MAVENIR
Trust the Future

5G O-RAN Architecture

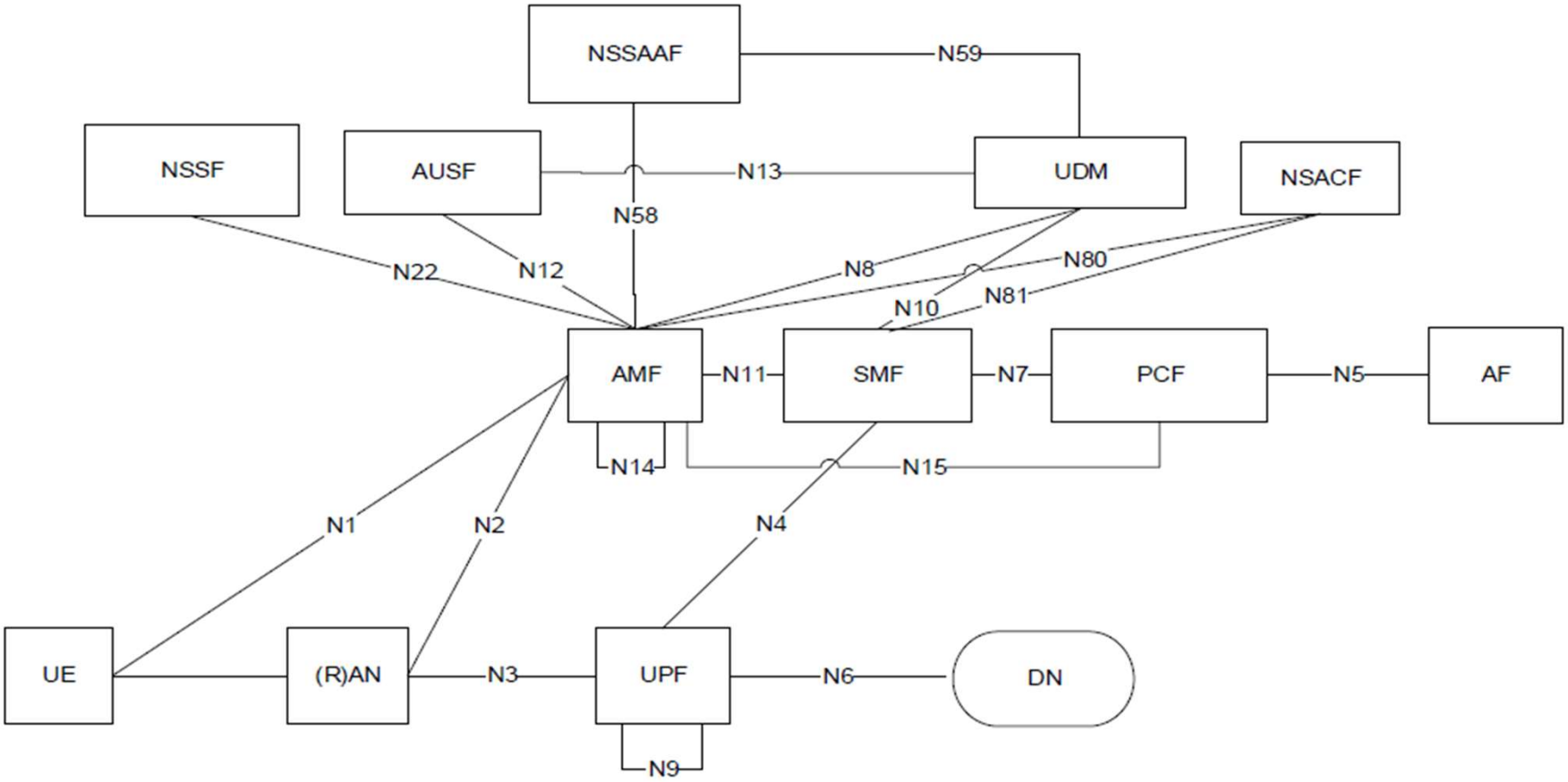
Mukesh Taneja,
Mavenir Systems

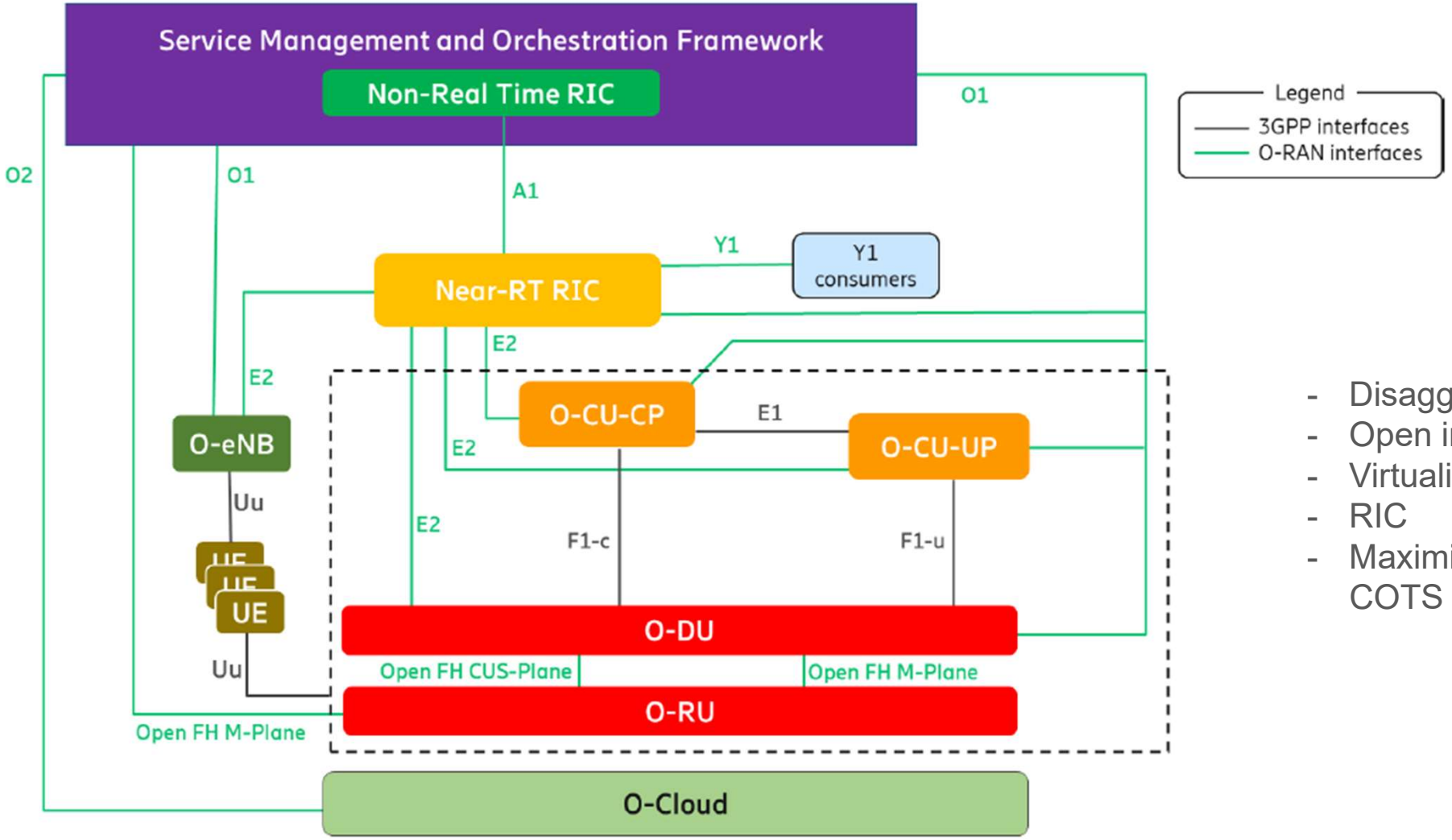
Agenda

- O-RAN Architecture – An Overview
  - gNB: O-RAN Architecture
  - RIC
  - Network slicing (Resource Isolation)

- Security

Non-roaming 5G Network Architecture (Ref: 3GPP TS 23.501)





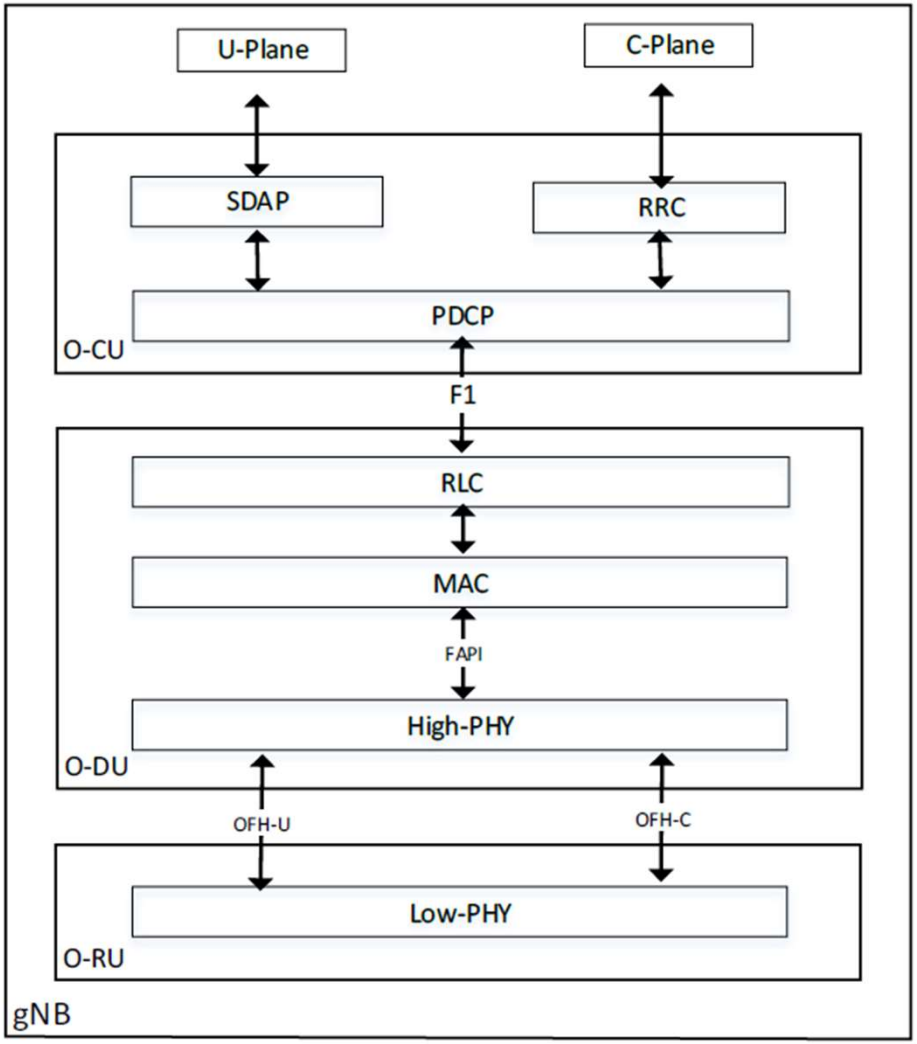
- Disaggregation
- Open interfaces
- Virtualization
- RIC
- Maximize use of COTS HW

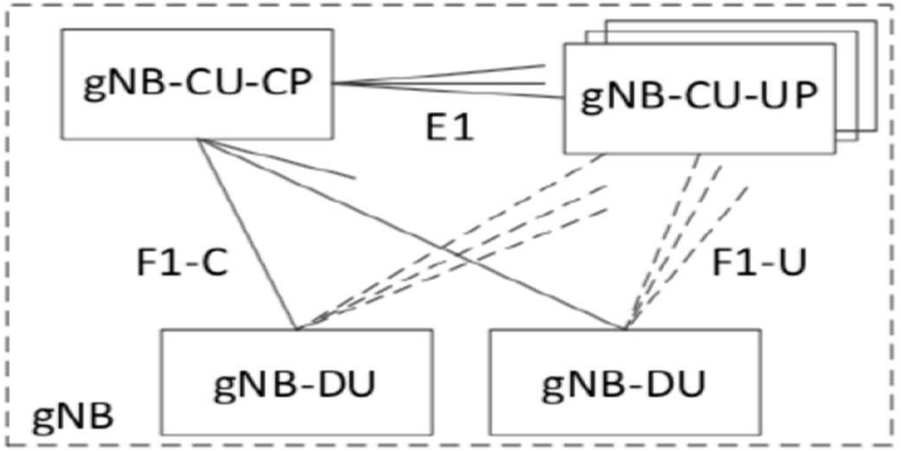
Ref: O-RAN.WG1.OAD-R003-v09.00

MAVENIR

gNodeB: O-RAN

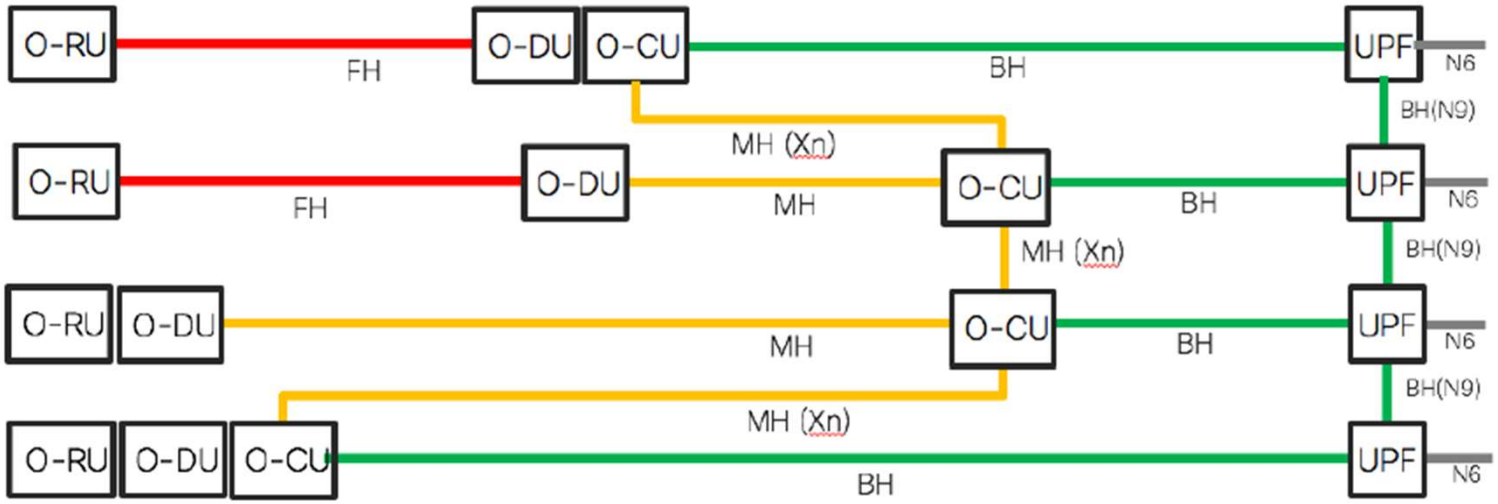
O-RAN 7.2 split





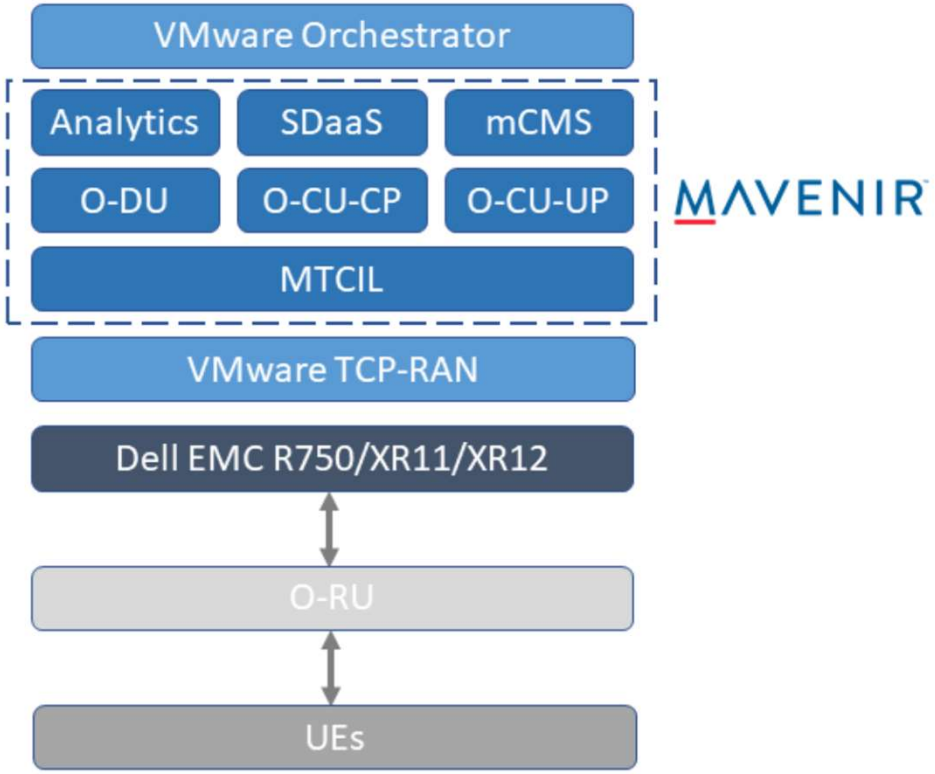
Ref: O-RAN.WG8.AAD.0-R003-v09.00

Deployment Models / Transport aspects



Ref: ORAN-WG9.XPSAAS.0-R003-v05.00

Reference Architecture



mCMS: Mavenir Centralized Management Service
sDaaS: Smart Deployment as a Service
MTCIL: Mavenir Telco Cloud Integration Layer
eCPRI: Enhanced Common Public Radio Interface
TCP: Telco Cloud Platform
O-RU: FFT/iFFT, PRACH extraction

https://www.mavenir.com/portfolio/mavair/radio-access/vran/

https://www.dell.com/en-in/dt/industry/telecom/open-ran.htm#accordion0&video-overlay=6306841678112

