5G AMF Overview

Product Description

The Access and Mobility Management Function (AMF) is one of the control plane network functions (NF) of the 5G core network (5GC). The 5G AMF, is an evolution of 4G MME, continuing with the Control Plane and User Plane Separation, and with further simplifications like moving the Sessions Management functions to the SMF and, providing common SBA interfaces.

Figure 1: EPC with Control Plane User Plane Separation Enhancement

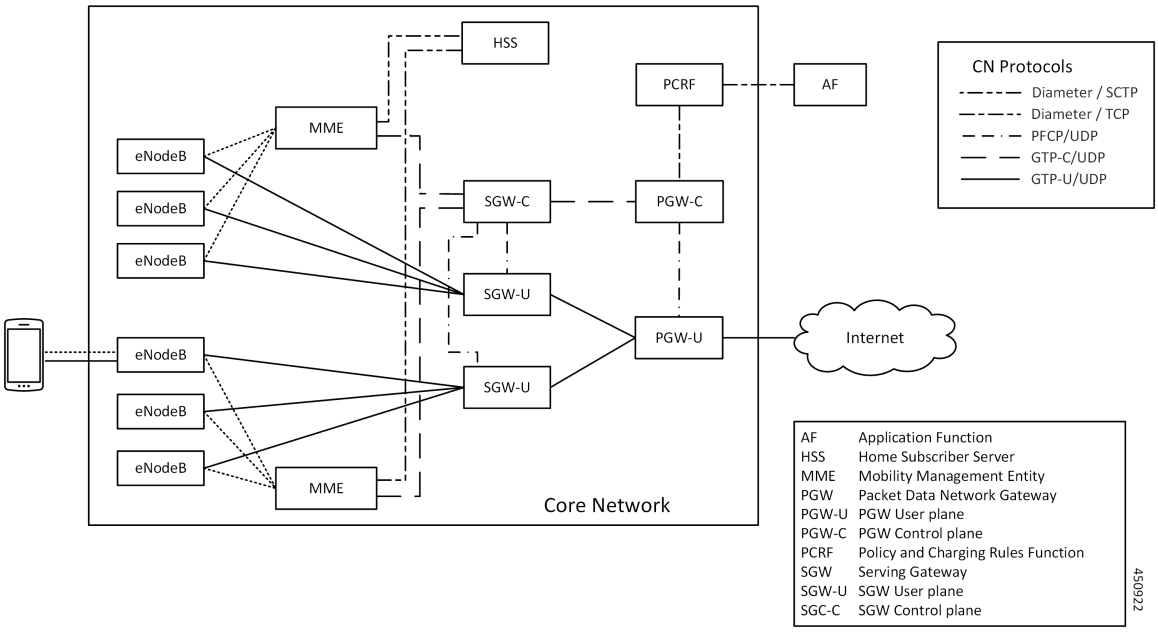
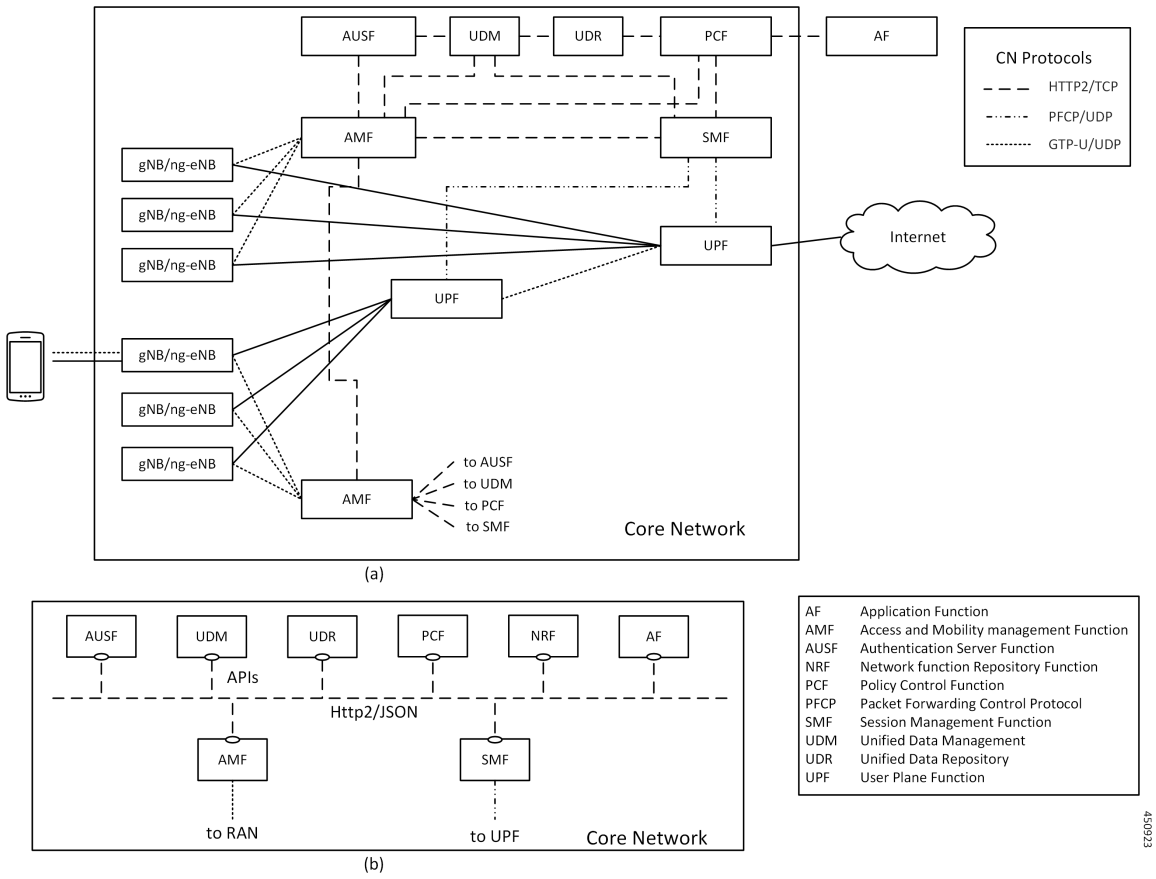


