 O-RAN-WG11.TR.O-RUCUM.0-R004-v04.00

Technical Report

O-RAN Working Group 11 (WG11)

Study on O-RU Centralized User Management

Copyright © 2025 by the O-RAN ALLIANCE e.V.

The copying or incorporation into any other work of part or all of the material available in this document in any form without the prior written permission of O-RAN ALLIANCE e.V. is prohibited, save that you may print or download extracts of the material of this document for your personal use, or copy the material of this document for the purpose of sending to individual third parties for their information provided that you acknowledge O-RAN ALLIANCE as the source of the material and that you inform the third party that these conditions apply to them and that they must comply with them.

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

Register of Associations, Bonn VR 11238, VAT ID DE321720189

Contents

Foreword 5

Modal verbs terminology 5

Introduction 5

1 Scope 6

2 References 7

2.1 Informative references 7

3 Definitions and Abbreviations 8

3.1 Terms 8

3.2 Definitions 8

3.3 Abbreviations 8

4 Background 9

4.1 Netconf Access Control 9

4.2 Software and Configuration Server (SCS) 9

5 Key Issues 10

5.1 Key Issue #1: Default account in O-RU 10

5.1.1 Key issue detail 10

5.1.2 Security threats 10

5.1.3 Potential security requirements 10

5.2 Key Issue #2: Default account get sudo role 10

5.2.1 Key issue detail 10

5.2.2 Security threats 10

5.2.3 Potential security requirements 11

5.3 Key Issue #3: The O-RU controller must keep track of locally defined users in each managed O-RU 11

5.3.1 Key issue detail 11

5.3.2 Security threats 11

5.3.3 Potential security requirements 11

5.4 Key Issue #4: How to get initial configuration to Central Server? 11

5.4.1 Key issue detail 11

5.4.2 Security threats 12

5.4.3 Potential security requirements 12

5.5 Key Issue #5: How does the O-RU connect securely to the Central Server? 12

5.5.1 Key issue detail 12

5.5.2 Security threats 12

5.5.3 Potential security requirements 12

5.6 Key Issue #6: Availability of the centralized user management server for the O-RUs 12

5.6.1 Key issue detail 12

5.6.2 Security threats 13

5.6.3 Potential security requirements 13

5.7 Key Issue #7: Categorisation of users that need to centrally and locally managed 13

5.7.1 Key issue detail 13

5.7.2 Security threats 13

5.7.3 Potential security requirements 13

5.8 Key Issue #8: Fetching initial security configuration data from a Software and Configuration Server 14

5.8.1 Key issue detail 14

5.8.2 Security threats 14

5.8.3 Potential security requirements 14

5.9 Key Issue #9: Secure transport to the centralized authentication server 14

5.9.1 Key issue detail 14

5.9.2 Security threats 14

5.9.3 Potential security requirements 14

5.10 Key Issue #10: Secure storage of O-RU credentials 15

5.10.1 Key issue detail 15

5.10.2 Security threats 15

5.10.3 Potential security requirements 15

6 Mitigations and Solutions 16

6.1 Key Issue Analysis 16

6.2 Solution #1: Centralized User Management 16

6.3 Solution 2#: Initial Provisioning 16

6.4 Solution #3 High Availability 16

7 Conclusions 18

7.1 Key Issue Solution Mapping 18

Annex: Change history/Change request (history) 19

# **Foreword**

This Technical Report (TR) has been produced by O-RAN Alliance.

# **Modal verbs terminology**

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

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

# Introduction

Current M-Plane specification mandates role-based access control with local user management. This implies that the Netconf Controller must keep track of locally defined users in each managed O-RU. It also means that some default behavior must be applied during installation of an O-RU, e.g. default users pre-defined by vendor for SSH and first trusted user connecting over TLS is given “sudo” role.

In this technical report key security issues due to locally defined users in each managed O-RU are analyzed. The option of using a centralized user management is also evaluated, and solutions proposed along with the necessary security requirements.

# Scope

The contents of the present document are subject to continuing work within O-RAN and may change following formal O-RAN approval. Should the O-RAN Alliance modify the contents of the present document, it will be re-released by O-RAN with an identifying change of version date and an increase in version number as follows:

version xx.yy.zz

where:

xx: the first digit-group is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc. (the initial approved document will have xx=01). Always 2 digits with leading zero if needed.

yy: the second digit-group is incremented when editorial only changes have been incorporated in the document. Always 2 digits with leading zero if needed.

zz: the third digit-group included only in working versions of the document indicating incremental changes during the editing process. External versions never include the third digit-group. Always 2 digits with leading zero if needed.