Dell Technologies, VMware, and Mavenir 5G O-RAN Reference Architecture Guide | Dell Technologies Info Hub

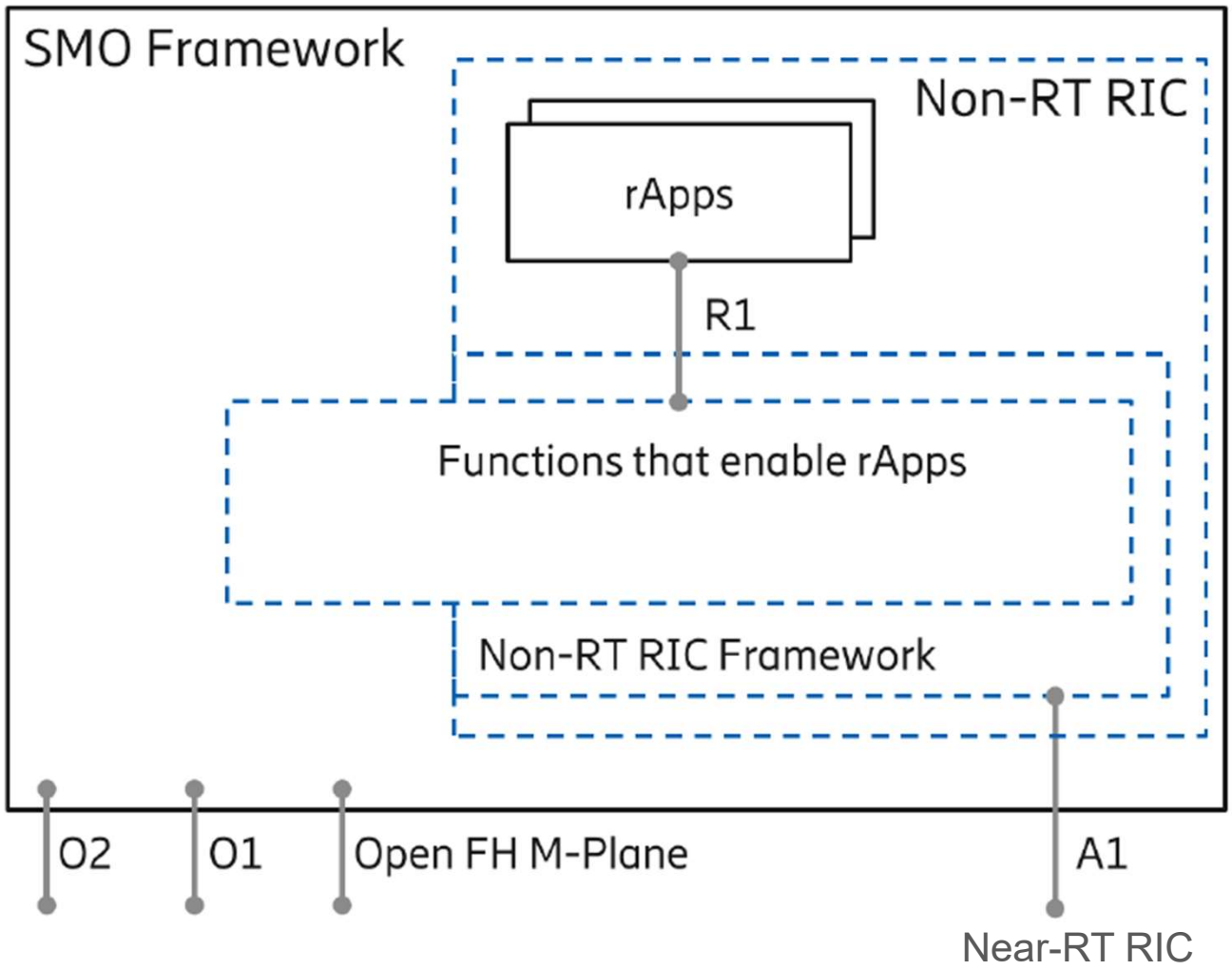
MAVENIR

Service Management and Orchestration

- SMO
  - FCAPS interface to O-RAN Network Functions
  - Non-RT RIC for RAN optimization
  - O-Cloud Management, Orchestration and Workflow Management

- A1, O1, O2, FH M-plane interfaces
  - A1 Interface between the Non-RT RIC in the SMO and the Near-RT RIC for RAN Optimization.
  - O1 Interface between the SMO and the O-RAN Network Functions for FCAPS support.
  - In the hybrid model, Open Fronthaul M-plane interface between SMO and O-RU for FCAPS support.
  - O2 Interface between the SMO and the O-Cloud to provide platform resources and workload management

[Ref: O-RAN.WG1.OAD-R003-v09.00]



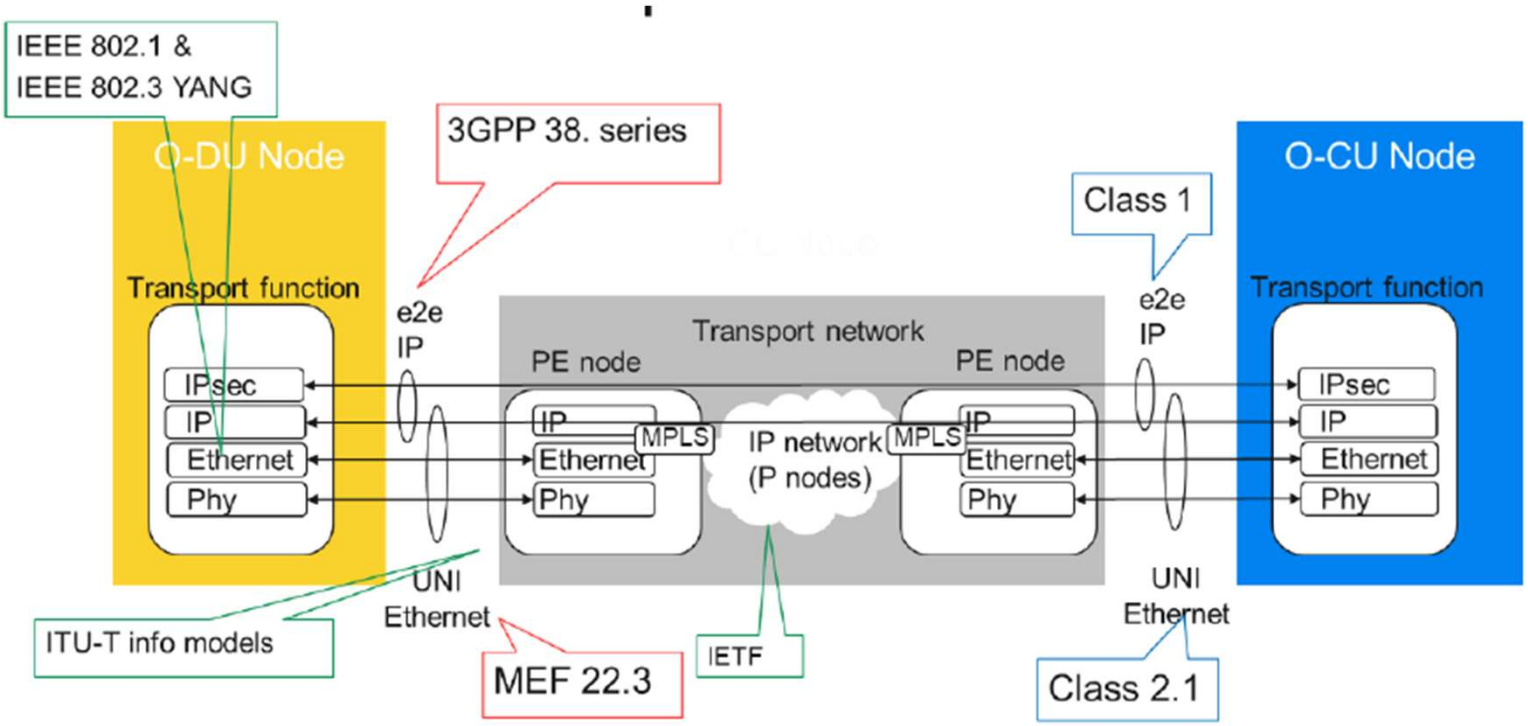
O1 interface:

- Performance Management (PM)
- Configuration Management (CM)
- Fault Management (FM)
- File Management
- Communications Surveillance (Heartbeat)
- Trace
- Physical Network Function (PNF) Discovery
- PNF Software Management.

O2: O-Cloud Management, Orchestration and Workflow Management

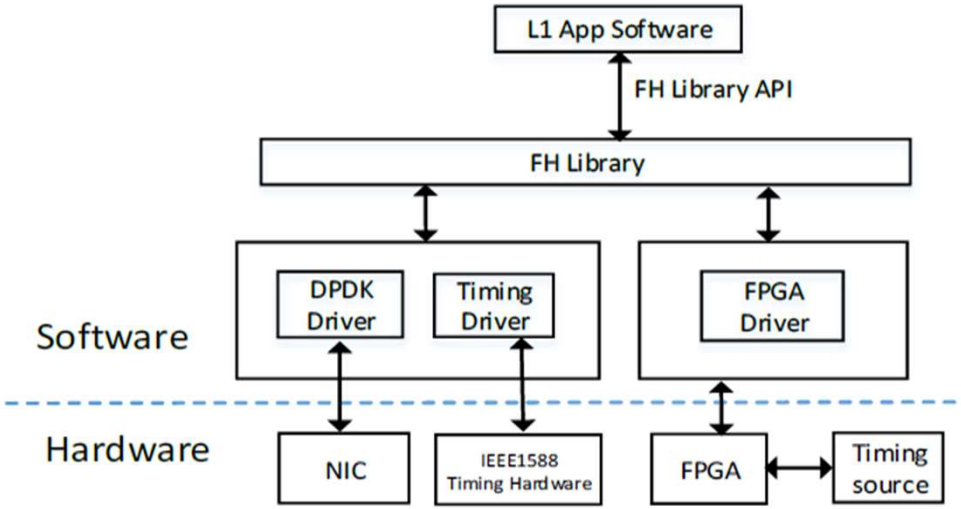
Ref: O-RAN.WG1.OAD-R003-v09.00

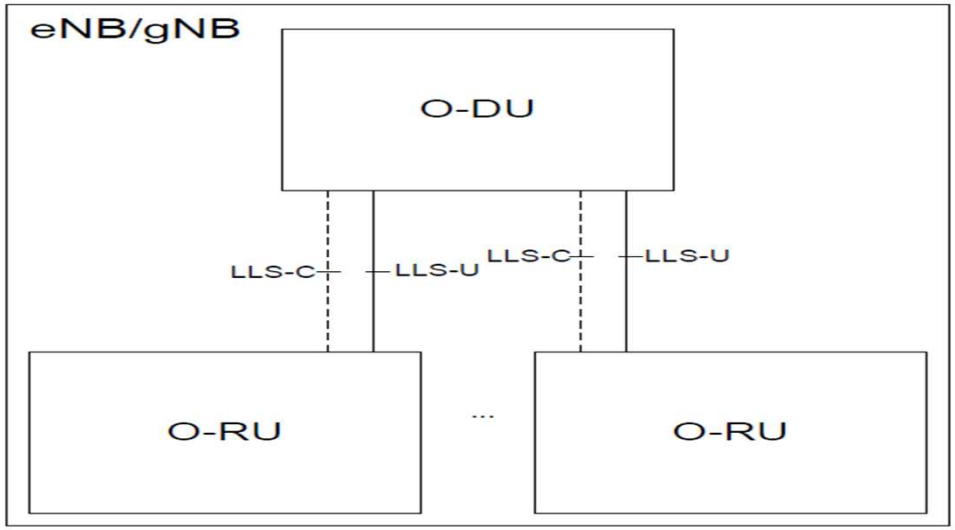
Transport



Ref: O-RAN Specs: WG9

Fronthaul transports C-Plane, U-Plane, S-Plane and M-Plane traffic.





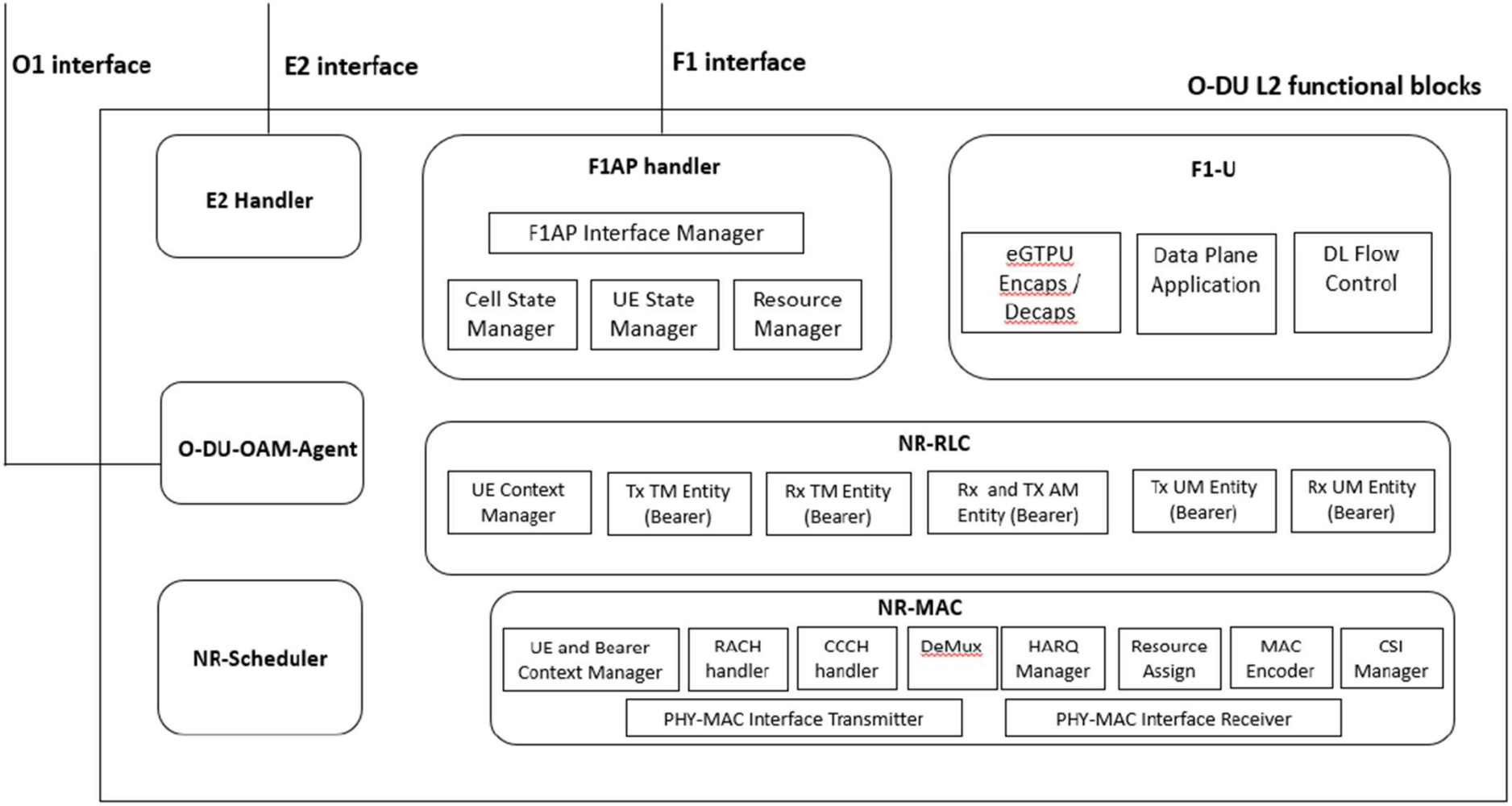
C-Plane: Control Plane: refers specifically to real-time control between O-DU and O-RU, and should not be confused with the UE's control plane.

