NOKIA Bell Labs

Securing 5G Mobile Networks Built on Distributed Telco Clouds

2017-06-15

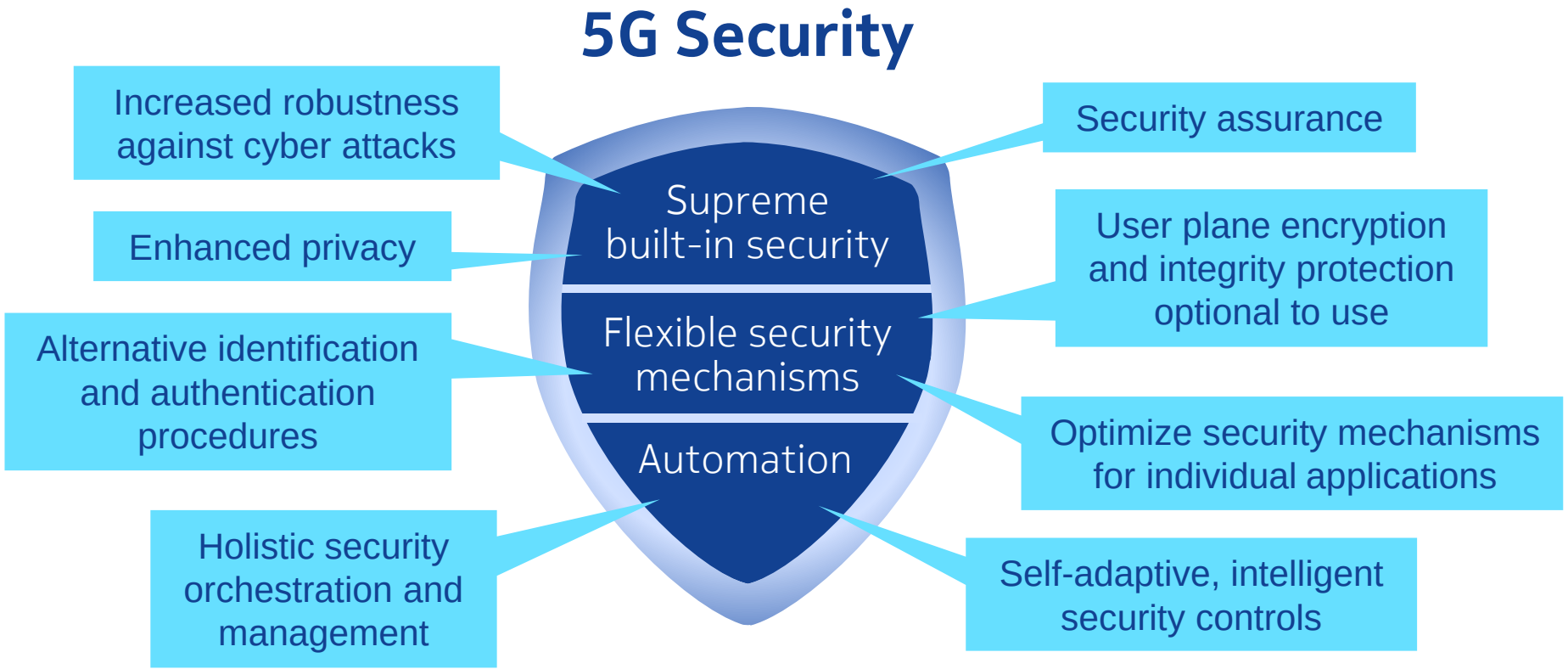
Peter Schneider, Nokia Bell Labs

Outline

- The goal: 5G security high level vision
- The Baseline: Mobile network security today
- Virtualized, programmable, sliced mobile networks
- Elements of a 5G security architecture
  - Secure SDN
  - Secure NFV
  - Secure Slicing
- Yes, we can!

This presentation uses results of work that has been carried out
in the H2020-ICT-2014-2 Project 5G NORMA (https://5gnorma.5g-ppp.eu/)

5G Security Vision

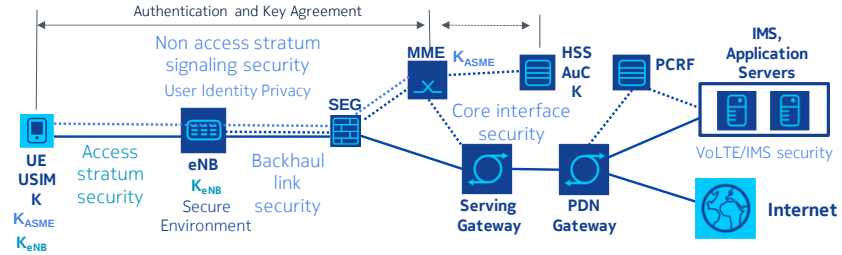


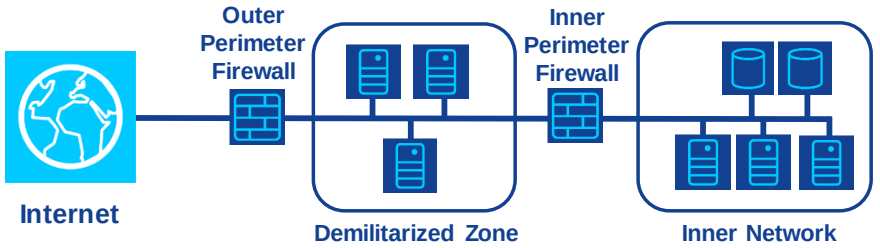
Layers of Mobile Network Security as of Today

