ETSI Security Conference 2022

Current 5G Security Standardization Overview

Suresh Nair, 3GPP SA3 Chair

26/09/2022

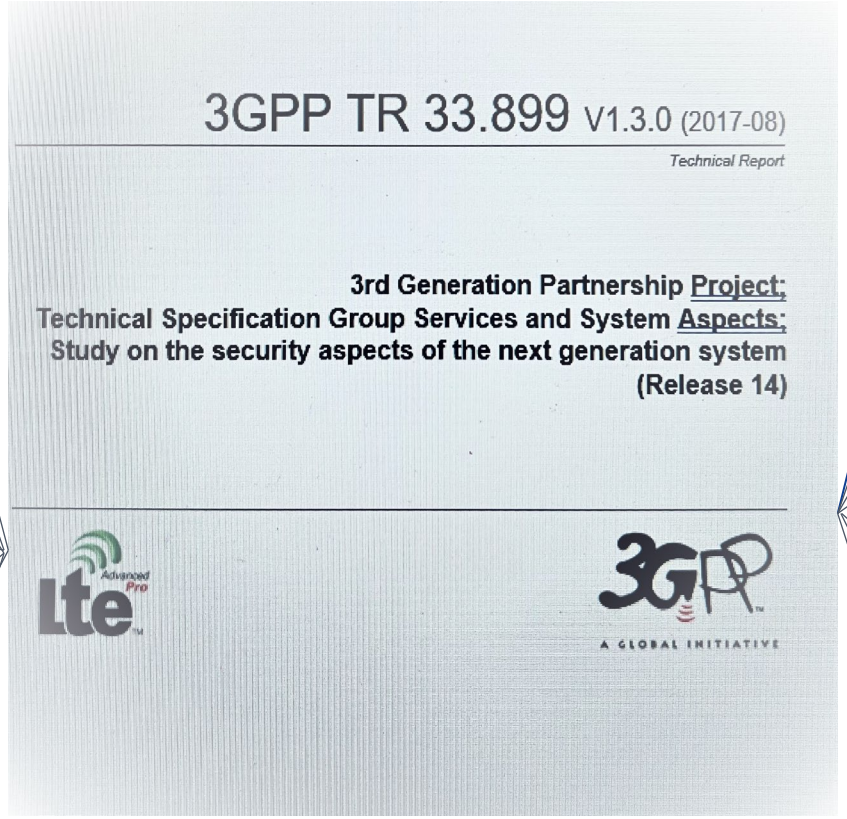
Contents

NOKIA

5G Security Foundations

3GPP Study on Security aspects of next Generation

- Architectural aspects
  21KI, 51 solutions
- Authentication
  11 KI, 30 Solutions
- Security context & Key management
  11 KI, 12 solutions
- RAN Security
  17 KI, 26 solutions
- Security within NG-UE
  4KI, 2 solutions
- Authorization
  3 KI, 4 solutions
- Subscription privacy
  10KI, 24 solutions

