5G Security

Alf Zugenmaier, Munich University of Applied Sciences

March 1, 2019

Warning

This presentation has a high density of acronyms.

If you would like to be reminded of their meanings, please ask or look up at http://webapp.etsi.org/Teddi/.

Agenda

- 5G Standardization Process
- 5G Architecture
- 5G's Security Goals
- 5G Key Enhancements
- Summary

Agenda

- **5G Standardization Process**
- 5G Architecture
- 5G's Security Goals
- 5G Key Enhancements
- Summary

5G Standardization Process - Actors

- ITU-T
  - High level requirements (IMT2020)
- IETF
  - RFCs – protocols
    - IPsec
    - TLS
    - EAP
- 3GPP
  - System specification
  - Interoperability
- Standards bodies
  - ETSI, etc.

5G Standardization Process – 3GPP

- Industry Association
- Organizational Partners
  - ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC
- Members can attend meetings
  - Companies, Ministries, etc.
- Output
  - Technical reports
    - Feasibility study
  - Technical specifications
  - System specification of procedures (API like view)

3GPP Process

- Structure
  - Technical Specification Groups (SA, CT, RAN)
  - Working Groups (e.g. WG SA3: security)
- Project planning
  - Study items (e.g. Study on Next Generation Security Architecture)
    - Output: none
  - Work items (e.g. 5G Phase 1 security)
    - Output: TS 33.501
- Releases
  - 5G phase 1 – R15
- Stages
  - Requirements, architecture, protocols

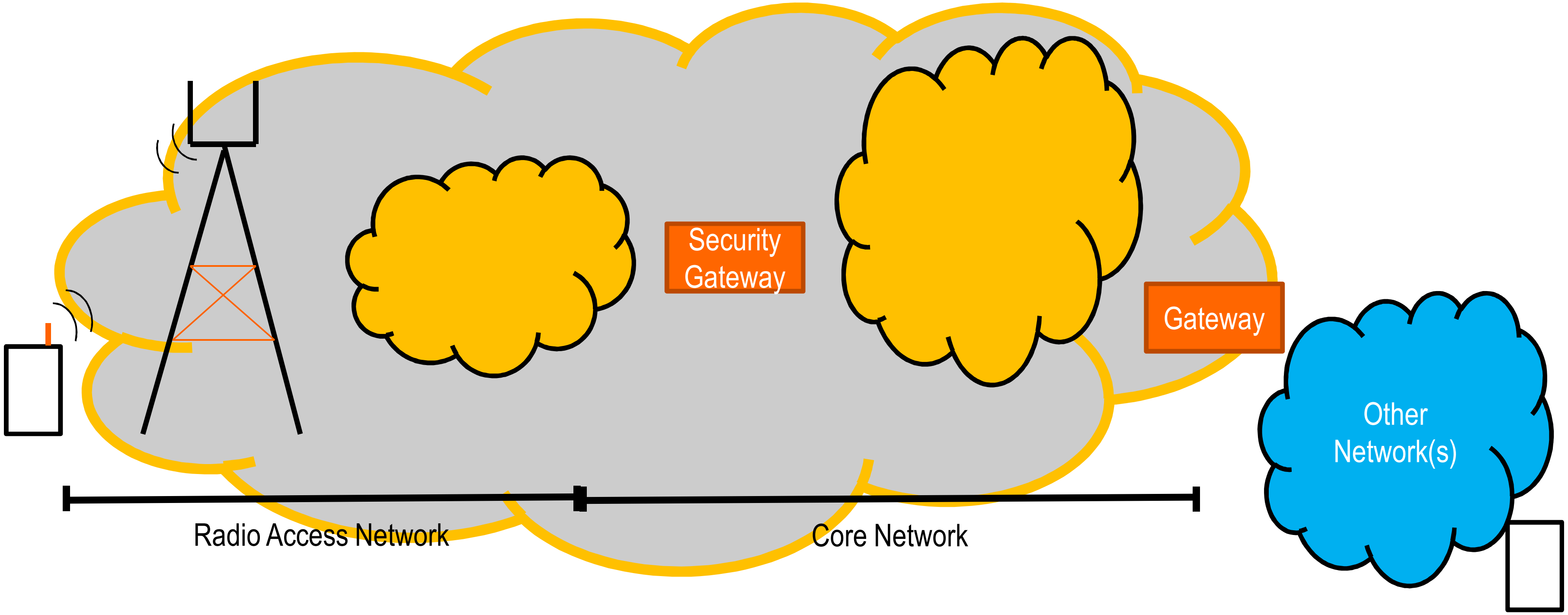
3GPP process

- Input
  - Contribution driven
  - Textual modifications to specifications
  - Member company contributions
- Consensus
  - Lack of sustained objection
  - Voting: more than 71% in favour

