5G Core Network

Andrii Konotop

November 2, 2025

Contents

1 Introduction

The fifth generation (5G) mobile communication system represents a fundamental shift in network architecture compared to its predecessor, LTE/EPC. Unlike the EPC, which was based on monolithic nodes, the 5G Core Network (5GCN) introduces a service-based and cloud-native architecture to enable flexibility, scalability, and support for a wide range of services such as enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communication (URLLC), and massive Machine-Type Communication (mMTC).

The goal of this report is to provide some overview on fundamentals and to introduce to some basic procedures of key functionalities.

2 5G Core Network Architecture

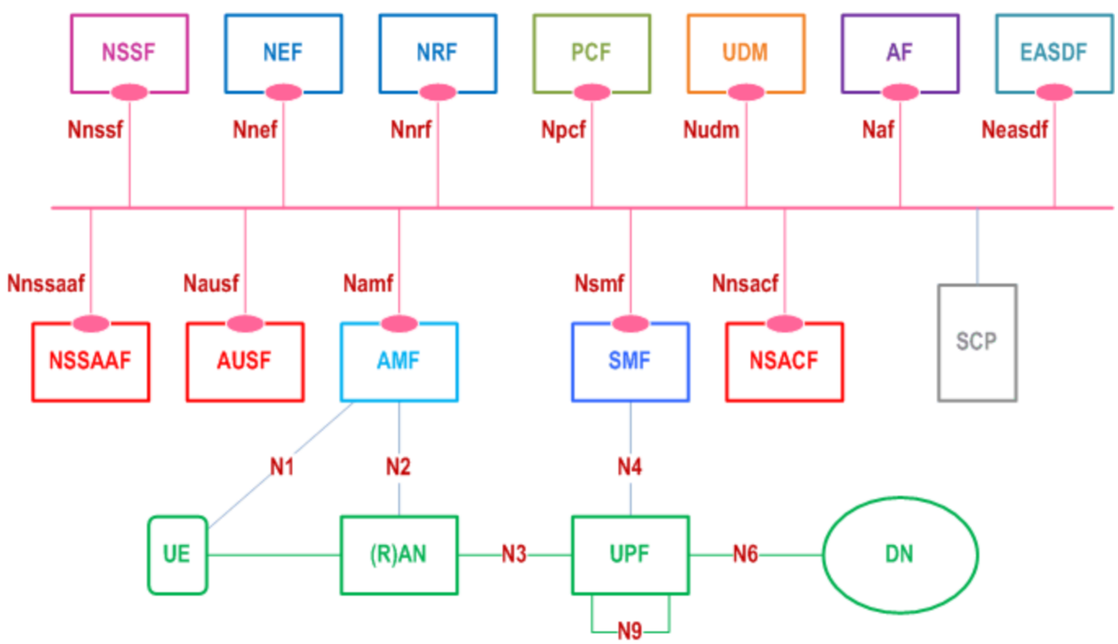
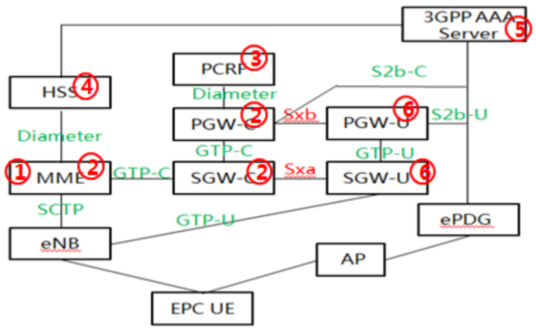


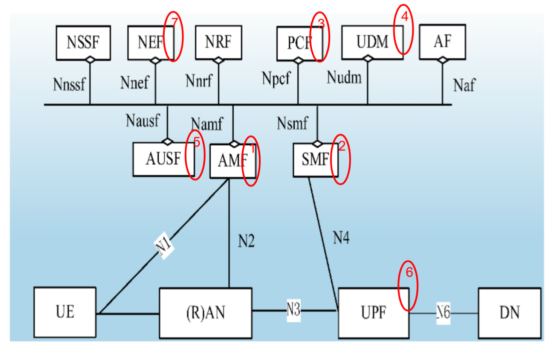
Figure 1: Non-Roaming 5G System Architecture

In comparison to EPC, where each entity (such as MME, S-GW, P-GW, etc.) represents a logical node (separate VM instance), 5GCN introduces Service-Based Architecture (SBA), where nodes (NFs) are usually deployed as containers (just a process with separated file and network systems which is sharing host OS kernel), so called microservices. Consequently, the communication is also somewhat new - over HTTP2 with JSON payloads. Such architecture improves flexibility, availability, and scalability.

Besides, the nodes itself are separated even further. Figure 2 illustrates this separation and which node corresponds to which NF in 5G.



4G network architecture



5G network architecture

Figure 2: 4G/5G Network Architecture Comparison

2.1 Network Functions

Below is the listing of main network functions in 5G architecture:

- **AMF (Access and Mobility Management Function):** Handles registration management, connection management, reachability, mobility management, access authentication, and authorization. Also supports lawful interception (LI), session management (SM) message forwarding between the UE and SMF, and SMS message forwarding between the UE and SMSF.
- **SMF (Session Management Function):** Responsible for UE IP address allocation and management, selection and control of UPFs, configuration of UPF traffic redirection, and forwarding traffic to the correct destination network. Also handles lawful interception (LI), charging data record (CDR) collection, downlink data notifications, policy control, and QoS enforcement.
- **UPF (User Plane Function):** Serves as the data-plane anchor and the PDU session point connected to the data network (DN). Provides packet routing and forwarding, packet parsing, and policy enforcement. Also supports lawful interception (UP collection).
- **UDM (Unified Data Management):** Manages subscription data and NF registration for subscriber services. Generates 3GPP AKA authentication parameters and performs subscription-based access authorization (e.g., roaming restrictions). Supports service/session continuity.
- **AUSF (Authentication Server Function):** Primarily responsible for authentication services.
- **PCF (Policy Control Function):** Provides unified policy management for network behavior and supplies policy rules to the control plane for enforcement. Retrieves subscription data from the UDR for policy decisions.

