NOKIA Bell Labs

Tutorial

5G Mobile Network Security Essentials

1st ITG Workshop on IT Security (ITSec)

Eberhard Karls Universität Tübingen, 3.4.2020

Peter Schneider, Nokia Bell Labs Security Research

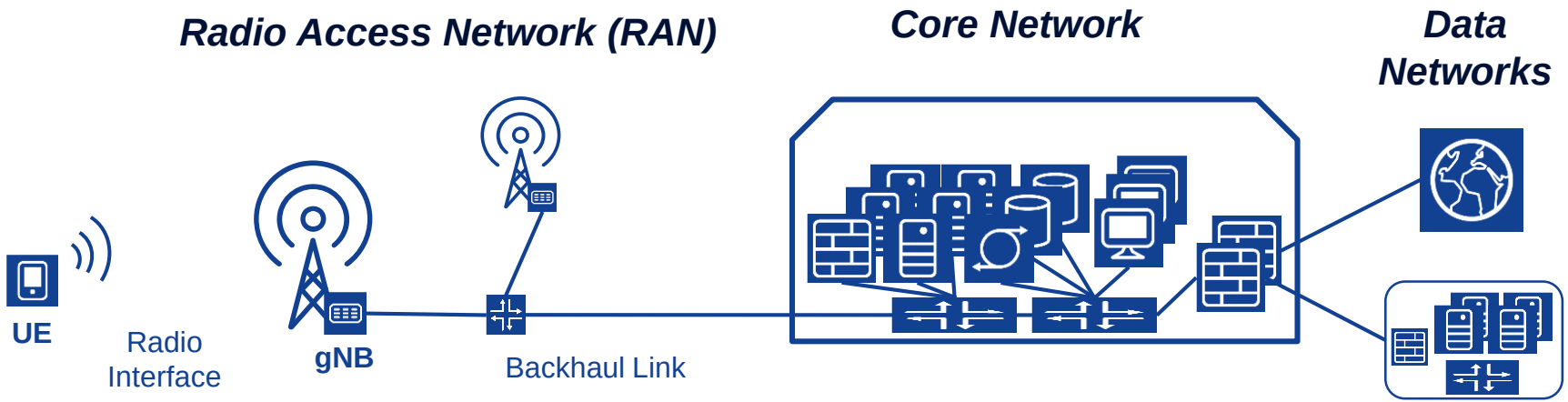
Contents

- The 5G System
- 3GPP 5G security specification
- Overall security architecture
- Network access security
  - Protecting the subscriber identity
  - Authentication
  - Attacks against 5G AKA (Authentication and Key Agreement)
  - Non Access Stratum (NAS) security setup
  - Access Stratum (AS) security setup
  - Key hierarchy
  - Encryption and Integrity Protection
  - Attacks against AS security
- Network domain security
  - Non-service-based interfaces
  - Service-based interfaces
  - Interconnection security
- How 5G Security covers known 4G Security issues
- Holistic 5G Security approach

NOKIA Bell Labs

Introduction: The 5G System

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

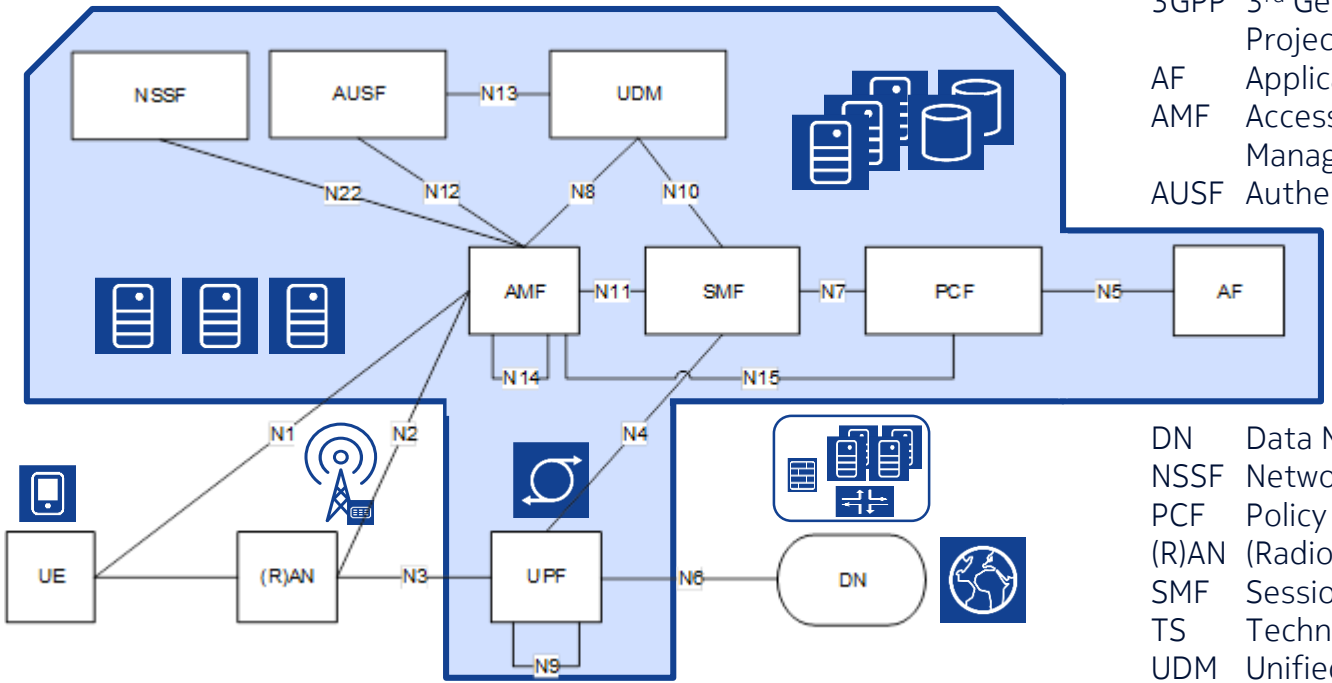
Examples:

- **The Internet**
- **Industrial IoT networks**
- **Enterprise networks**

NOKIA Bell Labs

“Non-Roaming 5G System Architecture in reference point representation”

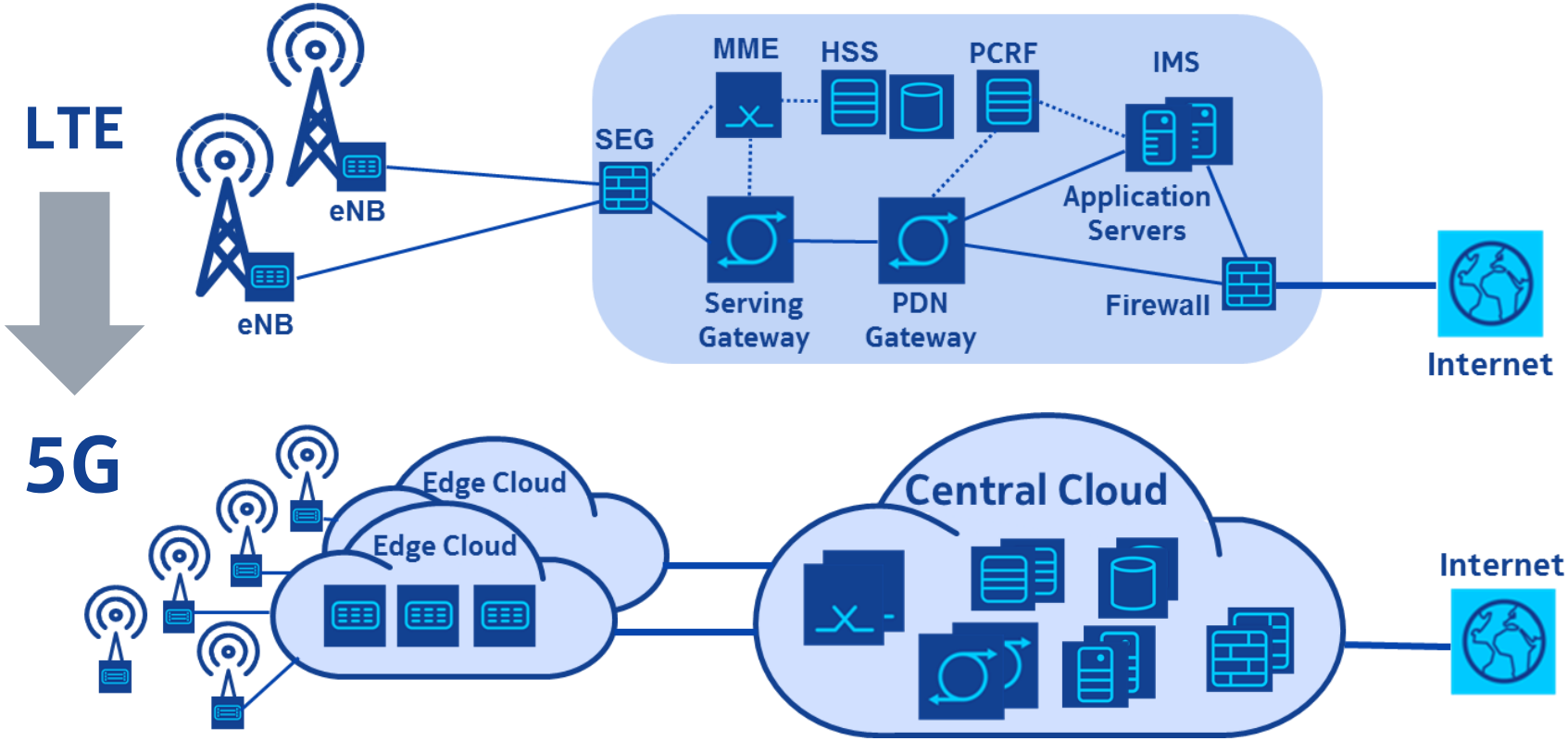
(Adapted from 3GPP TS 23.501 Rel.15)



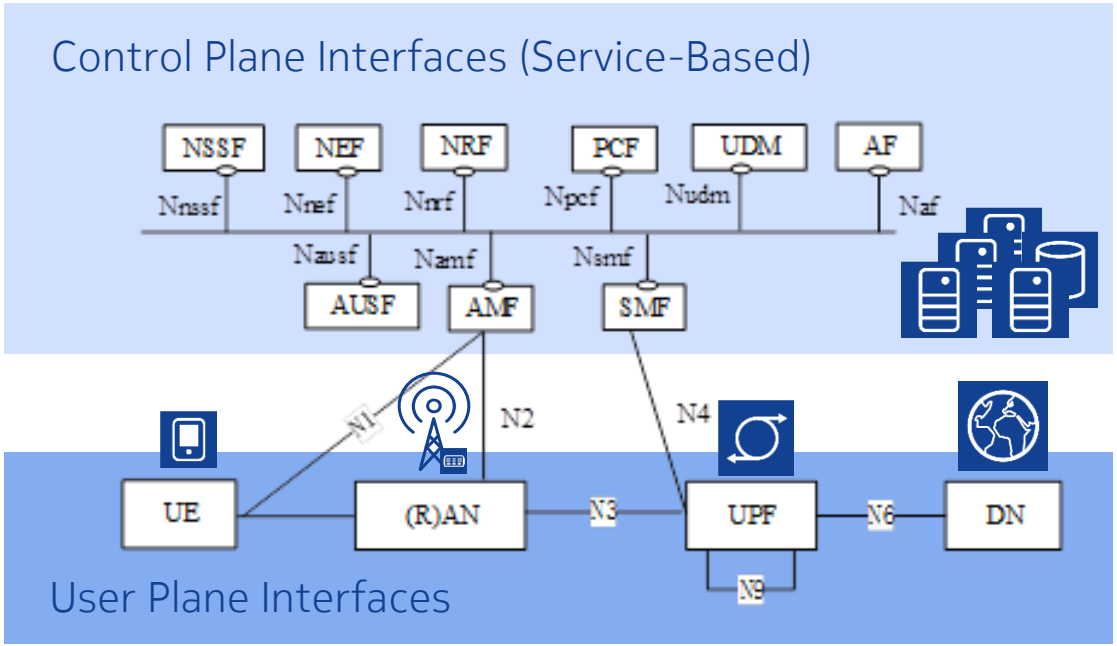
Reference Points N1, N2, N3, …

3GPP	3rd Generation Partnership Project
AF	Application Function
AMF	Access and Mobility Management Function
AUSF	Authentication Server Function
DN	Data Network
NSSF	Network Slice Selection Function
PCF	Policy Control Function
(R)AN	(Radio) Access Network
SMF	Session Management Function
TS	Technical Specification
UDM	Unified Data Management
UE	User Equipment
UPF	User Plane Function

From LTE to 5G: Adopting New Networking Paradigms

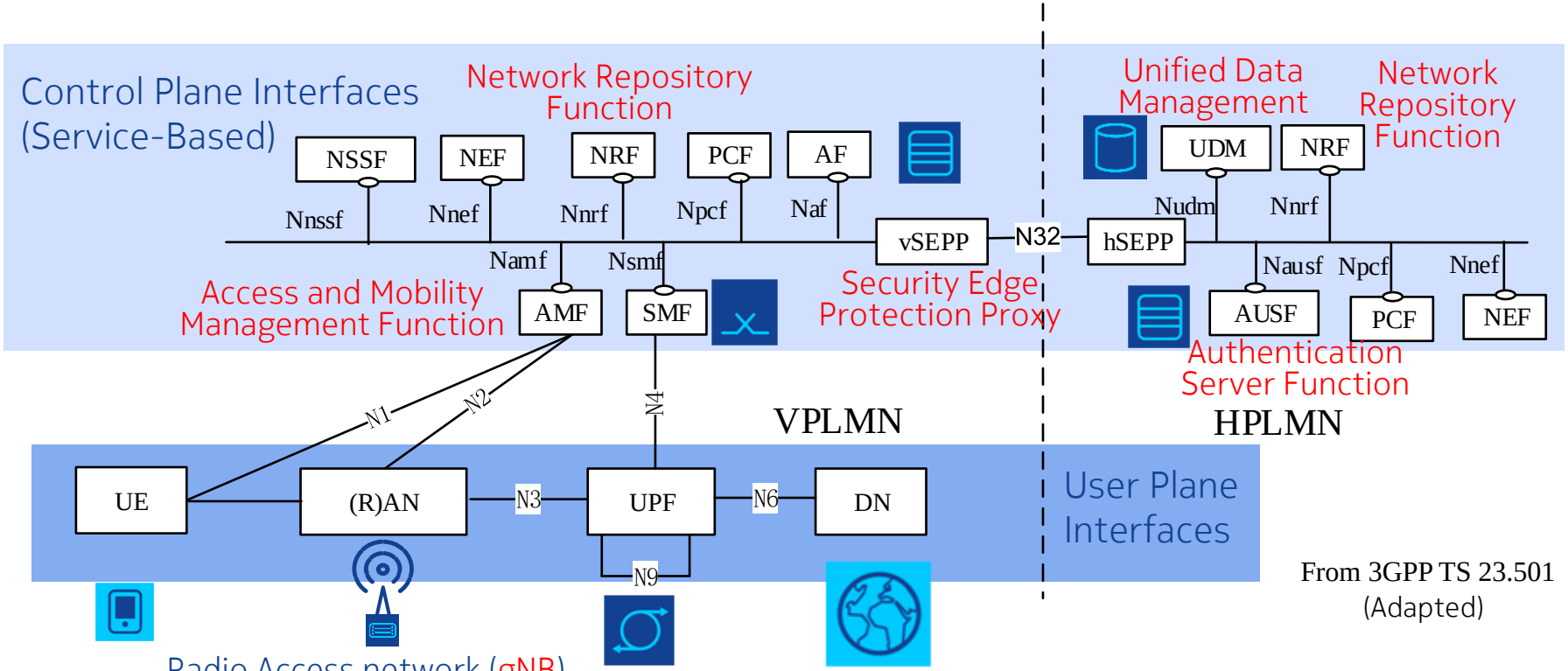


“Non-Roaming 5G System Architecture”
(Adapted from 3GPP TS 23.501 Rel.15)



AF	Application Function
AMF	Access and Mobility Management Function
AUSF	Authentication Server Function
DN	Data Network
NEF	Network Exposure Function
NRF	Network Repository Function
NSSF	Network Slice Selection Function
PCF	Policy Control Function
(R)AN	(Radio) Access Network
SMF	Session Management Function
UDM	Unified Data Management
UE	User Equipment
UPF	User Plane Function

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

NOKIA Bell Labs

NOKIA Bell Labs

3GPP 5G Security Specification

3GPP Specifications

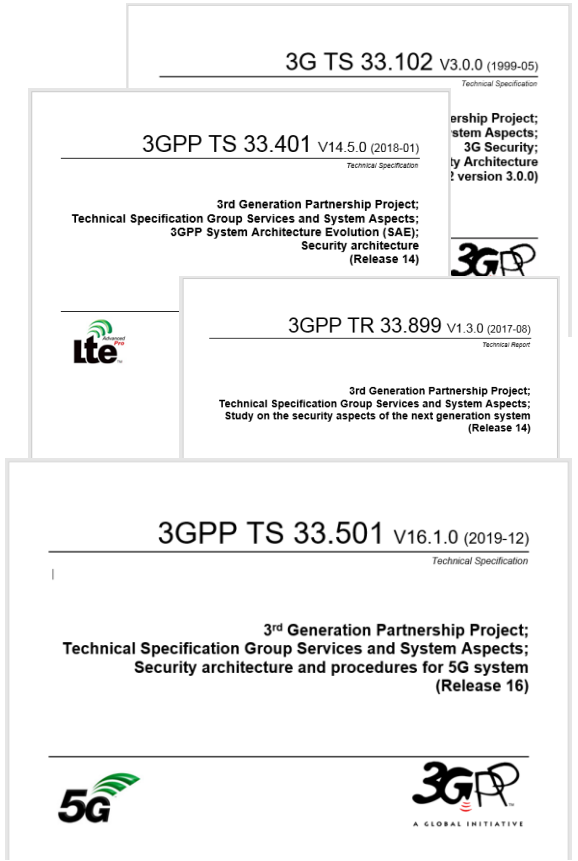
- All 3GPP specifications are publicly available on www.3gpp.org
- Specification overview: https://www.3gpp.org/specifications/specification-numbering
- Specifications are grouped into “series”, e.g. the “33-series” for security related specifications (https://www.3gpp.org/DynaReport/33-series.htm)
- Overall Architecture: TS 23.501, “System Architecture for the 5G System”
- 5G RAN overview: TS 38.300 “NR and NG-RAN Overall Description”
- A Technical Specification (TS) is a normative document, in contrast to a Technical Report (TR) that captures study results and sometimes recommendations for the normative work

3GPP 5G Security Specifications

3GPP Technical Specification 33.501, Release15 + “Security architecture and procedures for 5G system”

(http://www.3gpp.org/ftp//Specs/archive/33_series/33.501/33501-g10.zip)