M-Plane: Management Plane: refers to non-real-time management operations between the O-DU and the O-RU

S-Plane: Synchronization Plane: refers to traffic between the O-RU or O-DU and a synchronization controller which is generally an IEEE 1588 Grand Master.

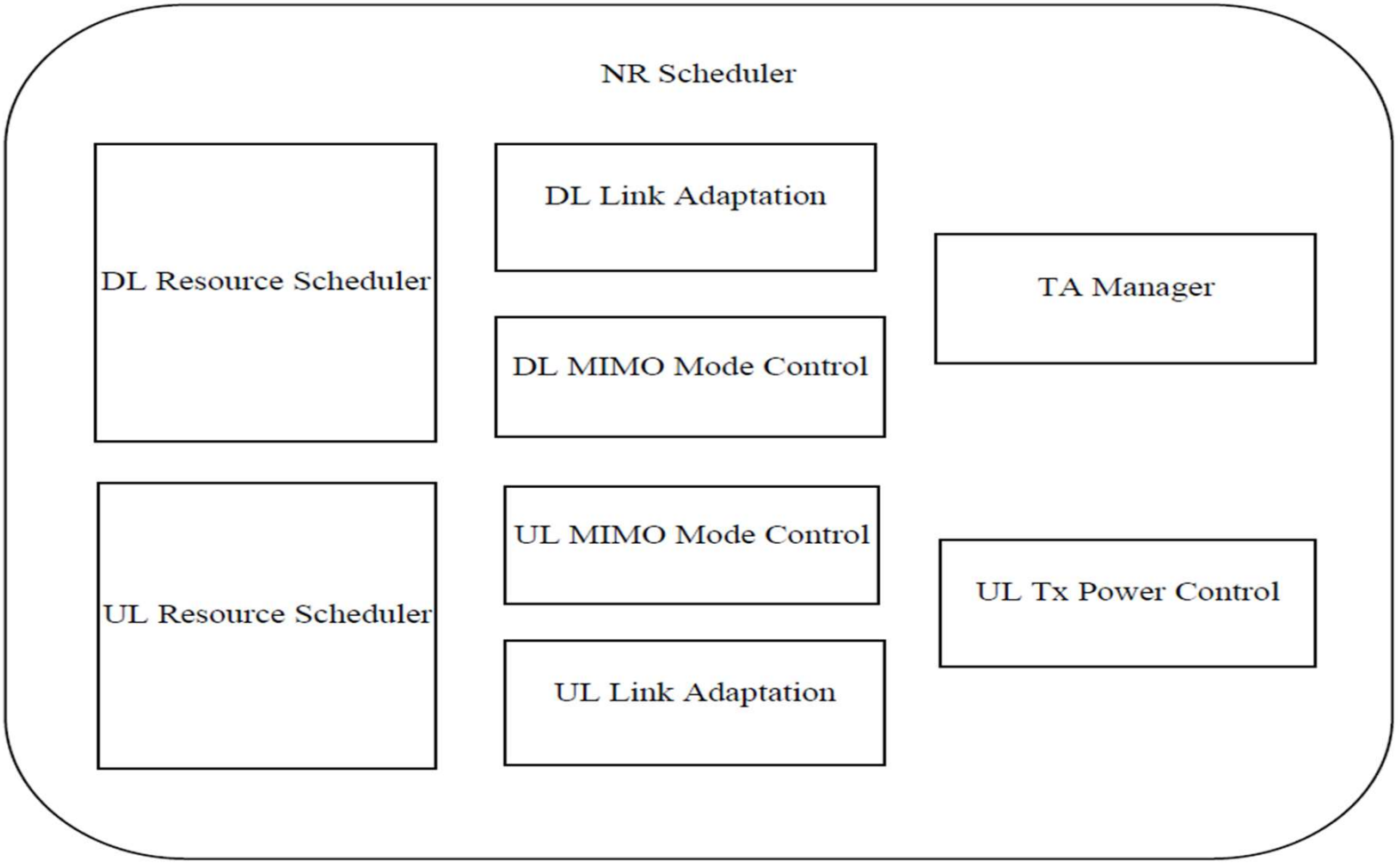
U-Plane: User Plane: refers to IQ sample data transferred between O-DU and O-RU

L2 / DU – Functional Architecture



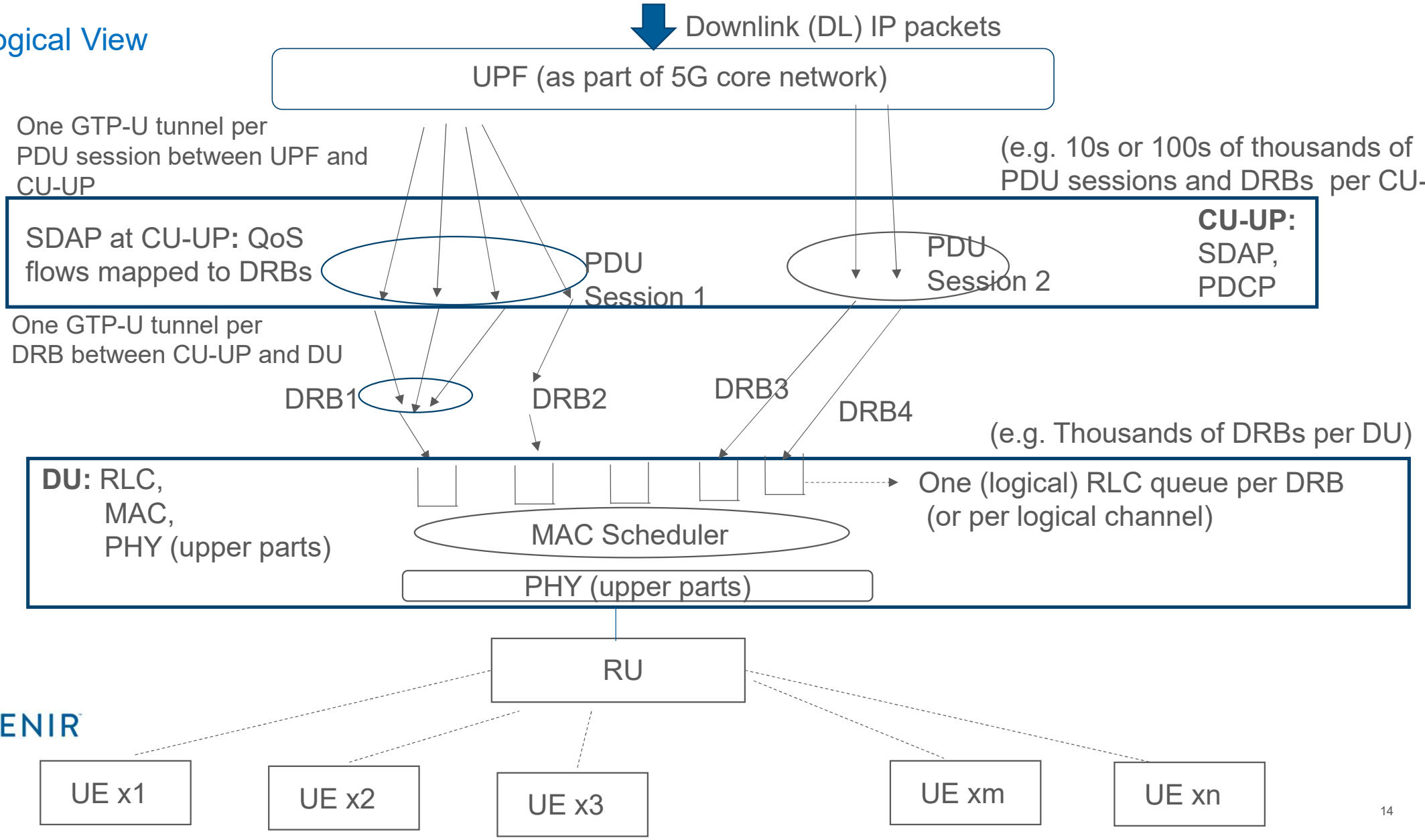
Ref: O-RAN.WG8.AAD.0-R003-v09.00

L2 / DU Scheduler - Functional Components (Contd.)