Figure 2: 5G Core Network - (a) Interface Representation, and (b) API Level Representation



Use Cases and Features

The main functions of AMF are to support:

- Connection management, registration, and mobility management with UE.
- It terminates the control plane of 5G Radio Access Network and manages the register/deregister status/mobility of UEs.

This section describes the use cases that AMF supports.

4G EPC Interworking with N26

The N26 interface is used to transfer mobiles authentication and session context as the mobile moves between the two systems (MME <-> AMF). This scheme provides seamless mobility to an UE's IP session and hence enables seamless mobility to voice sessions between 4G and 5G. Both Idle and Connected mode handovers are supported.

The following features are related to this use case:

- Internode Registration Support

- N26-based Handover Procedures - EPC Interworking
- N26 Stack Integration Support

AN Release Procedure

The AMF supports procedure to release the logical NGAP signalling connection and the associated N3 User Plane connections and RAN RRC signalling and resources.

- AN-initiated—The AMF supports RAN initiated release because of inactivity, UE initiated connection release, link failure or any other reason.
- AMF-initiated—The AMF supports AMF-initiated release because of:
  - IE value received as a part of prior procedure.
  - Optional timer expiry

The following feature is related to this use case:

- Idle Entry Procedure

Base AMF Configuration

AMF base configuration provides a detailed view of the configurations that are required for making AMF operational. This includes setting up the infrastructure to deploy AMF, deploying AMF through SMI, and configuring the Ops Center for exploiting the AMF capabilities over time.

For more information on SMI, see the *Ultra Cloud Core SMI Cluster Deployer Operations Guide*.

The following feature is related to this use case:

- Deploying and Configuring AMF through Ops Center

CMAS Support

The AMF supports interaction with Cell Broadcast Centre Function (CBCF) for public warning functionality and required messaging toward gNB as well as for realizing broadcast functionality.

The following feature is related to this use case:

- CMAS Service Support

Encryption and Integrity Protection

The AMF supports both 5G-AKA and EAP-AKA' authentications. The following encryption and integrity protection algorithms enable encryption and integrity protection on the N1 interface:

- NEA0/NIA0
- 128-NEA1/128-NIA1
- 128-NEA2/128-NIA2

The following features are related to this use case:

- EAP and AKA Authentication
- Encryption and Integrity Protection

Handover Procedure

The AMF supports procedures to handover a UE from source NG-RAN to target NG-RAN.