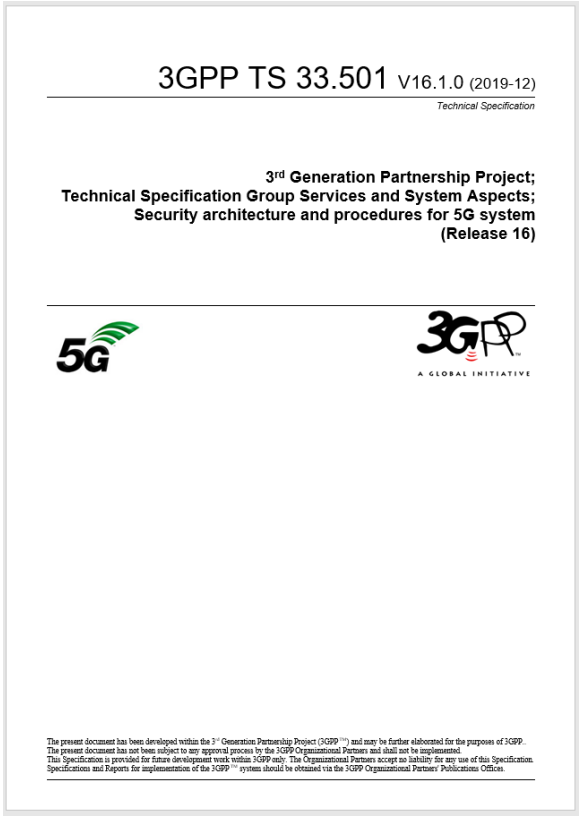
- Security Assurance Specs (TS 33.511 – TS 33.519)
- Dedicated documents for specific topics, e.g.
  TS 33.536, Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services
- A lot of earlier 33-series specifications are referred to in TS 33.501, e.g. TS 33.102 (3G Sec) , TS 33.210 (NDS/IP), TS 33.401 (4G Spec)
- Security Algorithms: “35-series”
- Various other specifications describe the exact content and format of security related messages and information elements, e.g.
  - TS 24.501, Non-Access-Stratum (NAS) protocol for 5G System (5GS)
  - TS 38.323, Packet Data Convergence Protocol (PDCP) specification
  - TS 38.331, Radio Resource Control (RRC) protocol specification



NOKIA Bell Labs

3GPP TS 33.501 Security Specification – Main Chapters

4	Overview of security architecture
5	Security requirements and features
6	Security procedures between UE and 5G network functions
7	Security for non-3GPP access to the 5G core network
8	Security of interworking
9	Security procedures for non-service based interfaces
10	Security aspects of IMS emergency session handling
11	Security procedures between UE and external data networks via the 5G Network
12	Security aspects of Network Exposure Function (NEF)
13	Service Based Interfaces (SBI) Includes “Interconnection Security”
14	Security related services
15	Management security for network slices


3GPP TS 33.501 V16.1.0 (2019-12)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Security architecture and procedures for 5G system
(Release 16)

5G

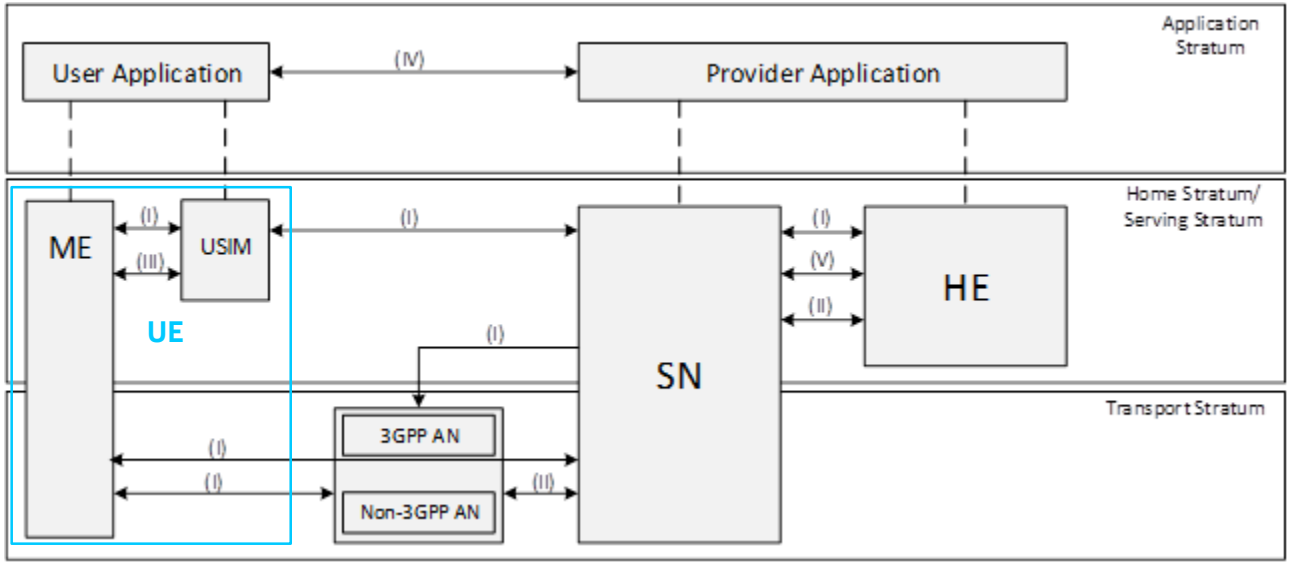
3GPP
A GLOBAL INITIATIVE

The present document has been developed within the 3rd Generation Partnership Project (3GPP ™) and may be further elaborated for the purposes of 3GPP..
The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and Reports for implementation of the 3GPP ™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

3GPP 5G Security Specification TS 33.501 v16.1.0 – Annexes

Annex A (normative):	Key Derivation Functions
Annex B (informative):	Additional EAP methods for primary authentication
Annex C (normative):	Protection schemes for concealing the subscription permanent identifier
Annex D (normative):	Algorithms for ciphering and integrity protection
Annex E (informative):	UE-assisted network-based detection of false base station
Annex F (normative):	3GPP 5G profile for EAP-AKA‘
Annex G (informative):	Application layer security on the N32 interface
Annex I (normative):	Non-public networks
Annex J (normative):	SRVCC from 5G to UTRAN
Annex K (normative):	Security for 5GLAN services
Annex L (normative):	Security for TSC service

Security Architecture
(Adapted from 3GPP TS 33.501)



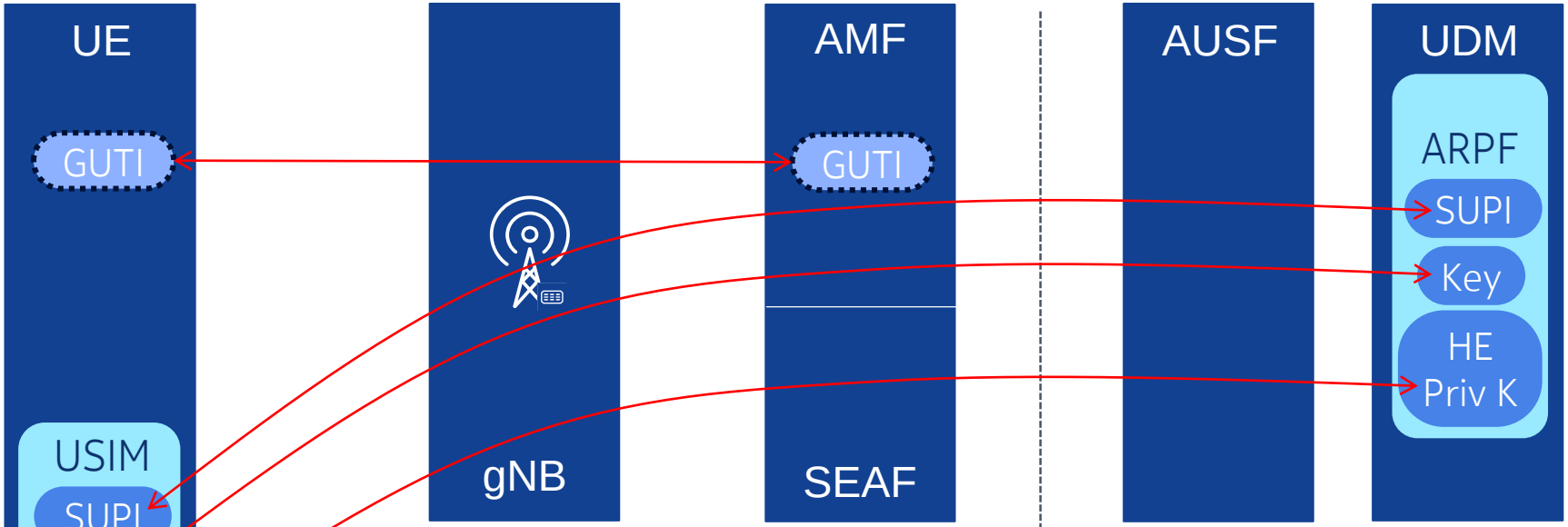
AN	Access Network
HE	Home Environment
ME	Mobile Equipment
SBA	Service Based Architecture
SN	Serving Network
USIM	Universal Subscriber Identity Module
UE	User Equipment

(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)

NOKIA Bell Labs

Network Access Security General

Entities Involved in Network Access Security (3GPP Access)



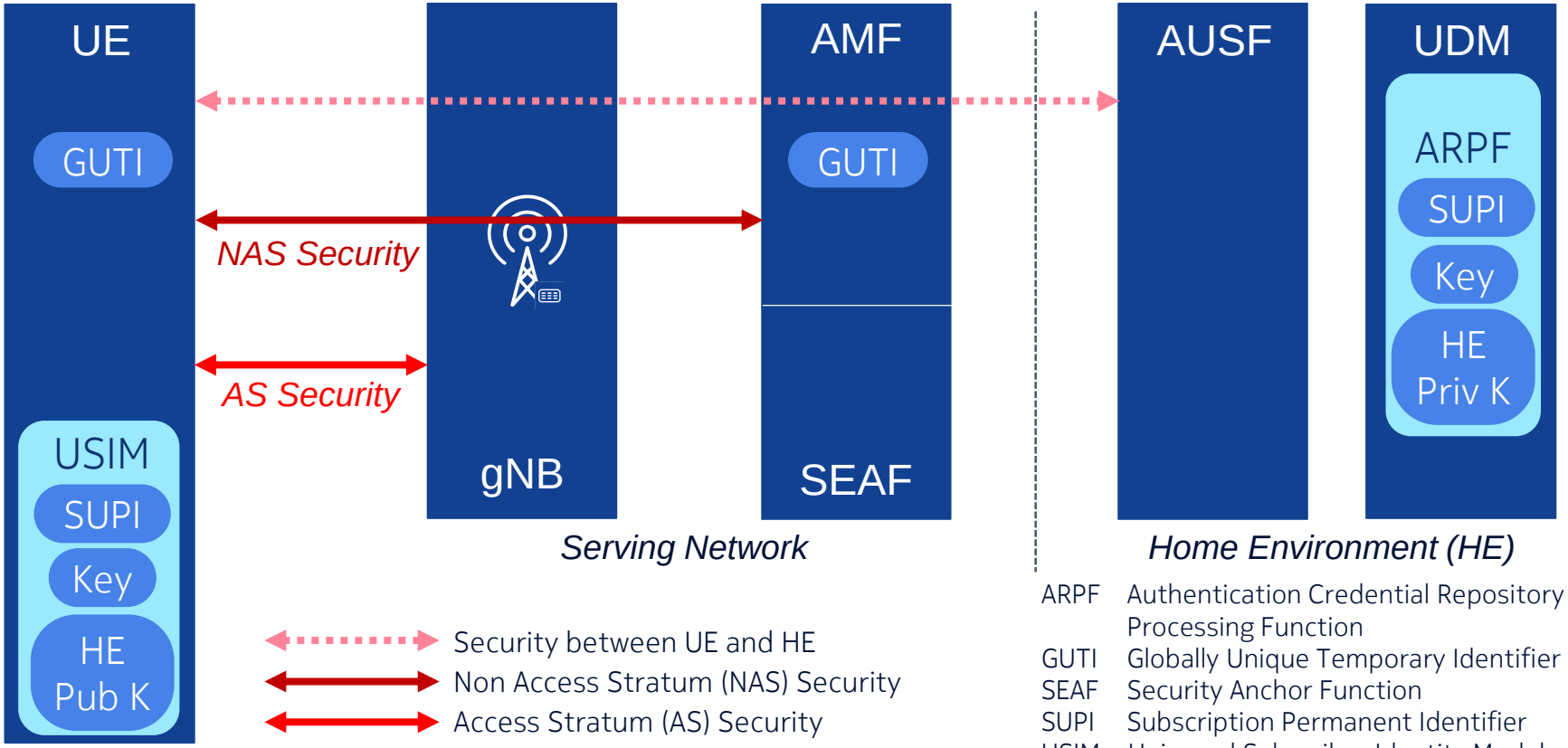
Serving Network

Home Environment (HE)

AMF	Access and Mobility Management Function
AUSF	Authentication Server Function
UDM	Unified Data Management
UE	User Equipment

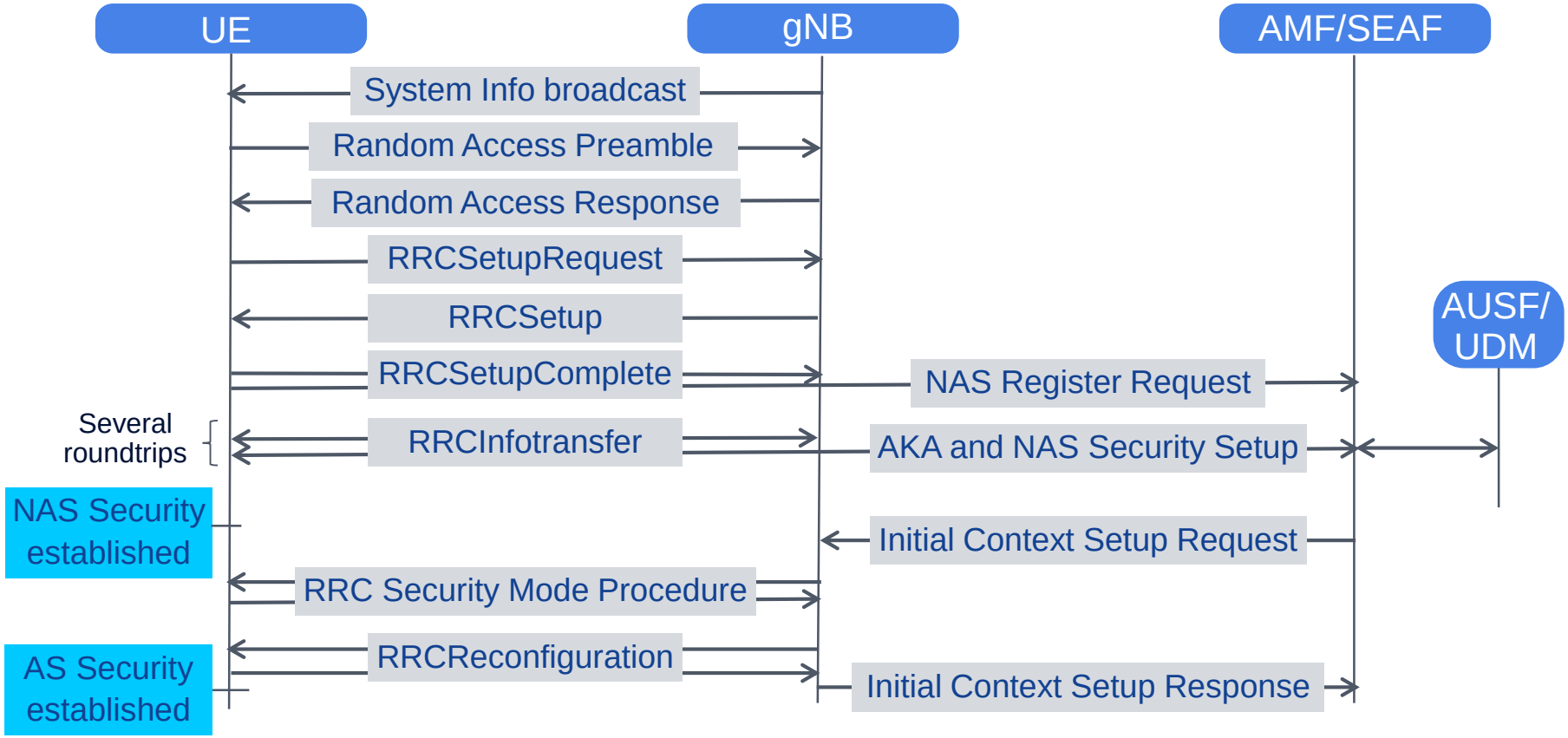
ARPF	Authentication Credential Repository and Processing Function
GUTI	Globally Unique Temporary Identifier
SEAF	Security Anchor Function
SUPI	Subscription Permanent Identifier
USIM	Universal Subscriber Identity Module

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

Network Access, Authentication and Key Agreement (AKA), Security Setup



RRC Radio Resource Control

NOKIA Bell Labs

NOKIA Bell Labs

Network Access Security
Protecting the Subscriber Identity

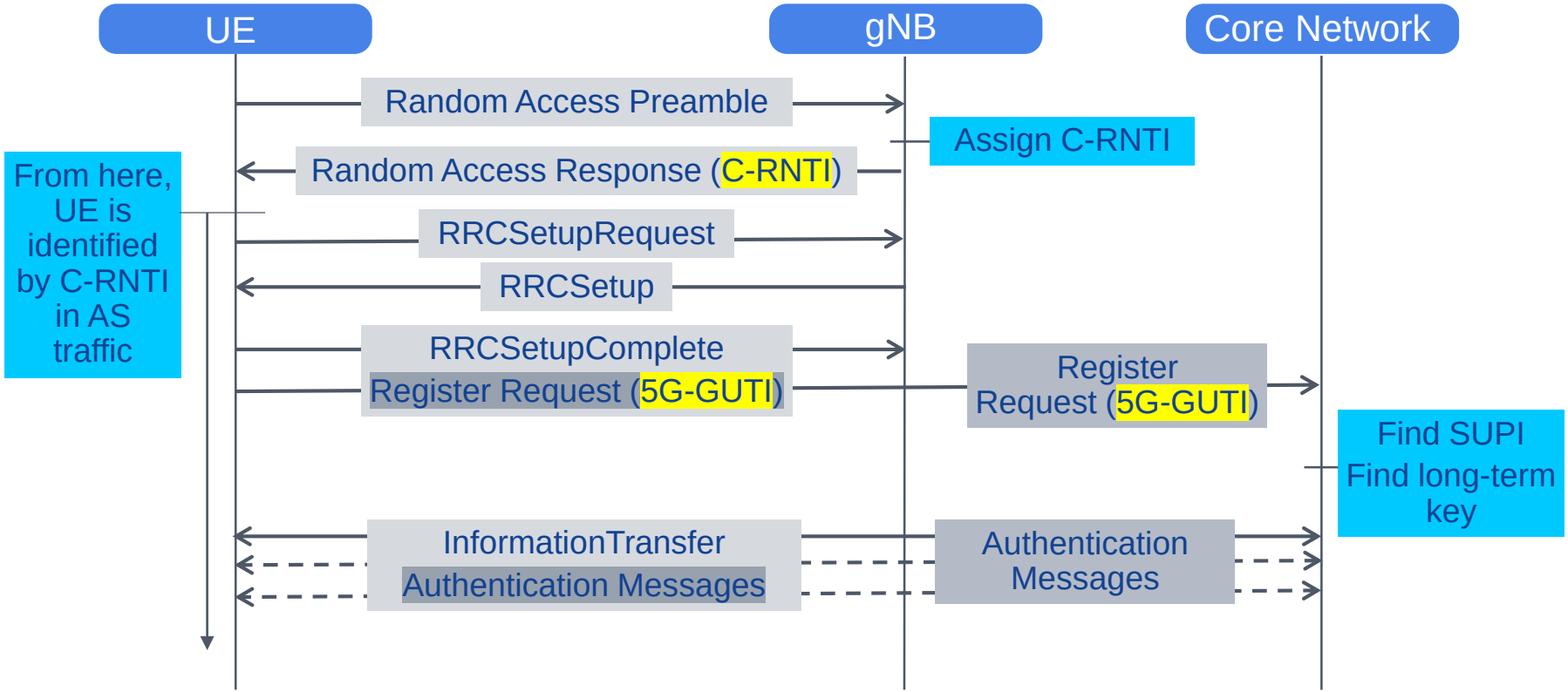
Identifying Mobile Subscribers / UEs: SUPI, GUTI, SUCI, C-RNTI

- Public Identifiers (e.g. phone number) to allow communication between subscribers
- Network internal permanent identifiers to allow the network to identify subscriptions and retrieve subscription data, including authentication credentials:
  → **SUPI (Subscription Permanent Identifier)**
- Permanent identifiers cannot be used in the clear over the radio interface:
  - Attackers could track UEs by listening to the radio interface in one or more cells
  - Even if a non-public permanent identifier was used, an attacker may find means to associate the non-public identifier with a public identifier (and a human)

