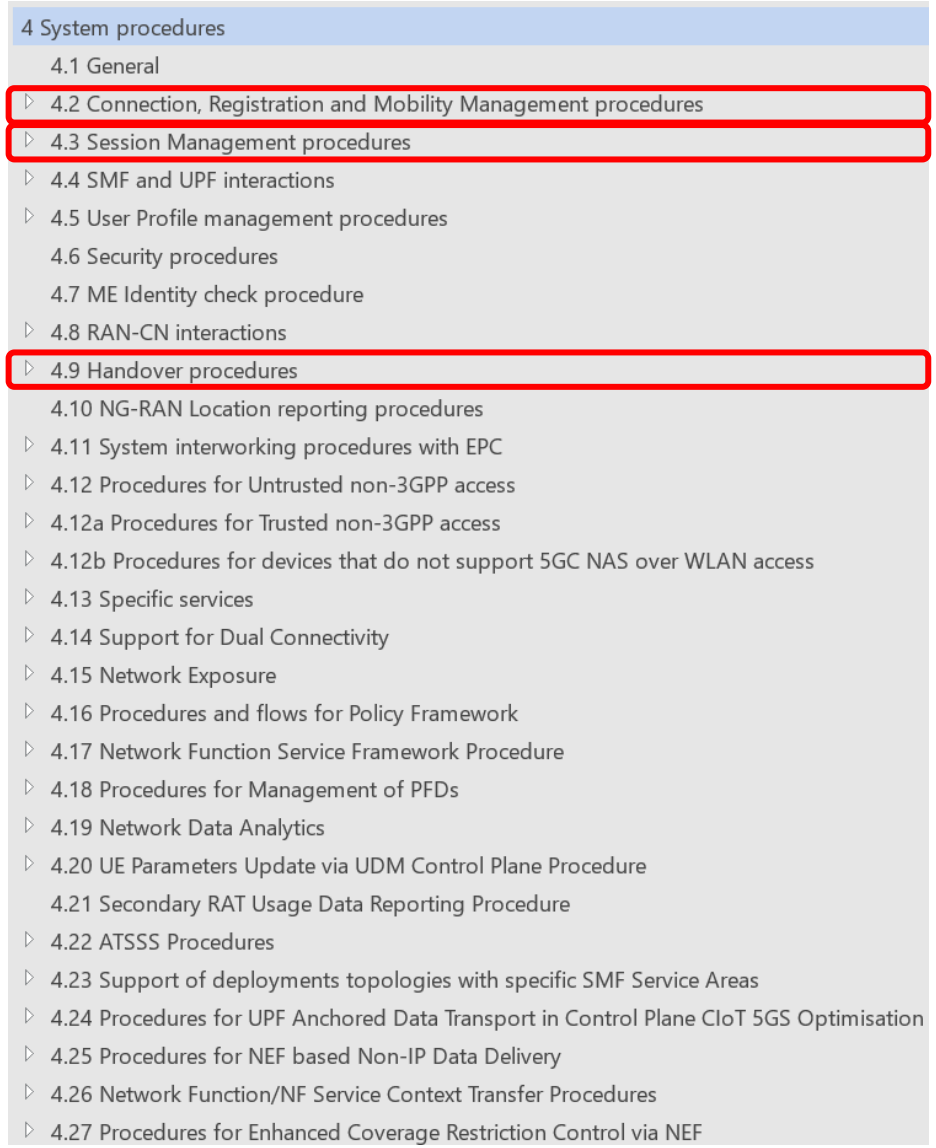
# Steps to connect to network
# UE states
# QoS Model
# Main 5G PDU Procedures

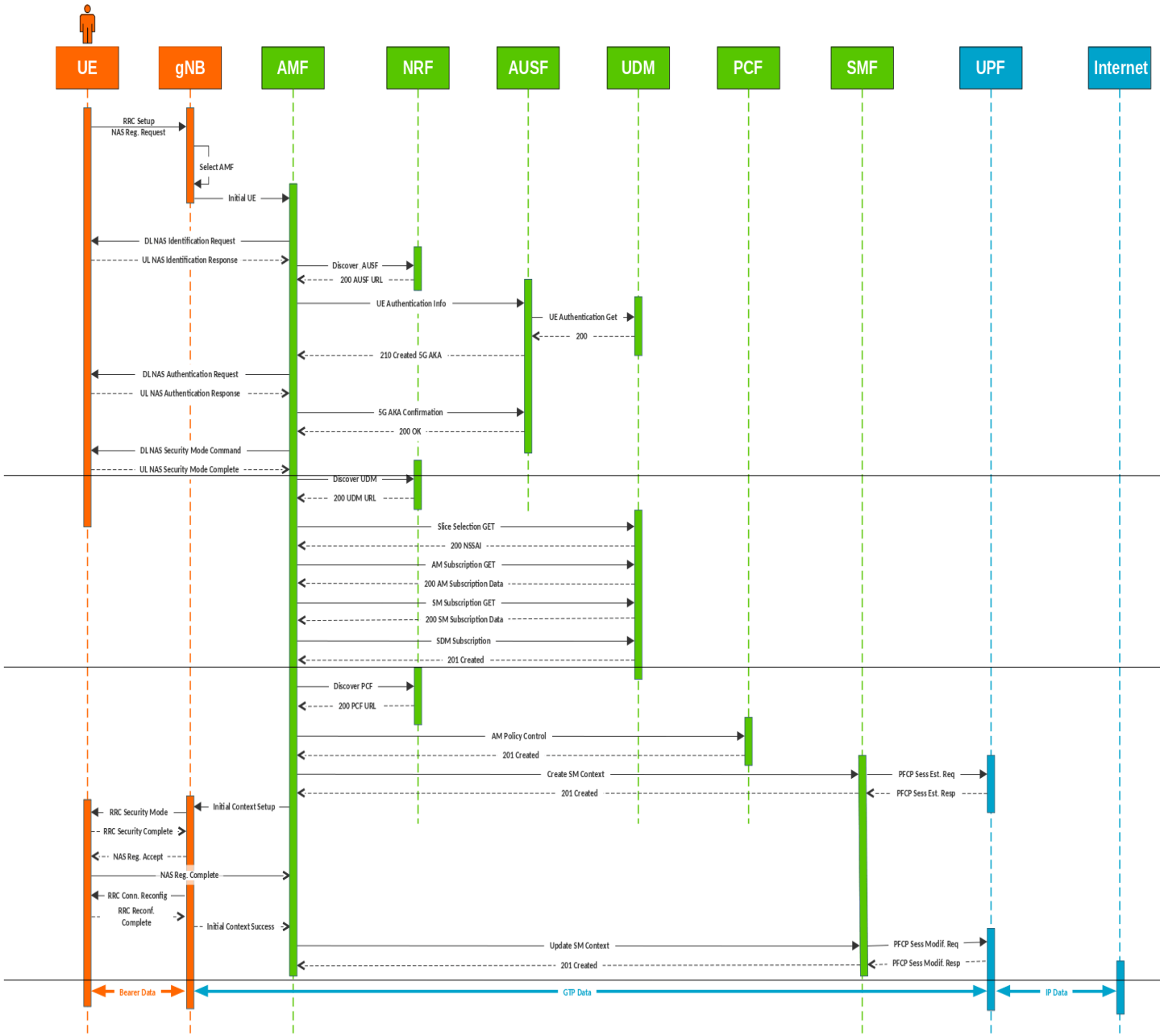
# 5G Core Procedures

**3GPP, TS 23.502, "Procedures for the 5G System (5GS)"**




1. **Connection, Registration and Mobility Management procedures**
2. **Session Management**
   1. **PDU Session Establishment**
   2. **PDU Session Modification**
   3. **PDU Session Release**
   4. **Session continuity, service continuity and UP path management**
3. **Handover procedures**

# 5G Standalone Registration




**Initialization & Authentication**

**Applicable Slices selection**

**PDUs establishment**

**Data session**

# Steps to achieve a data connection (PDU session)

## 1. Power-On and Initialization (UE)

- **Hardware Boot-Up**: Initializes baseband processor, RF front-end, memory, sensors, and GNSS
- **USIM Access**: Reads SUPI, PLMN lists, access class info, and subscription data
- **Protocol Stack Initialization**: Activates NR Layer 1–3, NAS, and RRC layers

## 2. PLMN Selection (UE ↔ gNB)

- **Automatic or Manual**: UE selects a *Public Land Mobile Network* (PLMN) either autonomously or via user input
- **SIB1 Decoding**: UE reads broadcast PLMN info from *System Information Block* 1
- **Forbidden PLMN Check**: Skips previously failed networks
- **Roaming and Access Barring**: Evaluates roaming permissions and barred cells

## 3. Frequency and Cell Search (UE ↔ gNB)

- **Frequency Scan**: UE scans supported NR bands for *Synchronization Signal Blocks* (SSBs)
  - *Stored List Search (SLS)*: Uses previously stored frequencies
  - *Blind Search (DBS)*: Scans all bands if no prior info is available
- **SSB Detection/Decoding**: UE detects *Synchronization Signal Blocks* (PSS, SSS, PBCH) to identify cell identity and timing

# Steps to achieve a data connection (PDU session)

## 4. Cell Selection and Synchronization (UE ↔ gNB)

- **MIB and SIB Decoding**: UE decodes *Master Information Block* and other SIBs for cell configuration
- **Cell Suitability Check**: Determines if the cell is acceptable and suitable for camping
- **Initial Cell Selection**: Chooses the best cell based on signal strength and configuration

## 5. *Random Access Procedure* (RACH, *Random Access Ch.*) (UE ↔ gNB)

- UE performs contention-based access to establish initial connection
  - **MSG1**: PRACH (*Physical RACH*) Preamble (UE → gNB)
  - **MSG2**: *Random Access Response* (RAR) (gNB → UE)
  - **MSG3**: RRC *Connection Request* (UE → gNB)
  - **MSG4**: RRC *Connection Setup* (gNB → UE)
  - **RRC Connection Setup Complete** (UE → gNB)
- **Timing Advance and Resource Allocation**: gNB assigns uplink resources and timing correction

# Steps to achieve a data connection (PDU session)

## 6. Registration and Authentication (UE ↔ gNB ↔ AMF)

- **Initial NAS Registration Request** (UE → AMF via gNB); UE sends identity and registration info to 5G Core (5GC)
  - Includes UE identity (SUCI), capabilities, and registration type.
- **Authentication Request / Response** (AMF ↔ UE)
  - Based on AKA (Authentication and Key Agreement) using USIM.
- **Security Mode Command / Complete** (AMF ↔ UE)
  - Mutual authentication and ciphering/integrity protection are established
  - Establishes ciphering and integrity protection
- **Registration Accept / Complete** (AMF ↔ UE)
  - UE is now registered with the 5G Core

## 7. PDU Session Establishment (UE↔gNB↔AMF↔SMF↔UPF)

- **Session Request**: UE requests a *Protocol Data Unit* (PDU) session for data connectivity
  - **NAS: PDU Session Establishment Request** (UE → AMF)
  - Includes desired DNN, S-NSSAI, and session type
- **SM Procedures**: Session Management configures QoS, IP address, and bearer setup
  - **Radio Resources Management**: Activate Dedicated Bearer (**UE ↔ gNB)**
  - **IP Address Assignment**: UE receives IP address from the 5GC (SMF)

## 8. IP Connectivity Achieved

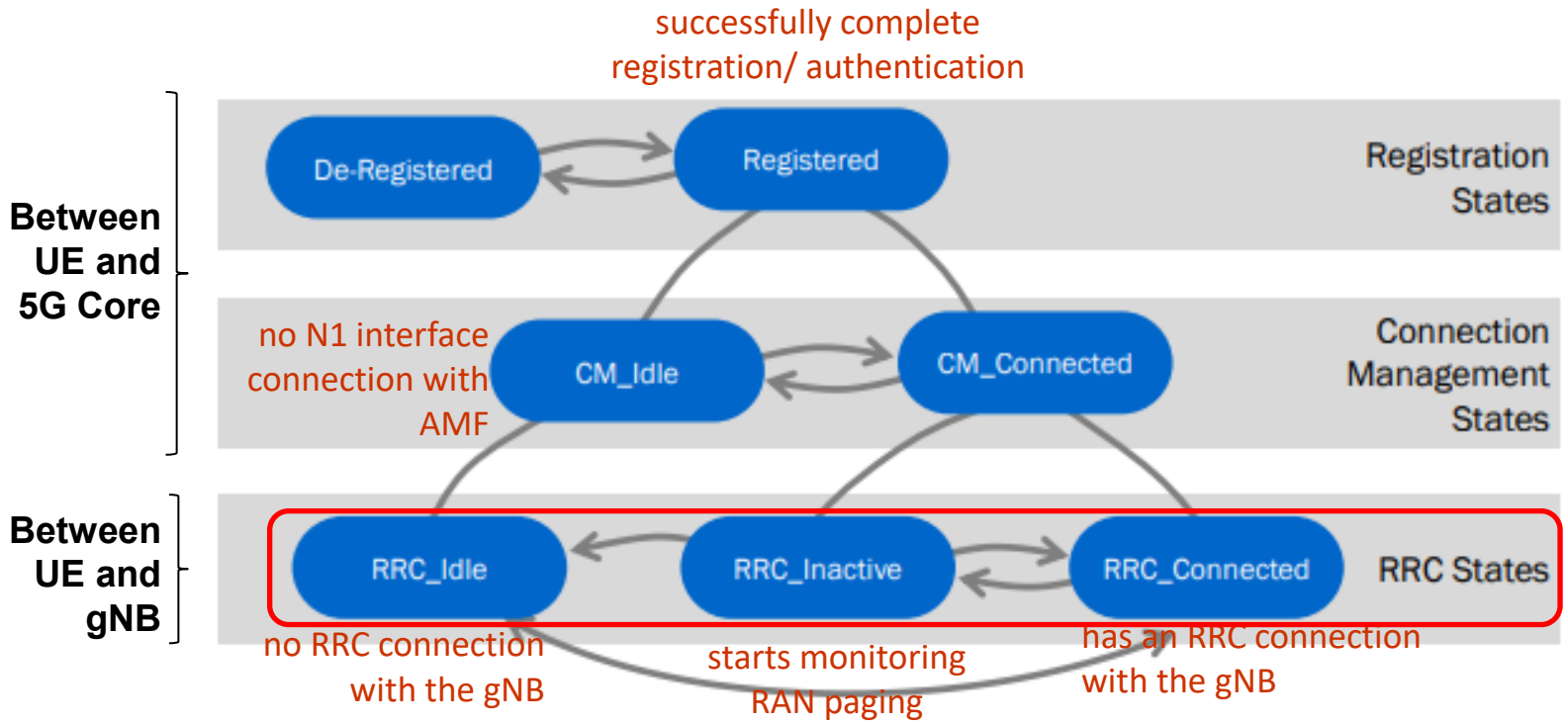
- **Data Flow Enabled**: UE can now send/receive IP packets over the 5G network, via the UPF
- DNS resolution, internet access, and app traffic begin
- **Application Layer Access**: Internet services, apps, and cloud resources become available