- **NEF (Network Exposure Function):** Exposes 3GPP network capabilities and events to (Application Functions) AFs, third parties, and edge computing platforms. Obtains external application information from AFs for internal use. Provides translation between internal and external information and stores exposed data in the UDR.
- **UDR (Unified Data Repository):** Stores and retrieves subscription data for the UDM, policy data for the PCF, and structured data for the NEF (for network capability exposure and application detection).
- **NSSF (Network Slice Selection Function):** Selects network slice instances for a UE. Determines the allowed NSSAI and, if needed, maps subscribed S-NSSAIs. Identifies an AMF set for serving the UE or provides a list of candidate AMFs through NRF queries.
- **NRF (Network Repository Function):** Enables NF service discovery and maintains information about available NFs, including their supported services.

2.2 Network Architecture Highlights

2.2.1 SBA

Service-based Architecture (SBA) is a cloud-native, modular design where network functions provide and consume services via a Service-based Interface (SBI) using RESTful APIs over HTTP/2.

In this communication, some NF may provide one or more services to other NFs. In certain situations, one is a consumer and the second is a producer.

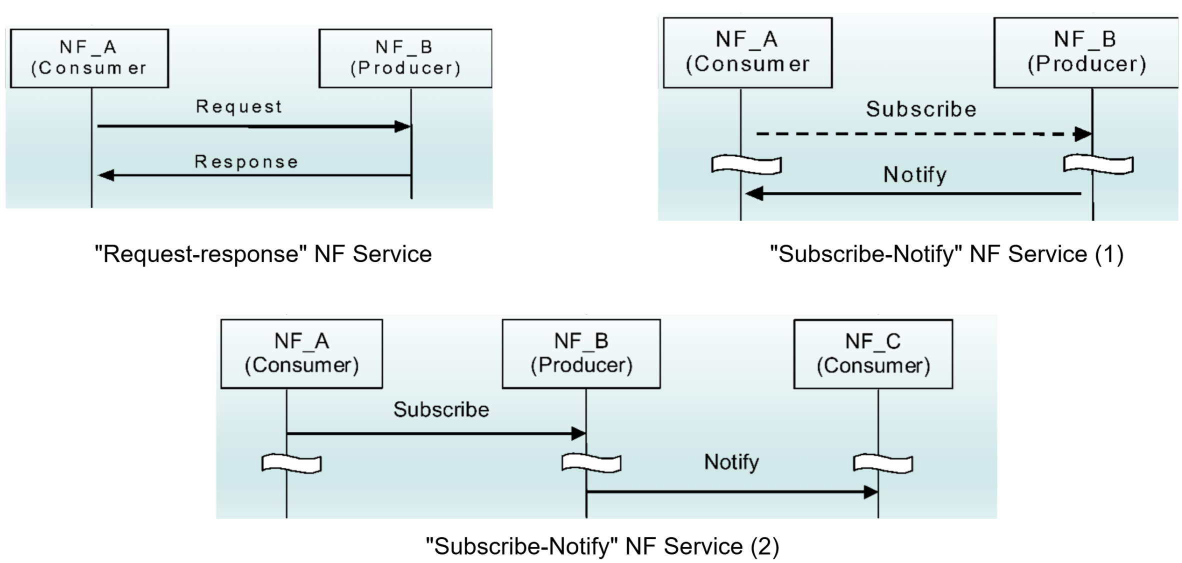


Figure 3: Illustration of interaction between NFs

Figure 4 depicts an example of AMF profile, which may be stored in NRF. Other NFs may query the NRF to find AMF instances that support a particular service, slice, or a region.

AMF Profile	
NF Type	AMF
NF ID	AMF instance ID
NF Service	Namf_Communication, Namf_EventExposure, Namf_MT, Namf_Location
PLMN ID	MNC,MCC
AMF Status	e.g. available/unavailable
NF Capability	Static capacity, indicating the relative weight of an AMF instance.
FQDN and/or IP	FQDN and/or IP address of an AMF.
AMF Load	Dynamic load of an AMF.
AMF Region ID	Region ID of an AMF.
AMF Set ID	Set ID of an AMF.
GUAMI list	GUAMI 1, 2, 3...
TAI List	List of TAIs supported by an AMF.
S-NSSAI list	S-NSSAI 1, 2, 3...

Figure 4: AMF Profile Example

2.2.2 Network Slicing

Network slicing allows a physical network to be divided into multiple virtual networks, each tailored to a specific business use case. Below are three common standardized 5G use cases:

- **eMBB (enhanced Mobile Broadband):** high data rate services such as video streaming and VR/AR.
- **URLLC (Ultra-Reliable Low-Latency Communication):** mission-critical services requiring low latency and high reliability.
- **mMTC (massive Machine-Type Communication):** massive IoT connectivity with low data rates per device.

Single Network Slice Selection Assistance Information (S-NSSAI) identifies each network slice instance. It consists of:

- **Slice/Service Type (SST)** — mandatory, indicates the type or characteristics of the slice.
- **Slice Differentiator (SD)** — optional, differentiates multiple slices of the same type.

S-NSSAIs containing only the standardized SST can be interpreted across different PLMNs.

Network Slice Selection Function (NSSF) is a 5G Core network function responsible for selecting network slices based on the UE's request, allowed subscriptions, and defined S-NSSAI values. NSSF also selects the appropriate set of AMFs to serve the UE. Additionally, it can consume network analytics from the **Network Data Analytics Function (NWDAF)** to optimize slice selection.

Logical Flow: When a UE initiates registration, it may include its requested S-NSSAI. The AMF forwards this to the NSSF, which determines the allowed slice(s) and the serving AMFs. This ensures that each UE is assigned to a network slice appropriate for its service requirements.

