1

O-RAN Operations and Maintenance Interface Specification V02.00

Revision History

Date	Revision	Author	Description
2019.03.18	0.01.00.00	David Kinsey (AT&T) Li Xiang(CMCC), Cagatay Buyukkoc (AT&T), Lyndon Ong (Ciena), Marge Hillis (Nokia) and Linda Horn (Nokia)	First draft of O-RAN OAM Interface Specification
2019.03.28	0.01.01.00	Marge Hillis (Nokia)	Updates from review remarks received
2019.05.21	0.01.01.01	Marge Hillis (Nokia)	Fault Supervision, Performance Assurance and File Management updates
2019.05.28	0.01.01.02	Marge Hillis, Linda Horn (Nokia)	References, Abbreviations, Definitions, Provisioning, Communication Surveillance, PNF Start Up and Registration updates
2019.06.13	0.01.01.03	Marge Hillis, Linda Horn (Nokia), David Kinsey (ATT)	Diagrams for File Management converted to UML, Performance Assurance UML, PNF Software Management Updates
2019.06.17	0.01.01.04	Marge Hillis, Linda Horn	Provisioning Updates
2019.07.01	v01.00	Marge Hillis, Linda Horn	Review Comments Addressed TSC approved copy
2019.09.27	02.00	Marge Hillis, Linda Horn	Updates for late review comments, additional CM notifications, NETCONF requirements and updated references to 3GPP SA5 Rel-16.

Contents

Revision History 2

Chapter 1. Introductory Material 5
1.1 Scope 5
1.2 References 5
1.3 Definitions and Abbreviations 6
1.3.1 Definitions 6
1.3.2 Abbreviations 7
1.4 Philosophy 7
1.5 Open Points 8
1.6 General Requirements 8
1.6.1 Service Management and Orchestration (SMO) 8
1.6.2 Transport Layer Security (TLS) 8
1.6.3 HyperText Transfer Protocol (HTTP) 8

Chapter 2. Management Services 9
2.1 Provisioning Management Services 9
2.1.1 General NETCONF Requirements 9
2.1.2 Create Managed Object Instance 9
2.1.3 Modify Managed Object Instance Attributes 12
2.1.4 Delete Managed Object Instance 14
2.1.5 Read Managed Object Instance Attributes 16
2.1.6 Notify Managed Object Instance Attribute Value Change 17
2.1.7 Notify Managed Object Instance Creation 18
2.1.8 Notify Managed Object Instance Deletion 19
2.2 Fault Supervision Management Services 20
2.2.1 Fault Notification 20
2.2.2 Fault Supervision Control 22
2.3 Performance Assurance Management Services 22
2.3.1 Performance Data File Reporting 22
2.3.2 Performance Data Streaming 24
2.3.3 Performance Assurance Control 24
2.4 Trace Management Services 24
2.4.1 Trace Data Reporting 24
2.4.2 Trace Session Activation 25
2.4.3 Trace Session Deactivation 25
2.4.4 Trace Recording Session Activation 25
2.4.5 Trace Recording Session Deactivation 25
2.5 File Management Services 26
2.5.1 File Ready Notification 26
2.5.2 List Available Files 27
2.5.3 File Transfer by File Management MnS Consumer 28
2.5.4 Download File 29
2.6 Communication Surveillance Management Services 31
2.6.1 Heartbeat Notification 31
2.6.2 Communication Surveillance Control 32
2.7 PNF Startup and Registration Management Services 33
2.7.1 PNF Plug-n-Play 34
2.7.2 PNF Registration 34
2.8 PNF Software Management Services 35
2.8.1 Software Package Naming and Content 35
2.8.2 Software Inventory 36
2.8.3 Software Download 37
2.8.4 Software Activation Pre-Check 39
2.8.5 Software Activate 40

Annex ZZZ O-RAN Adopter License Agreement 44
2.9 Section 1: DEFINITIONS 44
2.10 Section 2: COPYRIGHT LICENSE 44
2.11 Section 3: FRAND LICENSE 44
2.12 Section 4: TERM AND TERMINATION 45
2.13 Section 5: CONFIDENTIALITY 45
2.14 Section 6: INDEMNIFICATION 45
2.15 Section 7: LIMITATIONS ON LIABILITY; NO WARRANTY 46
2.16 Section 8: ASSIGNMENT 46
2.17 Section 9: THIRD-PARTY BENEFICIARY RIGHTS 46
2.18 Section 10: BINDING ON AFFILIATES 46
2.19 Section 11: GENERAL 46

Chapter 1. Introductory Material

1.1 Scope

This Technical Specification has been produced by the O-RAN.org.

The contents of the present document are subject to continuing work within O-RAN WG1 and may change following formal O-RAN approval. Should the O-RAN.org modify the contents of the present document, it will be re-released by O-RAN Alliance with an identifying change of release date and an increase in version number as follows:

Release x.y.z

where:

- x the first digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc. (the initial approved document will have x=01).
- y the second digit is incremented when editorial only changes have been incorporated in the document.
- z the third digit included only in working versions of the document indicating incremental changes during the editing process.

This document defines O-RAN OAM interface functions and protocols for the O-RAN O1 interface. The document studies the functions conveyed over the interface, including management functions, procedures, operations and corresponding solutions, and identifies existing standards and industry work that can serve as a basis for O-RAN work.

This document will follow the requirements specification language defined in IETF (RFC2119 updated by RFC 8174). For consistency requirements are specified using “SHALL” to indicate that the implementation is required.

1.2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in Release 15.

[1] 3GPP TR 21.905: Vocabulary for 3GPP Specifications

[2] 3GPP TR 28.890: Management and orchestration; Study on integration of Open Network Automation Platform (ONAP) and 3GPP management for 5G networks

[3] 3GPP TS 28.530: “Management and orchestration; Concepts, use cases and requirements”

[4] 3GPP TS 28.531: Management and orchestration; Provisioning

[5] 3GPP TS 28.532: Management and orchestration; Generic management services

[6] 3GPP TS 28.533: Management and orchestration: Architecture framework

[7] 3GPP TS 28.540: Management and orchestration; 5G Network Resource Model (NRM); Stage 1

[8] 3GPP TS 28.541: Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3

[9] 3GPP TS 28.545: Management and orchestration; Fault Supervision (FS)

[10] 3GPP TS 28.550: Management and orchestration; Performance assurance

[11] 3GPP TS 28.552: Management and orchestration; 5G performance measurements

[12] 3GPP TS 28.554: Management and orchestration; 5G end to end Key Performance Indicators (KPI)

[13] 3GPP TS 28.621: Telecommunication management; Generic Network Resource Model (NRM) Integration Reference Point (IRP); Requirements

[14] 3GPP TS 28.622: Telecommunication management; Generic Network Resource Model (NRM) Integration Reference Point (IRP); Information Service (IS)

[15] 3GPP TS 32.341: Telecommunication management; File Transfer (FT) Integration Reference Point (IRP); Requirements

[16] 3GPP TS 32.342: Telecommunication management; File Transfer (FT) Integration Reference Point (IRP); Information Service (IS)

[17] 3GPP TS 32.346: Telecommunication management; File Transfer (FT) Integration Reference Point (IRP): Solution Set (SS) definitions

[18] 3GPP TS 32.421: Telecommunication management; Subscriber and equipment trace; Trace concepts and requirements

[19] 3GPP TS 32.422: Telecommunication management; Subscriber and equipment trace; Trace control and configuration management

[20] 3GPP TS 32.423: Telecommunication management; Subscriber and equipment trace; Trace data definition and management

[21] 3GPP TS 32.508: Telecommunication management; Procedure flows for multi-vendor plug-and-play eNode B connection to the network

[22] 3GPP TS 32.509: Telecommunication management; Data formats for multi-vendor plug and play eNode B connection to the network

[23] 3GPP TS 38.401: NG-RAN; Architecture description

[24] 3GPP S5-193519: Add RESTful HTTP-based solution set of fault supervision for integration with ONAP VES

[25] 3GPP S5-191413: Integration of ONAP and 3GPP 5G management framework

[26] 3GPP S5-191461: Overview of the 5G specification structure

[27] 3GPP S5-192073: Heartbeat and Communication Surveillance

[28] O-RAN Whitepaper

[29] ORAN-WG4.MP.0-v01.00: O-RAN Alliance Working Group 4 Management Plane Specification

[30] O-RAN WG1 Operations and Maintenance Architecture v01.00

[31] ONAP VES Event Listener Specification V7.1

[32] RFC 6241, “Network Configuration Protocol (NETCONF)”, IETF, June 2011

[33] RFC 7950, “The YANG 1.1 Data Modeling Language”, IETF, August 2016

[34] RFC 2119, “Key words for use in RFCs to Indicate Requirement Levels”, IETF, March 1997

[35] RFC 8174, “Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words”, IETF, May 2017

1.3 Definitions and Abbreviations

1.3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

1.3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [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 [1].

3GPP	3rd Generation Partnership Project
EMS	Element Management System
FCAPS	Fault, Configuration, Accounting, Performance, Security
IOC	Information Object Class
JSON	JavaScript Object Notation
MANO	Management and Orchestration
ME	Managed Element
MF	Managed Function
MnS	Management Service
MO	Managed Object
MOC	Managed Object Class
MOI	Managed Object Instance
NAT	Network Address Translation
Near-RT RIC	O-RAN near real time RAN Intelligent Controller
NMS	Network Management System
Non-RT RIC	O-RAN non real time RAN Intelligent Controller
O-CU-CP	O-RAN Central Unit – Control Plane.
O-CU-UP	O-RAN Central Unit – User Plane
O-DU	O-RAN Distributed Unit
O-RAN	Open Radio Access Network
O-RU	O-RAN Radio Unit
ONAP	Open Network Automation Platform
OSM	Open Source Mano
PNF	Physical Network Function
RAN	Radio Access Network
RRH	Remote Radio Head
TR	Technical Report
TS	Technical Specification
SA5	Services & System Aspects Working Group 5 Telecom Management
SMO	Service Management and Orchestration
VES	VNF Event Stream
VNF	Virtualized Network Function

1.4 Philosophy

The O-RAN O1 management services follow existing standards wherever possible. The focus of this document is to identify the use cases which conform to existing standards, identify gaps in management services for O-RAN and define

needed extensions. For identified gaps, the goal is to modify the standards to include the needed O-RAN extensions and update the references in this document as the standards evolve to cover the gaps. If extensions and gaps are not specified, it is expected that the management services producers and consumers are conforming to referenced 3GPP specifications.

It is recognized that the O-RU follows the O-RAN Front-Haul m-plane specification [29] initially but will evolve over time to comply with the O1 specification supported by other O-RAN Managed Functions.

1.5 Open Points

As each Management Service is evaluated, the Use Cases and relevant specifications need to be assessed and augmented as needed to support O-RAN. The current list of Use Cases in Chapter 2 below is not exhaustive, and the list of specification references may not be complete.

Some Use Cases referred to in the standard may not be applicable to O-RAN and this needs to be addressed, as an exception.

The O1 team needs to be clear when citing a reference whether we are using it as a citation (meaning it will be strictly followed) or as a reference. Precise terminology needs to be included as this draft matures.

The O1 interfaces are defined assuming that the O-RAN OAM Architecture will ensure that Management Service Providers behind a NAT are able to communicate with their Management Service Consumer using the same interfaces as Management Service Providers not behind a NAT. The O-RAN OAM Architecture team has studied the topic and has a CR proposed for v02.00 confirming our assumption. When the document is approved this open point will be removed.

1.6 General Requirements

This section contains general requirements that are applicable to many O1 Interface Management Services.

1.6.1 Service Management and Orchestration (SMO)

REQ-SMO-FUN-1: O-RAN compliant SMOs SHALL support the O1 interfaces as defined in this document.

1.6.2 Transport Layer Security (TLS)

REQ-TLS-FUN-1: Management Service providers and consumers that use TLS SHALL support TLS v1.2 or higher.

1.6.3 HyperText Transfer Protocol (HTTP)

REQ-HTP-FUN-1: Management Service providers and consumers that use HTTP SHALL support HTTP v1.1 or higher. HTTP v2.0 is preferred.

Chapter 2. Management Services

2.1 Provisioning Management Services

Provisioning management services allow a Provisioning MnS Consumer to configure attributes of managed objects on the Provisioning MnS Provider that modify the Provisioning MnS Provider's capabilities in its role in end-to-end network services and allows a Provisioning MnS Provider to report configuration changes to the Provisioning MnS Consumer. NETCONF is used for the Provisioning Management Services to Create Managed Object Instance, Delete Managed Object Instance, Modify Managed Object Instance Attributes and Read Managed Object Instance Attributes. A REST/HTTPS event is used to notify the Provisioning MnS subscribed Consumers when a configuration change occurs.

Use cases are from 3GPP TS 28.531.

Reference documents include 3GPP TR 28.890, TS 28.531, RFC 6241, "Network Configuration Protocol (NETCONF)", IETF, RFC 7950, "The YANG 1.1 Data Modeling Language".

2.1.1 General NETCONF Requirements

REQ-GNC-FUN-1: The provisioning management service provider and consumer SHALL support the following NETCONF operations:

- get
- get-config
- edit-config
- lock
- unlock
- close-session
- kill-session

Other operations are optional.

REQ-GNC-FUN-2: The provisioning management service provider and consumer SHALL support the following NETCONF capabilities:

- writable-running
- rollback-on-error
- validate
- xpath

Other capabilities are optional.

REQ-GNC-FUN-3: The provisioning management service provider and consumer SHALL support a running datastore for NETCONF. Support for a candidate datastore is optional.

REQ-GNC-FUN-4: The provisioning management service provider and consumer SHALL support YANG1.1, defined in RFC 7950, including coexistence with YANG Version 1 as specified therein.

2.1.2 Create Managed Object Instance

2.1.2.1 Description

Provisioning MnS Consumer sends a synchronous provisioning update request to the Provisioning MnS Provider to create a Managed Object Instance (MOI) on the Provisioning MnS Provider and set its attribute values.

2.1.2.2 General NETCONF Session Requirements

Requirements are to be specified in a 3GPP spec for the Provisioning management services. Until that time, the requirements are provided in this O1 Interface Specification.

REQ-NCS-FUN-1: The provisioning management service provider SHALL have the capability to establish a NETCONF session with its authorized consumer upon request from the consumer.

REQ-NCS-FUN-2: The provisioning management service provider SHALL support an established NETCONF session until the authorized consumer terminates the session. NOTE: The consumer may want to perform multiple provisioning management services operations during a single NETCONF Session.

REQ-NCS-FUN-3: The provisioning management service provider SHALL have the capability to terminate a NETCONF session with its authorized consumer when requested to do so by the authorized consumer.

2.1.2.3 Create MOI Requirements

Requirements are to be specified in a 3GPP spec for the Create Managed Object Instance use case. Until that time, the requirements are provided in this O1 Interface Specification.

REQ-CMO-FUN-1: The provisioning management service provider SHALL have the capability to allow its authorized consumer to create MOI(s) and set attribute values of those MOIs via the NETCONF <edit-config> operation.

REQ-CMO-FUN-2: The provisioning management service provider SHALL have the capability to make the new MOI(s) persistent over a reset.

