5G Standardization, 5G Security Enhancements, and Supporting Infrastructure Security Considerations.

National Institute of Standards and Technology
U.S. Department of Commerce

Jeff Cichonski
Information Technology Laboratory
NIST

Foundational Standards Developing Organizations

Internet Engineering Task Force

Internet Protocols

- TCP/IP, TLS, IPSEC

3rd Generation Partnership Program

Cellular Systems

- 3G, LTE, VOLTE, 5G

European Telecommunications Standards Institute

Virtualization Standards

ICT Standards

Institute of Electrical and Electronics Engineers

802.11 – WiFi

5G Related work

3GPP Overview

- 3GPP is a global initiative responsible mobile communications specifications.
- 3GPP partners with regional SDO organizations (ETSI, ARIB, ATIS, CCSA, etc.) to set cellular telecommunications standards.

TLDR; 3GPP wrote (is writing) the technical specifications for 5G, defining interoperable interfaces, protocols, and security features.

3GPP Overview Cont.

- 3 overarching groups – Radio Access Network (RAN), Service and System Aspects (SA), and Core Network and Terminals (CT)
- Each group has a plenary group associated responsible for setting priorities, timelines, coordination

Radio Access Network (RAN)	Service & Systems Aspects (SA)	Core Network & Terminals (CT)
RAN 1 - Radio Layer 1 (Physical)	SA 1 - Services	CT 1 – User equipment & Core network radio protocols
RAN 2 - Radio Interface architecture and protocols	SA 2 - Architecture	CT 3 - Interworking between a 3GPP networks and external nodes or networks
RAN 3 - Radio architecture and Interface protocols	**SA 3 - Security**	CT 4 – Core network aspects
RAN 4 - Radio performance and protocol aspects	SA 4 - Codec	CT 6 – Smart card application aspects (SIMS)
RAN 5- Mobile terminal conformance testing	SA 5 - Telecom Management	
	SA 6 – Mission Critical	

3GPP Overview Cont.

- The RAN groups are responsible for the definition of the functions, requirements and interfaces of the Radio Network
- The SA groups are responsible for the overall architecture and service capabilities of systems based on 3GPP specifications.
- The CT groups are responsible for specifying terminal interfaces (logical and physical), terminal capabilities (such as execution environments) and the Core network part of 3GPP systems.
- 3GPP works using a three-stage methodology that is applied in 3GPP as follows;
  - Stage 1 is an overall service description from the user's standpoint.
  - Stage 2 is an overall description of the organization of the network functions to map service requirements into network capabilities.
  - Stage 3 is the definition of switching and signaling capabilities needed to support services defined in stage 1.