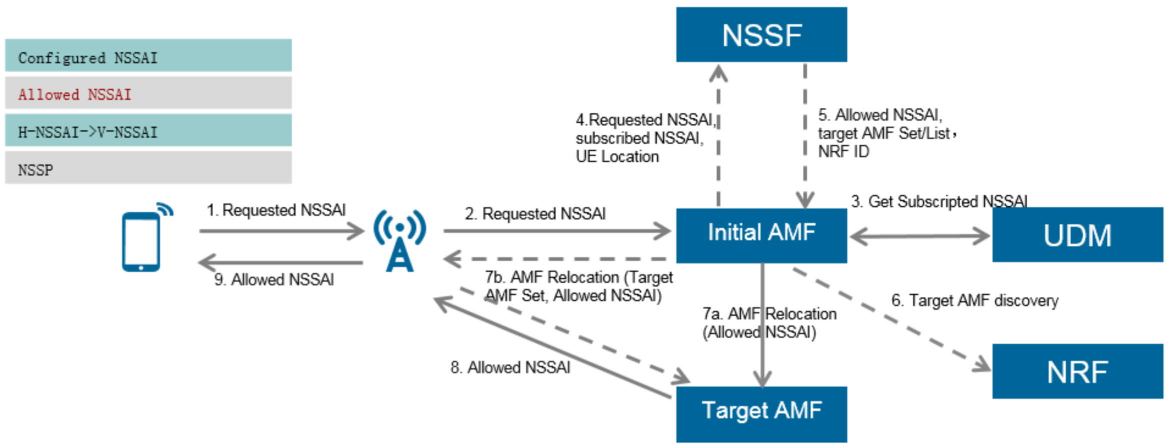


Figure 5: Slice Selection During Registration

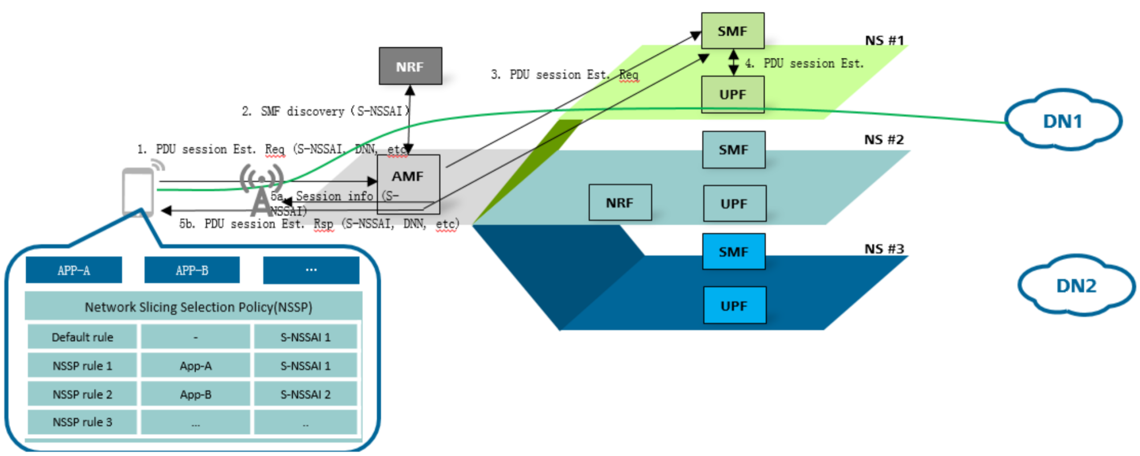


Figure 6: Slice Selection During PDU Session Establishment

2.3 Network Interfaces and Protocols

Service-Based Interfaces (SBIs) are used by network functions such as Namf, Nsmf, Nudm, Nnrf, Nnssf, Nausf, Nnef, Nsmsf, Nudr, Npcf, N5g-eir, and Nlmf. These interfaces rely on application-layer protocols such as JSON and Protobuf for data exchange.

Figure 7 depicts the high-level structure of the N1 interface protocol stack. The N1 interface connects the UE and the AMF and is control-plane only. It uses the NAS protocol for purposes such as:

- Initial registration;
- Session and mobility management;
- Authentication and security procedures;

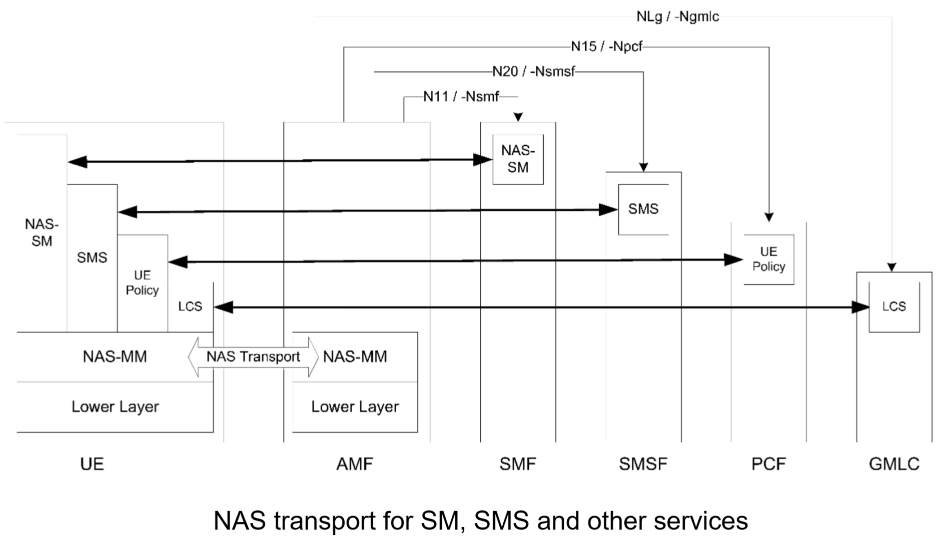


Figure 7: N1 Interface Protocols

Figure 8 illustrates the N4 interface protocol stack for the control plane. The N4 interface interconnects the SMF and the UPF and is also control-plane only. It uses the PFCP protocol for communication. The SMF controls the UPF via N4 by installing forwarding rules such as:

- Packet Detection Rules (PDRs);
- Forwarding Action Rules (FARs);

Figure 9 presents the protocol stacks for the N3 and N9 interfaces. These are user-plane interfaces using GTP-U:

- N3: Between the gNB and the UPF, responsible for user data transfer between RAN and the Core Network.
- N9: Between two UPFs, enabling inter-UPF connectivity for advanced use cases such as local breakout, uplink traffic classification (UL/CL), and session continuity.