- Xn Handover—The AMF supports Xn handover, used to handover a UE from source NG-RAN to target NG-RAN using Xn when the AMF is unchanged.
- N2 Handover—The AMF supports inter-AMF and intra-AMF N2 handovers. These can be triggered due to new radio conditions/load balancing, if there is no Xn connectivity between source and target NG-RAN or due to AMF change.

The following features are related to this use case:

- N2 Handover Procedure
- Xn Handover

Lawful Intercept

The Lawful Intercept (LI) feature enables law enforcement agencies (LEAs) to intercept subscriber communications. The LI functionality provides the network operator the capability to intercept and control messages of targeted mobile users.

For more details, contact your Cisco account representative.

NRF Register/Discovery

The AMF supports register/de-register/update with NRF. The AMF includes various query parameters, such as nf-type, plmn-info, slice-data, DNN, routing-indicator when it sends the NFDiscovery request towards the NRF during discovery of network elements. When AUSF, UDM, PCF, and SMF aren't locally configured, the AMF queries the NRF NF discovery API to discover them.

The following feature is related to this use case:

- NRF (Network Function Repository) Services

OAM Support

The AMF provide counters and alarms/alerts for monitoring the AMF-specific functionality and features.

The following features are related to this use case:

- Application-based Alerts
- Deploying and Configuring AMF through Ops Center
- Pods and Services Reference

- Smart Licensing
- AMF Rolling Software Upgrade
- Troubleshooting

For more information, you can also see the following documents:

- *UCC 5G AMF - Metrics Reference*
- *UCC 5G AMF - CLI Reference*

PDU Session Establishment

The UE receives data services through a Protocol Data Unit (PDU) session, which is a logical connection between the UE and core network. In a PDU session establishment, the UE establishes a PDU session for accessing data services. Unlike EPS, where a default PDU session is always created while the UE registers to the network, in 5G, the UE establishes a PDU session when service is needed.

The following feature is related to this use case:

- Compliance to 3GPP Specifications

PDU Session Modification

The PDU session modification procedure happens when one or several of the QoS parameters exchanged between the UE and the network are modified. Both UE- and SMF-initiated PDU session modifications are supported.

The following feature is related to this use case:

- Compliance to 3GPP Specifications

PDU Session Release

The PDU session release procedure is used to release all the resources associated with a PDU Session. This can either be initiated by the UE or the SMF.

The following feature is related to this use case:

- Compliance to 3GPP Specifications

Redundancy Support

The AMF support high availability for AMF specific pods and ensures session continuity in case of Pod failure.

The following feature is related to this use case:

- High Availability Services

Roaming and Restriction Support

The AMF supports subscribers moving seamlessly in geographies beyond their network reach. Restriction control is also supported. Steering of Roaming (SoR) is supported at AMF.

The following feature is related to this use case:

- Roaming Support

Service Request Procedure

The AMF supports the Service Request procedure used by a UE in CM-IDLE state or the 5GC to request the establishment for a secure connection to an AMF. The Service Request procedure is also used when the UE is in CM-IDLE and in CM-CONNECTED state to activate a User Plane connection for an established PDU Session.

- UE Triggered—The AMF supports UE in Idle state initiating Service request procedure for sending uplink signalling messages, user data or other reasons.
- Network Triggered Service Request/Paging—The AMF supports procedure when the network needs to send Paging Request to RAN based on trigger(s) from UDM, SMF and other NF nodes. The paging request triggers the UE to initiate Service Request procedure.

The following features are related to this use case:

- Paging Support
- Service Request Procedure

SMS over NAS

The AMF supports registration and deregistration for SMS over NAS. MO/MT SMS are supported in CM-IDLE/CM-CONNECTED state.

The following feature is related to this use case:

- SMS over the Non-Access Stratum Procedures

UE Configuration Update Procedure

The AMF supports UE Configuration Update procedure for access and mobility management related parameters, such as GUTI, TAI-list.

