ALTIOSTAR

Leading Network Transformation

Security in Open vRAN

June, 17th 2021

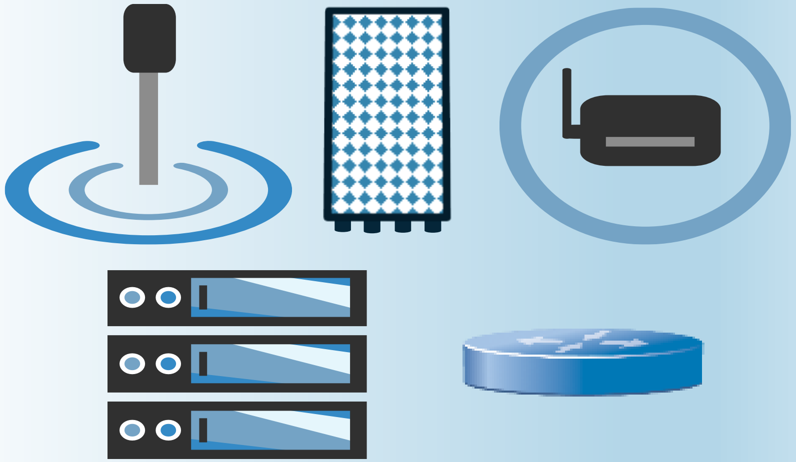
Nagendra Bykampadi
Director of Product Management and Standards (Security)
Altiostar

Altiostar Overview

Company

- First commercially deployed Open vRAN solution provider for 4G & 5G
- 500 people located in USA, India, UK, Italy, Japan, Dubai and Mexico
- 40+ patents
- $320M+ investment:
  - Rakuten
  - Qualcomm
  - Cisco
  - Telefónica
- Significant investment in R&D & QA

Products and Solutions



- Open RAN architecture solutions for 4G & 5G
- Cloud-Native RAN software (vCU & vDU)
- Macro, Indoor/Outdoor small cells, Massive MIMO & mmWave
- Running on COTS radios & servers
- IP reference design for Open RAN RRUs
- E2E certification

Market Traction

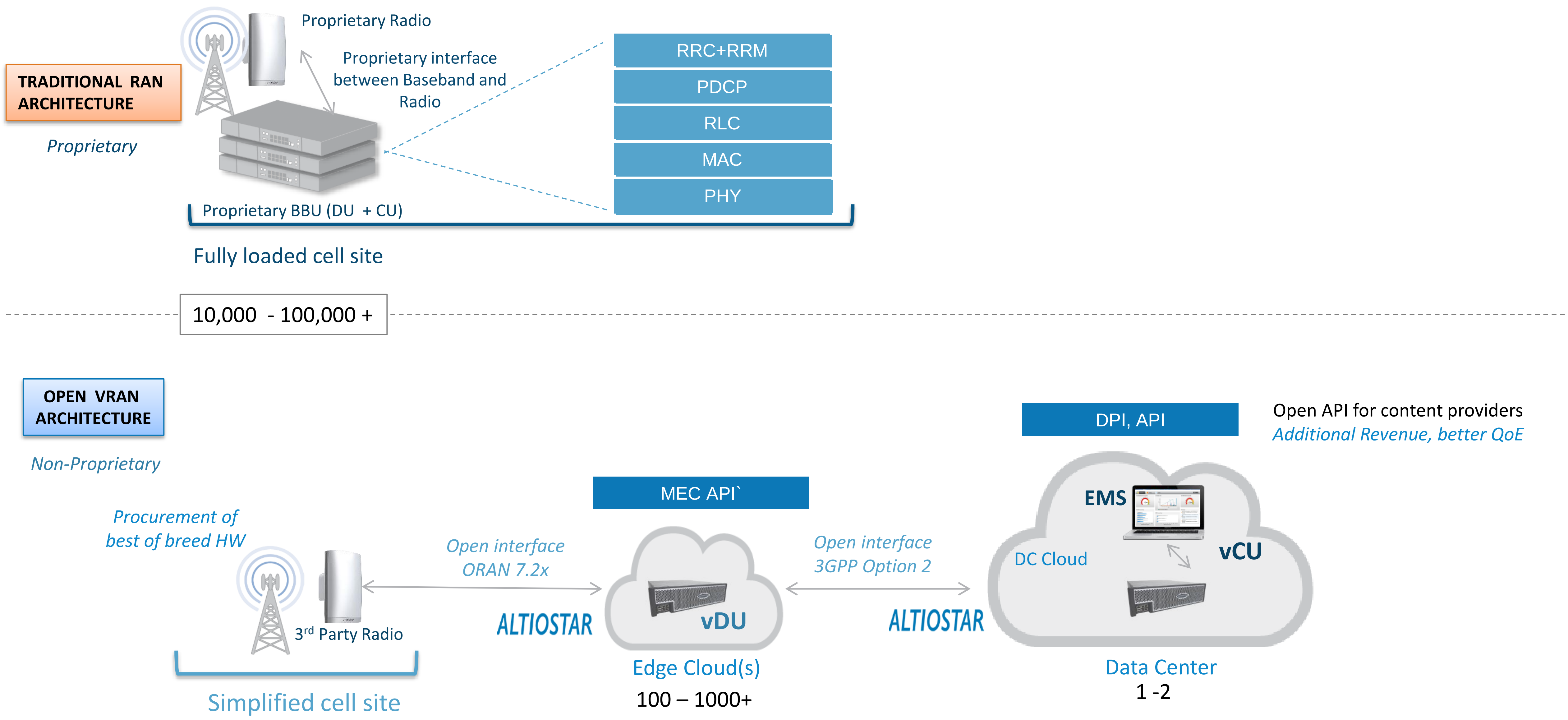
- Commercial Deployments (50000+ radios)
  - Rakuten Mobile (Japan)
  - Bharti Airtel (Small cells)
  - Telcel (Mexico)
  - GCI (USA)
  - TIM (Italy)
- Upcoming Deployments
  - Telefónica (4 countries)
  - DISH (USA) – first nation-wide Open RAN
  - Etisalat (UAE)
  - 10+ on-going projects across the globe
- Industry Associations
  - Open RAN Policy Coalition
  - O-RAN Alliance
  - Telecom Infra Project
  - 3GPP
  - GSMA
  - ETSI
  - Competitive Carriers Association
  - CBRS Alliance