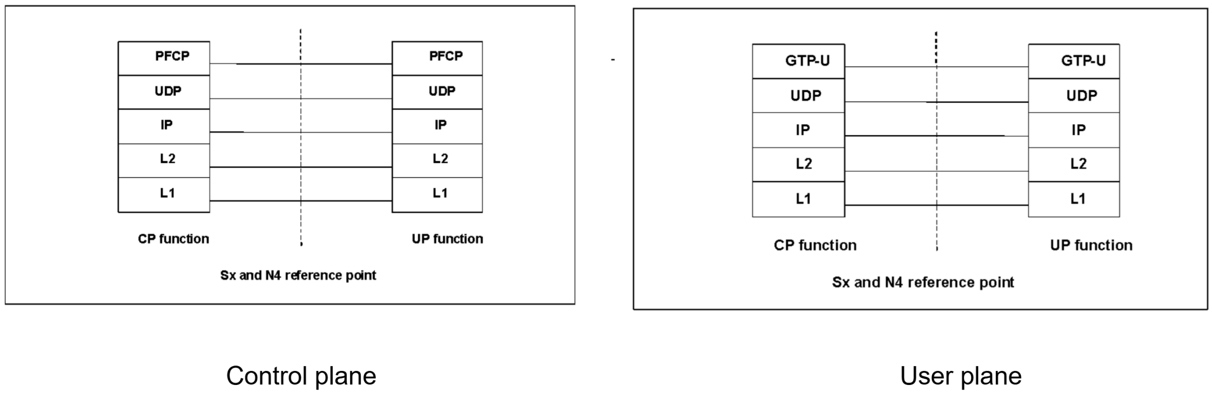


Figure 8: N4 Interface Protocols

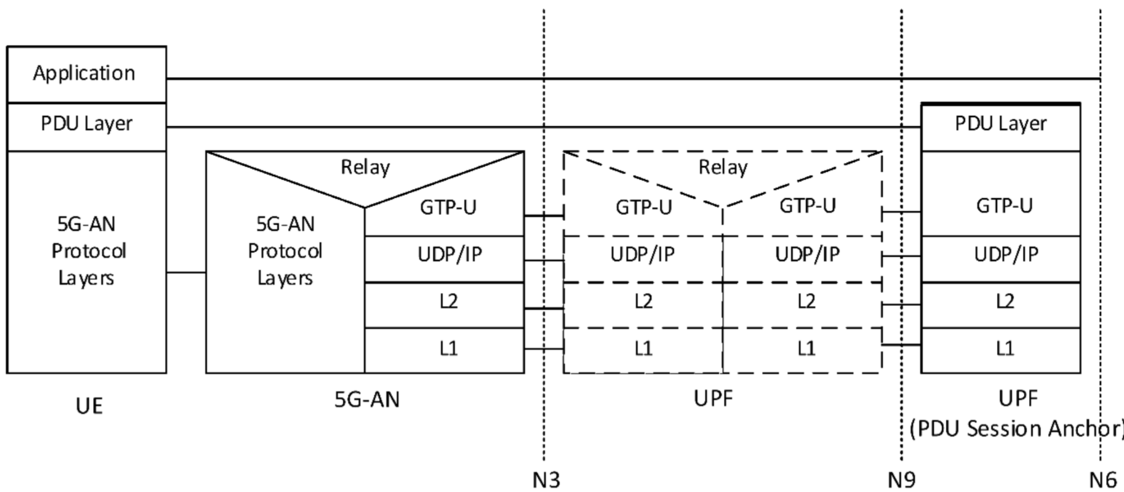


Figure 9: N3 and N9 Interface Protocols

3 Basic Concepts of 5G Core Network

3.1 Basic MM concepts

3.1.1 Subscriber Identifier and Location Identifier

Subscription Permanent Identifier (SUPI) represents IMSI (TS 23.003) or a network-specific identifier (TS 22.261) and is stored in the UDM/UDR. **SUPI** can be based on IMSI or non-IMSI and in NAI format (RFC 7542). The difference with the EPC IMSI is that **SUPI** is never sent in cleartext over the air in 5G; instead, it is protected by **Subscription Concealed Identifier (SUCI)**.

Generic Public Subscription Identifier (GPSI) represents a public identity of a UE inside and outside the 3GPP system.

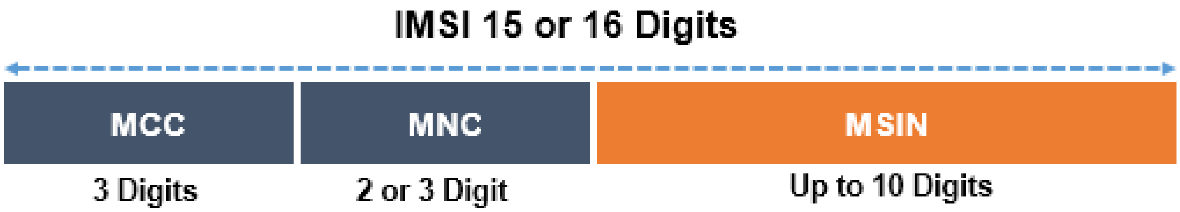


Figure 10: SUPI Format

GPSI is a public identifier used to address a subscriber's 3GPP subscription in external data networks. It is a public identifier, unlike the private SUPI, and can take the form of a Mobile Station ISDN Number (MSISDN) or an external ID. The 3GPP system stores the association between the GPSI and the corresponding SUPI within the subscription data, but there is no one-to-one mapping between them. GPSI is generic and is not limited to MSISDN—it supports Voice over New Radio (VoNR) and data-only services.

Permanent Equipment Identifier (PEI) represents a code that uniquely identifies the UE accessing the network. In 3GPP Release 15, PEI is in the format of IMEI.

	AA	-	BB	BB	BB	-	CC	CC	CC	D or EE
Old IMEI	TAC			FAC		Serial number				(Optional)D=Luhn checksum
New IMEI	TAC									
Old IMEISV	TAC			FAC						EE=Software Version Number(SVN).
New IMEISV	TAC									

Figure 11: PEI Format

5G Globally Unique Temporary Identifier (5G-GUTI) is allocated by the Access and Mobility Management Function (AMF). The AMF can allocate a 5G-GUTI to a UE at any time. 5G-GUTI is used for both 3GPP and non-3GPP systems. It serves as a substitute for the UE's permanent identity (SUPI) during interactions with the network, ensuring sensitive subscriber information is not transmitted over the air.

When a UE powers on or moves into a new network area (and does not have a valid GUTI), it sends a Registration Request to the gNB. If the UE already holds a valid GUTI from a previous session, it can include that in the Registration Request (instead of the SUPI) to expedite identification. If no valid GUTI exists, the UE might have to include its SUCI, which the network can use to derive the SUPI. From that point on, the AMF uses the 5G-GUTI to track the UE's NAS signaling context (mobility management, session management, etc.).

