NOKIA Bell Labs

5G Security

Future of Networking, March 19, 2019

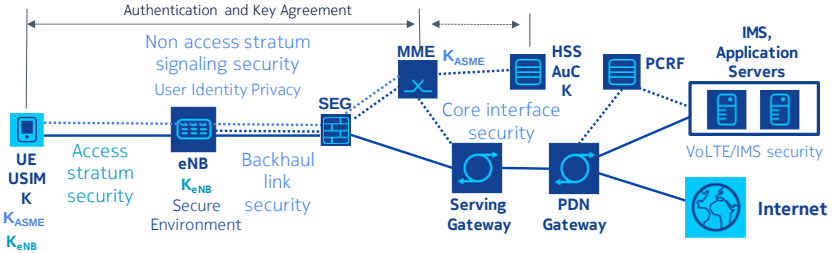
Peter Schneider, Nokia Bell Labs

Agenda

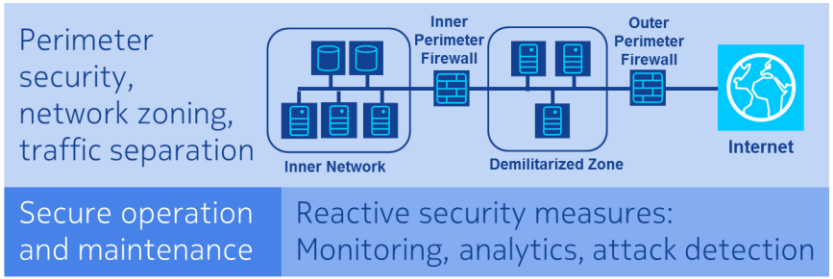
- Mobile network security today – example LTE
- 5G security: drivers, requirements, vision
- 5G networking paradigms: Network Function Virtualization (NFV), Software Defined Networking (SDN), Network Slicing
- Elements of a 5G security architecture
- NFV Security
- Network slicing security
- 3GPP 5G security specification
- Summary and conclusion