The present document specifies the outcome of the study on O-RU Centralized User Management performed by the O-RAN Security Work Group (WG11).

# References

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

## Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non‑specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies. In the case of a reference to a 3GPP document, a non-specific reference implicitly refers to the latest version of that document in Release 18, or the latest 3GPP release prior to Release 18 that includes that document.

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] O-RAN ALLIANCE TS, “O-RAN Security Requirements and Controls Specifications”

[i.2] O-RAN ALLIANCE TS, “O-RAN Management Plane Specification”

[i.3] 3GPP TS 28.314: "Management and orchestration; Plug and Connect; Concepts and requirements".

[i.4] 3GPP TS 28.315: "Management and orchestration; Plug and Connect; Procedure flows".

[i.5] 3GPP TS 28.316: "Management and orchestration; Plug and Connect; Data formats".

[i.6] O-RAN ALLIANCE TR, “O-RAN Security Threat Modeling and Risk Assessment

[i.7] 3GPP TR 21.905: “Vocabulary for 3GPP Specifications”.

[i.8] 3GPP TS 33.117: "Catalogue of general security assurance requirements"

[i.9] 3GPP TS 28.314: "Management and orchestration; Plug and connect; Concepts and requirements”

[i.10] 3GPP TS 28.315: "Management and orchestration; Plug and connect; Procedure flows”

# Definitions and Abbreviations

## Terms

For the purposes of the present document, no new terms are used.

## Definitions

For the purposes of the present document, no new definitions are defined.

## Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [i.1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [i.7].

AAS Active Antenna System

eNB e NodeB (applies to LTE)

gNB g NodeB (applies to NR)

O-DU O-RAN Distributed Unit

O-RU O-RAN Radio Unit

SCS Software and Configuration Server

# Background

## Netconf Access Control

Netconf access control is defined in the WG4 M-Plane Specification [i.2] to be used in the O-RU, but only with local user management configuration in each O-RU.

Netconf access control is also used on the O1 interface. The WG11 Security Requirements and Controls Specification [i.1] defines, for O1 entities, that (REQ-NAC-FUN-9): Netconf endpoints SHALL support external user to group mapping via at least one of the following protocols: LDAP with StartTLS, OAuth 2.0, RADIUS with EAP, and TACACS/TACACS+.

## Software and Configuration Server (SCS)

The 3GPP TS 28.314 [i.3] and TS 28.315 [i.4] describes the SCS as an entity and how it can be used in a Plug and Connect use case to provide initial configuration to a Network Element. The O-RU can be seen as a Network Element that during the provisioning needs to get configuration and find an O-RU controller.

The 3GPP TS 28.316 [i.5] describes how a Network Element can get the address to an SCS from a DHCP server.

The WG4 M-Plane Specification [i.2] clause on “Start-up installation” currently does not include the use of an SCS.

# Key Issues

This clause details the key issues identified for security aspects related to user management in the O-RU.

## Key Issue #1: Default account in O-RU

### Key issue detail

Current M-plane specification [i.2] requires a vendor specific default account. Default accounts should be avoided if possible.

The 3GPP TS 33.117 [i.8] section 4.2.3.4.2.2 states that predefined accounts shall be deleted or disabled. “*Should this measure not be possible the accounts shall be locked for remote login*“.

### Security threats

* An attacker can log on to the O-RU in these cases: The vendor defined default account (username/password) is leaked.
* Any entity that is connecting using an accepted certificate using
  + any operator-signed certificate verified by an installed trust anchor or
  + any certificate if the enrollment failed and the O-RU supports the optional feature of using its pre-installed vendor-signed certificate for setting up mTLS connections to its O-RU Controller(s) (see [i.2], clause 6.2.6.3), as in this case the O-RU does not have an installed trust anchor.

An attacker can use a successful log-on to connect to the O-RU before the connection to the O-RU controller is established. New accounts can be created.

If the default account is not being disabled, it can be used to connect and modify existing configuration.