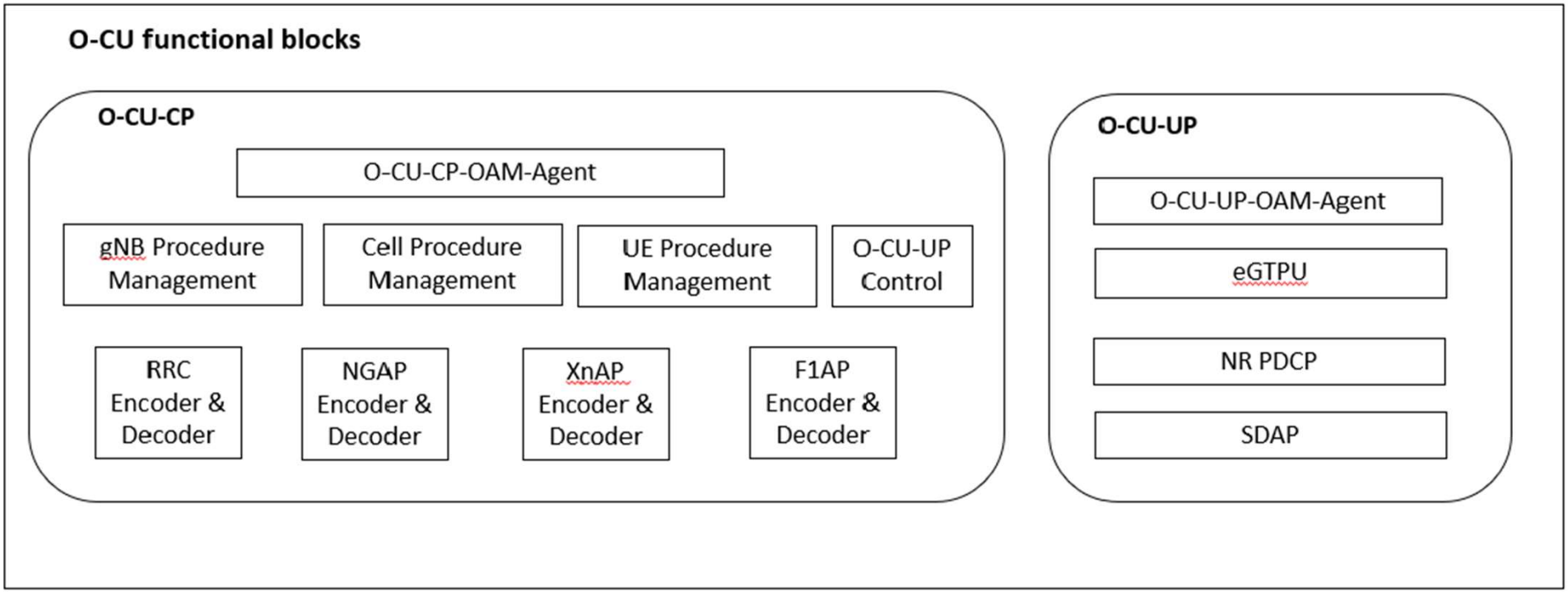
Ref: O-RAN.WG8.AAD.0-R003-v09.00

Logical View

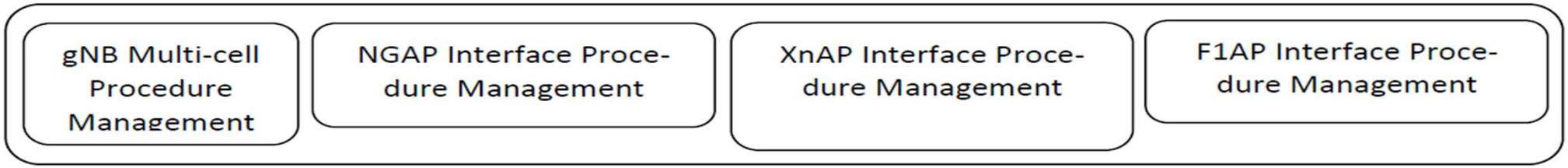


MAVENIR

CU-CP/UP: Functional Blocks

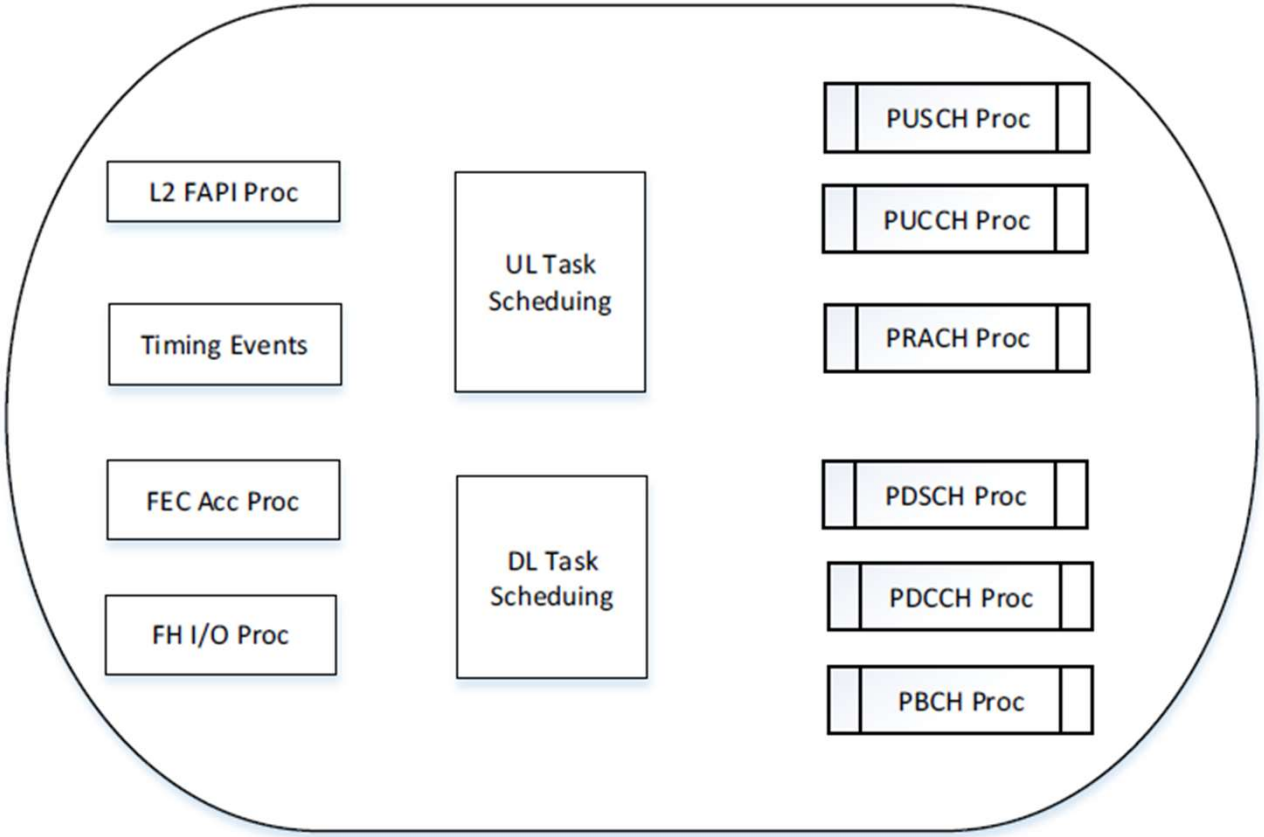


gNB Procedure Management



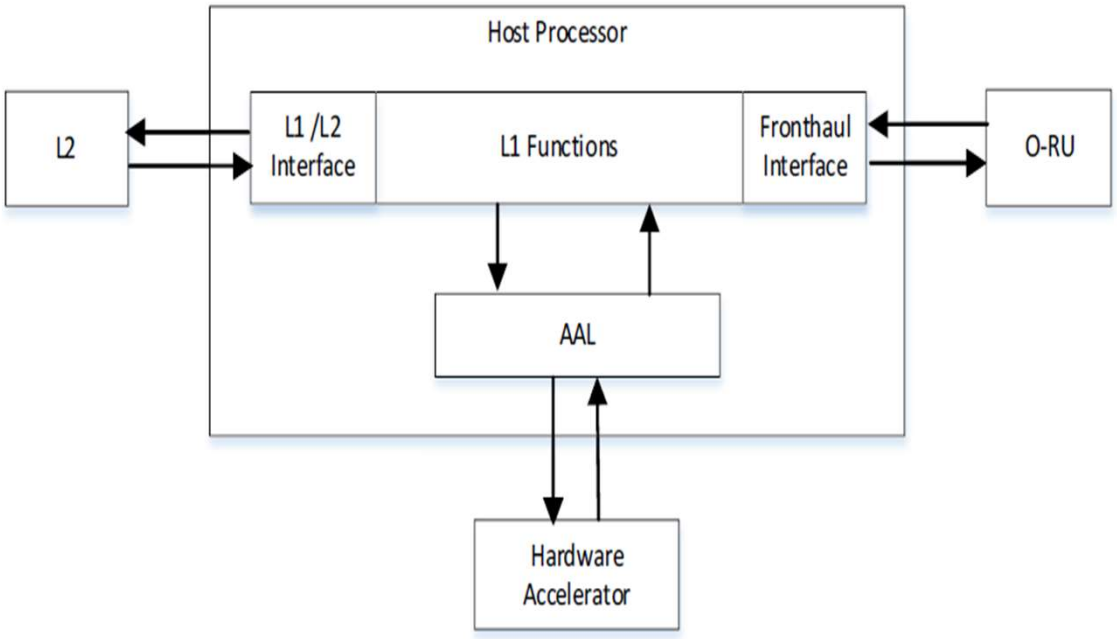
Ref: O-RAN.WG8.AAD.0-R003-v09.00

L1 related tasks

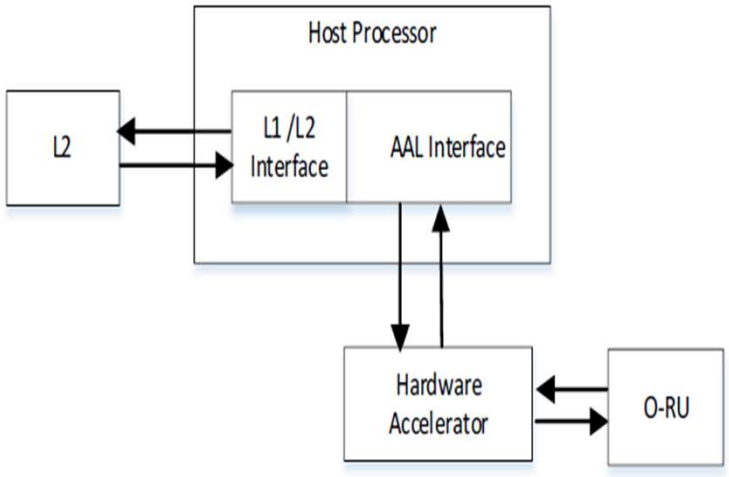


Ref: O-RAN.WG8.AAD.0-R003-v09.00

(Implementation dependent) L1 Accelerator

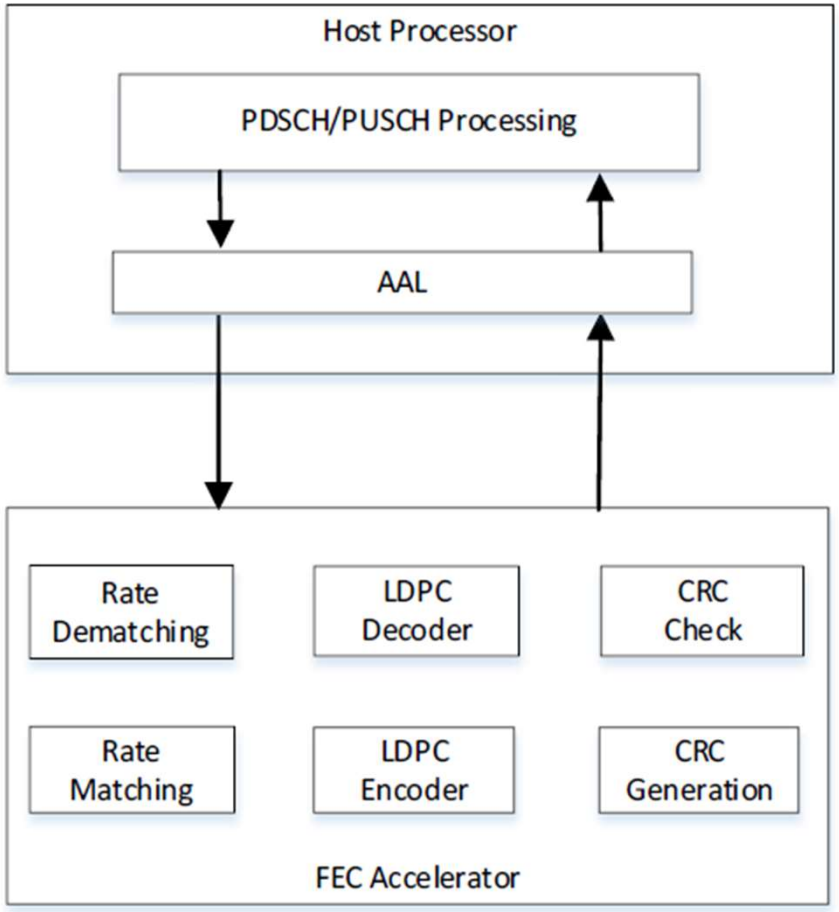


Lookaside Acceleration model



Inline acceleration model

Ref: O-RAN.WG8.AAD.0-R003-v09.00



Lookaside FEC accelerator
(implementation dependent)

Ref: O-RAN.WG8.AAD.0-R003-v09.00

MAVENIR
Trust the Future

O-RAN RIC, 3GPP-AIML

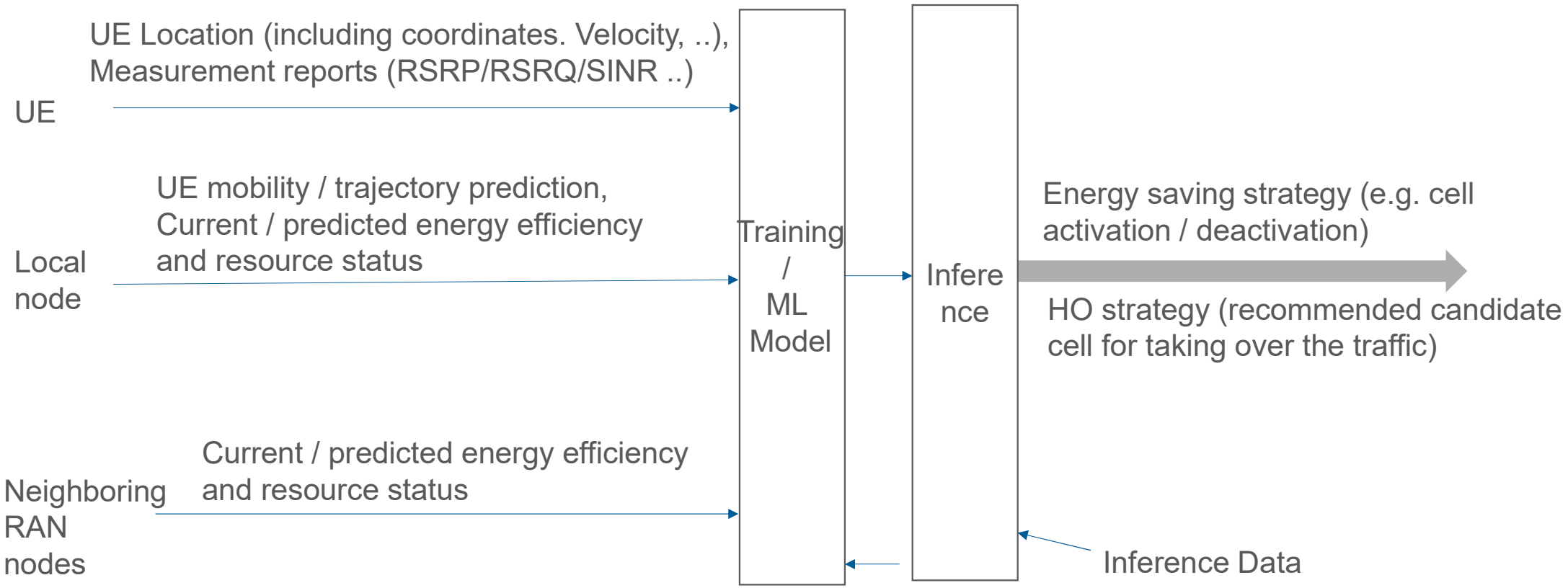
Some of RAN-AIML use cases: 3GPP, O-RAN

- Network Energy Saving
- Mobility Optimizations
- Load Balancing
- QoS / QoE
- CSI feedback enhancement (e.g., overhead reduction, improved accuracy, prediction)
- Beam management
  - (e.g., beam prediction in time, and/or spatial domain for overhead and latency reduction, beam selection accuracy improvement),
- Positioning accuracy enhancement for different scenarios including heavy NLOS conditions

Network Energy Saving

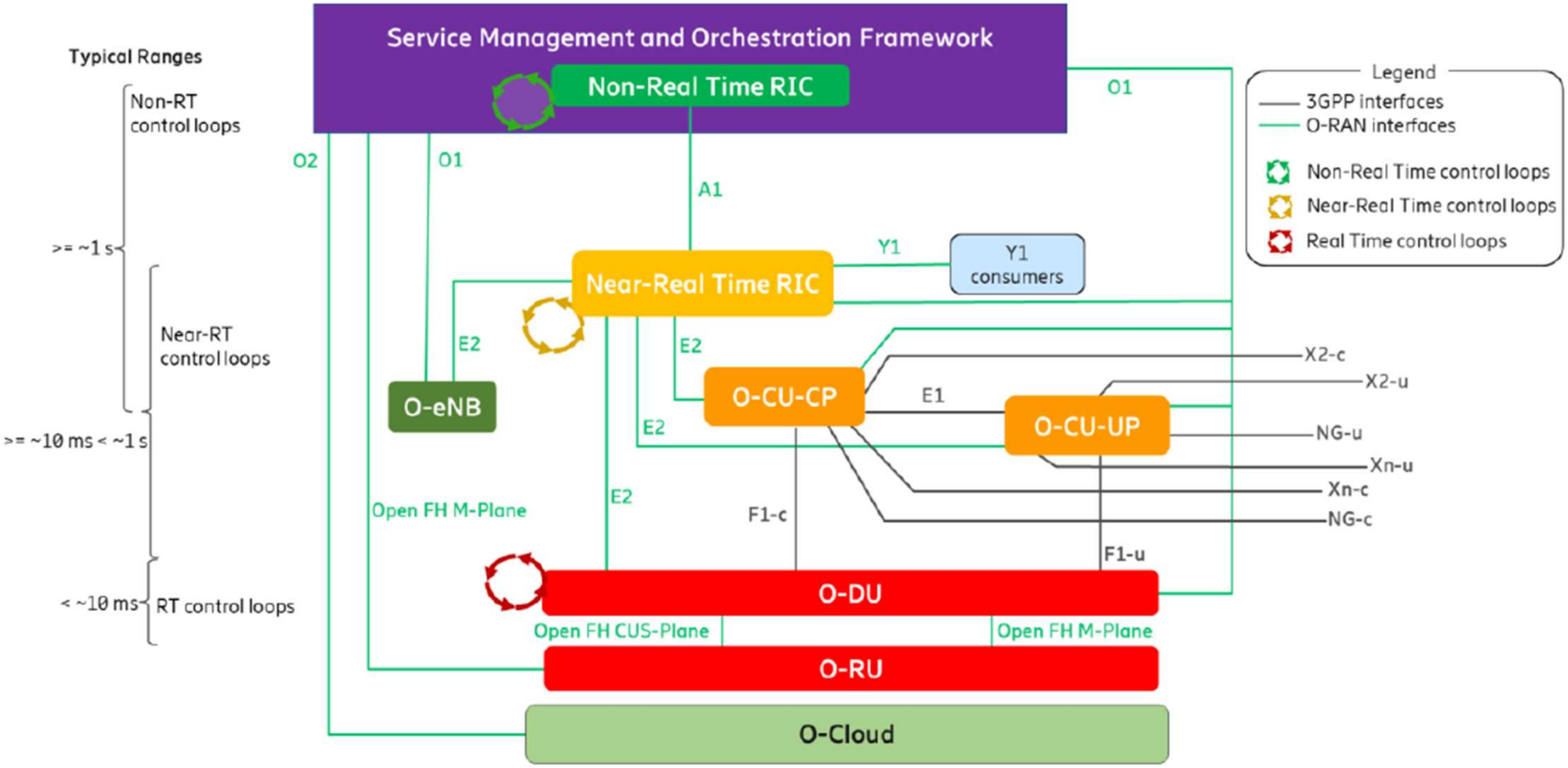
- Cell activation / deactivation
  - Traffic offloading in a layered structure
  - e.g. switch off a cell when traffic volume is lower than a fixed threshold and offload some UEs to a new target cell
- Some issues
  - Wrong switch-off of the cells and wrong traffic offload can degrade performance
  - Inaccurate cell load prediction
  - “System performance / KPIs vs. energy efficiency” trade-off
  - Difficult to find the right set of parameters (e.g, thresholds for activation / deactivation, time duration to switch-off, ..)
  - Local vs. global optimization decisions
- For optimal energy saving decisions
  - Load situation at different RAN nodes, KPI / QoS requirements, number of active UEs, mobility, cell utilization, etc.

Network Energy Saving (Contd.)