The following feature is related to this use case:

- UE Configuration Management Procedures

Deregistration

To enable UE to deregister from 5GS network.

- UE-init Deregistration—The deregistration procedure allows the UE to inform the network that it doesn't want to access the 5G data services.
- Network-init Deregistration—The deregistration can be initiated by the UDM if the subscription is withdrawn for the UE or UE has moved to another node. It can also be initiated by AMF based on OAM requirements.

The following feature is related to this use case:

- Compliance to 3GPP Specifications

Registration

To enable UE tracking and reachability, a UE must register with the authorized network to receive services.

- Initial Registration—The AMF supports initial UE registration to 5GS network.
- Mobility Registration Update—The AMF supports mobility registration update:
  - When changing to new Tracking Area (TA) outside the UE's Registration Area in Connected/Idle state.
  - When the UE needs to update its capabilities or negotiated parameters.

  AMF also supports registration with AMF change.
- Periodic Registration Update—The AMF supports periodic registration to the UE to confirm its availability. The procedure is controlled in the UE by the periodic registration update timer, T3512. The value of the T3512 timer is sent by the AMF to the UE in the Registration Accept message. The UE registers periodically as per the T3512 timer interval.
- Emergency Registration—The AMF supports Emergency Registration without authentication/subscription.

The following feature is related to this use case:

- Compliance to 3GPP Specifications

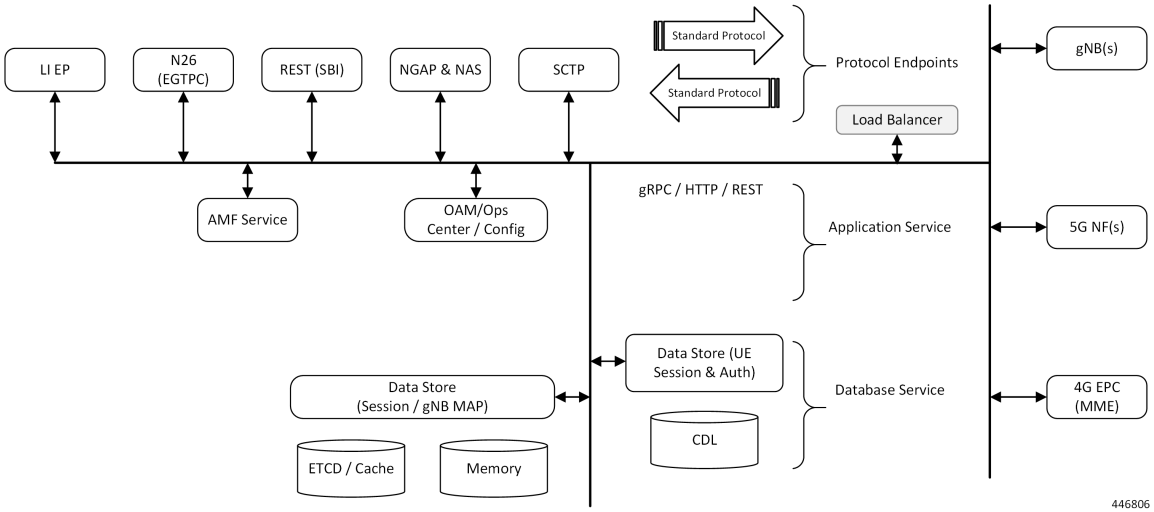
Deployment Architecture and Interfaces

The Cisco AMF is a part of the 5G core network functions portfolio with a common mobile core platform architecture. The core network functions include Session Management Function (SMF), Network Repository Function (NRF), Policy Control Function (PCF), Network Slice Selection Function (NSSF), and User Plane Function (UPF).

AMF Architecture

The software architecture of the AMF is shown in the following diagram.

Figure 3: AMF Architecture



The SCTP endpoint (EP) pod type supports the SCTP interface between the AMF and gNB. Only a single SCTP EP pod is run at a time. In addition to a GUAMI, the SCTP bind address is also unique to an AMF. If multiple SCTP EPs are run, they have to bind to different SCTP addresses, at which time they would not be part of the same AMF.

The SCTP EP converts each message into a GRPC message with the SCTP Payload. Unlike TCP, SCTP messages are delimited by the protocol, so there is no other knowledge that the SCTP EP needs to figure out message boundaries.