**This structured process ensures the UE is authenticated, resources and policies are provisioned, and the data path is configured end-to-end for secure and efficient 5G traffic**

# UE states in 5G: *Radio Resources Control* (RRC)

## The three RRC states

**They define the UE's connection status, power usage, and mobility management within the network.**




**RRC_IDLE:** the UE does not have an RRC connection and is in its lowest power-saving mode

- It monitors a paging channel and can perform cell reselection independently
- Mobility is controlled by the UE, and its location is known only at the level of a large *Tracking Area* (TA)

**RRC_INACTIVE:** This power-saving state is unique to 5G

- Allows the UE to minimize power consumption by entering a dormant mode while keeping a stored context with the network
- Enables a very fast and efficient return to the connected state when needed, reducing latency and signaling overhead

**RRC_CONNECTED:** the UE has an active connection and can send and receive data

- It is constantly monitored by the network, and its mobility is controlled by the RAN
- This state provides the highest performance but consumes the most power

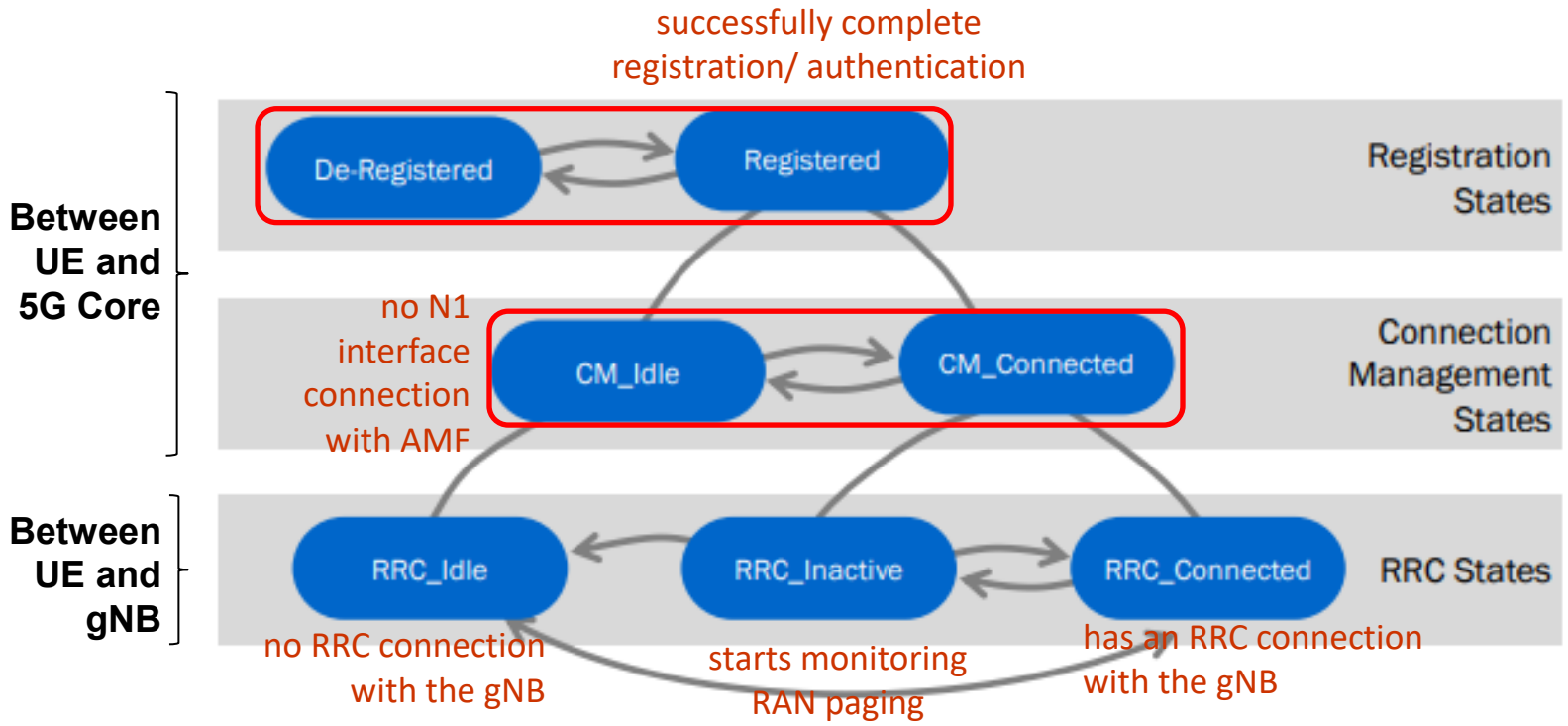
# UE states in 5G: *Registration and Connections Mgmt* (RM & CM)

### *Connection Management* (CM) states

- **CM_IDLE**: no *Non-Access Stratum* (NAS) connection with the core network)
- **CM_CONNECTED**: with an active NAS connection (A UE in RRC_INACTIVE is still seen as being in CM_CONNECTED by the core network)

### *Registration Management* (RM) states

- **RM-DEREGISTERED**: not registered with the 5G Core Network
- **RM-REGISTERED**: successfully authenticated and registered

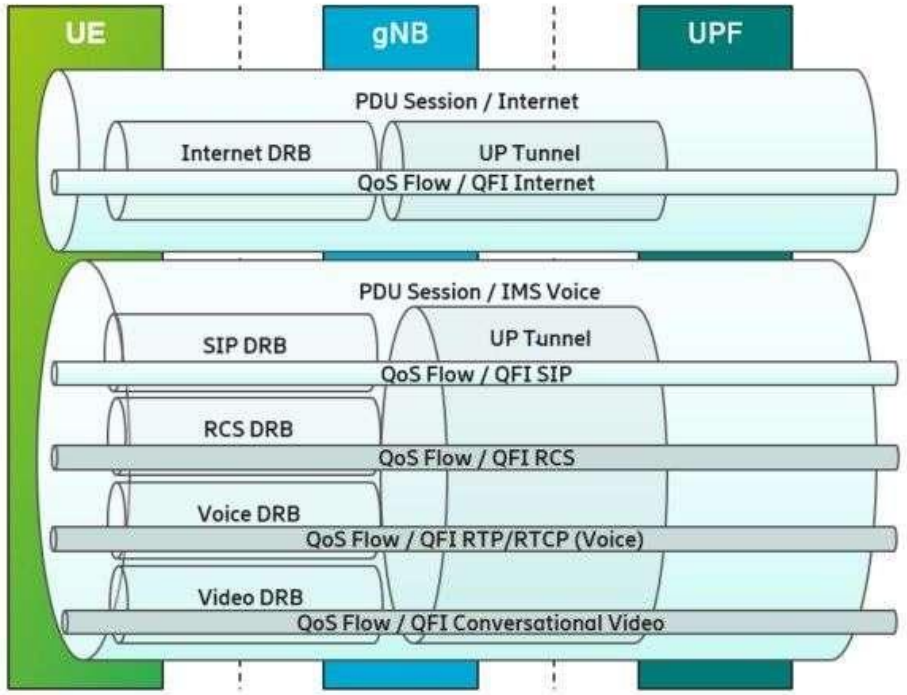



## RRC State transitions

- **Initial connection:** When the UE powers on, it starts in RRC_IDLE. It moves to RRC_CONNECTED via an "RRC Connection Setup" procedure.
- **From CONNECTED to INACTIVE:** If the UE has low data activity, the network can command it to transition to RRC_INACTIVE using an RRCRelease message.
- **From INACTIVE to CONNECTED:** The UE can resume its connection quickly by sending an RRCResumeRequest message, which uses its stored context.
- **From INACTIVE to IDLE:** This can happen if the resume procedure fails or the network releases the connection.

# 5G QoS

# PDUs and QoS Flows




**PDU Sessions**

- For each UE, the 5G Core Network (5GC) establishes one or more Protocol Data Unit (PDU) sessions for connectivity to a data network

**QoS Flows**

- Within a PDU session, one or more QoS Flows can exist, grouping packets with the same quality of service (QoS) requirements
- QoS flows are ***Guaranteed Bit Rate*** (GBR) or **non-GBR**
- The 5GC (UPF) and the UE use packet filters (based on IP addresses, port numbers, etc.) to map uplink and downlink traffic to the appropriate QoS Flow
- Each packet is marked with its unique *QoS Flow Identifier* (QFI) in the encapsulation header over the N3 interface (between gNB and UPF)
- A QoS Flow associated with the default QoS rule is required to be established for a PDU Session and remains established throughout the lifetime of the PDU Session; this QoS Flow should be a Non-GBR QoS Flow

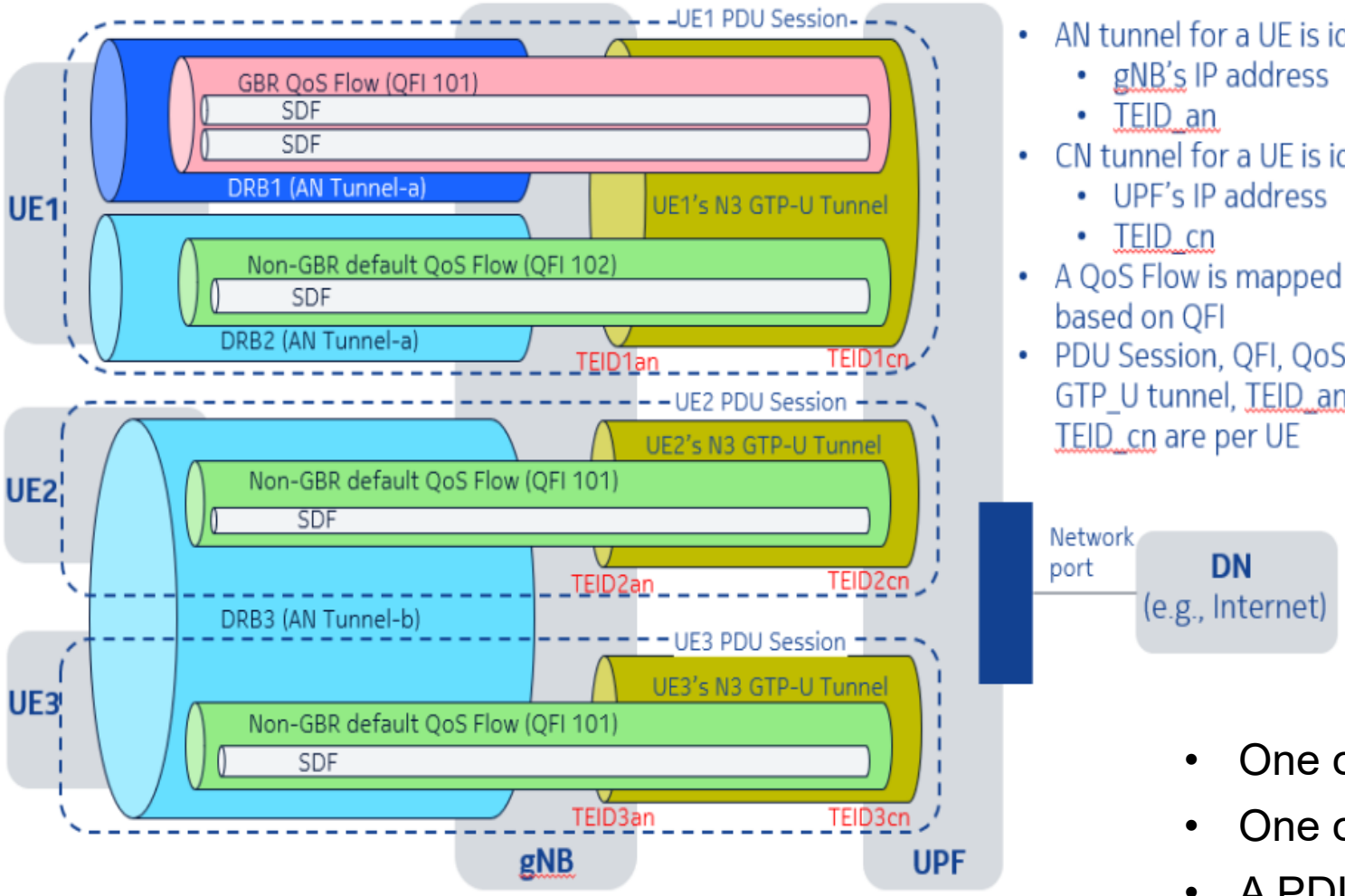
**Service Data Flows (SDF)**

- Flow of packets which represent a service being delivered to a subscriber

**Data Radio Bearers (DRBs)**

- The RAN decides how to map the QoS Flows to DRBs over the radio interface (Uu)
- They are configured to meet specific quality of service (QoS) requirements; A DRB serves packets with the same packet forwarding treatment
- Multiple QoS Flows with the same forwarding requirements can be multiplexed onto a single DRB