2.1.2.4 Procedures

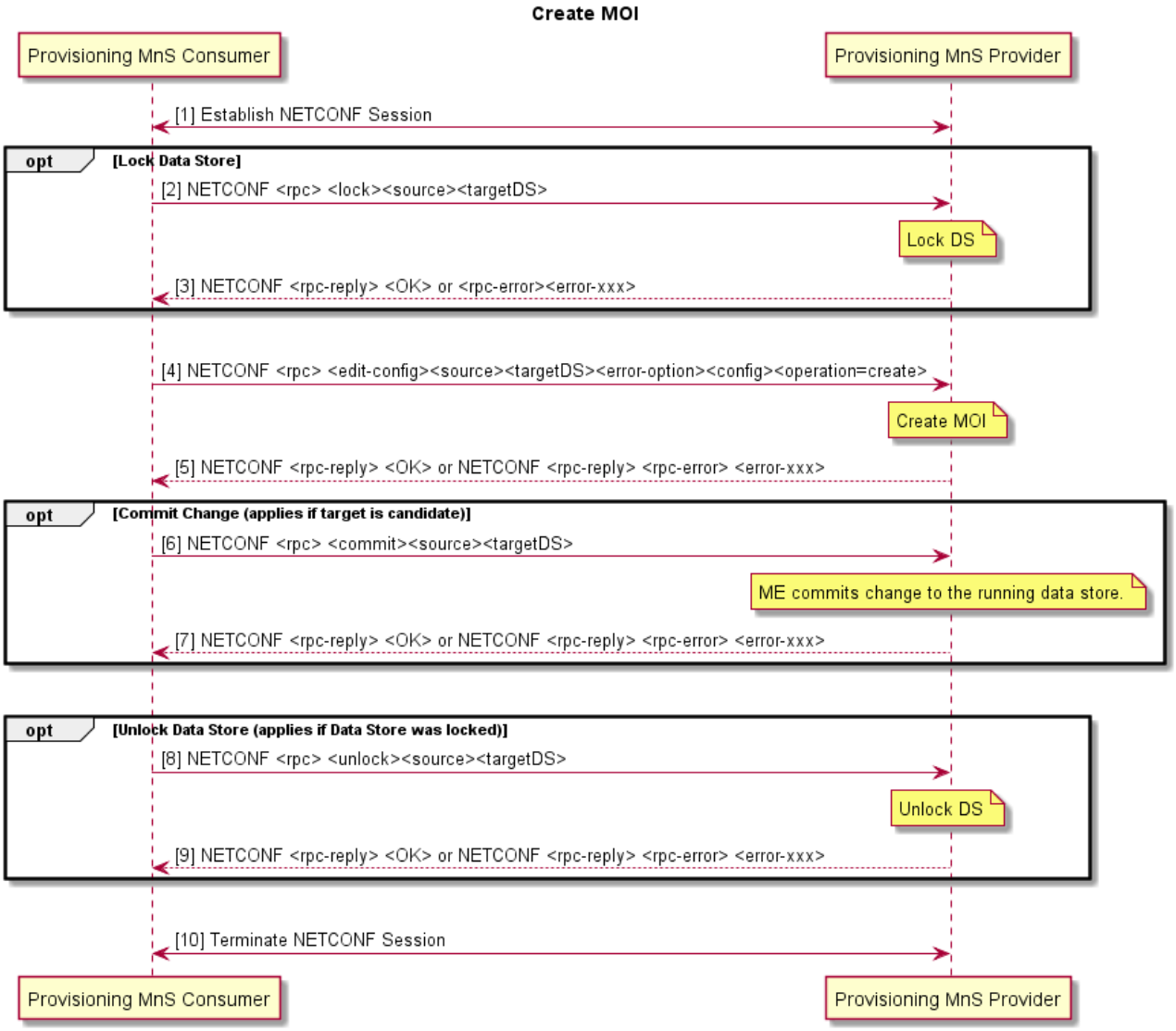

Figure 2.1.1.4-1 Creating MOIs

Pre-Condition: Provisioning MnS Consumer has current state of the target datastore of the Provisioning MnS Provider.

1. Provisioning MnS Consumer establishes NETCONF session with Provisioning MnS Provider. The NETCONF session has authorized create, read, update, and delete privileges into the identified section of the data store.

2. (Optional) Lock Datastore
    a. Provisioning MnS Consumer sends NETCONF <rpc> <lock> <source><target DS>.
    b. Provisioning MnS Provider locks target datastore (running or candidate).

3. Provisioning MnS Provider returns response <OK> or the appropriate rpc error code.

4. Create MOI
    a. Provisioning MnS Consumer sends NETCONF <rpc> <edit-config><source><targetDS><error-option><config><operation=create>.

b. Provisioning MnS Provider creates the MOI(s) and sets attribute values in the target datastore (DS) as specified in operation and config. If an error occurs, Provisioning MnS Provider behaves as specified in error-option.

5. Provisioning MnS Provider returns response <OK> or the appropriate rpc error code.

6. (Optional) Commit change if target was candidate
   a. Provisioning MnS Consumer sends NETCONF <rpc> <commit><source><targetDS>.
   b. Provisioning MnS Provider commits the change to the running DS.

7. Provisioning MnS Provider returns response <OK> or the appropriate rpc error code.

8. (Optional) Unlock Datastore
   a. Provisioning MnS Consumer sends NETCONF <rpc> <unlock><source><targetDS>.
   b. Provisioning MnS Provider unlocks the target DS.

9. Provisioning MnS Provider returns response <OK> or the appropriate rpc error code.

10. Provisioning MnS Consumer terminates NETCONF session with Provisioning MnS Provider.

2.1.3 Modify Managed Object Instance Attributes

2.1.3.1 Description

Provisioning MnS Consumer sends synchronous provisioning updates to the Provisioning MnS Provider to modify the attributes of a MOI on the Provisioning MnS Provider.

2.1.3.2 Requirements

Requirements are to be specified in a 3GPP spec for the Modify Managed Object Instance Attributes use case. Until that time, the requirements are provided in this O1 Interface Specification.

REQ-MMO-FUN-1: The provisioning management service provider SHALL have the capability to allow its authorized consumer to modify the attribute values of its MOIs via the NETCONF <edit-config> operation.

REQ-MMO-FUN-2: The provisioning management service provider SHALL have the capability to make the changes to the MOI(s) persistent over a reset.

2.1.3.3 Procedures

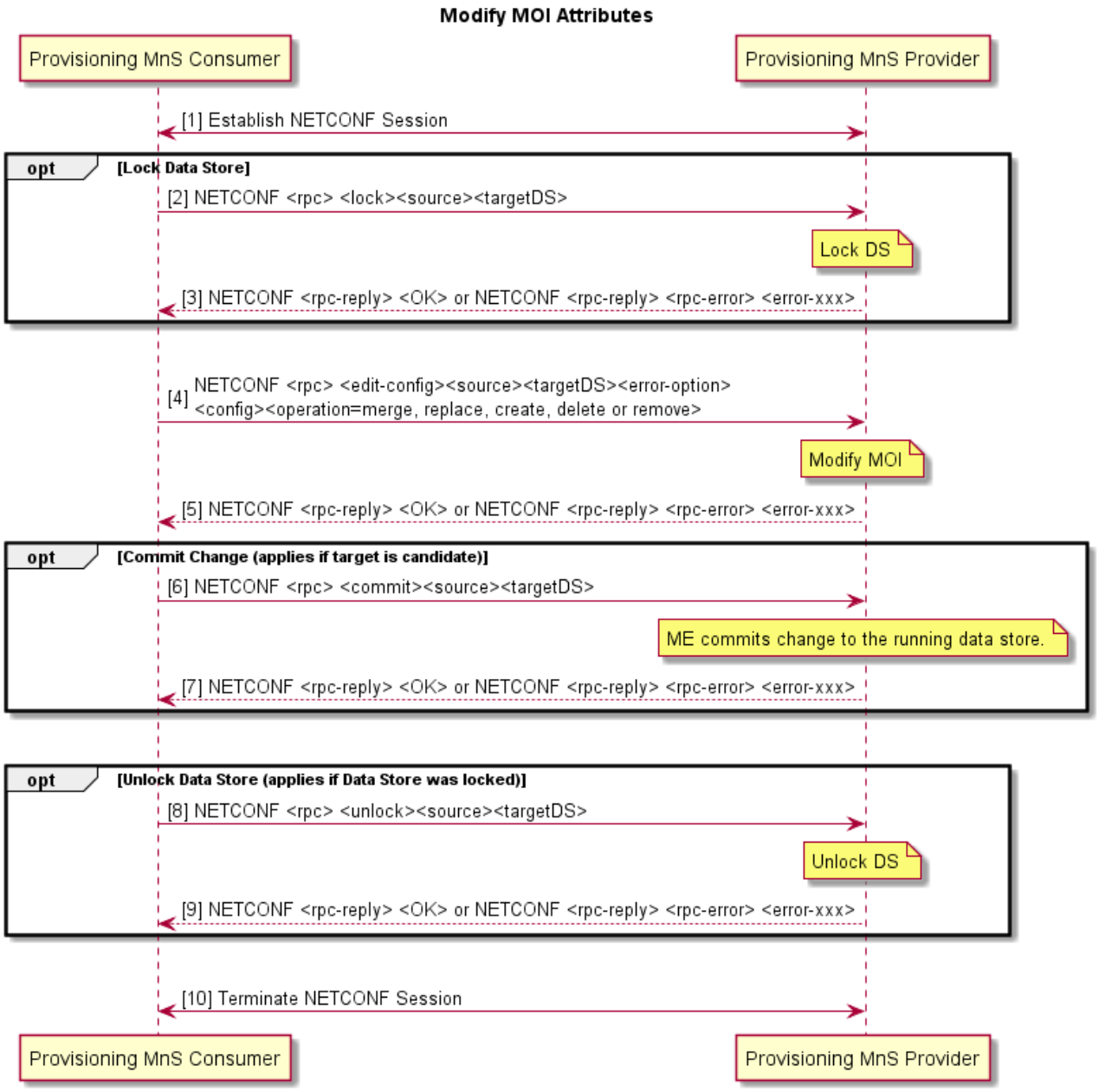

Figure 2.1.2.3-1 Modify MOI Attributes

Pre-Condition: Provisioning MnS Consumer has current state of the target datastore of the Provisioning MnS Provider.

1. Provisioning MnS Consumer establishes NETCONF session with Provisioning MnS Provider. The NETCONF session has authorized create, read, update, and delete privileges into the identified section of the data store.

2. (Optional) Lock Datastore--Provisioning MnS Consumer sends NETCONF <rpc> <lock> <source><target DS>.

a. Provisioning MnS Provider locks target datastore (running or candidate).

3. Provisioning MnS Provider returns response <OK> or the appropriate rpc error code.

4. Modify MOI Attributes
   a. Provisioning MnS Consumer sends NETCONF <rpc> <edit-config><source><targetDS><error-option><config><operation=merge, replace, create, delete or remove>.
   b. Provisioning MnS Provider modifies the attributes of the MOI(s) in the target datastore (DS) as specified in operation and config. If an error occurs, Provisioning MnS Provider behaves as specified in error-option.

5. Provisioning MnS Provider returns response <OK> or the appropriate rpc error code.

6. (Optional) Commit change if target was candidate
   a. Provisioning MnS Consumer sends NETCONF <rpc> <commit><source><targetDS>.
   b. Provisioning MnS Provider commits the change to the running DS.

7. Provisioning MnS Provider returns response <OK> or the appropriate rpc error code.

8. (Optional) Unlock Datastore
   a. Provisioning MnS Consumer sends NETCONF <rpc> <unlock><source><targetDS>.
   b. Provisioning MnS Provider unlocks the target DS.

9. Provisioning MnS Provider returns response <OK> or the appropriate rpc error code.

10. Provisioning MnS Consumer terminates NETCONF session with Provisioning MnS Provider.

2.1.4 Delete Managed Object Instance

2.1.4.1 Description

Provisioning MnS Consumer sends synchronous provisioning updates to the Provisioning MnS Provider to delete a MOI and its children on the Provisioning MnS Provider.

2.1.4.2 Requirements

Requirements are to be specified in a 3GPP spec for the Delete Managed Object use case. Until that time, the requirements are provided in this O1 Interface Specification.

REQ-DMO-FUN-1: The provisioning management service provider SHALL have the capability to allow its authorized consumer to delete its MOI(s) and its Children via the NETCONF <edit-config> operation.

REQ-DMO-FUN-2: The provisioning management service provider SHALL have the capability to make the deletions to the MOI(s)and its Children persistent over a reset.

2.1.4.3 Procedures

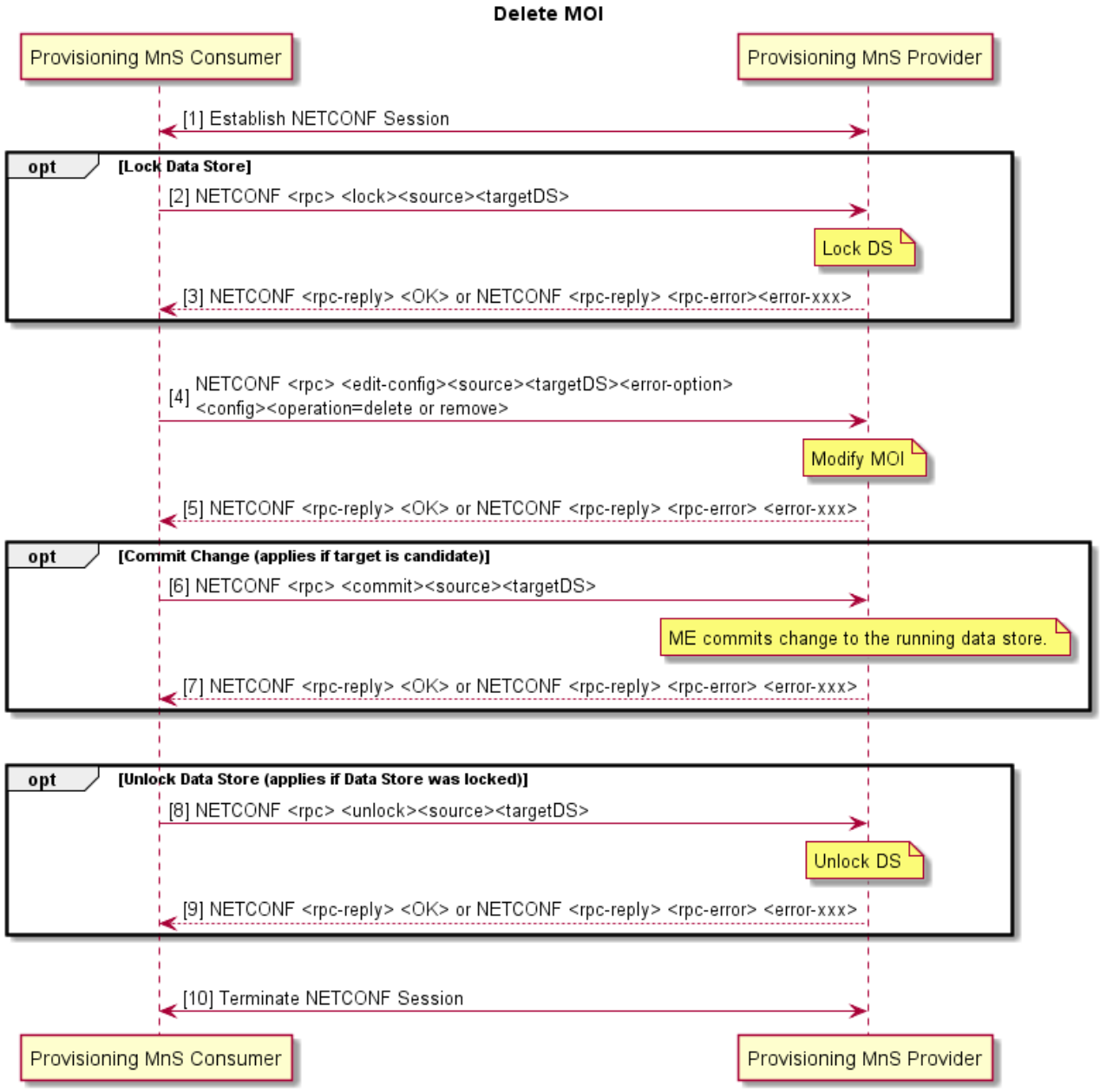

Figure 2.1.3.3-1 Deleting MOIs

Pre-Condition: Provisioning MnS Consumer has current state of the target datastore of the Provisioning MnS Provider.

