NOKIA Bell Labs

ITU Workshop on 5G Security

Geneva, Switzerland, 19 March 2018

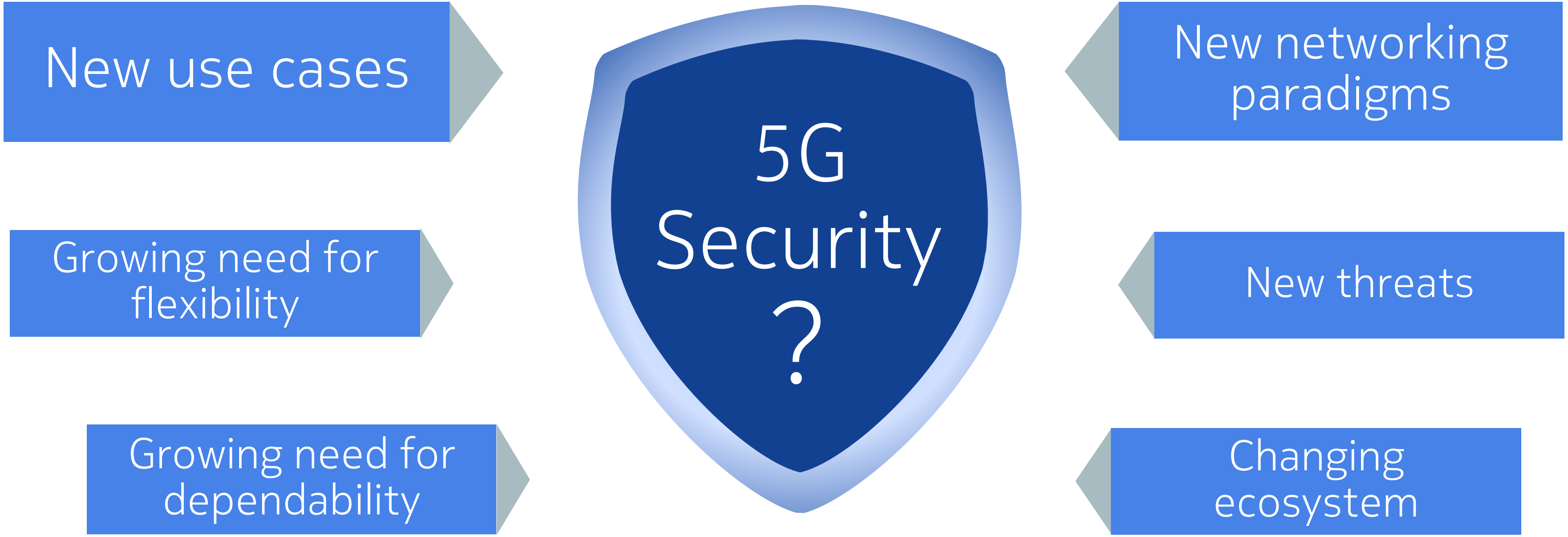
5G Security Overview: Security for Programmable Cloud-Based Mobile Networks

Peter Schneider, Nokia Bell Labs

Outline

- 5G security drivers, threats, requirements and high level vision
- Layers of mobile network security today
- From LTE to 5G – towards a programmable, cloud-based, sliced network
- Elements of a 5G security architecture
- Layers of mobile network security in a 3GPP-specified 5G System
- (Network slicing security)
- Summary: Securing programmable, cloud-based, sliced 5G networks

5G Security Drivers



New use cases

Growing need for flexibility

Growing need for dependability

5G Security ?

New networking paradigms

New threats

Changing ecosystem

5G Security Threats

The well-known large-scale threats apply:

- Exploits of software vulnerabilities
- Exploits of configuration errors and bad operational practices
- Flooding attacks (from multiple sources): (Distributed) DoS attacks

Adopting new networking paradigms increases the attack surface

- SDN: Separating forwarding and control, splitting up monolithic control into various control apps running on a common SDN controller
- NFV: Adding a virtualization layer, a new stack of management and orchestration (MANO) components and various new interfaces