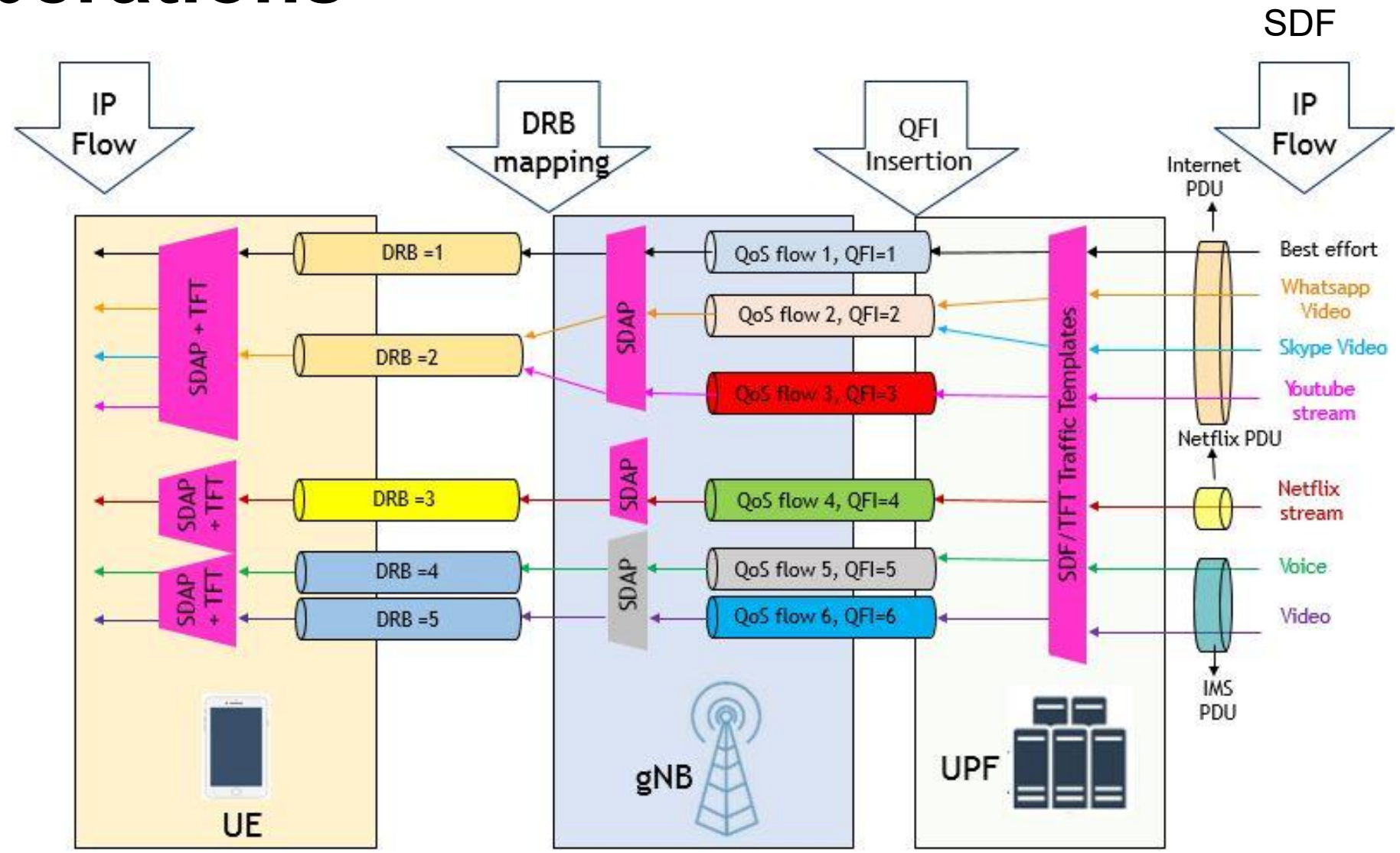
# PDU Sessions, QoS Flows and Service Data Flow




- AN tunnel for a UE is identified by:
  - gNB's IP address
  - TEID_an
- CN tunnel for a UE is identified by:
  - UPF's IP address
  - TEID_cn
- A QoS Flow is mapped to a DRB based on QFI
- PDU Session, QFI, QoS Flow, N3 GTP_U tunnel, TEID_an and TEID_cn are per UE

- One or more QoS Flow per PDU Session
- One or more SDF per QoS Flow
- A PDU session with multiple DRB
- A DRB shared by diferent PDU Sessions

# QoS operations

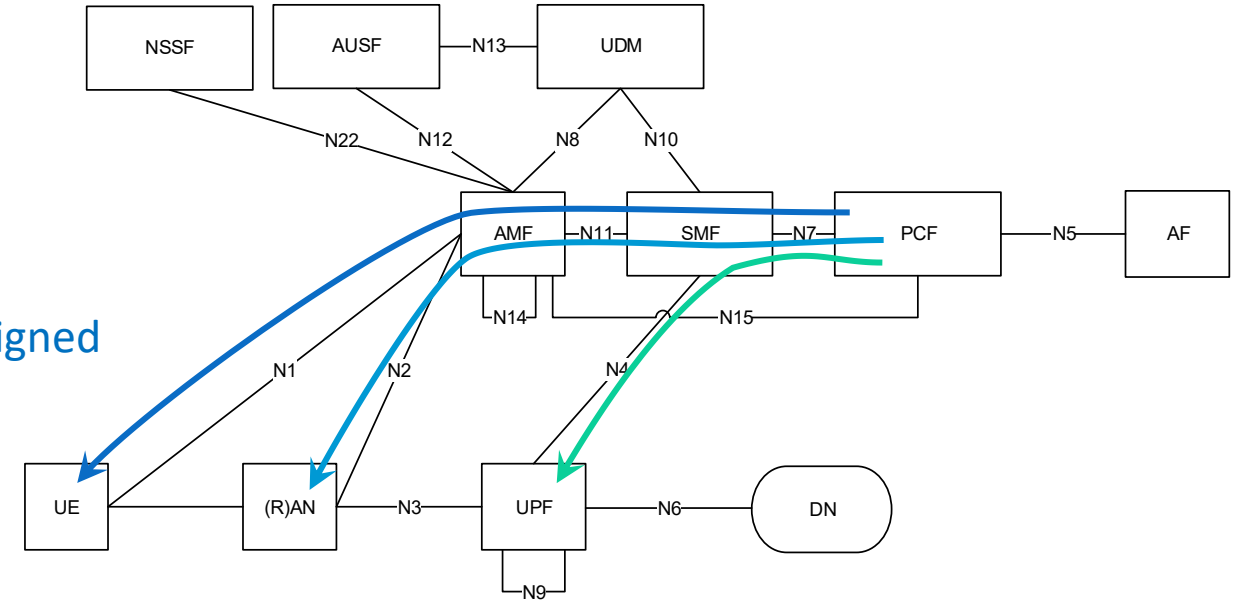


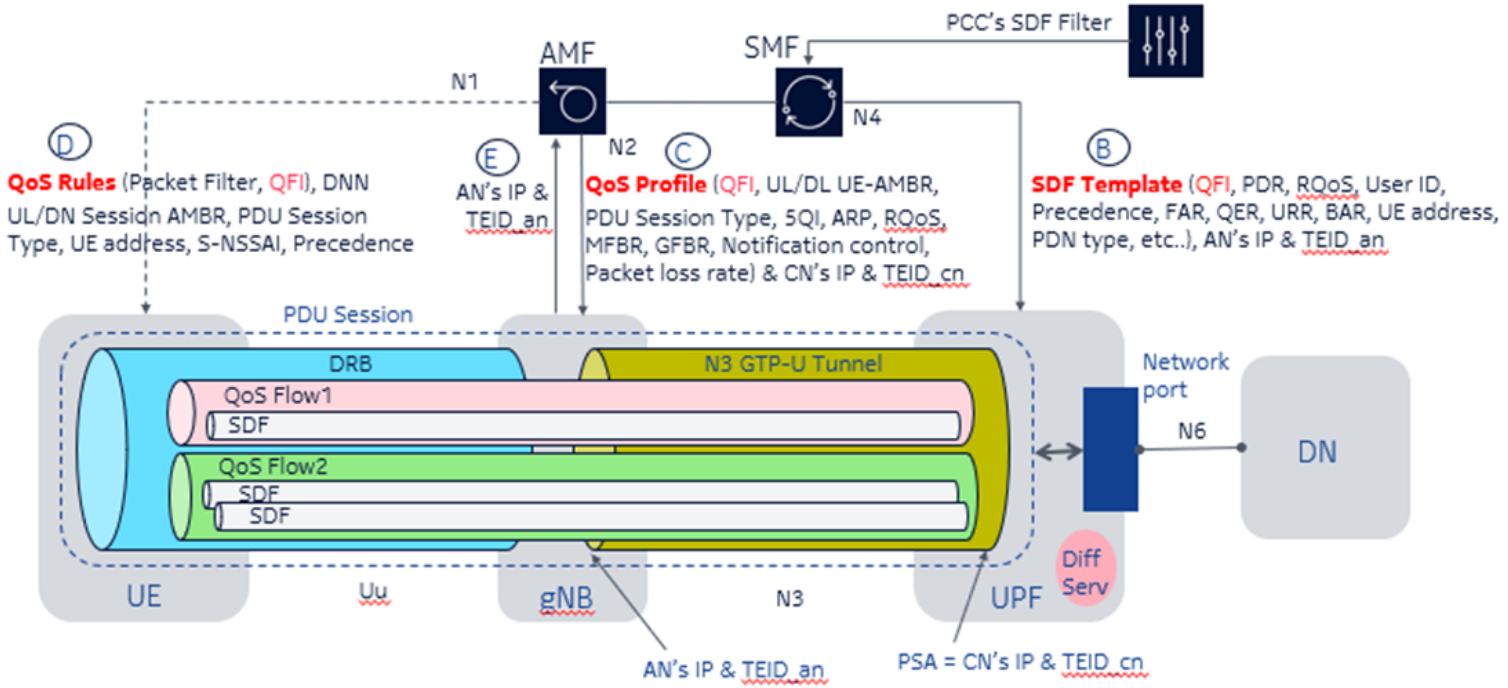
# QoS Model: PCF role

**Policy Control**

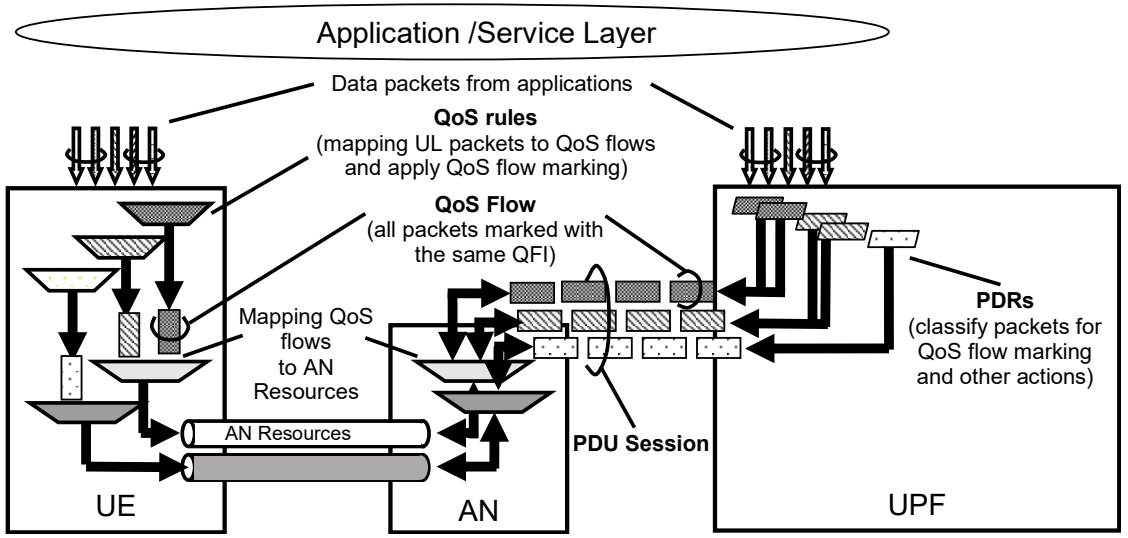
- The PCF manages and enforces QoS policies, interacting with the SMF to ensure consistent prioritization across the network based on the assigned 5QI values

1. **SDF Identification**: The SMF receives a PCC rule from PCF that defines an SDF
2. **PDR Creation**: The SMF creates one or more PDRs based on the PCC rule and installs them on the UPF, using PFCP
3. **Packet Classification**: When packets arrive at the UPF, they are matched against the PDRs
4. **QER Application**: The PDR for the matching SDF will include a QER that specifies the QoS treatment for that flow
5. **QoS Enforcement**: The UPF uses the QER to enforce the QoS, ensuring that the packet receives the correct quality of service treatment, such as being mapped to the correct QoS flow with the correct QFI