Agenda

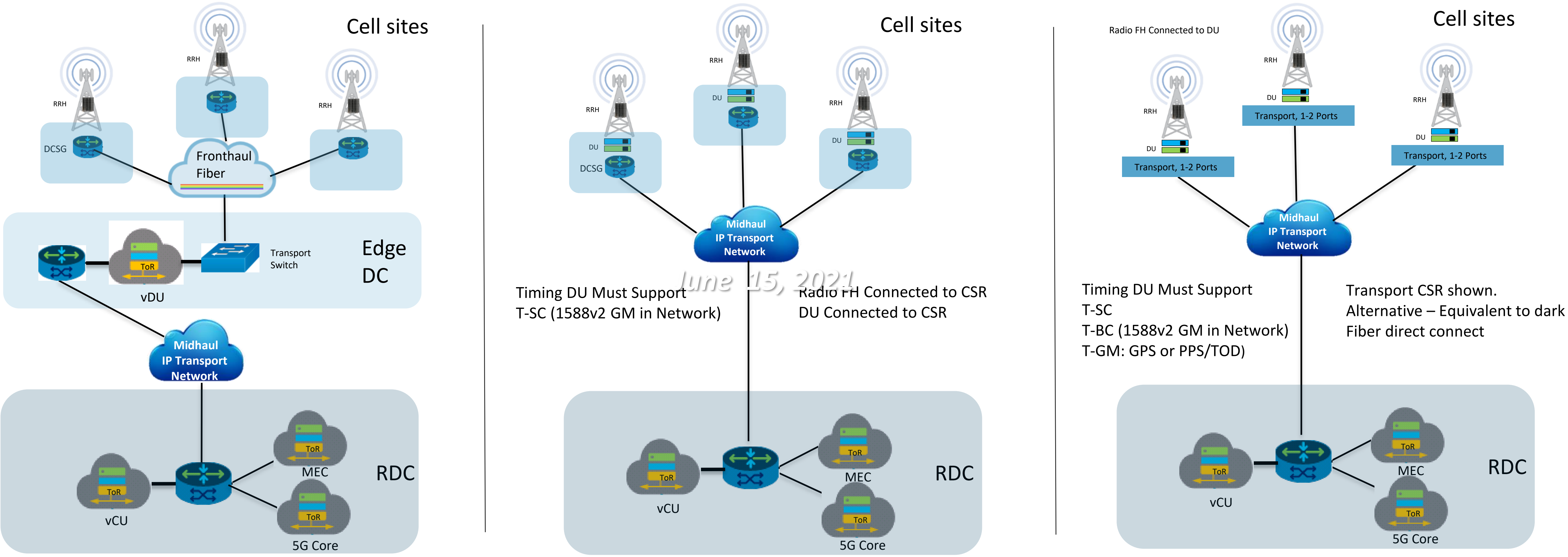
1. RAN virtualization, O-RAN architecture
2. Security in Open vRAN
3. Summary and key takeaways