The NGAP EP or Node Manager provides termination for NGAP messages. Node Manager terminates the handling of all NGAP messages from a gNB. All messages from gNB are handled by a single Node Manager, but one Node Manager can handle messages from multiple gNBs. This allows a Node Manager to manage the state of both gNB, and one connection between a UE, gNB and AMF. If messages from the same gNB were distributed across multiple instances of Node Manager, there is no single entity in the AMF that is responsible for the state of a gNB in the AMF.

The AMF Service pods implement the logic that is necessary to provide Access and Mobility functions to the UE. This includes handling registration, handover and PDU session related procedures.

AMF Deployment

Table 1: Feature History

Feature Name	Release Information	Description
AMF Deployment on Four Servers	2024.03.0	AMF now supports deploying a single AMF instance across a four-server configuration using M5 servers. This setup includes three master servers and one worker server. This deployment provides an enhanced scalability and reliability with the AMF instance distributed across the available M5 servers.

The AMF deployment supports standalone mode. In this mode, each NF together with the required microservices is deployed in the same namespace in Kubernetes.

Supported Interfaces

This section lists the interfaces supported between the AMF and other network functions in the 5GC.

- N1 - Reference point between UE and AMF.
- N2 - Reference point between R(AN) and AMF.
- N8 - Reference point between AMF and UDM.
- N11 - Reference point between AMF and SMF.
- N12 - Reference point between AUSF and AMF.
- N14 - Reference point between AMF and AMF.
- N15 - Reference point between AMF and PCF.
- N17 - Reference point between AMF and EIR.
- N20 - Reference point between AMF and SMSF.
- N22 - Reference point between AMF and NSSF.
- N50 - Reference point between AMF and CBCF.
- NL1 - Reference point between AMF and LMF.
- NL2 - Reference point between AMF and GMLC.
- X1 - Reference point between AMF and ADMF.
- X2 - Reference point between AMF and MDF.
- Nnrf - Reference point between AMF and NRF.

Life Cycle of Control Plane Message

This call flow uses initial registration by a UE at the AMF using a GUTI assigned by an MME. All the steps in the call flow are not shown. The procedure level call flow has all the messages. The intent here is to show all the components, and the actions that are taken by each component.

