
Ericsson Network Security
TDTS06
Imagine a world where limitless connectivity means
limitless possibility

Ericsson Network Security

TSTD06

https://www.ida.liu.se/~TDTS04/timetable/index.shtml

Pontus Sandberg, Manager Ericsson R&D Security
Joakim Aronius, Security Systems Manager
Magnus Öberg, Security Standardization Engineer

March 8th

Who we are

Pontus Sandberg

- R&D Manager in Security @ Development Unit Networks
- Started my career at Ericsson Research, followed by 4G development, Operations to 5G Resilience, Capacity and Security
- Global experience both from R&D and Customer interaction
- M.Sc from LiU

Mats Gustafsson

- Security and Privacy Advisor @ Development Unit Networks
- Worked with product security for 3G, 4G, and 5G base stations as well as with Ericsson's Network Management system
- Current focus is security assurance frameworks for products as well as operations and internal environments
- M.Sc. and Ph. Lic. from LiU

Who are we

Joakim Aronius

- Working with product security for 4G and 5G base stations
- Has worked with IPSec, IPv6, CMPv2 (certificate management) etc
- Has previously worked at Saab with information security and security in JAS 39 Gripen.
- M.Sc. from LiU, Computer Science and Engineering

Magnus Öberg

- Ericsson Standardization Delegate in O-RAN Security Focus Group
- Security Champion @ Development Unit Networks
- Worked with product security for 3G, 4G, and 5G base stations.
- Current focus is security assurance frameworks for products and security standardization
- M.Sc. and Ph. Lic. from LiU

Agenda March 8th

Ericsson 5G Security introduction

Baseband
auto integration

Standardization

5G brings new security challenges

Ever evolving security threats

Critical infrastructure concerns

Increasing regulatory requirements (e.g., GDPR)