RAN Virtualization and O-RAN Architecture

RAN Transformation With Virtualization



Open vRAN Network Topology



Aggregated DU vRAN

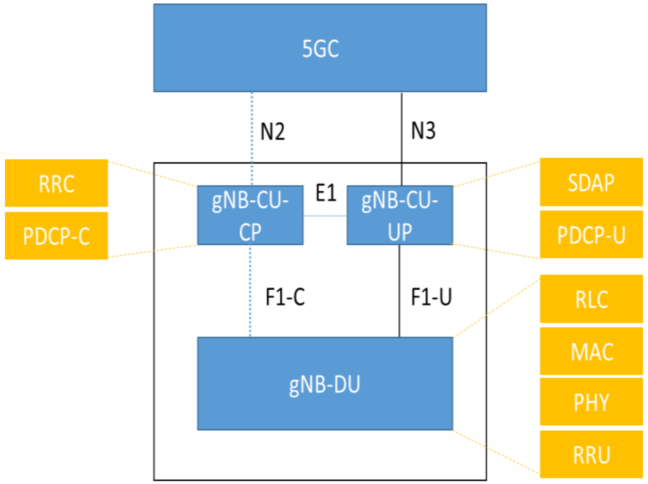
Distributed DU vRAN
LLS-C3

Distributed DU vRAN
LLS-C1

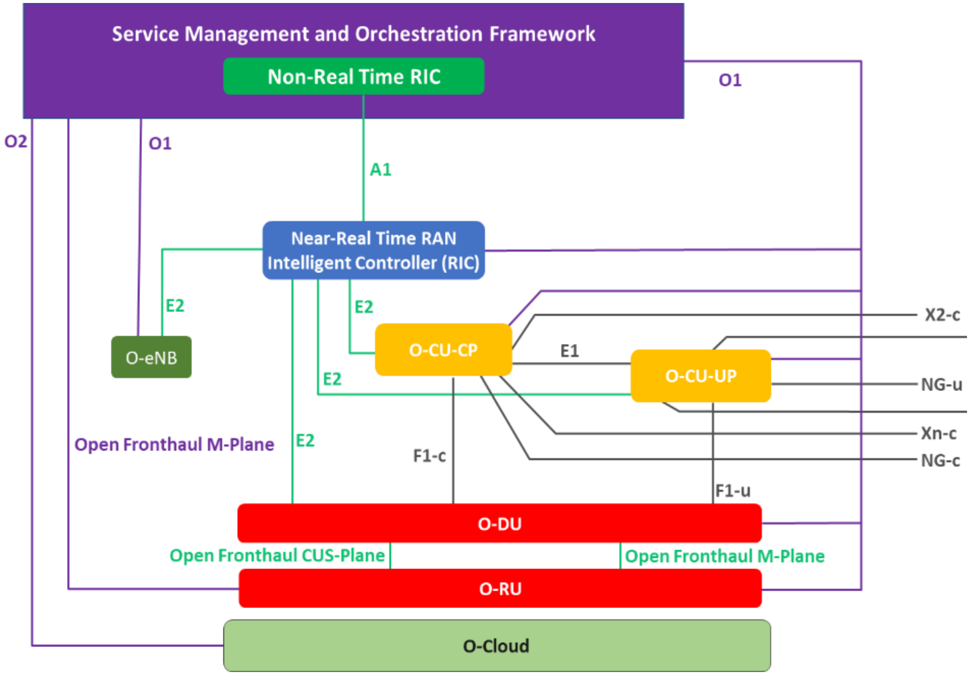
ALTIOSTAR

O-RAN Architecture

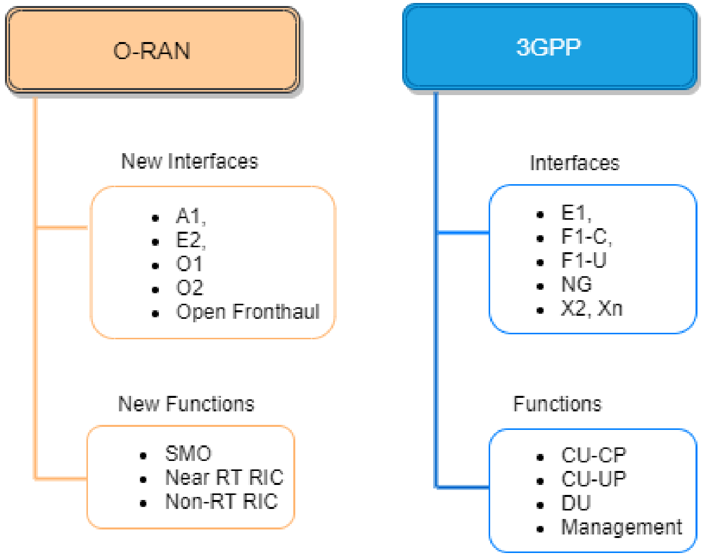
- O-RAN Alliance is specifying the O-RAN architecture. O-RAN is based on 3GPP's 5G NR architecture with the following enhancements:
  - Virtualizing RAN Network Functions
  - Open Fronthaul interface between O-RU and O-DU (LLS)
  - Disaggregating DU further into O-RU
  - Hardware – Software decoupling using cloud infra
  - RIC for intelligent management of Radio resources



gNB Logical Architecture in 3GPP



gNB Logical Architecture in O-RAN



Interfaces and Function split between O-RAN and 3GPP

Security in Open vRAN

ALTIOSTAR

Security concerns raised with Open RAN

Security threats coming from introducing an open interface between O-RU and O-DU (Open Fronthaul)

Threats due to malicious xApps in Near-RT RIC

- Being addressed by O-RAN Security Focus Group.
- Security countermeasures include protecting all open interfaces, authenticating and authorizing all Network Functions.

Security issues with s/w and h/w decoupling - VNFs running on COTS h/w (cloud infra)

Security risks attributed to containerization of the s/w

- 5GC has adopted Service Based Architecture based on cloud computing principles.
- Adopting best practices from cloud computing industry including hardening of cloud platforms, end-to-end container security based on DevSecOps.

Vulnerabilities due to the use of Open source s/w

- Not specific to Open RAN.
- Tools/mechanisms already available to handle this problem.

Security in Open vRAN

Rooted in the principle of "never trust, always verify," security in an Open vRAN network is based on the following three tenets:

Secure communication between Cloud native Network Functions (CNFs) through a mutually authenticated, protected communication channel between them.	**Adoption of Web-scale IT industry's best security practices** for CNFs at all stages of container lifecycle.	**Securing the hosted platform with hardening measures** based on cloud computing industry's best practices.