Figure 4: End-to-End Registration by an UE Call Flow

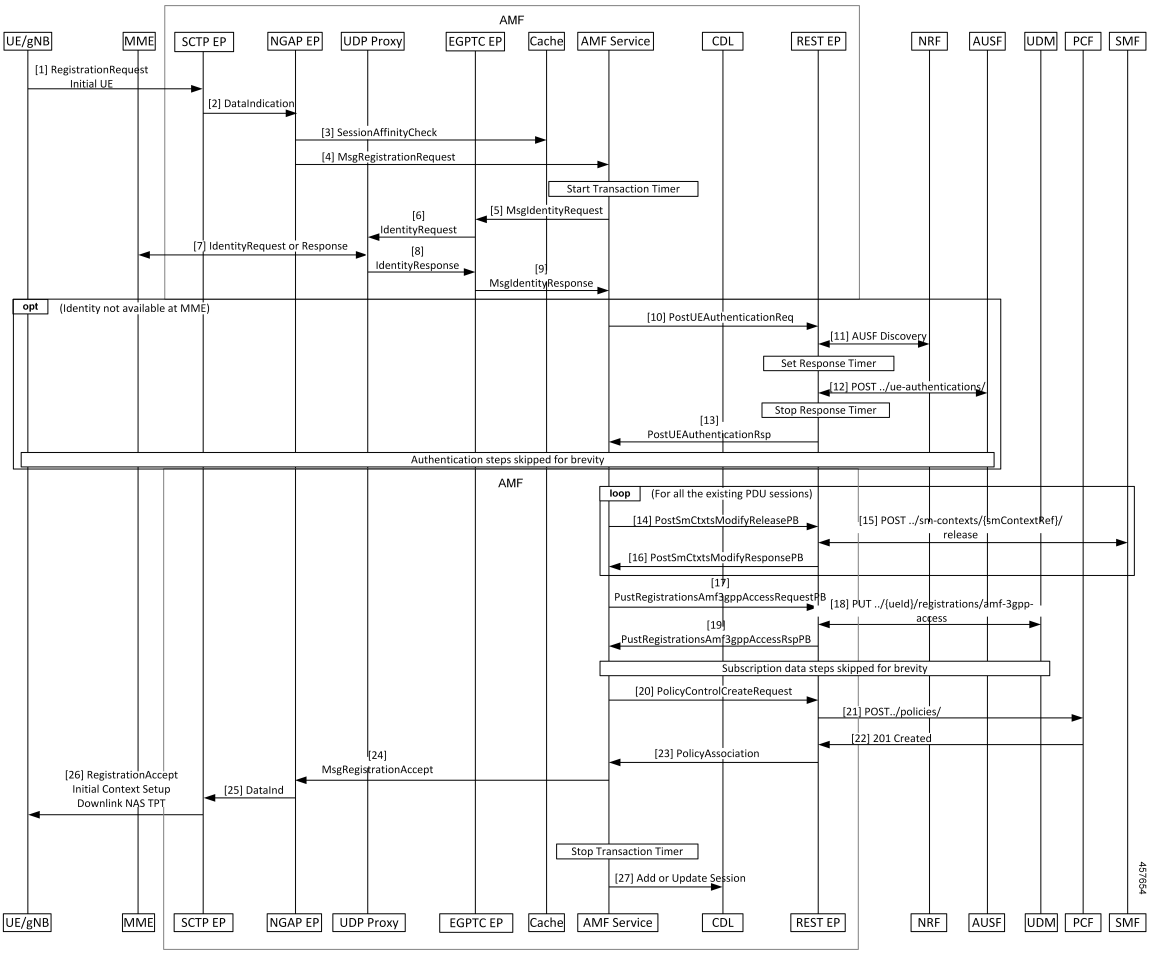


Table 2: End-to-End Registration by an UE Call Flow Description

Step	Description
1	The UE sends an Initial Registration Request to the gNB, which sends it to the AMF in an Initial UE message.
2	On the AMF, the message reaches the SCTP Endpoint (EP), which terminates the SCTP protocol and extracts the payload. It sends a DataInd GRPC message to the NGAP EP.

Step	Description
3	The NGAP EP parses the request. Both NGAP message parsing and NAS parsing are performed by the NGAP EP. It takes the ID that came in the initial message, and checks for any existing state in any AMF service by looking up the Session Affinity Cache.
4	To optimally serve the UE, the AMF maintains affinity of subscriber with service pod internally. If there's session affinity information for the UE, the NGAP EP forwards the message to that AMF service pod. Otherwise, it load balances the request to any available AMF service pod.
5	The AMF service finds the MME to check the identity of the UE. Currently, the MME information is locally configured. The AMF service sends this request to the EGTPC EP.
6	The EGTPC EP forwards the request to the UDP proxy after a transaction ID has been allocated.
7	The UDP proxy forwards this message to the MME and gets a response.
8	The response from the MME is forwarded to EGTPC EP. The EGTPC EP does the transaction matching for the request.
9	The identity response is sent to the AMF service.
10	If the security context is not present in the response from the MME, the AMF service decides to authenticate the UE. The authentication procedure is started by sending a AuthenticationRequest to the REST EP.
11	The REST EP handles all the client and server requests for the AMF, and all NRF interactions. REST EP makes a query to the NRF to find the AUSF to serve the UE. In further steps, the interaction with the NRF to resolve UDM and PCF are skipped.
12	The REST EP sends an Authentication Information Request to the AUSF and gets a response.
13	The response from the AUSF is forwarded to the AMF service. The authentication procedure between the AMF service and the UE is not explained here.
14	If there is any vestigial PDU state for the UE in the SMF, the AMF clears the state. The AMF service sends a message to REST EP for each SMF that needs to be cleared of state.
15	On the REST EP, there is no NRF interaction for this message, and the REST EP forwards this to the SMF identified in the request from the AMF service.
16	The response from the SMF is sent to the AMF service by REST EP.
17	The AMF service sends a UECM registration request to the REST EP.
18	The REST EP uses the NRF to resolve UDM selection for this request and sends a request to the UDM.
19	The response from the UDM is forwarded to the AMF Service. Retrieval of subscription data information and registering for notifications for change is not explained here.
20	The AMF service checks the configuration to see if an AM policy association needs to be done for this registration, and if it is, sends a request to the REST EP.
21	The REST EP does NRF discovery for PCF and sends a request to the PCF.