Once assigned, the UE uses this identifier to communicate with the network in subsequent NAS signaling procedures—rather than using its permanent identifier (SUPI, e.g., IMSI).

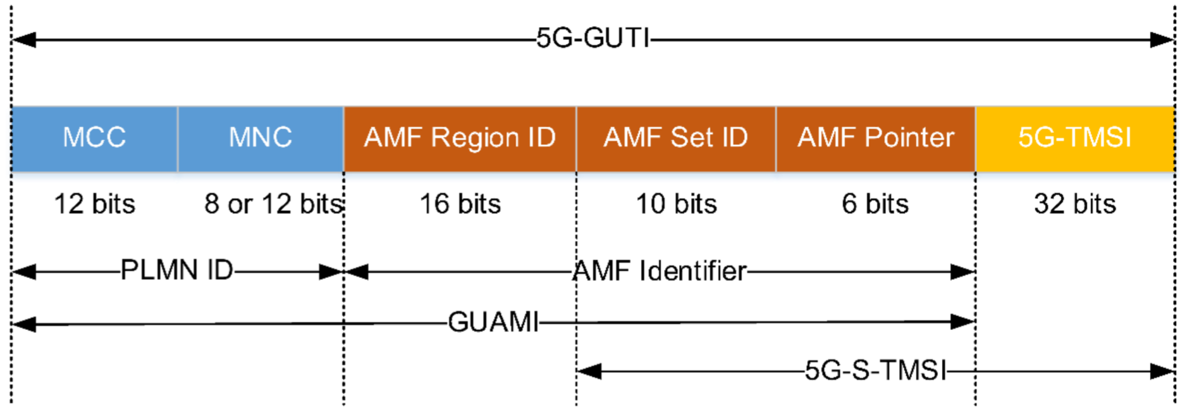


Figure 12: GUTI Format

5G Short-Term Mobile Subscriber Identity (5G S-TMSI) is a temporary identifier assigned to a mobile device by the network to protect the device's identity during normal operation. The S-TMSI is used instead of the IMSI to reduce signaling overhead and improve security.

It is used in paging messages and service requests (UE establishing a connection with AMF). 5G S-TMSI includes the AMF Set ID, AMF Pointer, and 5G-TMSI.

Subscription Concealed Identifier (SUCI) is a temporary identifier for hiding SUPI. The AMF/SEAF supports SUCI-triggered authentication. SUPI can be of IMSI or network-specific identifier type, but when the SUPI type is IMSI, the home network identifier is the PLMN ID. SUCI prevents IMSI catching attacks, which was a big weakness in LTE.

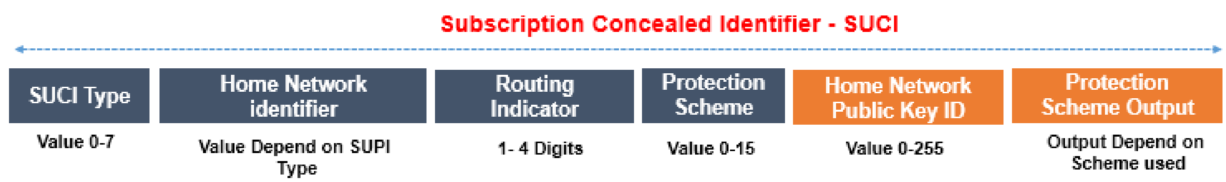


Figure 13: SUCI Format

3.1.2 Subscriber Status

5G introduces new mobility management (MM) status and provides on-demand MM through the mobility pattern. The Registration Management (RM) and Connection Management (CM) statuses are independent from each other. The RM status idicates whether a UE has registered with a network. The CM status indicates whether a signalling connection has been set up between a UE and the core network.

RRC-inactive state was introduced on the RAN side: A UE is in connected state for the core network, but in idle state for the RAN.

The SM status (PDU session state: active or inactive) is implicitly defined by the activation and deactivation procedures of the per-PDU session.

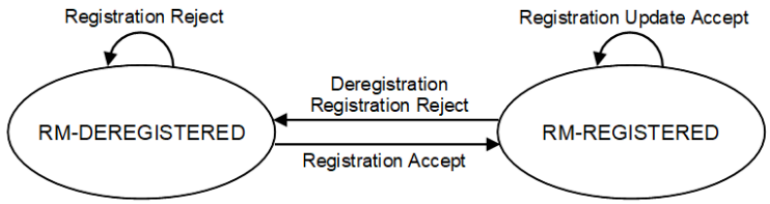


Figure 5.3.2.2.4-1: RM state model in UE

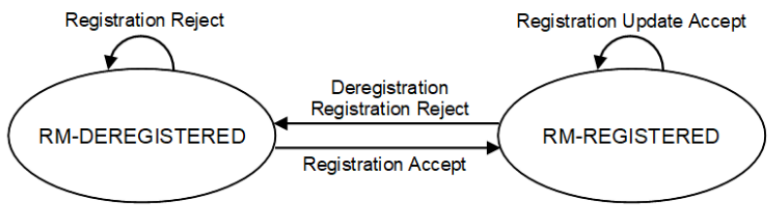


Figure 5.3.2.2.4-2: RM state model in AMF

Figure 14: RM states in UE and AMF

3.1.3 On-Demand Mobility Management (MM)

The AMF determines and updates the mobility pattern of a UE based on subscription data, UE mobility statistics, network policy, UE restrictions, or any combination thereof. This mobility pattern allows the AMF to optimize mobility support, such as registration area allocation. Additionally, the AMF can provide assistance data to the RAN to optimize RRC and CN states and improve paging efficiency.

Mobile Initiated Connection Only (MICO) mode allows a UE to stop listening to paging channels while still initiating communication proactively. This reduces power consumption and is particularly suitable for IoT devices with low-power requirements.

A UE can indicate preference for MICO mode during initial or periodic registration. The AMF then decides whether MICO is allowed. If the UE operates in MICO mode, the registration area allocated by the AMF may cover the entire PLMN or the service area supported by the AMF, reducing the frequency of mobility registration updates.

While in MICO mode, a UE suspends access stratum (AS) procedures in the CM-IDLE state but initiates them in the following situations:

- A change in the UE (e.g., configuration updates) requires registration with the network.
- The periodic registration timer expires, triggering a periodic registration update.