1. Provisioning MnS Consumer establishes NETCONF session with Provisioning MnS Provider. The NETCONF session has authorized create, read, update, and delete privileges into the identified section of the data store.

2. (Optional) Lock Datastore
    a. Provisioning MnS Consumer sends NETCONF <rpc> <lock> <source><target DS>.
    b. Provisioning MnS Provider locks target datastore (running or candidate).

3. Provisioning MnS Provider returns response <OK> or the appropriate rpc error code.

4. Delete MOI and its Children
    a. Provisioning MnS Consumer sends NETCONF <rpc> <edit-config><source><targetDS><error-option><config><operation=delete or remove>.
    b. Provisioning MnS Provider deletes the MOI(s)and its children in the target datastore (DS) as specified in operation and config. If an error occurs, Provisioning MnS Provider behaves as specified in error-option.
    .

5. Provisioning MnS Provider returns response <OK> or the appropriate rpc error code.

6. (Optional) Commit change if target was candidate
    a. Provisioning MnS Consumer sends NETCONF <rpc> <commit><source><targetDS>.
    b. Provisioning MnS Provider commits the change to the running DS.

7. Provisioning MnS Provider returns response <OK> or the appropriate rpc error code.

8. (Optional) Unlock Datastore
    a. Provisioning MnS Consumer sends NETCONF <rpc> <unlock><source><targetDS>..
    b. Provisioning MnS Provider unlocks the target DS.

9. Provisioning MnS Provider returns response <OK> or the appropriate rpc error code.

10. Provisioning MnS Consumer terminates NETCONF session with Provisioning MnS Provider.

2.1.5 Read Managed Object Instance Attributes

2.1.5.1 Description

Provisioning MnS Consumer sends synchronous provisioning request to the Provisioning MnS Provider to return the values of attributes of its MOI(s) on the Provisioning MnS Provider.

2.1.5.2 Requirements

Requirements are to be specified in a 3GPP spec for the Read Managed Object Instance Attributes use case. Until that time, the requirements are provided in this O1 Interface Specification.

REQ-RMO-FUN-1: The provisioning management service provider SHALL have the capability to allow its authorized consumer to retrieve the values of the attributes of its MOI(s) via the NETCONF <get> or <get.config> operation.

2.1.5.3 Procedures

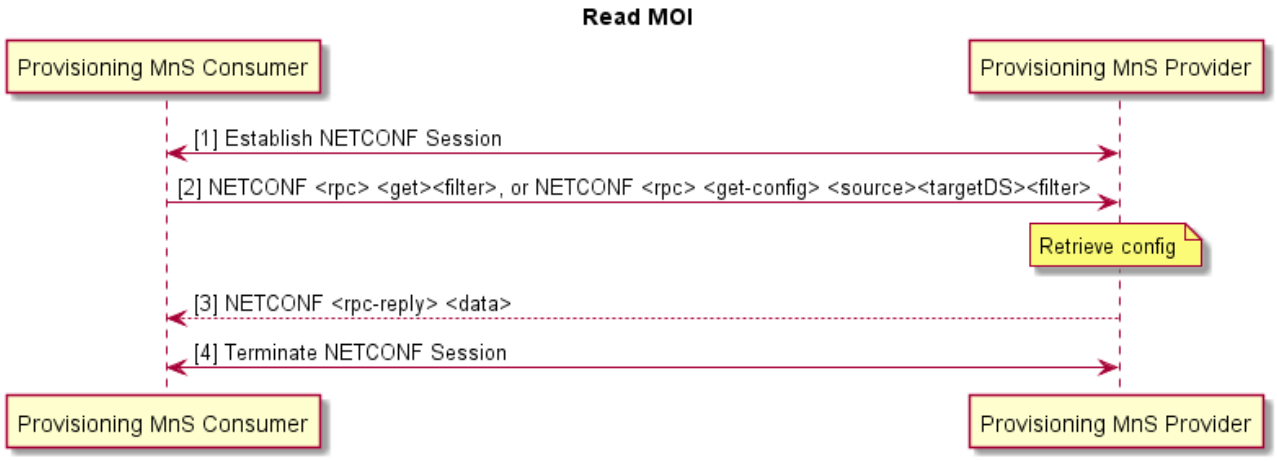

Figure 2.1.5.3-1 Read MOI

1. Provisioning MnS Consumer establishes NETCONF session with Provisioning MnS Provider.

2. Read MOI Attributes
   a. Provisioning MnS Consumer sends NETCONF <rpc> <get-config> <source><targetDS><filter> to retrieve an optionally filtered subset configuration from the source configuration datastore (running or candidate). filter can be used to identify the MOIs and attributes to be returned.

   OR

   Provisioning MnS Consumer sends NETCONF NETCONF <rpc> <get><filter> to retrieve an optionally filtered subset configuration and operational state of MOIs from the running configuration datastore. filter can be used to identify the MOIs and attributes to be returned.
   b. Provisioning MnS Provider retrieves the requested config from the specified DS.

3. Provisioning MnS Provider returns status in NETCONF response.

4. Provisioning MnS Consumer terminates NETCONF session with Provisioning MnS Provider.

2.1.6 Notify Managed Object Instance Attribute Value Change

2.1.6.1 Description

Provisioning MnS Provider sends an asynchronous notifyMOIAttributeValueChange Notification to the Provisioning MnS Consumer to report a configuration change on the Provisioning MnS Provider.

2.1.6.2 Requirements

Requirements are to be specified in a 3GPP specification for the Notify Managed Object Instance Attribute Value Change notification use case. Until that time, the requirements are provided in this O1 Interface Specification.

REQ-NMC-FUN-1: The provisioning management service provider SHALL have the capability to generate a restful asynchronous notifyMOIAttributeValueChange notification to its authorized consumer.

2.1.6.3 Procedures

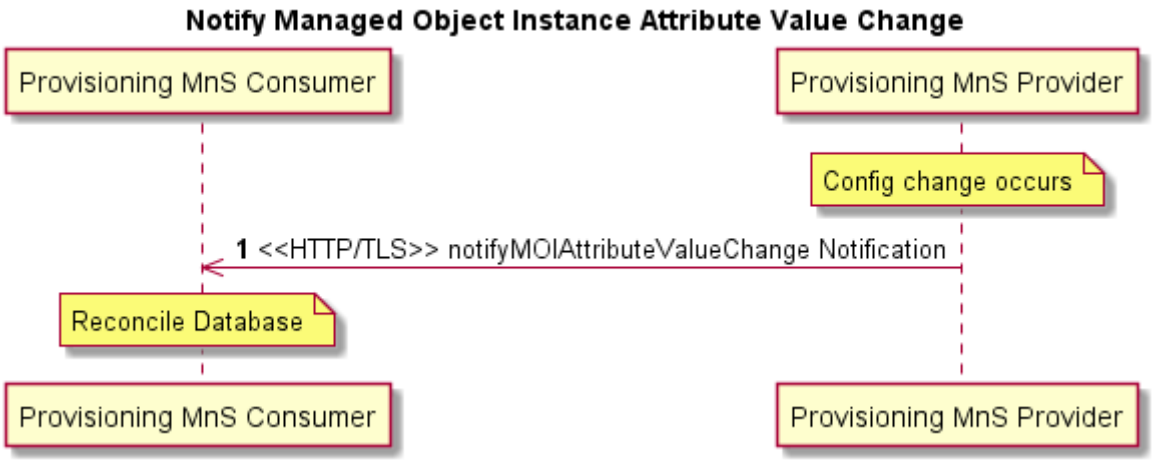

Figure 2.1.6.3-1 Notify Managed Object Instance Attribute Value Change

Pre-condition: A configuration change occurs on the running data store of the Provisioning MnS Provider.

1. Provisioning MnS Provider sends notifyMOIAttributeValueChange notification VES event to the Provisioning MnS Consumer over HTTP/TLS. Mutual certificate authentication is performed.

Post-condition: Provisioning MnS Consumer reconciles its copy of the Provisioning MnS Provider configuration database with the change.

2.1.6.4 Operations and Notifications

The notifyMOIAttributeValueChange Notification is a REST/HTTPS event sent from the Provisioning MnS Provider to the Provisioning MnS Consumer. The notification shall contain the information specified in TS 28.532 Rel-16 Section 11.1.1.9. The attributeNameValue pair is provided using YANG 1.1 encoded in JSON format as specificed in RFC 7951. . The VES event needs to be defined in 3GPP.

2.1.7 Notify Managed Object Instance Creation

2.1.7.1 Description

Provisioning MnS Provider sends an asynchronous notifyMOICreation Notification to the Provisioning MnS Consumer to report the creation of a MOI on the Provisioning MnS Provider.

2.1.7.2 Requirements

Requirements are to be specified in a 3GPP specification for the Notify Managed Object Instance Creation notification use case. Until that time, the requirements are provided in this O1 Interface Specification.

REQ-NMC-FUN-1: The provisioning management service provider SHALL have the capability to generate a restful asynchronous notifyMOICreation notification to its authorized consumer.

2.1.7.3 Procedures

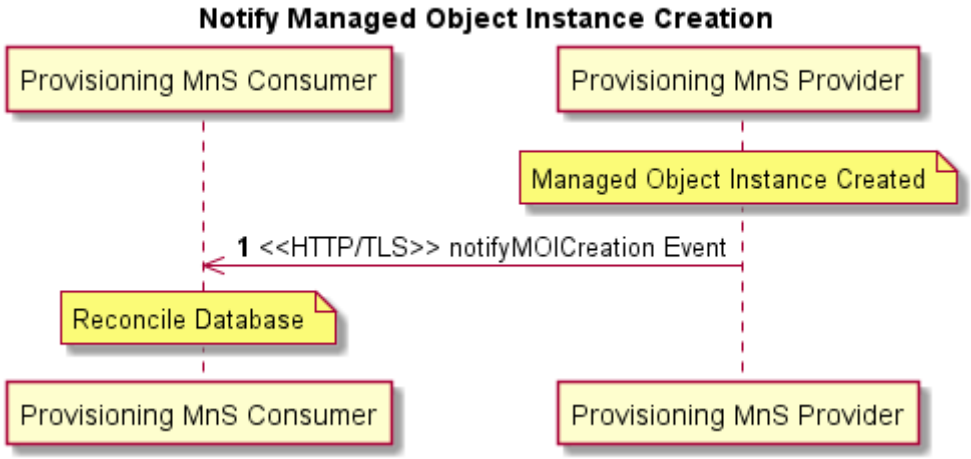

Figure 2.1.7.3-1 Notify Managed Object Instance Creation

Pre-condition: A MOI is created on the running data store of the Provisioning MnS Provider.

1. Provisioning MnS Provider sends notifyMOICreation notification VES event to the Provisioning MnS Consumer over HTTP/TLS. Mutual certificate authentication is performed.

Post-condition: Provisioning MnS Consumer reconciles its copy of the Provisioning MnS Provider configuration database with the change.

2.1.7.4 Operations and Notifications

The notifyMOICreation Notification is a REST/HTTPS event sent from the Provisioning MnS Provider to the Provisioning MnS Consumer. The notification shall contain the information specified in TS 28.532 Rel-16 Section 11.1.1.7. The VES event needs to be defined in 3GPP.

2.1.8 Notify Managed Object Instance Deletion

2.1.8.1 Description

Provisioning MnS Provider sends an asynchronous notifyMOIDeletion Notification to the Provisioning MnS Consumer to report the deletion of a MOI on the Provisioning MnS Provider.

2.1.8.2 Requirements

Requirements are to be specified in a 3GPP specification for the Notify Managed Object Instance Deletion notification use case. Until that time, the requirements are provided in this O1 Interface Specification.

REQ-NMC-FUN-1: The provisioning management service provider SHALL have the capability to generate a restful asynchronous notifyMOIDeletion notification to its authorized consumer.

2.1.8.3 Procedures

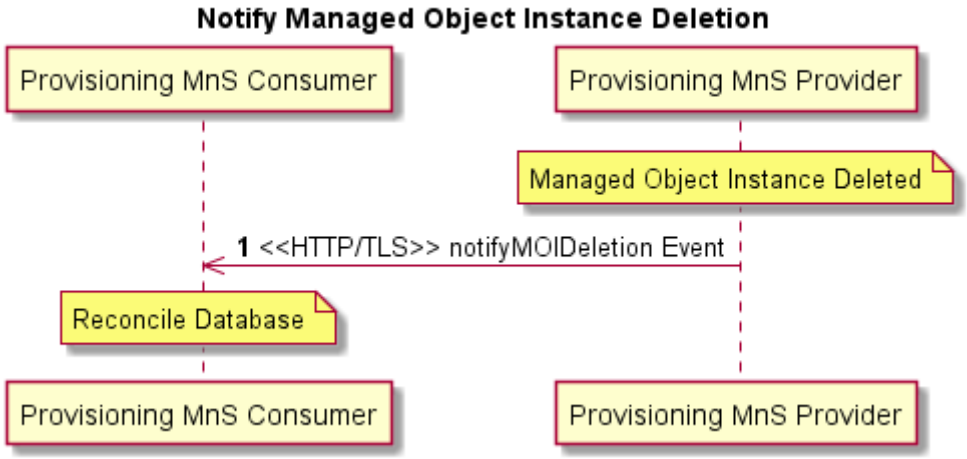

Figure 2.1.8.3-1 Notify Managed Object Instance Deletion

Pre-condition: A MOI is deleted from the running data store of the Provisioning MnS Provider.

1. Provisioning MnS Provider sends notifyMOIDeletion notification VES event to the Provisioning MnS Consumer over HTTP/TLS. Mutual certificate authentication is performed.