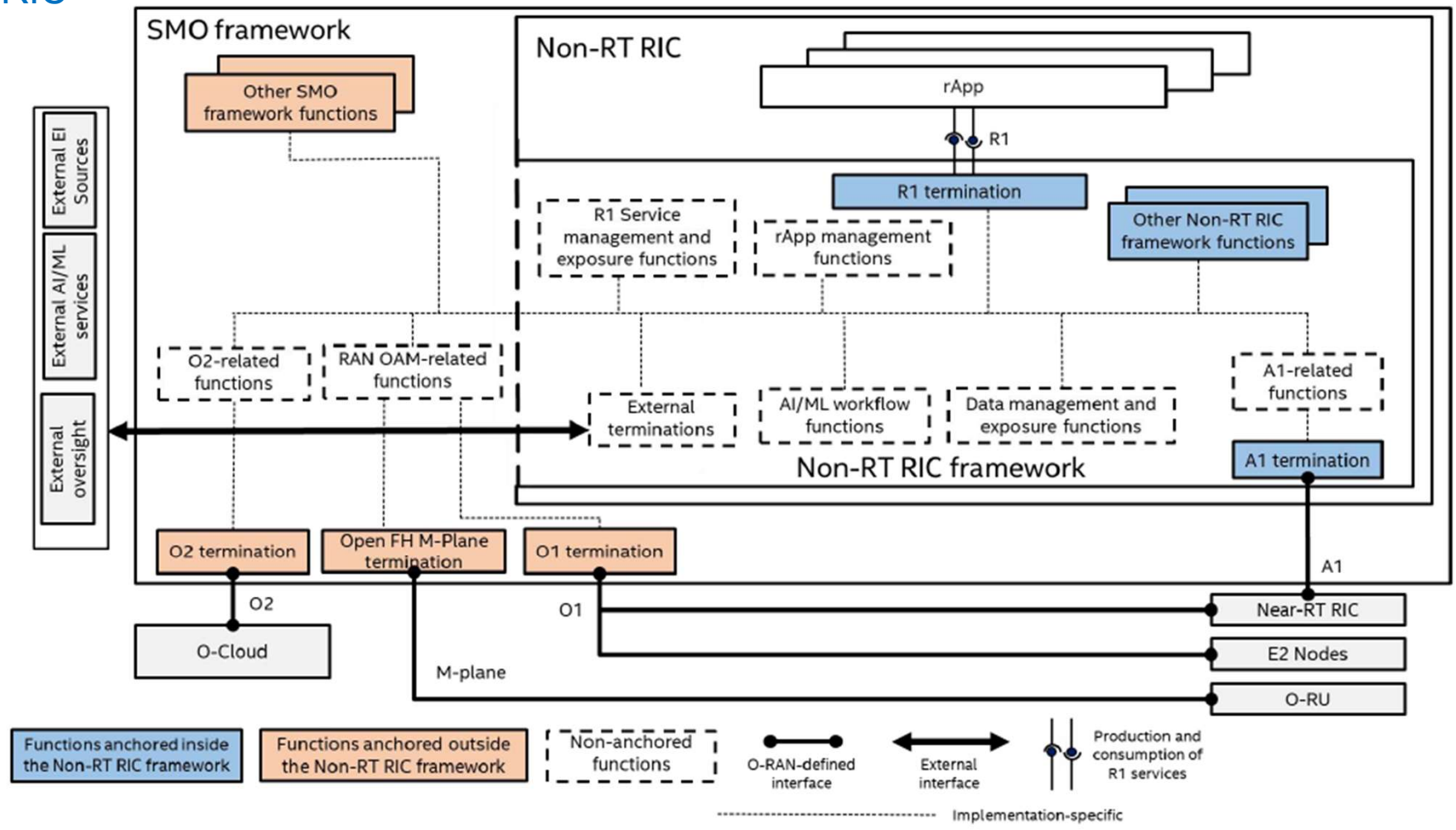
Ref: 3GPP

Non-RT, Near-RT and RT Control Loops



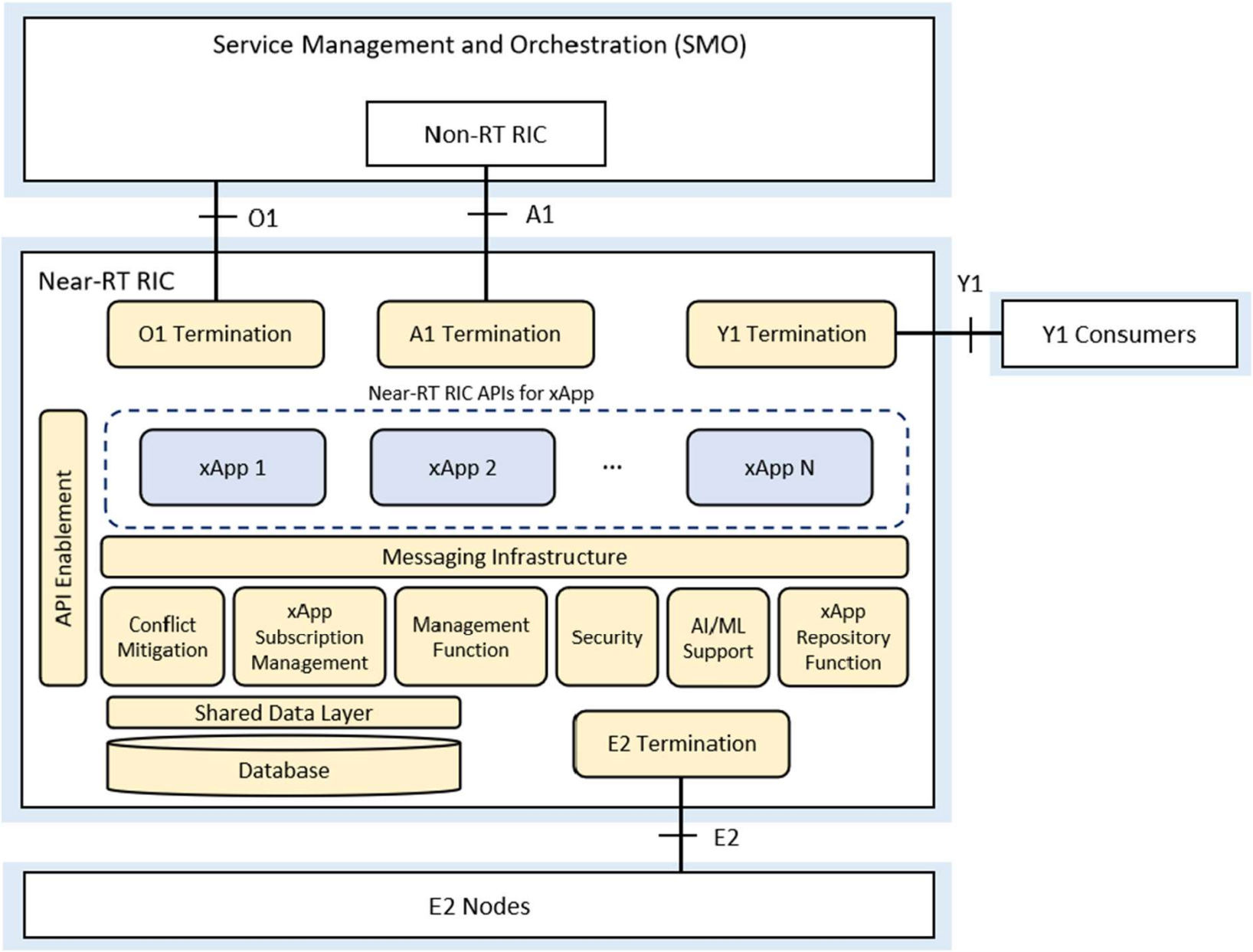
O-RAN: RIC Specs

Non-RT RIC



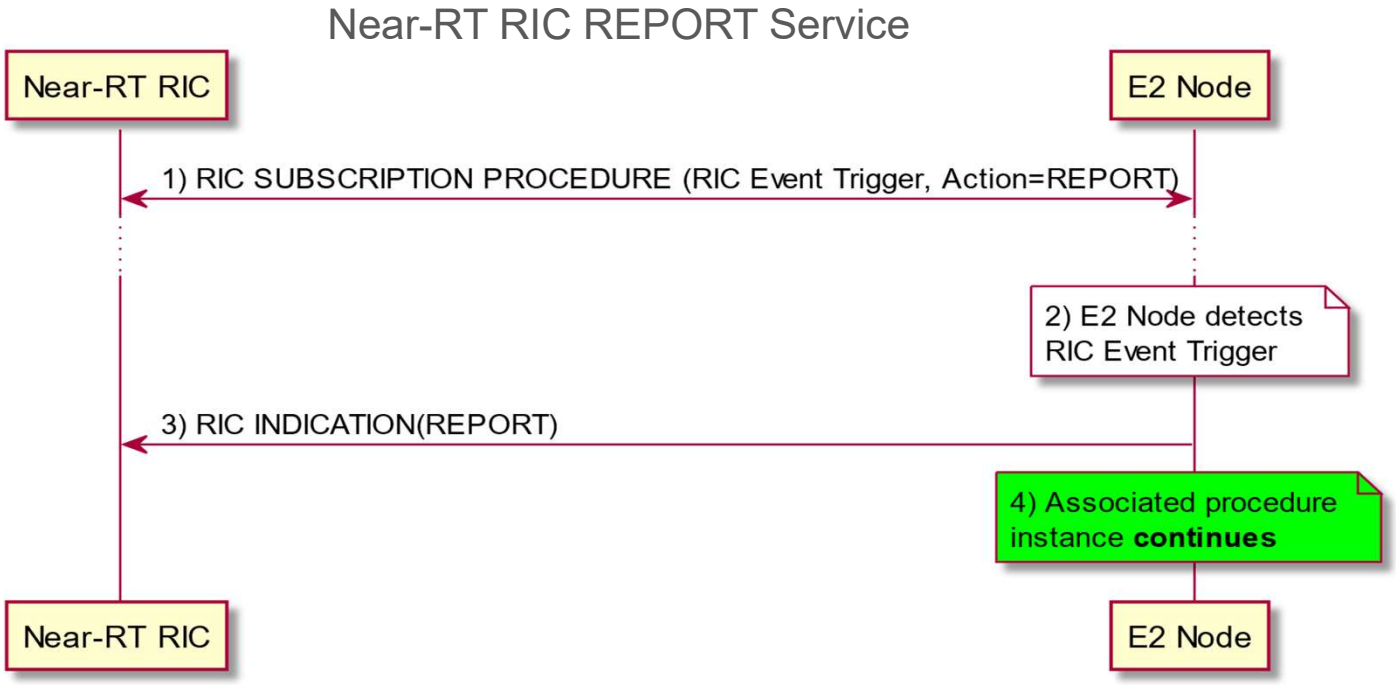
Ref: O-RAN.WG2.Non-RT-RIC-ARCH-R003-v03.00

Near-RT RIC



O-RAN: RIC Specs

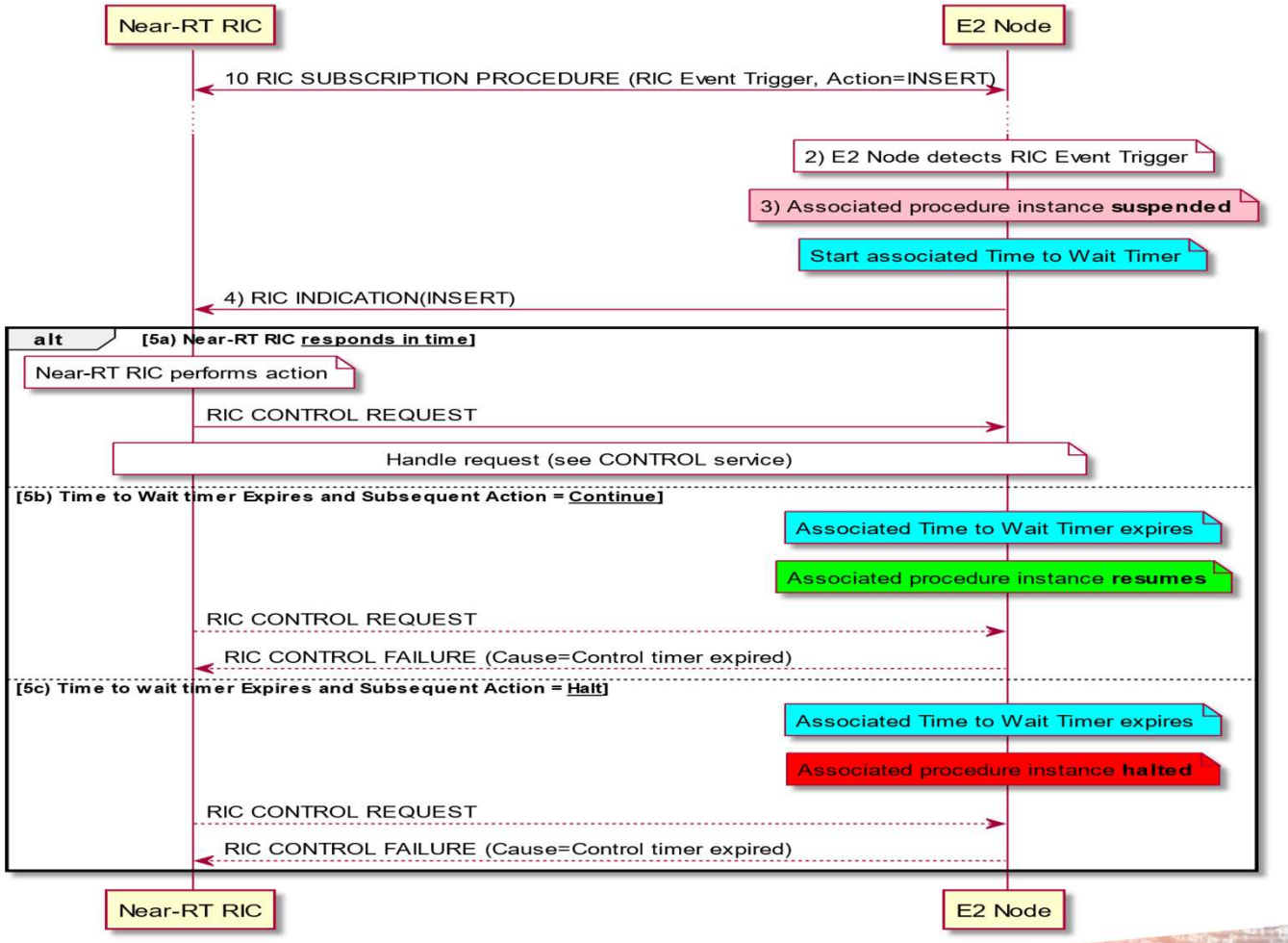
Near-RT RIC (Contd.)



Near-RT RIC Services (REPORT, INSERT, CONTROL and POLICY)

Near-RT RIC support functions, which include, e.g., E2 Interface Management (E2 Setup, E2 Reset, Reporting of General Error Situations etc.) and Near-RT RIC Service Update (capability exchange related to the list of E2 Node functions exposed over E2 etc.).