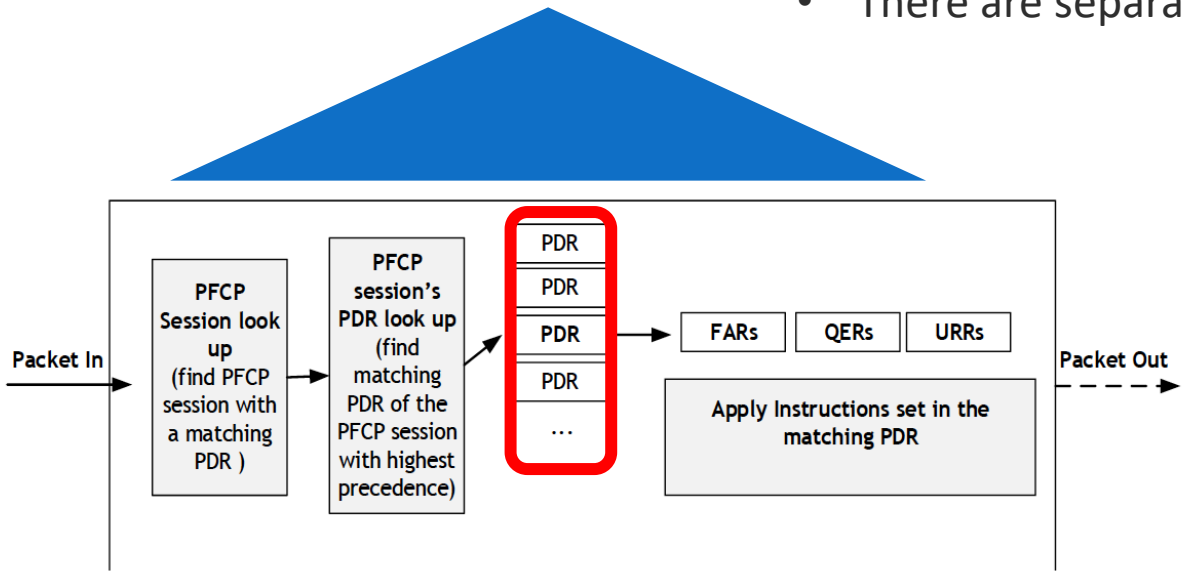



# QoS Model

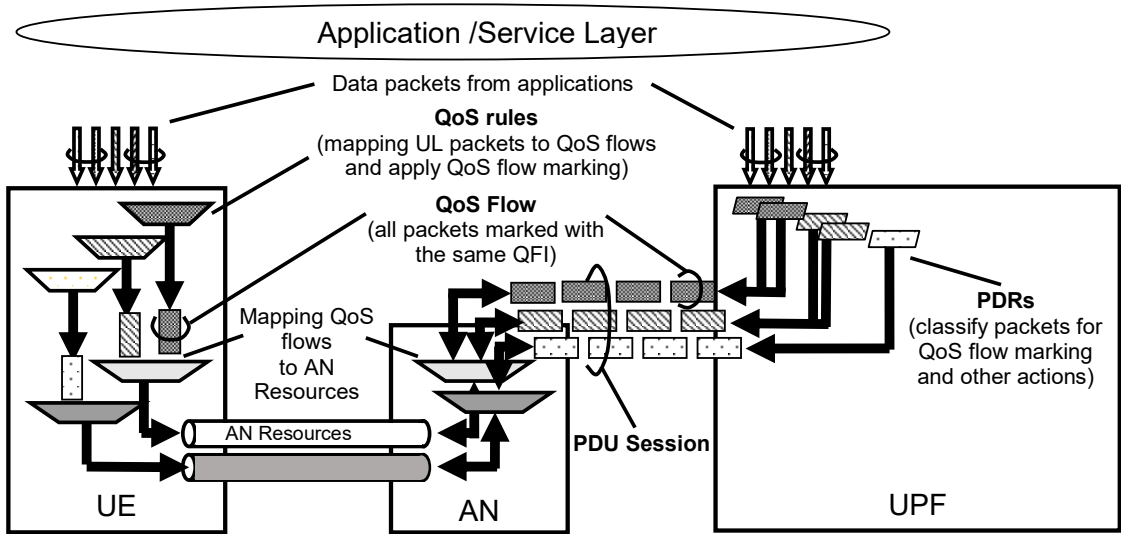


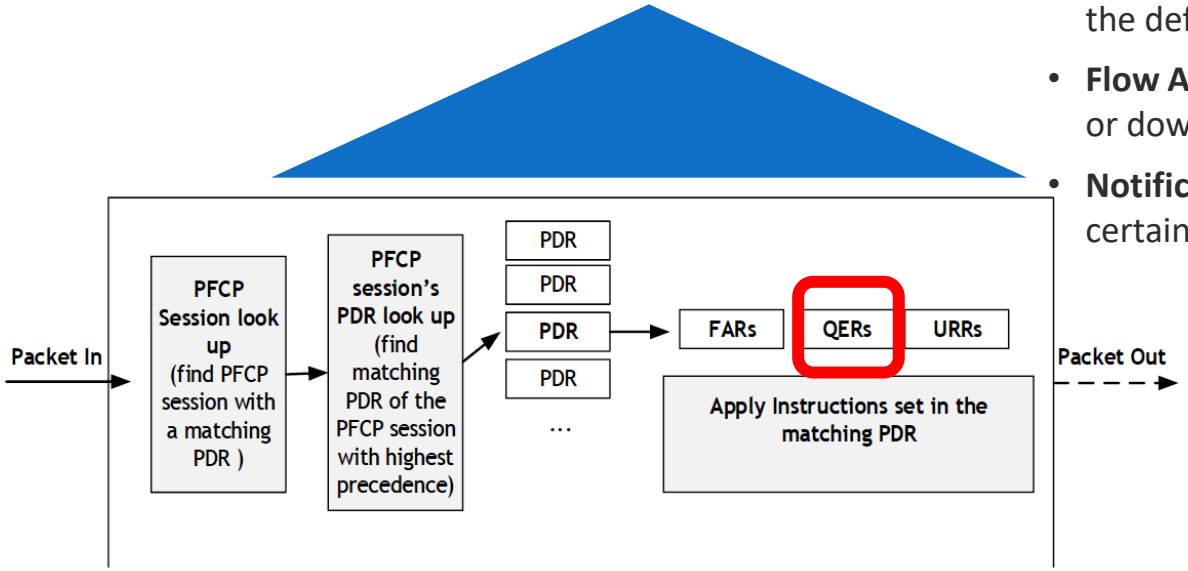

***Packet Detection Rule** (PDR)*

- Instructs the UPF how to detect incoming user data traffic (PDUs) and how to classify the traffic
- The PDR contains Packet Detection Information (e.g., IP filters) used in the traffic detection and classification
- There are separate PDRs for uplink and downlink



# QoS Model




***QoS Enforcement Rule*** *(QER)*: This rule contains information on how to enforce QoS, e.g., bit rate parameters.

- **5G QoS Identifier (5QI)**: identifies a specific set of QoS characteristics
- **Allocation and Retention Priority (ARP)**: determine the priority of a QoS flow for allocation and retention during network congestion
- **Guaranteed Flow Bit Rate (GFBR)**: guaranteed bit rate
- **Maximum Flow Bit Rate (MFBR)**: The maximum bit rate that can be delivered
- **Packet Delay Budget (PDB)**: maximum allowable delay for a data packet, applicable to GBR QoS flows
- **Packet Error Rate (PER)**: maximum acceptable error rate for a data packet
- **Maximum Data Burst Volume (MDBV)**: maximum amount of data that can be transmitted in a single burst; relevant for delay-critical GBR flows
- **Conform/Exceed Actions**: Actions to take when a data flow is within or exceeds the defined bit rate, such as conforming, exceeding, or discarding packets.
- **Flow Action**: action to be taken on a flow, which can include discarding uplink or downlink packets or terminating the flow
- **Notification Control**: Controls whether the user plane should be notified of certain events, such as exceeding a specific bit rate.

# 5G QoS parameters

The QoS profile of a QoS flow contains QoS parameters:

- For each QoS flow:
  - A *5G QoS Identifier* (5QI)
  - An *Allocation and Retention Priority* (ARP)
- In case of a GBR QoS flow only:
  - *Guaranteed Flow Bit Rate* (GFBR) for both uplink and downlink
  - *Maximum Flow Bit Rate* (MFBR) for both uplink and downlink
  - *Maximum Packet Loss Rate* for both uplink and downlink
- In case of Non-GBR QoS only:
  - *Reflective QoS Attribute* (RQA): the RQA, when included, indicates that some (not necessarily all) traffic carried on this QoS flow is subject to reflective quality of service (RQoS) at NAS

## Standardized 5QI to QoS characteristics mapping

| 5QI Value | Resource Type | Priority Level | Packet Delay Budget | Packet Error Rate | Default Averaging Window | Example Services |
|---|---|---|---|---|---|---|
| 1 | GBR | 20 | 100 ms | $10^{-2}$ | TBD | Conversational Voice |
| 2 | | 40 | 150 ms | $10^{-3}$ | TBD | Conversational Video (Live Streaming) |
| 3 | | 30 | 50 ms | $10^{-3}$ | TBD | Real Time Gaming, V2X messages |
| 4 | | 50 | 300 ms | $10^{-6}$ | TBD | Non-Conversational Video (Buffered Streaming) |
| 65 | | 7 | 75 ms | $10^{-2}$ | TBD | Mission Critical user plane Push To Talk voice (e.g., MCPTT) |
| 66 | | 20 | 100 ms | $10^{-2}$ | TBD | Non-Mission-Critical user plane Push To Talk voice |
| 75 | | 25 | 50 ms | $10^{-2}$ | TBD | V2X messages |
| 5 | Non-GBR | 10 | 100 ms | $10^{-6}$ | N/A | IMS Signalling |
| 6 | | 60 | 300 ms | $10^{-6}$ | N/A | Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.) |
| 7 | | 70 | 100 ms | $10^{-3}$ | N/A | Voice, Video (Live Streaming) Interactive Gaming |
| 8 | | 80 | 300 ms | $10^{-6}$ | N/A | Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file |
| 9 | | 90 | | | N/A | sharing, progressive video, etc.) |
| 69 | | 5 | 60 ms | $10^{-6}$ | N/A | Mission Critical delay sensitive signalling (e.g., MC-PTT signalling) |
| 70 | | 55 | 200 ms | $10^{-6}$ | | Mission Critical Data (e.g. example services are the same as QCI 6/8/9) |
| 79 | | 65 | 50 ms | $10^{-2}$ | N/A | V2X messages |
| | | | | | N/A | |

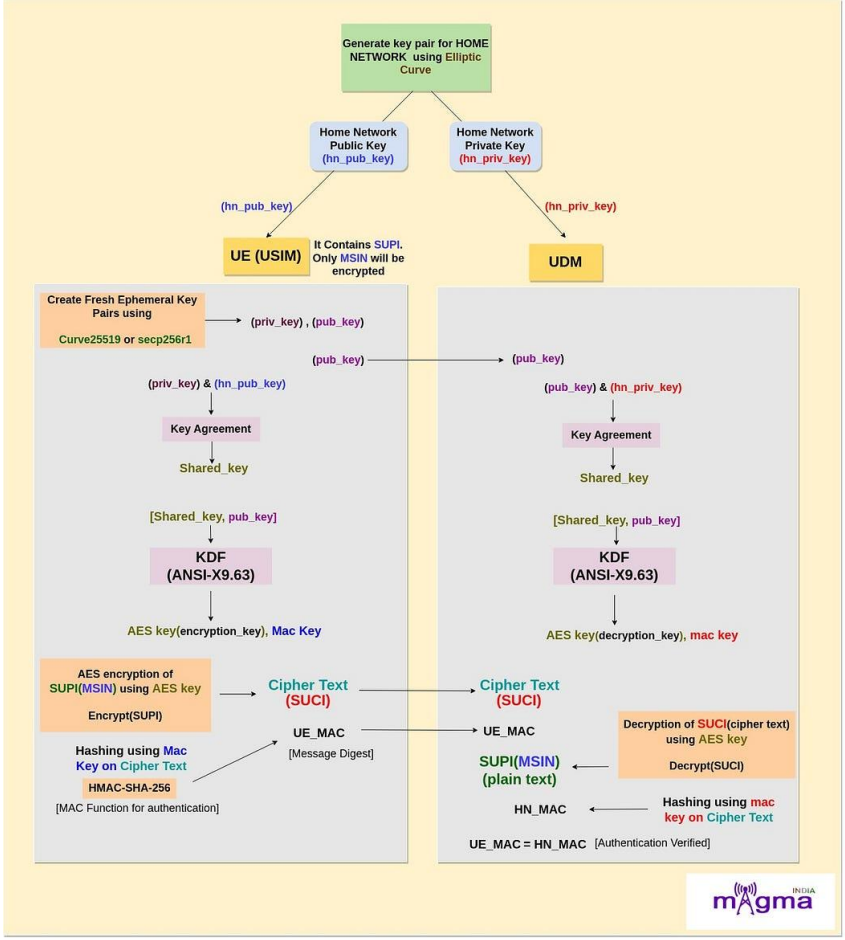
# Authentication and registration

# 5G Authentication

- Primary authentication:
  - Mutual authentication between the UE and the network and provide keying material that can be used between the UE and the serving network in subsequent security procedures
  - There can be a secondary authentication, delegated to third parties (external networks)
- 5G introduces new authentication methods:
  - 5G-AKA (*Authentication and Key Agreement*)
  - EAP-AKA' (*Extensible Authentication Protocol*), for integration with other non-3GPP access networks
- Goals:
  - Stronger security
  - Improved privacy (e.g. SUPI protection)
  - Support for 3GPP and non-3GPP access

# 5G Security Features

- Mutual authentication (UE ↔ Network)
- SUPI never exposed in cleartext
  - SUPI (*Subscription Permanent Identifier*) = permanent identity
  - SUCI (*Subscription Concealed Identifier*) = encrypted SUPI
    - SUCI ensures SUPI is never exposed over the air
    - Prevents IMSI-catcher style attacks
- Authentication anchored in home network