Post-condition: Provisioning MnS Consumer reconciles its copy of the Provisioning MnS Provider configuration database with the change.

2.1.8.4 Operations and Notifications

The notifyMOIDeletion Notification is a REST/HTTPS event sent from the Provisioning MnS Provider to the Provisioning MnS Consumer. The notification shall contain the information specified in TS 28.532 Rel-16 Section 11.1.1.8. The VES event needs to be defined in 3GPP.

2.2 Fault Supervision Management Services

Fault supervision management services allow a Fault Supervision MnS Provider to report errors and events to a Fault Supervision MnS Consumer and allows a Fault Supervision MnS Consumer to perform fault supervision operations on the Fault Supervision MnS Provider, such as get alarm list.

Use cases are specified in 3GPP TS 28.545 [9].

RESTful HTTP-based solution set of fault supervision for integration with VES API are found in TS 28.532 Rel-16 Section 12.2.2.[5]

2.2.1 Fault Notification

2.2.1.1 Description

Fault Supervision MnS Provider sends asynchronous Fault3gpp notification event to Fault Supervision MnS Consumer when an alarm occurs, is cleared, changes state or priority, etc.

2.2.1.2 Requirements

Requirements are specified in 3GPP TS 28.545 Section 5.2.5.

2.2.1.3 Procedures

Procedures are defined in 3GPP TS 28.545 Section 9.1.

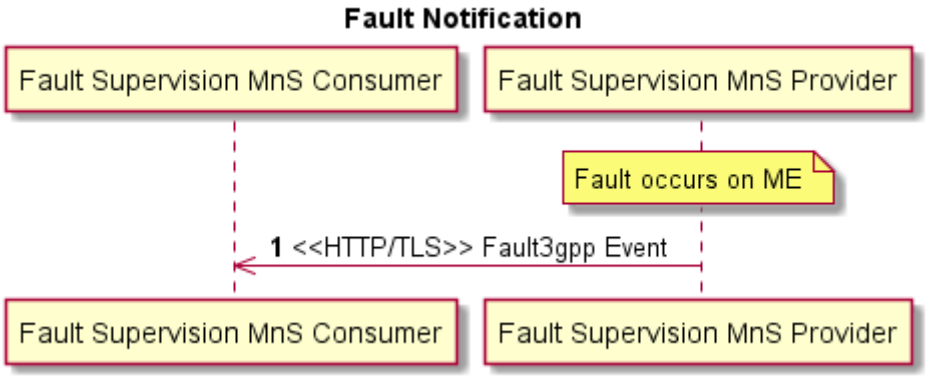

Figure 2.2.1.3-1 Fault Notification

Pre-condition: A fault occurs on the Fault Supervision MnS Provider.

1. Fault Supervision MnS Provider sends Fault3gpp notification VES event to Fault Supervision MnS Consumer over HTTP/TLS. Mutual certificate authentication is performed.

2.2.1.4 Operations and Notifications

Fault3gpp notification is a JSON encoded VES event sent from Fault Supervision MnS Provider to Fault Supervision MnS Consumers using REST/HTTPS. It consists of a Common VES Event Header and Fault3gpp Notification Fields. The fault3GPP event is specified in 3GPP TS 28.532, which provides the mapping from 3GPP IS notification parameters to the VES Common Event Header and the Fault3gpp Event Fields.

The table below is derived from TS 28.532 to provide a reference for the mapping of specific parameters for each 3GPP IS notification type to the fault3gpp Event.

Table 2.2.1.4-1

3GPP IS Notification	**TS 28.532 section Reference**
notifyNewAlarm	3GPP TS 28.532, Section 12.2.2.2.2
notifyNewSecurityAlarm	3GPP TS 28.532, Section 12.2.2.2.3
notifyAckStateChanged	3GPP TS 28.532, Section 12.2.2.2.4
notifyClearedAlarm	3GPP TS 28.532, Section 12.2.2.2.5
notifyAlarmListRebuilt	3GPP TS 28.532, Section 12.2.2.2.6
notifyChangedAlarm	3GPP TS 28.532, Section 12.2.2.2.7
notifyComments	3GPP TS 28.532, Section 12.2.2.2.8

notifyPotentialFaultyAlarmList	3GPP TS 28.532, Section 12.2.2.2.9
notifyCorrelatedNotificationChanged	3GPP TS 28.532, Section 12.2.2.2.10
notifyChangedAlarmGeneral	3GPP TS 28.532, Section 12.2.2.2.11

TS 28.532 Annex A.3 provides the JSON Schema of fault3gppFields.

2.2.2 Fault Supervision Control

2.2.2.1 Description

Starting with 3GPP Release 16, dedicated operations for Management Services Use Cases will be replaced by IOCs with attributes that can be read and/or set using generic provisioning mechanisms. For Fault Supervision, O-RAN requires the ability to Get Alarm List and Clear Alarm.

2.2.2.2 Requirements

3GPP spec should define a FaultSupervision Control IOC and FaultSupervision Reader IOC with appropriate attributes to support the required operations and submit them as a standards contribution using 3GPP TS 28.545 as a reference.

2.2.2.3 Procedures

NETCONF protocol and YANG data models are used to get and set the attributes from the FaultSupervisionControl IOC. 3GPP has not defined yet the FaultSupervisionReader and faultSupervisionControl IOCs. Refer to Provisioning management services section for examples of these definitions.

2.3 Performance Assurance Management Services

Performance Assurance Management Services allow a Performance Assurance MnS Provider to report bulk and/or real time performance data to a Performance Assurance MnS Consumer and allows a Performance Assurance MnS Consumer to perform performance assurance operations on the Performance Assurance MnS Provider, such as selecting the measurements to be reported and setting the frequency of reporting.

Use cases are specified in 3GPP TS 28.550 [10].

Alignment between 3GPP SA5 and VES is described in 3GPP TR 28.890 [2].

2.3.1 Performance Data File Reporting

2.3.1.1 Description

Performance Assurance MnS Provider sends asynchronous FileReady notification event to Performance Assurance MnS Consumer sent when PM File(s) is ready for upload. The FileReady notification contains information needed to retrieve the file such as filename and the location where the file can be retrieved.

Performance Assurance MnS Consumer uploads Bulk PM File(s) from the location specified in the notifyFileReady notification.

2.3.1.2 Requirements

Requirements are specified in 3GPP TS 28.550 section 5.2.2.

2.3.1.3 Procedures

Procedure is specified in 3GPP TS 28.550 section 5.1.1.2.

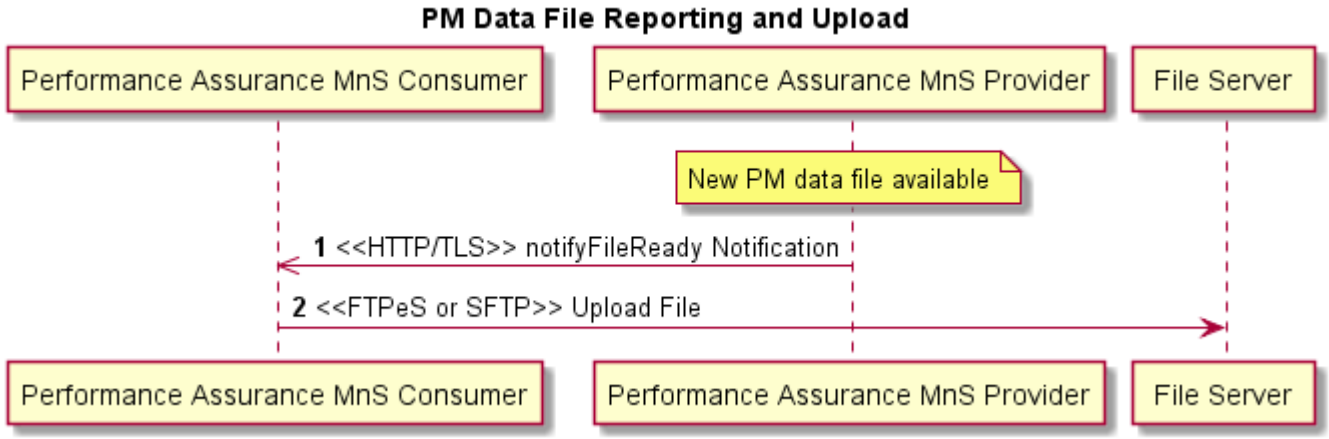

Figure 2.3.1.3-1 PM Data File Reporting and Upload

Pre-condition: A new PM data file is available on the Performance Assurance MnS Provider.

1. Performance Assurance MnS Provider sends FileReady notification VES event to Performance Assurance MnS Consumer over HTTP/TLS. Mutual certificate authentication is performed.
2. Performance Assurance MnS Consumer sets up a secure FTPeS or SFTP connection to the location specified in the notifyFileReady notification and uploads the PM data file(s). SFTP is authenticated with username/password, SSH keys or X.509 certificates. FTPES is authenticated with X.509 certificates.

2.3.1.4 Operations and Notifications

notifyFileReady notification is a JSON encoded VES event sent from Performance Assurance MnS Provider to Performance Assurance MnS Consumer using REST/HTTPS. It consists of a Common VES Event Header and notifyFileReady Notification Fields.

notifyFileReady notification event will be specified in 3GPP TS 28.532 as part of the 3GPP/VES alignment normative work. Until that time, the FileReady notification is specified in the VES Event Specification v7.1 [31].

2.3.1.5 PM File Generation and Reporting

PM file generation and reporting are specified in 3GPP 28.532 section 11.3.2.1.1.

2.3.1.6 PM File Content

PM file content is specified in 3GPP TS 28.532 section 11.3.2.1.2.

2.3.1.7 PM File Naming

PM file naming is specified in 3GPP TS 28.532 section 11.3.2.1.3.

2.3.1.8 PM File XML Format

PM file XML format is specified in 3GPP TS 28.550 Section 11.3.2.1.4.

2.3.1.9 5G Performance Measurements

3GPP defined 5G performance measurements are specified in 3GPP TS 28.552. In addition to the 3GPP-defined measurements, it is possible to have O-RAN defined measurements and vendor supplied measurements. O-RAN defined measurements are named with a “OR.” prefix. Vendor supplied measurements are named with a “VS.” prefix.

2.3.2 Performance Data Streaming

Editor's Note: This section will be updated in subsequent versions of the interface specification as 3GPP Release 16 changes are approved.

2.3.2.1 Description

Performance Assurance MnS Provider steams high volume asynchronous Real Time Performance Measurement (RTPM) data to Performance Assurance MnS Consumer at a configurable frequency.

2.3.2.2 Requirements

Requirements will be specified in a 3GPP spec.

2.3.2.3 Procedures

Procedures will be specified in a 3GPP spec.

2.3.3 Performance Assurance Control

2.3.3.1 Description

Starting with 3GPP Release 16, dedicated operations for Performance Assurance Control will be replaced by IOCs with attributes that can be read and/or set using generic provisioning mechanisms. For Performance Assurance, this includes operations such as Create Measurement Job, Terminate Measurement Job and Query Measurement Job. Measurement jobs can be created, terminated and queried by setting and/or getting attributes in the MeasurementControl and MeasurementReader IOCs.

2.3.3.2 Requirements

Measurement Control IOC is specified in 3GPP TS 28.622 [14] section 4.3.12. Measurement Reader IOC is specified in 3GPP TS 28.622 section 4.3.13. Measurement data type is specified in 3GPP TS 28.622 section 4.3.14.

2.3.3.3 Procedures

NETCONF protocol and YANG data models are used to get and/or set the MeasurementControl and MeasurementReader IOC attributes. Refer to Provisioning management services section.

2.4 Trace Management Services

Editor's Note: This section will be updated in subsequent versions of the interface specification as 3GPP Release 16 changes are approved.

Trace management services allow a Trace MnS Provider to report high volume asynchronous streaming of Subscriber and Equipment Trace data (e.g. Call, Cell, UE) to the Trace MnS Subscriber upon a triggering event and allows the Trace MnS Subscriber to configure the trace management capabilities on the Trace MnS Provider.

Use cases are based on 3GPP TS 32.421.

Relevant SA5 spec updates to 3GPP TS 32.421, 32.422, 32.423 for SBMA are targeted for Rel-16.

2.4.1 Trace Data Reporting

2.4.1.1 Description

High volume asynchronous streaming of Subscriber and Equipment Trace data (e.g. Call, Cell, UE, MDT) from Trace MnS Provider to Trace MnS Subscriber sent upon triggering event.

2.4.1.2 Requirements

Requirements will be specified in a 3GPP spec.

2.4.1.3 Procedures

Procedures will be specified in a 3GPP spec.

2.4.2 Trace Session Activation

2.4.2.1 Description

2.4.2.2 Requirements

2.4.2.3 Procedures

2.4.3 Trace Session Deactivation

2.4.3.1 Description

2.4.3.2 Requirements

2.4.3.3 Procedures

2.4.4 Trace Recording Session Activation

2.4.4.1 Description

2.4.4.2 Requirements

2.4.4.3 Procedures

2.4.5 Trace Recording Session Deactivation

2.4.5.1 Description

2.4.5.2 Requirements

2.4.5.3 Procedures

2.5 File Management Services

File management services allow a File Management MnS Consumer to request the transfer of files between the File Management MnS Provider and the File Management MnS Consumer.

Use cases are based on the O-RAN WG4 Front Haul Management Plane specification [29].

Relevant 3GPP specifications for file transfer are 3GPP TS 32.341 [15], TS 32.342 [16] and TS 32.346 [17]. O-RAN recommends that 3GPP update these specifications in SA5 Rel-17. This section will be updated when those specifications are finalized.

2.5.1 File Ready Notification

2.5.1.1 Description

The File Ready Notification notifies a File Management MnS Consumer that a file is available for upload from the File Management MnS Provider. In general, File Management MnS Provider sends a notifyFileReady notification for files that the File Management MnS Consumer has configured the File Management MnS Provider to collect on a periodic basis, such as file-based Trace Data or PM Measurement Reports.

2.5.1.2 Requirements

notifyFileReady notification event is a JSON encoded VES event, that consists of a Common VES Event Header and notifyFileReady Notification Fields. It will be specified in 3GPP TS 28.532 as part of the 3GPP/VES alignment normative work. Until that time, the VES Event Specification v7.1 specifies the FileReady notification.

2.5.1.3 Procedures

File Management MnS Consumer configures a File Management MnS Provider to collect data files with specific characteristics that the File Management MnS Consumer desires, such as file-based Trace Data or PM Measurement Reports described in the Performance Assurance Section of this document. After configuration, the File Management MnS Consumer terminates the configuration session and waits for the File Management MnS Provider to report that the file is ready for collection.

When a file is available, the File Management MnS Provider sends a notifyFileReady notification to the File Management MnS Consumer using REST/HTTPS.