3GPP-specified security architecture

Non-standardized network security measures

Network element security measures



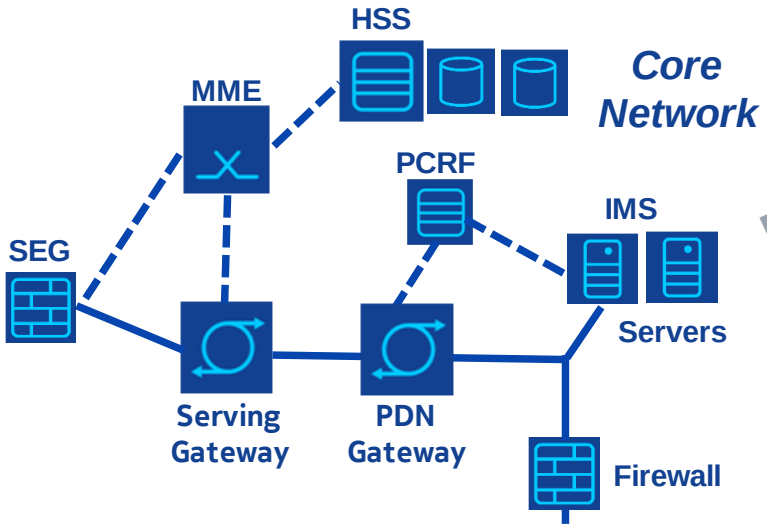


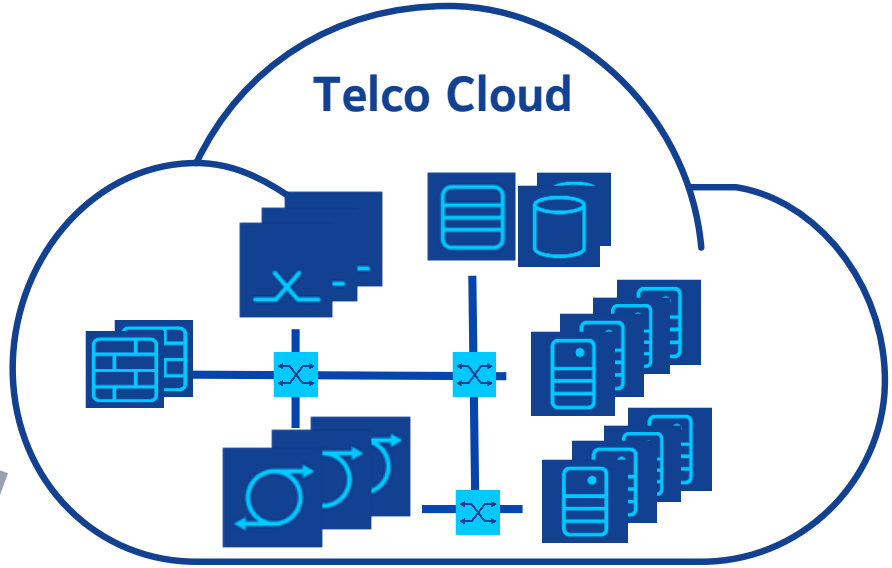
- threat and risk analysis per network element
- network element security architecture
- secure coding
- hardening
- security testing
- security audit
- security vulnerability monitoring
- patching process

NOKIA Bell Labs

A Mobile Core Network in the Telco Cloud

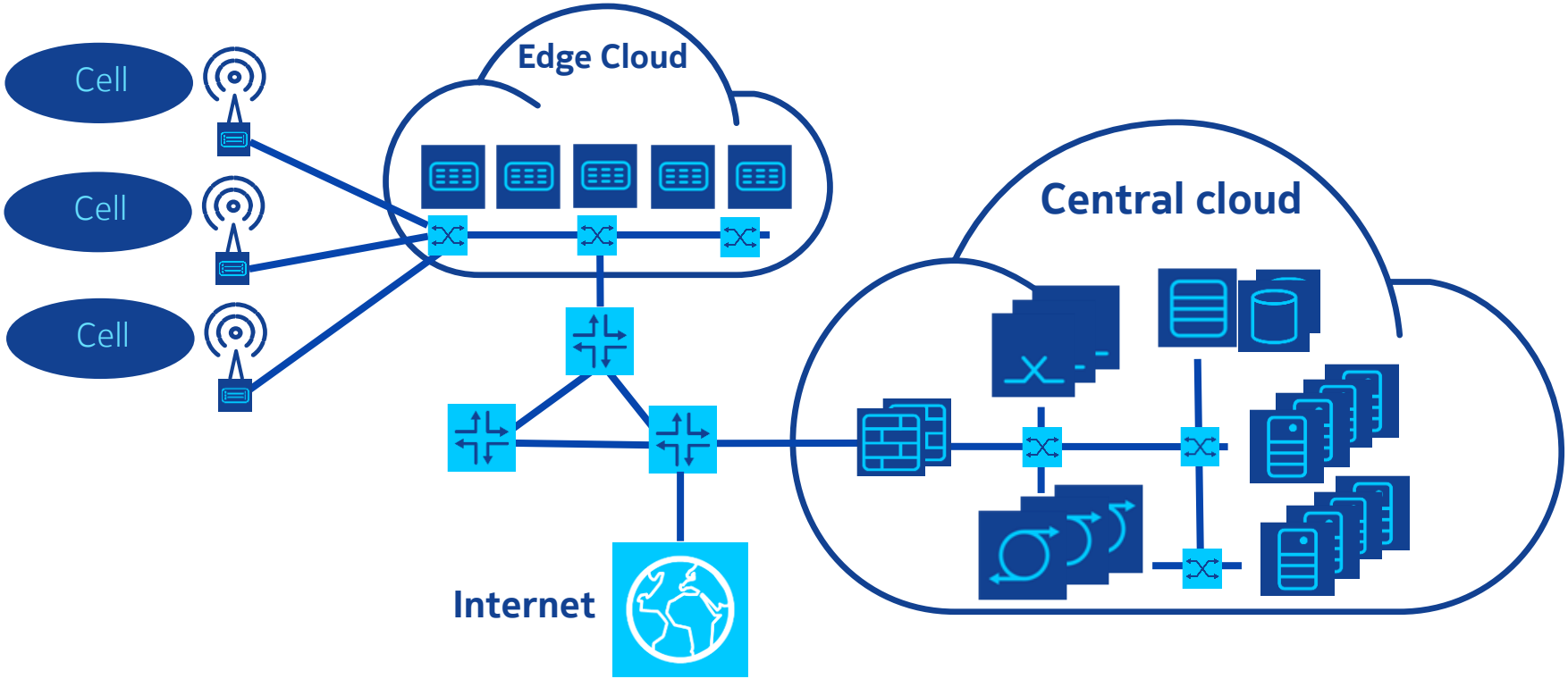
"Boxes interconnected by cables"