➢ Frequently changing temporary identifiers are used between UE and core network:
  → **5G-GUTI (Globally Unique Temporary Identifier)**
  Short form of 5G-GUTI: **5G-S-TMSI (Short Temporary Mobile Subscription Id)**

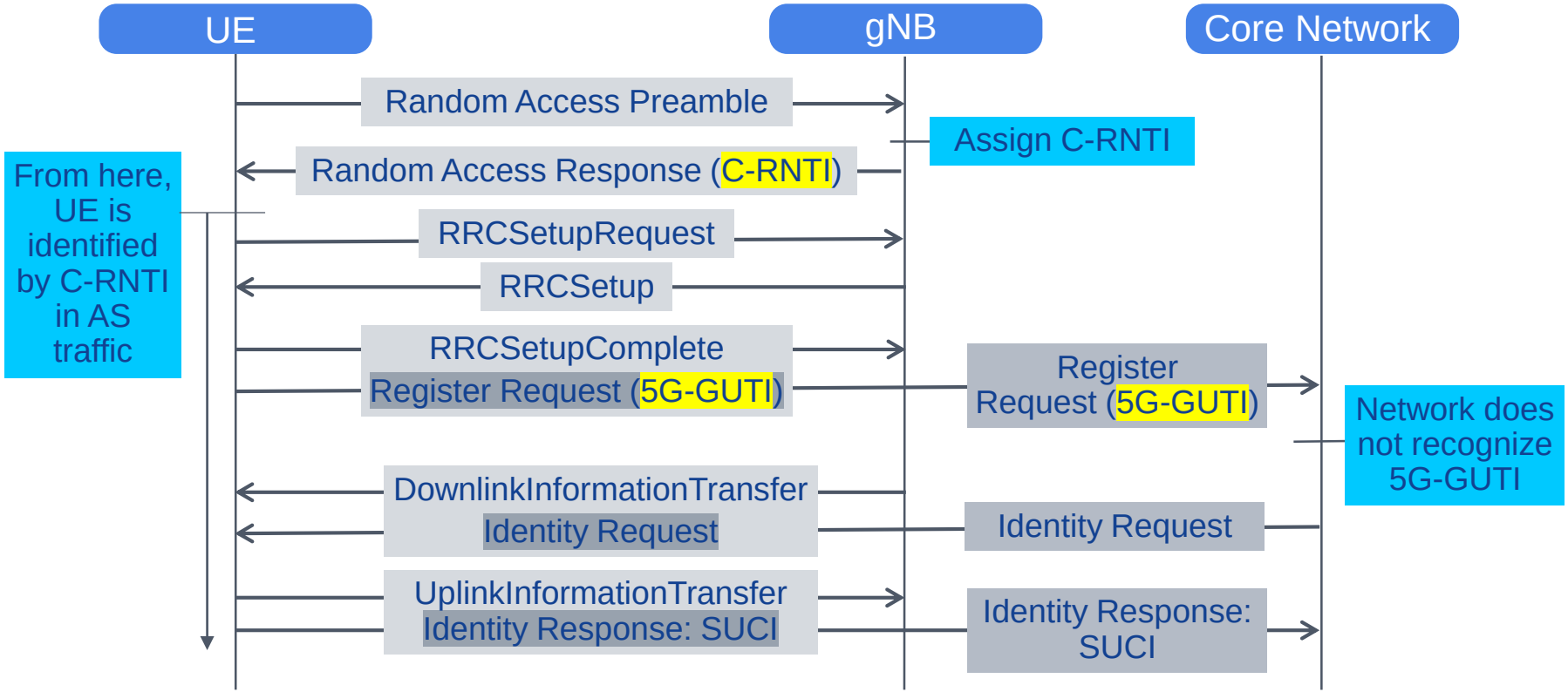
- There is a specific scheme to encrypt a SUPI
  → **SUCI (Subscription Concealed Identifier)** – see below for details
- Between UE and base station, there is an additional temporary identifier valid for the time the UE remains in a cell, the **C-RNTI (Cell Radio Temporary Identity)**

Network Access: Registration with Valid 5G-GUTI



NOKIA Bell Labs

Network Access: Registration with 5G-GUTI, Identity Request



Subscriber Privacy: Subscription Identifiers in LTE and 5G

LTE Subscription Identifiers

IMSI: International Mobile Subscriber Identity

GUTI: Globally Unique Temporary Identity

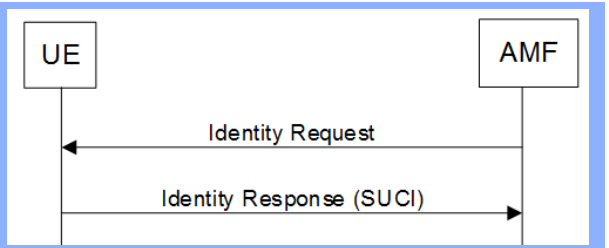
- Over the air, mostly the GUTI is used, but in some cases also the IMSI
- IMSI catching is possible: A fake base station can make the UE reveal its IMSI

5G Subscription Identifiers

SUPI: Subscription Permanent Identifier

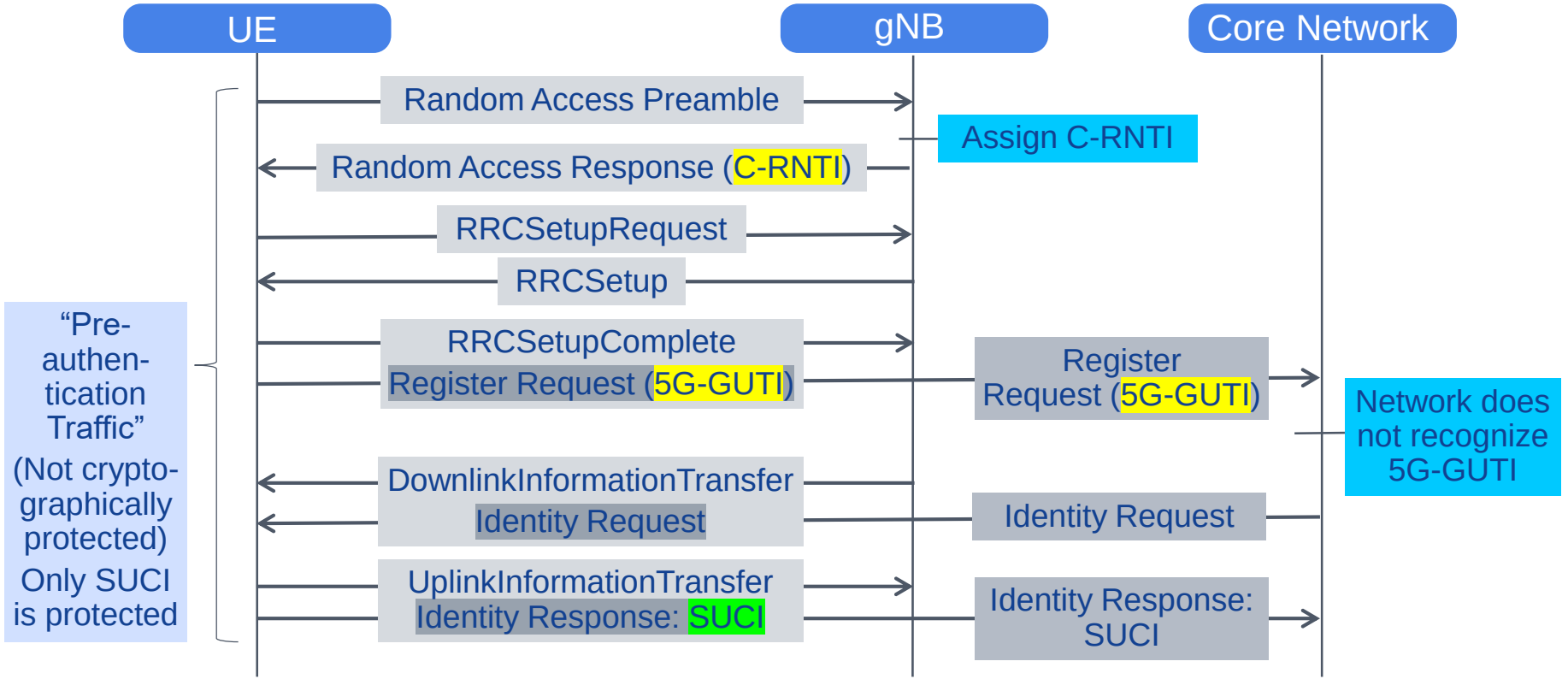
(5G-)GUTI: Globally Unique Temporary Identifier

SUCI: Subscription Concealed Identifier



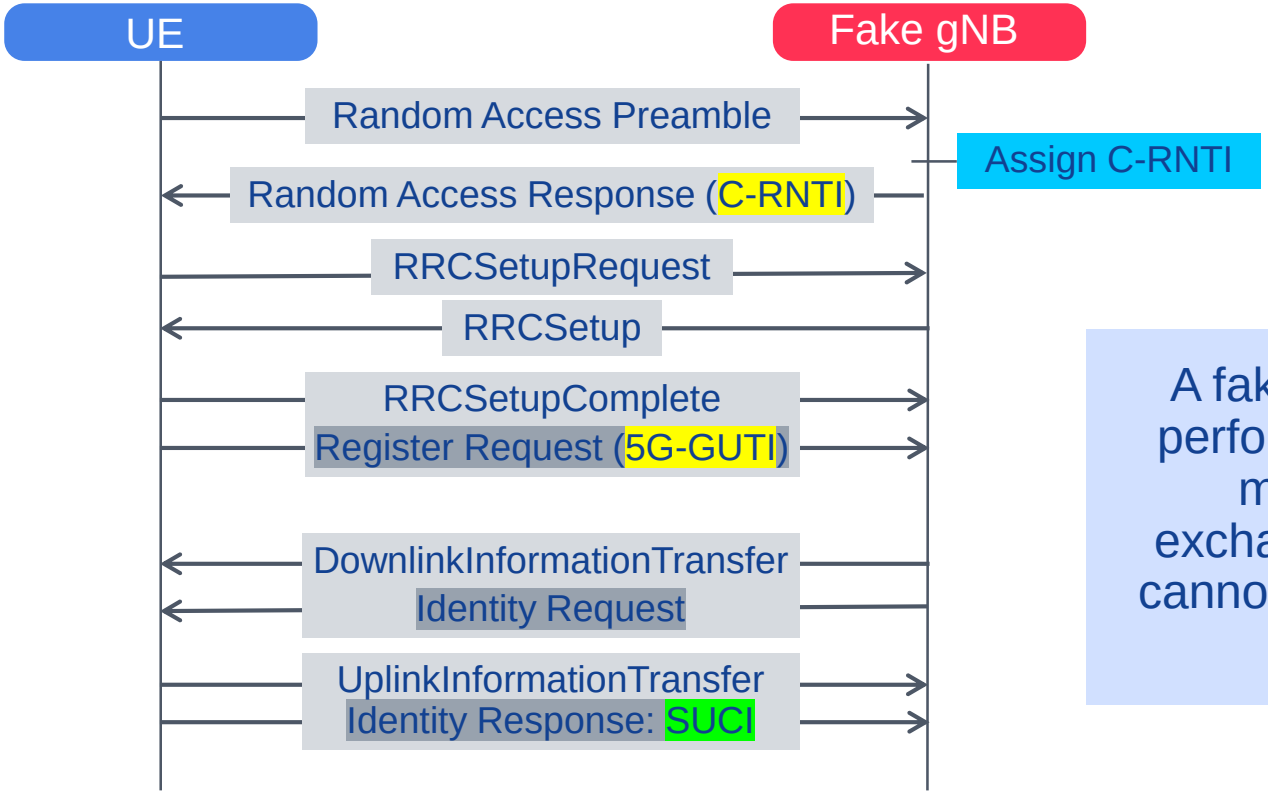
- The SUPI is never sent in the clear over the air
- Mostly the 5G-GUTI is used over the air, and in some cases the SUCI
- Stringent requirements for frequent reallocation of a new GUTI

Network Access: Registration with 5G-GUTI, Identity Request



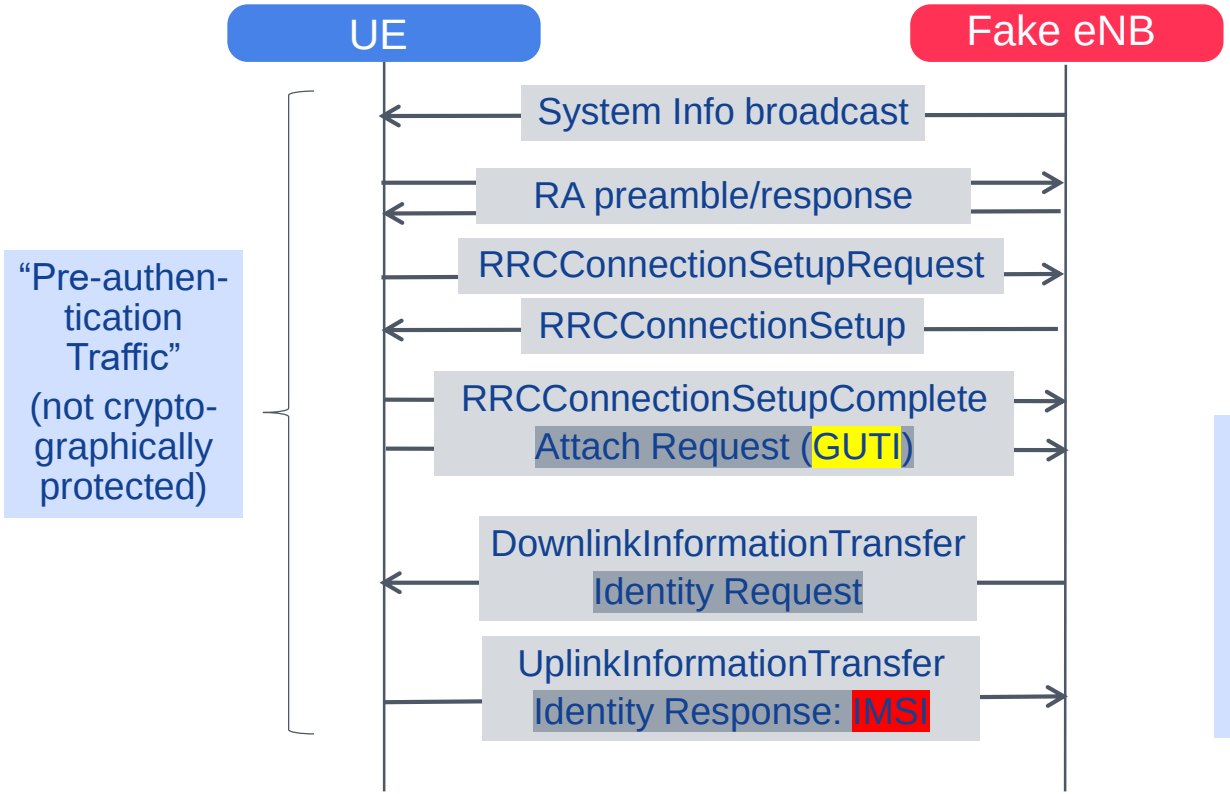
NOKIA Bell Labs

Network Access: Registration with a Fake Base Station



A fake gNB can perform all these message exchanges, but it cannot decrypt the SUCI

IMSI Catching in 4G with a Fake Base Station



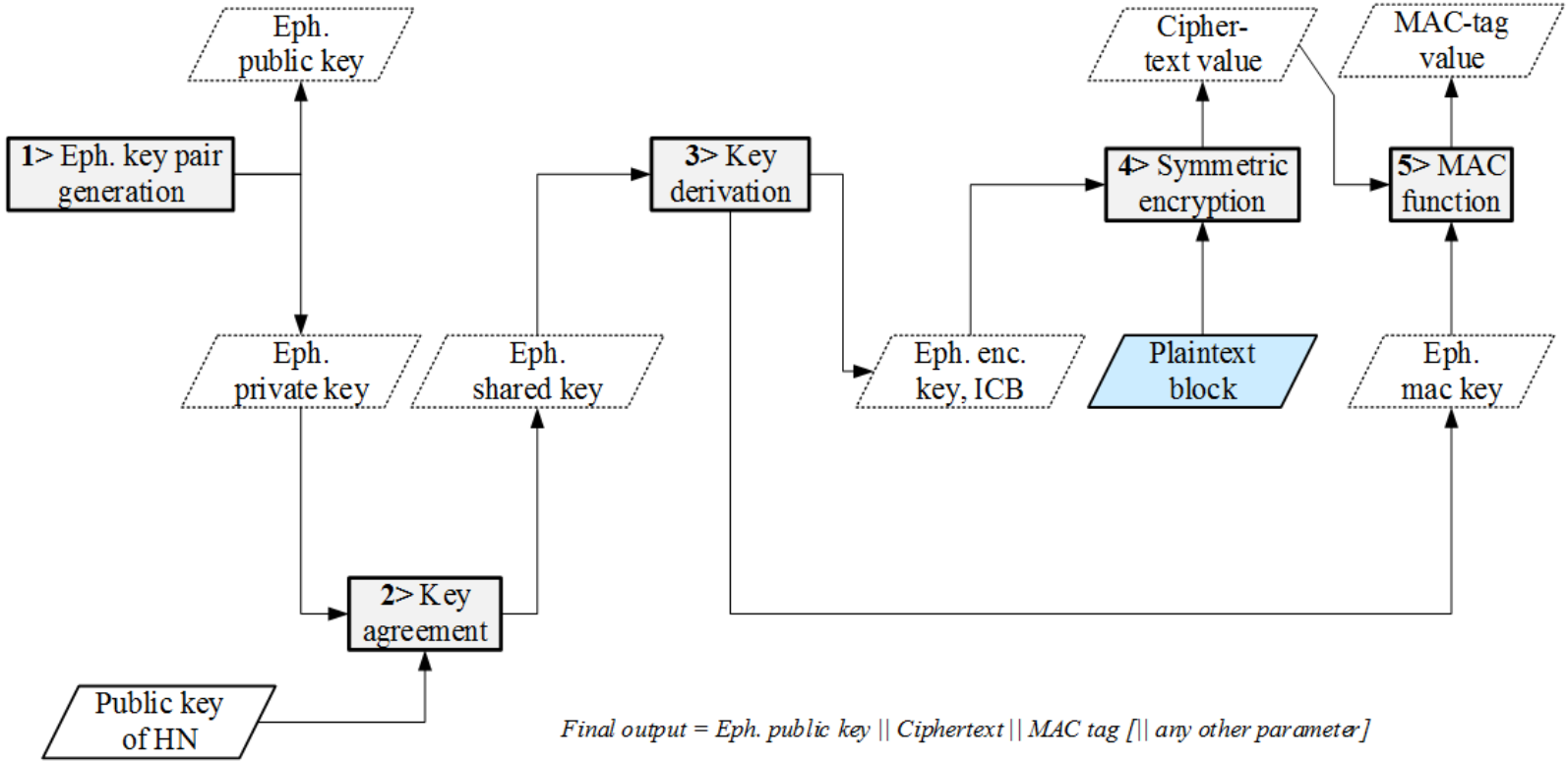
A fake 4G Base Station (eNB) can retrieve the UE’s IMSI (“IMSI catching”)

Enhanced Subscriber Privacy: The SUCI

SUCI: An encrypted form of the SUPI

- The parts of the SUPI that identify the home network are sent in the clear
- The individual parts of the SUPI are encrypted using the public key of the home network (which must be provisioned in the USIM)
- Algorithms:
  - Null scheme: No encryption
  - Elliptic Curve Integrated Encryption Scheme (ECIES) (with two profiles)
- At the UE, the algorithm may be executed in the USIM or outside of it (operator's decision)
- The Subscription Identity De-concealing Function (SIDF) in the home network decrypts the SUCI using the home network's private key