DevSecOps accelerating cycles

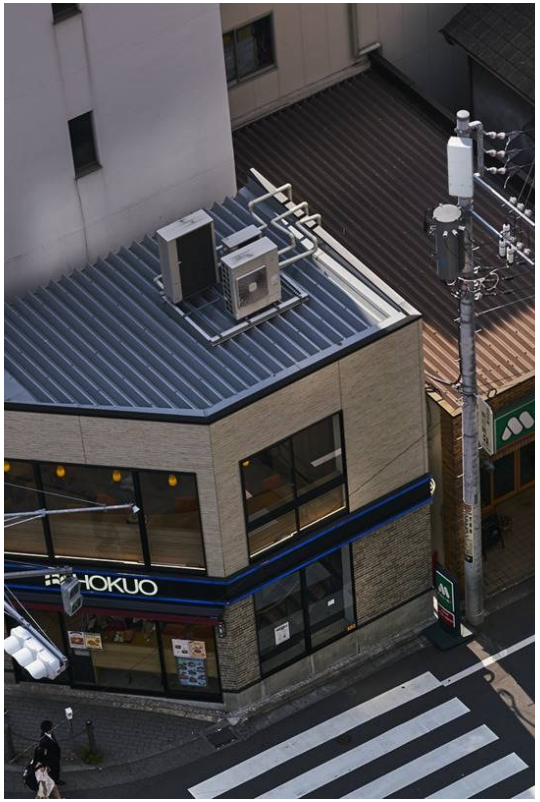
Billions of new devices

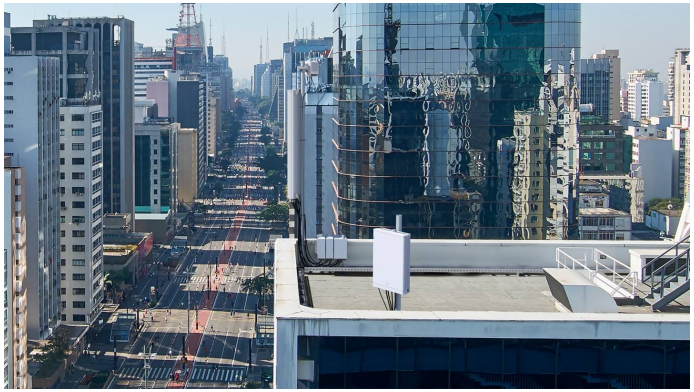
Distributed Cloud - specific challenges

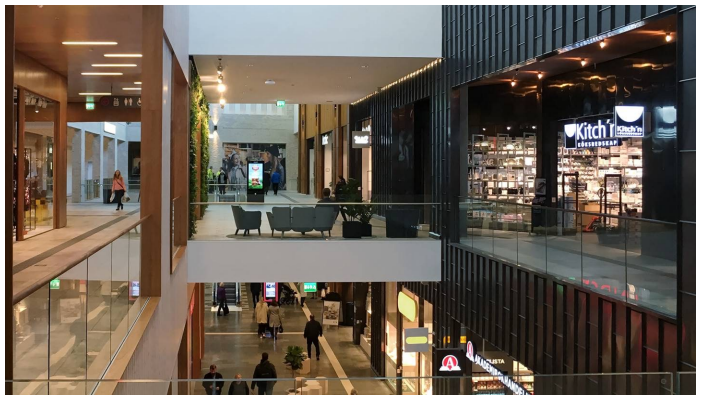
Baseband auto integration

Joakim Aronius

Network sites







Network rollout…

- Preparations
  - Radio Network planning