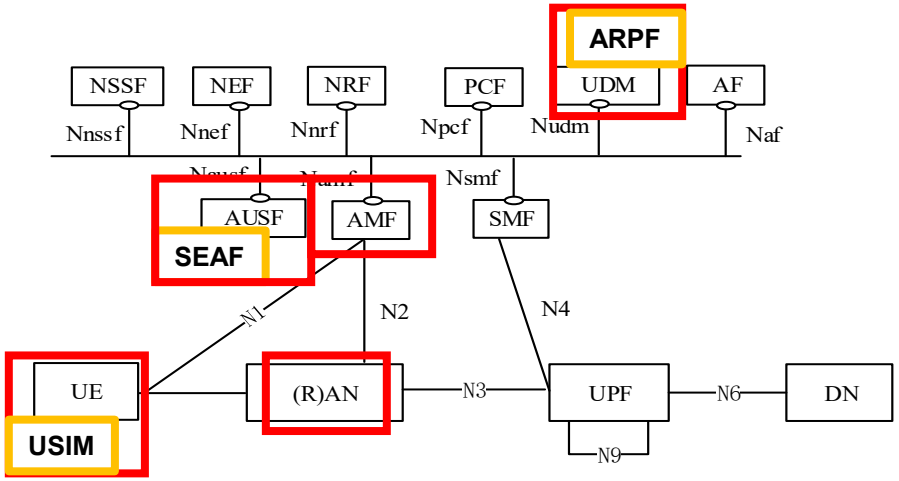



## Enhancements over previous generations

The 5G AKA process represents an improvement over older generations, particularly 4G:

- **Decentralized Authentication**: 5G distributes security functions across the network, reducing single points of failure and improving resilience
- **Home Network Control**: The home network plays a more active role in authentication decisions, improving oversight
- **Subscriber Privacy**: 5G encrypts the user's permanent identifier (SUPI) into a concealed identifier (SUCI), which prevents location tracking

# Key Entities in 5G Authentication




- UE (User Equipment)
  - USIM (*Universal Subscriber Identity Module*)
- gNB (5G *Base Station*)
- AMF (*Access & Mobility Management Function*)
- AUSF (*Authentication Server Function*)
  - SEAF (*Security Anchor Function*)
- UDM (*Unified Data Management* / subscriber database)
  - ARPF (*Authentication Credential Repository and Processing Function*)

# 5G Security Parameters : K, OP/OPc, SQN

**Key cryptographic components used in the 5G-AKA process to verify the user's identity and derive session keys**

**Crucial for preventing fraud and ensuring network and user data integrity**

- **K (Subscriber's Secret Key)**

Long-term cryptographic key (128 or 256 bit) shared exclusively between the subscriber's USIM and the home network's UDM database

Root of trust from which all other session-specific keys are derived

- **OP (Operator Code)**

Operator identifier, used in combination with K and other parameters to generate authentication data

In previous generation, was often shared among all subscribers on a network, which was a security risk

- **OPc (Derived Operator Code)**

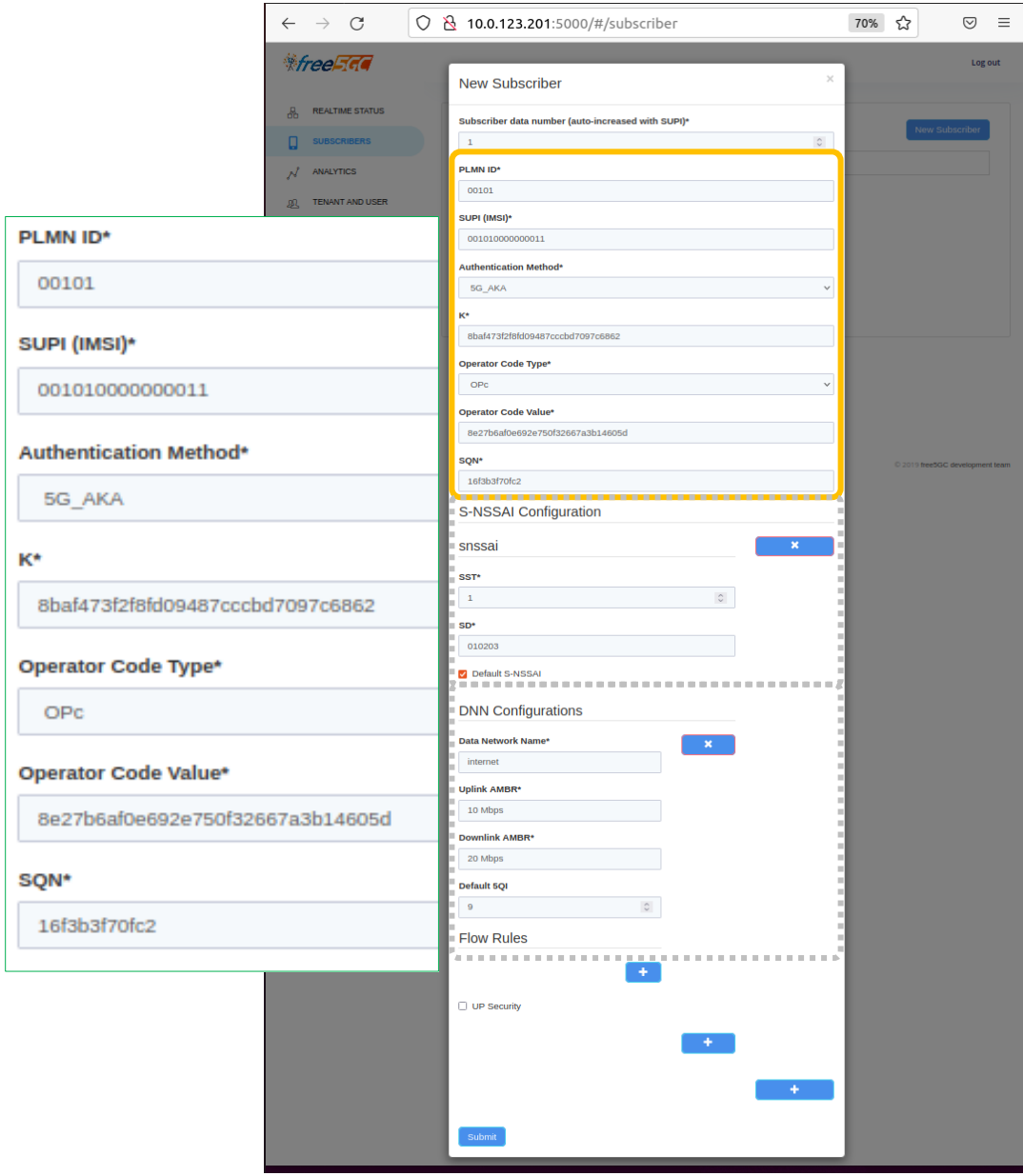
Derived, subscriber-specific operator code calculated by combining the original OP and the secret key K, used in Milenage and TUAK algorithms

Improves security by preventing attackers from using a single compromised key to attack multiple users

- **SQN (Sequence Number)**

Counter stored on both the USIM and in the home network's database, used during keys generation

Used to prevent replay attacks, where an attacker re-sends old authentication messages to impersonate a legitimate user




**Free5GC subscriber creation example**

# Authentication process

- 1. UE sends SUCI to AMF
- 2. AMF → AUSF → UDM: Authentication request
- 3. UDM generates Authentication Vectors (AV)

The home network's *Authentication Credential Repository and Processing Function* (ARPF), part of the UDM, uses the keys K and OPc, along with the SQN, to generate a set of *Authentication Vectors* (AV)

- 4. AUSF sends challenge to UE

The serving network sends a *RANDom challenge* (RAND) and an *AUthentication TokeN* (AUTN) to the *User Equipment* (UE), which contains the USIM

- 5. UE verifies and responds with RES*

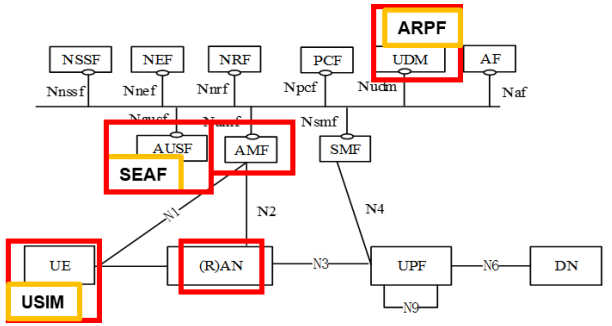
The USIM uses its stored K, OPc, and SQN, along with the RAND and AUTN, to compute a response. It also checks that the network is legitimate

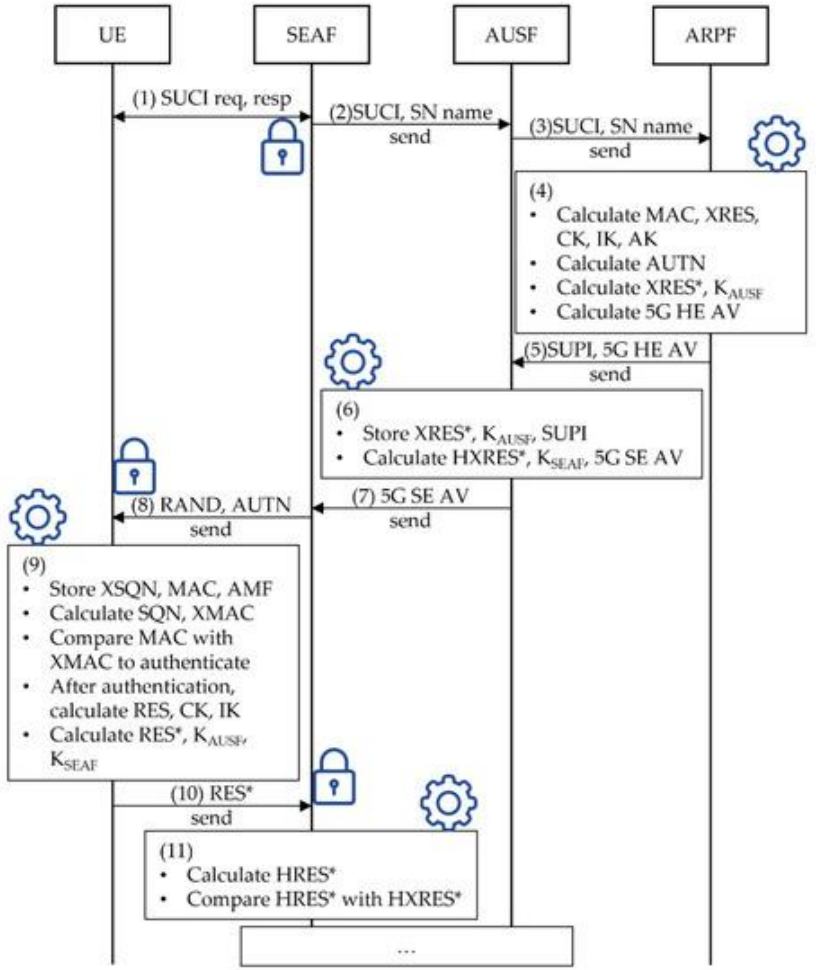
If the verification is successful, the UE sends the calculated response back to the network.

- 6. AUSF compares RES* with XRES*
- 7. Authentication success → Kseaf key derived

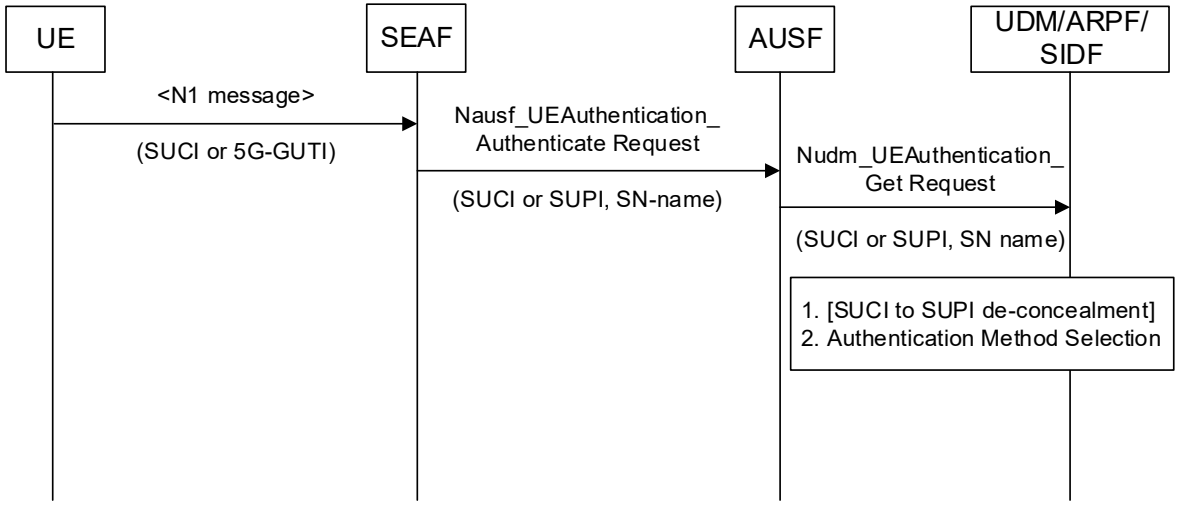
Both the network and UE then use the results of the AKA process to derive a new set of session-specific keys for encrypted communication

- 8. Security context established (KAMF, KNASint, KNASenc, …)