Enhanced Subscriber Privacy: SUCI Computation at the UE

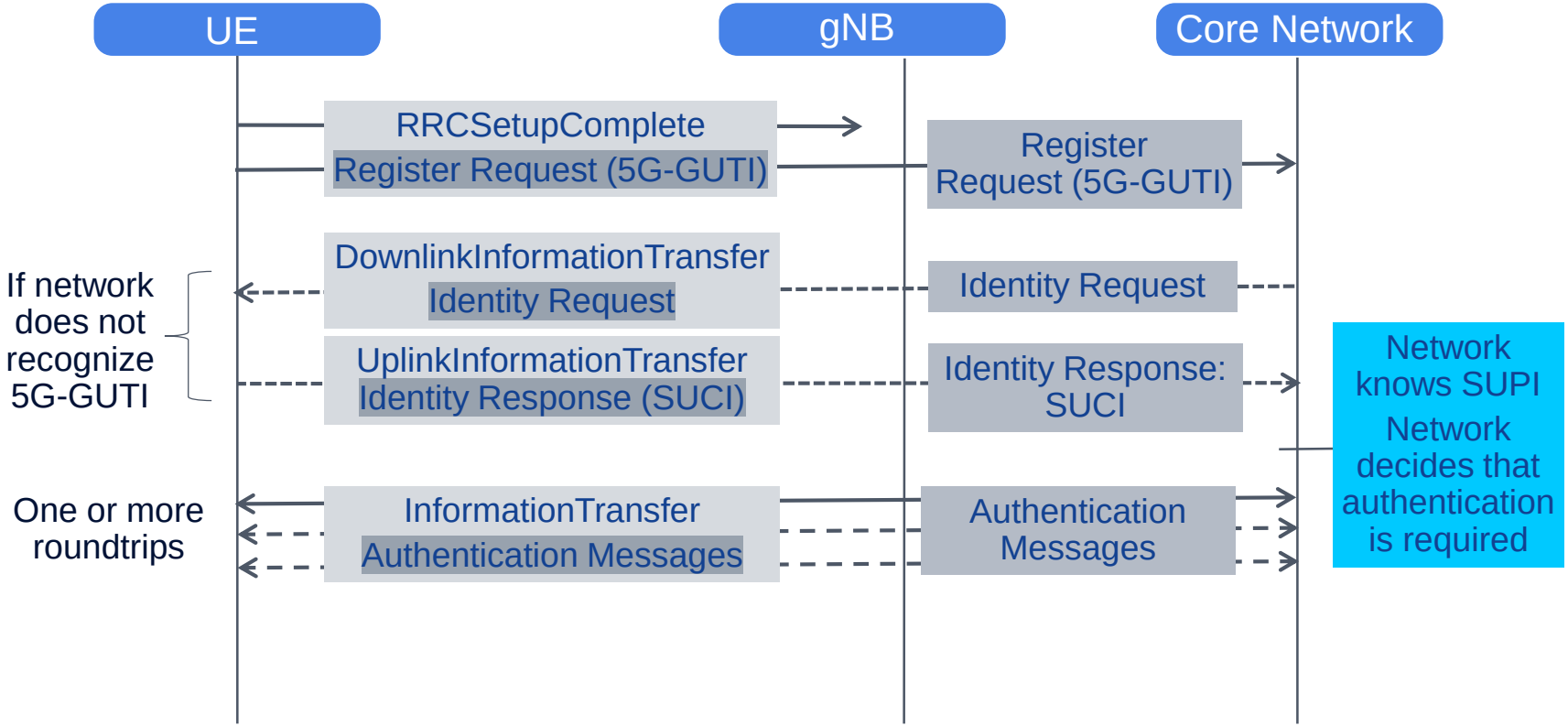


From 3GPP TS 33.501, Annex C

NOKIA Bell Labs

Network Access Security Authentication

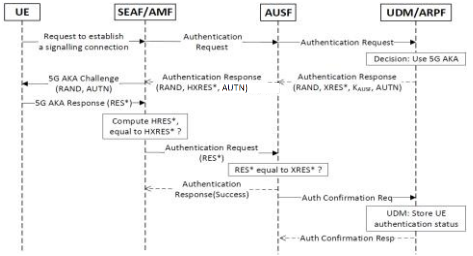
Network Access: Authentication

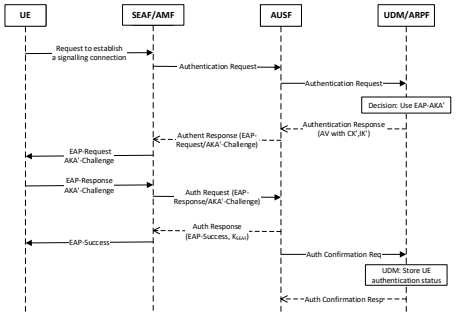


New Authentication Framework in 3GPP Release 15 (First 5G Release)

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'
- "Access agnostic": Both methods applicable for 3GPP as well as non-3GPP access
- 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)

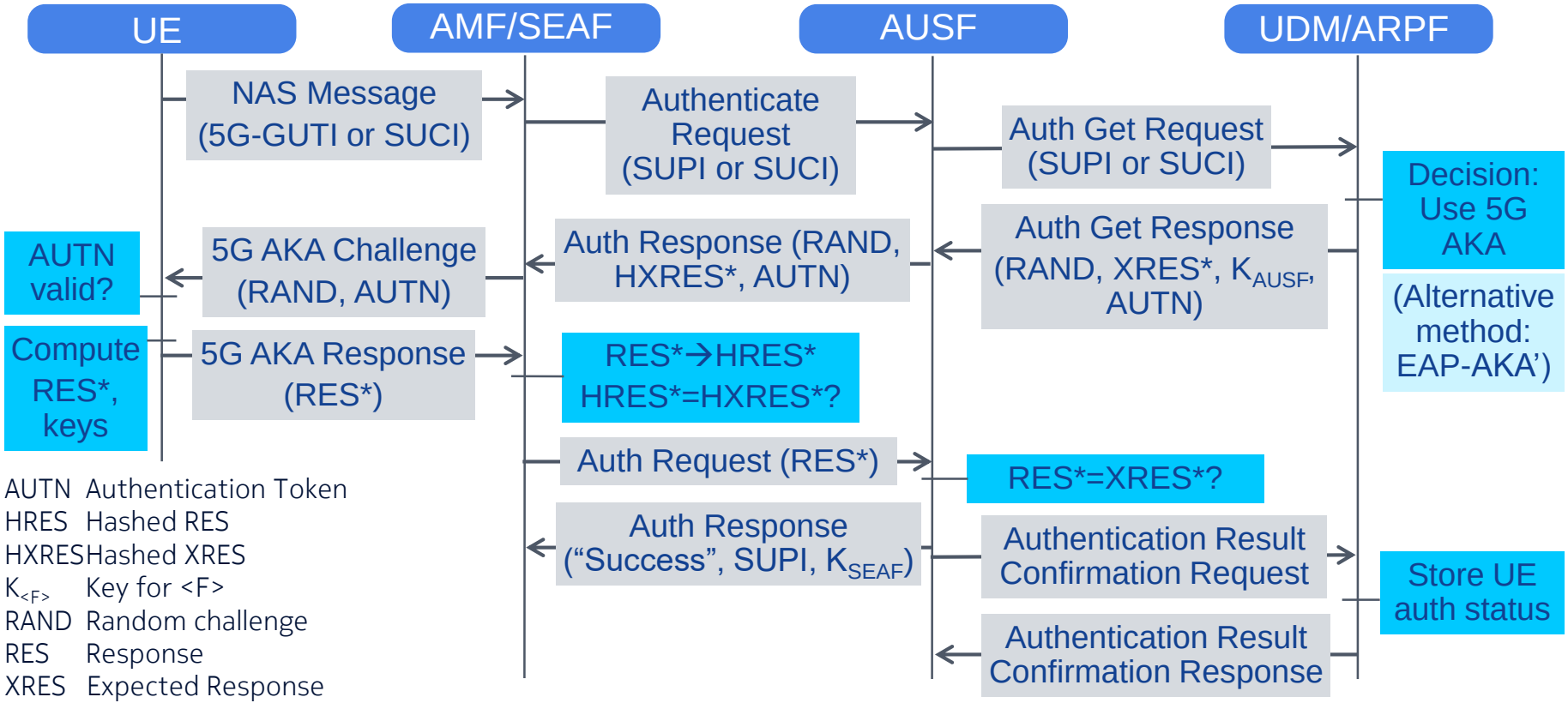




(Enlarged pictures in the following)

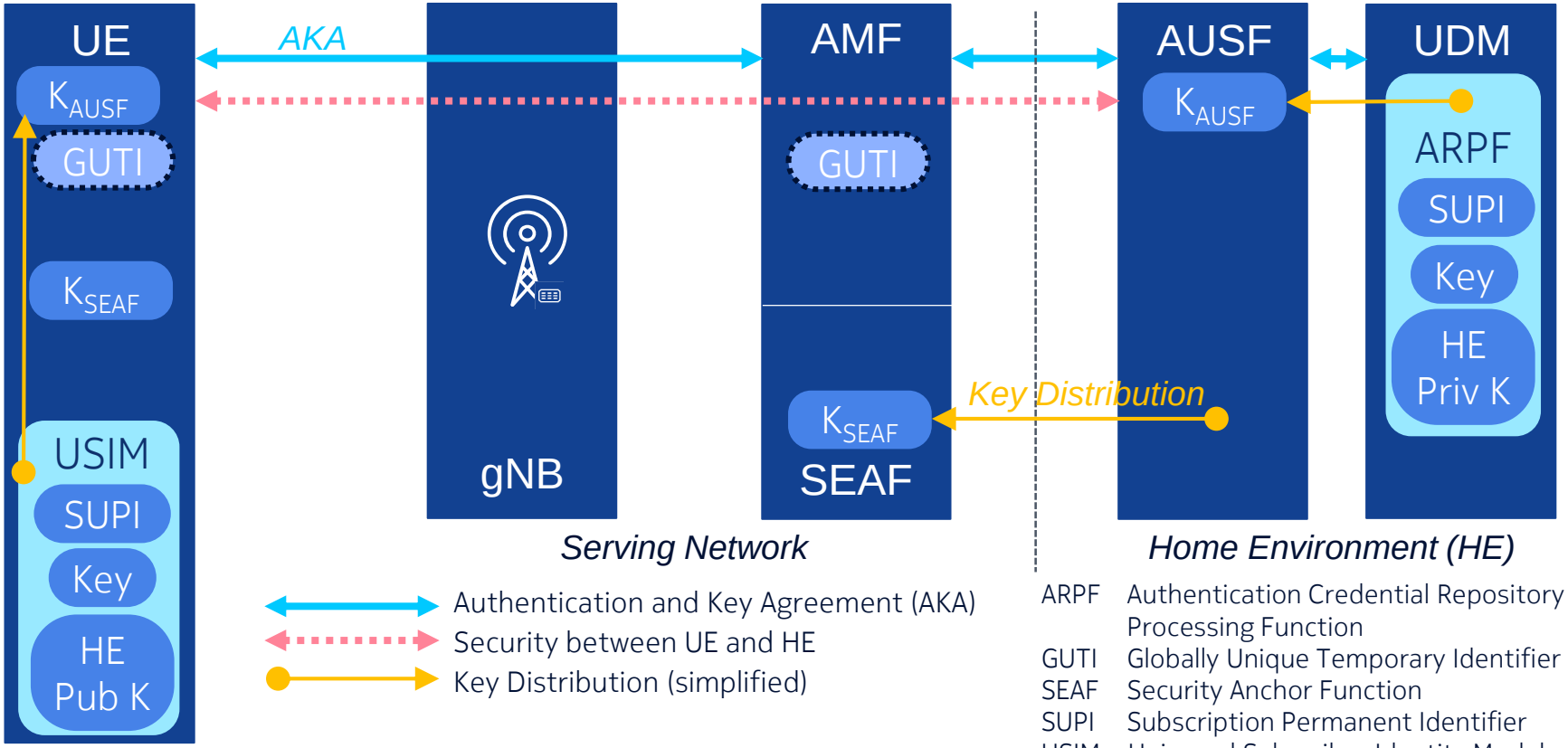
NOKIA Bell Labs

5G AKA (Authentication and Key Agreement) (informative view, success case)



AUTN Authentication Token
HRES Hashed RES
HXRES Hashed XRES
$K_{<F>}$ Key for <F>
RAND Random challenge
RES Response
XRES Expected Response

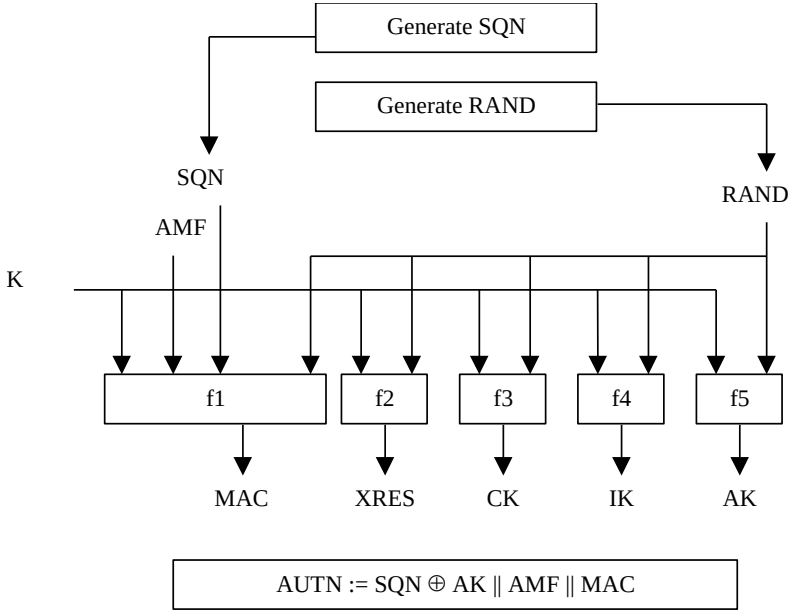
Network Access Security: AKA



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

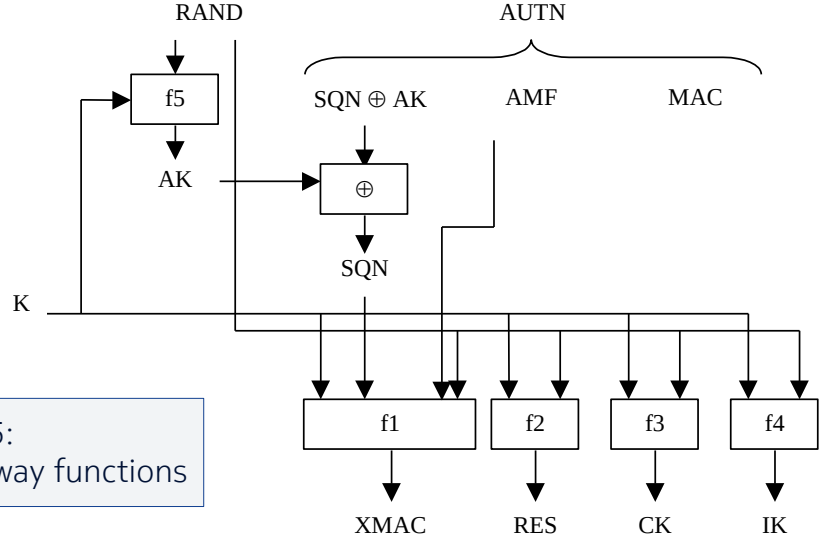
Deep Dive AKA: Details on Authentication Parameters (from TS 33.102)

Network: Create Authentication Information



AUTN := SQN ⊕ AK || AMF || MAC

UE: Evaluate AUTN



f1, ..., f5:
one-way functions

XMAC = MAC ?
SQN in correct range?

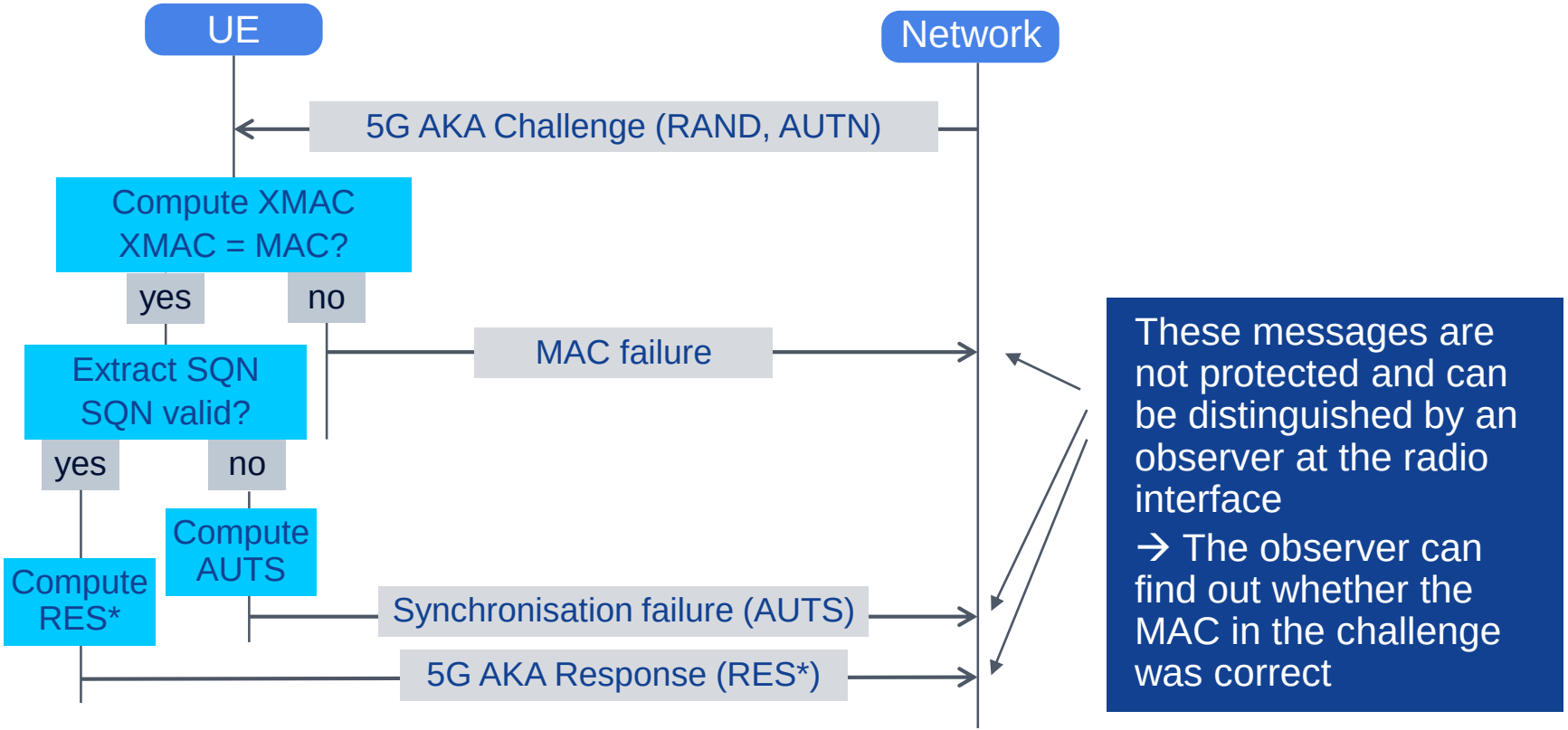
In 5G, K_{AUSF} is derived from CK, IK

NOKIA Bell Labs

NOKIA Bell Labs

Network Access Security Attacks against 5G AKA

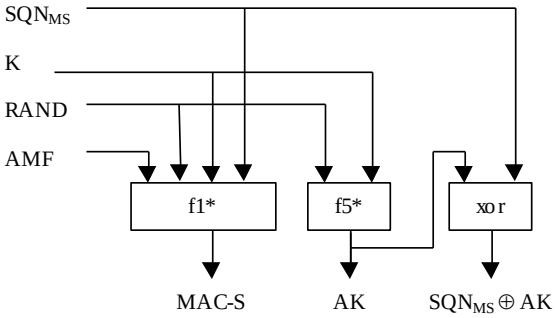
Deep Dive AKA: Failure Cases



Linkability Attack Against 5G AKA According to [1]