  - Node Provisioning

- Install new node
  - Physical installation
  - Integration into network

Important considerations

- No node pre-configuration
- Time on site
- Complexity/Required skills

Auto Integration Use Cases

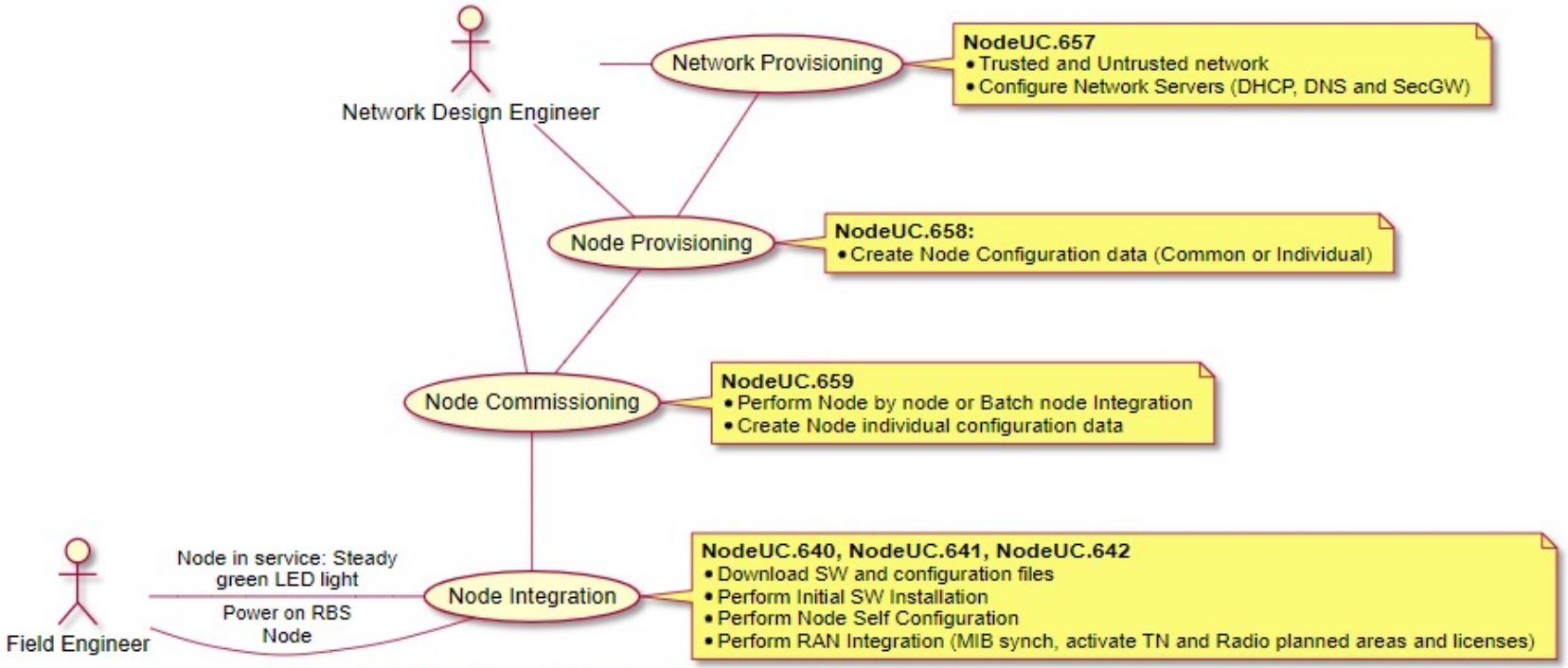
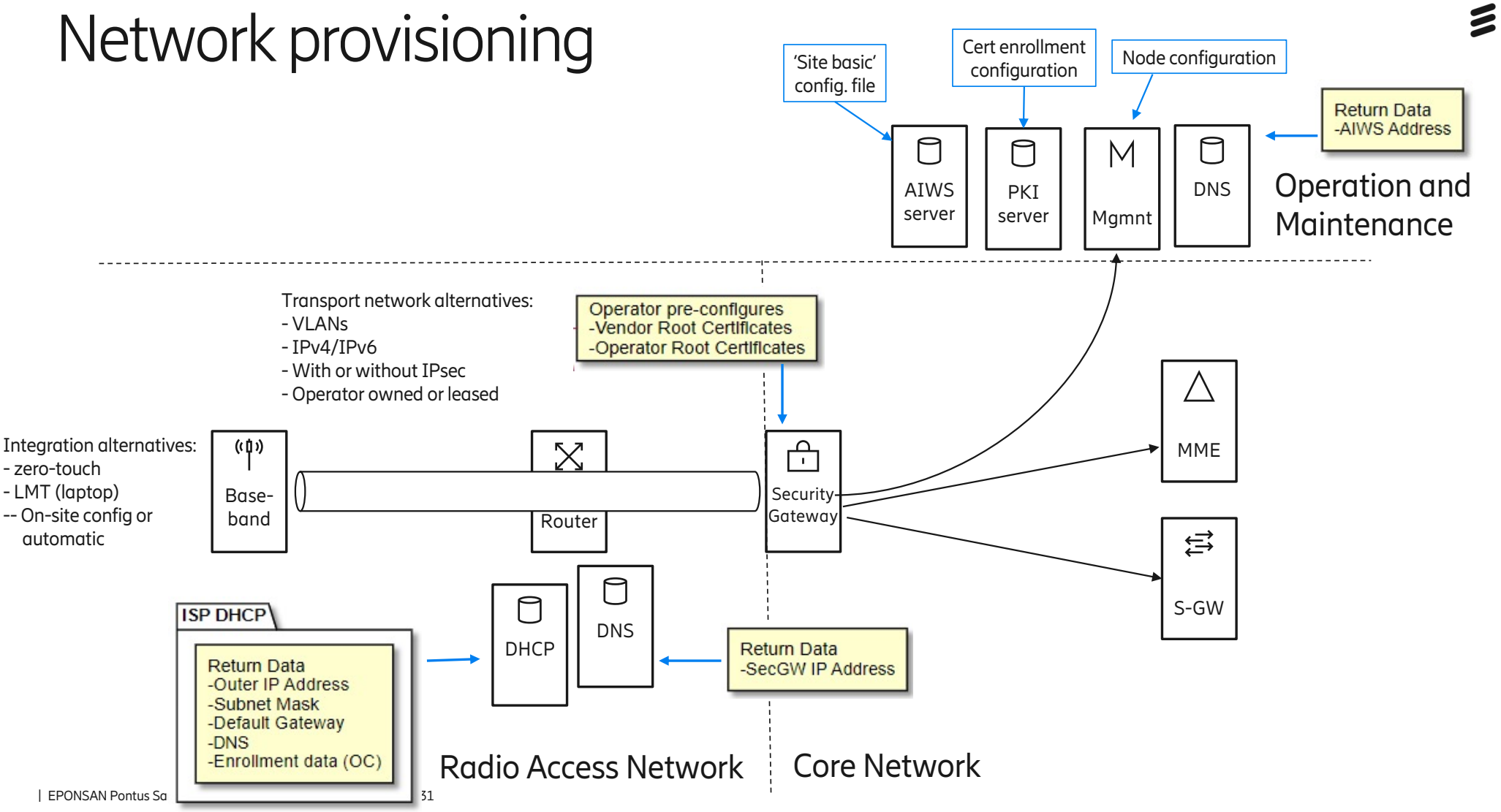
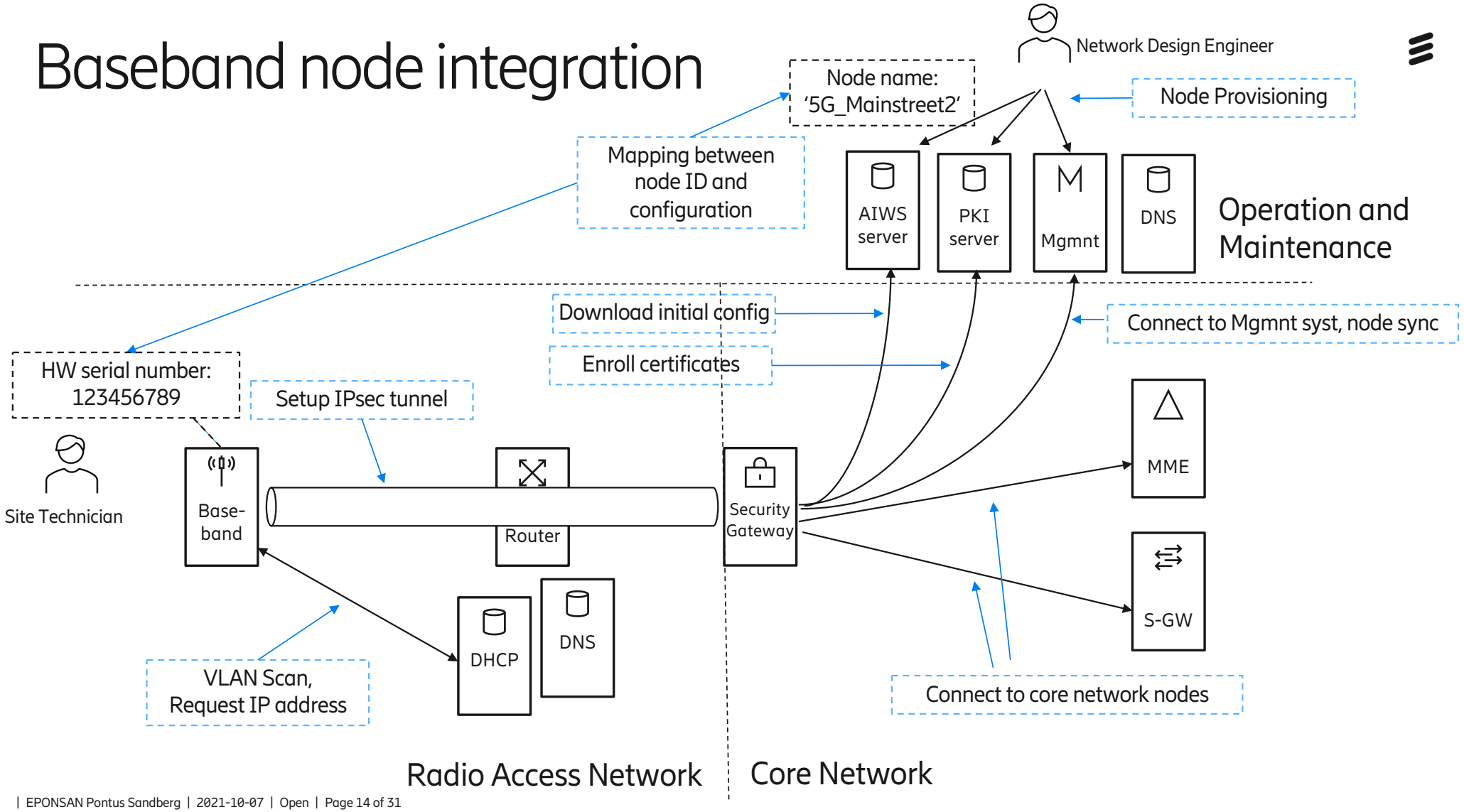


