider Management

CIS Control 16: Application Software Security

CIS Control 17: Incident Response Management

CIS Control 18: Penetration Testing

Relevant controls from the CSA CCM are 2. Application and Interface Security, 5. Cryptography, Encryption, and Key Management, 7. Data Security and Privacy Lifecycle Management, and 10. Identity and Access Management (IAM).

Relevant controls from ISO/IEC 27001:2013 are 5. Access Controls, 6. Cryptography, and 9. Communications Security.

Relevant controls from NIST SP 800-53r5 are 1. Access Controls, 16. Risk Assessment, 18. System and Communications Protection, and 19. System and Information Integrity.

Relevant controls from CISA's Security Guidance are mTLS 1.2, or higher, with PKI and X.509 certificates, Multi-Factor Authentication (MFA), Principle of Least Privilege, Continuous Monitoring and Logging, and data confidentiality and protection as components of a zero trust architecture as defined in NIST SP 800-207 [8].

With consideration of these external sources, the following security controls should be evaluated for the SMO risk analysis:

Control-1: mTLS 1.2 or 1.3 with PKI and X.509 certificates

Control-2: OAuth 2.0

Control-3: IAM (using RBAC, ABAC, PBAC, TBAC)

Control-4: Principle of Least Privilege

Control-5: Certificate Management

Control-6: API Message Integrity Protection and Input Validation

Control-7: API Message Authentication

Control-8: Encryption for Data at Rest

Control-9: Encryption for Data in Motion

Control-10: Integrity Protection for Data at Rest

Control-11: Integrity Protection for Data in Motion

Control-12: Integrity Protection for Data in Use

Control-13: Digital Signatures

Control-14: Monitoring and Logging

Control-15: Alerting

Control-16: Rate-Limiting

Control-17: Configuration Validation

Control-18: Network Segmentation and Traffic Filtering

# 6 Risk Assessment

This section provides risk assessment tables for each of the identified assets. These tables list the assets, threats, impacts, and possible security controls.

A malicious actor may be a nation-state adversary, cybercriminal, or employee. In a ZTA, perimeter defenses alone are insufficient. The SMO must be protected from untrusted external sources attempting to have access, while also assuming internal threat actors are inside the network with access to its functions and data. Security controls for a ZTA, protecting against external and internal threats, should be implemented through a risk-based approach. A risk analysis calculates risk levels by assessing the threat’s Likelihood of attack and the Impact from the attack.

Impact scores can be lowered with consideration of existing security controls. Impact scoring is based upon current security controls. Impact scoring does not consider security controls that may be potentially specified in the future.

Likelihood scores may be higher when the goal is a ZTA, because external and internal threats must be considered. When likelihood scoring during a risk analysis, it is necessary to consider internal threats performing reconnaissance attacks impacting confidentiality and privacy and attacks causing damage or degrading performance impacting availability. Internal threat actors are less likely to perform damaging attacks that are quickly and easily detected and blocked, but more likely to attempt reconnaissance attacks to collect information. As a result, reconnaissance type attacks can be scored Likelihood = High while damaging/availability attacks can be scored Likelihood = Medium or Low.

External and internal threats are from the perspective of the SMO. External Threats are external to the SMO and Internal Threats are internal to the SMO. An External Threat may be external to the SMO but internal to the O-RAN architecture.

A risk analysis of SMO threats is provided in the tables below covering general SMO risks, risks to the O2 interface, and risks to External interfaces.

Threats and risks to the A1 and R1 interfaces are assessed in a separate Technical Report, Study on Security for Non-RT-RIC [20].

Additional SMO threats may be added for Decoupled SMO and Shared O-RU.