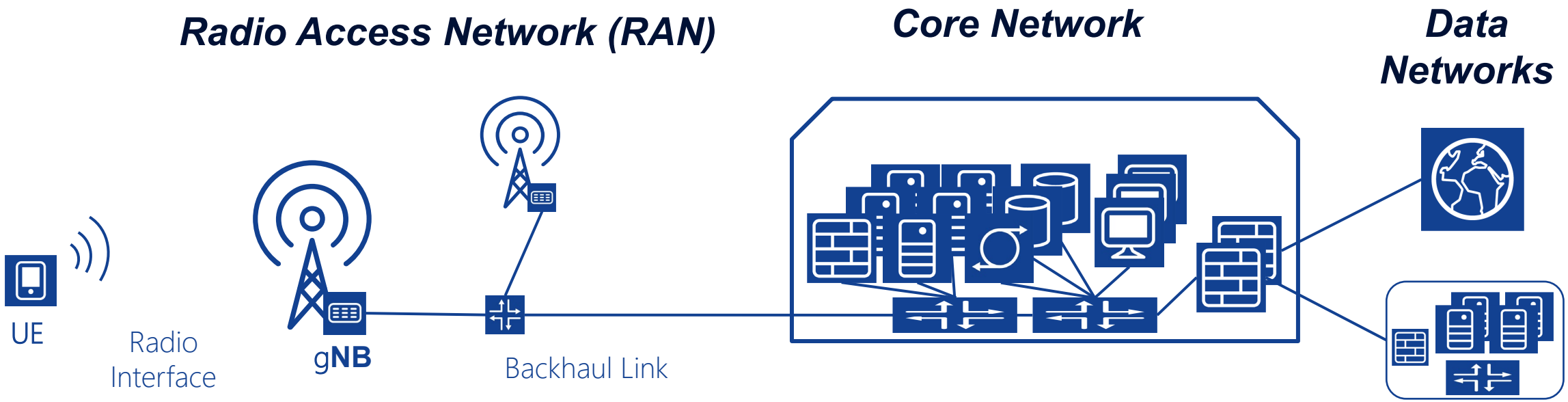


17 security areas

Conclusions led to the Rel-15 normative TS work

- Network Slicing security
  8KI, 14 solutions
- Relay Security
  3KI, 3 solutions
- Network domain security
  3 KI, 2 solutions
- Security visibility &configurability
  5 KI, 5 solutions
- Credential provisioning
  2 KI, 4 solutions
- Interworking & migration
  4KI, 2 solutions
- Small data
  4KI, 2 solutions

Overview 5G System (5GS), aka 5G Public Land Mobile Network (5G PLMN)



User Equipment (UE)

consisting of
Mobile Equipment (ME)
and
Universal Subscriber Identity Module (USIM)

Base station: "gNB"

Serves multiple "cells"

Some Core network functions:

AMF	Access and Mobility Management Function
AUSF	Authentication Server Function
SEAF	Security Anchor Function
SEG	Security Gateway
SMF	Session Management Function
UDM	Unified Data Management
UPF	User Plane Function

Examples:

- The Internet
- Industrial IoT networks
- Enterprise networks

5G security architecture features in Rel-15

Unified authentication framework & Access-agnostic authentication

Primary authentication (Registration)

Secondary authentication (Access to ext. DN)

Increased home control (UE in SN verification)

Enhanced subscriber privacy (no IMSI catcher anymore)

RAN security (now also user plane integrity protection)

Service based architecture & Interconnect security

5GS-EPS interworking security

LTE-NR Dual Connectivity

3GPP A GLOBAL INITIATIVE

Technical Specifications for security

3GPP TS 33.501

5G security

3GPP TS 33.401

LTE security with 5G enhancements on dual connectivity)