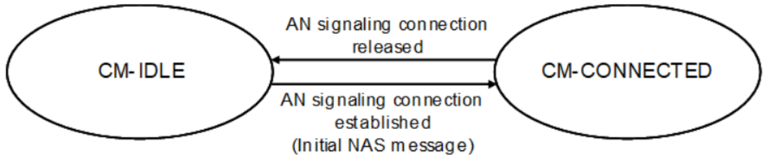


Figure 5.3.3.2.4-1: CM state transition in UE

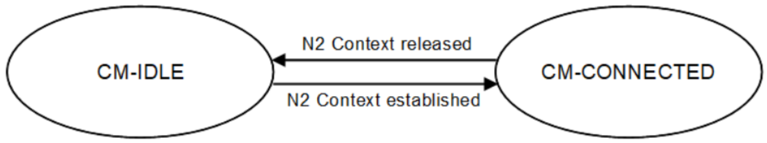


Figure 5.3.3.2.4-2: CM state transition in AMF

Figure 15: CM states in UE and AMF

- The UE initiates a Service Request (SR) due to pending Mobile Originated (MO) data.
- The UE initiates an SR due to pending MO signaling.

3.2 Basic Session Management Concepts

In EPC, user-plane connectivity is established using the concept of *EPS Bearers*. An EPS Bearer represents a logical tunnel with defined QoS parameters between the UE and the Packet Data Network Gateway (P-GW). Each PDN connection consists of one **default bearer** (best-effort service) and optionally multiple **dedicated bearers** for services requiring specific QoS characteristics. Bearer establishment, modification, and release involve signaling procedures over S5/S8 (between SGW and PGW) and S1-U (between eNB and SGW) using GTP-U encapsulation, with QoS enforced via TFT (Traffic Flow Template) rules.

On the other hand, 5GCN eliminates bearer-based granularity and introduces *PDU Sessions* as the fundamental unit of connectivity between the UE and a DN. Each PDU Session is associated with a single data network identified by a DNN and a single IP address or Ethernet MAC (or unstructured PDU). Within a PDU Session, QoS is provided at the QoS Flow level. QoS Flows are identified by QFI (QoS Flow Identifier) and are enforced by UPF via PDR/FAR rules over the N4 interface. All QoS Flows within a PDU Session are multiplexed into a single GTP-U tunnel between gNB and UPF (N3 interface), unlike EPC where each bearer has a dedicated tunnel.

3.2.1 PDU Session

A PDU session is a logical connection between a UE and a Data Network (DN) that enables the exchange of Protocol Data Units (PDUs). The UE always initiates the establishment of a PDU session. Each Data Network is identified by a Data Network Name (DNN). The PDU session can be of different types: *IPv4*, *IPv6*, *IPv4v6*, *Ethernet*, or *Unstructured*.

The allocated IP address for a PDU session may be either static (as provisioned in the UDM) or dynamic. Dynamic IP allocation can be provided by:

- *SMF:* Allocated by the H-SMF in the Home Routed (HR) scenario, or by the V-SMF in the Local Breakout (LBO) scenario;
- *DHCP Server*;
- *AAA Server*;

If multiple IP address allocation methods are available, the PCF may instruct the SMF to select a specific allocation mode.

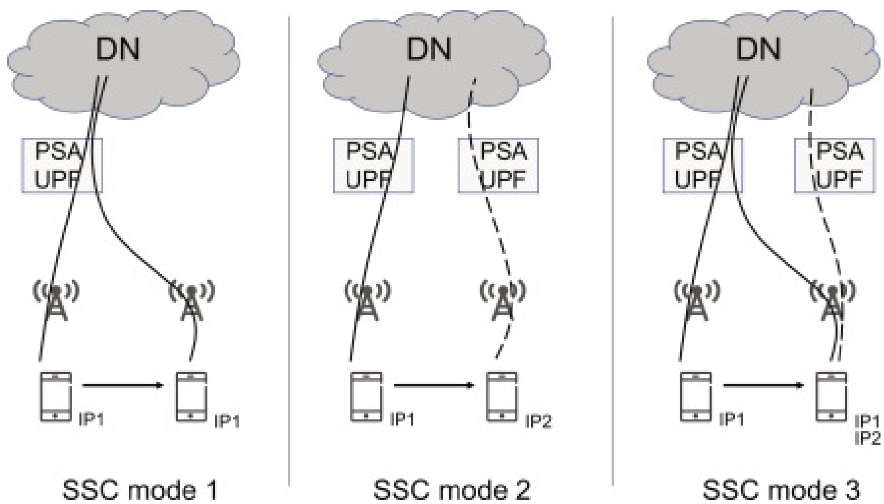


Figure 16: Three SSC Modes

Session and Service Continuity (SSC) Modes: SSC defines how the UE and the network maintain the IP address and service continuity during mobility events or session changes. There are three SSC modes supported in 5G:

- **SSC Mode 1:** The UE keeps the same IP address for the lifetime of the PDU session. This is similar to LTE's behavior and ensures continuity for applications requiring a stable IP address.
- **SSC Mode 2:** The UE can change its IP address during mobility events, but the PDU session remains the same. This mode provides flexibility and is suitable for applications that can handle IP changes.
- **SSC Mode 3:** A new PDU session is established when moving between different network areas, resulting in a new IP address. This mode is often used for session isolation or policy-based separation of services.

3.2.2 Data Network Name (DNN)

The Data Network Name (DNN), as defined in 3GPP TS 23.501 (Release 15), is functionally equivalent to the Access Point Name (APN) used in EPC networks. Both identifiers have similar meanings and convey the same type of information, serving as a reference to the target data network.

A DNN may be used for the following purposes:

- To select an appropriate SMF and UPF for establishing a PDU session.
- To identify the corresponding Data Network (DN) accessible via the N6 interface.
- To determine and enforce policies associated with the specific PDU session.

3.3 NF Selection

The selection of network functions in the 5GC depends on multiple factors, including subscription information, requested services, network policies, and load conditions. The following outlines the key impact factors for NF selection.

3.3.1 AN Selection of AMF

The AN selects an AMF based on:

1. AMF set selection based on the requested NSSAI;
2. AMF selection based on reachability and load balancing;
3. AMF selection based on UE identifiers, such as a previously assigned 5G-GUTI or S-TMSI.

3.3.2 AMF Selection of SMF

The AMF selects an SMF for PDU Session management based on:

1. Requested DNN;
2. Associated S-NSSAI;
3. Subscription data retrieved from the UDM;
4. Current load status and operator policies.