VNFs running on NFV infrastructure in a telco cloud

A 5G Mobile Network with Virtualized Core and RAN
Implemented on distributed telco clouds with SDN-based transport



NOKIA Bell Labs

Elements of a 5G Security Architecture

Authentication/authorization, key agreement

Security management and orchestration

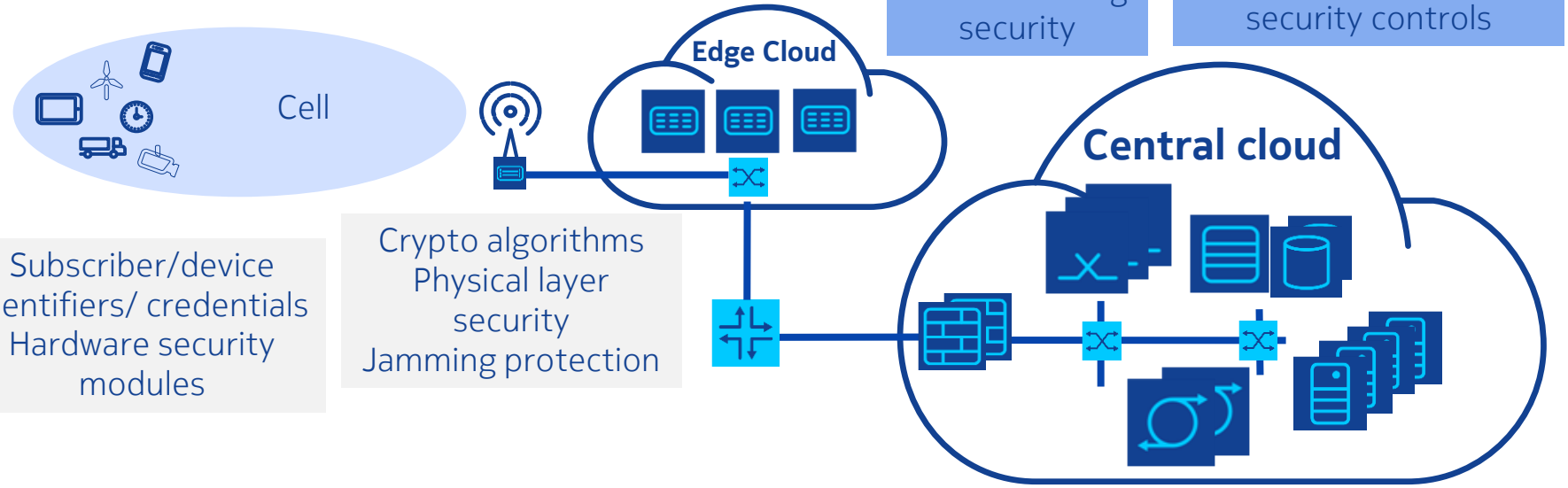
Security negotiation, key hierarchy
Enhanced control plane robustness
Enhanced subscriber privacy

NFV/SDN security

Security assurance for NFV environments

Network slicing security

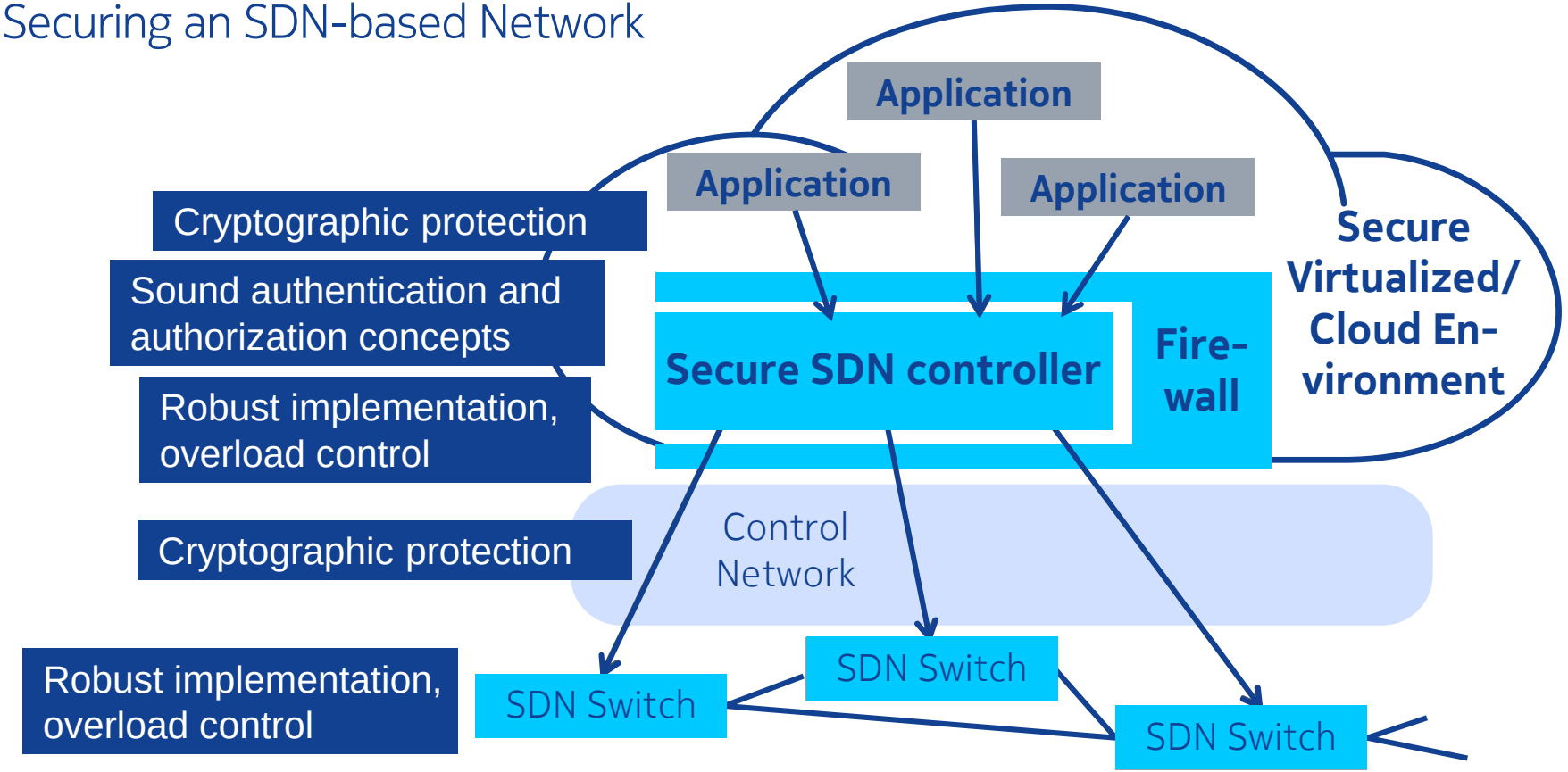
Self-adaptive, intelligent security controls