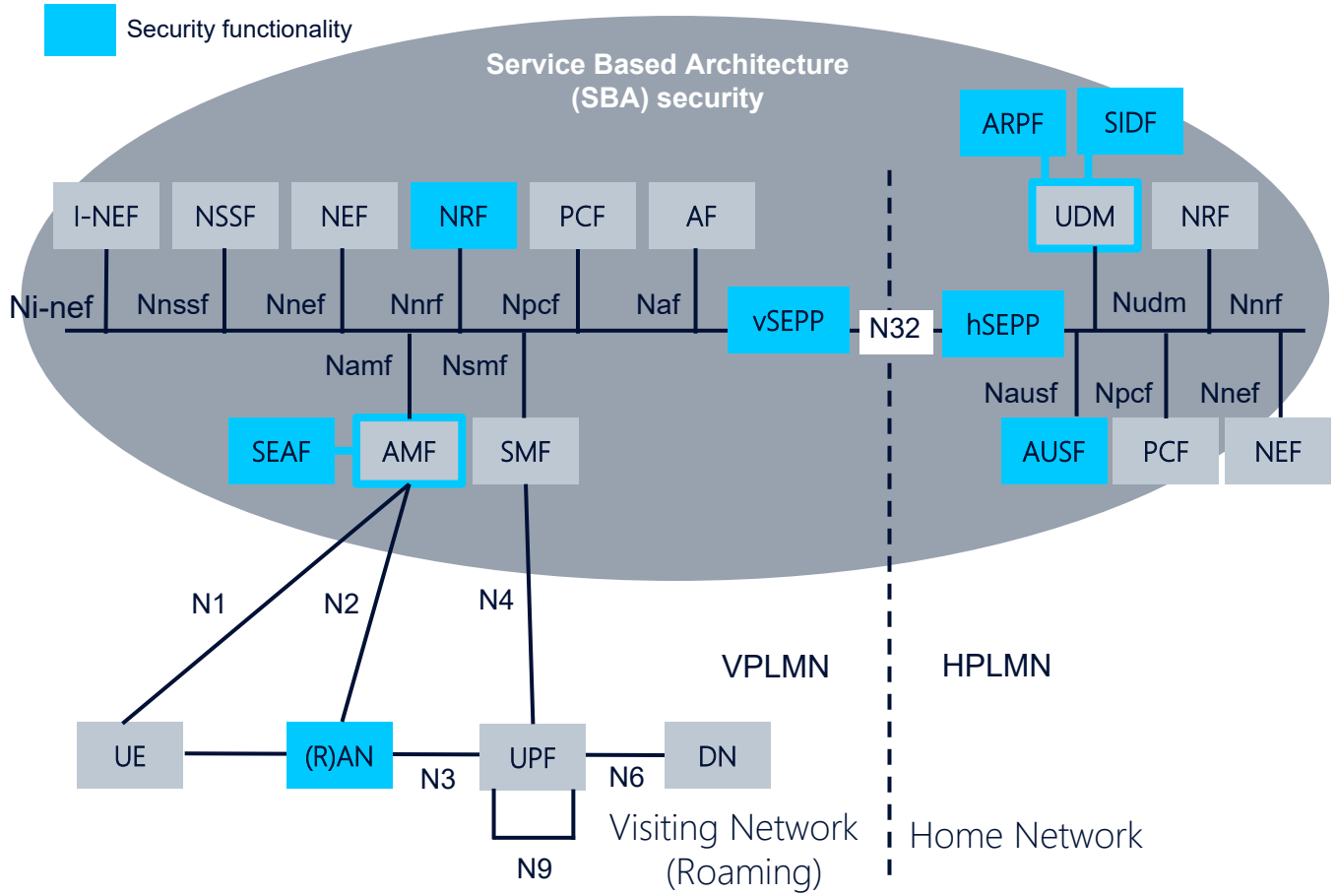
3GPP TR 33.899

(study for TS work; Refer to Annex for agreements)

NOKIA

3GPP security improvements with 5G

In the RAN:
- Enhanced subscriber (location) privacy: International Mobile Subscriber Identity (IMSI) encryption with Subscription Permanent Identifier (SUPI) / Subscription Concealed Identifier (SUCI)
- User plane integrity protection
- Device and network mutual authentication with the home network



In the CN:
- Security for service-based interfaces
- Enhancements for interconnection security: Security Edge Protection Proxy (SEPP) for secure roaming
- Steering of Roaming

End-to-End:
- Improved signaling plane and user plane protection: Use of TLS between 5G Core functions, with option to use DTLS to protect signaling between RAN and Core
- Network slicing for traffic segmentation & Slice-specific authentication
- Security assurance specifications

5G Rel-16 features

Annex to 3GPP TS 33.501 or independent TS

- Enhanced SBA
- Non Public Networks (NPN)
- Network Slice security
- CIoT Enhancements
- Security Assurance Specs for all 5G nodes
- Wireless Wireline Convergence (WWC)
- 5G Location services
- Integrated Access Backhaul (IAB)
- User Plane Integrity
- Long term key update
- Authentication Enhancements
- Authentication Key management for Applications (AKMA)
- V2X
- Security Impacts of Virtualization

5G Rel-17 features

Annex to 3GPP TS 33.501 or independent TS

- 5G Proximity Services
- 5G Multicast Broadcast Services
- Network Slice security
- Network Automation(Ph2)
- Security Assurance Specs for all 5G nodes
- Security for EDGE Applications
- Integration of GBA In to 5GC
- Uncrewed Aerial Systems
- LTE User Plane Integrity
- Long term key update
- Industrial IoT
- Non Public Networks
- 5GMSG
- Security Impacts of Virtualization
- Multi-USIM