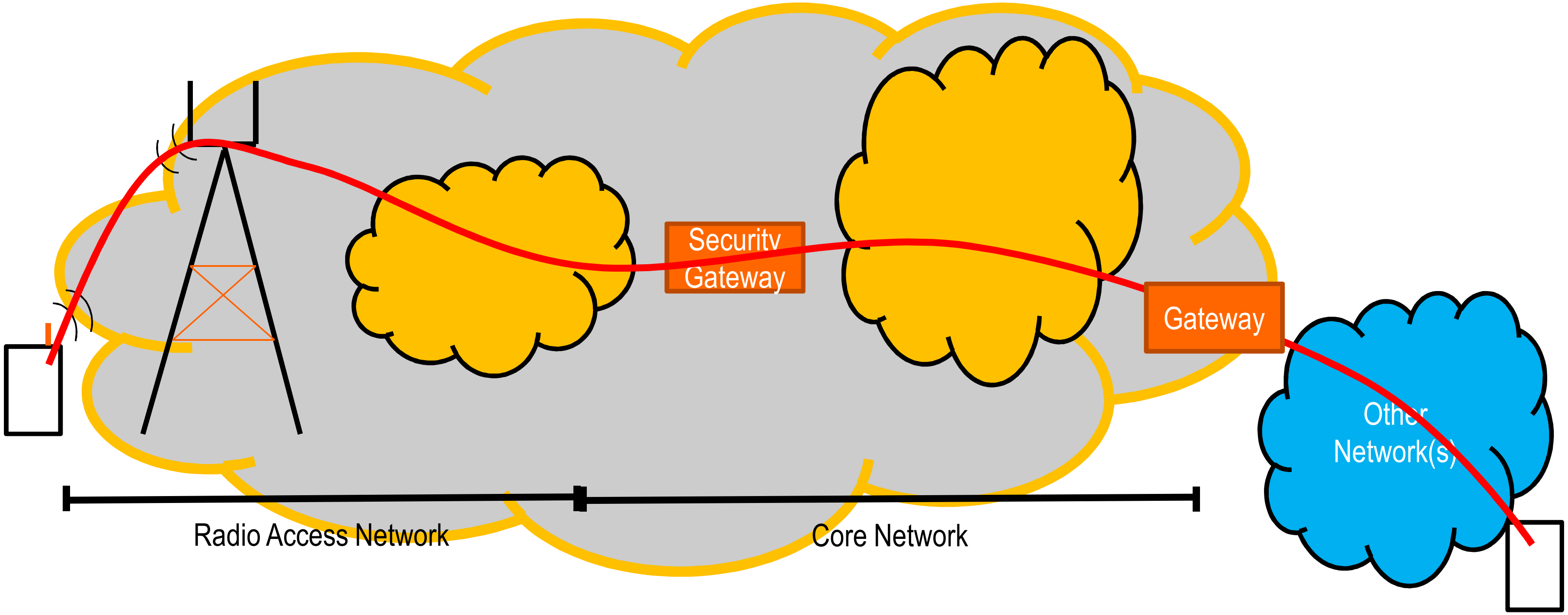
Agenda

- 5G Standardization Process
- **5G Architecture**
- 5G's Security Goals
- 5G Key Enhancements
- Summary

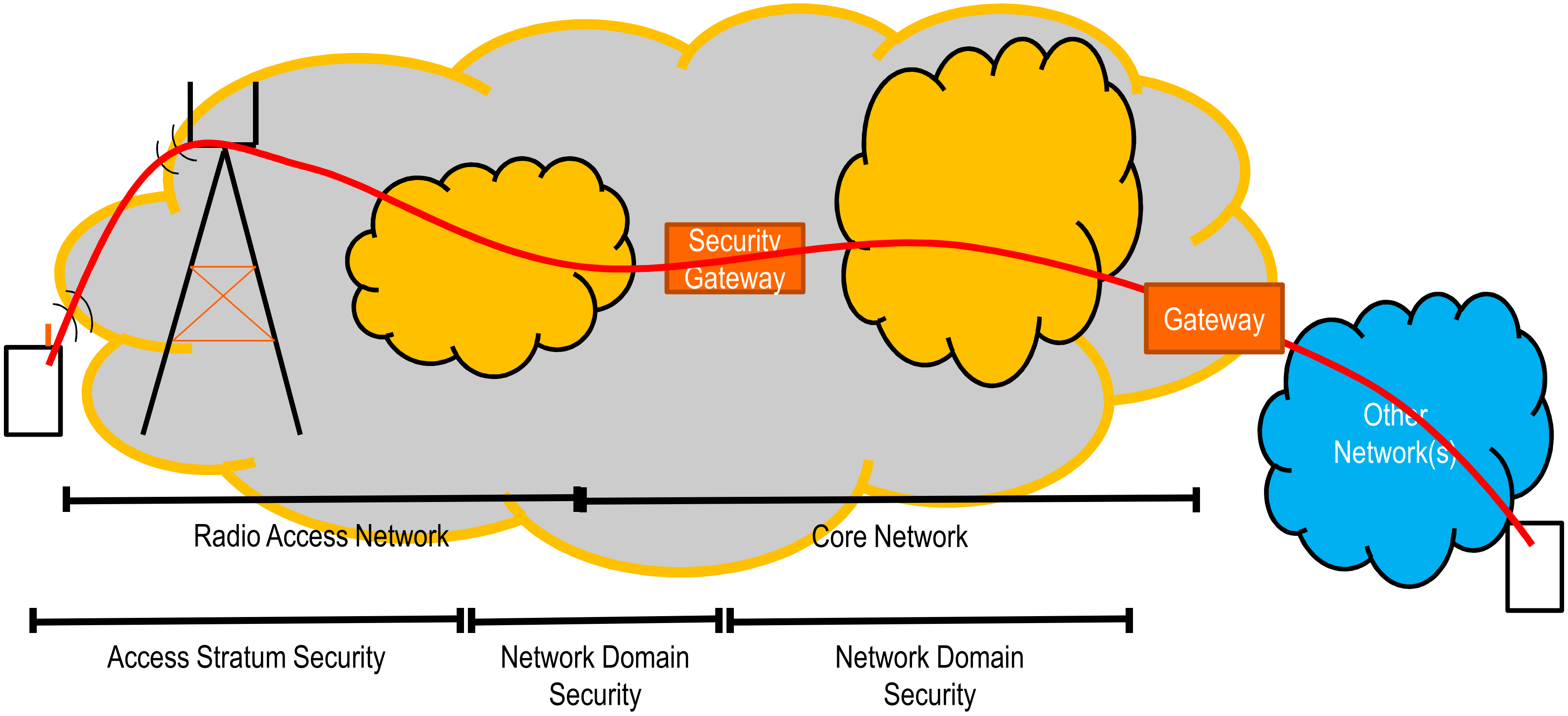
Mobile Network Architecture in a Nutshell