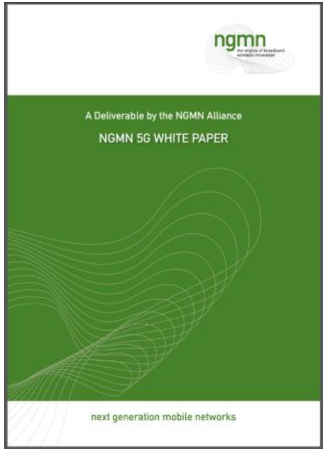
Infrastructure sharing facilitates side channel attacks

Critical services in 5G → Successful attacks may have higher impacts

5G Security Requirements: Example NGMN Alliance

NGMN Alliance 5G Whitepaper, Version 1.0, 17-February-2015:

> “enhanced performance is expected to be provided along … with the capability to, among others, **ensure security and trust, identity, and privacy**”


ngmn

A Deliverable by the NGMN Alliance

NGMN 5G WHITE PAPER

next generation mobile networks

“Specific security design for use cases which require extremely low latency (including the latency of initiating communications)”

”Improve security of 5G small cell nodes”

”provide better secrecy than 4G”

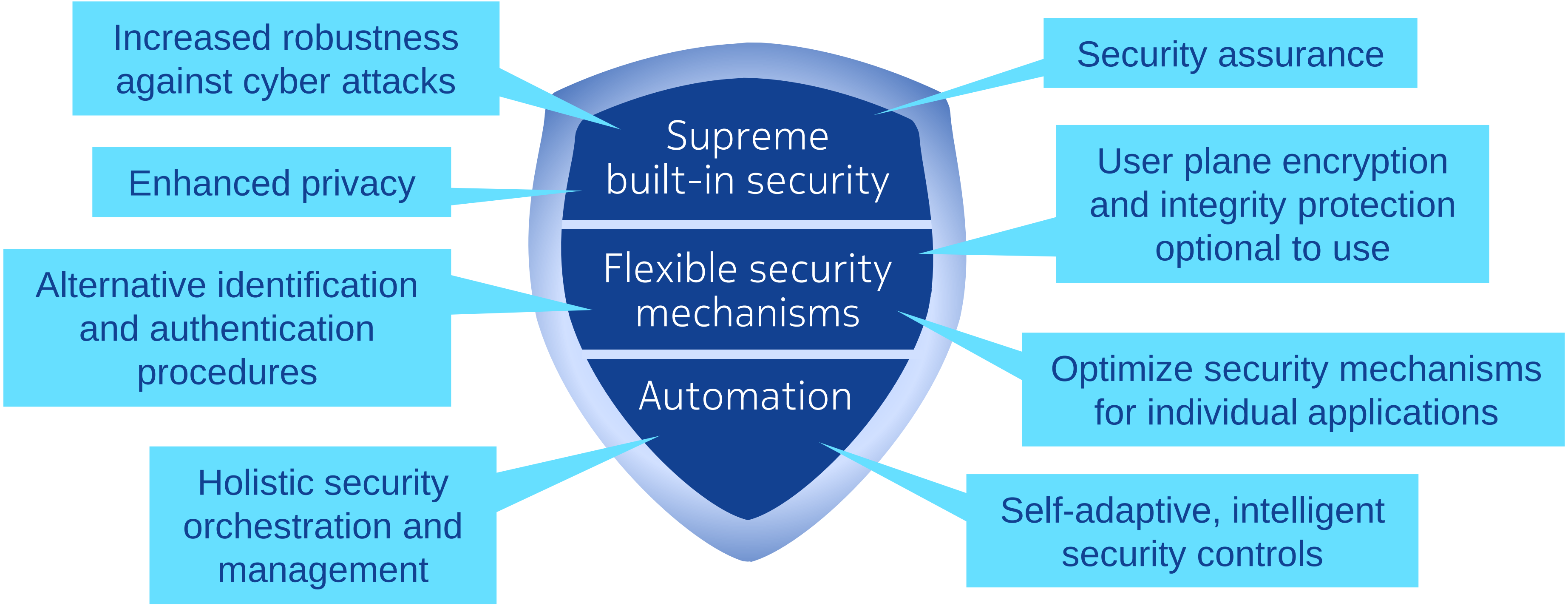
“Improve resilience and availability of the network against signalling based threats, including overload”

“Improve system robustness against smart jamming attacks”

➢ Substantial security requirements!