ALTIOSTAR

A. Securing communication between Cloud Native Network Functions (CNFs)

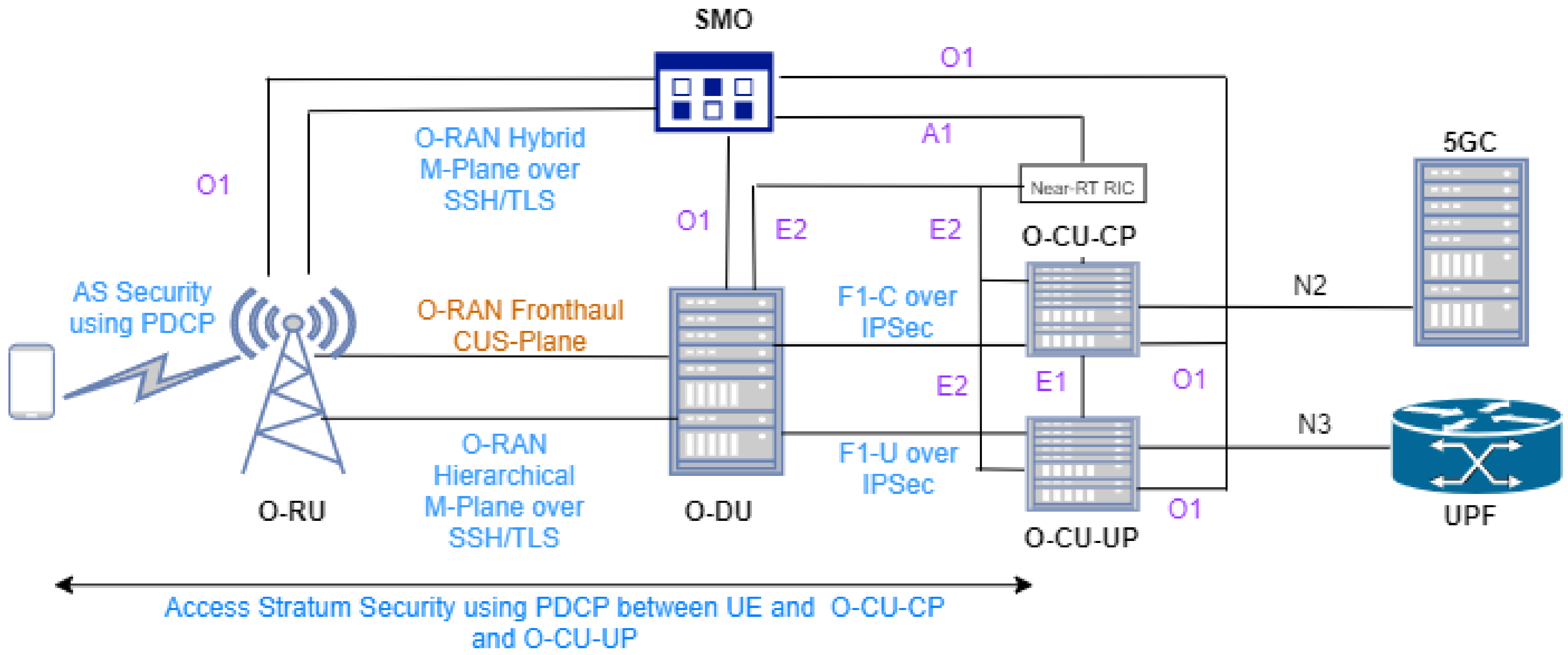
Secure communication between CNFs

Secure communication between CNFs is achieved as follows:

- Mutual authentication between Network Functions based on X.509 certificates
- Authorization using Role-Based Access Control on all access interfaces
- Securing communication path on all Open vRAN interfaces based on industry-standard security protocols such as TLS and 3GPP NDS/IP (IPSec)

ALTIOSTAR

Open vRAN Security Architecture



ALTIOSTAR

Open vRAN Interfaces and standardization

Interface	Between nodes	Security mechanism	Specified by
E1	O-CU-CP and O-CU-UP	NDS/IP (IPSec) or DTLS	3GPP
Xn	Source gNB and Target gNB	NDS/IP (IPSec) or DTLS	3GPP
Backhaul	O-CU-CP and 5GC (N2) O-CU-UP and 5GC (N3)	NDS/IP (IPSec) or DTLS	3GPP
Midhaul (F1)	O-CU-CP and O-DU (F1-C) O-CU-UP and O-DU (F1-U)	NDS/IP (IPSec) or DTLS	3GPP
Open Fronthaul (M-Plane)	O-RU and O-DU/SMO	TLS, SSHv2	O-RAN WG4
Open Fronthaul (CUS-Plane)	O-DU and O-RU	Work in progress (2Q21)	O-RAN SFG
O1	SMO and O-RAN Managed elements	Work in progress (2Q21)	O-RAN SFG
E2	Near-RT RIC (xAPPs) and O-CU-CP	NDS/IP (IPSec) or DTLS	O-RAN SFG
A1	Near-RT RIC and Non-RT RIC	Work planned (2Q21)	O-RAN SFG
O2	SMO and O-Cloud	Work planned (2Q21)	O-RAN SFG
r/xAPPs	Non/Near-RT RIC	Work planned (3Q21)	O-RAN SFG

O-RAN Alliance - Security Focus Group (SFG)

- SFG is responsible for security and privacy in O-RAN systems
- SFG is currently working on several high-priority activities:
  - Security for Open Fronthaul (C/U/S/M-plane)
  - Security for O1 interface
  - Threat modeling and Remediation analysis
  - Security testing framework specifications
- Planned activities
  - Security for xAPPs, E2 interface, O-Cloud

ORAN Alliance – Security for Open Fronthaul

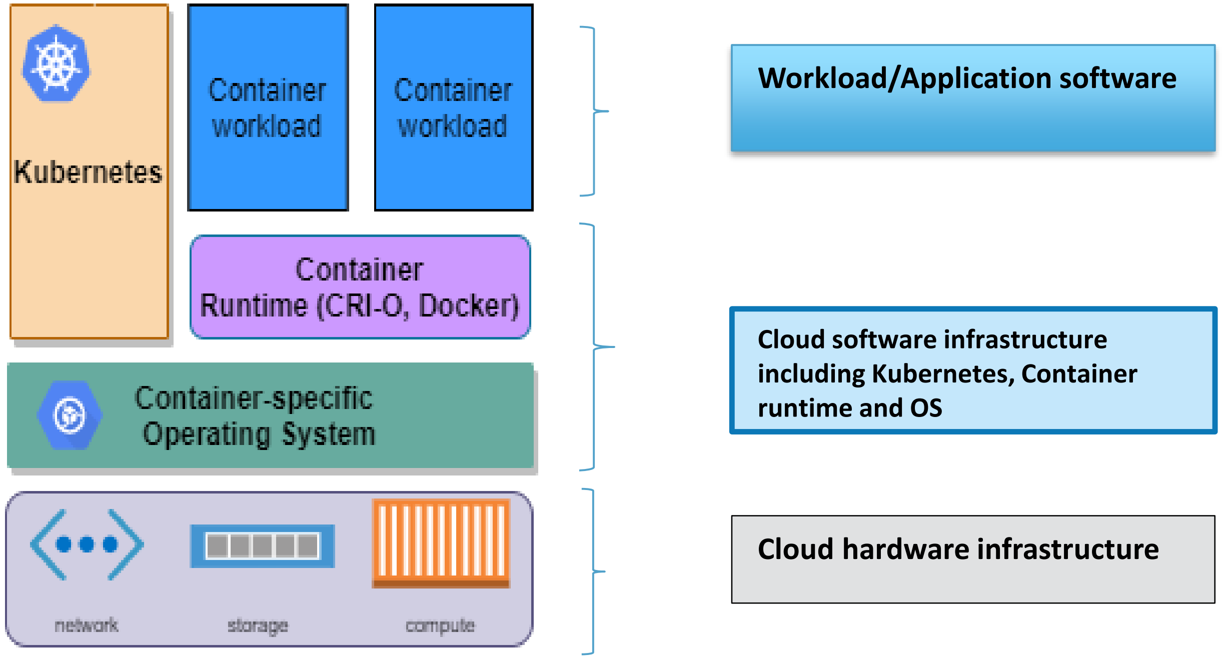
- SFG created a new Work Item – **FHCUSSec**, to study C/U/S-Plane Security between O-DU and O-RU
- Altiostar is the rapporteur for this WI
- Current focus areas:
  - Exploring IEEE 1588-2019 native security mechanism (Security TLV) for authentication and integrity protection of PTP messages on S-plane
  - Using Layer 2 MACSec for encryption of S-plane and C-plane
  - Using 802.1x Port based Network Access Control for device authentication on Open Fronthaul