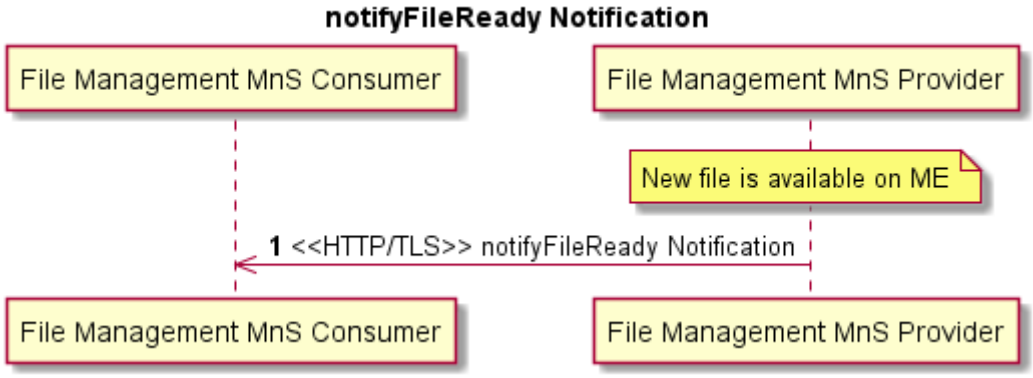

Figure 2.5.1.3-1 File Available for Transfer to Consumer

Pre-condition: A new file is available on the File Management MnS Provider.

1. File Management MnS Provider sends notifyFileReady notification to File Management MnS Consumer over HTTP/TLS. Mutual certificate authentication is performed.

2.5.1.4 Standards Additions to support O-RAN

O-RAN will contact 3GPP reps to propose that the 3GPP/VES alignment includes re-naming of some fields within the notification to provide more clarity, such as renaming the changeIdentifier field in the Notification event supporting VES FileReady to a name more aligned with the field's purpose, such as fileType or to add an additional field called fileType which can be utilized to specify the type of file available for upload. The 3GPP specification will need to be updated if O-RAN wants to put specific naming conventions on the types of files that will be available for upload.

O-RAN will request that 3GPP add FTPeS to the transport requirements supported in 3GPP TS 32.342.

2.5.1.5 File Types Supported

File Type requirements are documented in 3GPP TS 32.341 section 5.2.

2.5.1.6 File Naming Requirements

File Naming requirements are specified in 3GPP TS 32.342 Annex A.

2.5.2 List Available Files

2.5.2.1 Description

File Management MnS Consumer queries the File Management MnS Provider to identify files that are available on the File Management MnS Provider. Upon receipt of the available files and their locations, the File Management MnS Consumer can determine the next appropriate action.

2.5.2.2 Requirements

Requirements on the types of files are found in section 5.4 of 3GPP TS 32.341. O-RAN may request that additional file types be specified in Rel-17 as part of the NRM fragment creation for List Available Files.

2.5.2.3 Procedures

List Available Files Use Case allows the File Management MnS Consumer to obtain a list of available files and their locations by reading the AvailableFileList IOC as specified in 3GPP TS 32.342. A File Management MnS Consumer may use this management service in scenarios where the File Management MnS Provider is collecting information, such as logs, on a standard basis in support of debugging activities. Under normal operations, the File Management MnS Provider does not send this data to the File Management MnS Consumer as the File Management MnS Consumer does not need it. The File Management MnS Provider retains the data with the oldest data being over-written when space is exhausted. In some scenarios, the File Management MnS Consumer may want to upload some, or all, of the available log files to resolve an issue. In this case, File Management MnS Consumer sends a NETCONF <get> command to the File Management MnS Provider to obtain the list of available files. File Management MnS Provider responds with AvailableFileList which contains a list of available files and their locations and file types. File Management MnS Consumer may use this information to transfer the desired files. See Transfer File Service section 2.5.3.

The File Management MnS Consumer does not have to initiate a file upload as a result of the obtaining the list of available files. There are use cases where the File Management MnS Consumer may want to verify that files are being collected or verify that all files of a particular type (PM for example) have been uploaded.

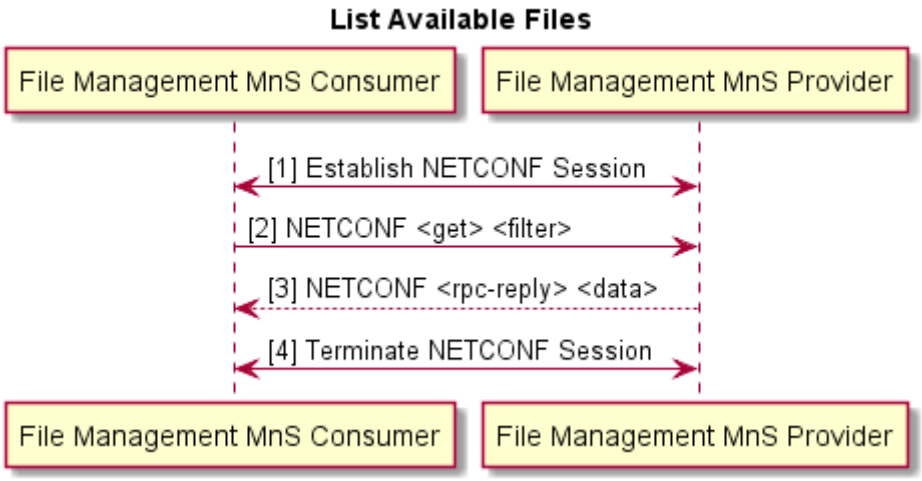

Figure 2.5.2.3-1 List Available Files

1. File Management MnS Consumer establishes NETCONF session with File Management MnS Provider.
2. File Management MnS Consumer sends NETCONF <get> <filter> to the File Management MnS Provider to retrieve the contents of the AvailableFileList.
3. File Management MnS Provider sends NETCONF <rpc-reply> <data>to the File Management MnS Consumer with list of available files on the File Management MnS Provider.
4. File Management MnS Consumer terminates NETCONF session with File Management MnS Provider.

2.5.3 File Transfer by File Management MnS Consumer

2.5.3.1 Description

The File Transfer by File Management MnS Consumer Use Case provides the capability for a File Management MnS Consumer to transfer files from or to the File Management MnS Provider. In this use case, File Management MnS Consumer is the client and File Management MnS Provider is the file server.

The File Management MnS Consumer may perform this action as a result of:

1. notifyFileReady notification from the File Management MnS Provider informing the File Management MnS Consumer that a file(s)is available
2. Querying the File Management MnS Provider for the list of available files (see section 2.5.2).
3. A need to transfer a file from a known location on the File Management MnS Provider.
4. A need to transfer a file to a known location on the File Management MnS Provider. Some examples of files that could be transferred to the FileManagement MnS Provider are:
   - Beamforming configuration file (Opaque Vendor specific data)
   - Machine Learning

- Certificates

File Transfer is performed using a secure file transfer protocol (SFTP or FTPeS) from or to the File Management MnS Provider.

2.5.3.2 Requirements

File Transfer Requirements are found in Section 5.3 of 3GPP TS 32.341.

2.5.3.3 Procedures

Case 1: File Management MnS Consumer determines that a file should be transferred from the the location provided by the File Management MnS Provider as a result of receiving a notifyFileReady notification from the File Management MnS Provider (described in 2.5.1).

Case 2: File Management MnS Consumer determines that a file should be transferred from the File Management MnS Provider as a result of receiving a list available files from the File Management MnS Provider (described in 2.5.2)

Case 3: File Management MnS Consumer determines that a file should be transferred from the File Management MnS Provider from a known location on the File Management MnS Provider.

Case 4: File Management MnS Consumer determines that a file should be transferred to the File Management MnS Provider to a known location on the File Management MnS Provider.

File Management MnS Consumer initiates a secure file transfer using FTPeS or SFTP to transfer a file from or to the File Management MnS Provider.

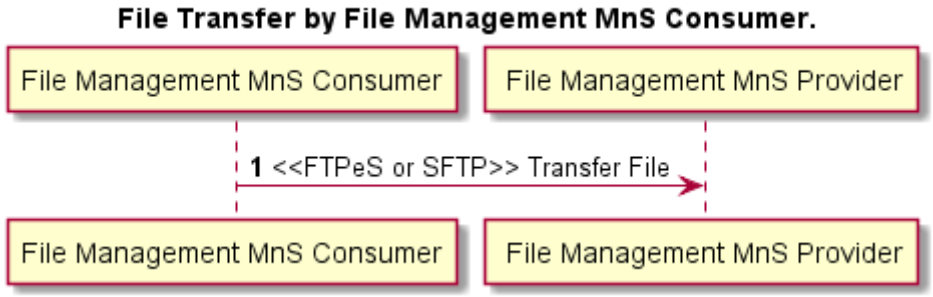

Figure 2.5.3.3-1 File Transfer by File Management MnS Consumer

2.5.4 Download File

2.5.4.1 Description

The File Management MnS Consumer has a file that needs to be downloaded to the File Management MnS Provider such as:

- Software file to upgrade software version executed on the File Management MnS Provider
- Beamforming configuration file (Opaque Vendor specific data)
- Machine Learning
- Certificates

The File Management MnS Consumer triggers the file download. The File Management MnS Provider uses a secure file transfer protocol to download the file from the location specified by the File Management MnS Consumer and then notifies the File Management MnS Consumer of the result of the download. In this use case, the File Management MnS Provider is the client. The file could be located on any File Server reachable by the File Management MnS Provider.

2.5.4.2 Requirements

General File Download requirements are found in section 5.3 of 3GPP TS 32.341.

2.5.4.3 Procedures

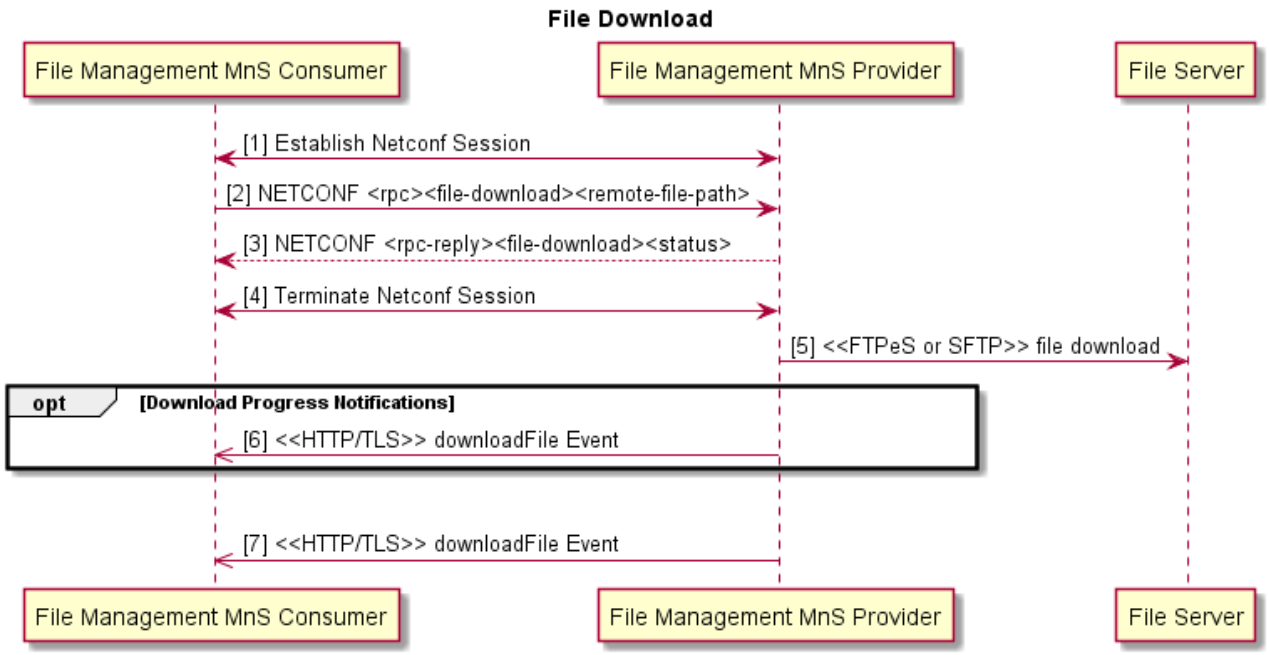

Figure 2.5.4.3-1 File Download

1. File Management MnS Consumer establishes NETCONF session with File Management MnS Provider.
2. File Management MnS Consumer sends NETCONF RPC file-download request, including the location of the file to download, to the File Management MnS Provider to trigger a file download.
3. File Management MnS Provider replies with its ability to begin the download.
4. File Management MnS Consumer terminates NETCONF session with File Management MnS Provider.
5. File Management MnS Provider sets up a secure connection and downloads the file via FTPeS or SFTP. SFTP is authenticated with username/password, SSH keys or X.509 certificates. FTPES is authenticated with X.509 certificates.
6. (Optional) If the download takes a long time, File Management MnS Provider may send periodic downloadFile notifications to the File Management MnS Consumer with the current status of the download (download in progress).
7. When download completes, File Management MnS Provider sends a downloadFile notification to the File Management MnS Consumer with the final status of the download (success, file missing, failure).

2.5.4.4 Operations and Notifications

downloadFile notification is a JSON encoded VES event sent from File Management MnS Provider to File Management MnS Consumer using REST/HTTPS. It consists of a Common VES Event Header and fileDownload Notification Fields to notify the File Management MnS Consumer of the progress and status of a file download. This event needs to be defined in VES and included in the 3GPP harmonization activity.

2.6 Communication Surveillance Management Services

Communication Surveillance MnS allow a Communication Surveillance MnS Provider to send heartbeats to the Communication Surveillance MnS Consumer and allow the Communication Surveillance MnS Consumer to configure the communication surveillance services on the Communication Surveillance MnS Provider.

Use cases are specified in 3GPP TS 32.351, TS 32.352.

Alignment between 3GPP SA5 and VES is described in 3GPP TR 28.890 and CR S5-192073 [27]. Normative work includes a new SA5 specification for Communication Surveillance based on 3GPP TS 32.352 and an update to 3GPP TS 28.532 to add the Heartbeat VES event.

2.6.1 Heartbeat Notification

2.6.1.1 Description

Communication Surveillance MnS Provider sends asynchronous heartbeat event to Communication Surveillance MnS Consumer at a configurable frequency to allow Communication Surveillance MnS Consumer to supervise the connectivity to the Communication Surveillance MnS Provider.

2.6.1.2 Requirements

Requirements are to be specified in a new 3GPP spec for Communication Surveillance as part of the 3GPP/VES alignment normative work. Until that time, the requirements are provided in this O1 Interface Specification.

REQ-HN-FUN-1: The communications surveillance management service provider SHALL have the capability to send heartbeat notifications to its authorized consumer periodically at the periodicity specified in the heartbeatPeriod attribute or whenever the countDownTimer attribute is set to 0.

REQ-HN-FUN-2: The communications surveillance management service provider SHALL allow the authorized consumer to set the destination address for the heartbeat notification.

2.6.1.3 Procedures

Procedures are to be specified in a new 3GPP spec for Communication Surveillance as part of the 3GPP/VES alignment normative work. Until that time, the procedures are provided in this O1 Interface Specification.