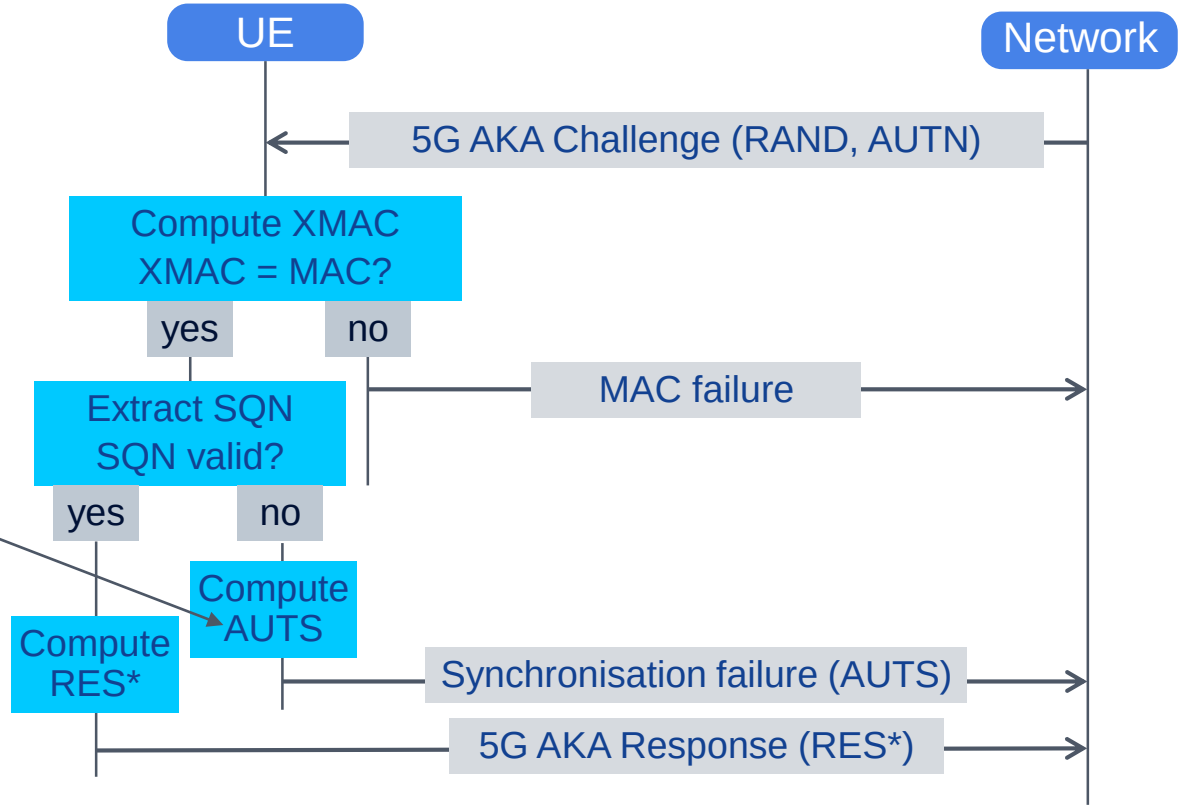
- [1] R.Borgaonkor et al., “New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols”
- When an attacker replays to a UEx a genuine AKA challenge that the network has computed for a UEa, then the attacker can find out whether UEx=UEa, because in this case UEx will send a synchronization failure, otherwise a MAC failure.
- Practical approach:
  - Attacker uses a radio interface sniffer to observe genuine successful authentication runs of a UE and to record the AKA challenge (RAND, AUTN). (Attacker sees only 5G-GUTIs of the UEs, needs to find out somehow which of them is the targeted victim UE.)
  - Attacker sets up a fake base station at the place where (s)he wants to detect the presence of the victim UE.
  - For all UEs trying to attach to the fake base station, the attacker performs the RRCsetup, replays the captured AKA challenge and checks whether the response is “Synchronisation error” (from the targeted victim) or “MAC failure” (from some other UE).
- Opinions differ on the practical impact of this linkability attack.

Deep Dive AKA: Failure Cases



AK = f5*(K, RAND)
AUTS = SQN_{MS} xor AK || …

Replay of AKA challenges can lead to the same AK encrypting different SQN-values
→ weak cryptography



NOKIA Bell Labs

“SQN-Bit-Leakage” Attack Against 5G AKA According to [1]

- “Break of SQN confidentiality”: By replaying AKA challenges to a UE and recording the answers, an attacker may discover the least significant bits of the UE’s SQN. If the attack is done two times successfully, the attacker sees how much the SQN has been increased in between.
  - The effort is exponential in the number of bits.
  - The UE must stay in the range of the attackers fake base station long enough to replay several AKA challenges
  - Knowledge of two SQNs does not allow to derive the number of authentications done in between, if SQN is incremented unpredictably, as proposed by two different schemes described in the standard (TS 33.102). No stringent conclusions about the number of service requests (e.g. calls, sessions, SMS messages) between the two successful attacks can be made.
- Although the practical impact of both attacks from [1]seems rather low, 3GPP considers several proposals to change the protocol to avoid the attacks. Main issue is backward compatibility.

Other Research Papers Claiming Attacks on 5G AKA

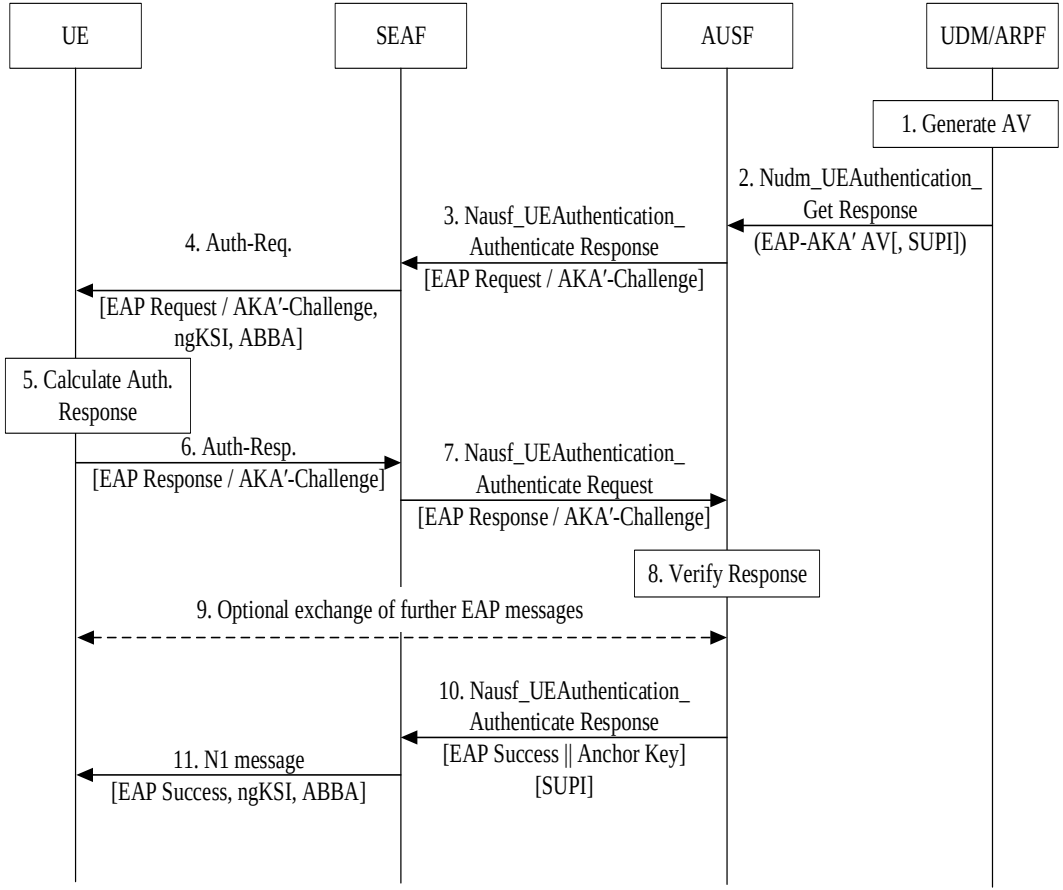
- Basin, David & Dreier, Jannik & Hirschi, Lucca & Radomirovic, Saša & Sasse, Ralf & Stettler, Vincent (2018). “A Formal Analysis of 5G Authentication” 1383-1396. 10.1145/3243734.3243846.
  - General claim that security goals are missing, and “critical security goals are not met” (in certain situations)
  - Attacks as in [1] mentioned – otherwise no practical attacks described
  - Wrong claims, e.g. that a K_{SEAF} could be mapped to a wrong SUPI
  - Errors probably due to the failure to model the protocol formally down to all details
  - General issue for formal analysis: There is no formal model of a mobile network
- A. Koutsos, "The 5G-AKA Authentication Protocol Privacy“, 2019 IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden, 2019, pp. 464-479.
  - Another linkability attack, based on the SUCI: When a UEx sends a request with a SUCI, and the attacker replaces the SUCI with a previously captured SUCI of a UEa, the attacker can find out whether UEx=UEa (by observing whether the subsequent authentication)
    → mitigation applicable as for the linkability attack in [1]
  - Proposes a modified protocol and claims that a weaker non-linkability property can be proved for it

NOKIA Bell Labs

Network Access Security
NAS Security Setup

EAP-AKA' (from TS 33.501)

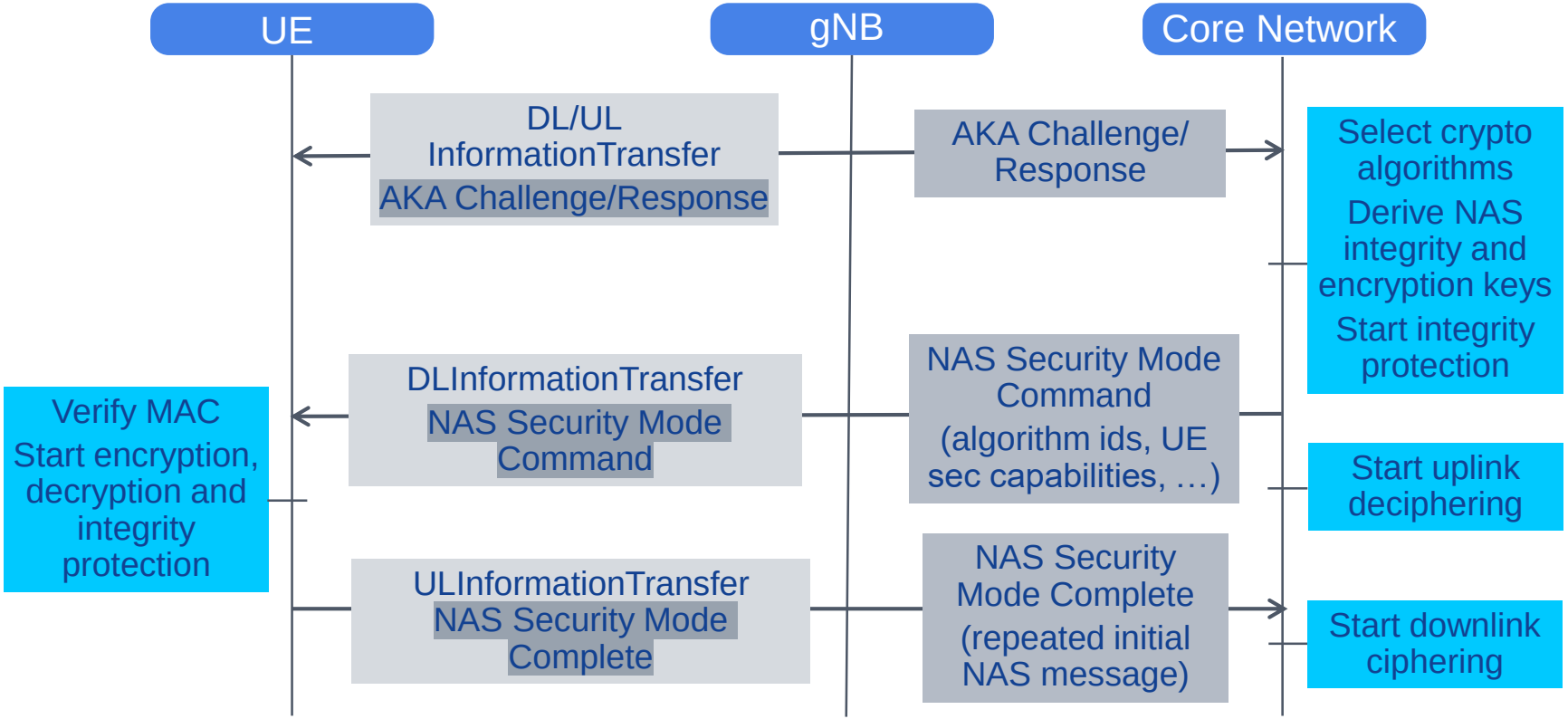
- Slightly different info provided by UDM/ARPF
- EAP messages are exchanged between UE, SEAF (authenticator) and AUSF (authentication server)
- EAP-AKA' uses similar parameters and mecha-nisms as 5G AKA (RAND, AUTN, RES/XRES)
- Authentication runs between UE and AUSF in the home network - no explicit authentication confirmation required



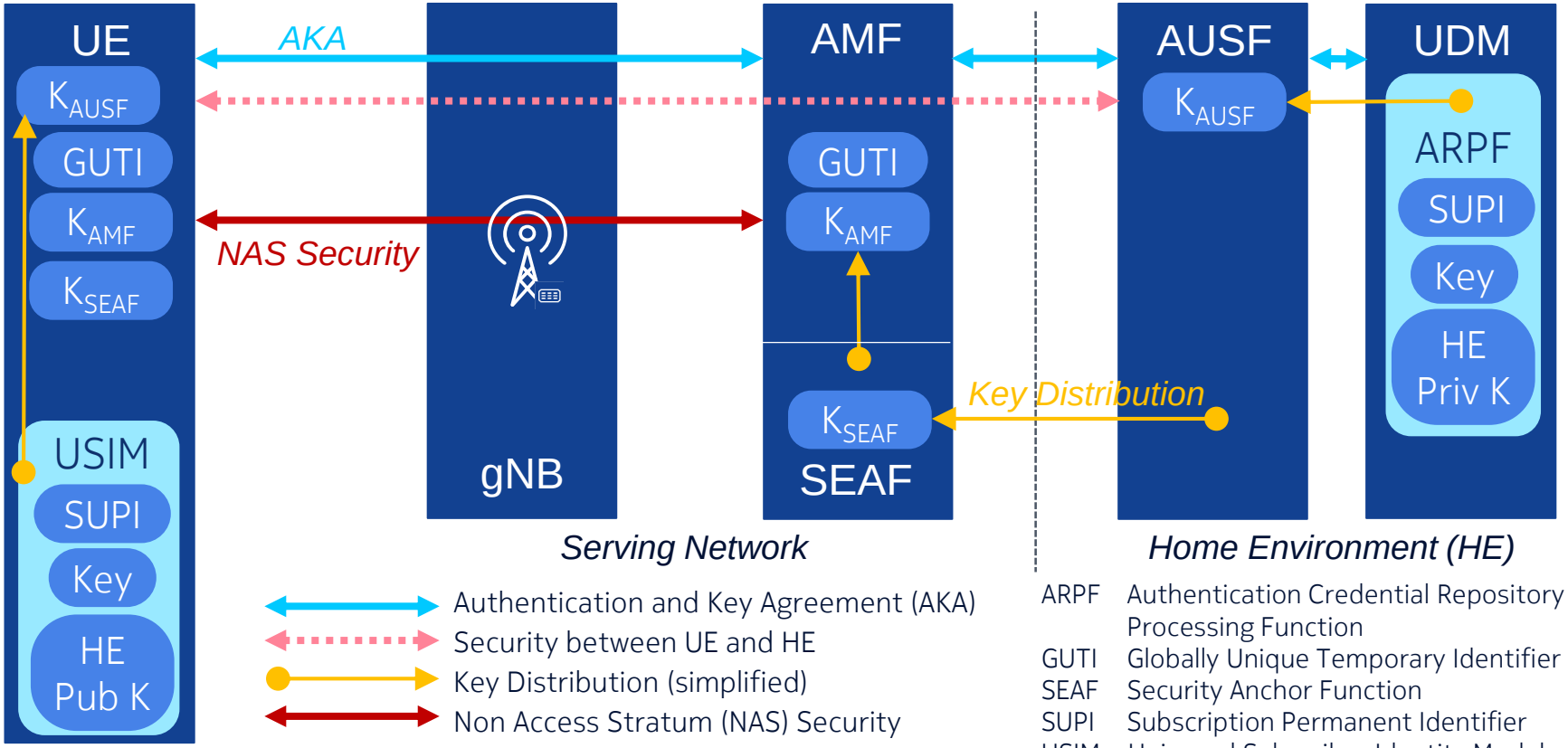
From TS 33.501

NOKIA Bell Labs

Network Access: NAS Security Mode Command Procedure



Network Access Security: AKA and NAS Security

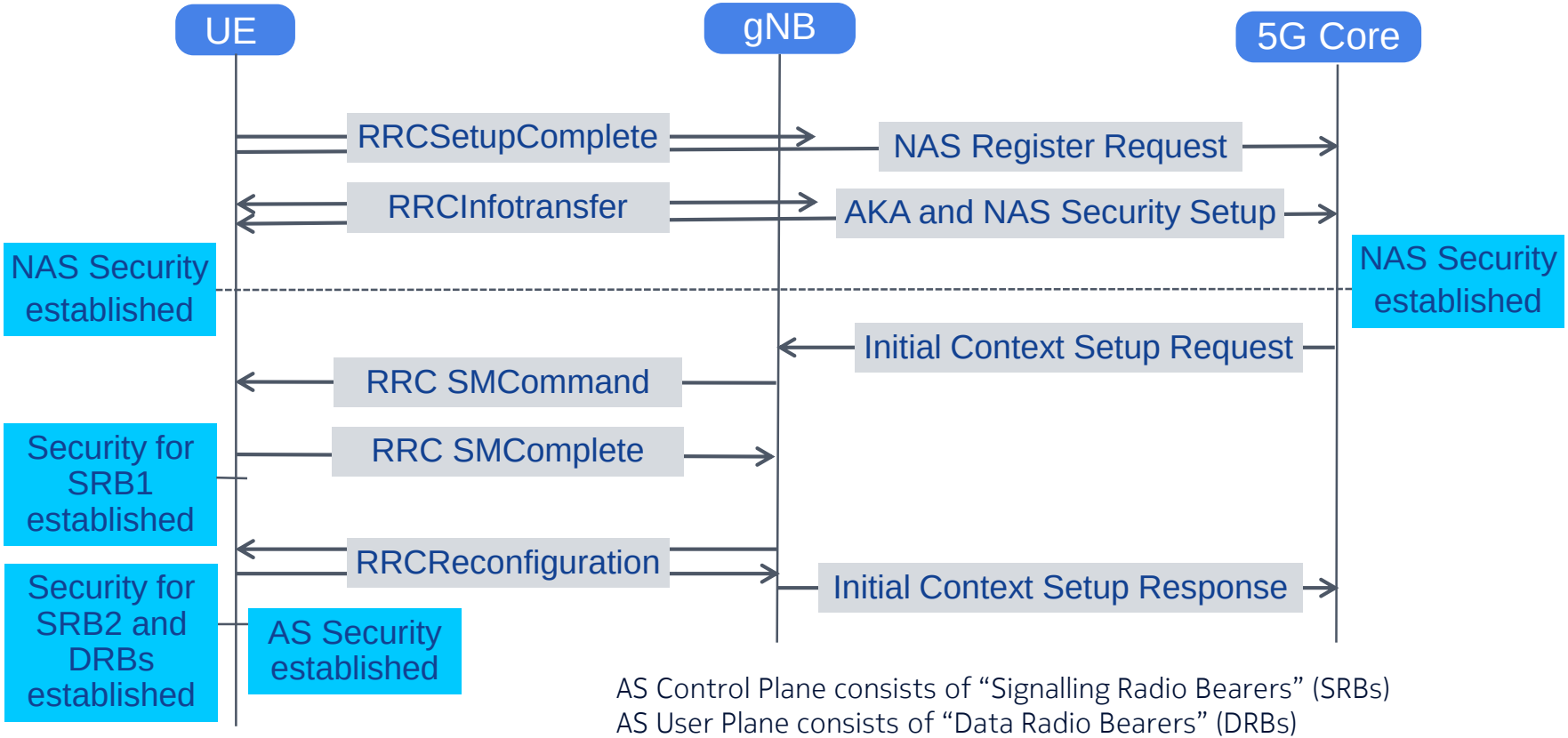


ARPF	Authentication Credential Repository and Processing Function
GUTI	Globally Unique Temporary Identifier
SEAF	Security Anchor Function
SUPI	Subscription Permanent Identifier
USIM	Universal Subscriber Identity Module