### Potential security requirements

To mitigate the threat of an attacker using a default account to create additional accounts, the O-RU controller can verify that no unwanted accounts exist. This can be done every time when the O-RU Controller connects to an O-RU by comparing the O-RU user account configuration with the planned settings. An alternative is to avoid using a default account and rely on centralized user management during provisioning.

## Key Issue #2: Default account get sudo role

### Key issue detail

Current M-plane specification requires that when first connection is made, the first (i.e. default) user get sudo role by default. Default accounts should be avoided if possible.

### Security threats

The security threats identified with first connected user getting sudo role:

An Attacker can connect using

* any operator-signed certificate verified by an installed trust anchor or
* any certificate if the enrollment failed and the O-RU supports the optional feature of using its pre-installed vendor-signed certificate for setting up mTLS connections to its O-RU Controller(s) (see [i.2], clause 6.2.6.3), as in this case the O-RU does not have an installed trust anchor or
* a leaked default username/password

will get “sudo” role. This can be used to connect to the O-RU before the connection to the O-RU controller is established. New accounts can be created.

If the default account is not disabled, it can also be used after the connection to the O-RU controller is established to connect and modify existing configuration.

### Potential security requirements

To mitigate the threat of an attacker using a default account, get “sudo” role and creates additional accounts, the O-RU controller can verify that no unwanted accounts exist. An alternative is to avoid using a default account and rely on centralized user management during provisioning.

## Key Issue #3: The O-RU controller must keep track of locally defined users in each managed O-RU

### Key issue detail

Current M-plane specification defines role-based access control configured in each O-RU. Allowing for centralized user management would simplify management.

### Security threats

The security threats identified with only local user management in O-RU, configured by the O-RU controller:

* If the same user configuration is used in all O-RUs, any O-RU controller can connect to any O-RU. Changes will have to be performed on every O-RU.

### Potential security requirements

To simplify management a centralized user management system can be used.

## Key Issue #4: How to get initial configuration to Central Server?

### Key issue detail

When the O-RU is started for the first time, it will not have any operator specific configuration on how to connect to the central server. To use centralized user management this configuration is required.

### Security threats

The security threats identified with the O-RU not having any operator specific configuration to use centralized user management:

* If the O-RU does not know the address to the Central AA server (e.g. LDAP) it will revert to the use of locally defined users, i.e. issue 1-3

### Potential security requirements

The O-RU can get this data from one of the entities that it connects to during provisioning, i.e. DHCP, DNS and RA/CA, or from a new entity, e.g. SCS.

## Key Issue #5: How does the O-RU connect securely to the Central Server?

### Key issue detail

The O-RU must have options to connect securely to the central server.

### Security threats

The security threats identified with O-RU not having a secure connection to the centralized user management server:

* Without a secure connection, the Central AA server (e.g. LDAP) can be fake
* Without a secure connection, the transferred response from the central AA server can be tampered

### Potential security requirements

The connection to the centralized server should be authenticated and should be confidentiality and integrity protected.

## Key Issue #6: Availability of the centralized user management server for the O-RUs

### Key issue detail

The centralized user management server should be available at all times. Hence the need to cover the below aspects

* Overloading of centralized server
  + Number of RUs connected to the server
  + Frequency of making Authentication and Authorization calls
  + Number of users that are managed centrally for the O-RU
* Network connectivity
  + Connectivity loss between the O-RU and centralized server
* SW/HW failure of centralized server
  + The centralized server might be unavailable due to a software or HW failure and hence needs to be highly available

### Security threats

* Slow response of the centralized server due to overloading
* Unavailability of the centralized server due to overloading
* No response due to network disconnection
* No response due to SW/HW failure of the centralized server

### Potential security requirements

* Load model to be defined to ensure no overloading of the centralized server
* Reliable connectivity between the O-RU and the centralized server
* High availability of the centralized server
* In case the connectivity to the central server is not available, local users to be activated and used until the connectivity is resolved

## Key Issue #7: Categorisation of users that need to centrally and locally managed

### Key issue detail

The purpose of centralized user management is to have effective administration and accountability of O-RU users. It is recommended that the users of the O-RU are being categorized into central and local users to ensure that centrally administered users are kept at a maximum and local users are at a minimum with a well defined need.