Figure 3.4.1: AutoIntegration - Use Case Diagram

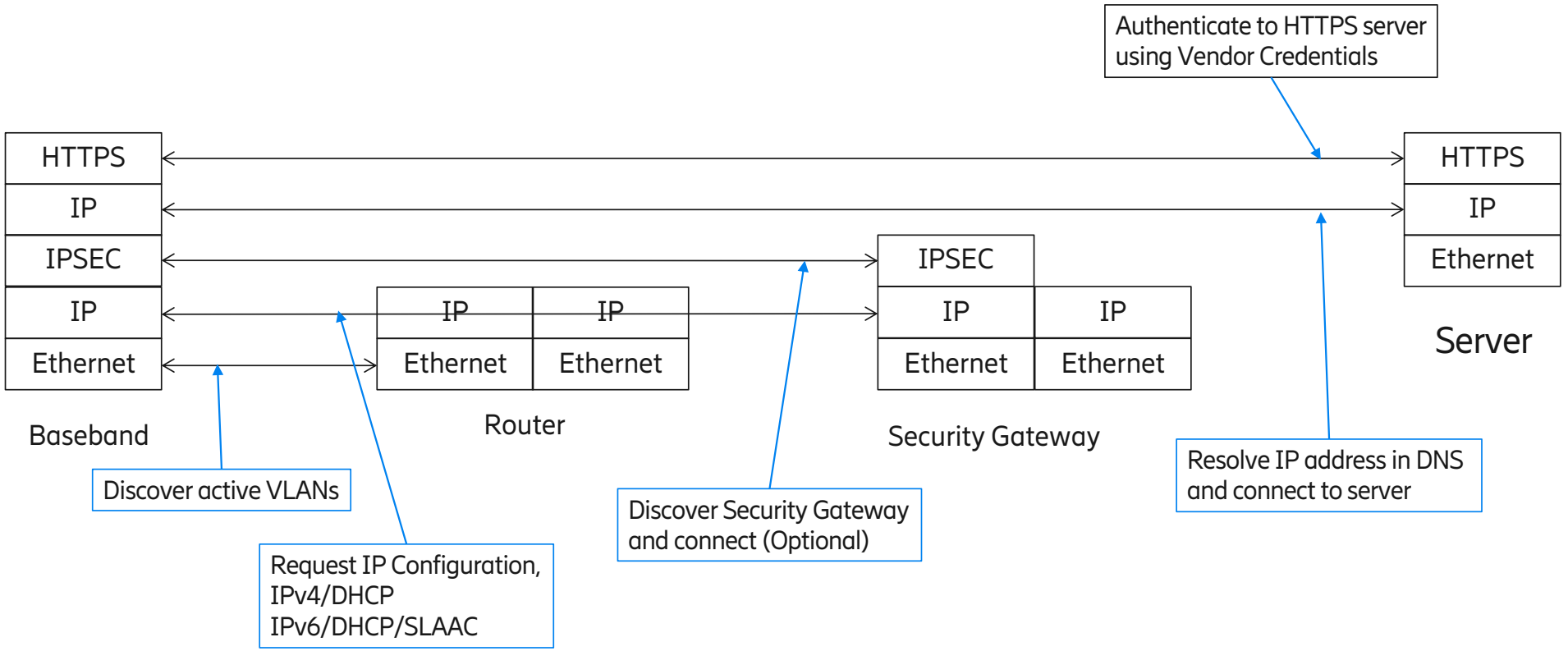
Network provisioning



Baseband node integration

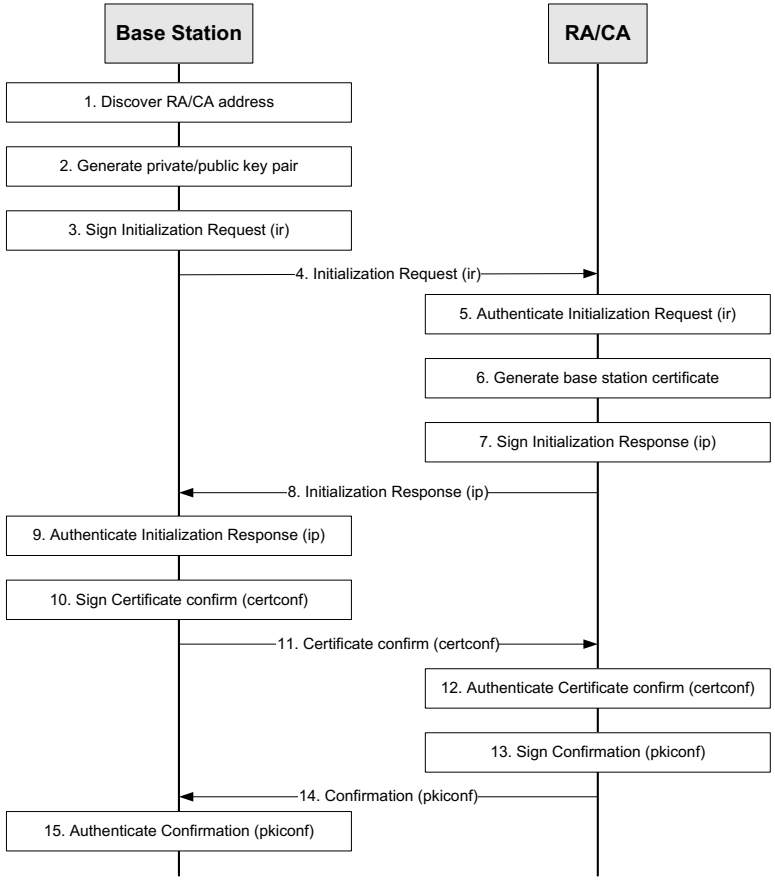


Download Configuration files, HTTPS over IPsec



Standardization

- Standardization needed as otherwise the vendors will create proprietary solutions...
- Transport protocols, IPv4, IPv6, IPsec etc standardized by IETF.
- 3GPP specifies profiles which parts of a standard that must be supported, e.g. IPsec/IKEv2, TLS, CMPv2 etc.



CMPv2 certificate enrollment sequence

Standardization

Magnus Öberg

Why standards?

- Standards – ”widely agreed ways of doing things“.
  - Formal standards – developed by Standards Development Organizations (SDOs)
    - Consensus built – generally agreed after negotiation among all involved stakeholders.
    - Fair development process – regulated so all involved parties are able to express their views.
  - De-facto standards – “standard in actuality”, something widely adopted

- Standardization – the work on defining a standard, ie agree on how something should be done.
  - Consensus built – generally agreed after negotiation among all involved stakeholders.
  - Fair development process – regulated so all involved parties are able to express their views.