NOKIA Bell Labs

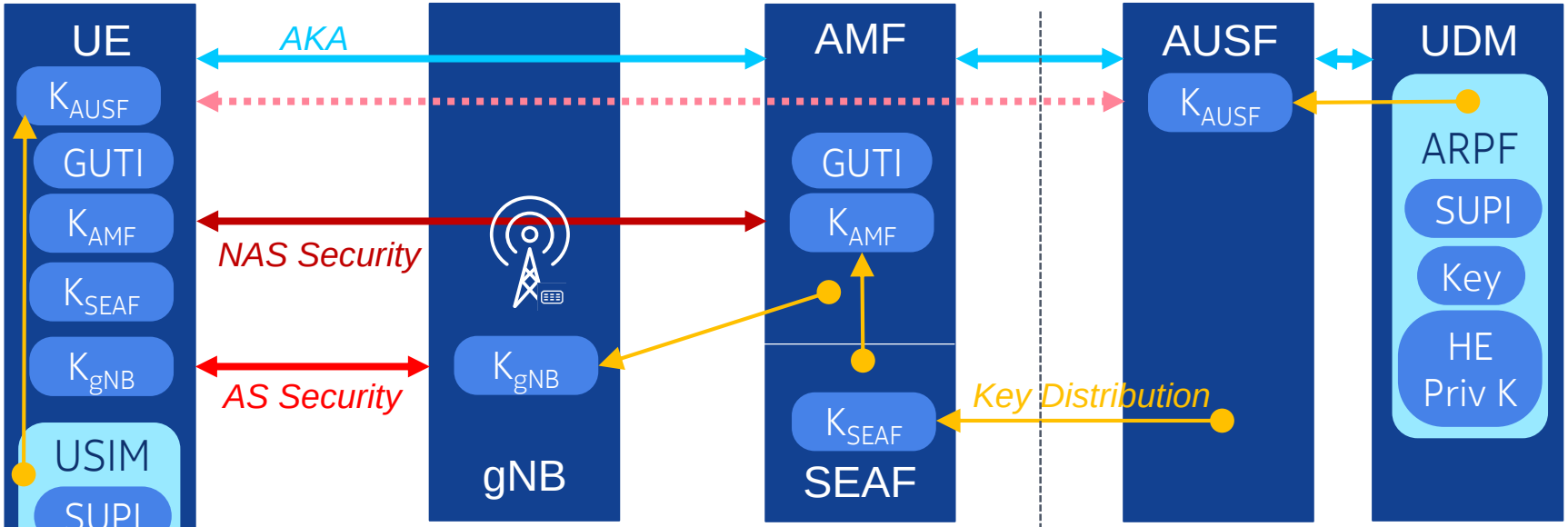
Network Access Security
AS Security Setup

Network Access: AS-Security Setup



AS Control Plane consists of “Signalling Radio Bearers” (SRBs)
AS User Plane consists of “Data Radio Bearers” (DRBs)

Network Access Security: AKA, NAS Security and AS Security



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

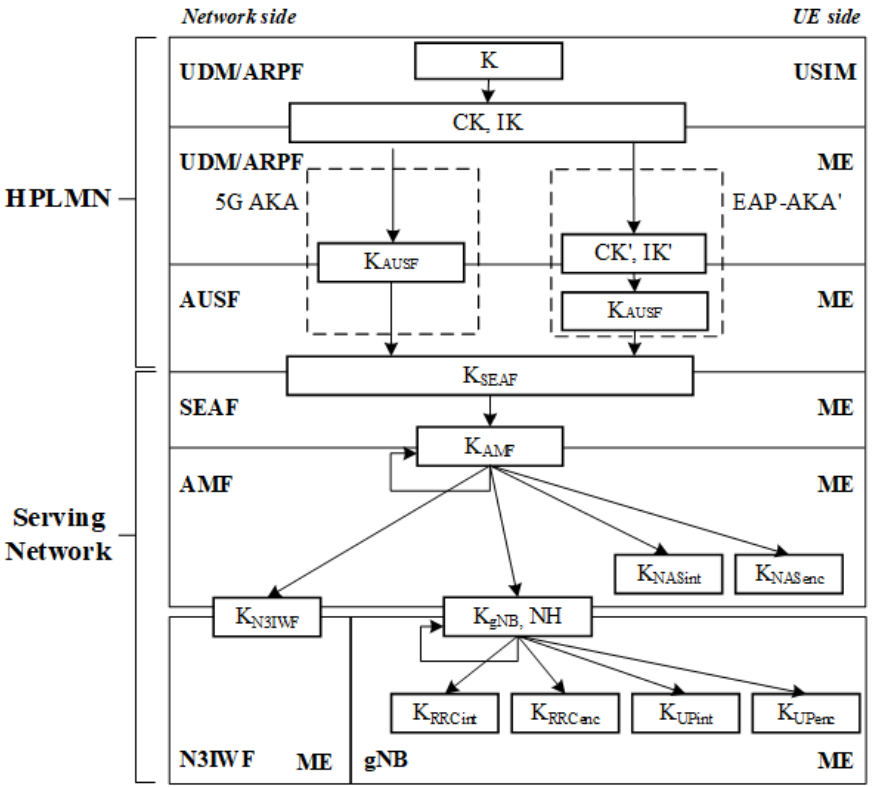
ARPF	Authentication Credential Repository and Processing Function
GUTI	Globally Unique Temporary Identifier
SEAF	Security Anchor Function
SUPI	Subscription Permanent Identifier
USIM	Universal Subscriber Identity Module

NOKIA Bell Labs

NOKIA Bell Labs

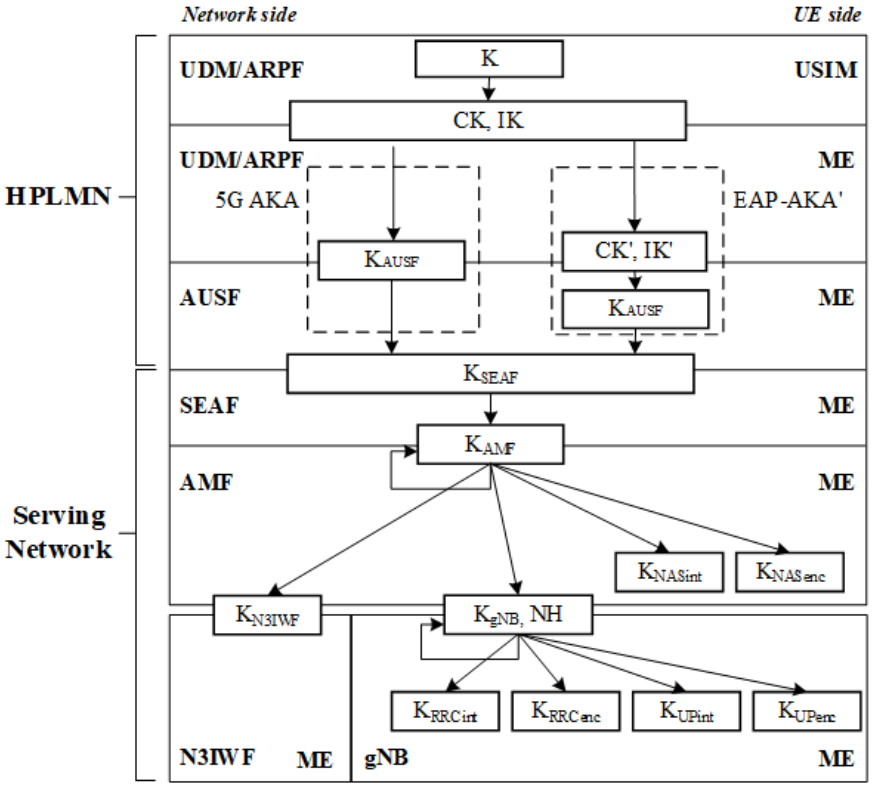
Network Access Security Key Hierarchy

Key Hierarchy (from TS 33.501) (1/2)



- K is the subscription's permanent key
- CK, IK: The 3G Ciphering and Integrity Keys
- UE side: USIM computes CK, IK; all other key derivations are done in the Mobile Equipment (ME), i.e. in the UE but outside the USIM
- CK' and IK' are derived taking the Serving Network Identity as an Input – from this point in the key hierarchy, all keys are only valid for this Serving Network
- A new K_{AMF} can be derived from an existing one
- K_{NASenc} and K_{NASint} are used to encrypt and integrity protect the NAS signaling

Key Hierarchy (from TS 33.501) (2/2)

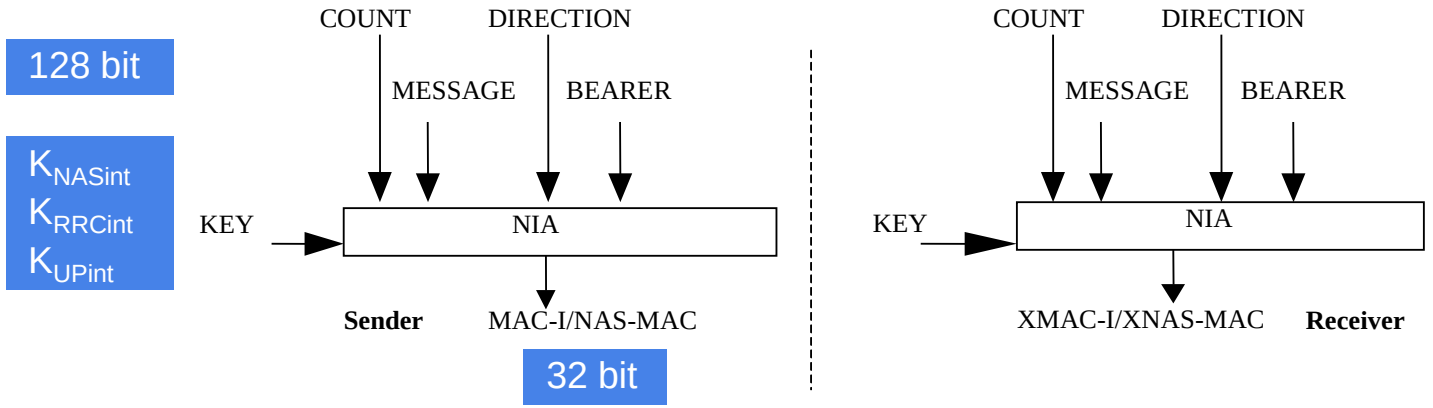


- When a K_{AMF} has been derived, the first K_{gNB} is derived directly from K_{AMF}
- Subsequent K_{gNB} (e.g. needed after a handover to the next gNB) are either derived from the current K_{gNB} or from an interim value NH (“Next Hop”) that is derived from K_{AMF}
- K_{RRCenc} and K_{RRCint} are used to encrypt and integrity protect the AS signaling
- K_{UPenc} and K_{UPint} are used to encrypt and integrity protect the User Plane (i.e. user data traffic) between UE and gNB
- N3IWF is the Non-3GPP Interworking Function that allows access to the 5G core via a non-3GPP network (e.g. WiFi)

NOKIA Bell Labs

Network Access Security Encryption and Integrity Protection

Integrity Protection Mechanism



From TS 33.501

NIA: Integrity Algorithm for 5G
MAC: Message Authentication Code
XMAX: Expected MAC

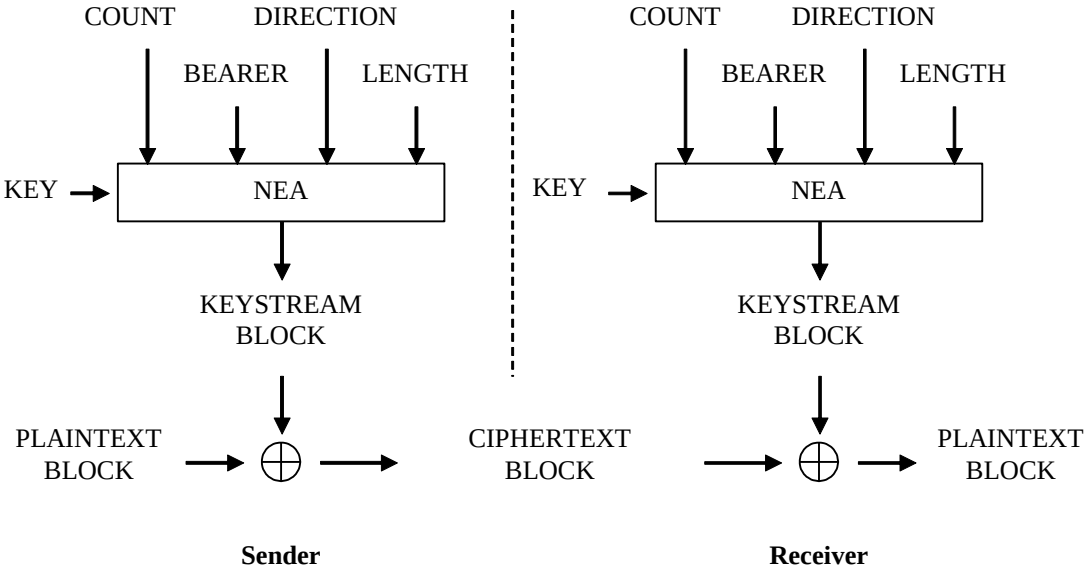
Three options for NIA:
AES-CMAC, Snow 3G, ZUC

NOKIA Bell Labs

Encryption Mechanism

128 bit

K_{NASenc}
K_{RRCenc}
K_{UPenc}

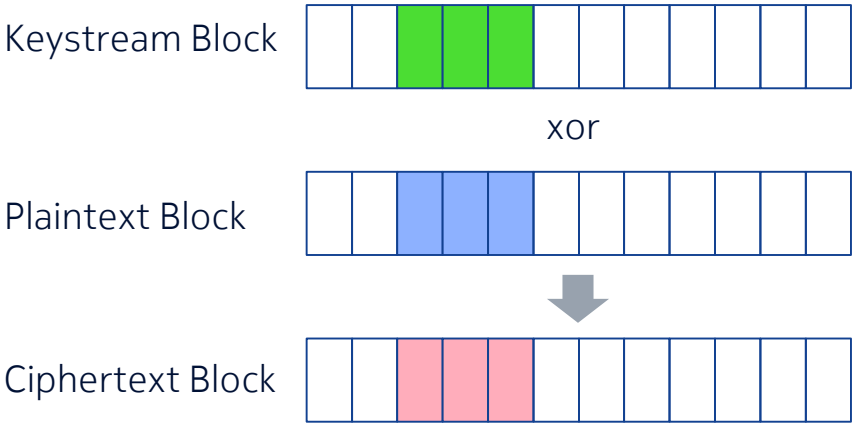


Three options for NEA:
AES, Snow 3G, ZUC

From TS 33.501

NEA: Encryption Algorithm for 5G

Known Plaintext Attack: Attacker can deterministically modify known plain text



Keystream part encrypting known Plaintext

Known Plaintext

Ciphered Known Plaintext

Known Plaintext xor Ciphered Plaintext → Keystream part

Keystream part xor Altered Plaintext → New Ciphertext

Attacker

New Ciphertext xor Keystream part → Altered Plaintext

Victim

NOKIA Bell Labs

Integrity Protection to Prevent Known Plaintext Attacks

- To prevent the known plaintext attack, integrity protection is required in addition to encryption
- 3GPP introduced integrity protection in 3G, but not for the user traffic
- Possible reasons:
  - There is much more user traffic than control traffic – doing integrity protection adds considerably to the effort on the UE and the base station.
  - The main service was voice. A bit error in a voice packet is completely harmless – discarding voice packets with bit errors (due to failing integrity protection) or having to repeat them impacts the voice quality.
  - In encrypted voice, known plaintext is rather unlikely.
- This was not changed in LTE (although specified 10 years later)

User Traffic Integrity Protection in 5G

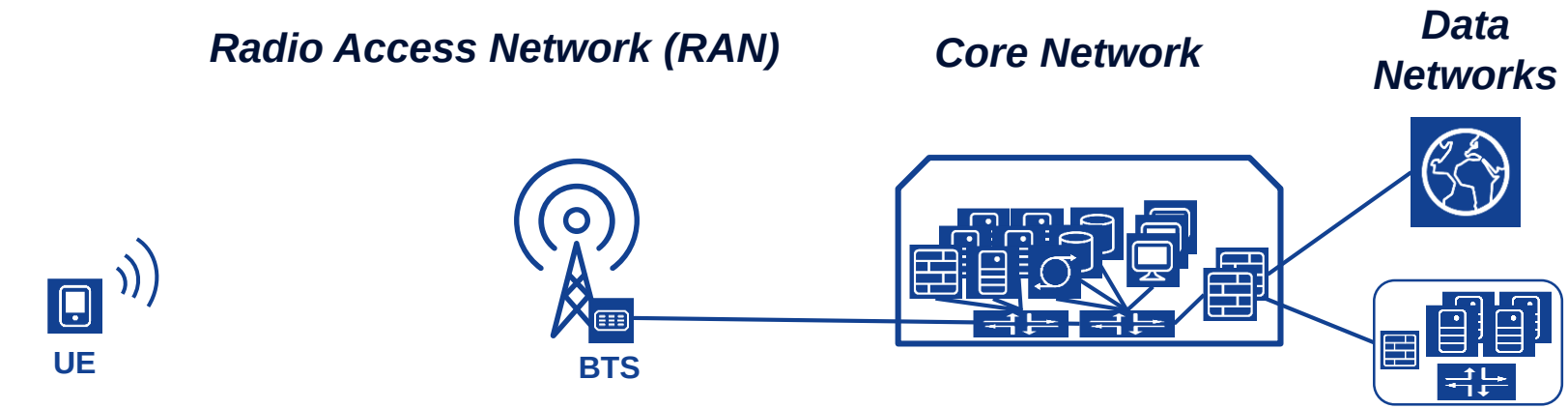
- Intention of SA3 (3GPP Security Specification Group): Make user plane integrity protection mandatory to support for UEs and base stations
  → TS 33.501 mandates this, without exceptions
- The use of user plane integrity protection is however not mandated
- Concerns of UE chip set vendors: Integrity protection is not supported at higher rates by their chip sets
  → According to TS 38.300 (RAN) and TS 24.501 (NAS) a UE can tell the network that it supports user plane integrity protection at a its full rate or only at a rate of 64 kbps
- If the UE does not support integrity protection at its full rate, all sessions with data rates above 64 kbps will be done without integrity protection
- In 5G Non-Stand-Alone deployments (i.e. 5G Base Station connected to a 4G core network), no user plane integrity protection is supported

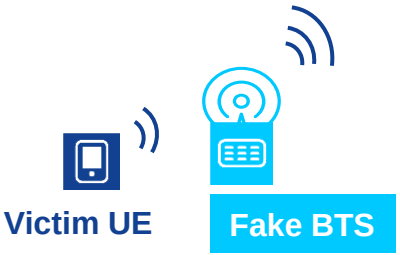
➢ In many cases (early) 5G will not use user plane integrity protection!