## 6.1 General SMO Risks

Table 6-1. SMO Risk Analysis

| Asset-Id | Asset Name | Threat-Id | Threat Description (Brief) | Impact/ Likelihood Raw Score | Possible Security Controls | Security Control-id |
|---|---|---|---|---|---|---|
| ASSET-C-01 | SMO | T-SMO-01 | External attacker exploits authentication weakness on SMO | Impact = High<br>Likelihood = Medium | Data encryption using mTLS 1.2 or 1.3 | Control-1 |
| ASSET-C-01 | SMO | T-SMO-02 | External attacker exploits authorization weakness on SMO | Impact = High<br>Likelihood = Medium | OAuth 2.0, IAM, principle of least privilege | Control-2,<br>Control-3,<br>Control-4 |
| ASSET-C-01 | SMO | T-SMO-03 | External Overload DoS attack targeted at SMO | Impact = High<br>Likelihood = Medium | Rate-Limiting | Control-16 |
| ASSET-C-01 | SMO | T-SMO-04 | Internal attacker exploits authentication weakness on a SMO function | Impact = High<br>Likelihood = Medium | Data encryption using mTLS 1.2 or 1.3 | Control-1 |
| ASSET-C-01 | SMO | T-SMO-05 | Internal attacker exploits authorization weakness on SMO | Impact = High<br>Likelihood = Medium | OAuth 2.0, IAM, principle of least privilege | Control-2,<br>Control-3 |
| ASSET-C-01 | SMO | T-SMO-06 | Internal Overload DoS attack targeted at SMO functions | Impact = High | Rate-Limiting | Control-16 |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
|  |  |  |  | Likelihood = Medium |  |  |
| ASSET-C-01 | SMO | T-SMO-07 | Internal DoS attack disables internal SMO function(s) or process(es) | Impact = High Likelihood = Medium | Monitoring, Logging, Alerting | Control-14, Control-15 |
| ASSET-C-01 | SMO | T-SMO-08 | Attacker exploits insecure API to gain access to SMO | Impact = High Likelihood = Medium | API input validation | Control-6 |
| ASSET-C-01 | SMO | T-SMO-09 | Sensitive data in motion is exposed to an internal attacker | Impact = High Likelihood = Medium | Data encryption and integrity protection using mTLS 1.2 or 1.3 | Control-1 |
| ASSET-C-01 | SMO | T-SMO-10 | Sensitive data at rest is exposed to an internal attacker | Impact = High Likelihood = High | Data encryption and integrity protection | Control-8, Control-10 |
| ASSET-C-01 | SMO | T-SMO-11 | AI/ML poisoning by internal attacker | Impact = High Likelihood = Medium | Integrity protection | Control-10 |
| ASSET-C-01 | SMO | T-SMO-12 | AI/ML exposure on external entity | Impact = High Likelihood = Medium | Data encryption, Integrity protection, API input validation | Control-6, Control-8, Control-10 |
| ASSET-C-01 | SMO | T-SMO-13 | Malicious actor views local logs | Impact = High Likelihood = High | Data encryption | Control-8 |
| ASSET-C-01 | SMO | T-SMO-14 | Malicious actor modifies local log entries | Impact = High Likelihood = Medium | Integrity protection | Control-10 |
| ASSET-C-01 | SMO | T-SMO-15 | Malicious actor deletes local logs | Impact = High Likelihood = Medium | Integrity protection | Control-10 |
| ASSET-C-01 | SMO | T-SMO-16 | Malicious actor intercepts exports of local logs | Impact = High Likelihood = High | Data encryption | Control-9 |
| ASSET-C-01 | SMO | T-SMO-17 | Malicious external actor gains unauthorized access to logs | Impact = High Likelihood = High | IAM, principle of least privilege | Control-3, Control-4 |
| ASSET-C-01 | SMO | T-SMO-18 | Malicious internal actor gains authorized access to logs | Impact = High Likelihood = High | Data encryption | Control-8 |

## 6.2 Threats at O2 interface

Table 6-2. SMO Risk Analysis for Internal Threats at O2 Interface

| Asset-Id | Asset Name | Threat-Id | Threat Description (Brief) | Impact/ Likelihood Raw Score | Possible Security Controls | Security Control-id |
|---|---|---|---|---|---|---|
| ASSET-C-01 | SMO | T-SMO-19 | Internal attacker exploits O2 interface to view data in transit between SMO and O-Cloud | Impact = High Likelihood = High | Data encryption using mTLS 1.2 or 1.3 | Control-1 |
| ASSET-C-01 | SMO | T-SMO-20 | Internal attacker exploits O2 interface to modify data in transit between SMO and O-Cloud | Impact = High Likelihood = Medium | Integrity protection using mTLS 1.2 or 1.3 | Control-1 |