Standardization bodies

Security Standardization

- Functional – requirements on product functionality, eg
  - Data in transit shall be confidentiality protected
  - Data at rest shall be integrity protected
- Assurance – requirements on development processes, eg
  - Source code shall be version controlled
  - The product shall have a Software Bill of Materials

3GPP TSG SA WG3 (SA3) - Security

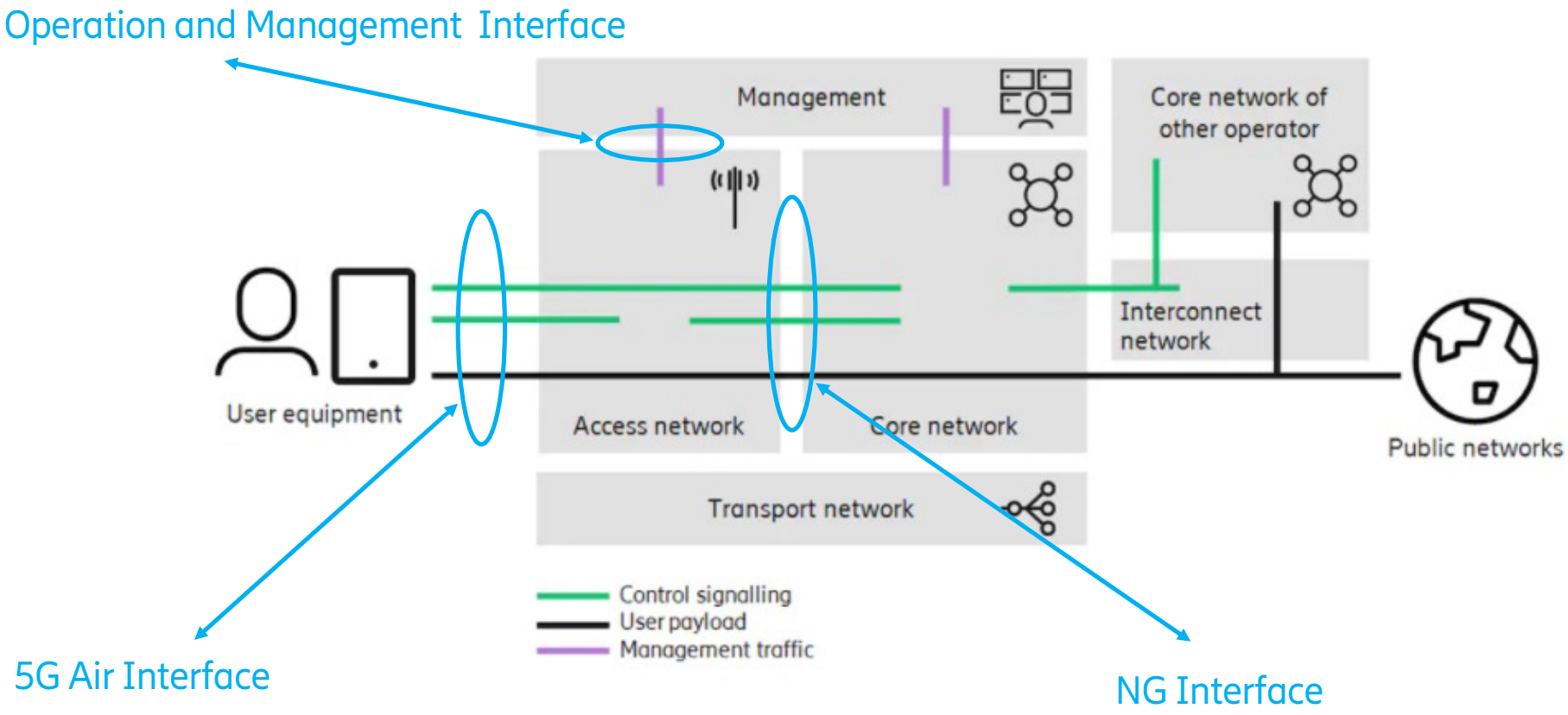
Main objectives

- Defining security requirements
- Specifying the architectures and protocols for security and privacy in 3GPP systems.

Some publications

- TS 33.117 - Catalogue of general security assurance requirements
- TS 33.210 - Network Domain Security (NDS); IP network layer security
- TS 33.216 - Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class
- TS 33.310 - Network Domain Security (NDS); Authentication Framework (AF)
- TS 33.401 - 3GPP System Architecture Evolution (SAE); Security architecture
- TS 33.501 - Security architecture and procedures for 5G system
- TS 33.511 - Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class