Subscriber/device identifiers/ credentials
Hardware security modules

Crypto algorithms
Physical layer security
Jamming protection

Securing an SDN-based Network



Securing a Network Implemented in an NFV Environment

- Sound, robust implementations of the virtualization layer (e.g. hypervisor) and the overall cloud platform software
- Sound, robust, security aware implementation of the VNFs
- Integrity (trust) assurance for both platform and VNFs

- Separation of VNFs provided by the virtualization layer (logical separation)
- Optional physical separation of VNFs – at a cost
- Traffic separation by dedicated virtual switches, VLANs and wide area VPNs

- Perimeter security and network internal traffic filtering by virtual firewalls
- Logically or even physically separated security zones

- Cryptographic protection of traffic and of data on storage

- Secure Operation&Maintenance

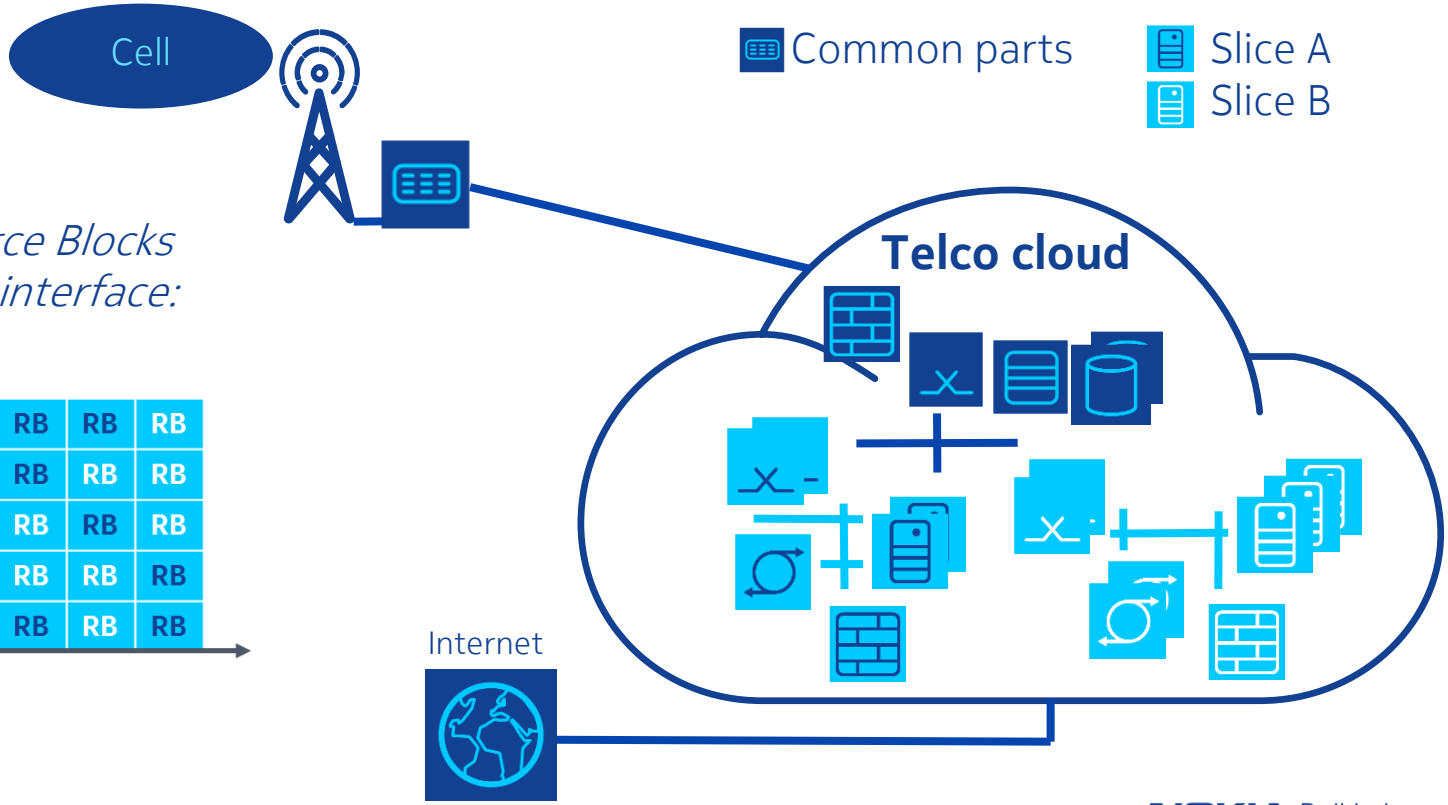