| | | | | | | |
|---|---|---|---|---|---|---|
| ASSET-C-01 | SMO | T-SMO-21 | Internal attacker uses O2 interface via SMO to exploit API vulnerability to gain access to O-Cloud infrastructure | Impact = High<br>Likelihood = High | API message authentication,<br>API input validation | Control-7, Control-6 |
| ASSET-C-01 | SMO | T-SMO-22 | Internal attacker floods O2 interface via SMO to cause DDoS on O-Cloud infrastructure | Impact = High<br>Likelihood = Medium | Rate-Limiting, Network segmentation | Control-16, Control-18 |
| ASSET-C-01 | SMO | T-SMO-23 | External attacker uses O2 interface via O-Cloud to exploit API vulnerability to gain access to SMO | Impact = High<br>Likelihood = Medium | API message authentication,<br>API input validation | Control-7, Control-6 |
| ASSET-C-01 | SMO | T-SMO-24 | External attacker floods O2 interface via O-Cloud to cause DDoS on SMO | Impact = High<br>Likelihood = Medium | Rate-Limiting, Network segmentation | Control-16, Control-18 |
| ASSET-C-01 | SMO | T-SMO-25 | External attacker uses O2 interface via O-Cloud to gain authorized access to sensitive data-at-rest at the SMO | Impact = High<br>Likelihood = Medium | Data encryption, Integrity protection | Control-8, Control-10 |

## 6.3 Threats at External Interfaces

Table 6-3. SMO Risk Analysis for External Threats at External interfaces

| Asset-Id | Asset Name | Threat-Id | Threat Description (Brief) | Impact/ Likelihood Raw Score | Possible Security Controls | Security Control-id |
|---|---|---|---|---|---|---|
| ASSET-C-01 | SMO | T-SMO-26 | External attacker exploits External interface to view data in transit between SMO and external service | Impact = High<br>Likelihood = High | Data encryption using mTLS 1.2 or 1.3 | Control-1 |
| ASSET-C-01 | SMO | T-SMO-27 | External attacker exploits External interface to modify data in transit between SMO and external service | Impact = High<br>Likelihood = Medium | Integrity protection using mTLS 1.2 or 1.3 | Control-1 |
| ASSET-C-01 | SMO | T-SMO-28 | External attacker uses External interface to exploit API vulnerability to gain access to SMO | Impact = High<br>Likelihood = Medium | API message authentication,<br>API input validation | Control-7, Control-6 |
| ASSET-C-01 | SMO | T-SMO-29 | External attacker floods External interface to cause DDoS at SMO | Impact = High<br>Likelihood = Medium | Rate-Limiting, Network segmentation | Control-16, Control-18 |
| ASSET-C-01 | SMO | T-SMO-30 | External attacker uses External interface to gain access to sensitive data-at-rest at the SMO | Impact = High<br>Likelihood = Medium | Data encryption, Integrity protection | Control-8, Control-10 |
| ASSET-C-01 | SMO | T-SMO-31 | External attacker poisons External AI/ML data to corrupt SMO | Impact = High<br>Likelihood = High | Data encryption, Integrity protection | Control-8, Control-10 |
| ASSET-C-01 | SMO | T-SMO-32 | External attacker poisons External Enrichment Information data sources to corrupt SMO | Impact = High<br>Likelihood = High | Data encryption, Integrity protection | Control-8, Control-10 |

# 7 Primary Security Issues

The following items were identified during the SMO Security Analysis phase 1 and are addressed in this TR v1:

1. External interfaces to the SMO and Non-RT RIC have risks of exploitation from external threat actors. The protocol and API used on an external interface is defined by the application or service and is not in-scope for the O-RAN Alliance. WG11 analyzed the threats, risks, and potential security controls with the goal to provide general security requirements for any implementation of an External interface with the goal to protect O-RAN network functions and data.

2. The O2 interface is at risk of being exploited by an internal threat actor at the SMO or the O-Cloud. This TR provides a security analysis of the O2 interface from the perspectives of the internal threat actor at the SMO and the O-Cloud, in addition to external threats. The work item team will need to collaborate with the O-Cloud security work item team to ensure complete coverage of O2 threats and security controls.

The following items were identified as SMO security topics that will require additional phases of the SMO Security Analysis to produce an update to the TR.

1. SMO Internal Communications may be implemented as a bus or direct communication. WG11 will need to form general security requirements for both implementations.

2. WG11 should contribute security requirements during efforts to develop specifications for a Decoupled SMO. A second phase of the SMO Security Analysis TR will need to be performed to address the Decoupled SMO architecture defined in WG1.