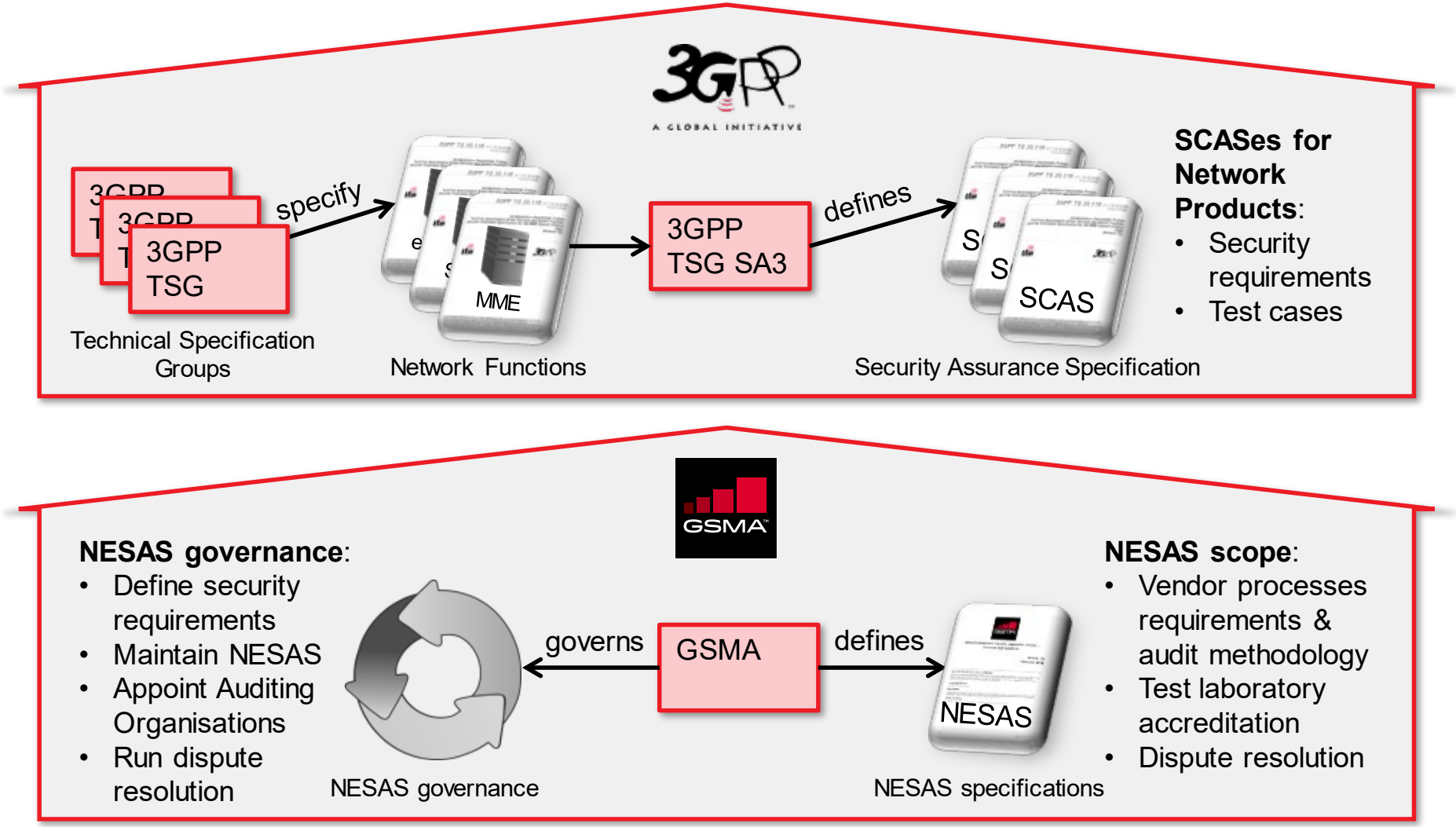
Rel-18 Studies and normative work

Study on 5G security enhancement against false base stations
Study on Security Impacts of Virtualisation
Study on Security Aspects of Proximity Based Services in 5GS Phase 2
Study on privacy of identifiers over radio access
Study on Standardising Automated Certificate Management in SBA
New SID on AKMA phase 2
Study of Security aspect of home network triggered primary authentication
Study on security aspects of enablers for Network Automation for 5G – phase 3
Study on Security Enhancement of support for Edge Computing — phase 2
Study on Personal IoT Networks Security Aspects
Study on SNAAPP security
Study on enhanced security for network slicing Phase 3
Study on Security aspects for 5WWC Phase 2

Rel-18 Studies and normative work

Study on the security aspects of Artificial Intelligence (AI)/Machine Learning (ML) for the NG-RAN
Study on security support for Next Generation Real Time Communication services
Study on security aspects of enhanced support of Non-Public Networks phase 2
Study on Security of Phase 2 for UAS, UAV and UAM
Study to enable URSP rules to securely identify Applications
Study on Security Aspects of Ranging Based Services and Sidelink Positioning
Study on Security and Privacy of AI/ML-based Services and Applications in 5G
Study on applicability of the Zero Trust Security principles in mobile networks
Study of Security aspects on User Consent for 3GPP Services Phase 2
Study on security enhancements for 5G multicast-broadcast services Phase 2
Study on enhanced Security Aspects of the 5G Service Based Architecture
Study on Security Aspects of Satellite Access

3GPP SCAS: Roles of GSMA and 3GPP in NESAS



SA3 has defined SCAS test for all 5G NFs

Year after year security breach of enterprises get published, but there is actually no incident of cracking 3GPP authentication protocols.