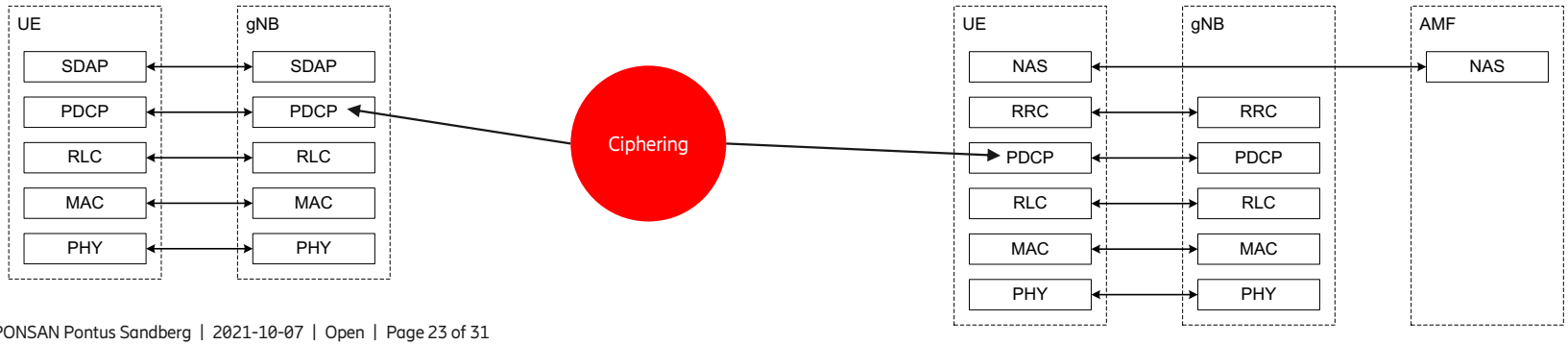
Telecom Networks



Protocol stacks – 5G Air interface

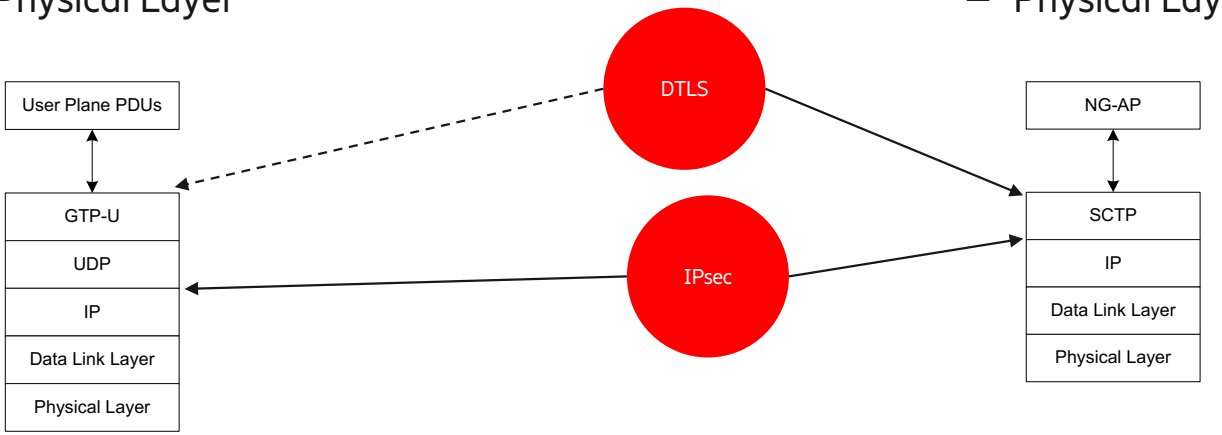
- User Plane
  - Service Data Adaptation Protocol (SDAP)
  - Packet Data Convergence Protocol (PDCP)
  - Radio Link Control (RLC)
  - Medium Access Control (MAC)
  - Physical Layer (PHY)

- Control Plane
  - Non-Access-Stratum (NAS)
  - Radio Resource Control (RRC)
  - Packet Data Convergence Protocol (PDCP)
  - Radio Link Control (RLC)
  - Medium Access Control (MAC)
  - Physical Layer (PHY)



Protocol stacks – NG interface

- User Plane
  - GPRS Tunneling Protocol for User Plane (GTP-U)
  - User Datagram Protocol (UDP)
  - Internet Protocol (IP)
  - Data Link Layer
  - Physical Layer
- Control Plane
  - NG Application Protocol (NG-AP)
  - Stream Control Transmission Protocol (SCTP)
  - Internet Protocol (IP)
  - Data Link Layer
  - Physical Layer



Security Protocols for Operation and Management

- TLS
- SSH

  Configuration and Troubleshooting
- SFTP
- FTPES

  File transfer
- HTTPS

  Emergency access
- LDAPS

  Authentication and Authorization
- CMPv2

  Certificate Management
- NTP

  Time of Day – required to check that certificates are valid!
- SNMP

  SNMP Traps - used to send alerts to the management system

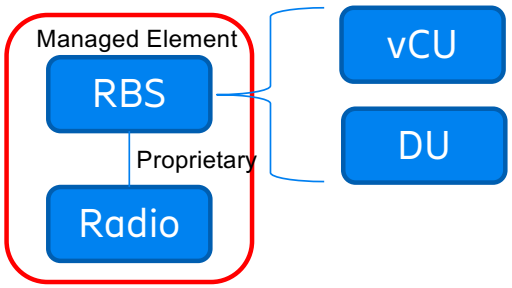
Application
TCP
IP
Data Link Layer
Physical Layer

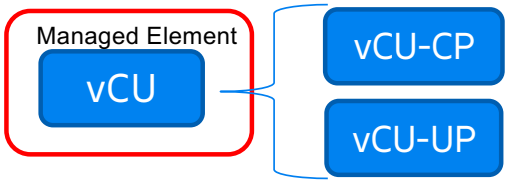
RAN Virtualization

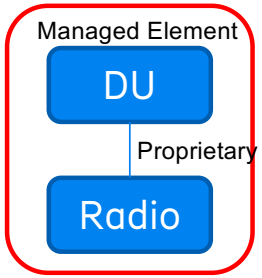
- **Open RAN** is the industry's generic term for an open radio access network architecture. An Open RAN has open interoperable interfaces, RAN virtualization, and support for big data and AI-enabled RAN. Providers deploying an Open RAN can choose between a 3GPP or O-RAN architecture.
- **vRAN** refers to the virtualization of RAN functions, particularly the higher layer and lower layer function of the baseband unit.
  3GPP Release 15 CU-DU split architecture facilitated this journey to begin by separating the centralized and distributed functions of RAN.
- **O-RAN** refers to the Open RAN standardized by the O-RAN Alliance. The O-RAN Alliance has four main objectives: Open Interfaces, Virtualization, Intelligence, and Interoperability.