3.3.3 SMF Selection of UPF

The SMF selects the UPF instance based on:

1. UPF load and capacity;
2. UPF location relative to the UE for latency optimization;
3. UE location;
4. DNN associated with the PDU Session;
5. Selected SSC mode;

6. Slice-related information such as S-NSSAI;
7. Policy decisions from the PCF.

3.3.4 Other NF Selection Rules

- AMF selects an AUSF based on the SUPI, the Home PLMN ID (HPLMN ID) derived from the SUCI, and the AUSF group ID.
- AMF selects a UDM based on SUPI, HPLMN ID of SUCI, GPSI, routing ID of SUCI, or UDM group ID.
- SMF selects a PCF based on DNN, S-NSSAI, SUPI range, and local policy.

4 Basic 5G Procedures

4.1 Mobility Management

The registration procedure is used for an initial registration, a registration triggered by an RA change, and a periodic registration update between the UE and network. There are four registratin procedures:

- initial registration, which is similar to an attach procedure on an LTE network
- Mobilit registration procedure, which is similar to a TAU procedure on an LTE network
- Periodic registration procedure, which is similar to a periodic TAU procedure in LTE network
- Emergency registration.

The Figure 17 and Figure 18 depicts high-level overview of the registration procedure.

4.2 Session Management

The PDU session establishment procedure is used to establish a PDU session. After a PDU session is established, the network assigns an IP address to a UE and establishes a dedicated channel from the UE to the DN. The UE can use this IP address to access services on the DN. Alternatively, the PDU session establishment procedure can be used for inter-RAT session handover or for 3GPP and non-3GPP session handovers.

The Figure 19 and Figure 20 depicts high-level communication flow example of the PDU session establishment.

5 References

- Basic concepts of 5G Core Network: O3 | GTS Community, `https://cn.o3.huawei.com/cg/cn/zh/training/courses/courseware?code=274e6374f79540d6960573b`

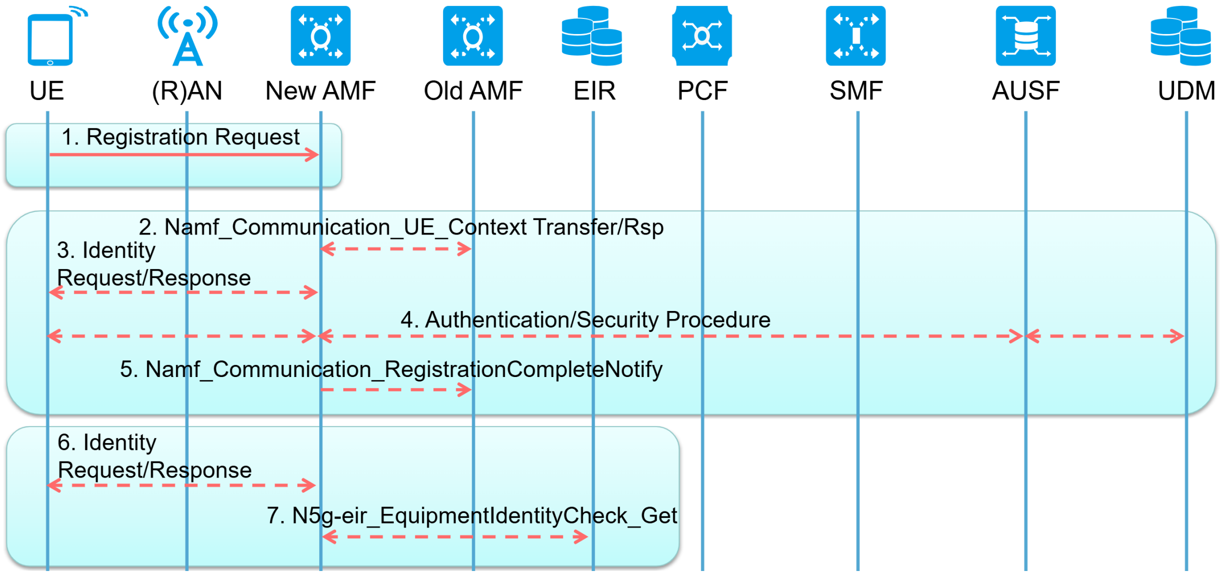


Figure 17: Registration Procedure

`98e5930af&from=JC&sessionId=EN-292&journeyId=EN-1229&planId=undefined&type=coursesa`

- 5G GUTI Overview, `https://www.sharetechnote.com/html/5G/5G_GUTI.html`
- 5G UE IDs Explanation, `https://www.sharetechnote.com/html/5G/5G_UEID.html`
- 3GPP TS 23.316: Wireline Access to 5GC (5G-RG and FN-RG) Overview, `https://www.tech-invite.com/3m23/toc/tinv-3gpp-23-316_j.html`
- 3GPP TS 23.502: 5GS Registration Procedures, `https://www.tech-invite.com/3m23/toc/tinv-3gpp-23-502_b.html`
- SUPI and SUCI Identifiers in 5G, `https://www.techplayon.com/5g-identifiers-supi-and-suci/#Related_Posts`
- 5G Technology Video Presentation, `https://www.3g4g.co.uk/5G/5Gtech_video0038.pdf`