Famous loot of IMSIs from the vault of SIM card vendors, but that they had to do it by stealing shows the strength of the protocol. They couldn't break the LTE AKA protocol using reasonable computing power.

Security Success of SA3

Multiple parties are attempting to break the security protocols defined by 3GPP/SA3.

Good and Bad,

Good: protocols, algorithm gets verified by multiple means.

Bad : any small gap or leakage gets published with such a euphoria that operators, general public gets alarmed.

Recent years, so many CVD papers have been submitted in GSMA and SA3, Are all the papers were worth publishing?

Big misses from SA3

Irrespective of these success, SA3 did miss on big issues.

1) Exposing the permanent Subscription identifier IMSI in LTE.

- When LTE was defined, this was not considered a critical security requirement, but subsequently it became a serious vulnerability.
- Without requirement, nothing moves in 3GPP.
- But why are the regulatory bodies silent, why don't they prohibit exposure of IMSI in the network?
- It is not too late to fix this if there is a collective will !

2) Lack of PWS security.

Time and again, in different countries the issue of the lack of PWS security pops up. SA3 did a study and the solutions in TR 33.968 were not agreed because of the lack of regulations.

Unless multiple parties work together, good standardization doesn't happen resulting in strong secure networks !

Input from regulatory bodies: Always necessary ! Are current mechanisms sufficient?