### Security threats

* O-RU user information could be mismanaged, classifying users managed centralized as local users, defeating the purpose of central authentication, authorization and administration.

### Potential security requirements

* Categorisation of central and local users for the O-RU
* Minimise the usage of local users and maximise the usage of central users

When a user connects to a O-RU, first check if the user exists in central server, if no user found then check locally

## Key Issue #8: Fetching initial security configuration data from a Software and Configuration Server

### Key issue detail

The SCS is a server that can provide initial configuration data to an O-RU before first connection to an O-RU Controller similar to what is described in 3GPP TS 28.314 [9] and TS 28.315 [10]. The O-RU can get the address to the SCS from the DHCP server.

The initial configuration data can be security related data such as the address to a central AA server, trusted certificates etc.

### Security threats

The security threats identified with O-RU fetching initial configuration from SCS:

* Without a secure connection, the SCS can be fake.
* Without a secure connection, the configuration data can be tampered with in transit.
* Without trust information, e.g. a trusted certificate, the O-RU cannot verify that the SCS is ok. This is however the same risk as the O-RU has with the O-RU Controller in current specification.

### Potential security requirements

The connection to the SCS server that can provide initial configuration data to an O-RU should be authenticated and should be confidentiality and integrity protected.

## Key Issue #9: Secure transport to the centralized authentication server

### Key issue detail

Data in transit can be intercepted between the O-RU and the central server. From this perspective, there should be options of secure transport for the reason that credentials will be shared for authentication and authorization purposes which should not be compromised. There is a possibility to also have a compromised central server.

### Security threats

* Security related credentials required for authentication and authorization purpose between the O-RU and the central server could be compromised. ([i.1] T-O-RAN-08)
* Threats to compromised central server

### Potential security requirements

To protect against malicious activity on the transport between the O-RU and central server, the service interface should provide for

* Confidentiality: protect the data transferred against eavesdropping
* Integrity: protect the data transferred against malicious change
* Authenticity: mutually authenticate both endpoints (O-RU and central server)

As an option, secure and efficient standard protocols could be considered from the below to guard against the above threats

* LDAPS
* OpenID and OAuth
* RADIUS due to the presence of Netconf/Yang on the O-RUs

## Key Issue #10: Secure storage of O-RU credentials

### Key issue detail

Improper or missing controls for protection of security credentials at rest, generated by O-RAN components, may not allow a correct and rapid audit in case of a security incident occurrence. Security restoration is delayed. Missing availability and integrity of security credentials could lead to delays, wrong results, delays in security restoration and threat persistence ([i.1] §5.4.1.1). A secure mechanism for storing the credentials of the O-RU in the central server should be required. The credentials of the O-RU could be

* Username and password
* Certificates
* Tokens

### Security threats

* O-RU related credentials could be compromised by an attacker if the storage is not secure. The important aspect is that as all the data is stored centrally and the entire network could be potentially sabotaged if not secured. ([i.1] T-O-RAN-06).

### Potential security requirements

Secure mechanism of storing various types of credentials of the O-RU

* Management of username and password centrally with salting mechanisms and a one-way hash
* Certificates centrally managed with respect to users encompassing the life cycle management of enrollment, renewal and revocation.
* Tokens created centrally in OAuth server and encrypted during motion and refreshing actions

# Mitigations and Solutions

## Key Issue Analysis

The 10 identified Key Issues can be grouped into these groups, Local User Management issues, Initial Provisioning, and Central Server Issues.

The Local User Management Issues can be mitigated by using a Centralized User Management Service, however that means that the other two groups of issues come into play.

The Key Issues with Initial Provisioning of data needed to securely connect to the central AA server can be mitigated by the services proposed for distributing Trust Anchors, i.e. Voucher based protocols, BRSKI based or SCS based solutions. It is concluded that DHCP, DNS and RA/CA methods would either not be secure or have the same Initial Provisioning issues.

The Key Issues related to the Central AA server can be mitigated by placing security requirements on the Central AA server itself. This is however not a component designed by the O-RAN Alliance specifications so only recommendations can be made to the operators.

## Solution #1: Centralized User Management

To mitigate the listed Key Issues related to Local User Management it is proposed to allow the use of centralized user management services. There are many protocols to choose from and the investigation done on this topic before setting requirements on O1, showed that it was not possible to agree on one single protocol. It is proposed to allow the same protocols on the O-RU as on the O1 entities.