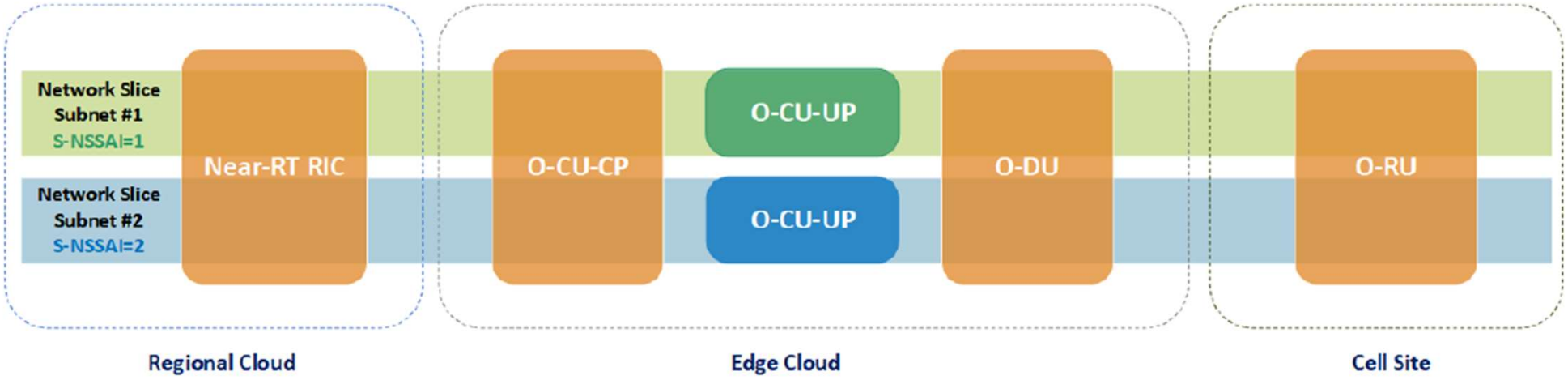
Near-RT RIC INSERT and RIC CONTROL



MAVENIR
Trust the Future

Network Slicing

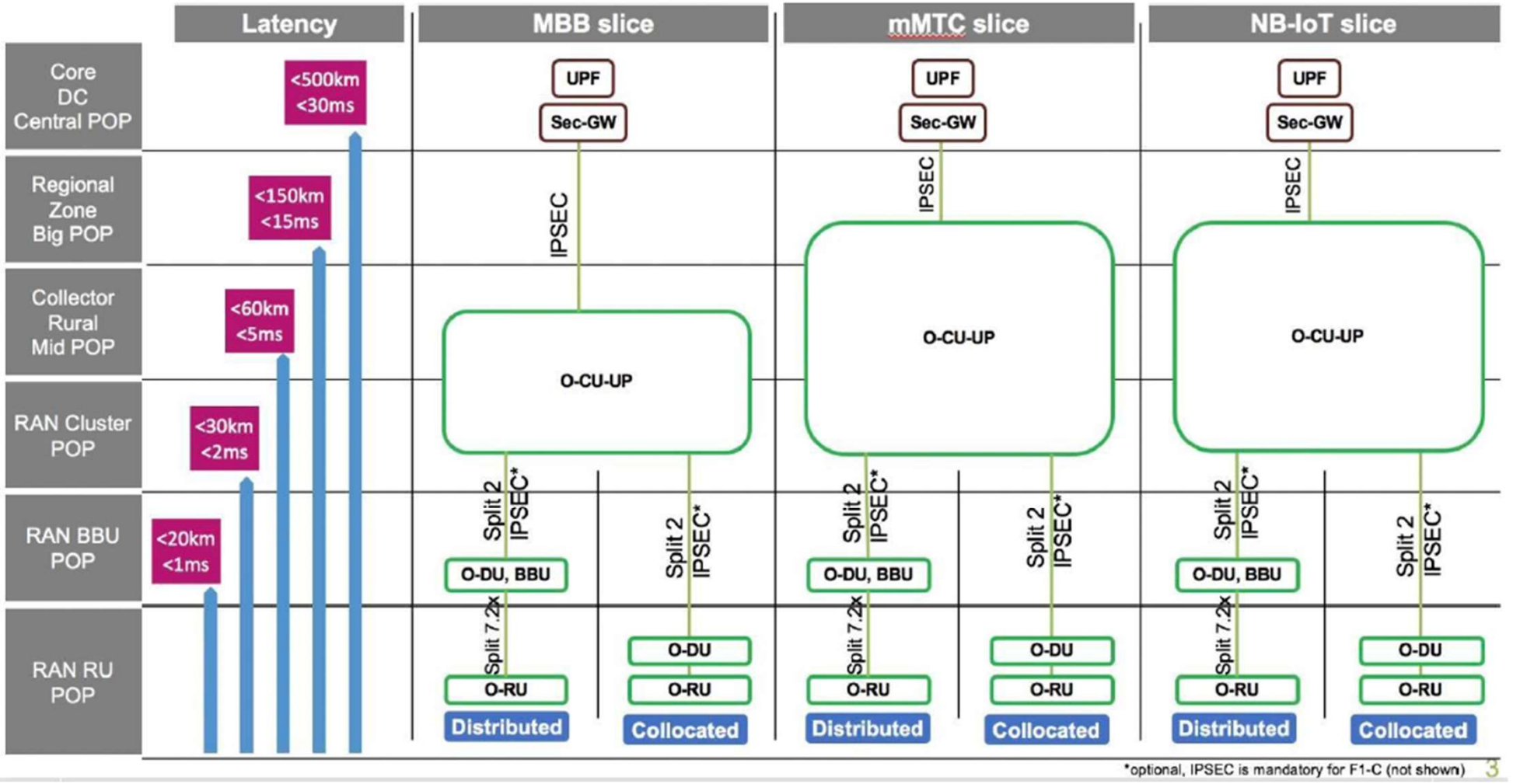
Slicing Deployment – An Example



Ref: O-RAN.WG1.Slicing-Architecture-R003-v10.00

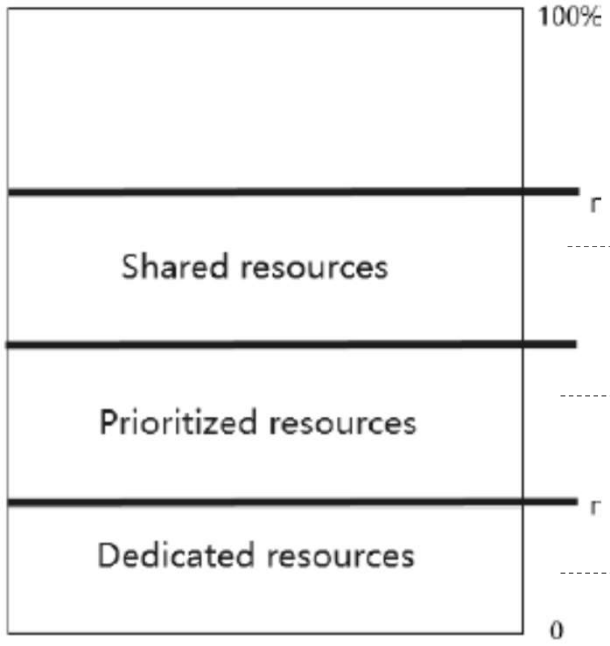
Slice/Service type	SST value
eMBB	1
URLLC	2
MIoT	3
V2X	4
HMTC	5

Ref: 3GPP TS 23.501



Ref: O-RAN.WG1.Slicing-Architecture-R003-v10.00

Slicing – Data Model



Structure of RRMPolicyRatio

rRMPolicyMaxRatio

rRMPolicyMinRatio

rRMPolicyDediatedRatio

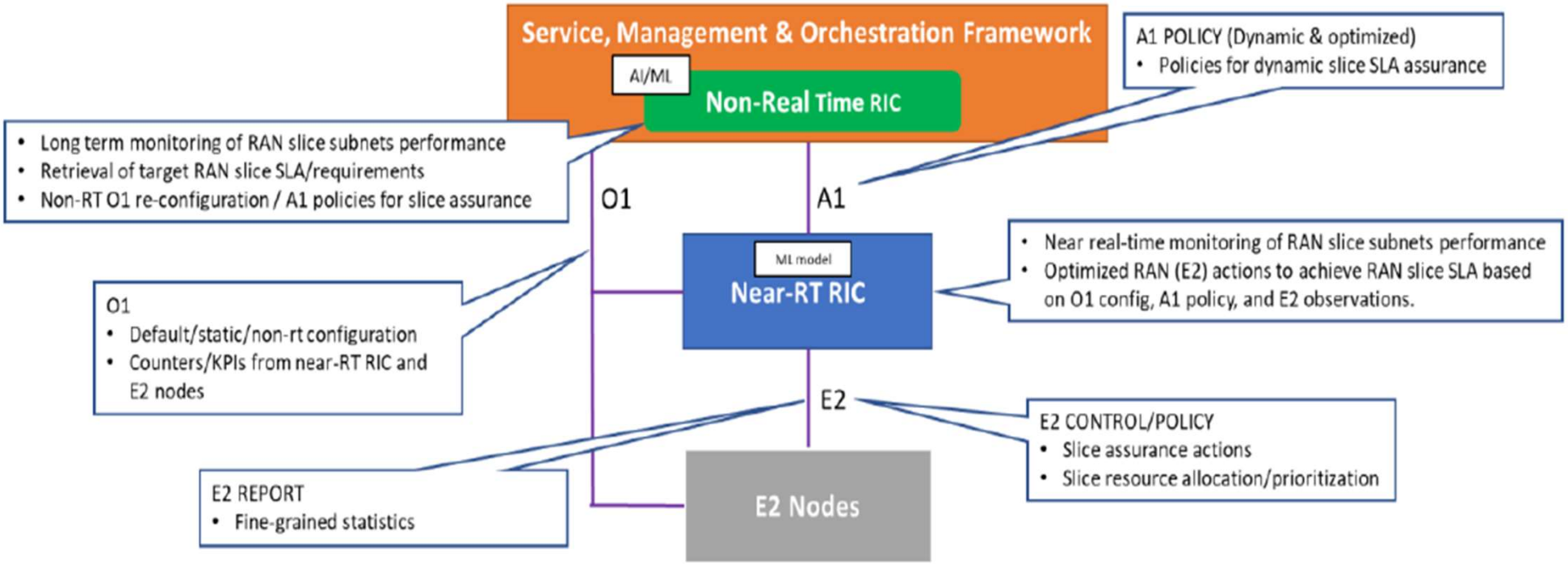
Shared resources: Shared among slices with no specific guarantees per slice

Prioritized resources: Guaranteed for use by specific slices but other slices can use these are available (i.e. when the slices for which these are prioritized are not using these)

Dedicated resources: Dedicated resources for the associated slices

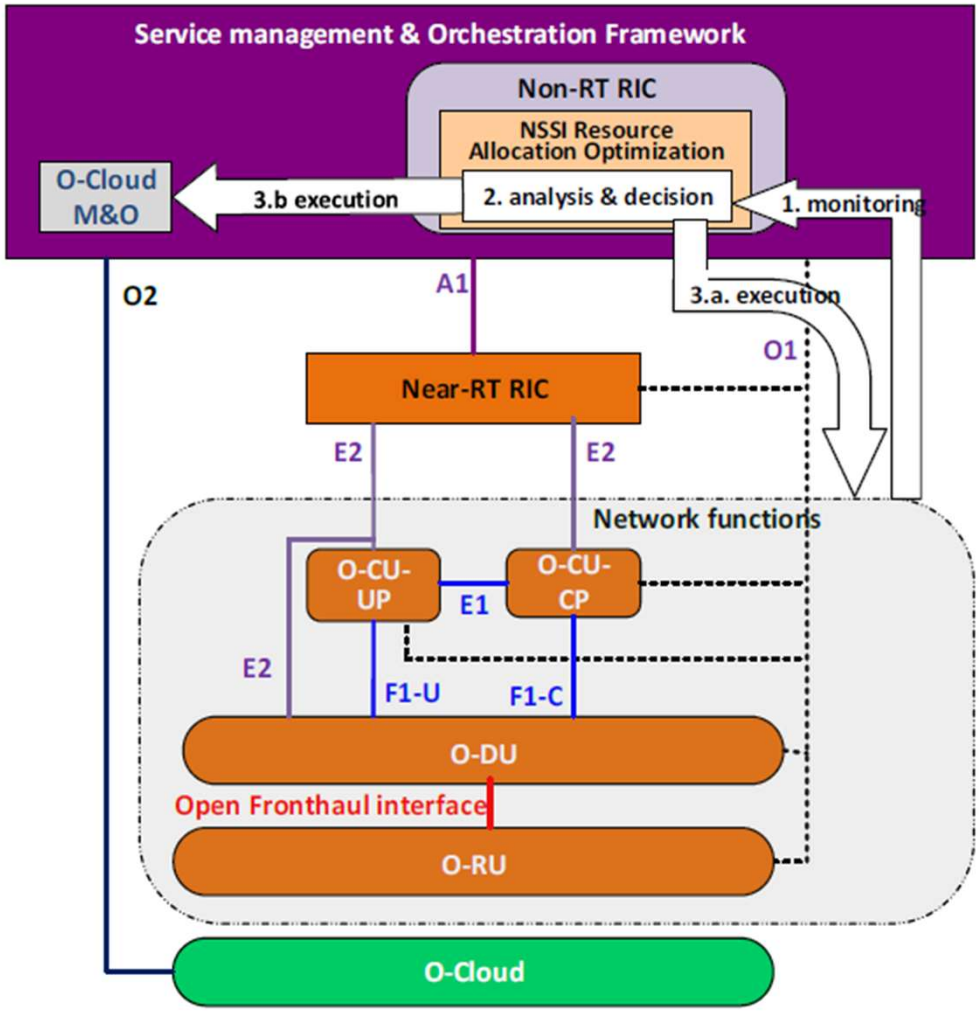
Reference: 3GPP TS 28.541

RAN Slice Assurance



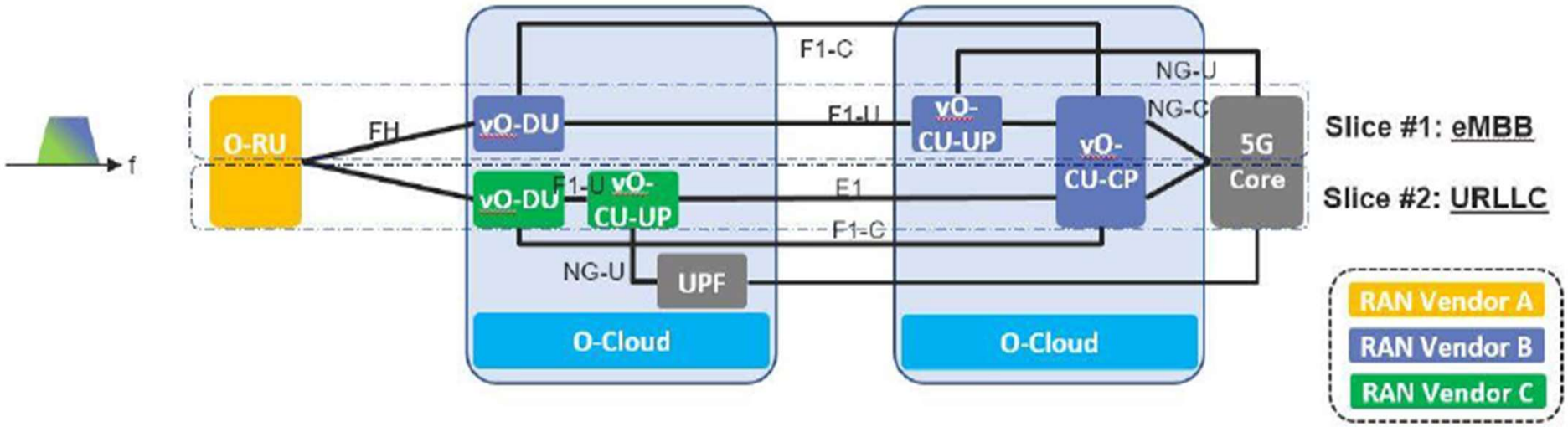
Ref: O-RAN.WG1.Slicing-Architecture-R003-v10.00

Resource Allocation Optimization



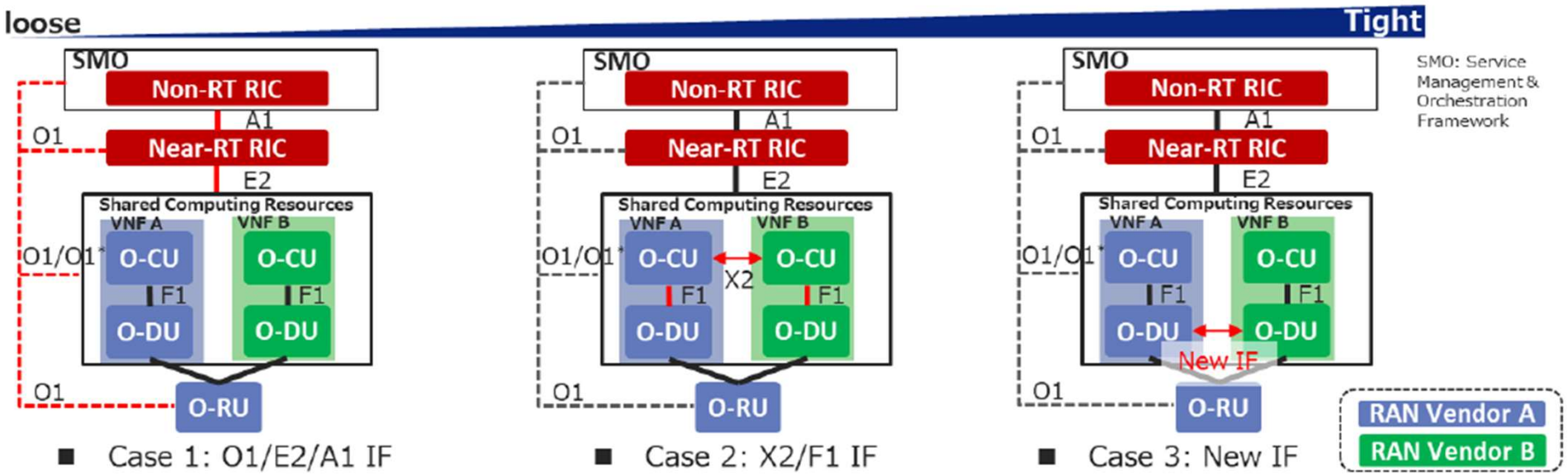
Ref: O-RAN.WG1.Slicing-Architecture-R003-v10.00

Multi-Vendor Slices



Ref: O-RAN.WG1.Slicing-Architecture-R003-v10.00

Multi-Vendor Slices (Contd.)



Ref: O-RAN.WG1.Slicing-Architecture-R003-v10.00

MAVENIR
Trust the Future

3GPP and O-RAN Security

5G – Security

- UICC / USIM
- (K)

4G / eNodeB, MME, ….

HSS
(K)

- UICC / SUPI,
- SUCI (Subscriber Concealed Identifier)
- (K)

5G / gNodeB, AMF,
- Security Anchor Function (SEAF / AMF)

- Authentication Server Function ,
- UDM,
- ARPF, SIDF (Subscriber Identifier De-concealing Function)
- (K)

3GPP: Ciphering and Integrity Algorithms

Ciphering Algorithms

NEA0	Null ciphering algorithm;
128-NEA1	128-bit SNOW 3G based algorithm;
128-NEA2	128-bit AES based algorithm; and
128-NEA3	128-bit ZUC based algorithm.

NEA0, 128-NEA1, 128-NEA2: Mandatory for gNB

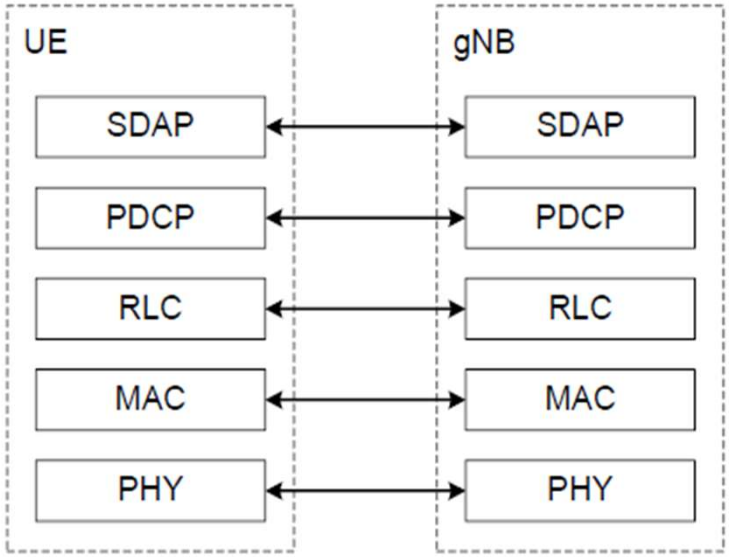
Integrity Algorithms

NIA0	Null Integrity Protection algorithm;
128-NIA1	128-bit SNOW 3G based algorithm;
128-NIA2	128-bit AES based algorithm; and
128-NIA3	128-bit ZUC based algorithm.