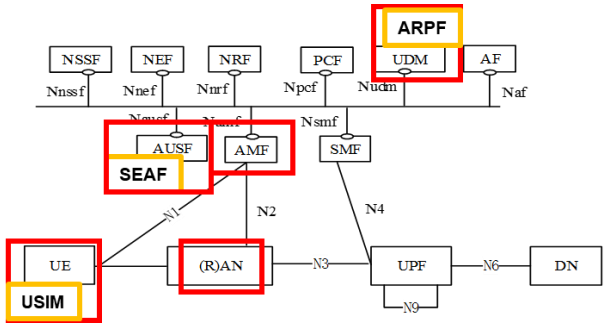


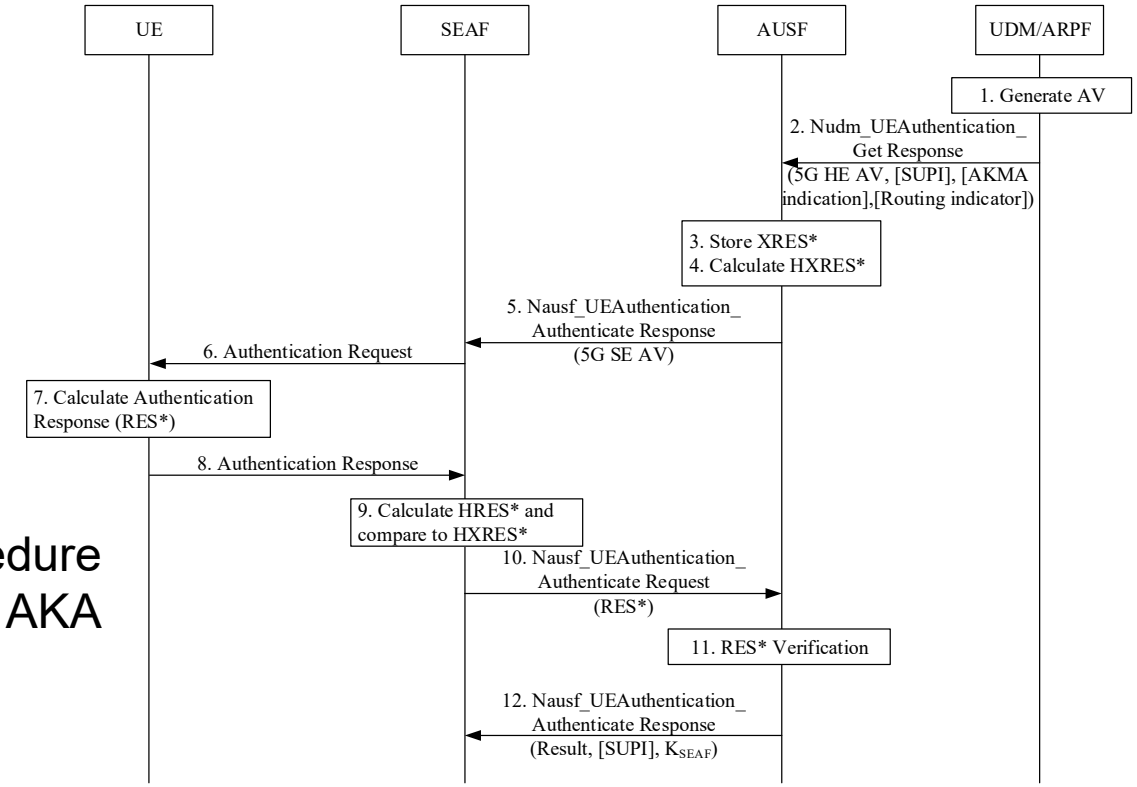



# Authentication process



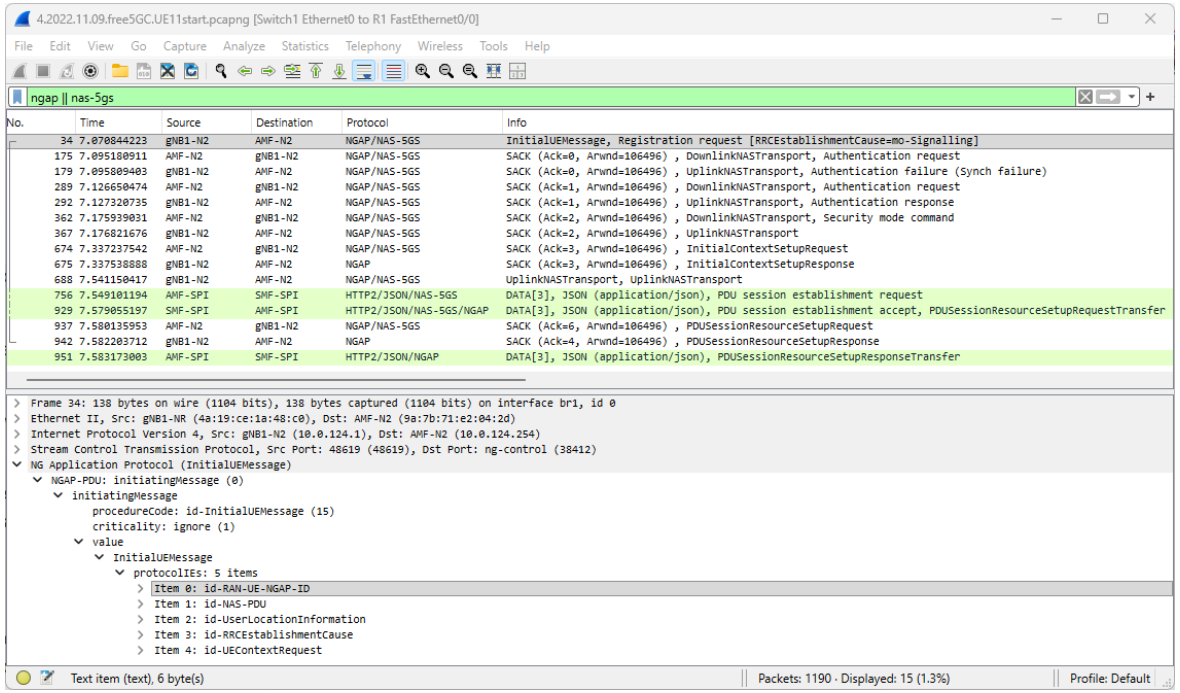

Initiation of authentication procedure and selection of authentication method



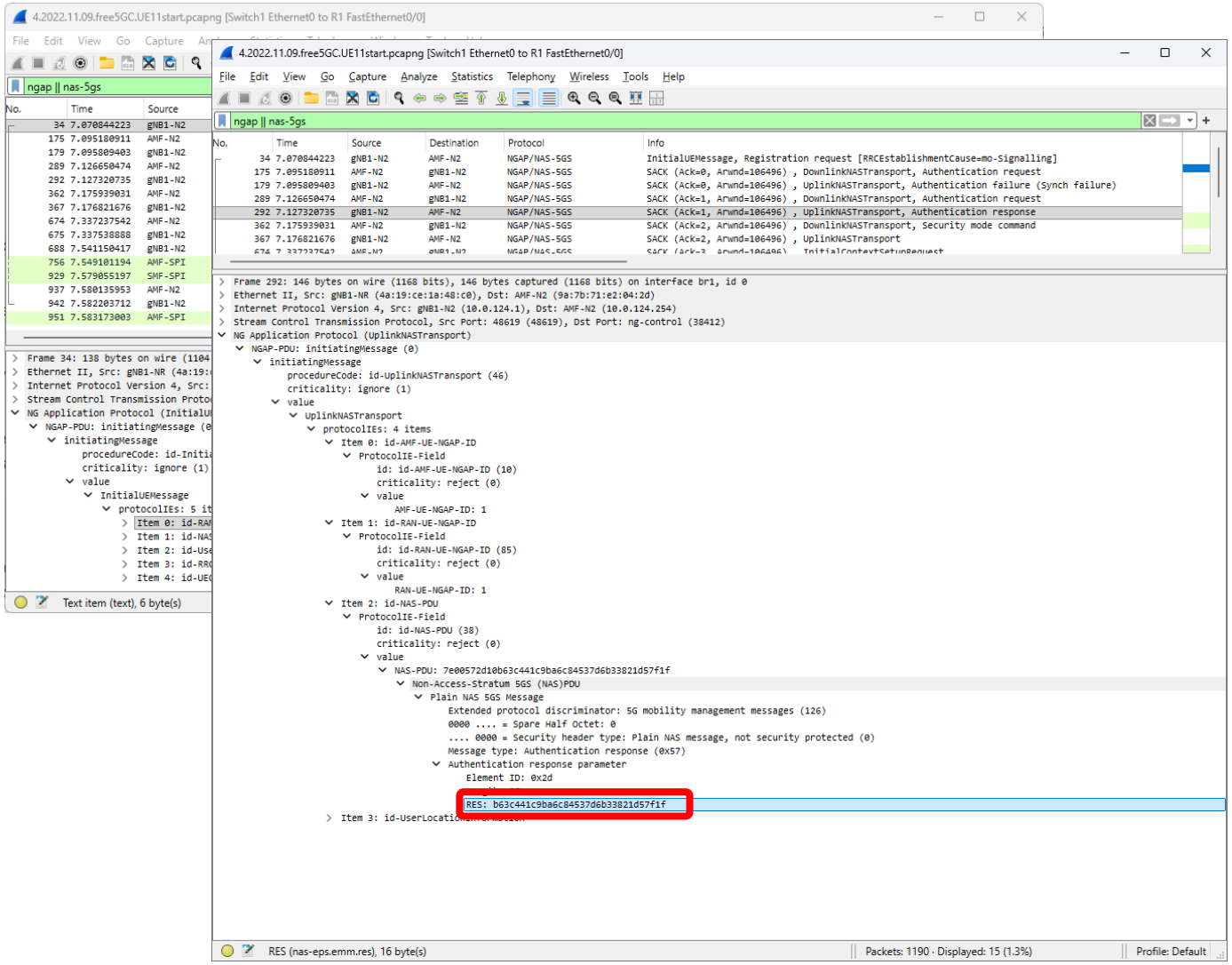

Authentication procedure for 5G AKA

# 5G-AKA Authentication Flow

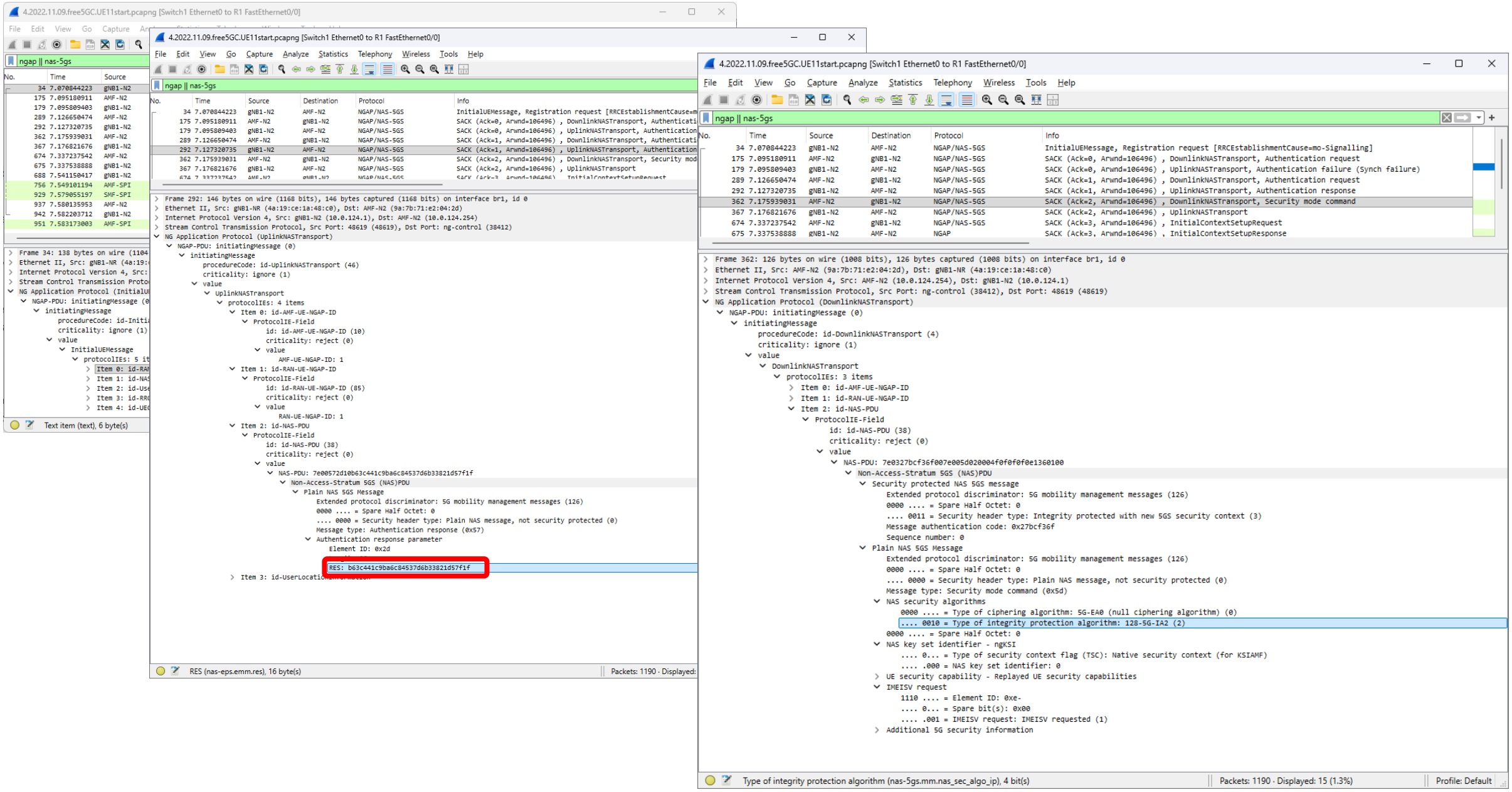



5G AKA ‘synch failure’ (21) refers to a specific authentication failure in the 5G network, triggered when the UE's SIM (USIM) detects that the SQN) is out of sync during the AKA process

# 5G-AKA Authentication Flow



# 5G-AKA Authentication Flow



# Milenage algoritm

A set of cryptographic algorithms standardized by ETSI for 3G and 4G mobile networks, which uses AES (Rijndael) encryption

**Key Derivation:** K, along with other inputs like a **random challenge (RAND)**, is used in the MILENAGE functions (f1 to f5) to produce CK, IK, and other keys. This hierarchical structure prevents the compromise of lower-level keys (like CK and IK) from compromising the higher-level master key (K)