NGMN Next Generation Mobile Networks

5G Security Vision



Supreme built-in security

Flexible security mechanisms

Automation

Increased robustness against cyber attacks

Enhanced privacy

Alternative identification and authentication procedures

Holistic security orchestration and management

Security assurance

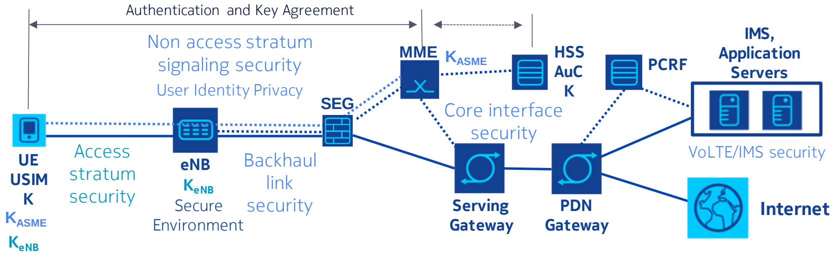
User plane encryption and integrity protection optional to use

Optimize security mechanisms for individual applications

Self-adaptive, intelligent security controls

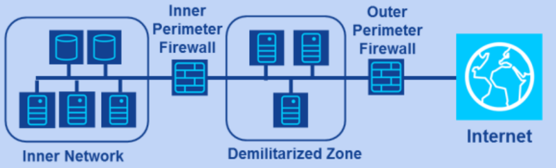
Layers of Mobile Network Security as of Today (Example LTE)