NOKIA Bell Labs

Network Access Security
Attacks against AS security

Fake BTS Acting as a Relay Between Victim UE and Genuine BTS





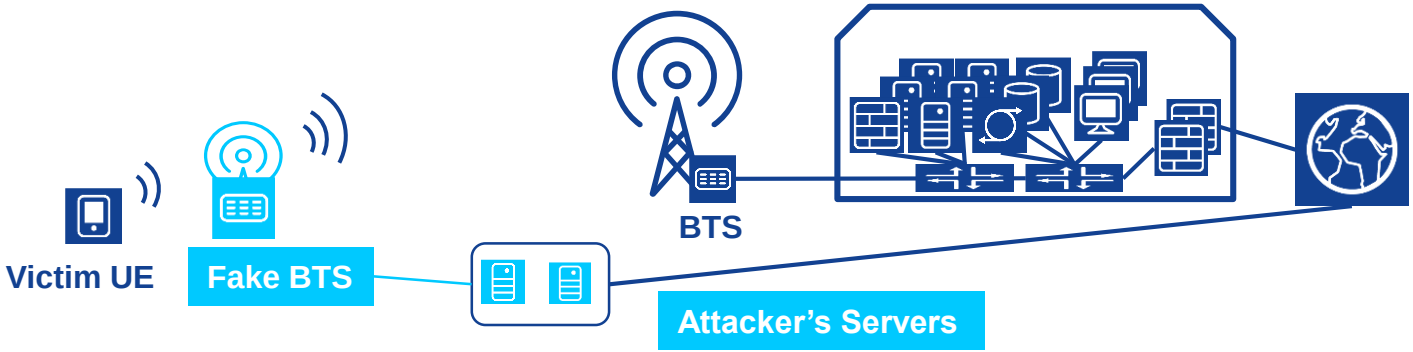
- Impersonates the network towards the UE
- Acts on behalf of the victim UE towards the network, e.g. relays traffic
- Cannot read encrypted traffic
- Cannot change integrity protected traffic covertly
- **Can execute a known plaintext attack on encrypted traffic that is not integrity protected**

aLTEr Attack from [2], Put Simply

- Know the address of the DNS server the victim uses
- Detect at the fake BTS when the user sends a DNS request
- Known plaintext attack: Change at the fake BTS the destination address to the address of your malicious DNS server
- Connect the victim to faked malicious application servers

[2] David Rupprecht, Katharina Kohls Kohls, Thorsten Holz, Christina Pöpper, "Breaking LTE on Layer Two“, IEEE Symposium on Security & Privacy (Oakland), May 2019, https://alter-attack.net/

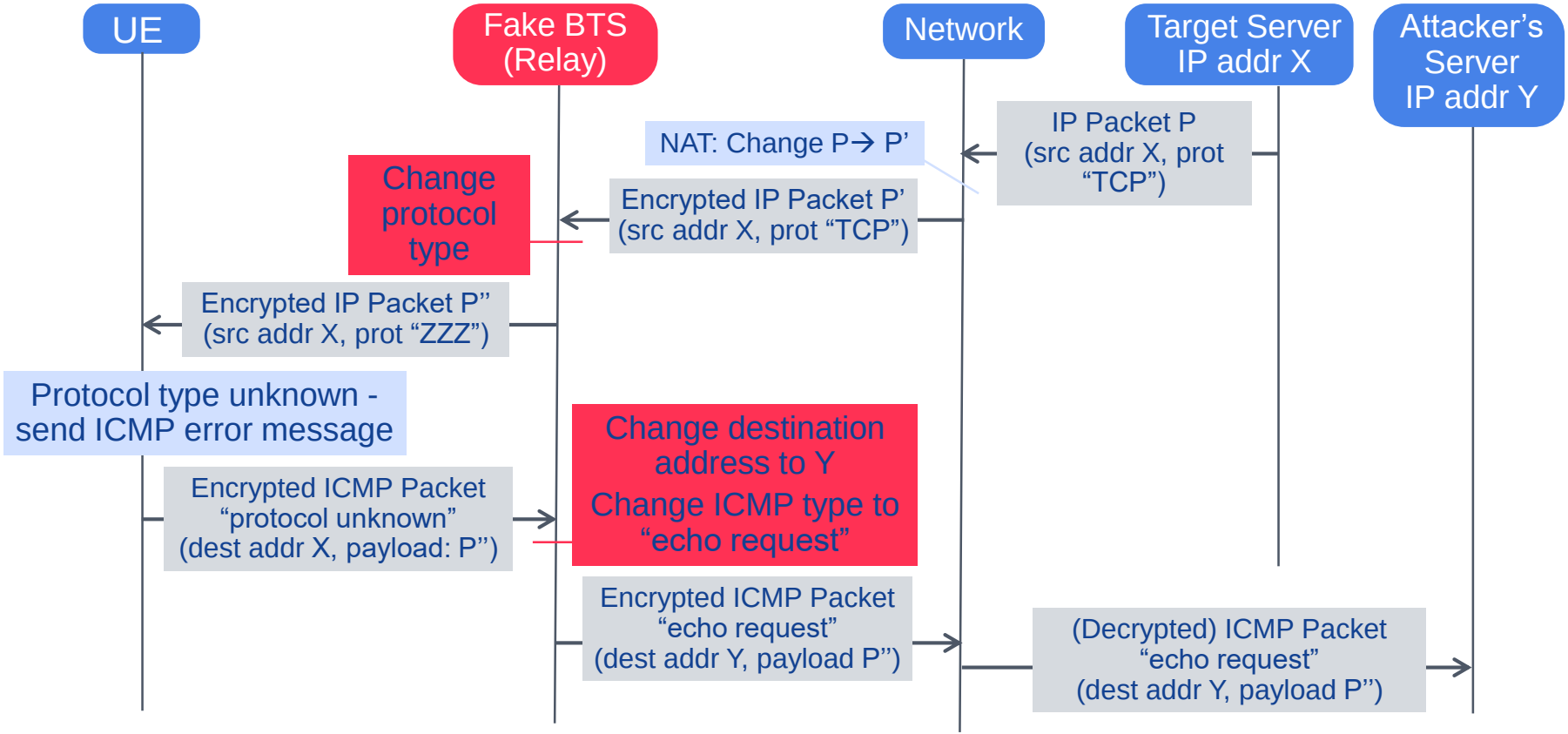
IMP4GT Attack from [3]: Basic Setup



- Same setup as in the aLTEr attack
- aLTEr attack can be used as a first step to connect the victim to a malicious TCP proxy when the victim wants to setup a TCP connection
  (but this is NOT a prerequisite – there are other options)

[3] David Rupprecht, Katharina Kohls Kohls, Thorsten Holz, Christina Pöpper, "MP4GT: IMPersonation Attacks in 4G NeTworks", Network and Distributed System Security Symposium (NDSS), San Diego, California, USA, February 2020, https://imp4gt-attacks.net/

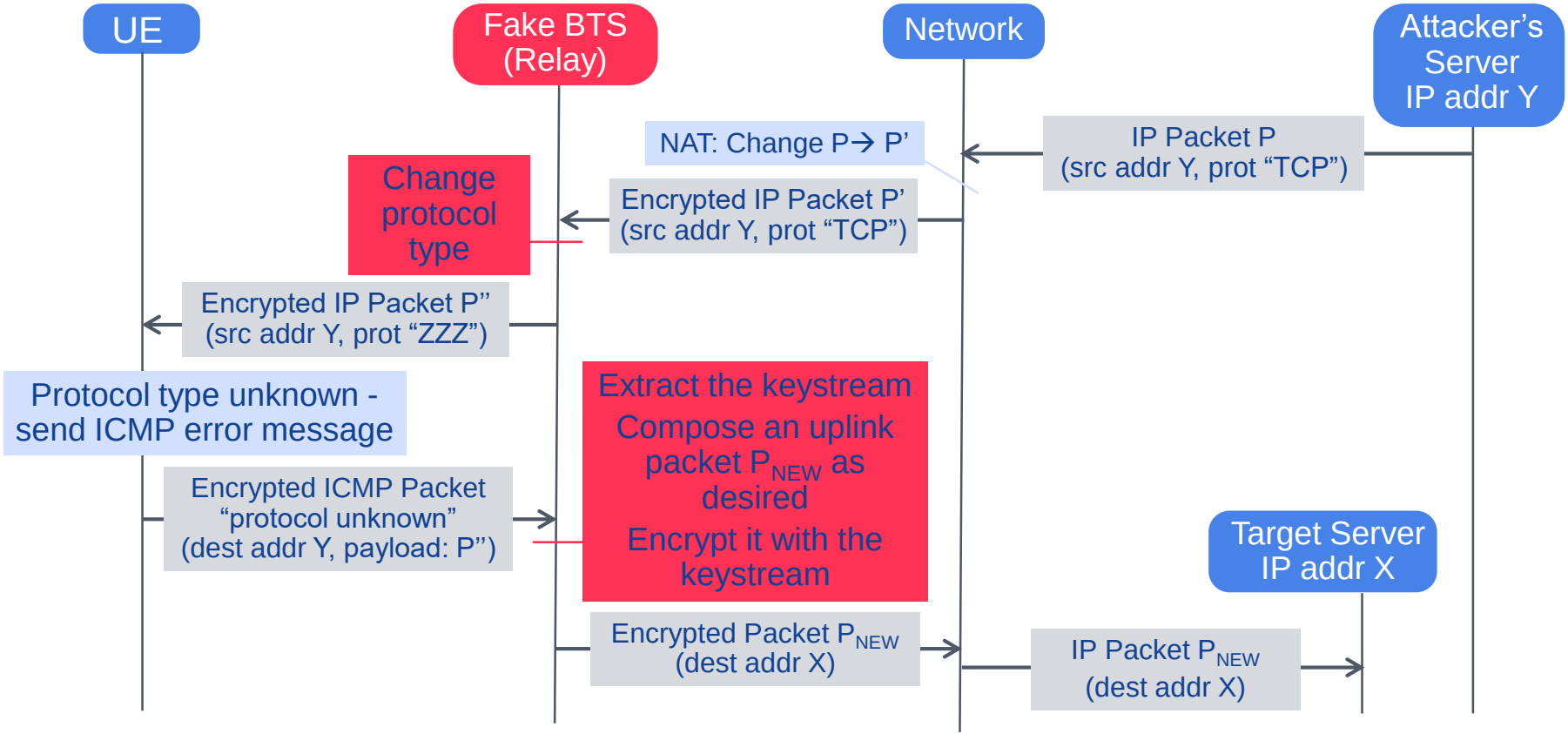
IMP4GT Attack: Reflection and Downlink Decryption



IMP4GT Attack: Reflection and Downlink Decryption

- When the fake base station receives an encrypted downlink packet (towards the UE) of which the attacker knows IP source address and protocol type (e.g. “TCP”), the attacker can change the protocol type to some unknown value
- IETF standardized IP behavior for the UE is to reply with an ICMP error message (“protocol unknown”) that comprises the received packet → “Reflection”
- This ICMP will be encrypted by the UE and sent towards the fake base station, which changes the destination address to the address the attacker’s server and the ICMP type to “echo request” and forwards the packet to the genuine base station (changing the ICMP type ensures that the packet is not discarded by the firewall between the PLMN and the Internet)
- The packet will be decrypted by the (genuine) base station and passed on through the firewall to the attacker’s server

IMP4GT Attack: Uplink Encryption



IMP4GT Attack: Uplink Encryption + Uplink Impersonation

- Attacker needs a valid keystream to encrypt a (crafted) uplink packet:
  - Attacker sends an arbitrary packet from an attacker's server to the UE.
  - Attacker changes protocol type at the fake BTS, thus lets the packet be reflected by the UE
  - Attacker knows the exact content of the reflected packet and can extract the complete keystream
- Uplink impersonation: Attacker impersonates the UE towards a server
  - The attacker must be able to send crafted packets → Uplink encryption
  - The attacker must understand what the server sends → Downlink decryption
- This impersonation is only on the IP layer (attacker can communicate with servers using the victim's IP address)
- Main exploits: Access to a subscriber portal in the PLMN that relies only on the radio layer security, or upload of criminal content to a web server

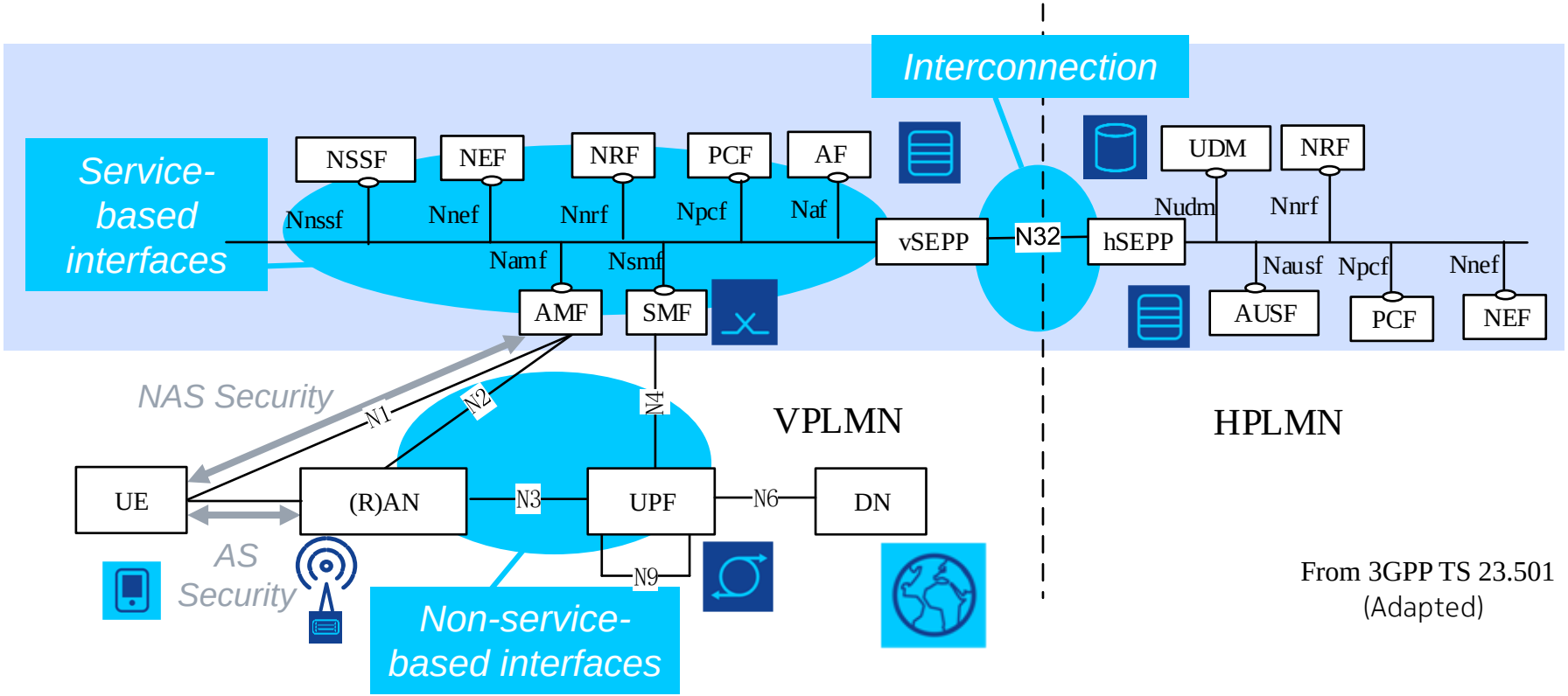
IMP4GT Attack: Downlink Impersonation, Restrictions, Countermeasures

- With similar means, the attack allows impersonation of servers towards the UE
  → The main exploit is firewall evasion – the attacker can send arbitrary traffic to the UE, evading the PLMN's firewall
- The IMP4GT attack has significant restrictions (only against victims in the range of the fake base station, impersonation only on IP layer, no decryption of downlink/uplink traffic with unknown source/destination address, limited rate of ICMP error message generation at UEs, limited size of ICMP packets)
- There are some workarounds that can make the attack less effective, but the obvious countermeasure is to apply integrity protection
  - ➢ Not supported in LTE
  - ➢ Supported in 5G (stand alone), but currently UEs may not support it at full rate
- Still, wide-spread use of this attack in the field is not expected

NOKIA Bell Labs

Network Domain Security
Non-service-based Interfaces

Security Between Network Functions



From 3GPP TS 23.501 (Adapted)

Security for Non-Service-Based Network Interfaces

- 3GPP specifies usage of IPsec ESP (see TS 33.210 and RFC 4301)
  → provides encryption and integrity protection
- Specific cases where protection is required:
  - Traffic “between security domains”
  - “Backhaul link” between (non-cloudified) gNB and core network
- Certificate enrolment procedure for gNB: Automatic procedure for provisioning an operator certificate to a gNB based on its manufacturer certificate
- IPsec mandatory to use unless (equivalent) protection is provided by other means
- Example: Low layer encryption/integrity protection by an optical transport network interconnecting an edge cloud hosting the gNB and a central cloud hosting the core functions

NOKIA Bell Labs

Network Domain Security Service-based Interfaces

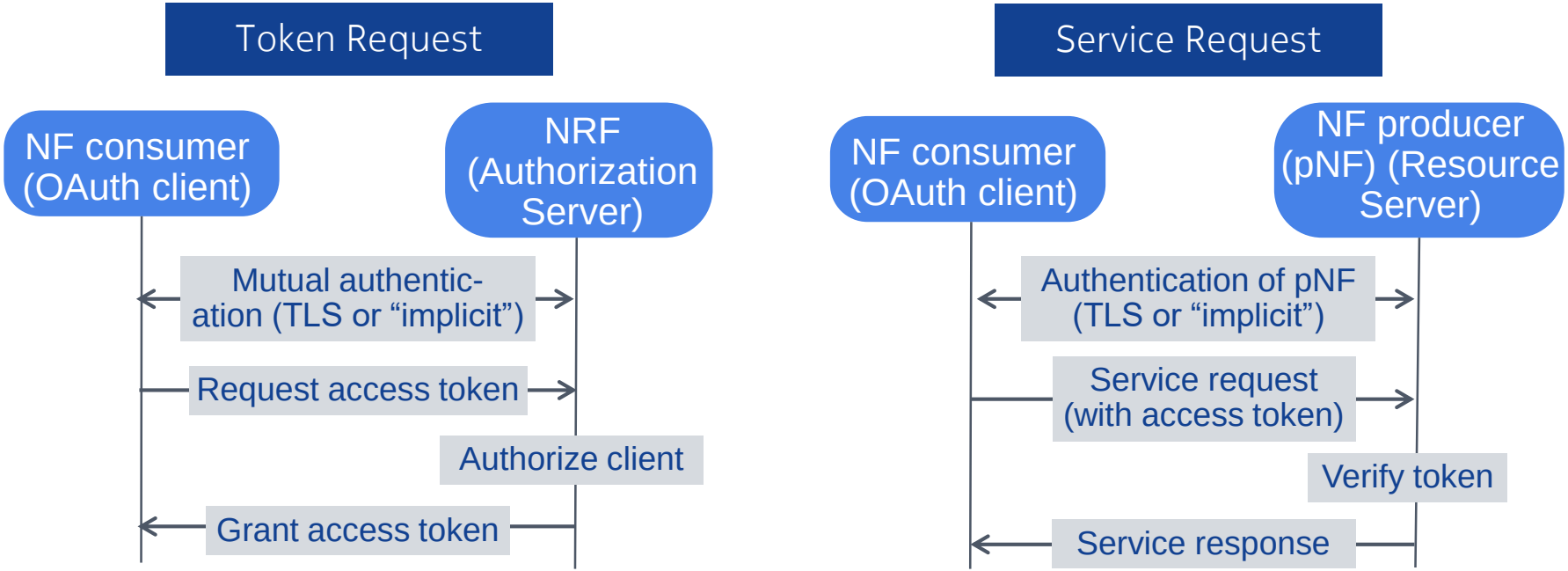
Service-Based Architecture: Security for Service-Based Interfaces