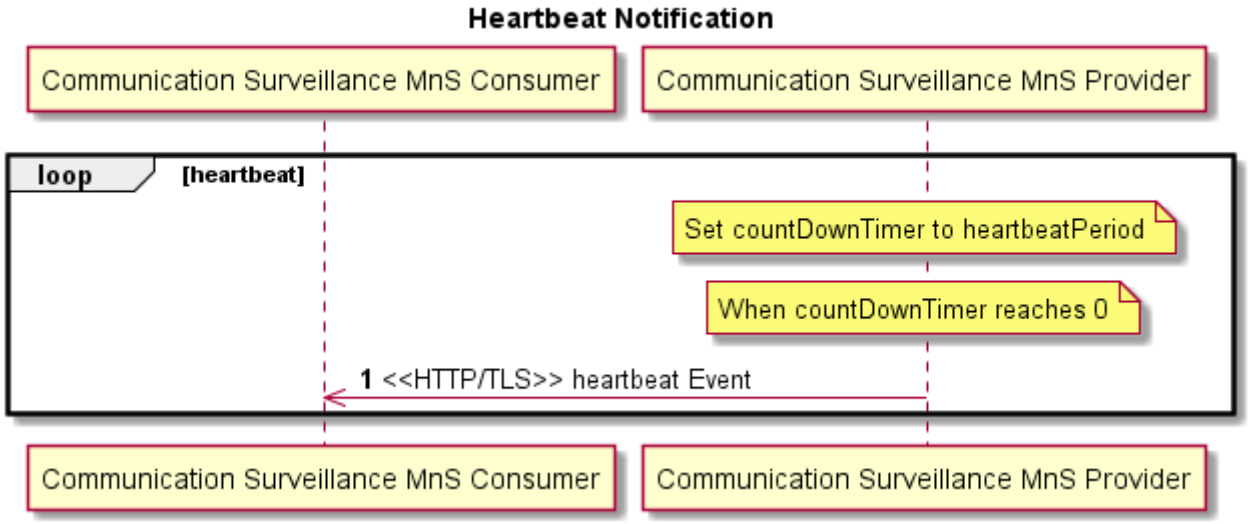

Figure 2.6.1.3-1 Heartbeat Notification

Pre-condition: heartbeatPeriod > 0

Loop

The Heartbeat notification provider sets the countDownTimer to the heartbeatPeriod.

When countDownTimer reaches 0,

1. Communication Surveillance MnS Provider sends Heartbeat notification VES event to Communication Surveillance MnS Consumer over HTTP/TLS. Mutual certificate authentication is performed.

End Loop

2.6.1.4 Operations and Notifications

Heartbeat is a JSON encoded VES event sent from Communication Surveillance MnS Provider to Communication Surveillance MnS Consumer using REST/HTTPS. It consists of a Common VES Event Header and Heartbeat Fields.

Heartbeat event will be specified in 3GPP TS 28.532 as part of the 3GPP/VES alignment normative work. Until that time, the Heartbeat event is specified in the VES Event Specification v7.1 [31].

2.6.2 Communication Surveillance Control

Starting with 3GPP Release 16, dedicated operations for Management Services Use Cases will be replaced by IOCs with attributes that can be read and/or set using generic provisioning mechanisms. For Communication Surveillance, this includes operations Set Heartbeat Period, Get Heartbeat Period, Trigger Heartbeat and Get Countdown Timer Value.

2.6.2.1 Requirements

Requirements are to be specified in a new 3GPP spec for Communication Surveillance. Until that time, the requirements are provided in this O1 Interface Specification.

REQ-CSC-FUN-1: The communication surveillance management service provider SHALL have the capability to allow its authorized consumer to set the heartbeat period.

REQ-CSC-FUN-2: The communication surveillance management service provider SHALL have the capability to allow its authorized consumer to read the current heartbeat period value.

REQ-CSC-FUN-3: The communication surveillance management service provider SHALL have the capability to allow its authorized consumer to trigger a Heartbeat Notification.

2.6.2.2 Procedures

NETCONF protocol and YANG data models are used to get and set the heartbeatPeriod and the countDownTimer in the HeartbeatControl IOC. Refer to the Provisioning management services section.

2.6.2.3 HeartbeatControl IOC Definition

HeartbeatControl IOC definition is to be specified in a new 3GPP spec for Communication Surveillance as part of the 3GPP normative work. Until that time, the IOC attributes and definitions provided in the tables below are based on 3GPP TS 32.352.

This IOC represents the capabilities to emit a heartbeat notification periodically. The emission periodicity is controlled by an attribute named heartbeatPeriod.

Table 2.6.2.3-1 Heartbeat IOC Attributes

Attribute name	Support Qualifier	isReadable	isWritable	isInvariant	isNotifiable
heartbeatPeriod	M	T	T	F	F
countDownTimer	M	T	T	F	F

Attribute definitions and legal values are shown in the table below.

Table 2.6.2.3-2 Heartbeat Attribute Definitions

Attribute Name	Definition	Legal Values
heartbeatPeriod	It specifies the time between two emissions of heartbeat notifications. A value of zero implies there is no heartbeat emission. The unit isseconds	Type: Integral numeric value Range: value range of heartbeat period is from 1 second to 3600 seconds., 0 is also a legal value.
countDownTimer	It represents the current value of a count down timer.	Range: value range of heartbeatPeriod. Heartbeat is emitted when value reaches or is set to 0.

2.7 PNF Startup and Registration Management Services

PNF Startup and Registration management services allow a physical PNF Startup and Registration MnS Provider to acquire its network layer parameters either via static procedures (pre-configured in the element) or via dynamic procedures (Plug-n-Play) during startup. During this process, the PNF Startup and Registration MnS Provider also acquires the IP address of the PNF Startup and Registration MnS Consumer for PNF Startup and Registration MnS Provider registration. Once the PNF Startup and Registration MnS Provider registers, the PNF Startup and Registration MnS Consumer can then bring the PNF Startup and Registration MnS Provider to an operational state.

Relevant 3GPP specification for PNF Plug-n-Play (PnP) is 3GPP TS 32.508 [21]. Additional Plug-n-Play information for IPV6 and other O-RAN extensions can be found in ORAN-WG4.MP.0-v01.00: O-RAN Alliance Working Group 4 Management Plane Specification.

Alignment between 3GPP SA5 and VES is described in 3GPP TR 28.890. Normative work includes an update to 3GPP TS 28.532 to add the pnfRegistration VES event. O-RAN may want to propose a new 3GPP SA5 Stage 1 specification for PNF Plug-n-Play and Registration.

2.7.1 PNF Plug-n-Play

2.7.1.1 Description

PNF Plug-n-Play (PnP) scenario enables a PNF ME to obtain the necessary start-up configuration to allow it to register with a PNF Startup and Registration MnS Consumer for subsequent management.

2.7.1.2 Requirements

Assuming O-RAN proposes a new Stage 1 spec for PNF Plug-n-Play and Registration, the PNF PnP requirements will be specified there. Until that time, the PNF PnP requirements are found in 3GPP TS 32.508.

2.7.1.3 Procedures

Assuming O-RAN proposes a new Stage 1 spec for PNF Plug-n-Play and Registration, the PNF PnP procedures will be specified there. Until that time, the PNF PnP procedures are found in 3GPP TS 32.508.

2.7.2 PNF Registration

2.7.2.1 Description

PNF Startup and Registration MnS Provider sends an asynchronous pnfRegistration event to a PNF Startup and Registration MnS Consumer after PnP to notify PNF Startup and Registration MnS Consumer of new PNF Startup and Registration MnS Provider to be managed

2.7.2.2 Requirements

Assuming O-RAN proposes a new Stage 1 spec for PNF Plug-n-Play and Registration, the PNF Registration requirements will be specified there. Until that time, the PNF Registration requirements are provided in the VES Event Listener Specification [11]

2.7.2.3 Procedures

Assuming O-RAN proposes a new Stage 1 spec for PNF Plug-n-Play and Registration, the PNF Registration procedures will be specified there. Until that time, the PNF Registration procedures are provided in this O1 Interface Specification.

2.7.2.4 Procedures

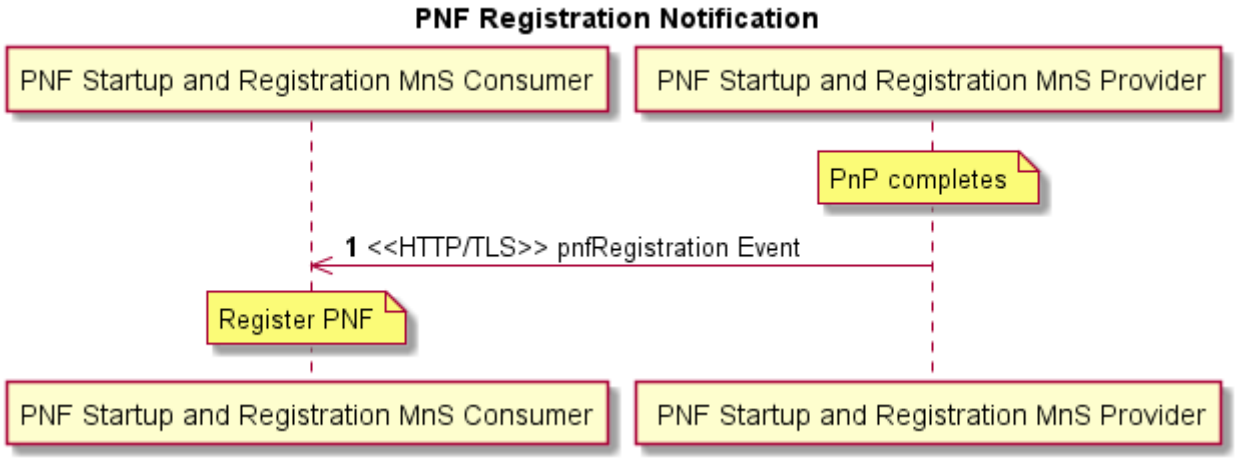

Figure 2.7.2.4-1 PNF Registration Notification

Pre-condition: PNF completes Plug-n-Play.

1. PNF Startup and Registration MnS Provider sends pnfRegistration notification VES event to PNF Startup and Registration MnS Consumer over HTTP/TLS. Mutual certificate authentication is performed.

Post-condition: PNF Startup and Registration MnS Consumer registers the PNF Startup and Registration MnS Provider so that it can be managed.

2.7.2.5 Operations and Notifications

pnfRegistration notification is a JSON encoded VES event sent from PNF Startup and Registration MnS Provider to PNF Startup and Registration MnS Consumer using REST/HTTPS. It consists of a Common VES Event Header and pnfRegistration Notification Fields.

pnfRegistration notification event will be specified in 3GPP TS 28.532 as part of the 3GPP/VES alignment normative work. Until that time, the pnfRegistration notification is specified in the VES Event Specification v7.1 [31].

2.8 PNF Software Management Services

Software management services allow a PNF Software MnS Consumer to request a physical PNF Software MnS Provider to download, install, validate and activate a new software package and allow a physical PNF Software MnS Provider to report its software versions. O-RAN will utilize the liaison to 3GPP to initiate enhancements to the 3GPP specifications for PNF Software Management. Until those enhancements are put in place, O-RAN PNF Software Management will be described in this specification. Software management described in this document is modeled on the O-RAN Alliance Working Group 4 Management Plane Specification [29].

2.8.1 Software Package Naming and Content

PNF Software Package naming, content and format are vendor specific and do not require standardization in O-RAN. A PNF Software Package may contain one or more files. Some of the files in the Software Package may be optional for the PNF (example: a file that has not changed version). The PNF is aware of the content and format of its available Software Packages and can determine which files it needs to download.

The softwarePackage Managed Object Class (MOC) contains attributes about a software package such as: software package name, version, fileList, integrityStatus (valid, invalid, empty), runningState (active, passive), vendor, productName, softwareType (operational, factory), etc. This MOC is applicable to VNFs and PNFs and is a generic term that O-RAN will use to refer to the software available on the PNF rather than the legacy term of software slot

The PNF creates one instance of softwarePackage for each software package supported concurrently on the PNF. Typically, a PNF will have two softwarePackage MOIs for operational software; one with runningState = active and one with runningState = passive. Some PNFs also have a softwarePackage MOI for the factory software which would be read only. O-RAN may have PNFs that support more than one passive slot. In this case the inventory query result would show multiple MOIs with runningState=passive.

2.8.2 Software Inventory

2.8.2.1 Description

The PNF Startup and Registration MnS Consumer sends a Software Inventory Request and retrieves information about the software packages on the PNF Software MnS Provider.

2.8.2.2 Requirements

Requirements are to be specified in a 3GPP spec for PNF Software Management. Until that time, the requirements are provided in this O1 Interface Specification.

REQ-SWI-FUN-1: The PNF software management service provider SHALL have the capability to provide its authorized consumer information about the software packages on the PNF software management service provider.

2.8.2.3 Procedures

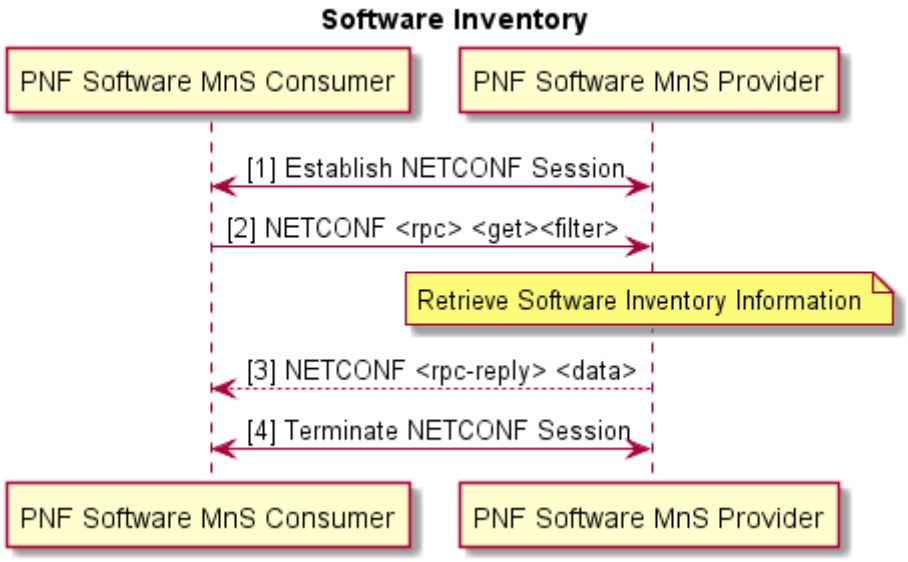

Figure 2.8.2.3-1 Software Inventory

1. PNF Software MnS Consumer establishes NETCONF session with PNF Software MnS Provider. The NETCONF session has authorized read privileges into the identified section of the data store.
2. PNF Software MnS Consumer sends NETCONF <rpc> <get><filter> to retrieve an optionally filtered subset configuration from the running configuration datastore. <filter> can be used to identify the software package MOIs. GET retrieves configuration and operational-state of softwarePackage MOIs.
    a. PNF Software MnS Provider retrieves software inventory information.
3. PNF Software MnS Provider returns requested data in NETCONF <rpc-reply> response.

4. PNF Software MnS Consumer termintes NETCONF session with PNF Software MnS Provider.

2.8.3 Software Download

2.8.3.1 Description

Software Download triggers the download of a specific software package to the PNF Software MnS Provider. This download service includes integrity checks on the downloaded software and the installation of the software into the software slot corresponding to the softwarePackage MOI.