3GPP-specified security architecture



Network security not specified by 3GPP

Perimeter security, network zoning, traffic separation



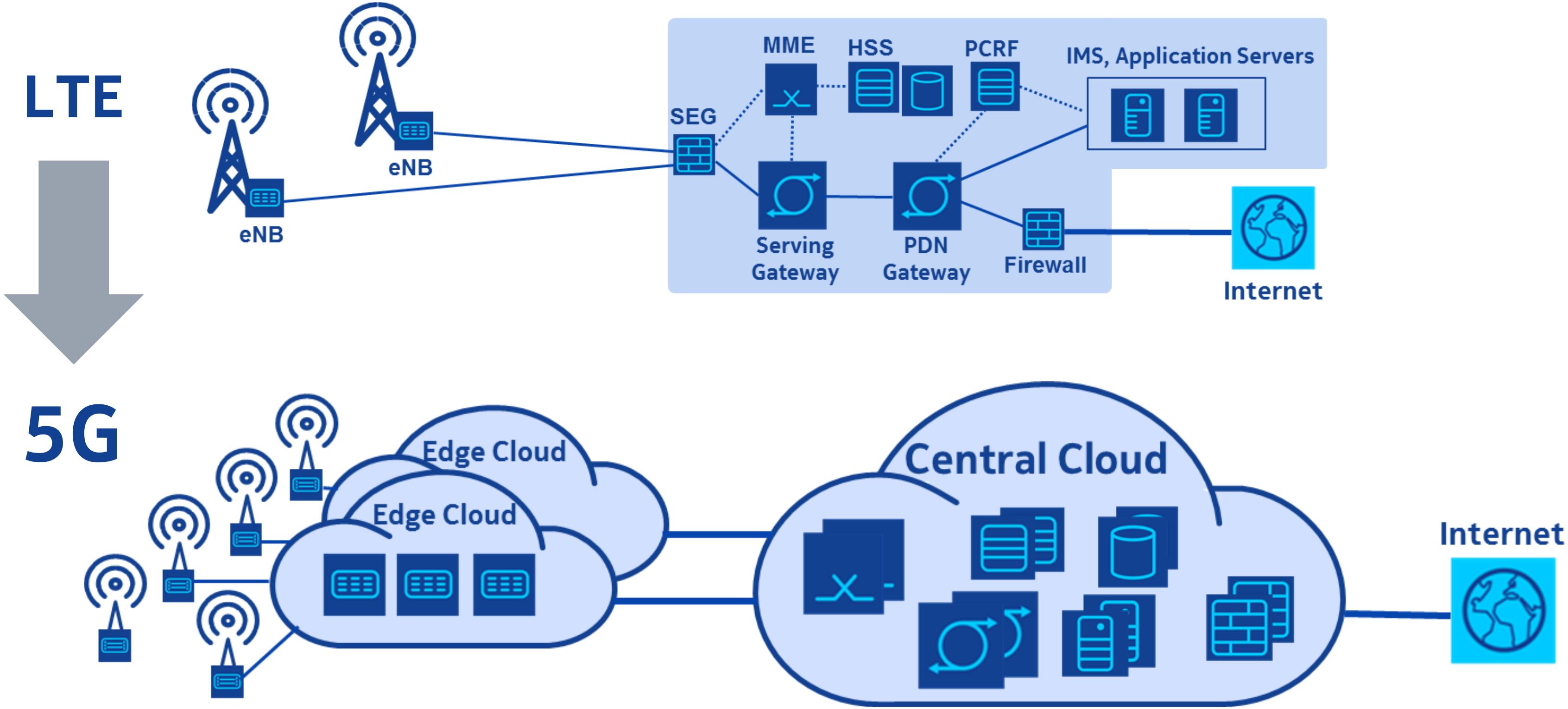
Secure operation and maintenance

Reactive security measures: Monitoring, analytics, attack detection

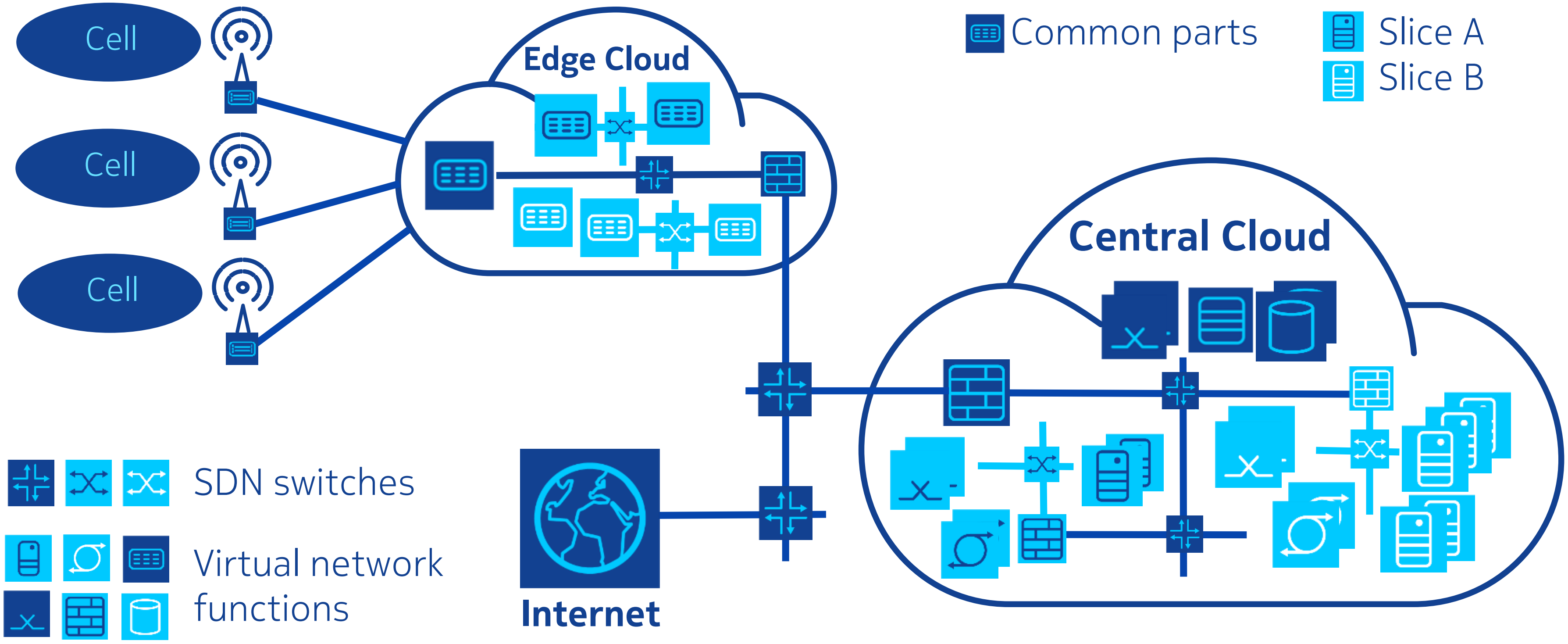
Network element security measures

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

From LTE to 5G: Adopting New Networking Paradigms



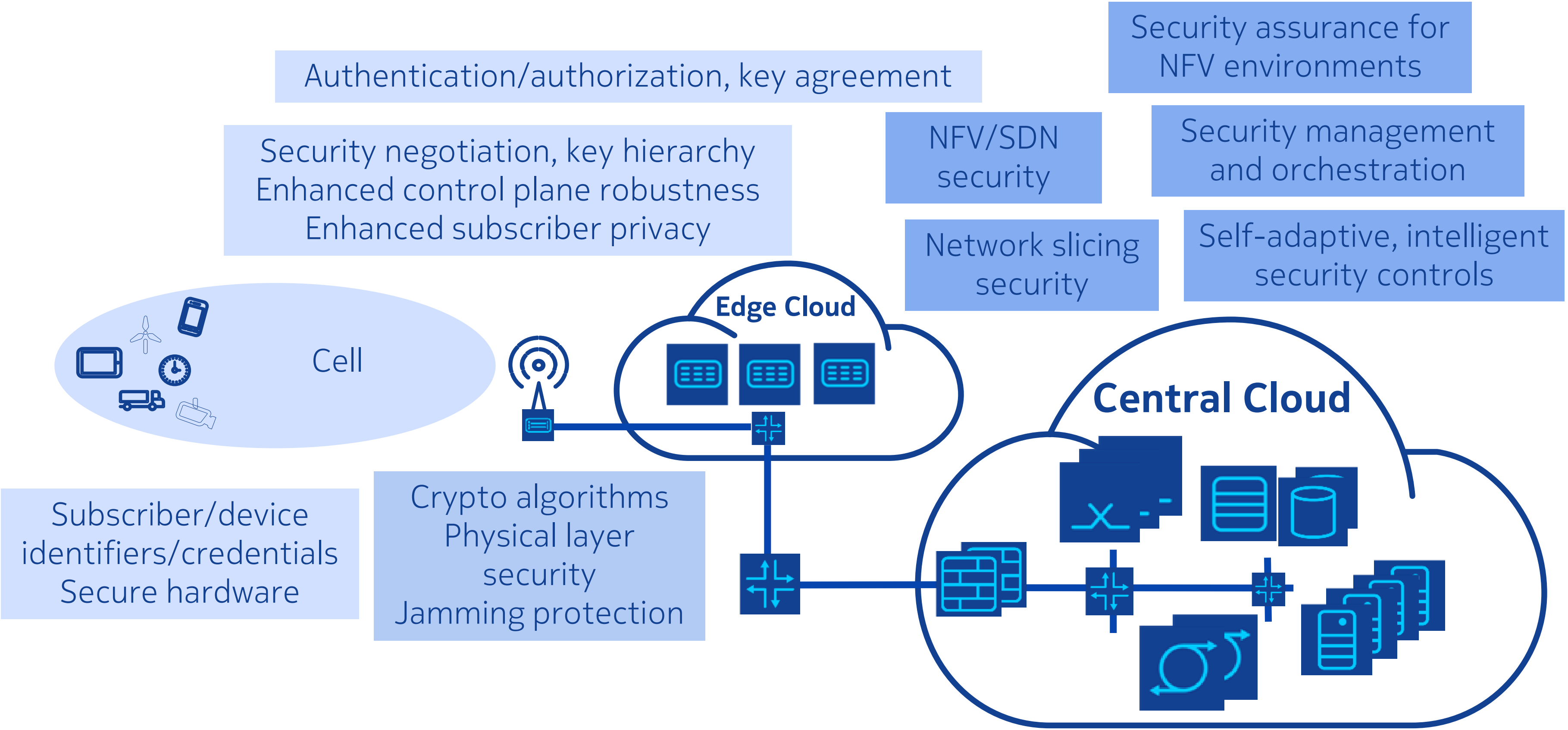
A Programmable, Cloud-Based, Sliced 5G Network



Public

NOKIA Bell Labs

Elements of a 5G Security Architecture



Authentication/authorization, key agreement

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

Subscriber/device identifiers/credentials
Secure hardware

Crypto algorithms
Physical layer security
Jamming protection

Security assurance for NFV environments

NFV/SDN security

Security management and orchestration

Network slicing security

Self-adaptive, intelligent security controls

Layers of Mobile Network Security in a 3GPP 5G System

3GPP-specified security architecture

New access-agnostic authentication framework
Enhanced subscription privacy and user plane protection
EAP-based “secondary authentication”
Security for service-based interfaces
Enhancements for interconnection security