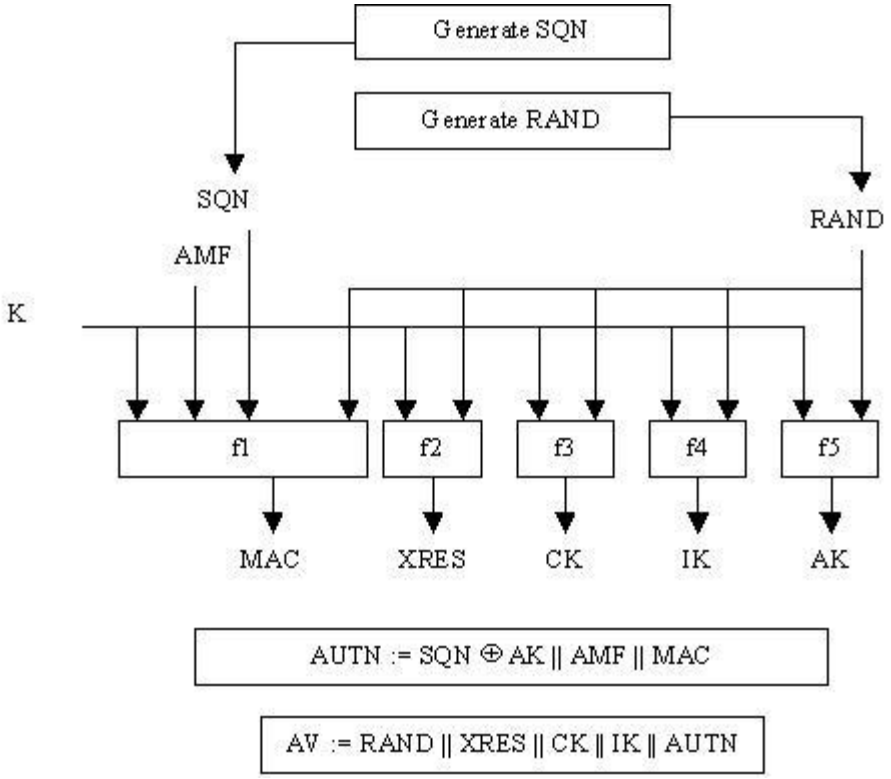
**K (*Subscriber Key*):** The master secret key shared between the user's SIM and the network's home network

**MAC** (***Message Authentication Code***): 64-bit code that is used in mobile network security for authenticating a network

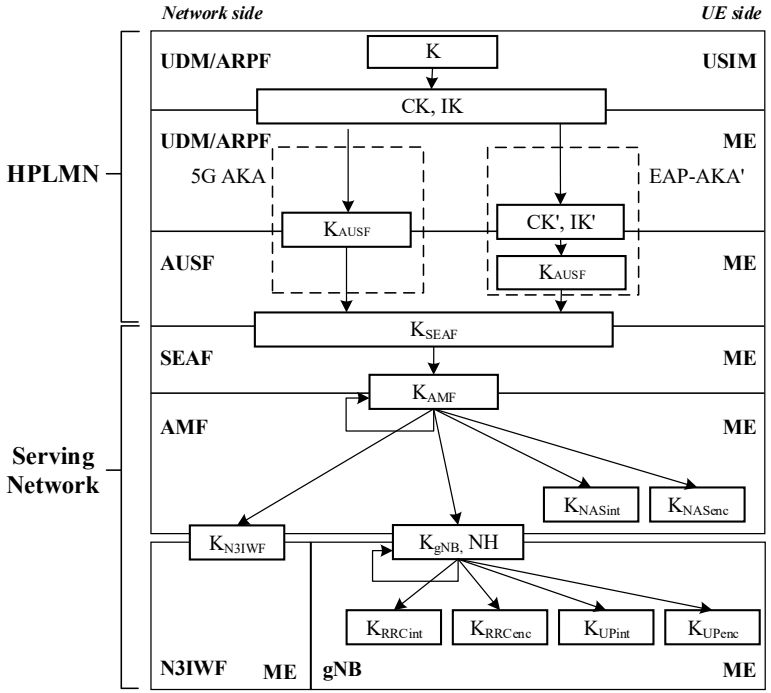
**CK (*Confidentiality Key*):** A 128-bit key used to encrypt data to ensure privacy

**IK (*Integrity Key*):** A 128-bit key used to protect data from being altered during transmission, ensuring its integrity

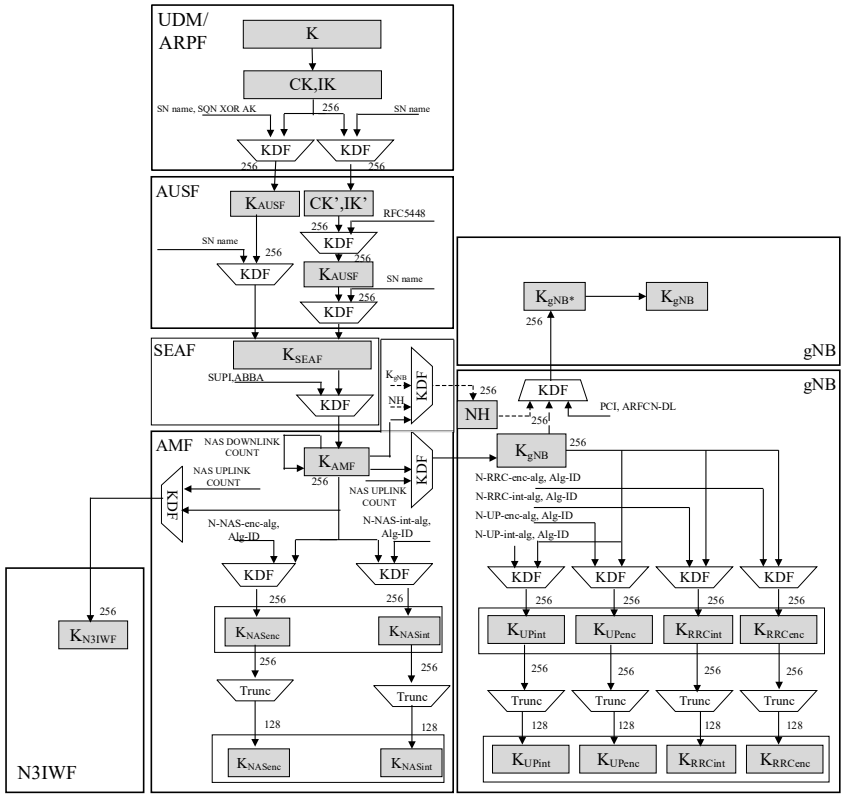
**AK (*Anonymity Key*):** a 48-bit value generated by the HN to hide the SQN



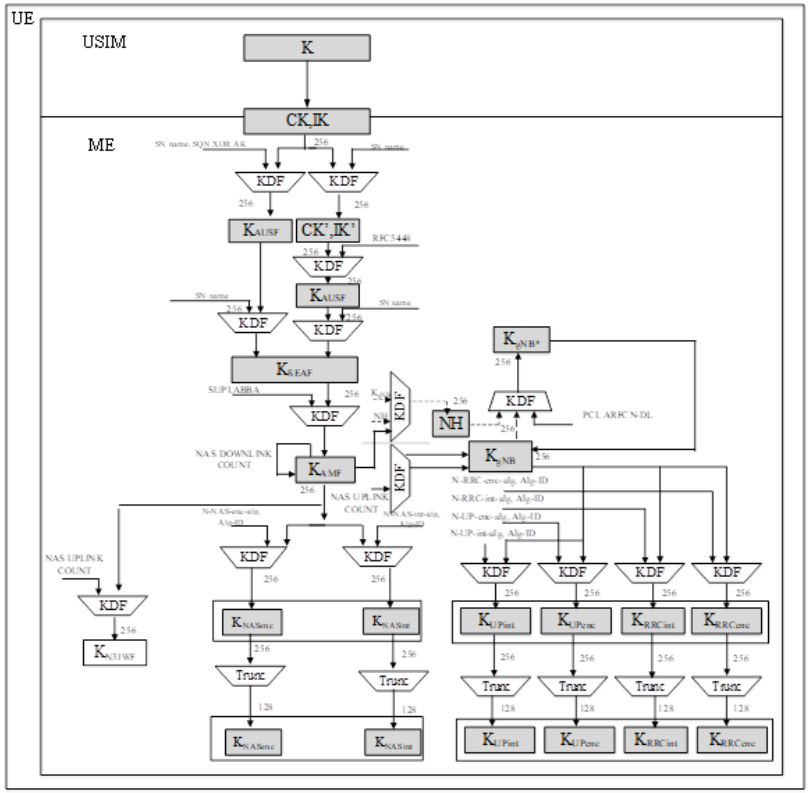
# Keys generation from K




3GPP, TS 33.501, Figure 6.2.1-1:
Key hierarchy generation in 5GS




3GPP, TS 33.501, Figure 6.2.2-1:
Key distribution and key derivation scheme for 5G for network nodes




3GPP, TS 33.501, Figure 6.2.2-2:
Key distribution and key derivation scheme for 5G for the UE

CK: Cipher Key
IK: Integrity Key

# PDU establishment

# PDU Sessions definition

A PDU Session establishment may correspond to:

- a UE initiated PDU Session Establishment procedure
- a UE initiated PDU Session handover between 3GPP and non-3GPP
- a UE initiated PDU Session handover from EPS (4G) to 5GS
- a Network triggered PDU Session Establishment procedure; a trigger is sent to an Application in the UE, which initiated the PDU Session establishment

The **UE always initiate PDU Sessions** → requests access to a specific DNN, via a specific Slice

- S-NSSAI guides the network to select the **right Network Slice**
- The network Slice partially determines **how traffic is handled** (QoS, latency, etc.)
- The DNN routes the session to the **correct external data network**

The PDU Session is the actual data tunnel, carrying traffic with slice-specific policies

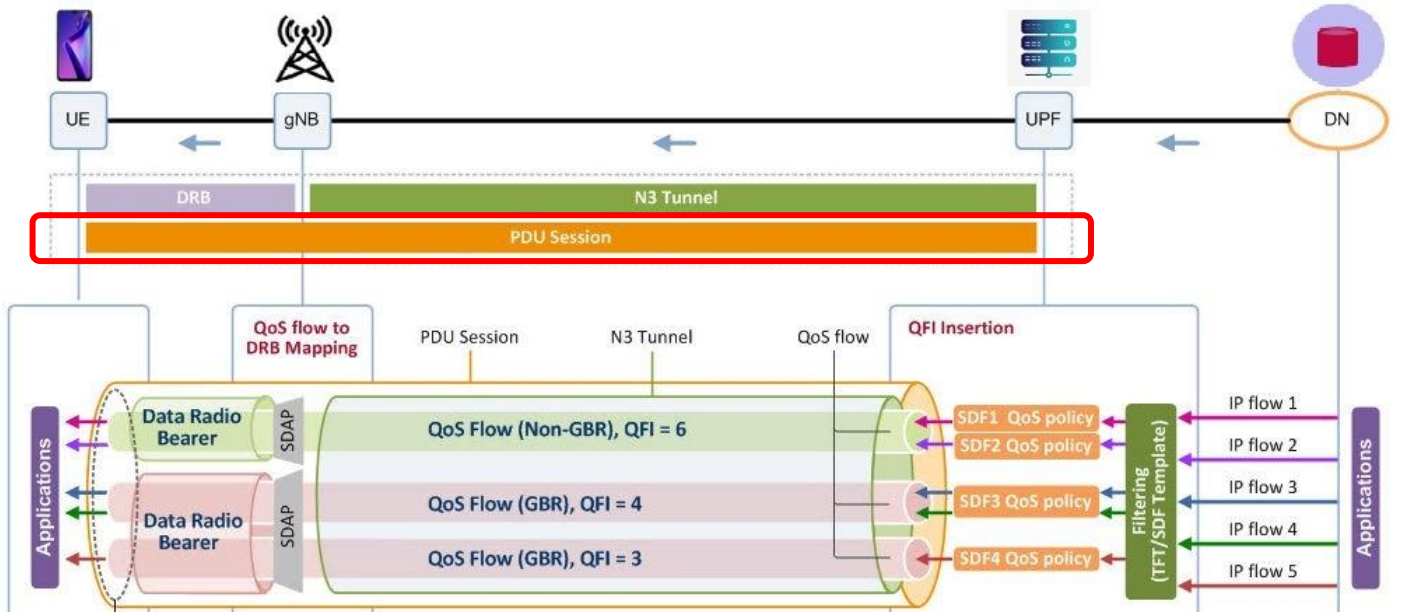
An initial default PDU Session is established; additional ones are established on demand, whenever existing ones to not fulfill requirements for new QoS Flows

A PDU Session can support different types of data units, known as PDU types; the main PDU types are:

- **IPv4**: Supports only IPv4 addressing for user data
- **IPv6**: Supports only IPv6 addressing for user data
- **IPv4v6**: Supports both IPv4 and IPv6 addressing simultaneously
- **Unstructured**: Used for services that do not require IP addressing, such as Ethernet or non-IP data
- **Ethernet**: Supports Ethernet frames, enabling services like enterprise LAN connectivity over 5G

# PDU session

A PDU (**Protocol Data Unit**) session in 5G is the logical connection between a UE (**User Equipment**) and the Data Network (**DN**) through the 5G Core, via a suitable **Slice**. It enables data transfer for services like Internet access or private applications.