- Reactive security measures

Slicing and Isolation

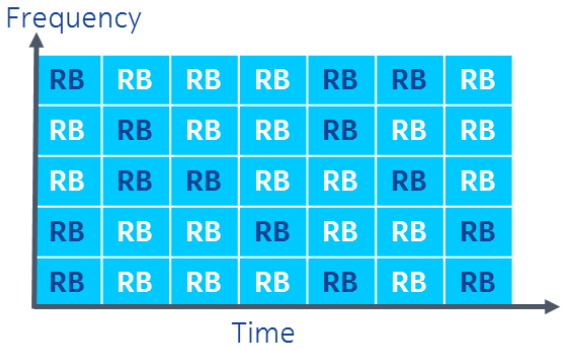
- **Slicing** a mobile network: creating partitions inside the mobile network
  - Different flavors: core network slices, RAN slices, e2e slices
  - Common infrastructure (NFV infrastructure, SDN-based transport)
  - Tailored slices for specific services (eMBB, V2X, mIoT)
  - Multiple slice instances to be rented by multiple verticals (?)
- **Resource Isolation**
  - Resources dedicated to one slice cannot be consumed by another slice.
- **Security isolation**
  - Data/traffic cannot be intercepted/faked by entities of another slice.
- **Isolation**: Resource Isolation + Security Isolation.

➢ The crucial security aspect in network slicing!

A Mobile Network with Two Core Network Slices
Slices share a common RAN



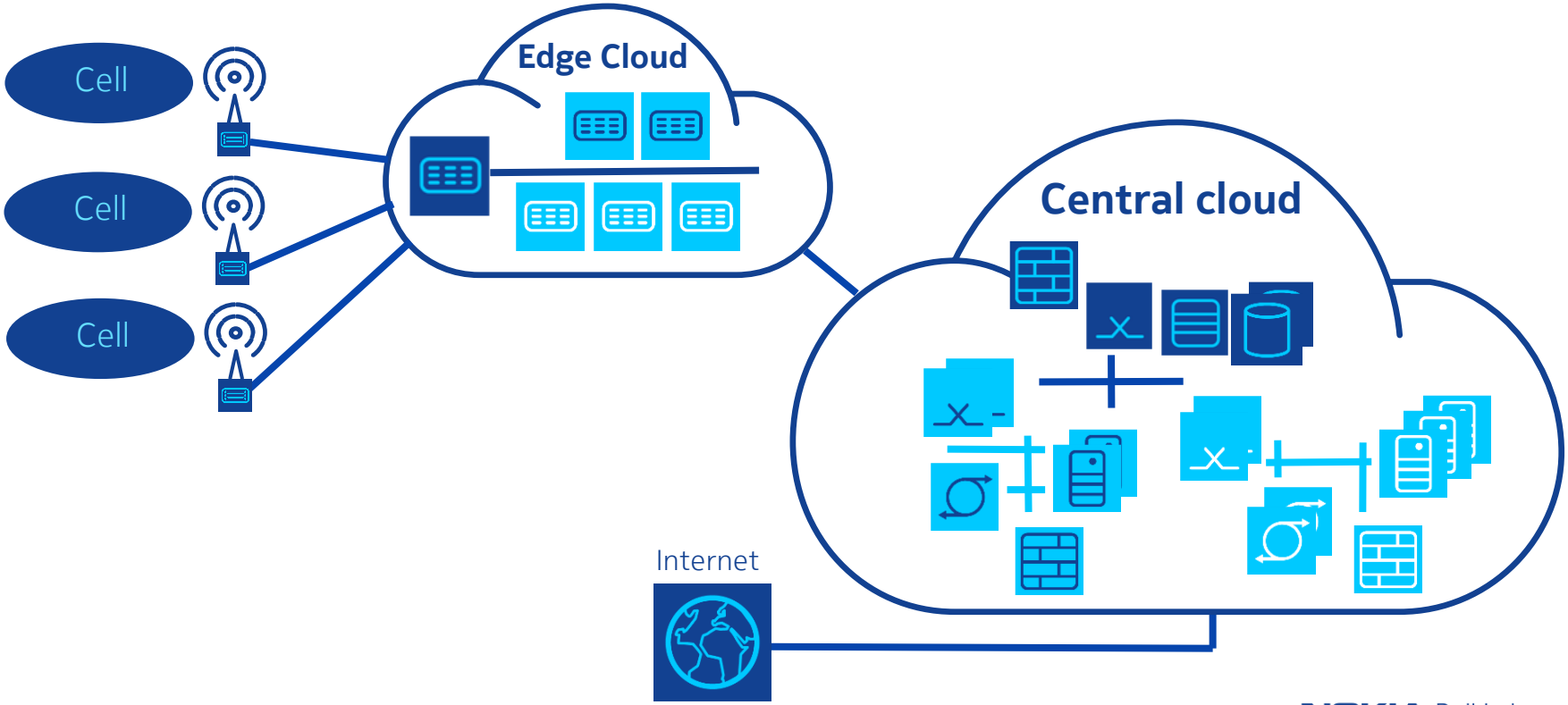
Scheduling Resource Blocks (RBs) on the radio interface:



NOKIA Bell Labs

A Mobile Network with Two RAN/Core Network Slices

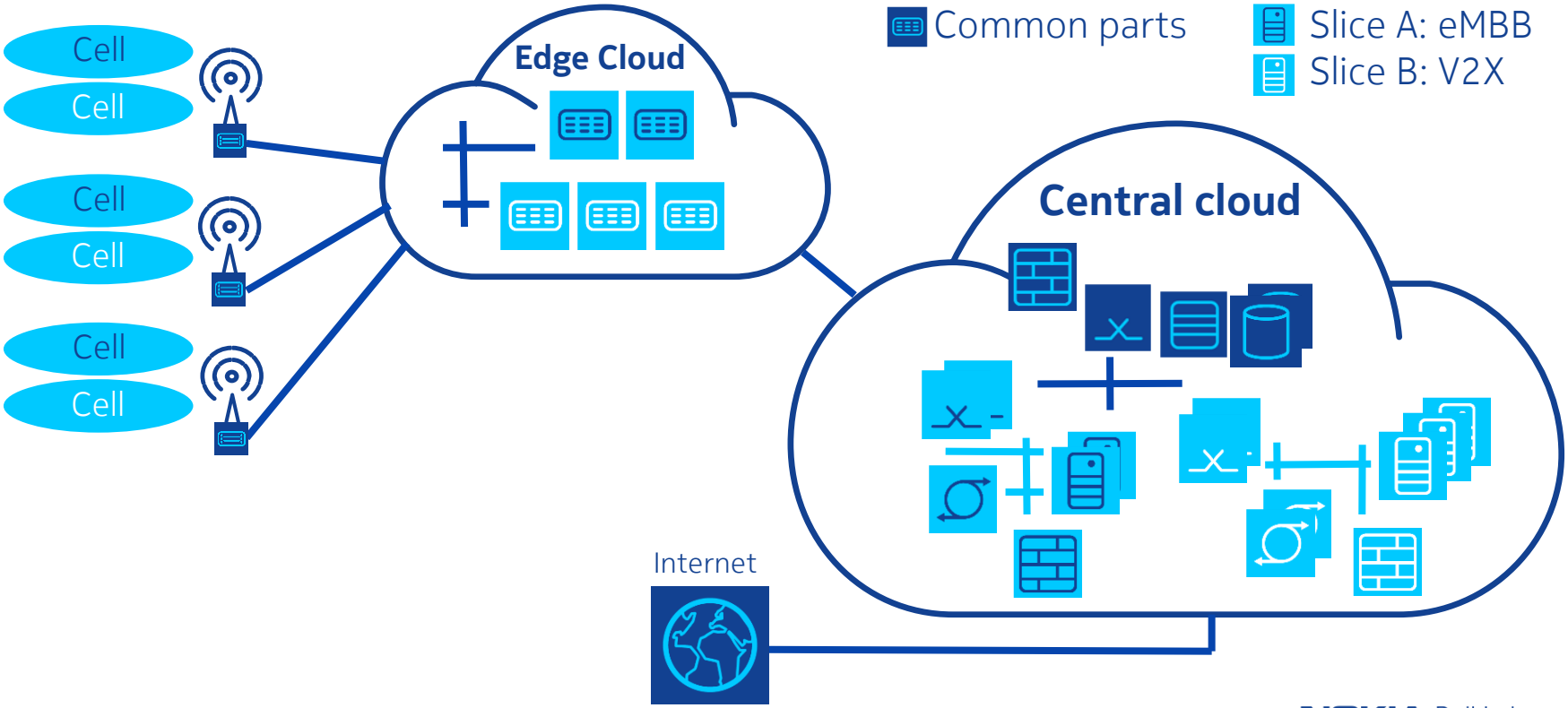
Slices share a common RAN infrastructure plus some RAN functions



NOKIA Bell Labs

A Mobile Network with Two RAN/Core Network Slices, Separated Cells

Fixed radio interface resources per slice



Slice Isolation Issues in the Shared Telco Cloud

Isolation between slices in the cloud by NFV mechanisms

- Relies on a secure telco cloud - security measures as discussed

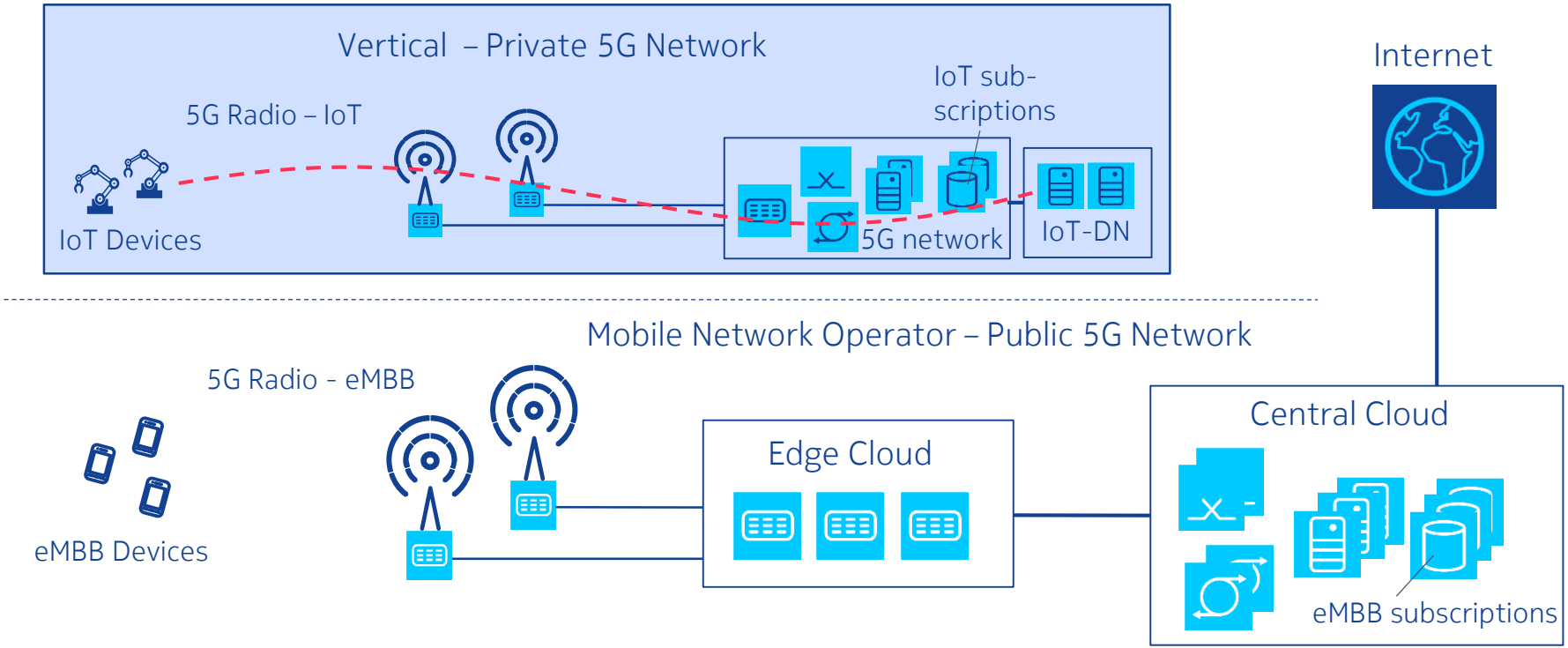
An industry vertical renting/operating a slice needs to trust the telco cloud provider (typically the mobile network operator):