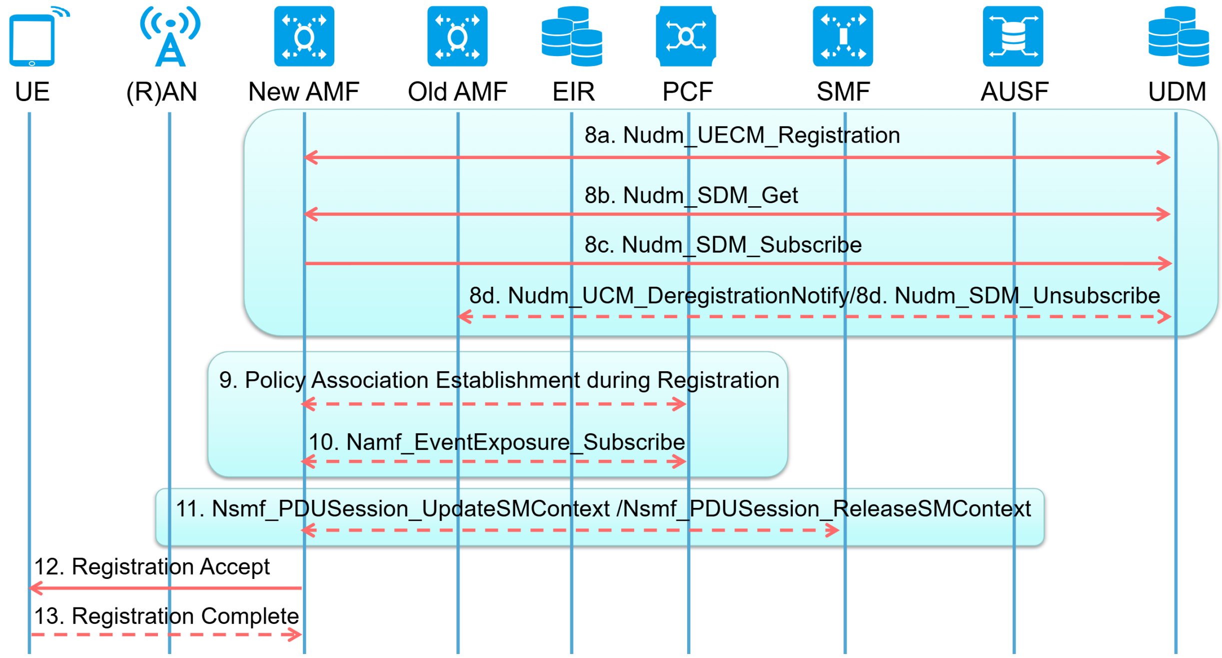


Figure 18: Registration Procedure

6 Appendix

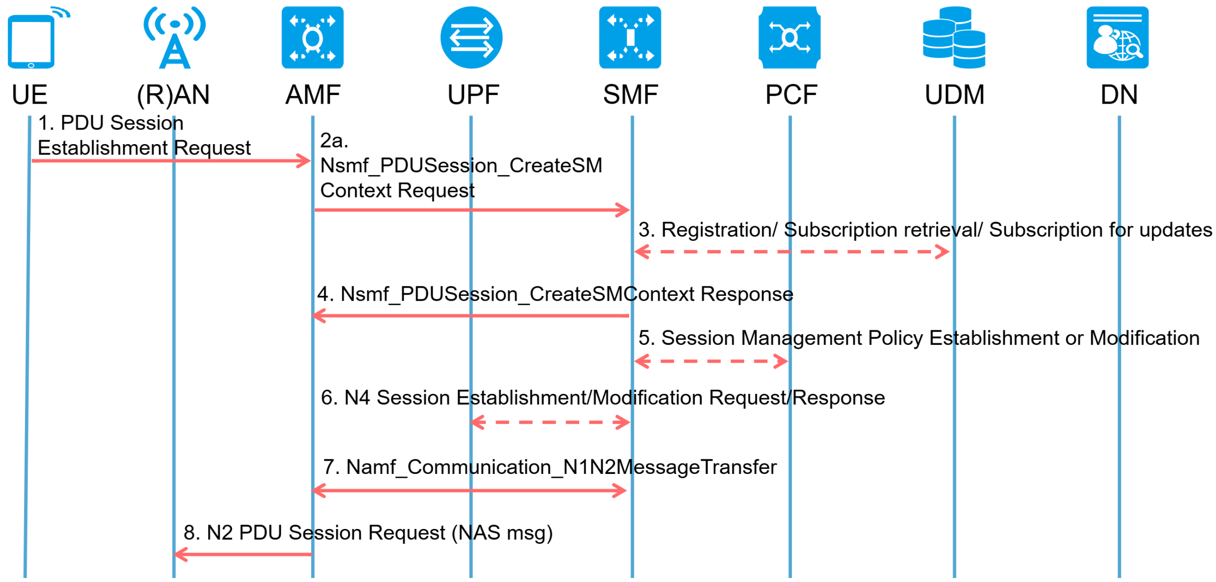


Figure 19: Session Establishment Procedure

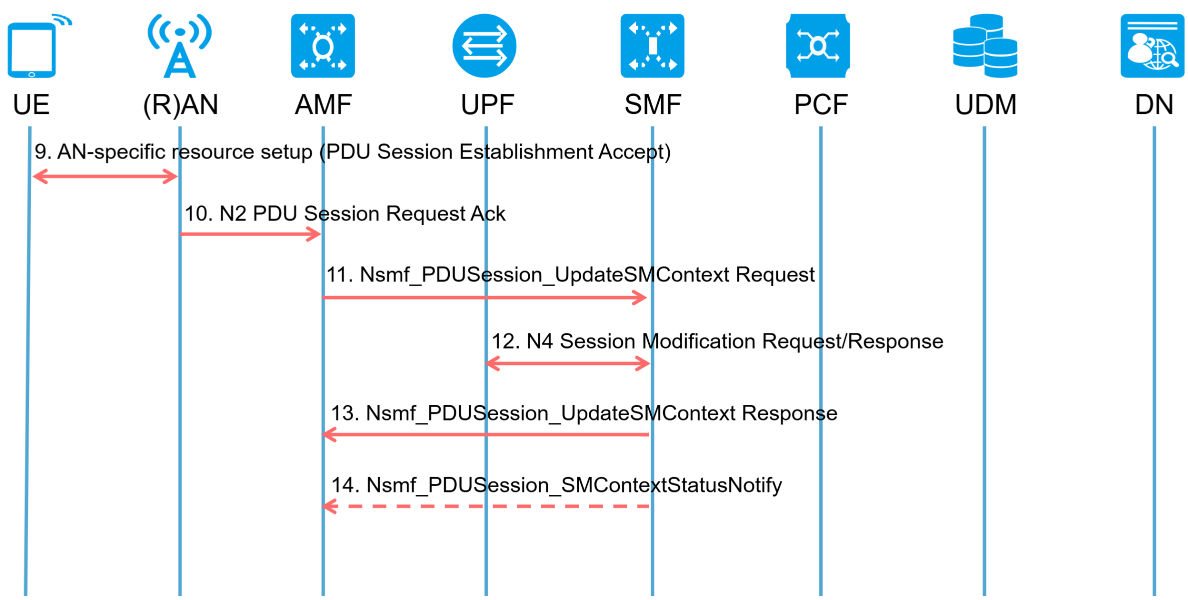


Figure 20: Session Establishment Procedure