First set of Stage 2 requirements and recommendations expected in July 2021

B. **Adoption of Web-scale IT industry's best security practices for CNF security**

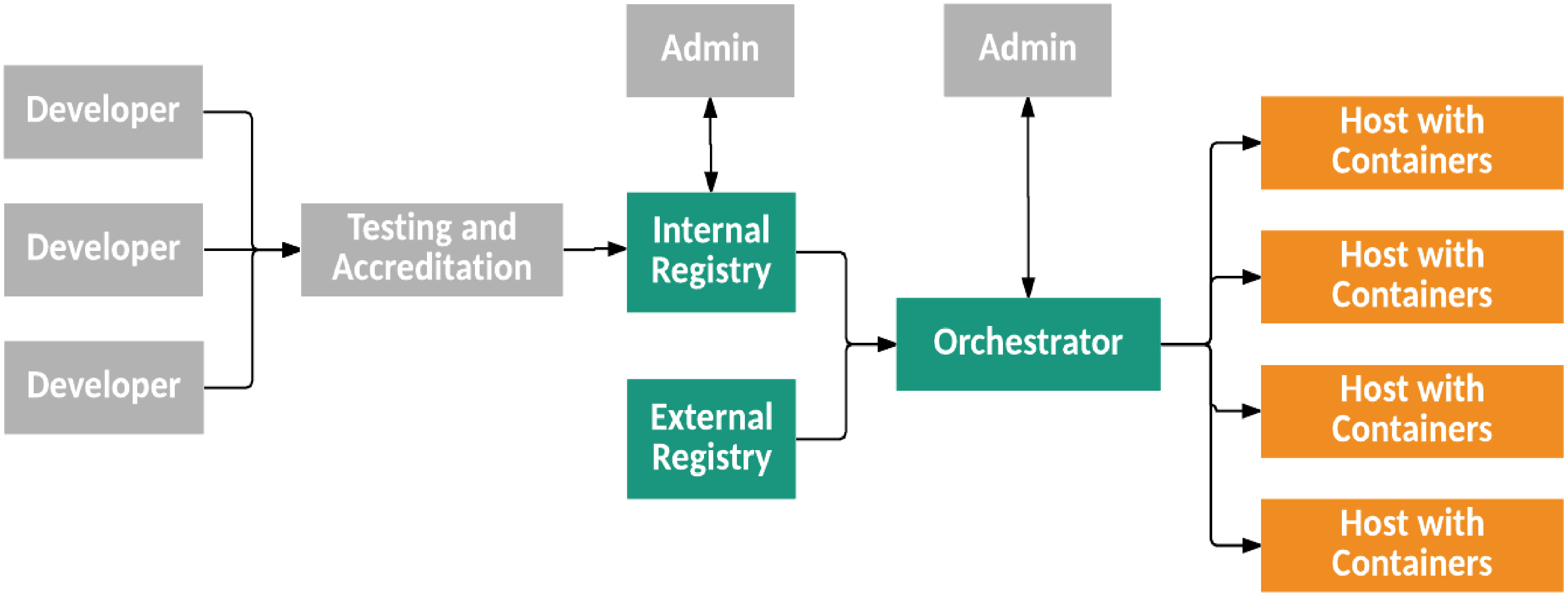
ALTIOSTAR

Cloud native platform



Cloud native platform for containerized applications

Securing containers across its lifecycle



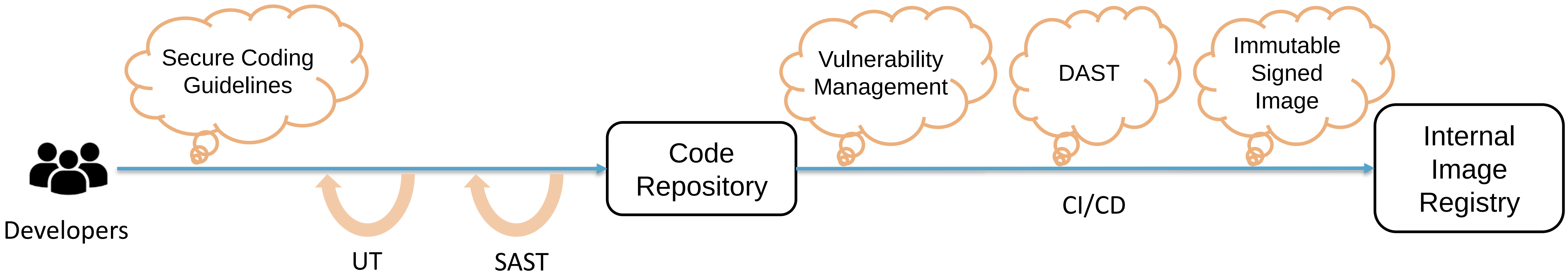
Build
Image creation and testing

Distribute
Image storage and retrieval

Deploy
Container deployment and management

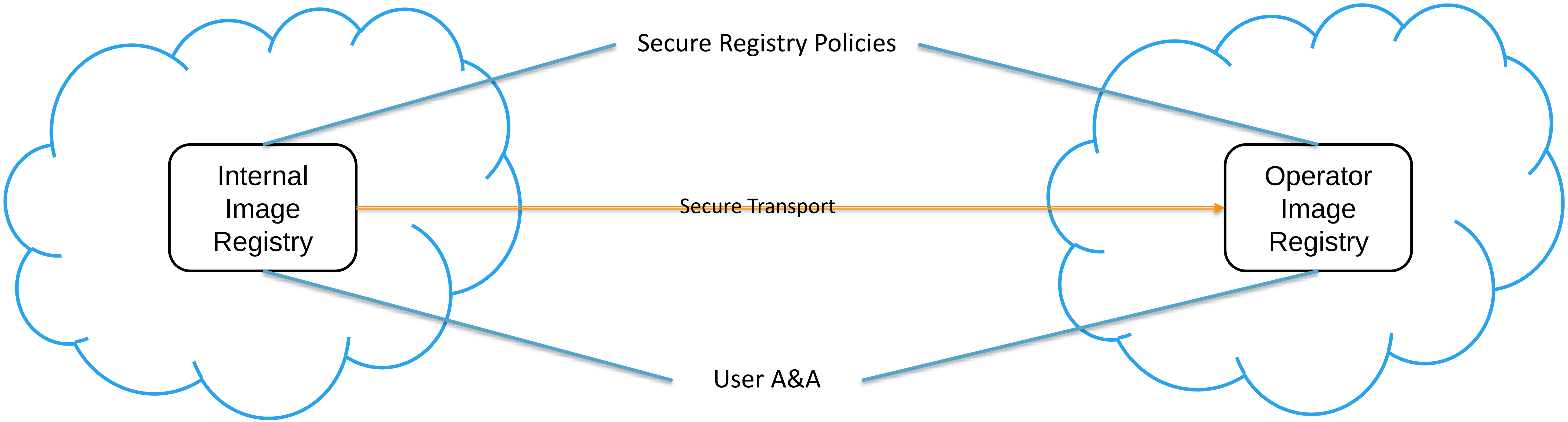
Container Lifecycle. Ref NIST 800-190 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf

Build phase - Use of DevSecOps



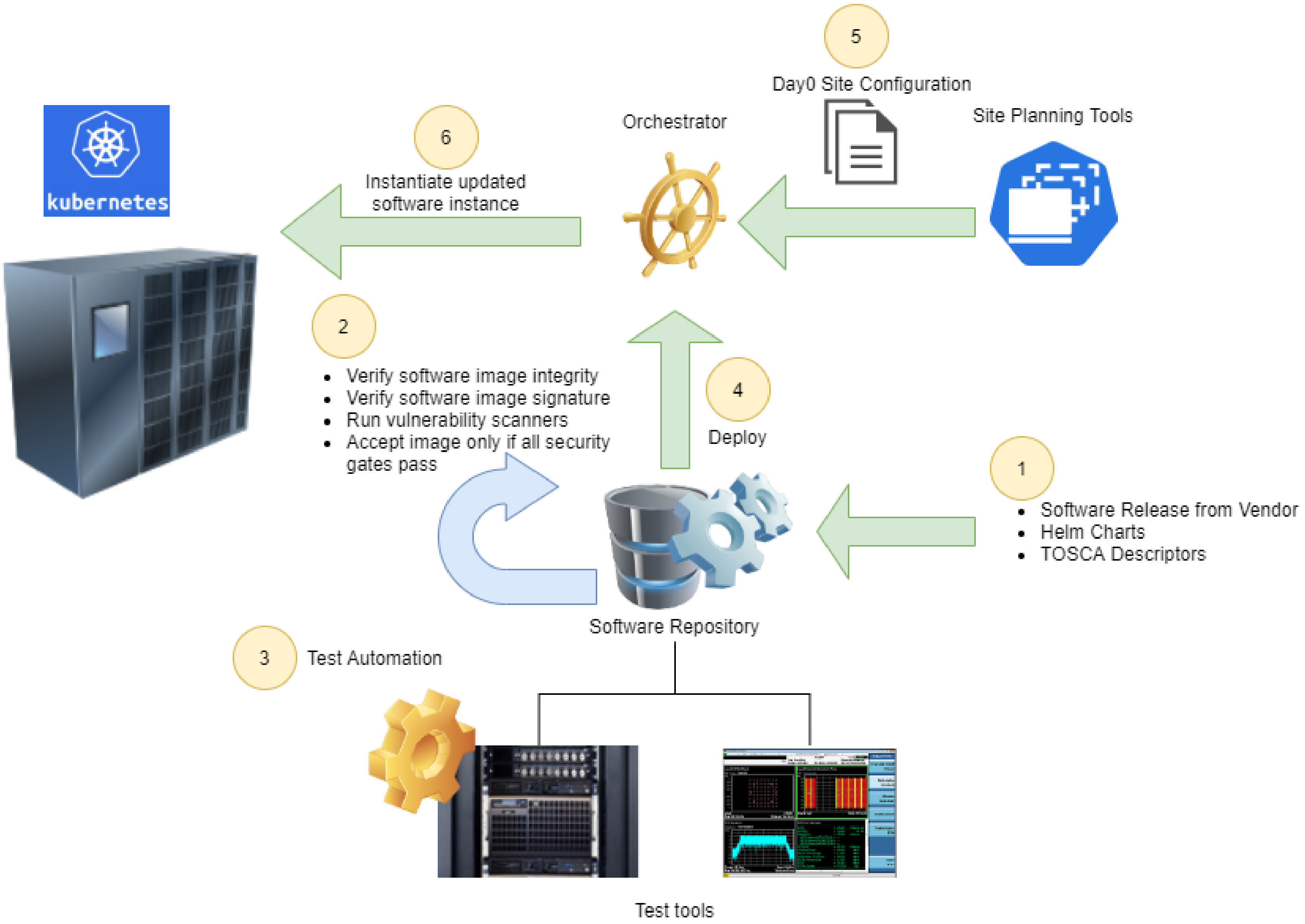
- DevSecOps are the set of development processes followed during the product development stage with security integrated into each stage
  - i. **Secure Coding** practices and verification based on Static Application Security Testing (SAST) tools
  - ii. **Vulnerability Analysis and Remediation** of container images using Image scanning tools
  - iii. **Dynamic Application Security Testing** (DAST) based black box testing for identifying vulnerabilities that may be exploited from outside by an external attacker
  - iv. Creation of **immutable signed container images** or packages using vendor certificates
  - v. Maintain **Software Bill of Materials (SBOM)** of all open source and third party components. Software Component Analysis (SCA) tools may be used for this purpose