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

3GPP-specified security architecture



Network security not specified by 3GPP



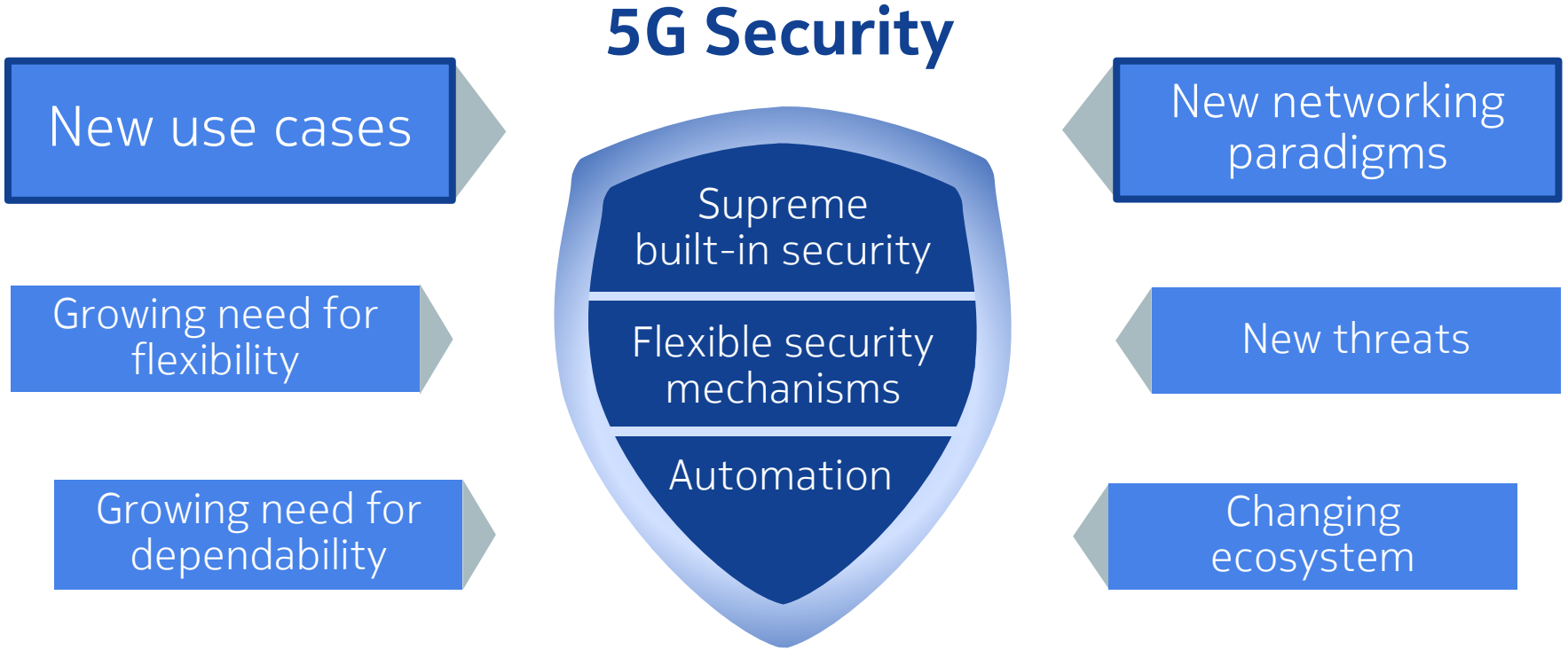
Network element security measures

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

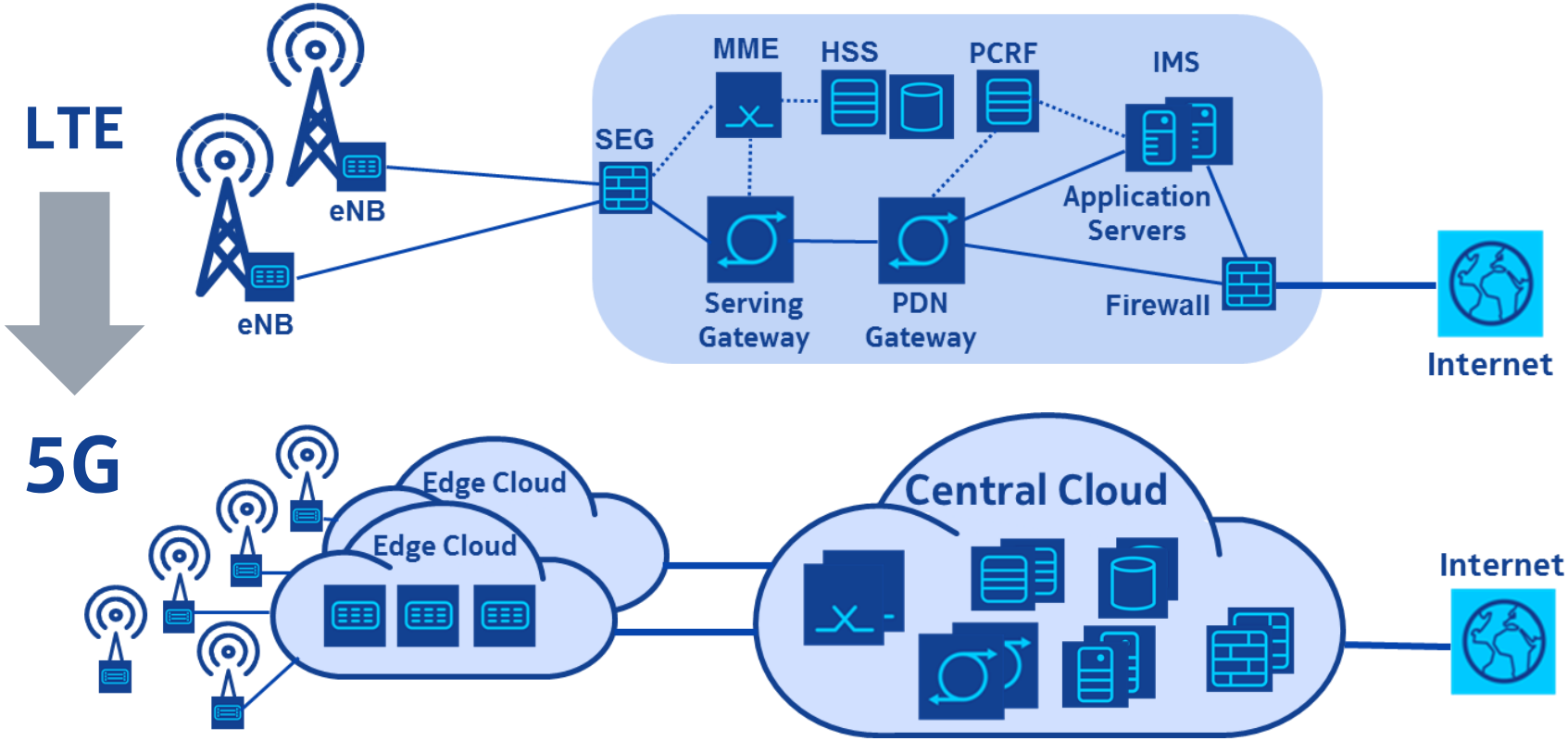
NOKIA Bell Labs

5G Security Drivers

5G Security Drivers

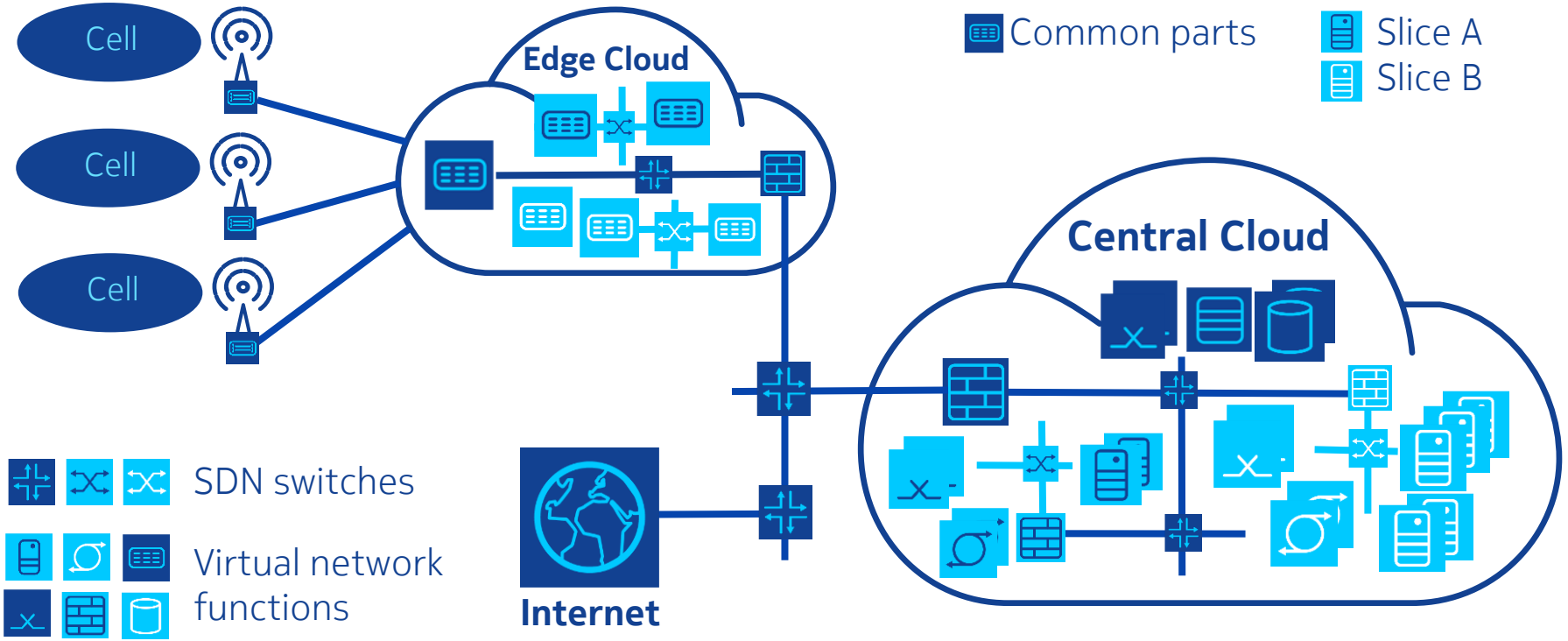