2.8.3.2 Requirements

Requirements are to be specified in a 3GPP spec for PNF Software Management. Until that time, the requirements are provided in this O1 Interface Specification.

REQ-SWD-FUN-1: The PNF software management service provider SHALL have the capability to allow its authorized consumer to specify the location of software that is to be downloaded and to specify into which softwarePackage the software is to be stored.

REQ-SWD-FUN-2: The PNF software management service provider SHALL have the capability to verify if a software download is in progress and the ability to reject subsequent download commands until the one in progress completes.

REQ-SWD-FUN-3: The PNF software management service provider SHALL have the capability to deny download of software if the download request is not valid for the PNF software management service provider.

REQ-SWD-FUN-4: The PNF software management service provider SHALL have the capability to download needed files from a software server at a specified location.

REQ-SWD-FUN-5: The PNF software management service provider SHALL have the capability to perform integrity checks on downloaded software.

REQ-SWD-FUN-6: The PNF software management service provider SHALL have the capability to install the software into the software slot corresponding to the softwarePackage MOI identified by its authorized consumer in the download command. The PNF software management service provider SHALL not allow installation of newly downloaded software into the running software slot.

2.8.3.3 Procedures

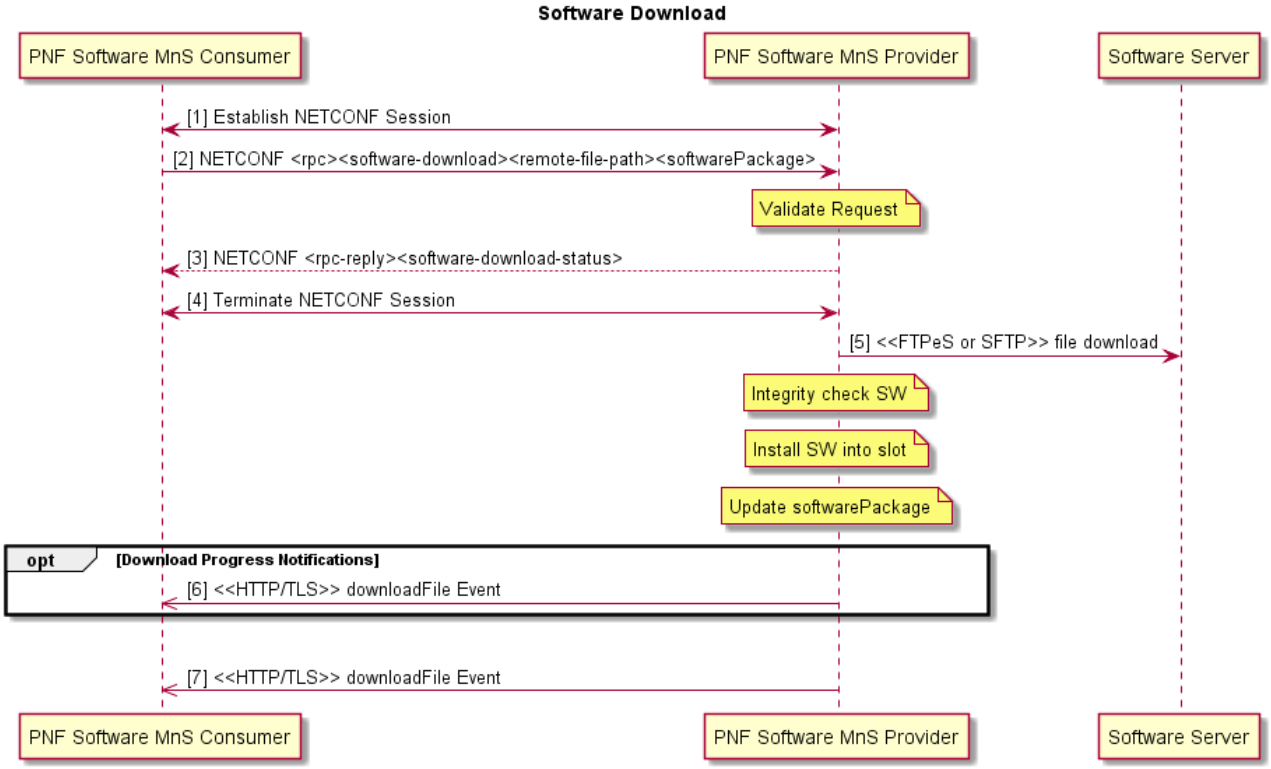

Figure 2.8.3.3-1 Software Download

1. PNF Software MnS Consumer establishes NETCONF session with PNF Software MnS Provider. The NETCONF session has authorized execution privileges for retrieve file list and file-download rpcs.

2. PNF Software MnS Consumer sends NETCONF <rpc><software-download><remote-file-path><softwarePackage> to trigger a download of the software located at remoteFilePath and save its information in softwarePackage.

    a. PNF Software MnS Provider validates the request. Validation includes determining if the operation can be performed. This is PNF Software MnS Provider specific but could include things like: checking that there is not a software download already in progress, softwarePackage is runningState = passive and softwareType = operational, etc.

3. PNF Software MnS Provider returns NETCONF <rpc-reply><software-download-status>.

4. PNF Software MnS Consumer terminates NETCONF session with PNF Software MnS Provider.

5. PNF Software MnS Provider initiates SFTP or FTPES connection and downloads the software package from remoteFilePath. SFTP is authenticated with username/password, SSH keys or X.509 certificates. FTPES is authenticated with X.509 certificates. PNF Software MnS Provider understands the software package format and downloads all the files it needs from the package. PNF Software MnS Provider decides where to store the software internally. This is PNF Software MnS Provider specific but could be a temporary location like /tmp.

    a. PNF Software MnS Provider integrity checks the downloaded software. This is PNF Software MnS Provider specific but could include checking-checksum, correct software for the hardware, etc.

    b. PNF Software MnS Provider installs software into the software slot corresponding to the softwarePackage.

c. PNF Software MnS Provider updates softwarePackage; name, version, fileList, integrityStatus, runningState, etc.

6. (Optional) If the download takes a long time, PNF Software MnS Provider may send periodic downloadFile notifications to the PNF Software MnS Consumer with the current status of the download (download in progress, integrity checks passed, install complete).

7. When download operation completes, PNF Software MnS Provider sends downloadFile notification to PNF Software MnS Consumer with the final status of the download (success or the reason for failure).

2.8.3.4 Operations and Notifications

downloadFile notification is a JSON encoded VES event sent from PNF Software MnS Provider to PNF Software MnS Consumer using REST/HTTPS. It consists of a Common VES Event Header and fileDownload Notification Fields to notify the PNF Software MnS Consumer of the progress and status of a file download. This event needs to be defined in VES and included in the harmonization activities between 3GPP and VES.

2.8.4 Software Activation Pre-Check

2.8.4.1 Description

Activation Pre-check is an optional Use Case that the Service Provider may choose to utilize prior to software activation to confirm that the PNF Software MnS Provider is in a good state to activate the new software and provide information needed for planning the timing of the software replacement--such as whether a reset or a data migration is required.

2.8.4.2 Requirements

Requirements are to be specified in a 3GPP spec for PNF Software Management. Until that time, the requirements are provided in this O1 Interface Specification.

REQ-SPC-FUN-1: The PNF software management service provider SHALL have the capability to confirm that the software in the passive slot targeted for activation is good.

REQ-SPC-FUN-2: The PNF software management service provider SHALL have the capability to determine whether the activation of the targeted software requires a reset and/or data migration.

2.8.4.3 Procedures

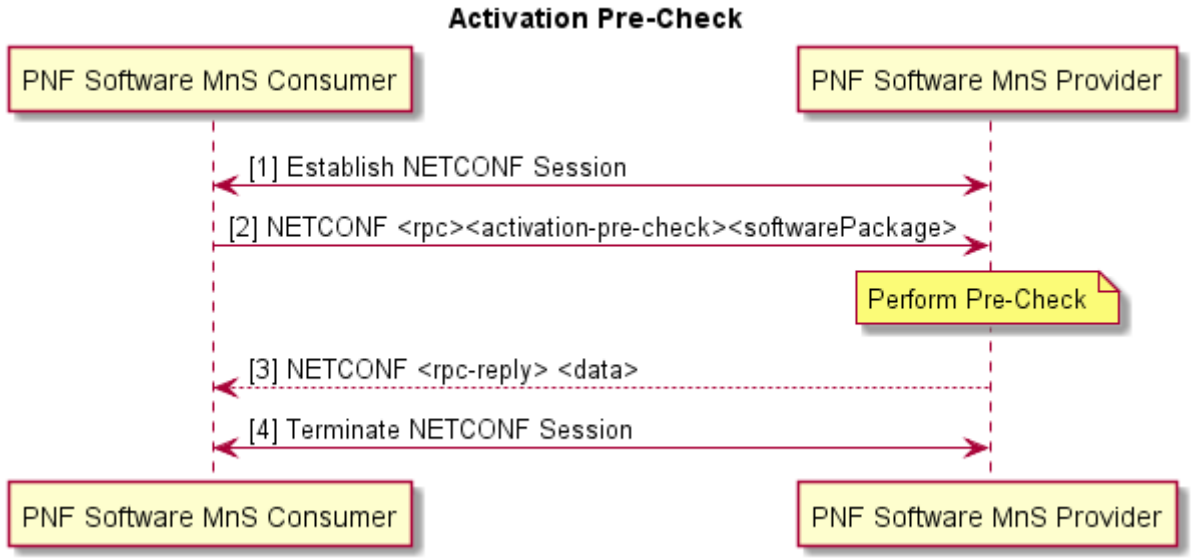

Figure 2.8.4.3-1 Software Activation Pre-Check

1. PNF Software MnS Consumer establishes NETCONF session with PNF Software MnS Provider.
2. PNF Software MnS Consumer sends NETCONF <rpc><activation-pre-check><softwarePackage> to trigger a pre-check of the software stored in softwarePackage and to return the results of the pre-check.
    a. PNF Software MnS Provider performs the activation pre-check which includes validating that the software in softwarePackage is good, whether the activation of the software in softwarePackage will result in a reset and whether data migration is needed, etc.
3. PNF Software MnS Provider returns NETCONF <rpc-reply> to the PNF Software MnS Consumer with the results of the pre-check.
4. PNF Software MnS Consumer terminates NETCONF session with PNF Software MnS Provider.

2.8.5 Software Activate

2.8.5.1 Description

PNF Software MnS Consumer triggers the activation of a software package on the PNF Software MnS Provider including data migration and reset if needed.

2.8.5.2 Requirements

Requirements are to be specified in a 3GPP spec for PNF Software Management. Until that time, the requirements are provided in this O1 Interface Specification.

REQ-SWA-FUN-1: The PNF software management service provider SHALL have the capability to allow its authorized consumer to activate valid software in a specific softwarePackage.

REQ-SWA-FUN-2: The PNF software management service provider SHALL have the capability to verify whether a software activation is in progress and deny a concurrent activation of software.

REQ-SWA-FUN-3: The PNF software management service provider SHALL have the capability to deny activation of software if the activation request is not valid for the PNF software management service provider.

REQ-SWA-FUN-4: The PNF software management service provider SHALL have the capability to activate the softwarePackage.

REQ-SWA-FUN-5: The PNF software management service provider SHALL have the capability to reset the PNF software management service provider if the software activation requires it.

REQ-SWA-FUN-6: The PNF software management service provider SHALL provide the capability for the PNF software management service provider to send a re-set reason notification to its authorized consumer if the activation results in a reset.

REQ-SWA-FUN-7: The PNF software management service provider SHALL have the capability to perform data migration on the PNF software management service provider if the software activation requires it.

REQ-SWA-FUN-8: The PNF software management service provider SHALL have the capability to fallback to the previously active software if the new software cannot be activated.

REQ-SWA-FUN-9: The PNF software management service provider SHALL have the capability to fallback to the factory software if the new and the previously active software can not be activated.

2.8.5.3 Procedures

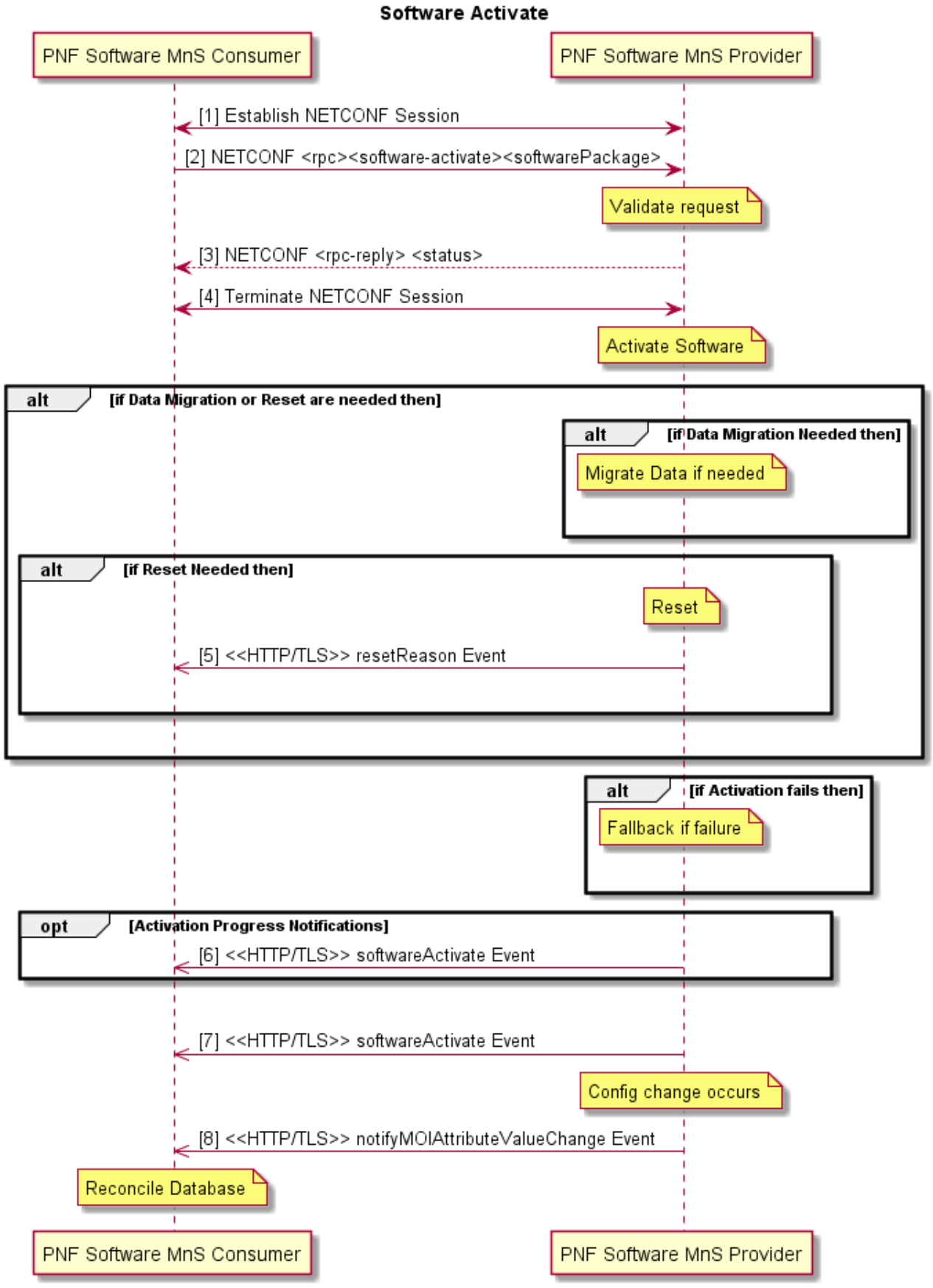

Figure 2.8.5.3-1 Activate Software

1. PNF Software MnS Consumer establishes NETCONF session with PNF Software MnS Provider.
2. PNF Software MnS Consumer sends NETCONF <rpc><software-activate><softwarePackage> to trigger an activation of the software in softwarePackage.
    a. PNF Software MnS Provider validates the request. This is PNF Software MnS Provider specific but could include things like checking that there is not a software activation already in progress, softwarePackage is runningState = passive and integrityStatus = valid, etc.
3. PNF Software MnS Provider returns status to the PNF Software MnS Consumer in the NETCONF <rpc-reply> response.
    a. PNF Software MnS Provider performs the steps needed to make the softwarePackage the active one. This is PNF Software MnS Provider specific but includes things like updating the runningState of the about-to-be-active and previously-active software packages.
4. PNF Software MnS Consumer terminates NETCONF session with PNF Software MnS Provider.