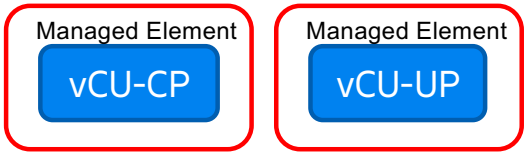
Source: https://www.ericsson.com/en/security/security-considerations-of-open-ran

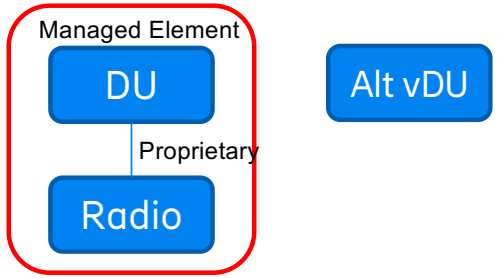
3GPP Legacy vs 3GPP Split architecture



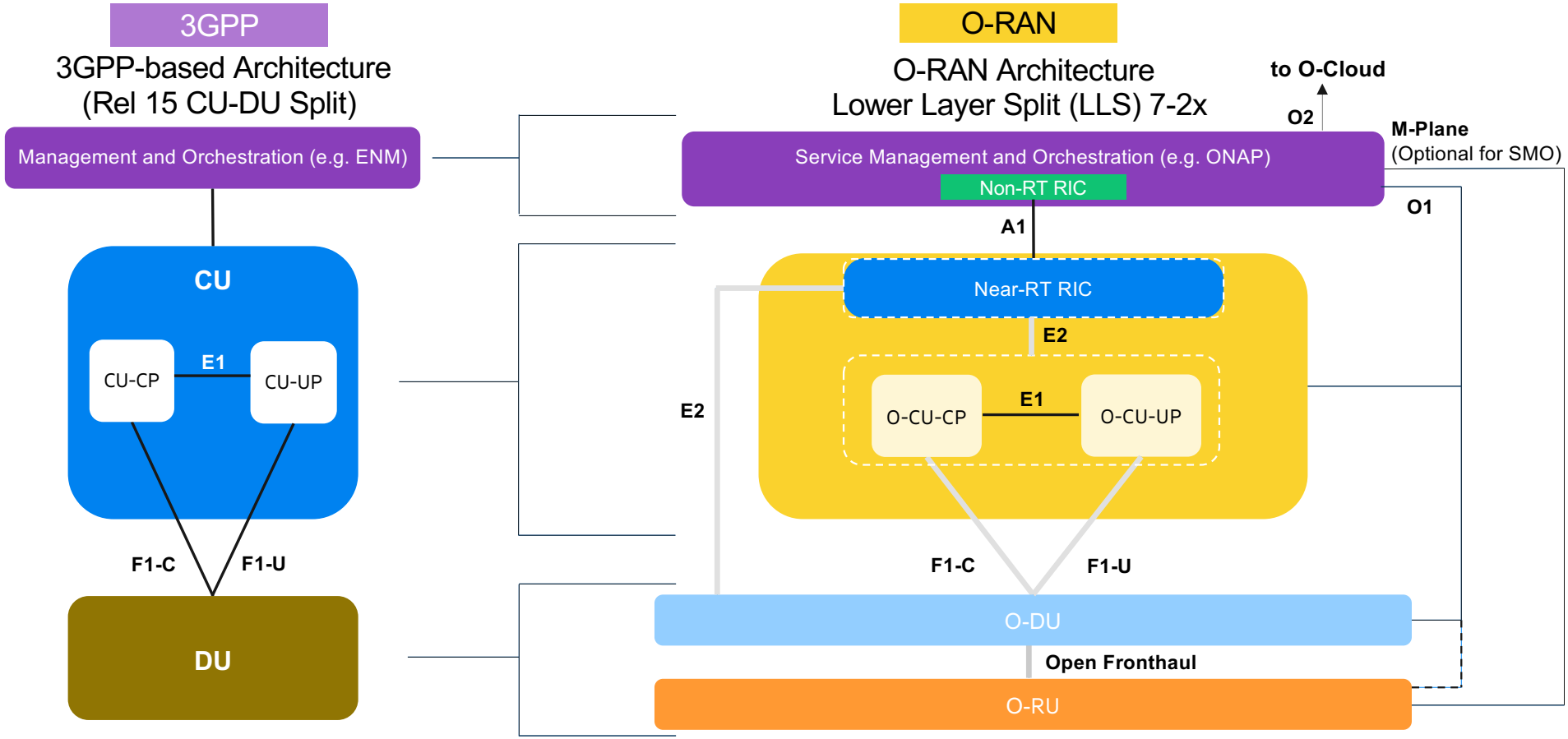








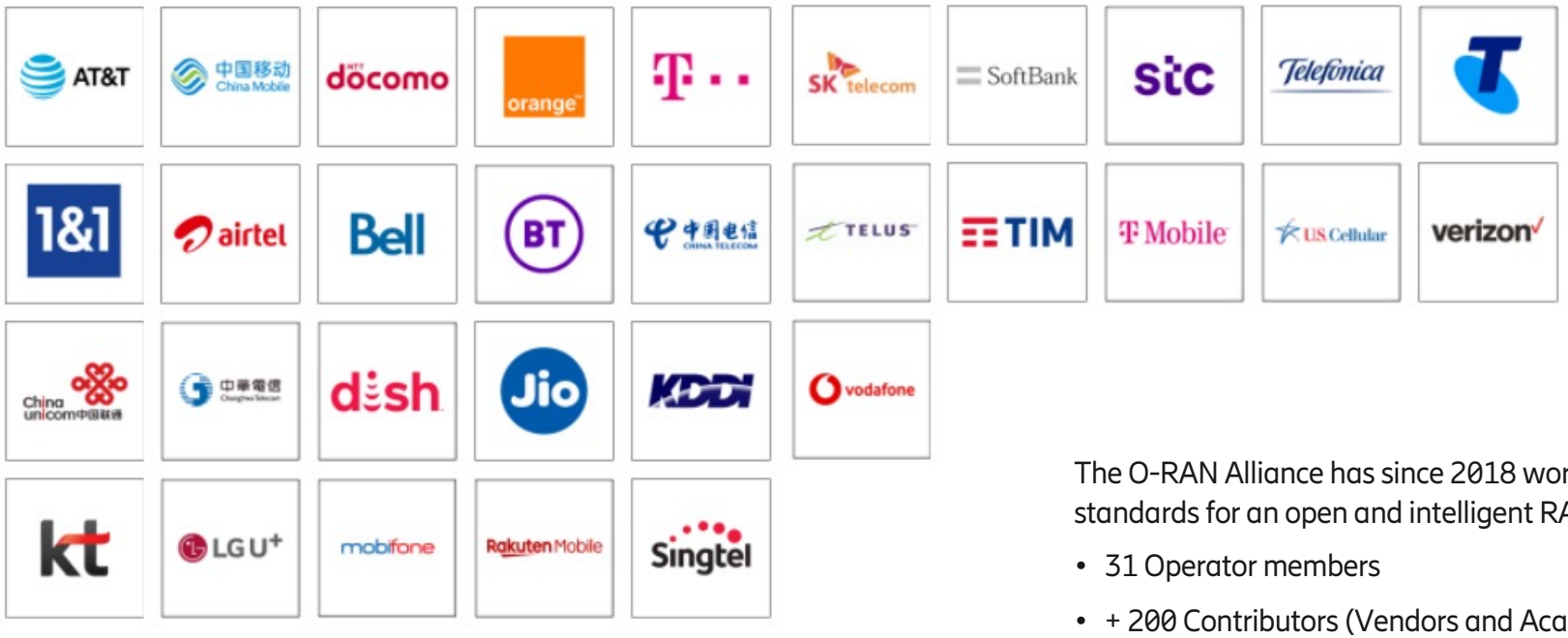
3GPP and O-RAN architectures



Source: Ericsson

O-RAN introduces additional interfaces, functional splits and disaggregation

O-RAN Alliance



The O-RAN Alliance has since 2018 worked to define standards for an open and intelligent RAN.

- 31 Operator members
- + 200 Contributors (Vendors and Academic)

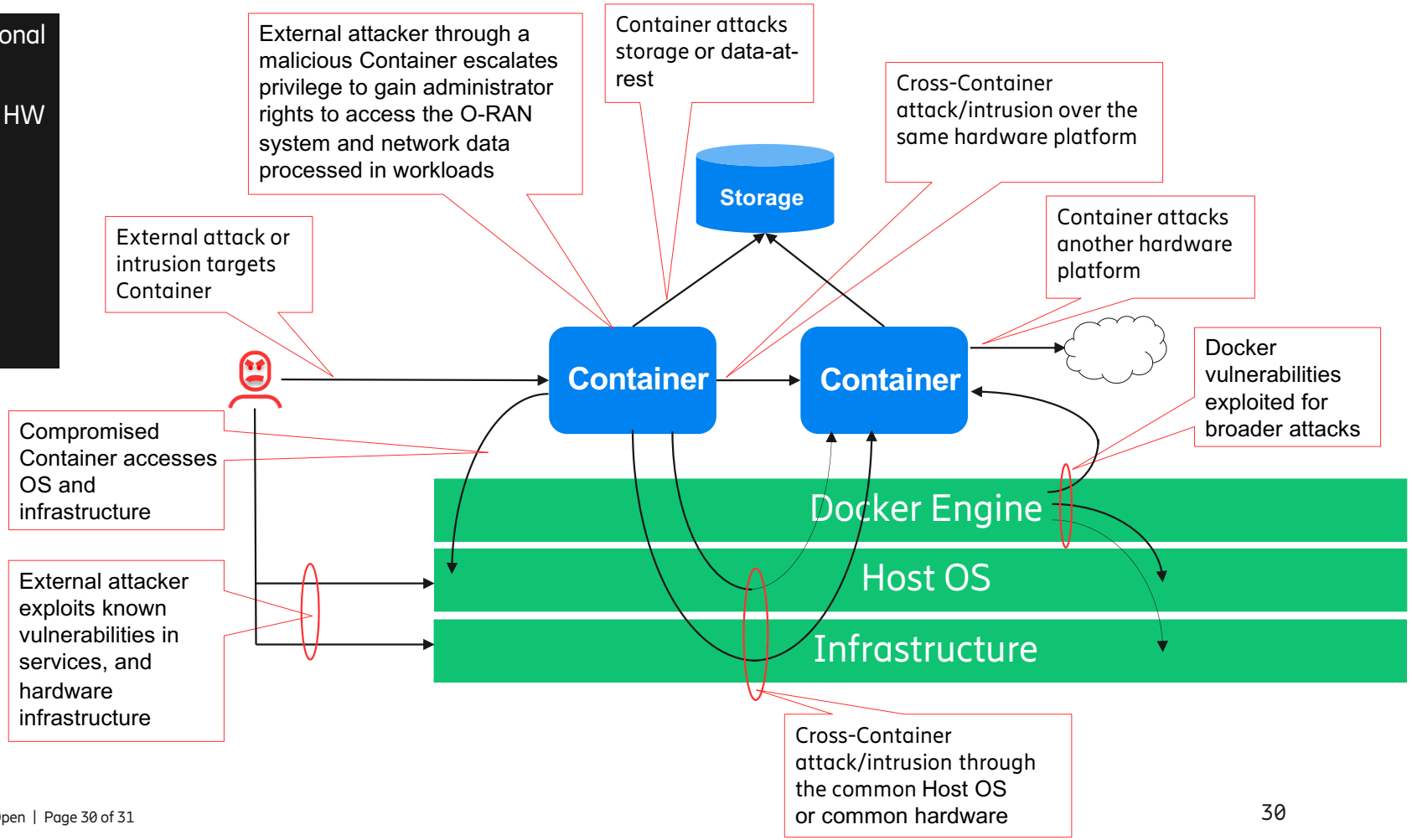
Ref: https://www.o-ran.org/

Cloud Attack Vectors

Ericsson view of cloud security

New trust relations require additional security considerations:

- SW decoupled from dedicated HW
- Another organization may share the same HW
- 3-party organization may be managing the infrastructure
- Open source components may have vulnerabilities



Key takeaways

5G networks are critical infrastructure – Security is a must!

Network rollout requires planning - with good preparations zero touch integration can be performed securely!

Standardization enables interoperability - many standardization organizations work with security!

Virtualization brings new security considerations - new attack vectors must be evaluated!


Thank you!
https://www.ericsson.com/future-technologies
https://www.ericsson.com/security
https://www.ericsson.com/careers