From LTE to 5G: Adopting New Networking Paradigms



NOKIA Bell Labs

A 5G Mobile Network Implemented on Distributed Telco Clouds and Supporting Multiple Network Slices



Elements of a 5G Security Architecture

Authentication/authorization, key agreement

Security assurance for NFV environments

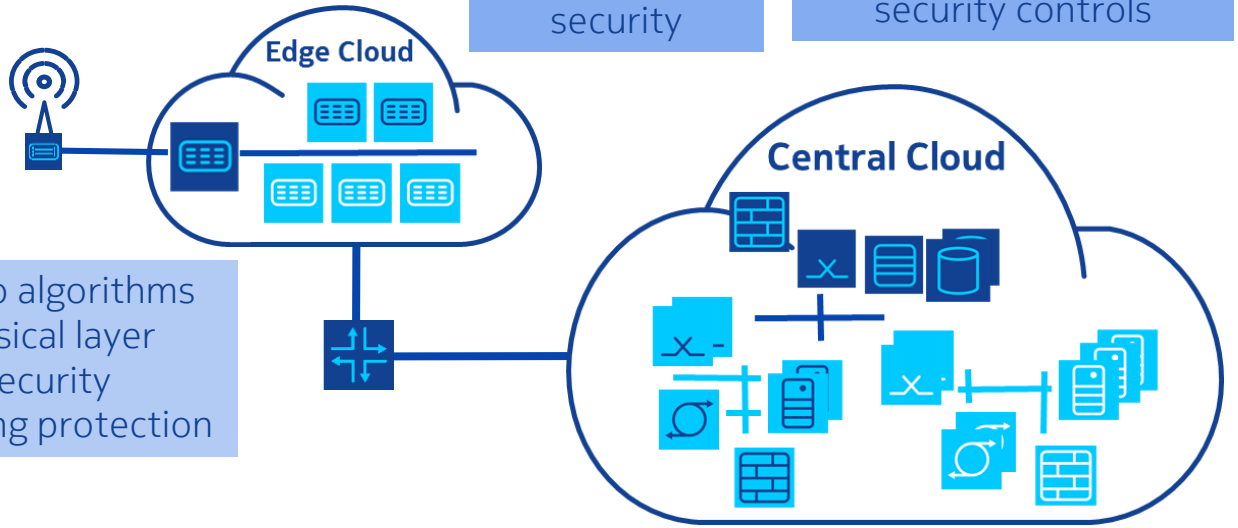
Security negotiation, key hierarchy
Enhanced control plane robustness
Enhanced subscriber privacy

NFV/SDN security

Security management and orchestration

Network slicing security

Self-adaptive, intelligent security controls



Subscriber/device identifiers/credentials
Secure hardware

Crypto algorithms
Physical layer security
Jamming protection

Network Function Virtualization Security

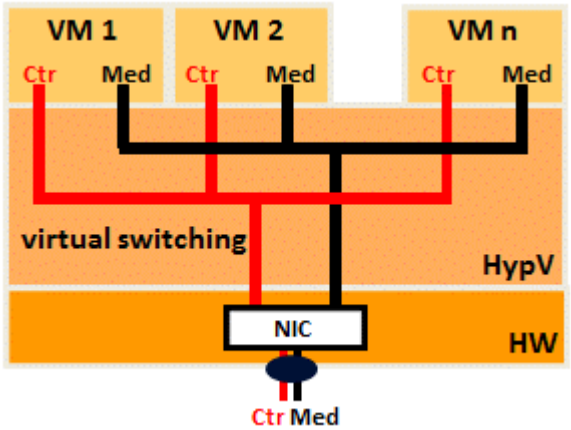
“Network Element Security” for Virtualized Networks