(Optional) PNF Software MnS Provider performs data migration if necessary. PNF Software MnS Provider knows whether this is necessary.

5. (Optional) PNF Software MnS Provider performs reset if necessary. PNF Software MnS Provider knows whether reset is necessary. If a reset occurs, PNF Software MnS Provider sends a resetReason notification to the PNF Software MnS Consumer with the reason for the reset; in this case software activation.

(Optional) If the PNF Software MnS Provider can not activate the software, PNF Software MnS Provider shall have recovery logic to fallback to the previously active software and potentially fallback to the factory software in a worst-case scenario.

6. (Optional) If the activation takes a long time, PNF Software MnS Provider may send periodic softwareActivate notifications to PNF Software MnS Consumer with the current status of the activation (e.g. activation in progress, data migration successful).
7. After activation operation completes, PNF Software MnS Provider sends a softwareActivate notification to PNF Software MnS Consumer with the final status of the activation.
8. PNF Software MnS Provider sends notifyMOIAttributeValueChange to the PNF MnS Consumer updating the active software running on the PNF.

2.8.5.4 Operations and Notifications

softwareActivate notification is a JSON encoded VES event sent from PNF Software MnS Provider to PNF Software MnS Consumer using REST/HTTPS. It consists of a Common VES Event Header and softwareActivate Notification Fields to notify the PNF Software MnS Consumer of the progress and status of a software activation.

resetReason notification is a JSON encoded VES event sent from PNF Software MnS Provider to PNF Software MnS Consumer using REST/HTTPS. It consists of a Common VES Event Header and resetReason Notification Fields to notify the PNF Software MnS Consumer that a reset has occurred and the reason for the reset.

These events need to be defined in VES and included in the harmonization activities between 3GPP and VES.

Annex ZZZ O-RAN Adopter License Agreement

BY DOWNLOADING, USING OR OTHERWISE ACCESSING ANY O-RAN SPECIFICATION, ADOPTER AGREES TO THE TERMS OF THIS AGREEMENT.

This O-RAN Adopter License Agreement (the "Agreement") is made by and between the O-RAN Alliance and the entity that downloads, uses or otherwise accesses any O-RAN Specification, including its Affiliates (the "Adopter").

This is a license agreement for entities who wish to adopt any O-RAN Specification.

2.9 Section 1: DEFINITIONS

1.1 "Affiliate" means an entity that directly or indirectly controls, is controlled by, or is under common control with another entity, so long as such control exists. For the purpose of this Section, "Control" means beneficial ownership of fifty (50%) percent or more of the voting stock or equity in an entity.

1.2 "Compliant Implementation" means any system, device, method or operation (whether implemented in hardware, software or combinations thereof) that fully conforms to a Final Specification.

1.3 "Adopter(s)" means all entities, who are not Members, Contributors or Academic Contributors, including their Affiliates, who wish to download, use or otherwise access O-RAN Specifications.

1.4 "Minor Update" means an update or revision to an O-RAN Specification published by O-RAN Alliance that does not add any significant new features or functionality and remains interoperable with the prior version of an O-RAN Specification. The term "O-RAN Specifications" includes Minor Updates.

1.5 "Necessary Claims" means those claims of all present and future patents and patent applications, other than design patents and design registrations, throughout the world, which (i) are owned or otherwise licensable by a Member, Contributor or Academic Contributor during the term of its Member, Contributor or Academic Contributorship; (ii) such Member, Contributor or Academic Contributor has the right to grant a license without the payment of consideration to a third party; and (iii) are necessarily infringed by a Compliant Implementation (without considering any Contributions not included in the Final Specification). A claim is necessarily infringed only when it is not possible on technical (but not commercial) grounds, taking into account normal technical practice and the state of the art generally available at the date any Final Specification was published by the O-RAN Alliance or the date the patent claim first came into existence, whichever last occurred, to make, sell, lease, otherwise dispose of, repair, use or operate a Compliant Implementation without infringing that claim. For the avoidance of doubt in exceptional cases where a Final Specification can only be implemented by technical solutions, all of which infringe patent claims, all such patent claims shall be considered Necessary Claims.

1.6 "Defensive Suspension" means for the purposes of any license grant pursuant to Section 3, Member, Contributor, Academic Contributor, Adopter, or any of their Affiliates, may have the discretion to include in their license a term allowing the licensor to suspend the license against a licensee who brings a patent infringement suit against the licensing Member, Contributor, Academic Contributor, Adopter, or any of their Affiliates.

2.10 Section 2: COPYRIGHT LICENSE

2.1 Subject to the terms and conditions of this Agreement, O-RAN Alliance hereby grants to Adopter a nonexclusive, nontransferable, irrevocable, non-sublicensable, worldwide copyright license to obtain, use and modify O-RAN Specifications, but not to further distribute such O-RAN Specification in any modified or unmodified way, solely in furtherance of implementations of an ORAN Specification.

2.2 Adopter shall not use O-RAN Specifications except as expressly set forth in this Agreement or in a separate written agreement with O-RAN Alliance.

2.11 Section 3: FRAND LICENSE

3.1 Members, Contributors and Academic Contributors and their Affiliates are prepared to grant based on a separate Patent License Agreement to each Adopter under Fair Reasonable And Non- Discriminatory (FRAND) terms and conditions with or without compensation (royalties) a nonexclusive, non-transferable, irrevocable (but subject to

Defensive Suspension), non-sublicensable, worldwide patent license under their Necessary Claims to make, have made, use, import, offer to sell, lease, sell and otherwise distribute Compliant Implementations; provided, however, that such license shall not extend: (a) to any part or function of a product in which a Compliant Implementation is incorporated that is not itself part of the Compliant Implementation; or (b) to any Adopter if that Adopter is not making a reciprocal grant to Members, Contributors and Academic Contributors, as set forth in Section 3.3. For the avoidance of doubt, the foregoing licensing commitment includes the distribution by the Adopter's distributors and the use by the Adopter's customers of such licensed Compliant Implementations.

3.2 Notwithstanding the above, if any Member, Contributor or Academic Contributor, Adopter or their Affiliates has reserved the right to charge a FRAND royalty or other fee for its license of Necessary Claims to Adopter, then Adopter is entitled to charge a FRAND royalty or other fee to such Member, Contributor or Academic Contributor, Adopter and its Affiliates for its license of Necessary Claims to its licensees.

3.3 Adopter, on behalf of itself and its Affiliates, shall be prepared to grant based on a separate Patent License Agreement to each Members, Contributors, Academic Contributors, Adopters and their Affiliates under Fair Reasonable And Non-Discriminatory (FRAND) terms and conditions with or without compensation (royalties) a nonexclusive, non-transferable, irrevocable (but subject to Defensive Suspension), non-sublicensable, worldwide patent license under their Necessary Claims to make, have made, use, import, offer to sell, lease, sell and otherwise distribute Compliant Implementations; provided, however, that such license will not extend: (a) to any part or function of a product in which a Compliant Implementation is incorporated that is not itself part of the Compliant Implementation; or (b) to any Members, Contributors, Academic Contributors, Adopters and their Affiliates that is not making a reciprocal grant to Adopter, as set forth in Section 3.1. For the avoidance of doubt, the foregoing licensing commitment includes the distribution by the Members', Contributors', Academic Contributors', Adopters' and their Affiliates' distributors and the use by the Members', Contributors', Academic Contributors', Adopters' and their Affiliates' customers of such licensed Compliant Implementations.

2.12 Section 4: TERM AND TERMINATION

4.1 This Agreement shall remain in force, unless early terminated according to this Section 4.

4.2 O-RAN Alliance on behalf of its Members, Contributors and Academic Contributors may terminate this Agreement if Adopter materially breaches this Agreement and does not cure or is not capable of curing such breach within thirty (30) days after being given notice specifying the breach.

4.3 Sections 1, 3, 5 - 11 of this Agreement shall survive any termination of this Agreement. Under surviving Section 3, after termination of this Agreement, Adopter will continue to grant licenses (a) to entities who become Adopters after the date of termination; and (b) for future versions of ORAN Specifications that are backwards compatible with the version that was current as of the date of termination.

2.13 Section 5: CONFIDENTIALITY

Adopter will use the same care and discretion to avoid disclosure, publication, and dissemination of O-RAN Specifications to third parties, as Adopter employs with its own confidential information, but no less than reasonable care. Any disclosure by Adopter to its Affiliates, contractors and consultants should be subject to an obligation of confidentiality at least as restrictive as those contained in this Section. The foregoing obligation shall not apply to any information which is: (1) rightfully known by Adopter without any limitation on use or disclosure prior to disclosure; (2) publicly available through no fault of Adopter; (3) rightfully received without a duty of confidentiality; (4) disclosed by O-RAN Alliance or a Member, Contributor or Academic Contributor to a third party without a duty of confidentiality on such third party; (5) independently developed by Adopter; (6) disclosed pursuant to the order of a court or other authorized governmental body, or as required by law, provided that Adopter provides reasonable prior written notice to O-RAN Alliance, and cooperates with O-RAN Alliance and/or the applicable Member, Contributor or Academic Contributor to have the opportunity to oppose any such order; or (7) disclosed by Adopter with O-RAN Alliance's prior written approval.

2.14 Section 6: INDEMNIFICATION

Adopter shall indemnify, defend, and hold harmless the O-RAN Alliance, its Members, Contributors or Academic Contributors, and their employees, and agents and their respective successors, heirs and assigns (the "Indemnitees"), against any liability, damage, loss, or expense (including reasonable attorneys' fees and expenses) incurred by or

imposed upon any of the Indemnitees in connection with any claims, suits, investigations, actions, demands or judgments arising out of Adopter's use of the licensed O-RAN Specifications or Adopter's commercialization of products that comply with O-RAN Specifications.

2.15 Section 7: LIMITATIONS ON LIABILITY; NO WARRANTY

EXCEPT FOR BREACH OF CONFIDENTIALITY, ADOPTER'S BREACH OF SECTION 3, AND ADOPTER'S INDEMNIFICATION OBLIGATIONS, IN NO EVENT SHALL ANY PARTY BE LIABLE TO ANY OTHER PARTY OR THIRD PARTY FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES RESULTING FROM ITS PERFORMANCE OR NON-PERFORMANCE UNDER THIS AGREEMENT, IN EACH CASE WHETHER UNDER CONTRACT, TORT, WARRANTY, OR OTHERWISE, AND WHETHER OR NOT SUCH PARTY HAD ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES.

O-RAN SPECIFICATIONS ARE PROVIDED "AS IS" WITH NO WARRANTIES OR CONDITIONS WHATSOEVER, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. THE O-RAN ALLIANCE AND THE MEMBERS, CONTRIBUTORS OR ACADEMIC CONTRIBUTORS EXPRESSLY DISCLAIM ANY WARRANTY OR CONDITION OF MERCHANTABILITY, SECURITY, SATISFACTORY QUALITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, ERROR-FREE OPERATION, OR ANY WARRANTY OR CONDITION FOR O-RAN SPECIFICATIONS.

2.16 Section 8: ASSIGNMENT

Adopter may not assign the Agreement or any of its rights or obligations under this Agreement or make any grants or other sublicenses to this Agreement, except as expressly authorized hereunder, without having first received the prior, written consent of the O-RAN Alliance, which consent may be withheld in O-RAN Alliance's sole discretion. O-RAN Alliance may freely assign this Agreement.

2.17 Section 9: THIRD-PARTY BENEFICIARY RIGHTS

Adopter acknowledges and agrees that Members, Contributors and Academic Contributors (including future Members, Contributors and Academic Contributors) are entitled to rights as a third-party beneficiary under this Agreement, including as licensees under Section 3.

2.18 Section 10: BINDING ON AFFILIATES

Execution of this Agreement by Adopter in its capacity as a legal entity or association constitutes that legal entity's or association's agreement that its Affiliates are likewise bound to the obligations that are applicable to Adopter hereunder and are also entitled to the benefits of the rights of Adopter hereunder.

2.19 Section 11: GENERAL

This Agreement is governed by the laws of Germany without regard to its conflict or choice of law provisions.

This Agreement constitutes the entire agreement between the parties as to its express subject matter and expressly supersedes and replaces any prior or contemporaneous agreements between the parties, whether written or oral, relating to the subject matter of this Agreement.

Adopter, on behalf of itself and its Affiliates, agrees to comply at all times with all applicable laws, rules and regulations with respect to its and its Affiliates' performance under this Agreement, including without limitation, export control and antitrust laws. Without limiting the generality of the foregoing, Adopter acknowledges that this Agreement prohibits any communication that would violate the antitrust laws.

By execution hereof, no form of any partnership, joint venture or other special relationship is created between Adopter, or O-RAN Alliance or its Members, Contributors or Academic Contributors. Except as expressly set forth in this Agreement, no party is authorized to make any commitment on behalf of Adopter, or O-RAN Alliance or its Members, Contributors or Academic Contributors.

In the event that any provision of this Agreement conflicts with governing law or if any provision is held to be null, void or otherwise ineffective or invalid by a court of competent jurisdiction, (i) such provisions will be deemed stricken from the contract, and (ii) the remaining terms, provisions, covenants and restrictions of this Agreement will remain in full force and effect.

Any failure by a party or third party beneficiary to insist upon or enforce performance by another party of any of the provisions of this Agreement or to exercise any rights or remedies under this Agreement or otherwise by law shall not be construed as a waiver or relinquishment to any extent of the other parties' or third party beneficiary's right to assert or rely upon any such provision, right or remedy in that or any other instance; rather the same shall be and remain in full force and effect.