NOTE: An enquiry to companies participating in WG11 meetings resulted in a change proposal towards the O1 requirement where LDAP with StartTLS was selected as the primary choice of protocol. Proposed requirement:

REQ-x The O-RU MAY support external user-to-groupmapping with the role based access control concept.

Proposed security controls:

CTL-y An O-RU that supports external user to group mapping should support LDAP with StartTLS, and may also support OAuth 2.0, RADIUS with EAP, and TACACS/TACACS+.

CTL-z The centralized server may be an external 3rd party system or within the ORAN reside within a SMO or O-DU (depending on hierarchical or hybrid mode).

CTL-zz The centralized server stores the necessary credentials for the O-RU in a secure manner with access control (mapping to KI10)

CTL-zx An O-RU that supports external user to group mapping may support SAML and OIDC.

## Solution 2#: Initial Provisioning

To mitigate the listed Key Issues related to Initial Provisioning of data needed to securely connect to the central AA server it is possible to use the already defined security control [i.1]:

SEC-CTL-TAP-5: An O-RAN PNF may support 3GPP SCS [66], [67], [68] for download of initial security configuration.

## Solution #3 High Availability

To mitigate the listed Key Issues related to the use of a Centralized Authentication and Authorization Server it is proposed to recommend operators to plan the deployment with high availability.

Proposed requirement:

REQ-x A Centralized Authentication and Authorization Server should support high availability

REQ-y An O-RU supports minimal local users so that they can be activated during possible disconnection due to unavailability of the centralized user management server.

# Conclusions

## Key Issue Solution Mapping

This document currently contains 10 key issues and 3 solutions proposals to address or reduce the risk associated with the key issues. A mapping of the solutions to the key issues is shown here.

Table 7.1‑1 Key Issue Solution mapping for O-RU Centralized User Management

| *Key issue* | Sol # 1 | Soln#2 | Sol #3 |
| --- | --- | --- | --- |
| *KI 1* | X |  |  |
| *KI 2* | X |  |  |
| *KI 3* | X |  |  |
| *KI 4* |  | X |  |
| *KI 5* | X |  |  |
| *KI 6* |  |  | X |
| *KI 7* |  |  |  |
| *KI 8* |  | X |  |
| *KI 9* | X |  |  |
| *KI 10* | X |  |  |

# Annex: Change history/Change request (history)

|  |  |  |
| --- | --- | --- |
| Date | Revision | Description |
| 2022.07.06 | 00.10 | First draft version |
| 2022.09.28 | 01.00 | First approved version. Key issues identified |
| 2022.11.23 | 01.01 | Included Ericsson CR0033 |
| 2023.02.13 | 01.02 | Included Nokia CR0010, CR0014, CR0015 and Ericsson CR0043 |
| 2023.02.14 | 01.03 | Updated table of contents and history |
| 2023.02.22 | 01.04 | Included Nokia CR0040 and CR0041 |
| 2023.03.01 | 01.05 | Minor editorial corrections |
| 2023.03.01 | 01.06 | Corrected clause numbering |
| 2023.03.02 | 02.00.00 | Moved to new template and removed template text |
| 2023.03.09 | 02.01 | Removed O-RAN Release information as agreed in the plenary. Removed the duplicated Key Issue |
| 2023.07.06 | 03.00 | Added approved CRs to v02.01 |
| 2023.10.02 | 03.01 | Included Nokia CR0108, Nokia CR0109 and NEC CR0003 |
| 2023.11.08 | 01.00.00 | First external version. Renamed to follow naming convention for external documents. |
| 2024.03.06 | R003-v01.00 | Included NEC CR0010, NEC CR0014 |
| 2024.06.19 | R004-v00.01 | Preliminary version for R004 release |
| 2024.06.19 | R004-v00.02 | Included Ericsson CR0143 |
| 2024.07.24 | R004-v03.00 | Final version for July release 2024 |
| 2024.11.05 | R005-v04.00.01 | Included NEC CR0028, ERI CR0169 |
| 2024.11.06 | R005-v04.00.02 | Editorial changes |
| 2024.11.27 | R005-v04.00.03 | Editorial changes |
| 2024.12.03 | R004-v04.00 | Final version for November release 2024 |