5G Phase 1
Rel.15

Network security not specified by 3GPP

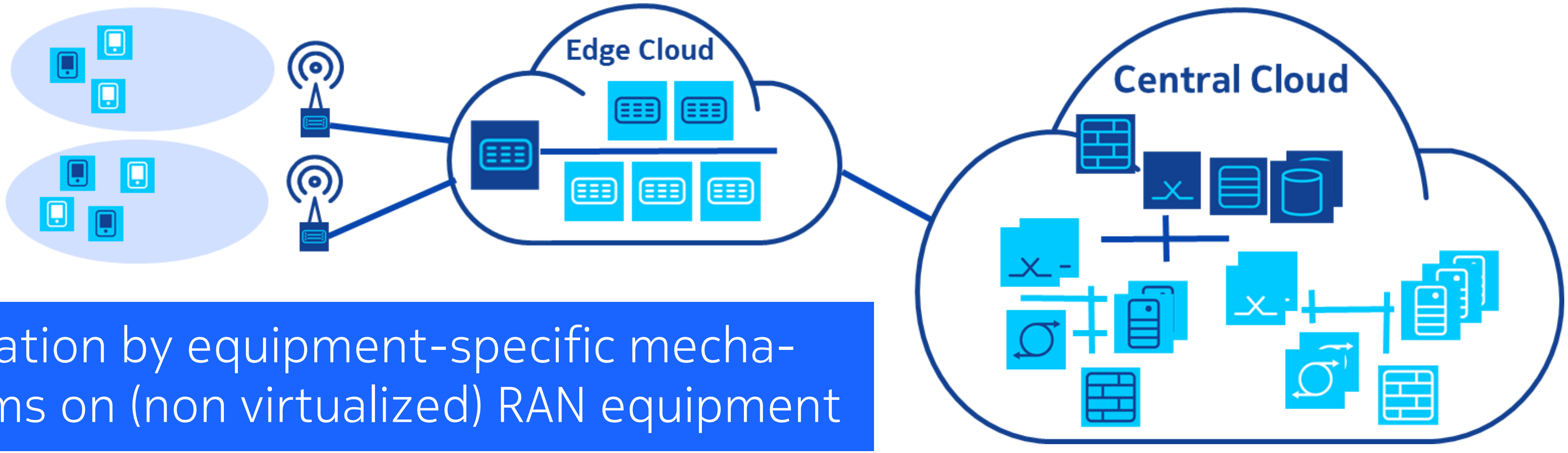
Holistic, automated security management and orchestration
Perimeter security and traffic filtering by virtual firewalls
Logically or even physically separated security zones
Traffic separation by VLANs and wide area VPNs
Automated, self-adaptive, intelligent security controls

VNF security
Telco cloud security

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

Network Slice Isolation – The Crucial Slicing Security Aspect

Isolation in the cloud by NFV mechanisms in the (central/edge) cloud



Isolation by equipment-specific mechanisms on (non virtualized) RAN equipment

Isolation in the transport by VPNs created via SDN

Specific Attacks Against Sliced Networks

Slicing-specific attacks

DoS attacks on “small” slices

Attacks on interfaces to common network parts (vertical → mobile network operator)

Attacks on management interfaces provided for verticals to manage their slices

Attacks via inter-slice interfaces

Attacks on slicing-specific procedures: Slice selection, slicing-specific authentication and authorization, slice management

Malicious message routing between different slices

➢ Mitigation by state-of-the-art means – with room for improvement

Summary: Securing Programmable, Cloud-Based, Sliced 5G Networks

Demanding new use cases require supreme, built-in security.

The variety of use cases requires increased flexibility in the security setup.

Making networks programmable, moving into the telco cloud and introducing multi-tenancy has a strong impact on 5G security concepts:

- Securing SDN and NFV;
- Transferring filtering, network zoning and traffic separation concepts into the telco cloud, where physical separation is much less an option;
- Isolating multiple slices of multiple tenants (e.g. industry verticals).

Highly dynamic 5G networks require a high level of automation in security orchestration and management, as well as automated, analytics- and machine-learning-based attack detection and mitigation.