- PDU characterization parameters:

| Parameter | Description |
|---|---|
| PDU Session Identifier | A **unique ID** for the PDU session between the User Equipment (UE) and the 5G network |
| S-NSSAI (Single-Network Slice Selection Assistance Information) | Identifies the specific network slice the PDU session belongs to. It's composed of the **Slice/Service Type** (SST) and **Slice Differentiator** (SD). |
| DNN (Data Network Name) | The name of the data network (e.g., an internet service provider) the PDU session provides connectivity to |
| PDU Session Type | The type of data the session will carry, such as **IPv4, IPv6, IPv4v6 (dual-stack), Ethernet, or unstructured data** |
| **SSC Mode** (*Service and Session Continuity*) | Defines how sessions are handled (how the user plane anchor point of the PDU session is managed throughout its lifecycle) when the UE moves between different network access points. |
| User Plane Security Information | Indicates whether user-plane traffic will be ciphered and have its integrity protected |
| Quality of Service (QoS) | **5QI (5G Quality of Service Identifier**): determines the QoS characteristics, including **Guaranteed Bit Rate** (GBR), **Non-Guaranteed Bit Rate** (non-GBR), and **Delay Critical GBR** |
| PDU Session Establishment Request Parameters | Depending on the session, other parameters like UE capabilities and DNS information |

# PDU Sessions call flow

5G NAS-SM (*Session Management*) is responsible for setting up and managing (establishment, modification, deletion) the PDU session for user-plane connectivity between UE and Data Networks

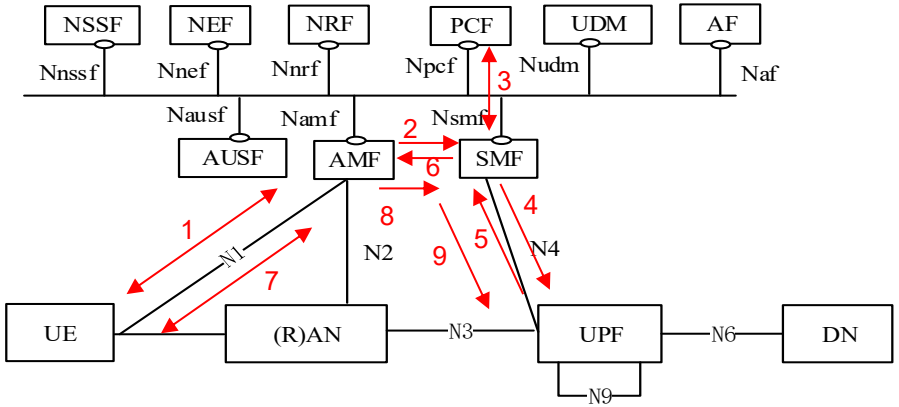
- UE to SMF

Other protocols involved:

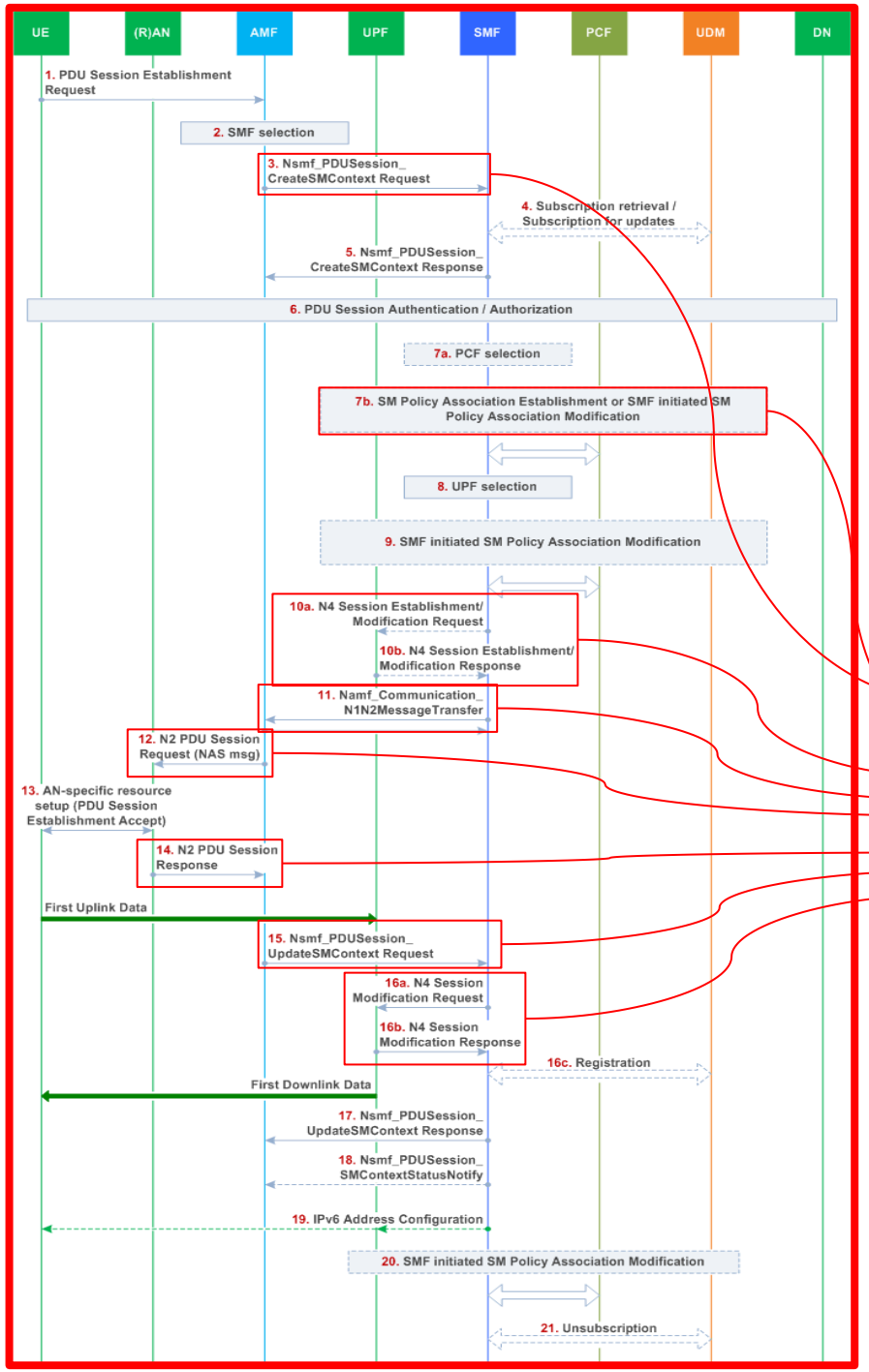
- PFCP (between SMF and UPF)
- HTTP/2 & JSON (SBA entities: AMF, SMF, PCF)

Requires interactions between:

1. UE
2. gNB
3. AMF
4. PCF
5. SMF
6. UPF



# UE registration and PDU establishment




Involded protocols

Excluded entities: NRF, UDR and UDM

4.2022.11.09.free5GC.UE11start.pcapng [Switch1 Ethernet0 to R1 FastEthernet0/0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(pfcp || json || ngap) && !ip.addr == 10.0.123.1 && !ip.addr == 10.0.123.2 && !ip.addr == 10.0.123.3

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 34 | 7.070844223 | gNB1-N2 | AMF-N2 | NGAP/NAS-5GS | InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling] |
| 62 | 7.075097701 | AMF-SBI | AUSF-SBI | HTTP2/JSON | DATA[3], JSON (application/json) |
| 172 | 7.094574481 | AUSF-SBI | AMF-SBI | HTTP2/JSON | DATA[3], JSON (application/json) |
| 175 | 7.095180911 | AMF-N2 | gNB1-N2 | NGAP/NAS-5GS | SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request |
| 179 | 7.095809403 | gNB1-N2 | AMF-N2 | NGAP/NAS-5GS | SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Authentication failure (Synch failure) |
| 188 | 7.096652384 | AMF-SBI | AUSF-SBI | HTTP2/JSON | DATA[3], JSON (application/json) |
| 288 | 7.126075820 | AUSF-SBI | AMF-SBI | HTTP2/JSON | DATA[3], JSON (application/json) |
| 289 | 7.126650474 | AMF-N2 | gNB1-N2 | NGAP/NAS-5GS | SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request |
| 292 | 7.127320735 | gNB1-N2 | AMF-N2 | NGAP/NAS-5GS | SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response |
| 302 | 7.128343092 | AMF-SBI | AUSF-SBI | HTTP2/JSON | DATA[3], JSON (application/json) |
| 358 | 7.175060986 | AUSF-SBI | AMF-SBI | HTTP2/JSON | DATA[3], JSON (application/json) |
| 362 | 7.175939031 | AMF-N2 | gNB1-N2 | NGAP/NAS-5GS | SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command |
| 367 | 7.176821676 | gNB1-N2 | AMF-N2 | NGAP/NAS-5GS | SACK (Ack=2, Arwnd=106496) , UplinkNASTransport |
| 583 | 7.325205197 | AMF-SBI | PCF-SBI | HTTP2/JSON | DATA[3], JSON (application/json) |
| 656 | 7.331888824 | PCF-SBI | AMF-SBI | HTTP2/JSON | DATA[3], JSON (application/json) |
| 665 | 7.333862669 | AMF-SBI | PCF-SBI | HTTP2/JSON | DATA[3], JSON (application/json) |
| 670 | 7.334259562 | PCF-SBI | AMF-SBI | HTTP2/JSON | DATA[3], JSON (application/json) |
| 674 | 7.337237542 | AMF-N2 | gNB1-N2 | NGAP/NAS-5GS | SACK (Ack=3, Arwnd=106496) , InitialContextSetupRequest |
| 675 | 7.337538888 | gNB1-N2 | AMF-N2 | NGAP | SACK (Ack=3, Arwnd=106496) , InitialContextSetupResponse |
| 688 | 7.541150417 | gNB1-N2 | AMF-N2 | NGAP/NAS-5GS | UplinkNASTransport, UplinkNASTransport |
| 724 | 7.546940725 | NSSF-SBI | AMF-SBI | HTTP2/JSON | DATA[3], JSON (application/json) |
| 756 | 7.549101194 | AMF-SBI | SMF-SBI | HTTP2/JSON/NAS-5GS | DATA[3], JSON (application/json), PDU session establishment request |
| 852 | 7.562159144 | SMF-SBI | PCF-SBI | HTTP2/JSON | DATA[3], JSON (application/json) |
| 892 | 7.571887561 | PCF-SBI | SMF-SBI | HTTP2/JSON | DATA[3], JSON (application/json) |
| 915 | 7.575626116 | SMF-SBI | AMF-SBI | HTTP2/JSON | DATA[3], JSON (application/json) |
| 916 | 7.575561222 | SMF-N4 | UPF-N4 | PFCP | PFCP Session Establishment Request |
| 919 | 7.576759436 | UPF-N4 | SMF-N4 | PFCP | PFCP Session Establishment Response |
| 929 | 7.579055197 | SMF-SBI | AMF-SBI | HTTP2/JSON/NAS-5GS/NGAP | DATA[3], JSON (application/json), PDU session establishment accept, PDUSessionResourceSetupRequestTransfer |
| 937 | 7.580135953 | AMF-N2 | gNB1-N2 | NGAP/NAS-5GS | SACK (Ack=6, Arwnd=106496) , PDUSessionResourceSetupRequest |
| 939 | 7.580308473 | AMF-SBI | SMF-SBI | HTTP2/JSON | DATA[3], JSON (application/json) |
| 942 | 7.582203712 | gNB1-N2 | AMF-N2 | NGAP | SACK (Ack=4, Arwnd=106496) , PDUSessionResourceSetupResponse |
| 951 | 7.583173003 | AMF-SBI | SMF-SBI | HTTP2/JSON/NGAP | DATA[3], JSON (application/json), PDUSessionResourceSetupResponseTransfer |
| 958 | 7.584659733 | SMF-N4 | UPF-N4 | PFCP | PFCP Session Modification Request |
| 963 | 7.585547591 | UPF-N4 | SMF-N4 | PFCP | PFCP Session Modification Response |
| 965 | 7.593099130 | SMF-SBI | AMF-SBI | HTTP2/JSON | DATA[3], JSON (application/json) |

```
> Frame 756: 864 bytes on wire (6912 bits), 864 bytes captured (6912 bits) on interface br1, id 0
> Ethernet II, Src: AMF-SBI (7e:bc:88:b7:bb:8d), Dst: SMF-N4 (ae:18:de:d4:c3:19)
> Internet Protocol Version 4, Src: AMF-SBI (10.0.123.6), Dst: SMF-SBI (10.0.123.9)
> Transmission Control Protocol, Src Port: 45546 (45546), Dst Port: irdmi (8000), Seq: 224, Ack: 1, Len: 798
v HyperText Transfer Protocol 2
  v Stream: DATA, Stream ID: 3, Length 789
      Length: 789
      Type: DATA (0)
    > Flags: 0x01, End Stream
      0... .... .... .... .... .... .... .... = Reserved: 0x0
      .000 0000 0000 0000 0000 0000 0000 0011 = Stream Identifier: 3
      [Pad Length: 0]
      Data [...]: 2d2d303232303839666665316632646237653063396238383839656537366463333337613037633133363331373838323966313737633233393866643360d0a436f6e74656e742d547970653a206170706c696361746
      [Connection window size (before): 65535]
      [Connection window size (after): 64746]
      [Stream window size (before): 65535]
      [Stream window size (after): 64746]
  v MIME Multipart Media Encapsulation, Type: multipart/related, Boundary: "022089ffe1f2db7e0c9b8889ee76dc337a07c1363178829f177c2398fd36"
      [Type: multipart/related]
      First boundary: --022089ffe1f2db7e0c9b8889ee76dc337a07c1363178829f177c2398fd36\r\n
    v Encapsulated multipart part:  (application/json)
        Content-Type: application/json\r\n\r\n
    v JavaScript Object Notation: application/json
```

4.2022.11.09.free5GC.UE11start.pcapng

# 5G-AKA Authentication and initial PDU Session establishment Flow