- Correct assignment of NFV infrastructure resources
- Isolation against other slices
- No traffic interception or meta data collection by the telco cloud provider

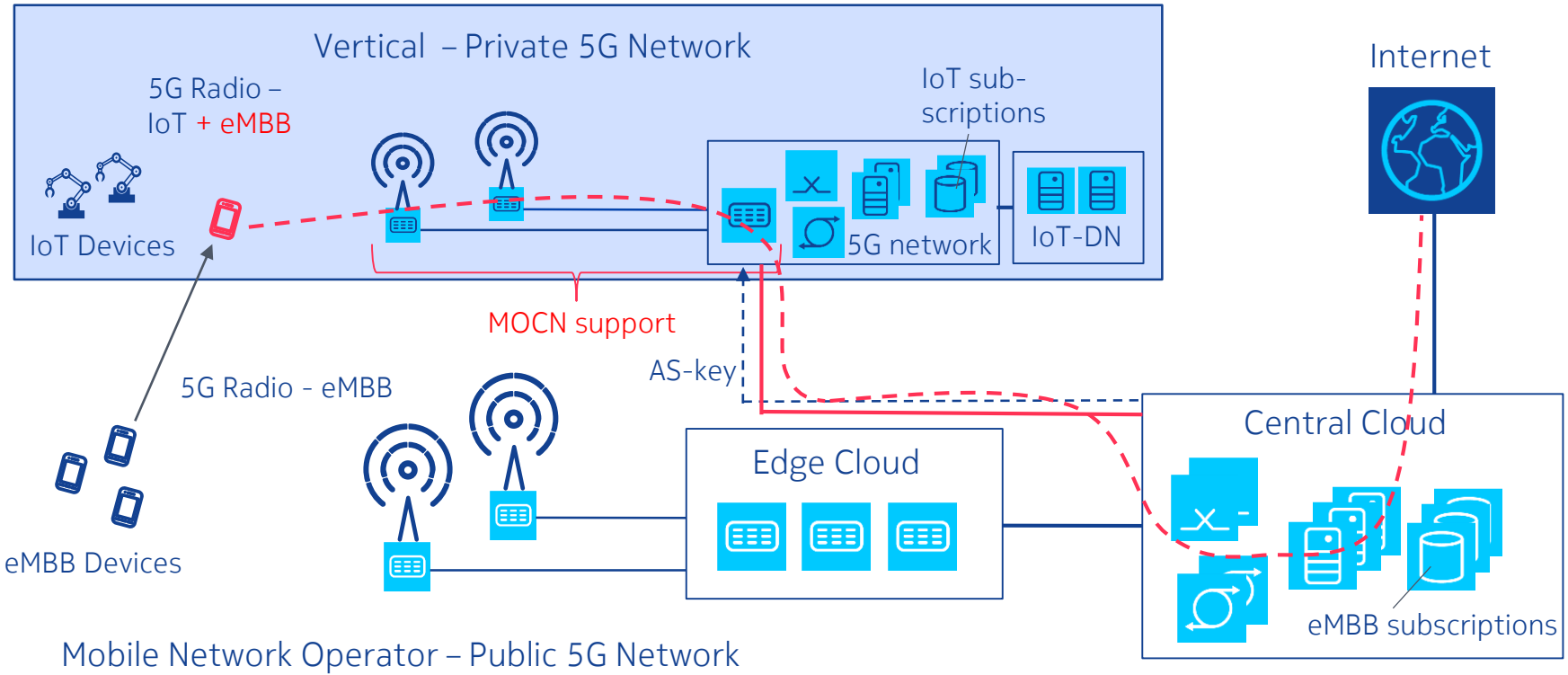
Option: Security isolation via over-the-top security

- Option: Usage of vertical-owned infrastructure
- Investigated in 5G PPP project 5G NORMA (work in progress)