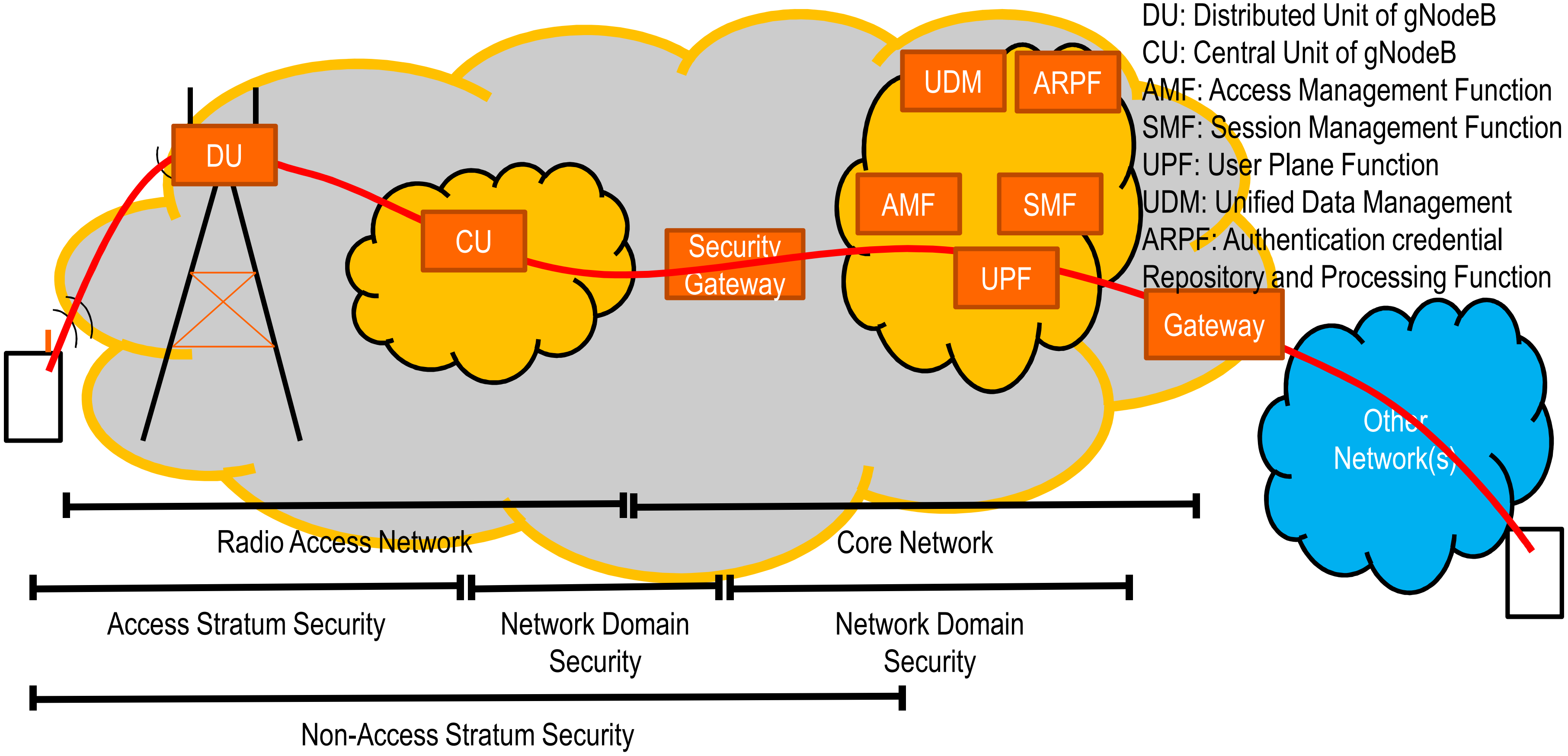
Mobile Network Architecture in a Nutshell