NOKIA

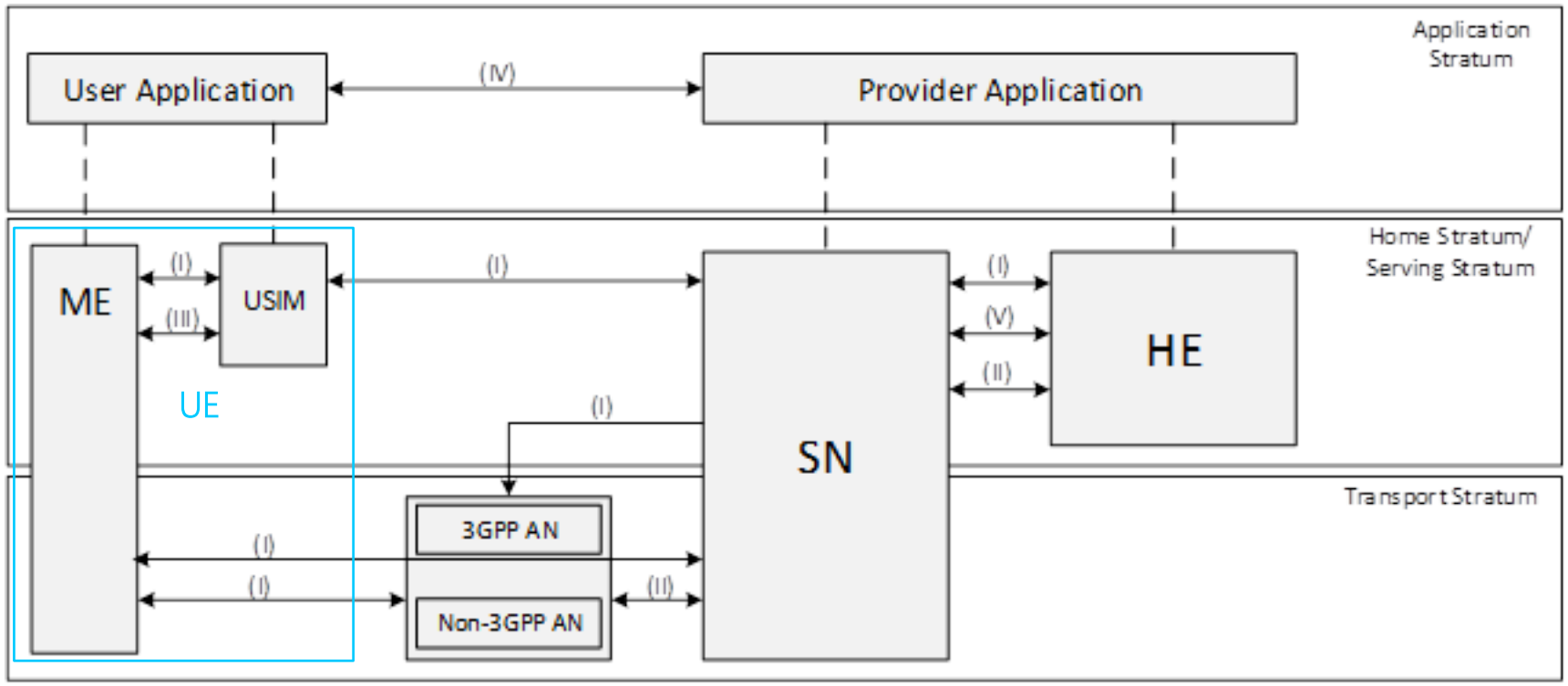
NOKIA Bell Labs

Thanks for your attention!

10
4 © Nokia Solutions and Networks 2020 For internal use

NOKIA

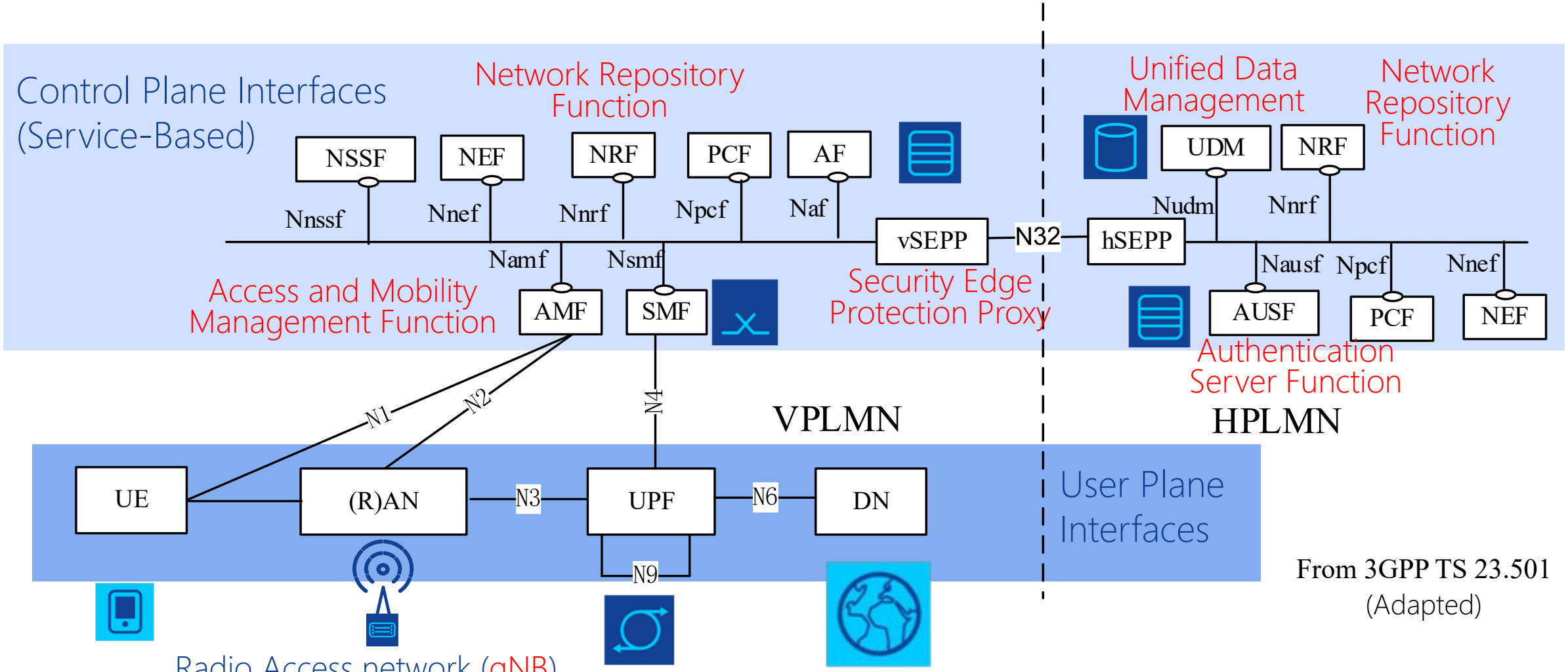
Security Architecture
(Adapted from 3GPP TS 33.501)