3. WG11 should contribute security requirements during efforts to develop specifications for RAN-Core Data Sharing. A second phase of the SMO Security Analysis TR will need to be performed to address the RAN-Core Data Sharing defined in WG1.

4. WG11 should contribute security requirements during efforts to develop specifications for Shared O-RU. A new phase of the SMO Security Analysis TR may need to address the Shared O-RU architectural options.

5. A new phase of the SMO Security Analysis TR may need to consider Transport Node (TN) Termination, as specified in WG9, and Cooperative Transport Interface (CTI), as specified in WG4.

# 8 Recommendations

The Security Analysis presented in this technical report used the following process:

1. Asset identification -> 2. Threat identification -> 3. Threat analysis -> 4. Risk analysis -> 5. Recommend Security Controls

The SMO is a logical framework, not an implementation architecture, with external interfaces and internal functions and interfaces that are assets which should be protected with security controls. The SMO may be implemented as a monolithic platform or multiple disaggregated functions, such as SMO functions and Non-RT-RIC functions, which should be protected assets. Other SMO assets are the R1, A1, O1, O2, OFH M-Plane, and External interfaces and data at rest and in transit.

**Recommendation 1**: WG11 should update the Security Threat Modeling and Remediation Analysis document [6] to include the assets identified in this security analysis technical report. A CR will be generated.

For the threat analysis, external and internal threats were considered from the perspective of the SMO. Internal threats are internal the SMO and external threats are external to the SMO. External threats may be external to the SMO and internal to the O-RAN architecture. More than 30 threats were identified, categorized as general SMO threats, O2 interface threats, and External interfaces threat.

**Recommendation 2**: WG11 should update the Security Threat Modeling and Remediation Analysis document [6] to include the threats and threat tables created in this security analysis technical report. A CR will be generated.

Risk analysis of the identified threats included impact-likelihood scoring. All 30+ of the identified threats were score either high-medium or high-high. External data sources are considered the greatest threat to the SMO due to the risk of an external threat actor poisoning external data that is imported into the SMO and the risk of an external threat actor exploiting an API on the external interface to gain access to the SMO or perform a remote code execution attack.

Likelihood scoring was influenced by the consideration of a zero trust architecture (ZTA), which is a publicly expressed goal of the O-RAN Alliance to consider external and internal threats. ZTA is built on the foundational principles that perimeter defenses are insufficient to secure a network as internal external threats pose risk to a network. There are two guidelines for designing a network and its network functions for a ZTA:

1. There is no implicit trust granted to an asset based upon ownership, physical location, or network location [8].

2. Assume the adversary is already inside the network [9].

The security controls recommended in this TR protect the SMO from confidentiality, integrity, and availability attacks from external and internal threats, consistent with a ZTA.

**Recommendation 3**: The SMO should have security controls implemented to protect its functions and interfaces from external and internal threats, consistent with a ZTA. Specific requirements will be formed as this work item continues. A CR for the WG11 Security Requirements Specifications is planned for the March release train.

Consistent with a ZTA, the SMO should be secure by design in which its security posture does not assume that the SMO internal functions and interfaces are secure.

**Recommendation 4**: WG11 should collaborate with WG1 to ensure the WG11 security specifications are referenced by WG1 in its SMO specifications. This process will build-in security to the evolving specifications for the SMO and Decoupled SMO.

The SMO architecture is continuing to evolve to support Decoupled SMO and direct communication between internal SMO functions and applications. In addition, the security analysis will also need to consider Transport Node (TN) Termination, as specified in WG9, and Cooperative Transport Interface (CTI), as specified in WG4.

**Recommendation 5**: This SMO Security work item continues its security analysis to produce a TR v2 for the March release train, addressing Decoupled SMO, TN, and CTI.

The SMO role in certificate management is currently unspecified.

**Recommendation 6:** The WG11 Certificate Management work item team should investigate a potential role, if any, for the SMO in certificate management.

# History

| **Date** | **Revision** | **Doc status** | **Author** | **Description** |
|---|---|---|---|---|
| July 2022 | V01.00.00 | First release | WG11 | Document creation, template |
| March 2023 | V02.00 | Second release | WG11 | Update architecture diagrams in Section 2 – Assets. |
| November 2023 | V03.00 | Third release | WG11 | Add security analysis for Decoupled SMO and RAN-Core Data Sharing |