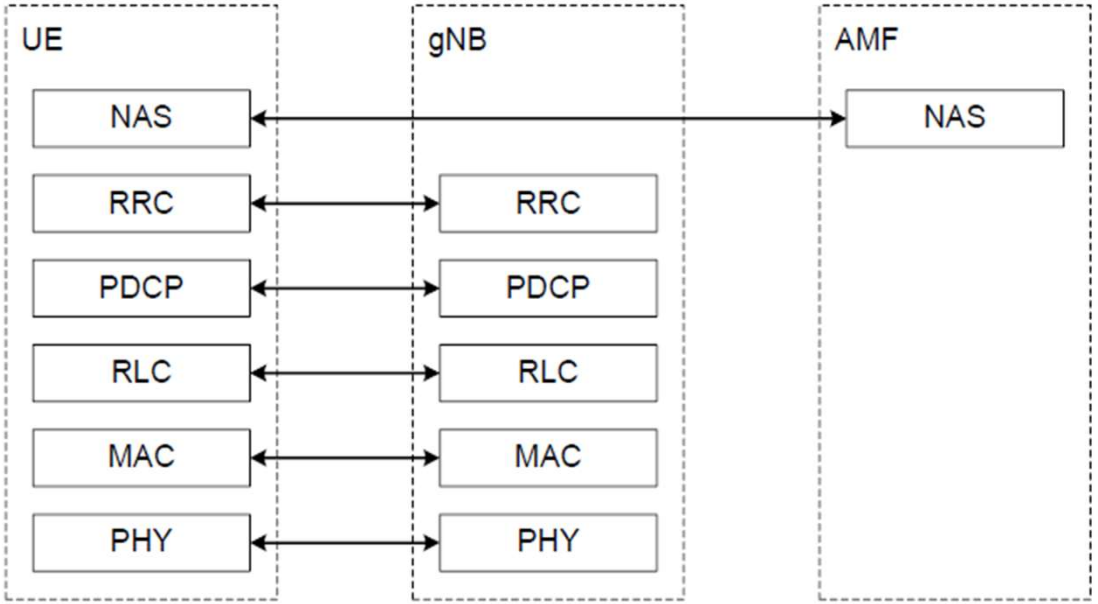
Ref: 3GPP TS 33.501

5G User and Control Plane: Security aspects

- User plane: Ciphering and integrity protection (PDCP)
  - Supported (though optional to use)
- Control plane (RRC and NAS): Ciphering and integrity protection
  - Integrity protection for signaling: mandatory except for some messages



User Plane



Control Plane

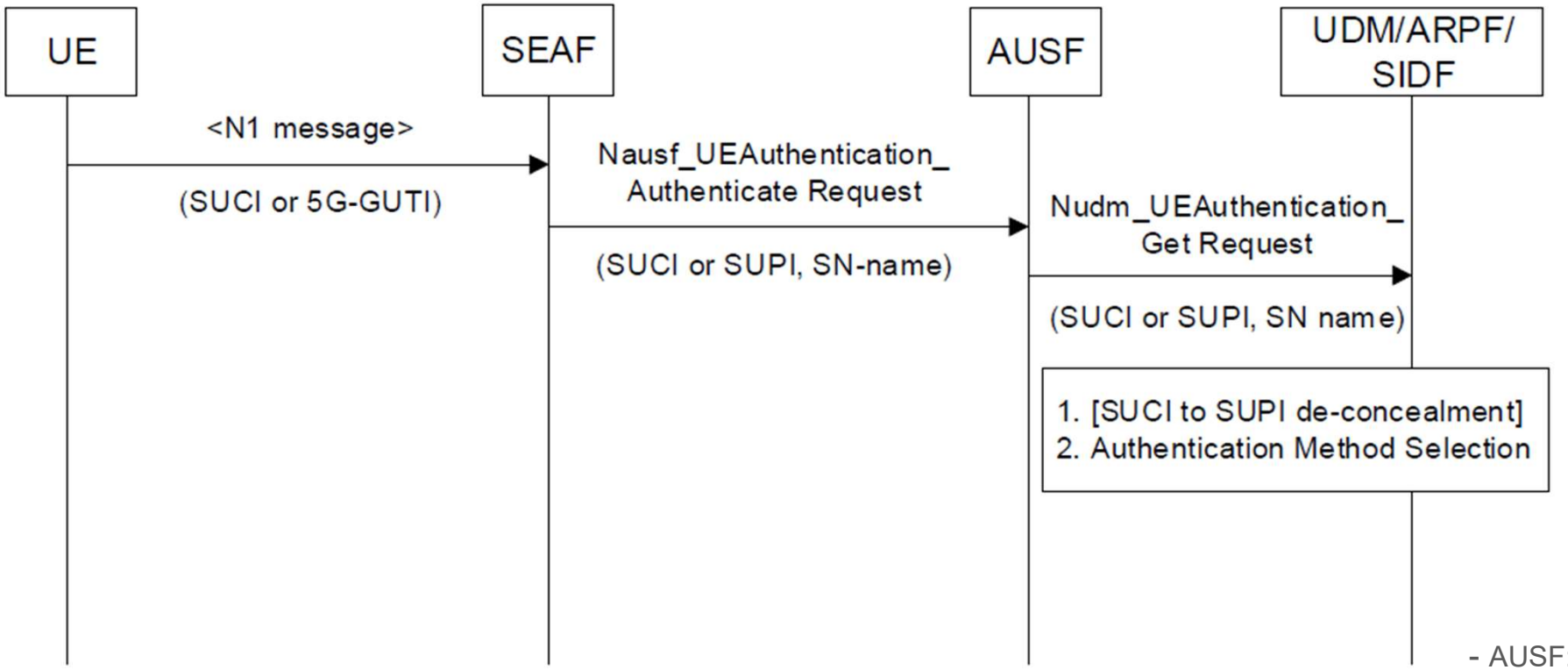
Subscriber Privacy

- SUPI
  - IMSI - MCC, MNC, Mobile Subscriber Identification number
  - NAI (for non-3GPP access)

- SUCI (Subscriber Concealed Identifier)
  - UE generates SUCI using public key of the Home Network
    - Conceals SUPI, ..
    - ECIES-based protection scheme with public key of the HN
  - On identification failure via GUTI, SUCI used instead of plain text SUPI
  - UDM / SIDF (Subscriber Identity De-Concealing Function)

- 5G GUTI (Global unique temporary identifier)

Authentication and Key Management



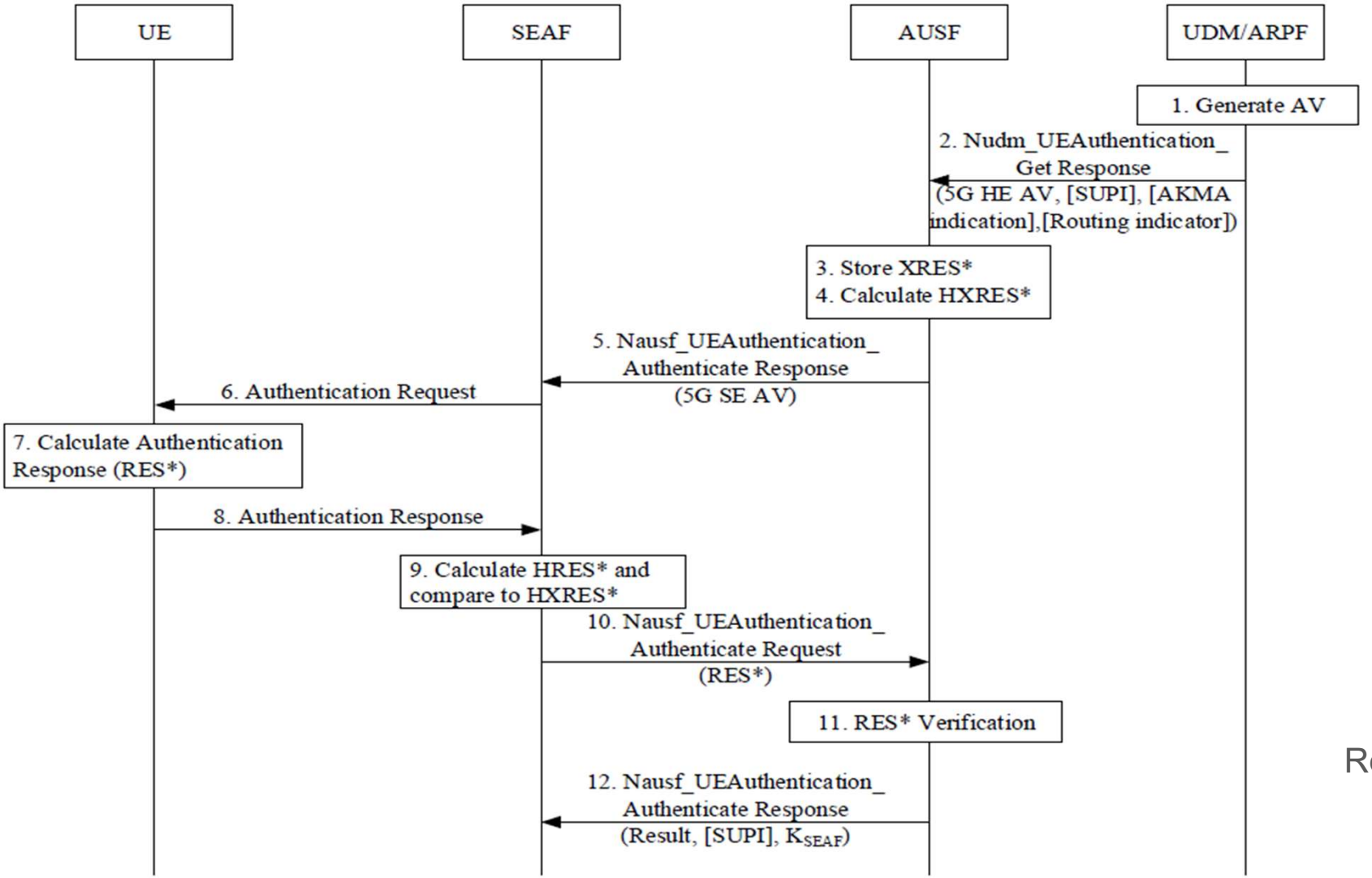
5G AKA, EAP-AKA' : Initiation

EAP-TLS can be used for Private 5G networks

Ref: 3GPP TS 33.501

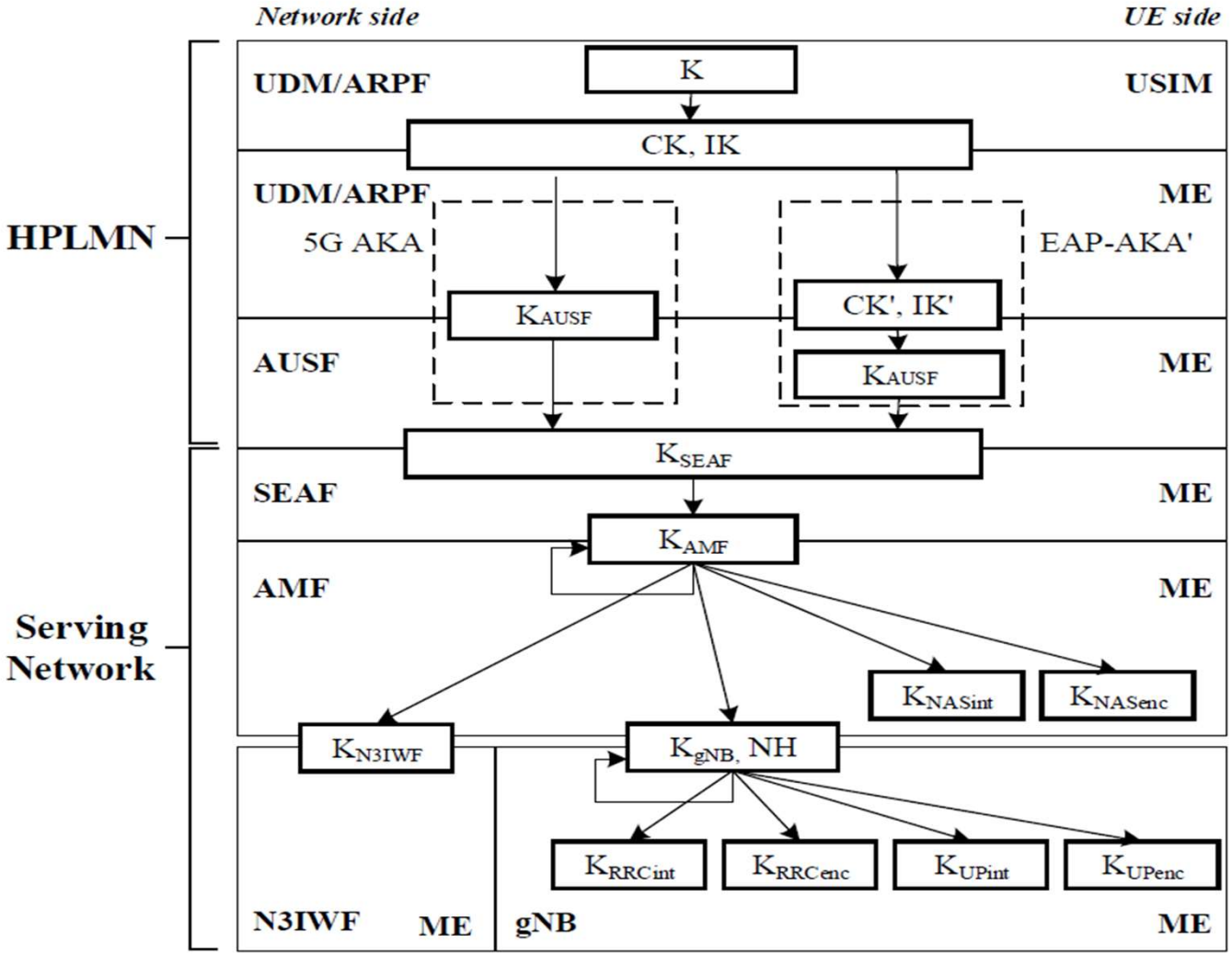
- AUSF: Authentication Server Function (AUSF)
-UDM: Unified Data Management
-ARPF: Authentication Credential Repository and Processing Functio (generates 5G HE AV)
-SEAF: Security Anchor Function
- Kseaf: Anchor key

5G AKA (Contd.)