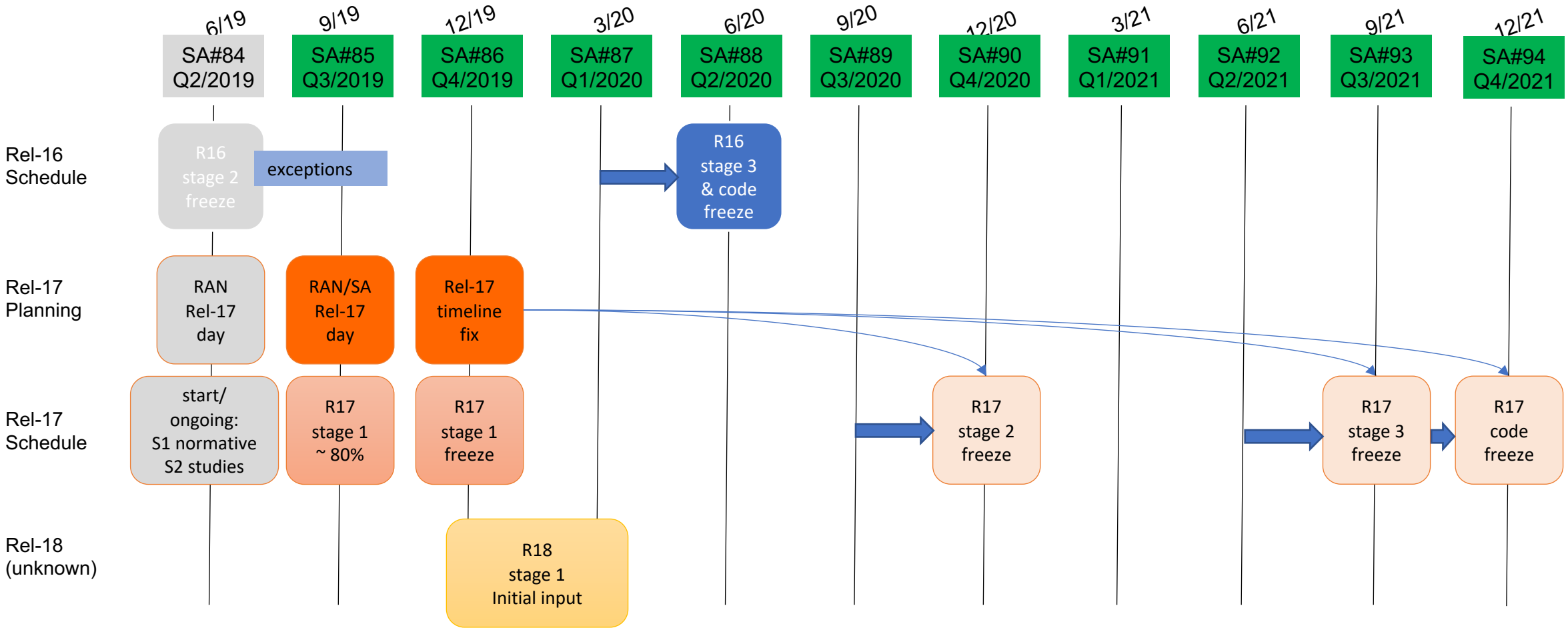
3GPP Working Groups

Radio Access Network (RAN)	Service & Systems Aspects (SA)	Core Network & Terminals (CT)
RAN 1 - Radio Layer 1 (Physical)	SA 1 - Services	CT 1 – User equipment & Core network radio protocols
RAN 2 - Radio Interface architecture and protocols	SA 2 - Architecture	CT 3 - Interworking between a 3GPP networks and external nodes or networks
RAN 3 - Radio architecture and Interface protocols	**SA 3 - Security**	CT 4 – Core network aspects
RAN 4 - Radio performance and protocol aspects	SA 4 - Codec	CT 6 – Smart card application aspects (SIMS)
RAN 5- Mobile terminal conformance testing	SA 5 - Telecom Management	
	SA 6 – Mission Critical	