Mobile Network Architecture in a Nutshell

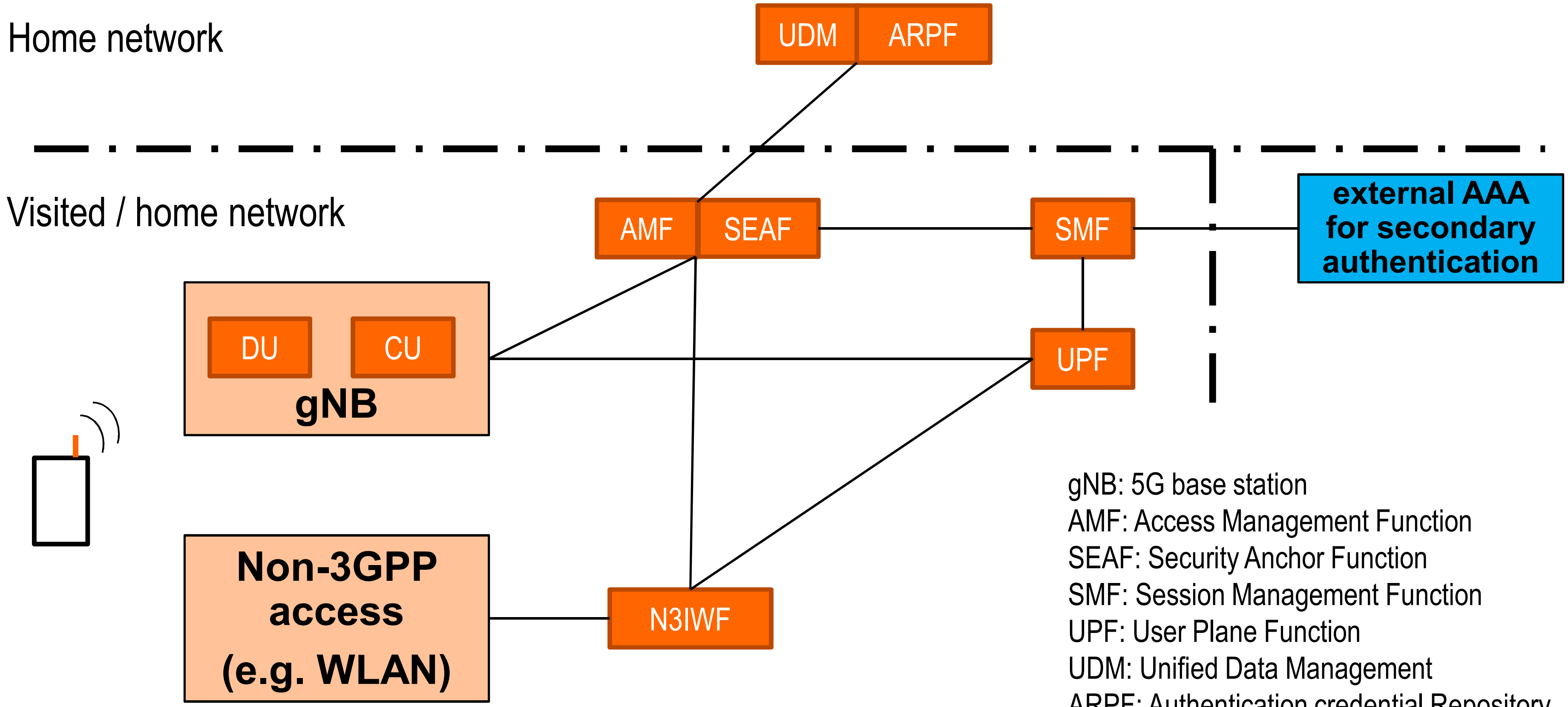


5G Mobile Network Architecture in a Nutshell



DU: Distributed Unit of gNodeB
CU: Central Unit of gNodeB
AMF: Access Management Function
SMF: Session Management Function
UPF: User Plane Function
UDM: Unified Data Management
ARPF: Authentication credential Repository and Processing Function

5G Mobile Network Architecture


Home network
UDM
ARPF
Visited / home network
AMF
SEAF
SMF
external AAA for secondary authentication
DU
CU
gNB
UPF
Non-3GPP access (e.g. WLAN)
N3IWF

gNB: 5G base station
AMF: Access Management Function
SEAF: Security Anchor Function
SMF: Session Management Function
UPF: User Plane Function
UDM: Unified Data Management
ARPF: Authentication credential Repository and Processing Function
N3IWF: Non-3GPP InterWorking Function

RAN architecture option

- Non standalone with 4G core

- Dual Connectivity
- 5G NR to increase capacity

- eNB as master node
- gNB as secondary node

- Security as in 4G

Agenda

- 5G Standardization Process
- 5G Architecture
- **5G's Security Goals**
- 5G Key Enhancements
- Summary

5G Security Goals

- At least as good as 4G
  - Subscriber authentication
  - Encryption on radio interface
  - Protection of subscriber identity
  - Network authentication
  - Key separation

  - Good for homogenous security requirements
    - Same security applied to all users and services

- Make it better
  - Evolution instead of revolution

5G Security Goals

- Fix known weaknesses
  - Some of them
- Provide unified framework for authentication
- Enable secondary authentication for applications

- Network and service flexibility

Agenda

- 5G Standardization Process
- 5G Architecture
- 5G's Security Goals
- **5G Key Enhancements**
- Summary

SUPI (IMSI) Privacy

- 4G
  - Initial attach with permanent identity
  - Response to identity request in clear
- 5G
  - Encryption of SUPI with public key of home operator (SUCI)
  - Routing information (home network ID) in clear
  - SUPI revealed to VPLMN only after authentication
  - Binding of SUPI into key
    - UE and HPLMN have to use the same SUPI: requested for lawful intercept purposes
  - Respond to identifier request with SUCI
  - No SUPI based paging

More Privacy

- Service request messages
  - Network may have lost UE keys
  - UE sends in clear only information for locating security context
  - → Initial NAS protection

- Reallocation of temporary IDs
  - After security set up
  - On every periodic mobility registration update
  - After use in paging

Unified Security Framework

- Credential storage on secure hardware (UICC)