Ref: 3GPP TS 33.501

5G AKA, EAP-AKA' : Key management

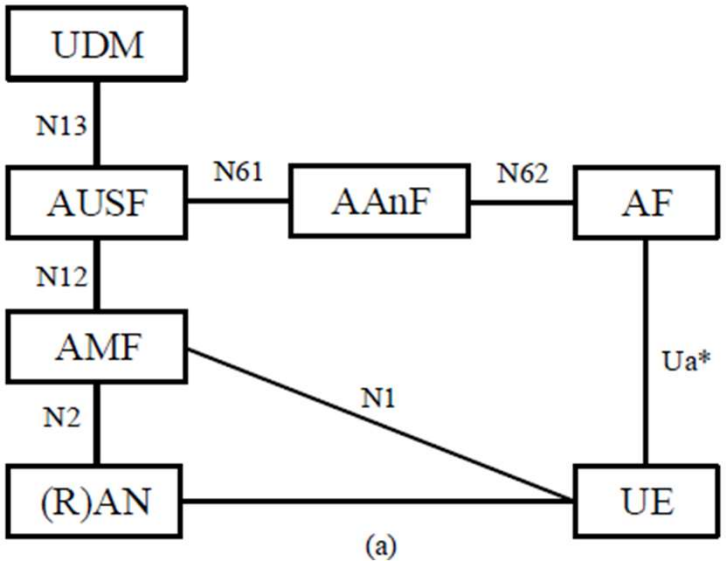


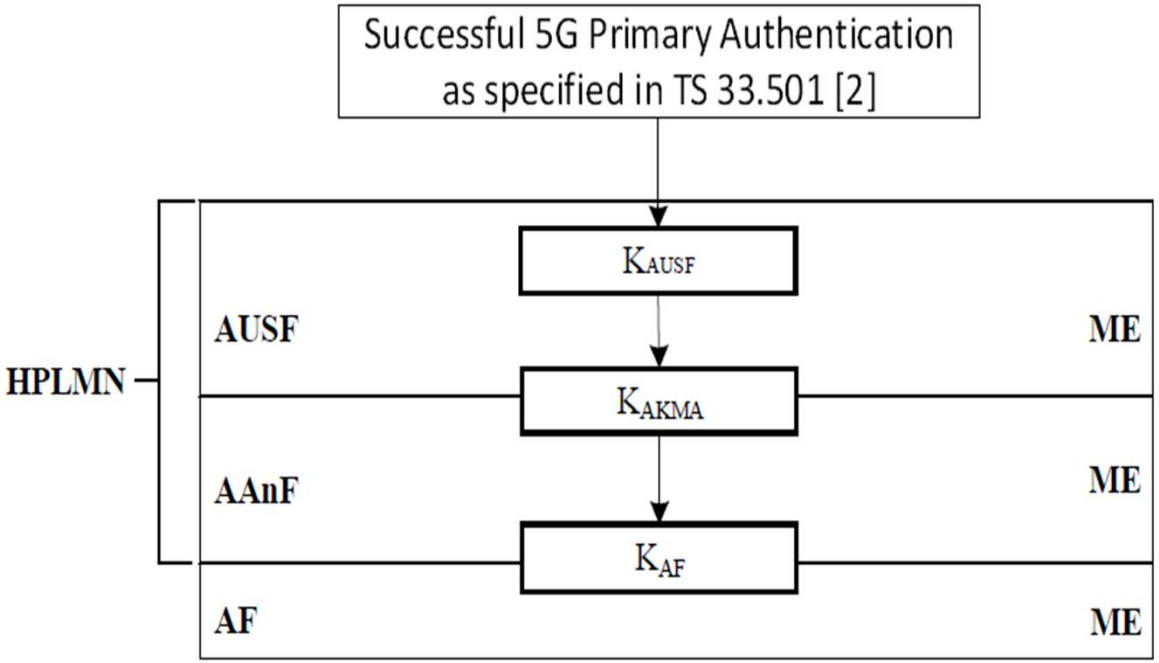
- Shared key
- Challenge response protocol

EAP-AKA': EMSK derived using EAP and first 256 bits used by Kausf

Ref: 3GPP TS 33.501

AKMA : AKM for Applications (Ref: 3GPP TS 33.535)



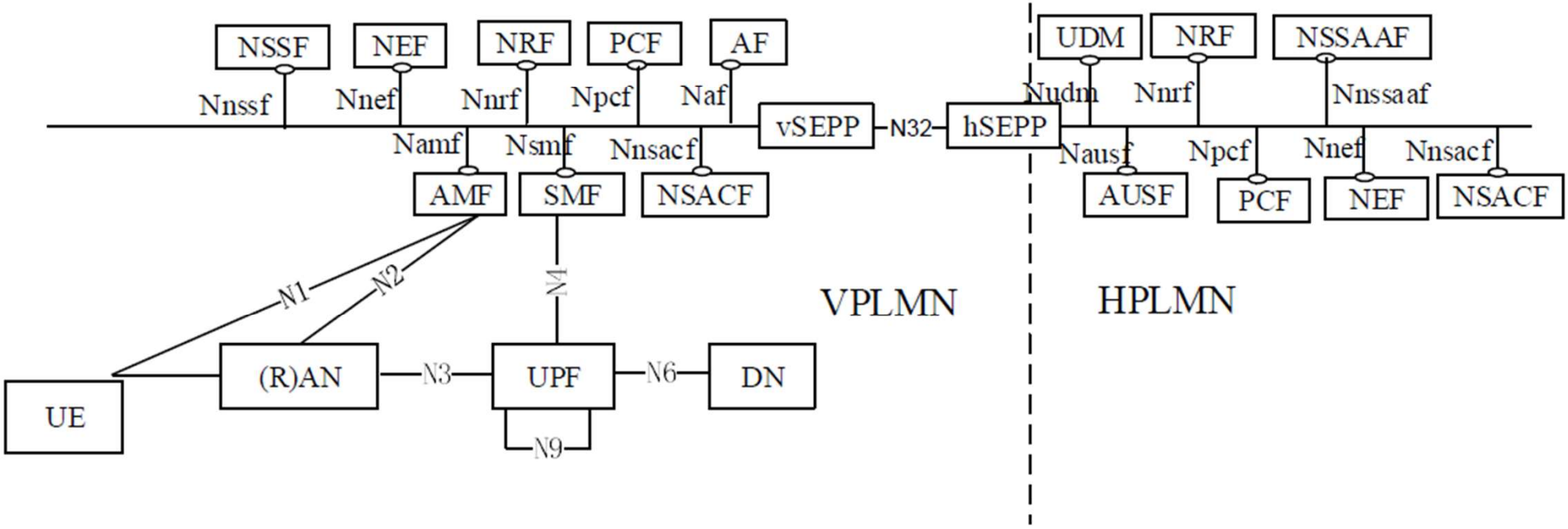


AAnF AKMA Anchor Function

- AKMA anchor key and SUPI stored in AAnF (after 5G authentication)
- Generates keys to be used between UE and AF

SEPP: Security Edge Protection Proxy

Roaming 5G Network Architecture (Ref: 3GPP TS 23.501)



SEPP: Security Edge Protection Proxy
AUSF: Authentication Server Function
UDM: Unified Data Management
AMF: Access and Mobility Management Function

The SEPP enforces inter-PLMN security on the N32 interface.

O-RAN Attack Surface

- O-RAN specific
  - SMO,
  - near-RT-RIC,
  - non-RT-RIC
  - A1,
  - E2,
  - O1,
  - O2,
  - FH

- Not exclusive to O-RAN
  - Decoupling of HW and SW with use of third-party x-Apps and r-Apps
  - Containerization and virtualization

  -

Need to protect data / control plane over various interfaces

O-RAN

- A1 interface
- O1 interface
- O2 interface
- E2 interface
- Y1 interface
- O-Cloud Notification interface
- Open Fronthaul interface

3GPP

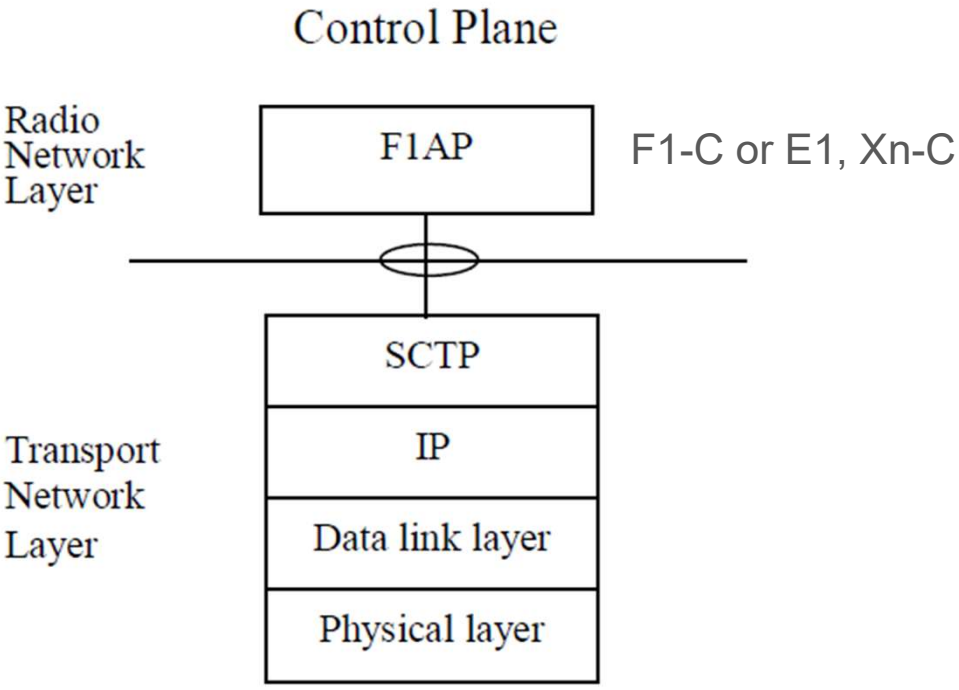
- E1 interface
- F1-c interface
- F1-u interface
- NG-c interface
- NG-u interface
- X2-c interface
- X2-u interface
- Xn-c interface
- Xn-u interface
- Uu interface

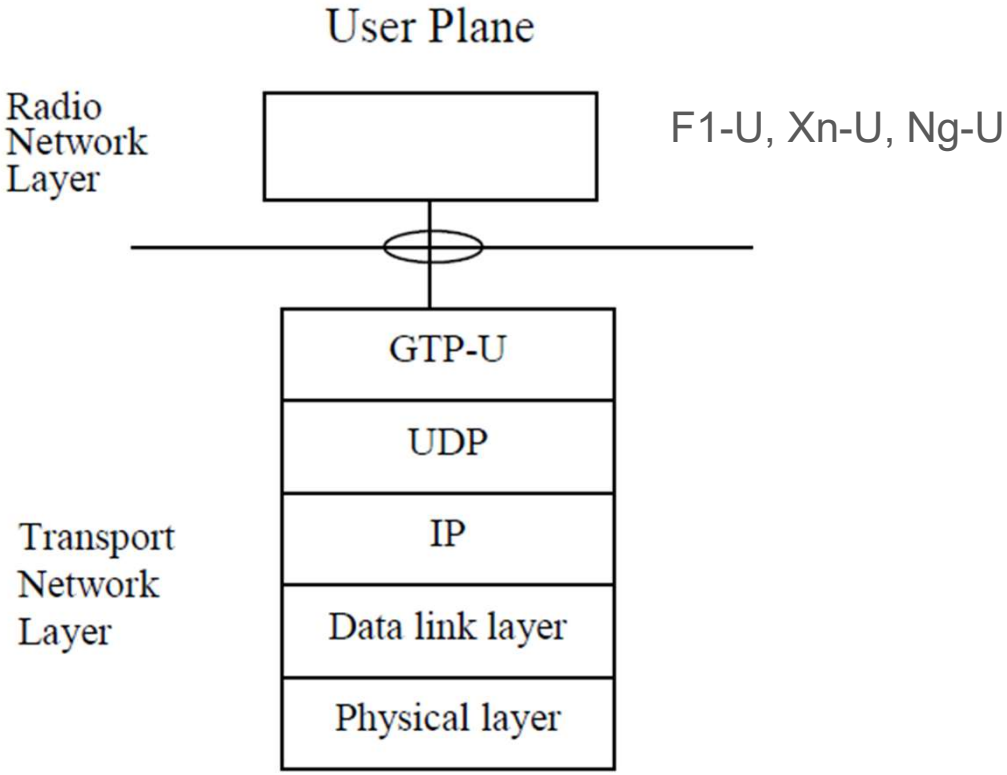
Some of the security protocols used in O-RAN networks

- TLS 1.2 and 1.3
  - O1 interface for NETCONF over TLS and JSON/REST over TLS
  - A1 interface
  - Open FH-M plane
- IPsec
  - E2, F1-U, Xn-U, Ng-U
  - F1-C, E1, Ng-C
- SSHv2 (Secure Shell 2.0)
  - O1 interface and Fronthaul M-Plane for NETCONF over SSH
- DTLS 1.2
  - E1, F1-C, Xn-C, Ng-C
- IEEE 802.1X
  - 802.1X port-based network access control for authentication and authorization of PTP nodes
  - RU – C/S
- FTPS
  - Protect file transfer over O1, open-FH M plane

F1, E1, Xn, Ng Interfaces – Security aspects

F1-C, E1, Xn-C, Ng-C: IPsec or DTLS
F1-U, Xn-U, Ng-U: IPsec





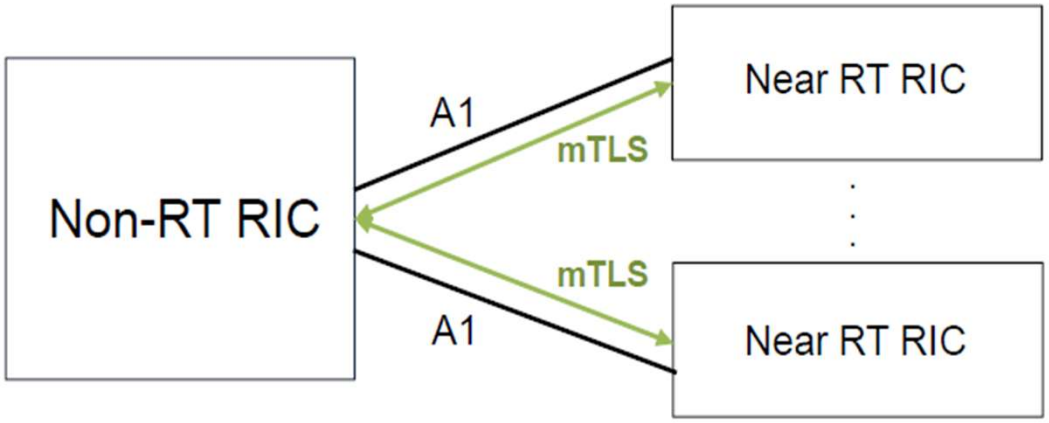
near-RT-RIC APIs: Security aspects

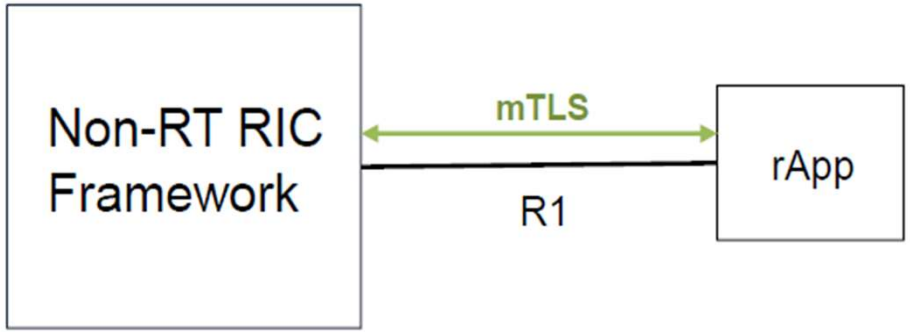
- Transactional APIs (REST and gRPC): mutual TLS (mTLS) authentication via X.509v3 certificates
  - e.g. between xApp and near-RT-RIC platform
- Time critical APIs (e.g. E2 related APIs): IPsec with IKEv2 certificated-based authentication

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

Ref: O-RAN.WG11.SecReqSpecs.0-R003-v05.00

Near-RT RIC Interfaces (Contd.): A1, R1 - Security aspects

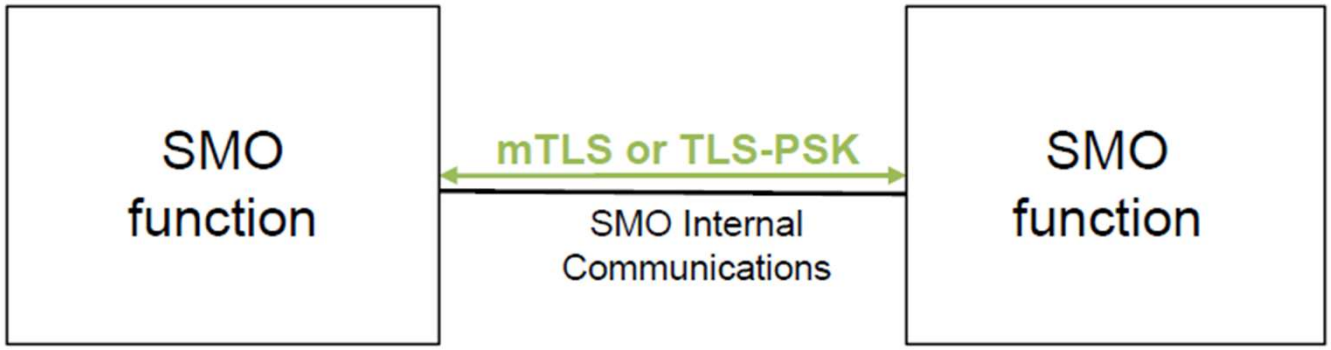




A1:
- Mutual authentication (mTLS),
- Ciphering, integrity protection…. (TLS), ..

R1
- Mutual authentication (mTLS),
- Ciphering, integrity protection…. (TLS), ..

SMO – Security aspects



- Security protection at transport layer: TLD
- Mutual authentication: mTLS, TLS-PSK

SMO Internal Communication

- Mutual authentication
- Confidentiality and integrity protection

Ref: O-RAN.WG11.SecReqSpecs.0-R003-v05.00

Some Challenges (and ongoing work)

- Time scale for AIML based decision making:
  - (Non-real-time → near-real-time) → real-time
- Works well for typical transport / mid-haul networks deployed by cellular opertaors
  - Performance optimizations for extremely unreliable mid-haul
- URLLC

References for standards related specs..

- https://www.o-ran.org/specifications
- https://www.3gpp.org/specifications-technologies
- https://www.ietf.org/


Thank You
MAVENIR