Distribute phase – Security in the Image Registry



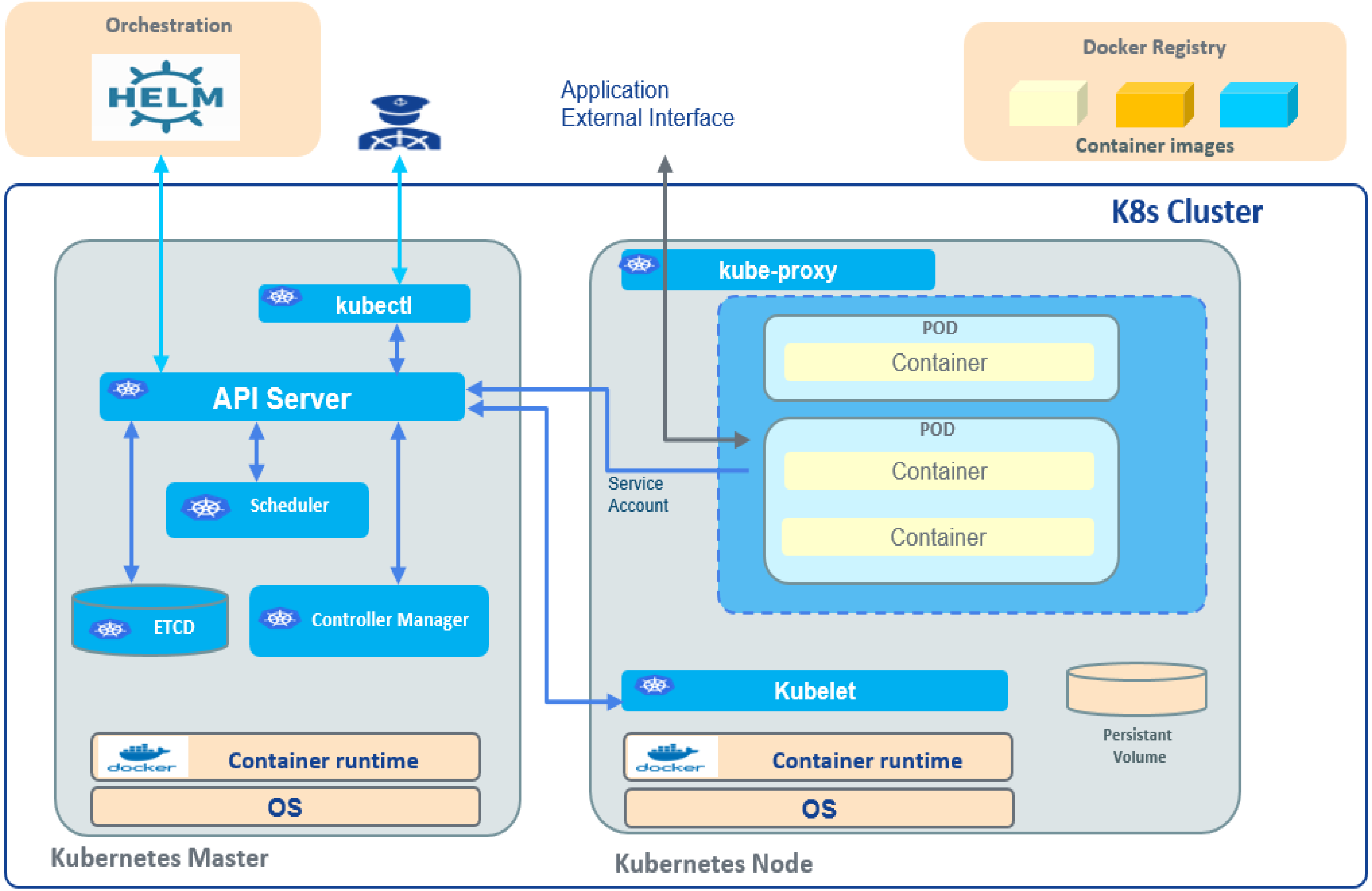
- Security for Image Registry is based on the following -
  - Secure transfer of images to the operator image registry
  - Registry policies for image selection – based on age, vulnerabilities present
  - Proper Authentication and Authorization of users of the Registry
  - Container **image signature verification** by NFVO (as per ETSI SOL 4)

Deploy phase - Secure CI / CD pipeline (Operator)



ALTIOSTAR

Deploy phase – Run time security measures



Host Security

Kubernetes/Cloud Security

Application Security

Run-time Security

Deploy phase - Run time security measures

Host OS Security

- Host OS hardening and adhering to CIS benchmarks using Linux kernel's security features such as SELinux, AppArmor, Seccomp

Protecting workload using native K8s security mechanisms

- Using **K8s Namespaces** to provide workload isolation (micro-segmentation)
- Enforcing Principle of Least Privileges (PLoP) using **K8s Pod Security Policy (PSP)** and **Security context**
- Regulating network communication between pods, and between pods and other n/w endpoints using **K8s Network policies**
- Limiting resource usage using **Resource Quota** and **Limit Ranges**
- Support integration with external vaults such as Hashicorp to **protect data at rest** (certificates, keys etc.)