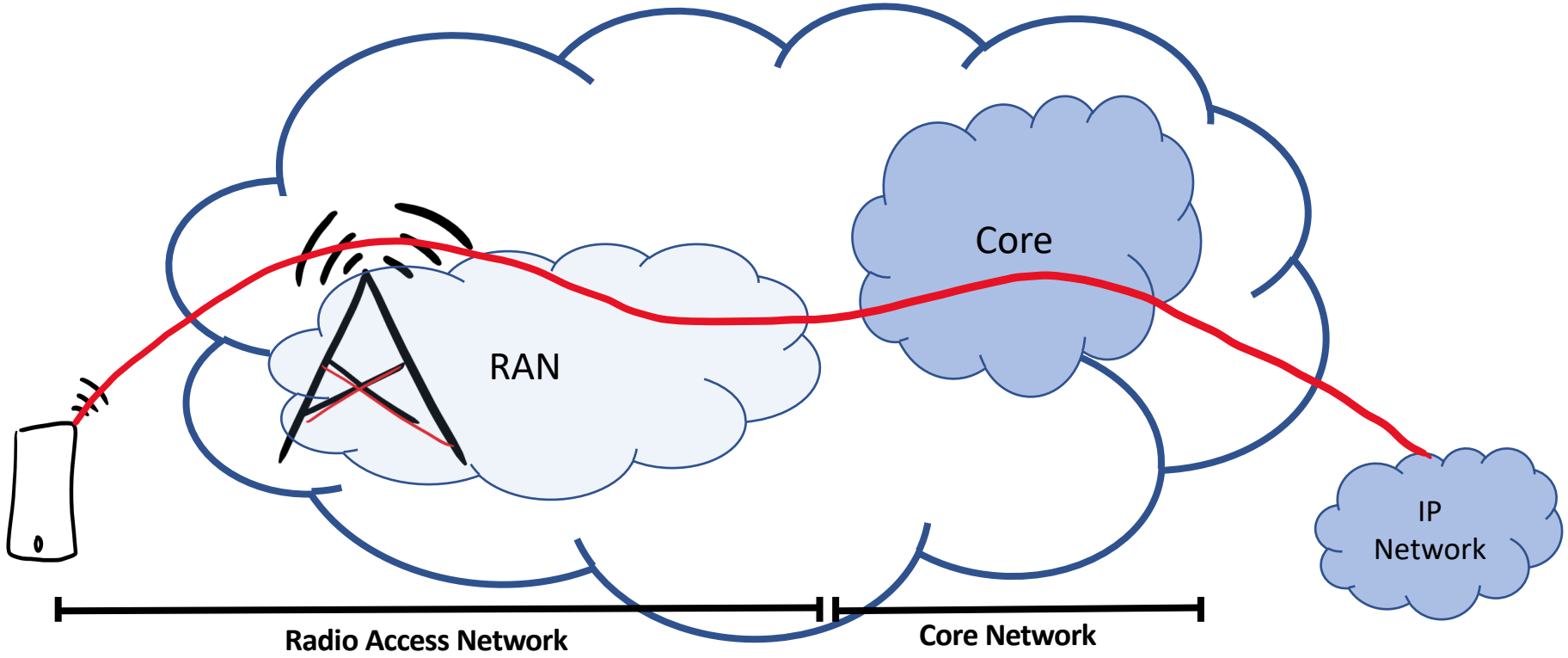
3GPP Process (SA3 Perspective)

- General approach: Study document (TR), followed by technical specifications (TS)
  - TR analyzes security issues and potential solutions
  - TS presents definitive solutions
  - Leverages protocols from other SDOs (e.g. IETF, IEEE)
- Iterative pipeline
  - SA3 (security) defines solutions based on SA1's requirements and SA2's architecture (for Mission Critical, SA6's architecture)
  - Tight timelines require groups to work in parallel and re-work or add to solutions as needed
- SA3's security solutions are concretized by CT1
  - Optimal/feasible solutions require back-and-forth between SA3 and CT1
- Consensus process
  - Resorting to a vote is rare, viewed as a process failure