- Access via 3GPP radio and non-3GPP radio

- Authentication
  - EAP AKA' for 3GPP and non 3GPP
  - Native AKA for 5G access

- One security context for both access technologies

Radio Network Security

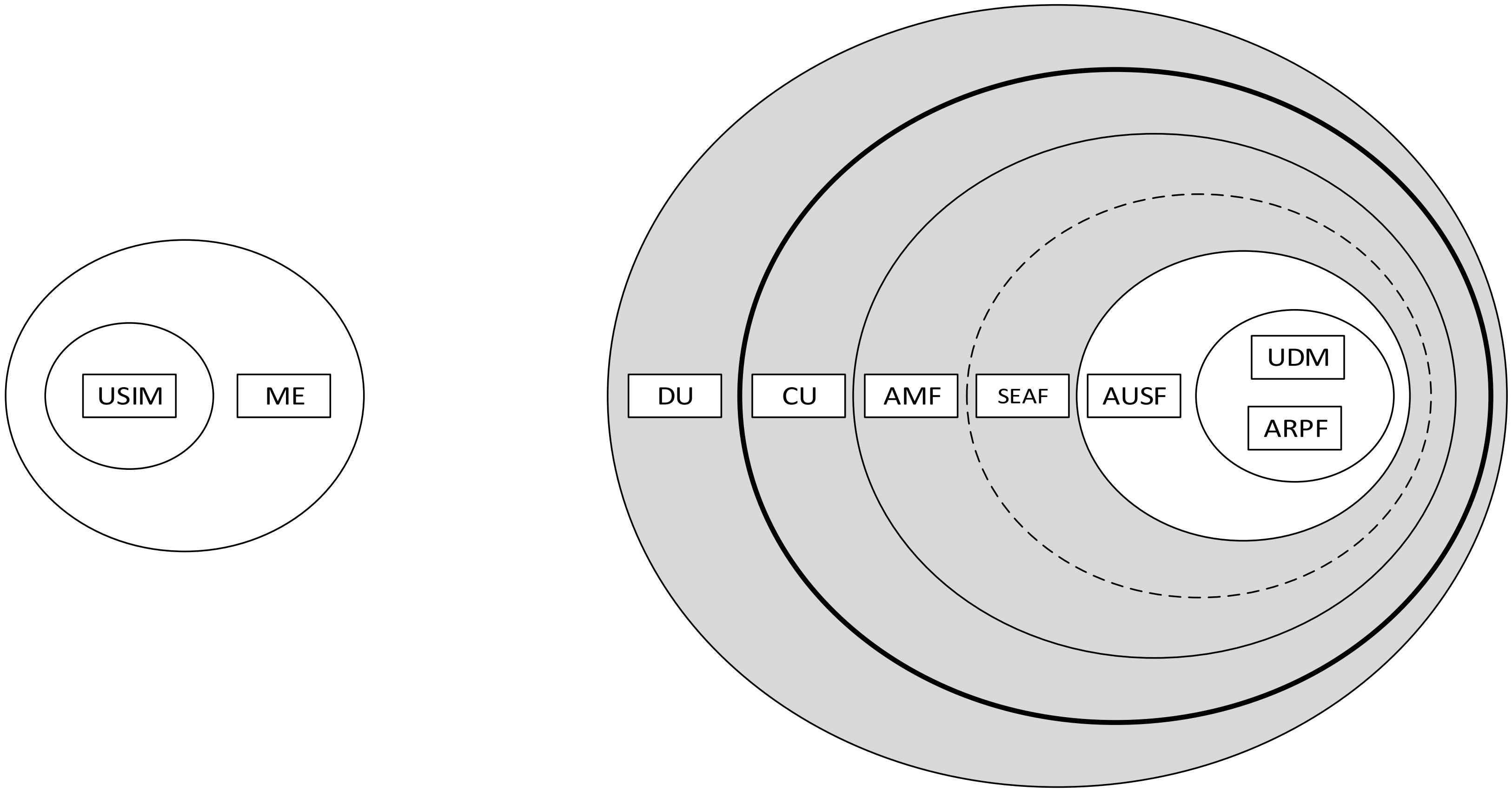
- Integrity protection
  - Finally!
- Split of gNB into Central and Distributed Unit (CU/DU)
  - CU performs security functions (confidentiality/integrity)
  - Can be located closer to the core
- Visibility
  - Requirement to enable applications to check security being applied to the connection

Increased home network control

- Proof of presence
  - UE is in visited network
- Native to EAP AKA
- 5G AKA
  - Challenge Response with UE
  - Visited network receives hash of response
  - Response has to be forwarded to home network
- Linking of subsequent procedures
  - Registration procedure only accepted after successful authentication