Run time security measures

- Using **Kubernetes operators** to manage components and services in an automated way. One such service is to deploying operators to fight configuration drift and enforce a secure configuration by eliminating human errors - Configuration Security Posture Management (CSPM) tools
- Network monitoring using Intrusion Detection and Prevention systems

C. Securing the hosted platform with hardening measures

ALTIOSTAR

Security hardening

- An unprotected Network Element can be used by a malicious attacker to gain access to it and a) perform harm to the attacked NE, and b) target other NEs to which the attacked NE is connected to.
- **Security hardening** is a collection of tools, techniques and best practices to reduce potential attack surfaces in applications, cloud infrastructure including orchestrator, host OS and underlying hardware.

Security hardening

A non-exhaustive list of security hardening practices that may be used to secure the Open vRAN include:

- Integrating security best practices into the software development process
- Ensuring adequate security measures are taken in the registry where images are stored
- Taking appropriate countermeasures in the Orchestrator to eliminate potential risks (as per NIST 800-190 guidance)
- Configuring required security controls (configuration) across all layers of the platform (Containers, Orchestration, Host OS) in every Network element of the O-RAN network
- Using automated tools to continuously assess security configurations and ensure compliance to industry-best runtime security recommendations from organizations such as Center for Internet Security (CIS)
- Implement hardware root of trust to ensure that OS images, container run time and container images, are properly verified that it is from a trusted source and a chain of trust is built rooted in hardware (e.g. TPM)

Integrating security during s/w development

a. Enforce secure-by-design by adopting DevSecOps principles into s/w development
b. Ensure sanity of the image that is getting built by using industry standard or 3GPP/NIST specified security measures such as:

i. **Resolving open source and 3rd party s/w vulnerabilities at all layers of the image by updating and keeping all patches up-to-date**
ii. Adopting tools and practices to validate image configurations (in manifests) and enforce compliance with secure configuration best practices (for e.g. CIS configuration recommendations)
iii. **Ensuring that images are scanned for vulnerabilities**
iv. Incorporate software signing (during build) and verification (in registry) to detect image tampering
v. **Ensure that there are no clear-text secrets in the image (like password/ private keys etc.)**
vi. Ensuring that images use PLoP (principle of least privilege)
vii. Implementing 3GPP specified security requirements for gNB
viii. Where possible, using FIPS 140-2 compliant cryptographic algorithms

Secure configuration of CU/DU

- Secure configuration of CU/DU becomes a shared responsibility between all the suppliers and the operator.

- Security controls of CU/DU include:
  a. Security related configuration in the container images which are built into the containers in manifest files
  b. Security related configuration at deployment phase which includes configuration of workloads, and underlying infrastructure (K8s cluster, container runtime and Host OS)

- Automated tools are used to perform compliance checks against Center for Internet Security (CIS) benchmark configurations at various stages of the container image lifecycle:
  i. Supplier performs automated scanning of the images in CI/CD to detect insecure configuration of images
  ii. Operator performs automated scanning of all the images (from all suppliers) for compliance
  iii. Configuration Posture Management - Once deployed, container workloads and infrastructure are checked automatically to detect and remediate configuration drifts that happen in CU/DU over a period of time

ALTIOSTAR

Summary

ALTIOSTAR

Key security differentiators in O-RAN

Differentiator	O-RAN	Traditional RAN
Operator has full control in building a secure platform	Open RAN's disaggregated architecture allows network operators to build virtualized platforms by **selecting suppliers** that meets all the required industry security standards and certifications.	Operator has no control of how the virtualized platform is assembled. It is fully vendor driven.
Better enforcement of security controls in cloud infrastructure	Cloud infrastructure supplier will be directly under an **agreement** with the operator, and will be responsible for security of the cloud infrastructure.	Operator has no direct visibility of the cloud infrastructure provider
Disaggregated platform allows for better visibility and automated monitoring of the network	Cloud native architecture allows operators to deploy the **latest security tools** for monitoring vulnerabilities and automated remediation measures as required	Operator has no visibility to this information. The operator is fully dependent on the vendor to detect and remediate vulnerabilities in the network
Adoption of industry best practices in development of containerized applications	Allows **adoption of industry best practices** such as "secure by design", DevSecOps, automated testing in development of containerized applications. Operator also has an option to work with the supplier to determine and influence CI/CD processes used by the supplier.	It is fully vendor driven, and operator has no mechanism to verify software development process used by the vendor.
Security of Open Fronthaul	**Provides visibility** to the security measure taken to protect this interface. Open, standardized interfaces remove vulnerabilities or risk that comes with proprietary and potentially untrusted implementation.	Protection measure taken to protect CPRI interface in a closed RAN is not known

Joint white paper on Security in Open RAN (Altiostar, Fujitsu, Mavenir, Red Hat): **https://www.altiostar.com/security-for-open-ran/**

Summary

O-RAN security framework is based on the **shared security responsibility model -** security responsibilities are split between the suppliers and the operator

Adoption of cloud native principles is not new in a mobile n/w. 5G Core (5GC) is already based on that.

Operators need to invest in security tools and automation in building their secure CI/CD pipeline before onboarding CNFs in their production environment

Run time security measures to monitor/policy traffic within the K8s cluster is critical. Using container firewalls (next gen FWs) to prevent lateral movement between K8s pods in different security zones.

Misconfiguration caused by configuration drift is a leading cause for data preaches in the cloud. Early detection and remediation through automation is essential to prevent configuration drifts in the network

System Integrator, specifically focused on security, is recommended when designing security for the O-RAN network

Thank You

ALTIOSTAR