Network elements replaced by VNFs running on a cloud platform

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

- ➢ Secure the platform
- ➢ Secure the VNFs
- ➢ Security assurance for VNFs that can be deployed on different platforms

Isolation and Traffic Separation in the Telco Cloud



- Separation of VMs relies on the hypervisor – software flaws may compromise it completely (e.g. allow VM1 to access the memory of VM2)
- Virtual networking allows logical traffic separation
- No physical separation of interfaces for different traffic types at a single VM
- No physical separation of traffic of different VMs running on the same HW platform
- Traffic separation relies on the hypervisor

Network Security Measures for Virtualized Networks

Network zoning can be implemented in a straightforward way:

- The NFV environment facilitates separation, e.g. virtual machines are separated by a hypervisor
- Dedicated VLANs to provide connectivity between the VMs forming a zone
- Traffic between zones may be filtered by virtual firewalls
- Even physical separation may be possible – on the cost of resource usage efficiency

The external perimeter may be secured by a virtual firewall; physically separated firewalls can protect the overall data center infrastructure

Traffic separation by dedicated virtual switches, VLANs and wide area VPNs – physical separation is hardly applicable

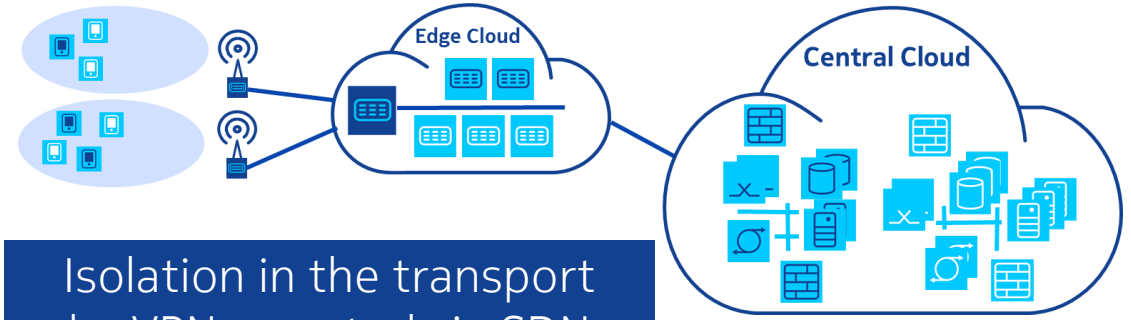
Network Slicing Security

Network Slice Isolation – The Crucial Slicing Security Aspect

Isolation means resource isolation + security isolation

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

➢ Slice isolation can be achieved assuming sound implementations (NFV environment, SDN transport, non-virtualized equipment)

Other Slicing Security Aspects

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 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