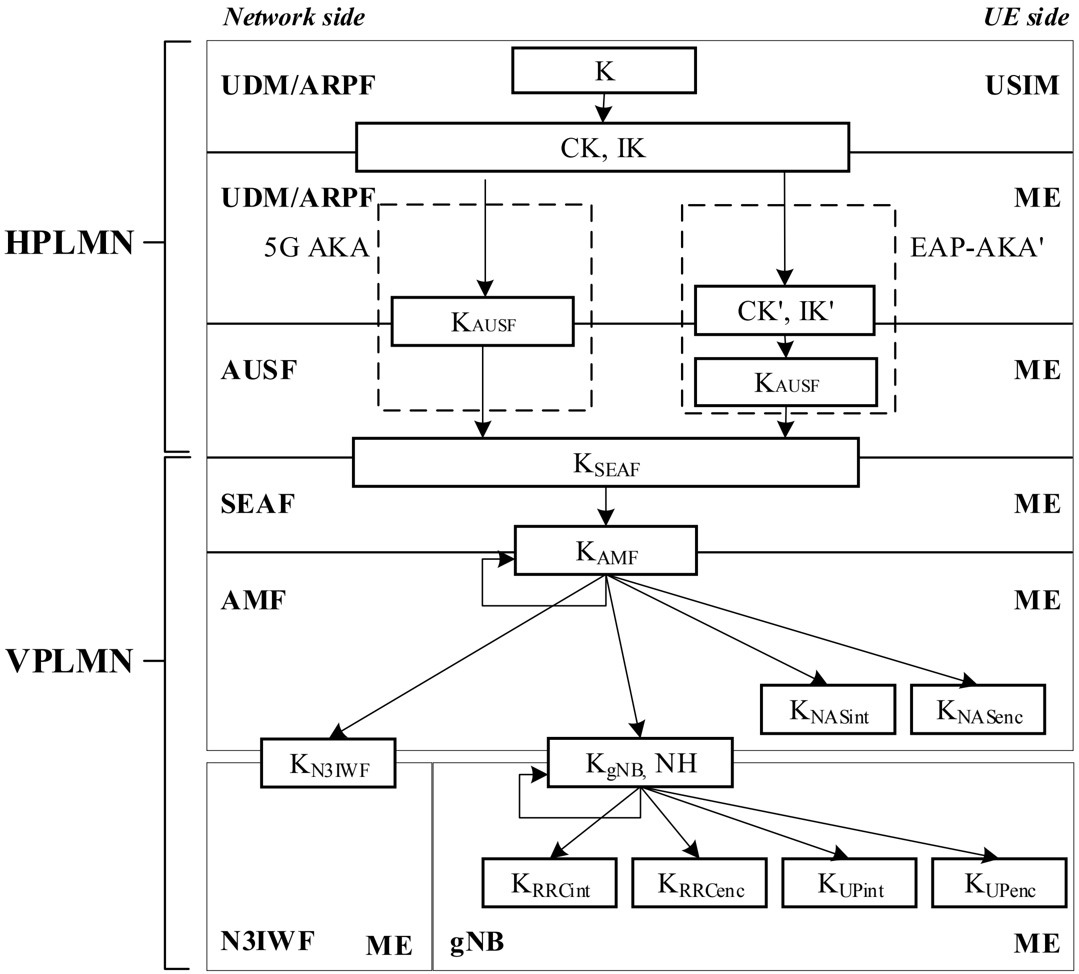
Trust model – non roaming

- **Separation of AMF (mobility) and SEAF (security)**

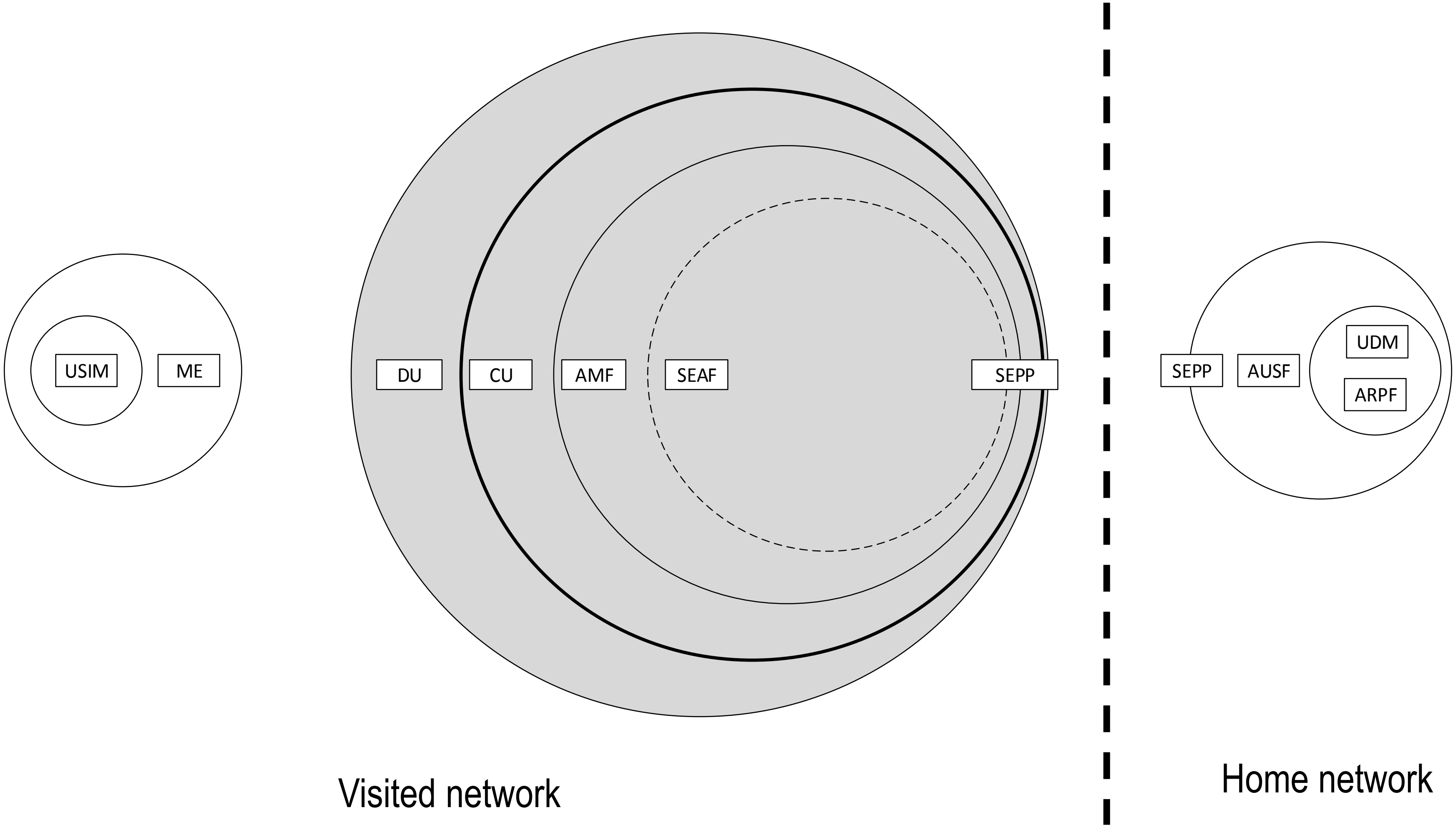


Key hierarchy

- Key separation between trust domains