AN	Access Network
HE	Home Environment
ME	Mobile Equipment
SBA	Service Based Architecture
SN	Serving Network
USIM	Universal Subscriber Identity Module
UE	User Equipment

(I) Network access security
(II) Network domain security
(III) User domain security
(IV) Application domain security
(V) SBA domain security
(VI) Visibility and configurability of security (not shown in the figure)

Crucial Security Functions in the 3GPP 5G System

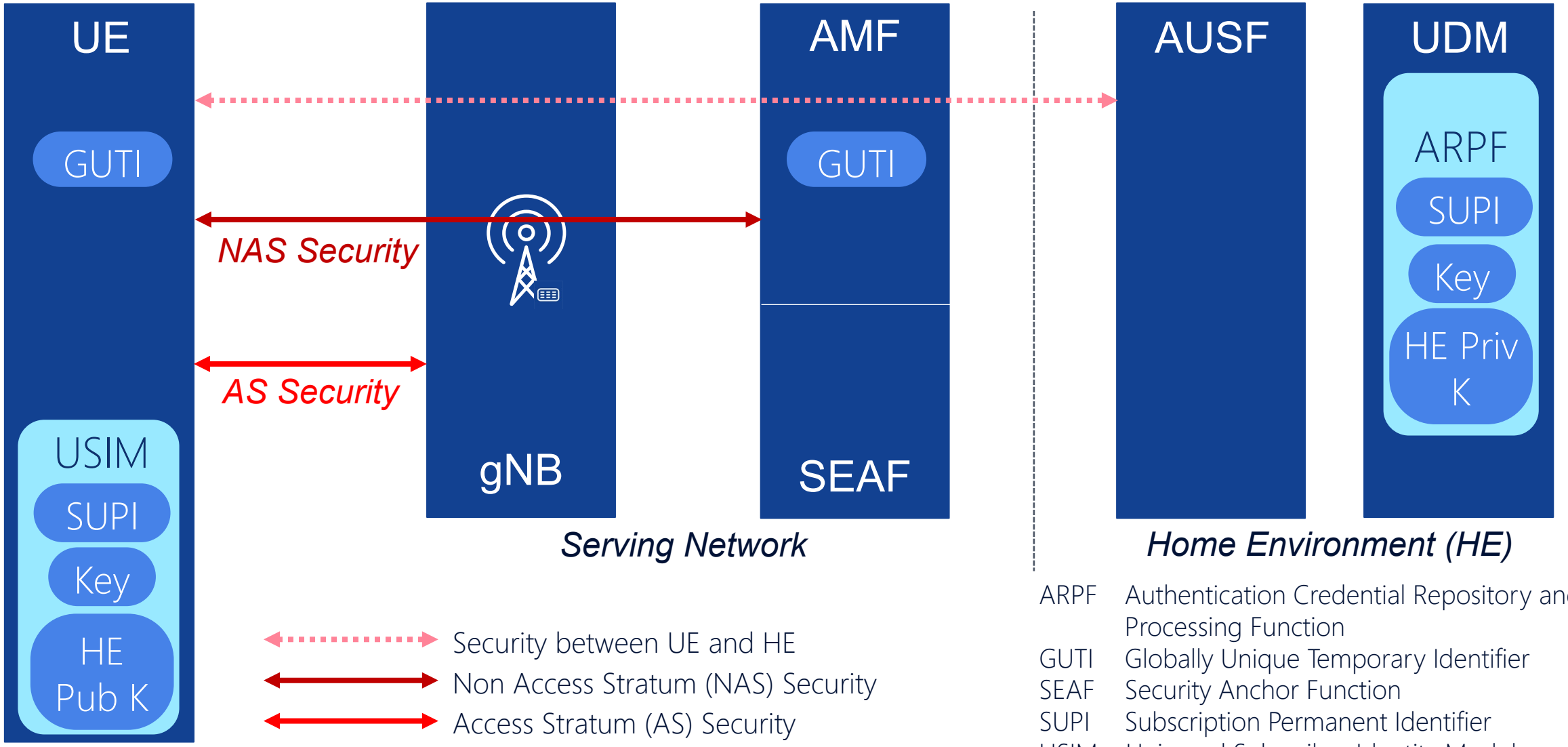


From 3GPP TS 23.501 (Adapted)