A Fully Isolated Private 5G IoT Network Owned by a Vertical

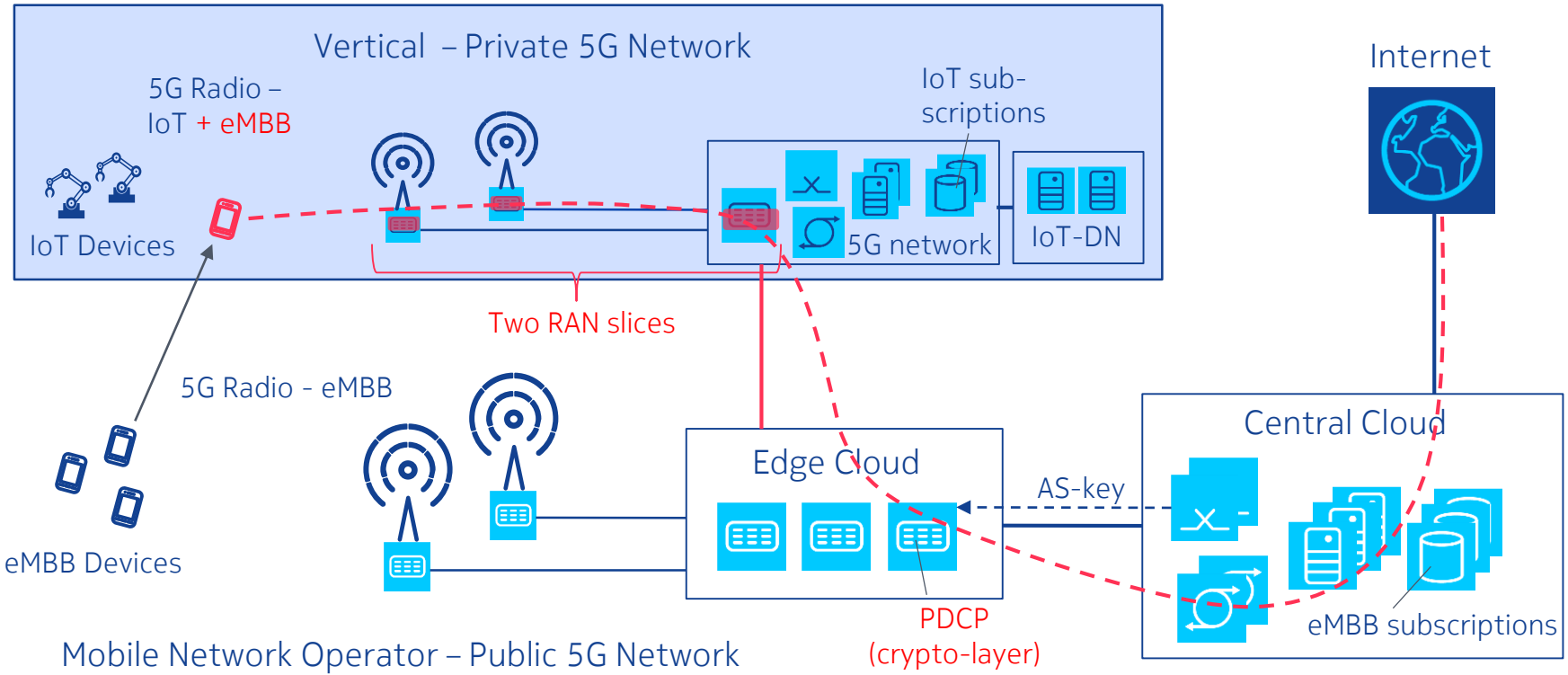


Public eMBB Service in a Private Network: MOCN-like Solution



AS: Access Stratum MOCN: Multi-Operator Core Network

Public eMBB Service in a Private Network: Slicing Solution



Summary: Securing 5G Mobile Networks Built on Distributed Telco Clouds

In 5G, there is a substantial change in the network architecture:

- NFV and SDN support highly dynamic networking
- Network slicing supports multi-tenancy

Strong impact on the security architecture

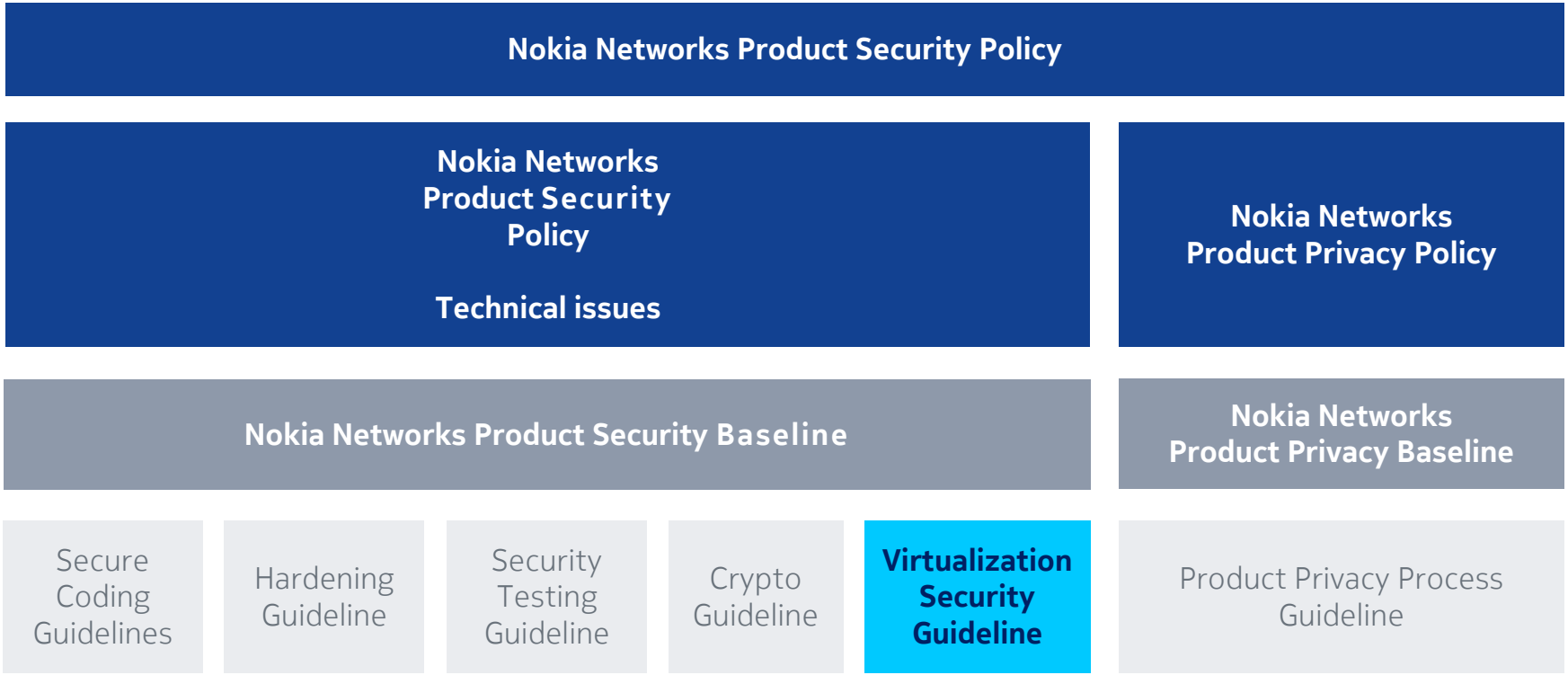
- Securing the NFV infrastructure + the VNFs
- Transferring network security measures into the telco cloud – physical separation is much less likely than in 4G

We can secure 5G networks built on distributed telco clouds - but we must work for it!

Backup

NOKIA

Security for NFV-Based Products (Example Nokia)



NOKIA Bell Labs


NOKIA