- Future proofing: bid down protection by ABBA parameter in K_{AMF} derivation



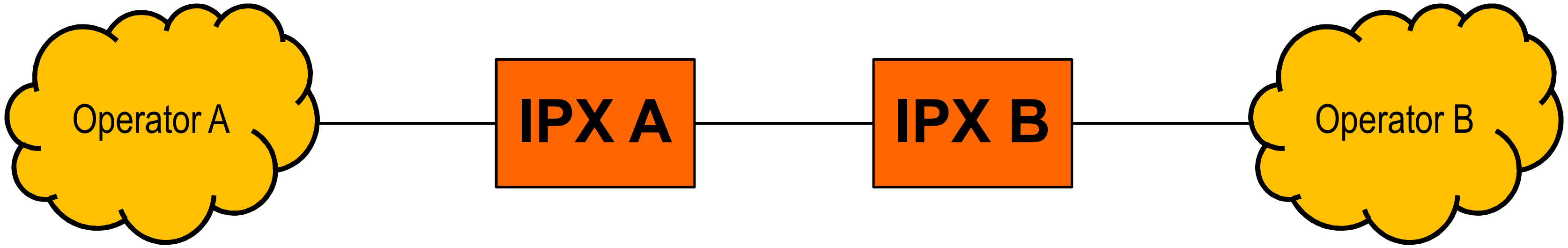
Trust model - roaming



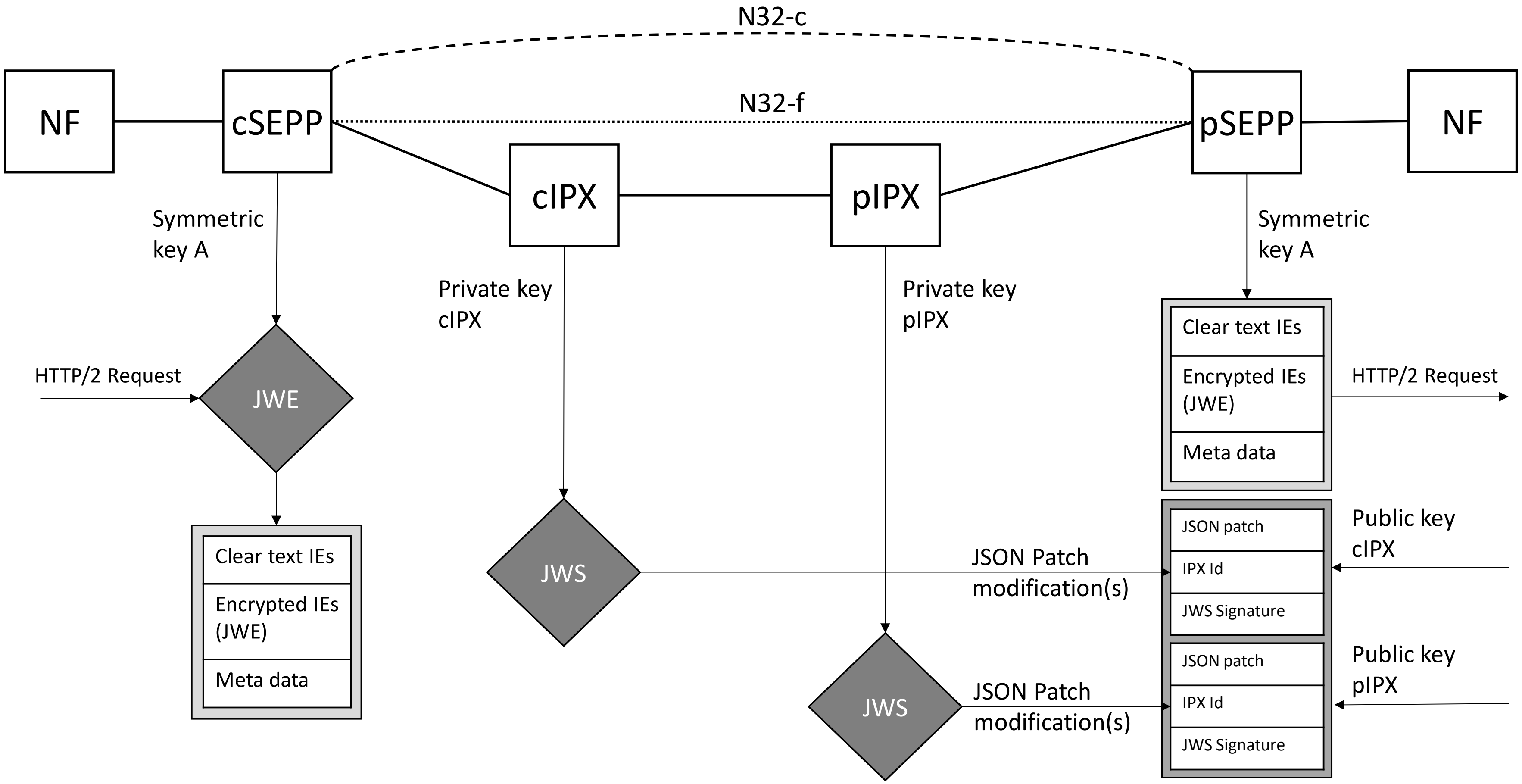
Requirements for Interoperator Interconnect