Red: Functions crucial for the security architecture

V/HPLMN Visited/Home Public Land Mobile Network

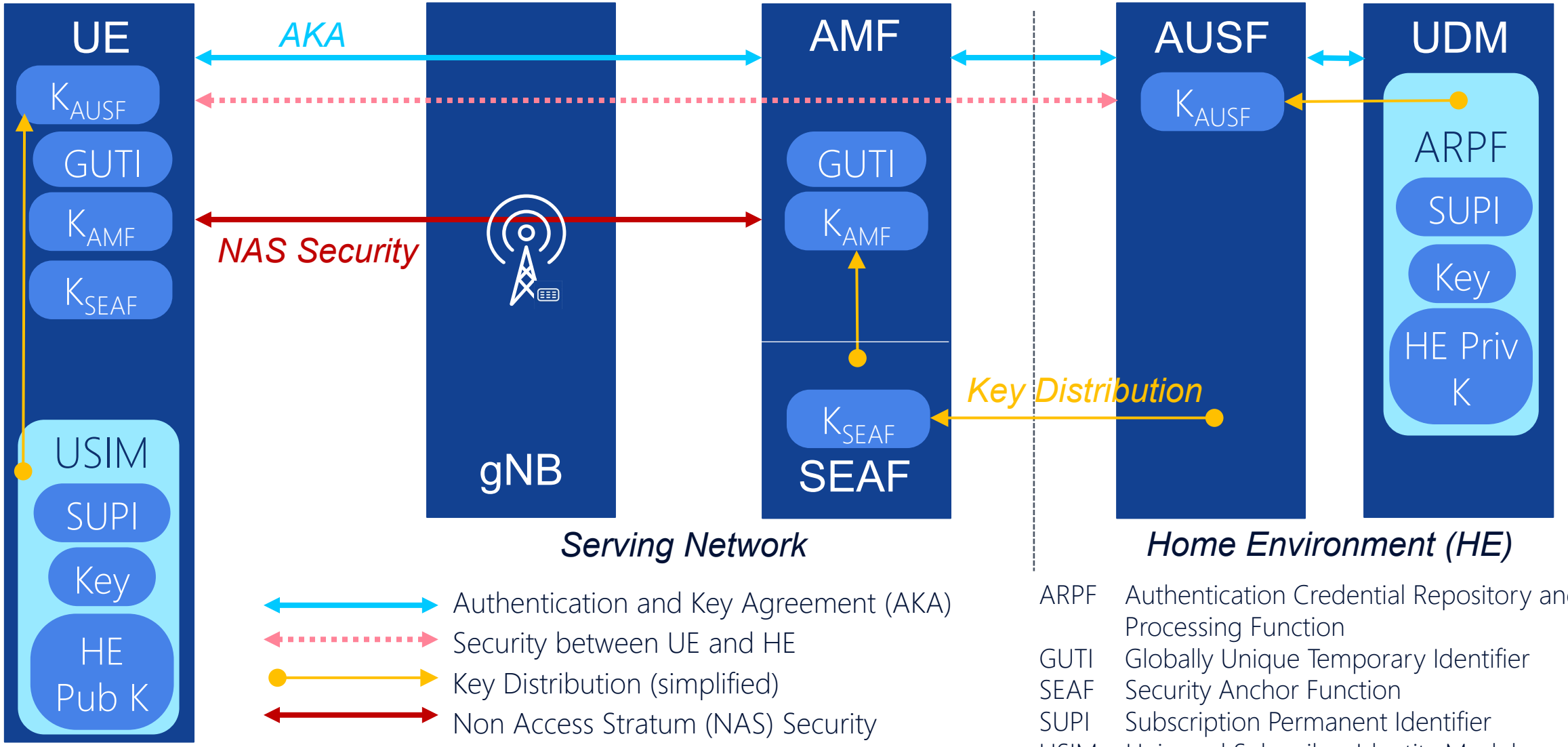
Network Access Security: Security Associations of a Connected UE



ARPF	Authentication Credential Repository and Processing Function
GUTI	Globally Unique Temporary Identifier
SEAF	Security Anchor Function
SUPI	Subscription Permanent Identifier
USIM	Universal Subscriber Identity Module

NOKIA

Network Access Security: AKA and NAS Security



Authentication and Key Agreement (AKA)
Security between UE and HE
Key Distribution (simplified)
Non Access Stratum (NAS) Security

ARPF	Authentication Credential Repository and Processing Function
GUTI	Globally Unique Temporary Identifier
SEAF	Security Anchor Function
SUPI	Subscription Permanent Identifier
USIM	Universal Subscriber Identity Module

NOKIA