Slicing facilitates individual security mechanisms per slice

Slicing facilitates different security assurance levels per slice

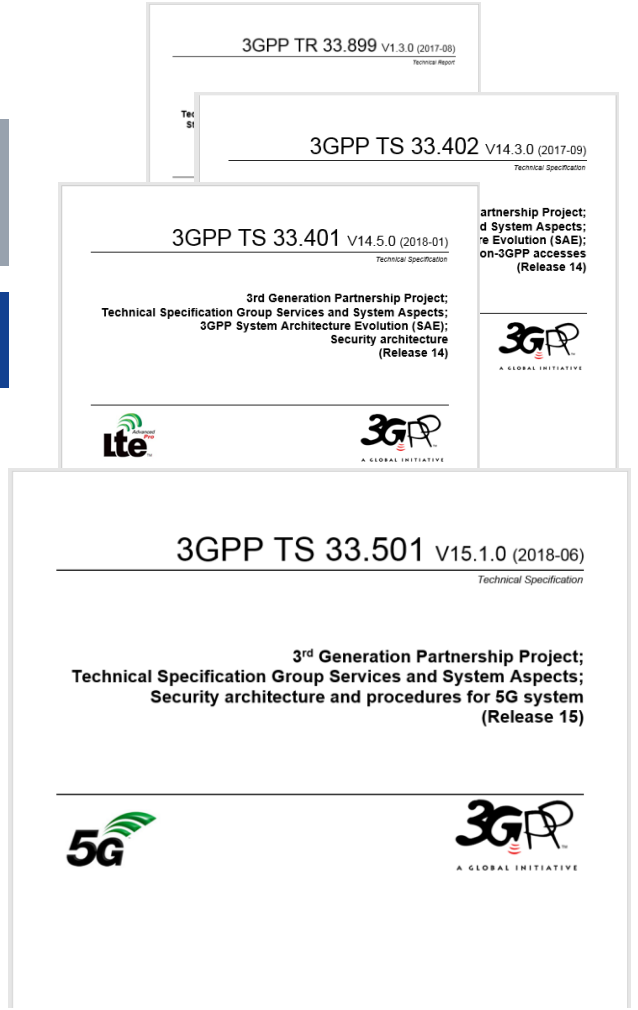
3GPP 5G Security Specification

Overview 3GPP 5G Security Standardization

3GPP Technical Specification 33.501, Release15 “Security Architecture and Procedures for 5G System”

➢ New 5G security features at a glance:

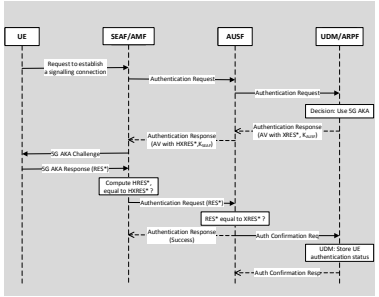
- New access-agnostic authentication framework with improved home network control in roaming scenarios
- Enhanced subscription privacy
- User plane integrity protection
- EAP-based “secondary authentication”
- Security for service-based interfaces
- Enhancements for interconnection security

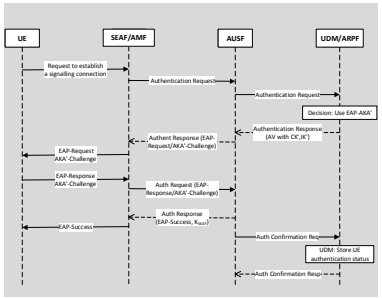


New Security Features in 3GPP Release 15

New access-agnostic authentication framework with improved home network control in roaming scenarios

- Two authentication methods, 5G AKA (enhancing LTE's EPS AKA) and EAP-AKA'
- Both provide assurance to the Home Network that the UE is present in the Visited Network
- Besides EAP-AKA', other EAP methods can be implemented by operators (not for public use)
- "Access agnostic": Both methods applicable for 3GPP as well as non-3GPP access





Scaled up pictures in the backup

NOKIA Bell Labs

Enhanced Subscription Privacy, User Plane Integrity Protection

IMSI catching (and thus subscriber location tracking) is possible in LTE
(a deliberate decision in LTE)

- **Fully covered in 5G** by Subscription Concealed Identity (SUCI)
- However, there is also a “null scheme” (without encryption)
  - Will some legislations prefer their law enforcement agencies remain capable of IMSI catching ?

No user plane integrity protection
(a deliberate decision in LTE)

- **Fully covered in 5G**: Mandatory to support by network and UE
- Not mandatory to use – not all traffic will require it

Summary: 5G Security

Summary: 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

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


NOKIA