- End to end confidentiality and integrity
- Authenticity of the sending network

- Support addition, deletion, modification of information elements by intermediate nodes



Security for Interoperator Interconnect



Steering of Roaming

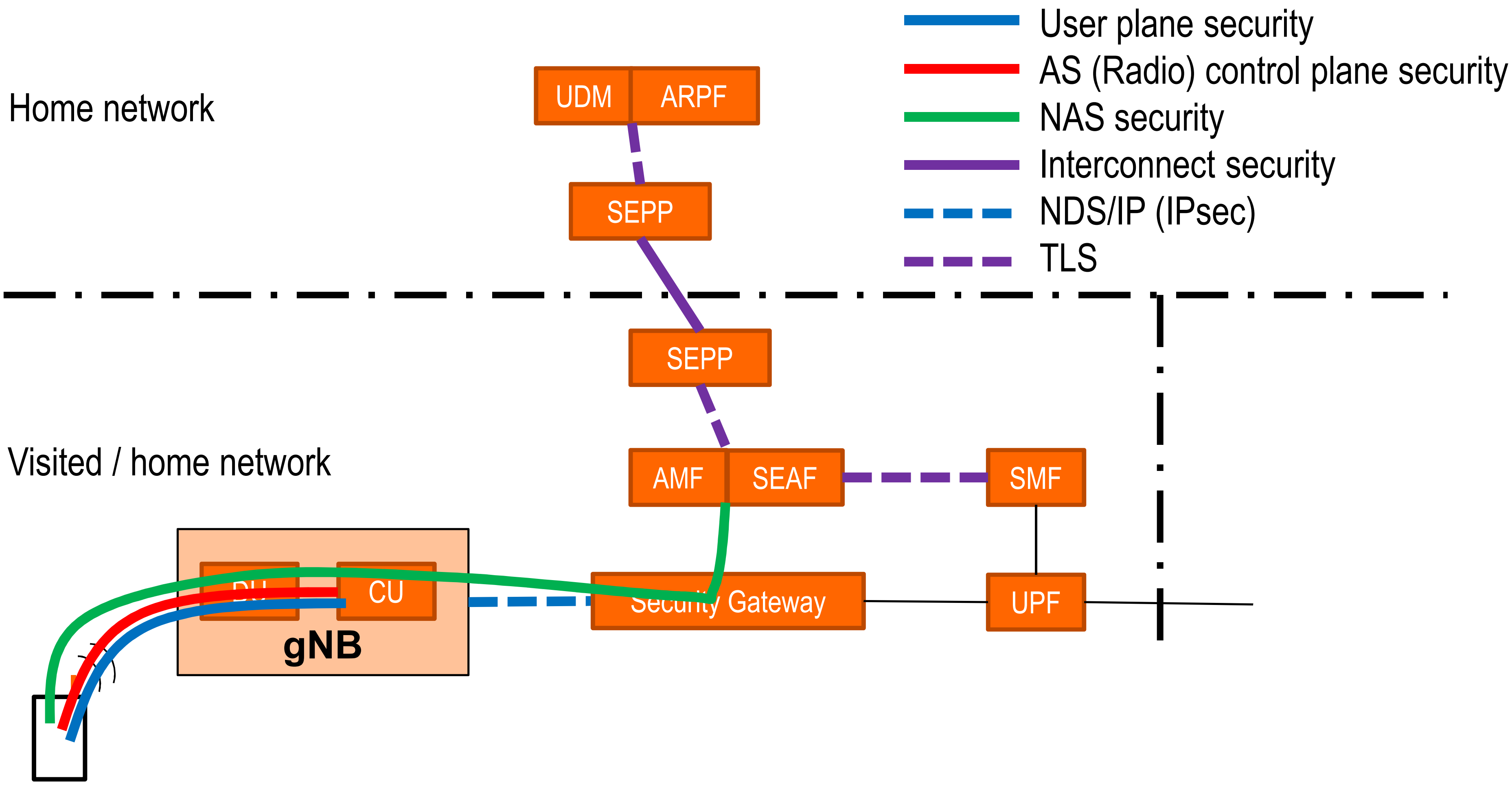
- UE connects to "best" network
- Home operator may want to reconfigure UE about "best"

- Inclusion of steering list in registration accept
- Optional confirmation

Agenda

- 5G Standardization Process
- 5G Architecture
- 5G's Security Goals
- 5G Key Enhancements
- **Summary**

5G Security Architecture



Home network

UDM ARPF

SEPP

SEPP

Visited / home network

AMF SEAF

SMF

DU CU

gNB

Security Gateway

UPF

- User plane security
- AS (Radio) control plane security
- NAS security
- Interconnect security
- NDS/IP (IPsec)
- TLS

Summary

- Evolution of 4G security

- More privacy
- Unified security framework
- RAN security
  - Integrity
  - Security termination point
- Future proofing
- Interconnect Security

Thank you for your attention