Step	Description
22	Response from the PCR is forwarded to the AMF service.
23	The AMF service sends a Registration Accept Message to NGAP.
24	The NGAP encodes both the NAS message and the NGAP message and sends a message to the SCTP EP.
25	The SCTP EP sends the message out to the gNB.
26	The rest of the message has been excluded.
27	The AMF sends an Add or Update Session message to the CDL.

License Information

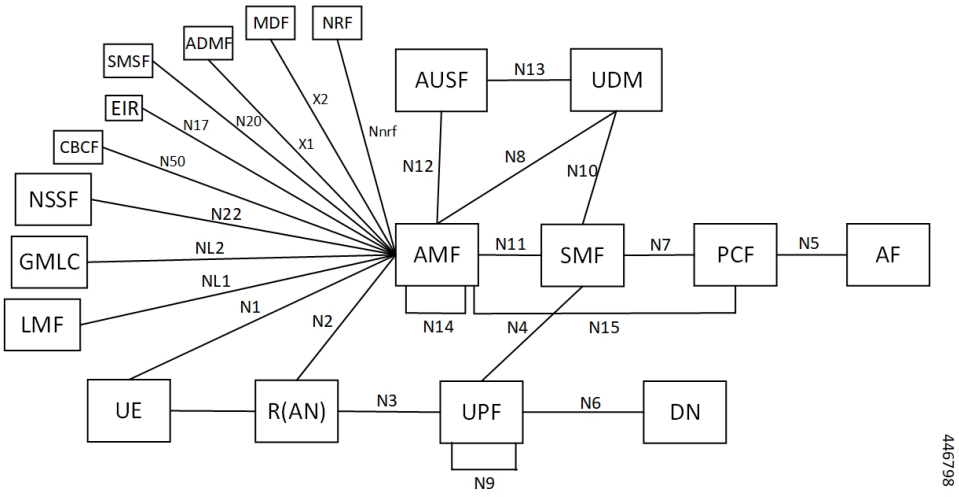
The AMF supports Cisco Smart Licensing. For more information, see the *Smart Licensing* chapter in this document.

Standards Compliance

Cisco AMF complies with the 3GPP standards.

The AMF is one of the control plane (CP) NFs of the 5G core network. The AMF uses different interfaces to communicate with the other NFs or nodes. For example, the N11 interface exists between the AMF and Session Management Function (SMF). Each of the AMF interfaces comply to a specific version of the 3GPP specification depending on the compliance version supported.

Figure 5: Interfaces



Use the following table to determine the compliance mapping for each AMF interface and the 3GPP Standards specification version revision 16.

Table 3: Compliance Mapping

Interface	Relationship	3GPP Specification	Version
N1	Between UE and AMF	24.501	Compliance Support: 16.6.0
N2	Between R(AN) and AMF	38.413	Compliance Support: 16.6.0
N8	Between AMF and UDM	29.503	Compliance Support: 16.6.0
N11	Between AMF and SMF	29.502	Compliance Support: 16.6.0
N12	Between AUSF and AMF	29.509	Compliance Support: 16.6.0
N14	Between AMF and AMF	29.518	Compliance Support: 16.6.0
N15	Between AMF and PCF	29.507	Compliance Support: 16.6.0
N17	Between AMF and EIR	29.511	Compliance Support: 16.4.0
N20	Between AMF and SMSF	29.540	Compliance Support: 16.6.0
N22	Between AMF and NSSF	29.531	Compliance Support: 16.3.0
NL1	Between AMF and LMF	29.572 23.273	Compliance Support: 16.4.0
NL2	Between AMF and GMLC	29.515	Compliance Support: 16.4.0
X1	Between AMF and ADMF	103.221-1	Compliance Support: 1.8.1
X2	Between AMF and MDF	103.221-2 33.128	Compliance Support: 1.4.1 16.7.0
Nnrf	Between AMF and NRF	29.510	Compliance Support: 16.9.0