Security for service-based interfaces (mandatory to support, optional to use)

- TLS with client- and server-certificates between all network functions (NFs)
- Token-based authorization of service requests to network functions (using the OAuth 2.0 framework)
- NRF (Network Repository Function) acting as OAuth authorization server, authorizes NFs for using services provided by other NFs, according to policies

OAuth Framework according to IETF RFC 6749 “The OAuth 2.0 Authorization Framework"

SBA: Token Request and Service Request (Simplified View)

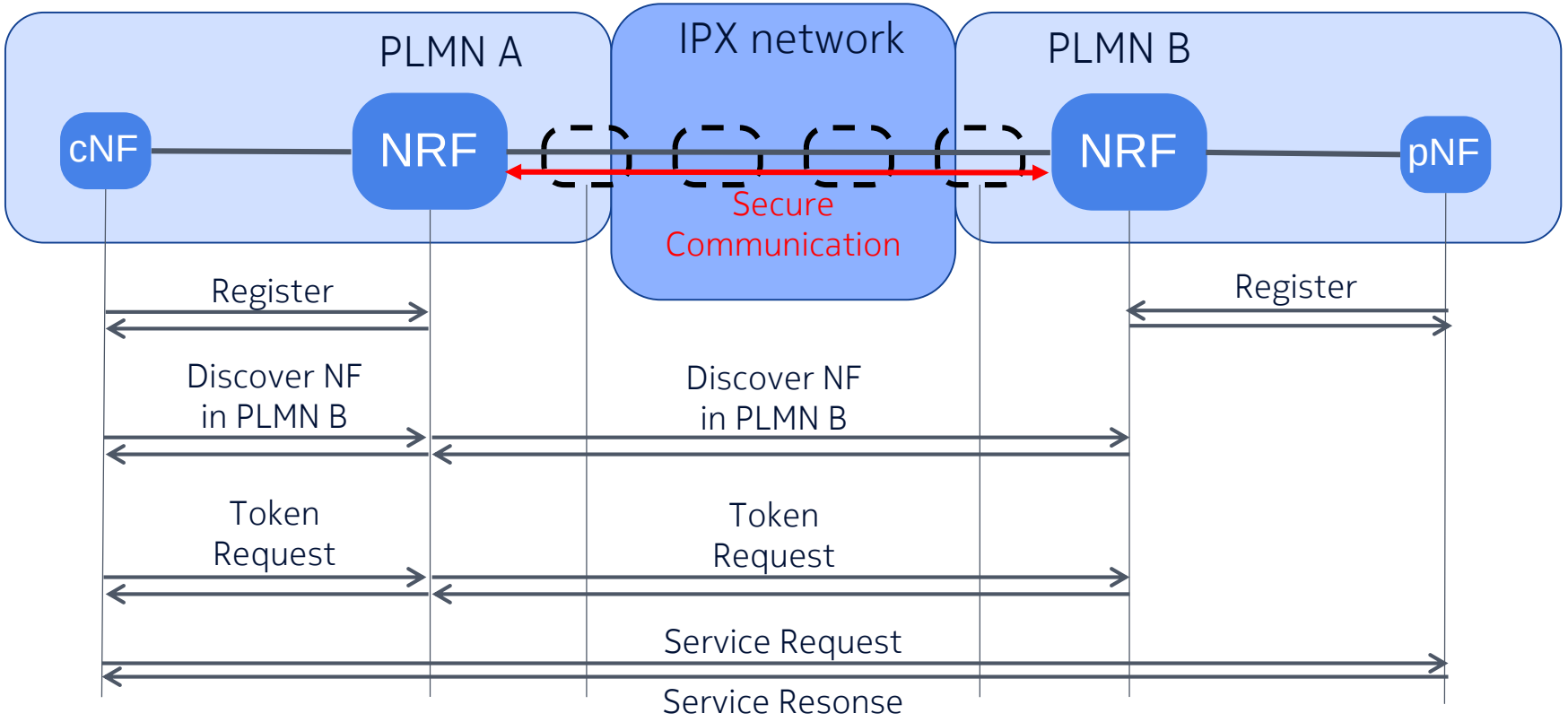


Token Format: JSON (Java Script Object Notation) web tokens (RFC 7519), secured by digital signatures or MACs (Message Authentication Codes) based on JSON Web Signature (RFC 7515)

NOKIA Bell Labs

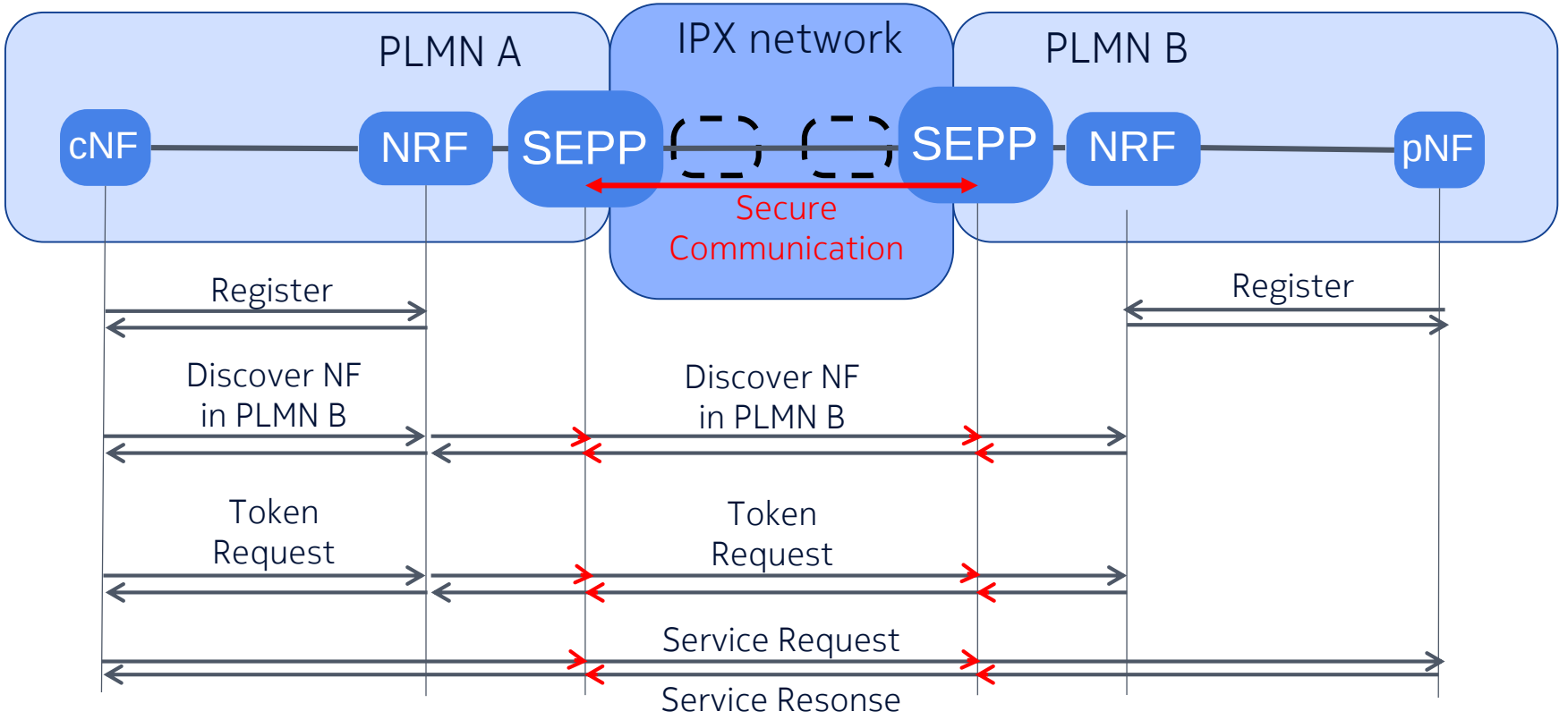
Network Domain Security
Interconnection Security

SBA – Interworking Between PLMNs



NOKIA Bell Labs

SBA – Closer View on the Interworking Between PLMNs



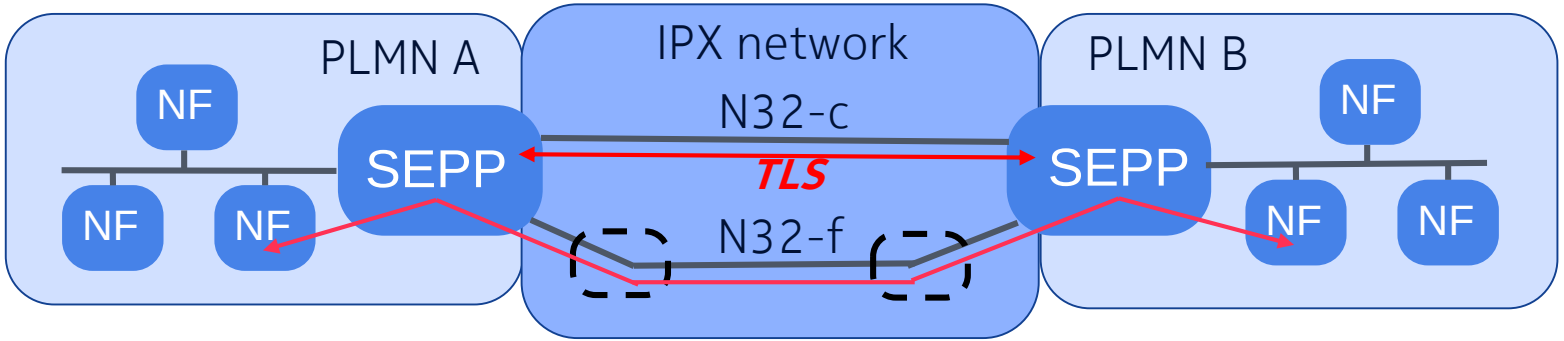
Interconnection Security Enhancements in 3GPP Rel. 15

Interconnection security for service-based interfaces

- New entity SEPP (Security Edge Protection Proxy)
- All roaming control traffic is routed via the SEPP and the N32 interface to the SEPP of the other PLMN
- TLS between SEPPs and between SEPP and next-hop intermediary in IPX
- Security capability negotiation between each pair of SEPPs
- PRINS (PRotocol for N32 INterconnect Security) for JSON (Java Script Object Notation) information elements on N32

User Plane between PLMNs: No specific protection mechanisms standardized in 3GPP Rel 15; VPN techniques may be used

Interconnection Security in 5G – Security Negotiation Between SEPPs



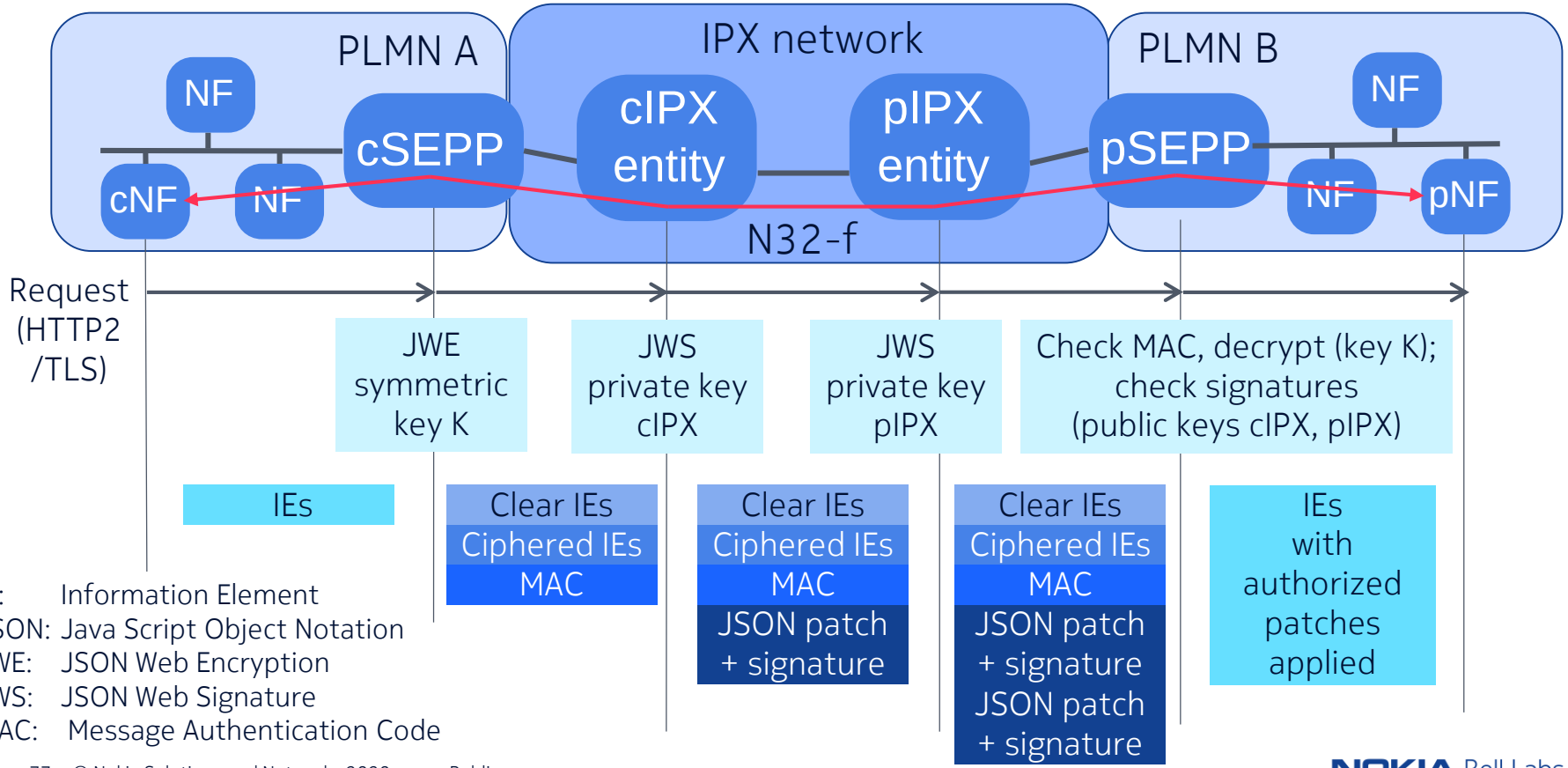
N32-c: Mutually authenticated TLS connection, to negotiate security for N32-f

N32-f (NF-related signalling):

- Either TLS (direct connection)
- Or PRINS (connection via entities in the IPX), requires:
  - Agreement of keys and cipher suites
  - Agreement of IE protection polices (encryption, modification)

IE: Information Element

Interconnection Security in 5G – PRINS



IE: Information Element
JSON: Java Script Object Notation
JWE: JSON Web Encryption
JWS: JSON Web Signature
MAC: Message Authentication Code

NOKIA Bell Labs

5G versus 4G Security

Known LTE Security Issues – Mitigation in 5G

LTE security specified in 3GPP TS 33.401 and TS 33.402

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

Settled

No user plane integrity protection

Settled

The IP exchange (IPX) network interconnecting mobile networks is often not suitably secured, and some mobile networks are vulnerable by attacks or fraud from the IPX

Improvements

LTE is not resistant against smart jamming

Improvements

Physical exposure of LTE base stations (eNBs) may facilitate attacks against user traffic confidentiality

Improvements

LTE does not prevent downgrade to GSM

Issue remains


3GPP TS 33.401 V14.5.0 (2018-01)

Technical Specification

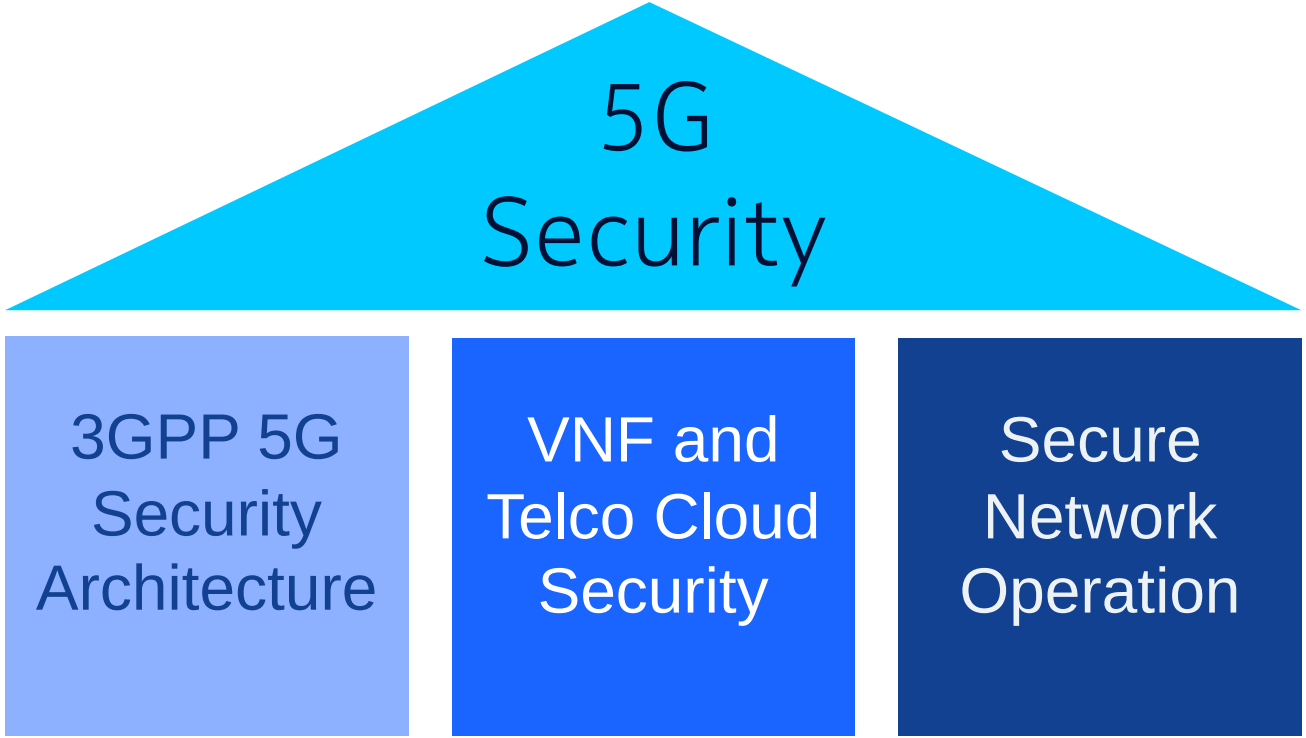
3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3GPP System Architecture Evolution (SAE);
Security architecture
(Release 14)

NOKIA Bell Labs

NOKIA Bell Labs

Holistic 5G Security Approach

A Holistic 5G Security Approach



Pillars of 5G Mobile Network Security

3GPP 5G Security Architecture

- Authentication between user equipment and network/network slices
- Traffic encryption and integrity protection
- Subscriber location privacy
- Security for internal and external network interfaces, including service-based interfaces
- Secure interconnection between PLMNs

VNF and telco cloud security

- Sound, robust, security aware implementation of
  - the VNFs
  - the virtualization layer (e.g. hypervisors, container platforms)
  - the overall cloud platform software (MANO stack)
- Integrity (trust) assurance for both platform and VNFs

Secure Network Operation

- Perimeter security and traffic filtering by virtual firewalls
- Traffic separation by VLANs and wide area VPNs
- Network slice isolation
- Holistic, automated security management and orchestration
- Automated, self-adaptive, intelligent security controls

NOKIA Bell Labs

Thanks for your attention!


NOKIA