Current 3GPP Timeline

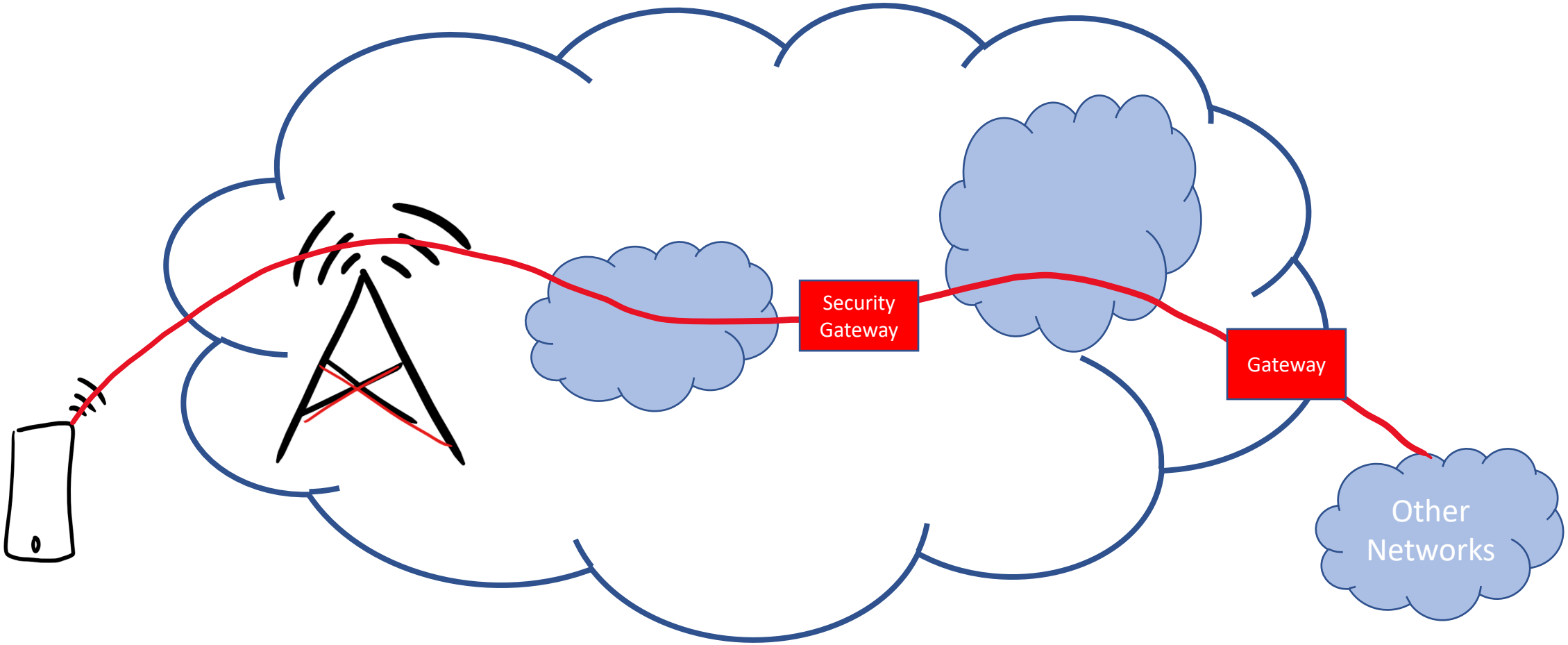


Mobile Network – The Basics

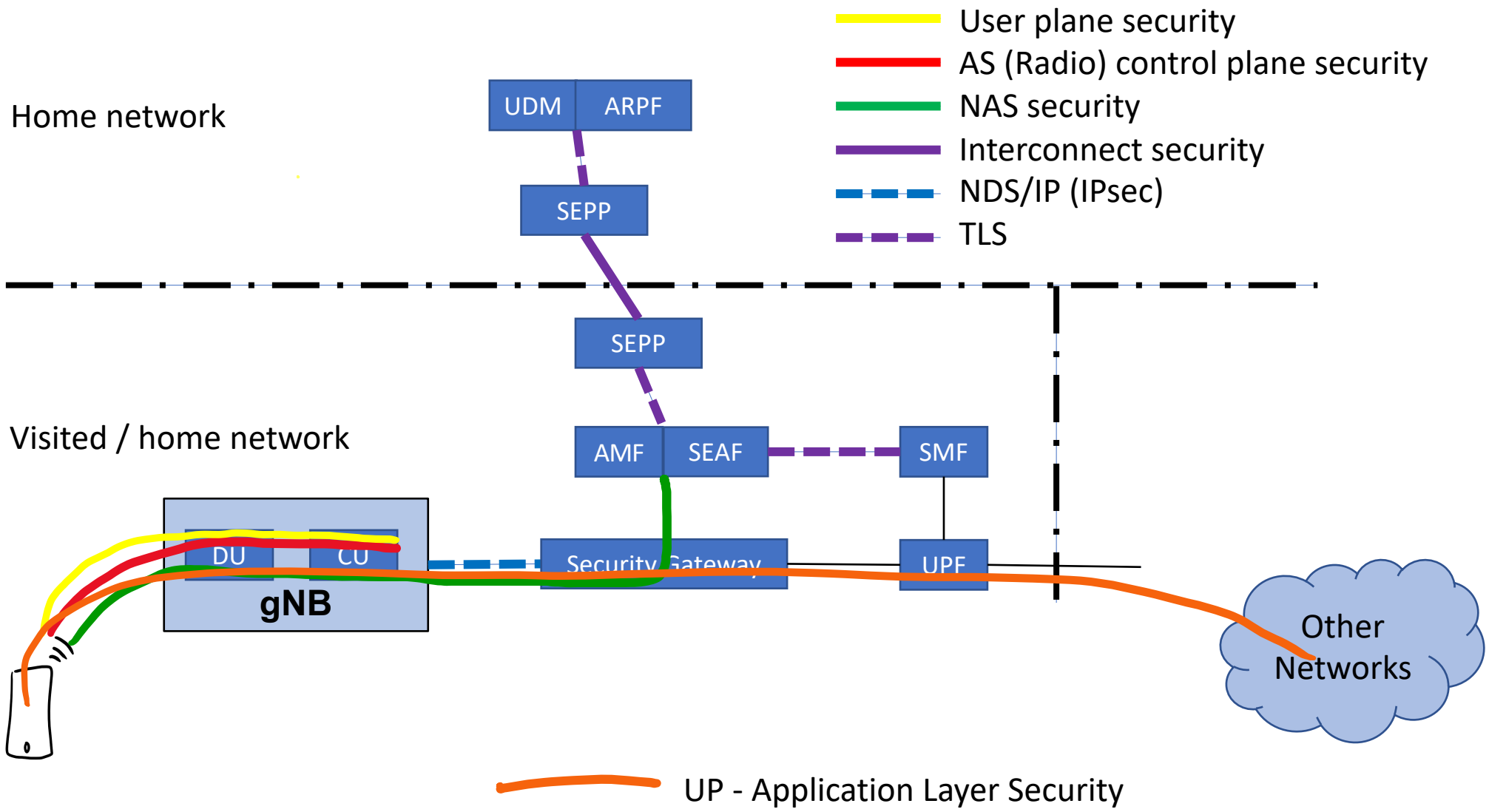


- A device connects to a network of base stations or Radio Access Network (RAN)
- The RAN connects to a 3GPP Packet Core (Core)
- The Packet Core provides connectivity to the internet or other IP network.

Mobile Network Security



5G System Security Architecture



Known Security Issues With LTE

- Subscriber tracking
- No user plane integrity protection
- Roaming issues (SS7 & diameter threats)
- False Base stations

New Security Features

- User Plane Traffic Integrity
- Subscriber Privacy
- Security Edge Protection Proxy
- Increased Home Control
- Unified Authentication Framework
- CU / DU Separation

Radio Network Security

Integrity protection for user plane

- Finally!
- Control plane integrity protection was available since UMTS

Split of gNB into Central and Distributed Unit (CU/DU)

- CU performs security functions (confidentiality/integrity)
  - AS (air interface) security terminates at the CU.
- Can be located closer to the core

Visibility

- Requirement to enable applications to check security being applied to the connection

5G Privacy Protections

Objectives;

- Protect permanent identifiers
- Cycle temporary identifiers regularly
- Avoid re-authentication

Outcomes;

- 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
- Respond to identifier request with SUCI
- No SUPI based paging
- Reallocation of temporary Ids after security set up, on every periodic mobility registration update and after use in paging

5G Authentication Framework Enhancements

Credential storage on secure hardware (UICC)

- Allows the use of integrated secure element (e.g. integrated UICC)

Same Primary authentication method can be used over both 3GPP & non-3GPP access

- WiFi / fixed broadband networks
- N3IWF – Non-3GPP Interworking Function

One security context for both access technologies

Native EAP support over 3GPP access networks

- Enables operator to plug-in different credentials and authentication methods without impacting other intermediate network functions

Optional EAP based secondary authentication for access to specific data networks/services

- Allows applications to use their own credentials & authentication before allowing access to their dedicated application/service specific data networks (e.g., Amazon, Facebook, Enterprises)

Beyond the 3GPP System

- 5G networks are comprised of many components utilizing different modern information technologies
- 3GPP Network Functions are ONLY one piece of the evolution to 5G deployments
- Cybersecurity best practices used for the various components of the technology stack

Supporting Infrastructure and Security Protocols

- Cloud computing platforms
  - Virtualization
  - Containerization
  - Orchestration
- Internet security protocols
  - IPSec
  - TLS
  - JOSE, etc.

Questions / Comments?