GeniusCore

Private 5G-Core Solution Description

Document version 20230223 - SW Version 02.2023

Notices

This document serves for introducing readers to the concept and features of the GeniusCore 5G-core software.

CampusGenius reserves the right to, without notice, modify or revise all or part of this document and/or change product features or specifications and shall not be responsible for any loss, cost, or damage, including consequential damage, caused by reliance on these materials.

Content

Contents

Notices 2
Content 3
5G, private 5G, and 5GaaS 4
Introduction to 5G 4
Private 5G 5
5GaaS 7
GeniusCore 8
Introduction to GeniusCore 8
Architecture: Network Functions and Interfaces 8
Supported Network Functions 8

5G, private 5G, and 5GaaS

Introduction to 5G

5G follows 4G as the next generation of standardized mobile networking and is known for ultra-high speed data transport, high reliability, the option to connect a high number of end-devices, and for low latency communication. Most of these are the perfect fit for industrial machine communication. With 5G speed and the number of mobile subscribers will also be paired with new radio technologies, which may even be chosen depending on the requirements for such 5G network.

To address scalability and deployment flexibility, the 3GPP designed a 5G system architecture consisting of separated network functions in a service-based architecture, which is different from the (hardware) component-based setups in older 3GPP mobile network generations. The combination of this 5G Service Based Architecture (SBA), and additional components, such as a gNodeB (gNB) or radio equipment separates specialized functionalities and also allows to separate user plane and control plane data traffic. Due to this nature of the SBA, it is perfectly suited to be deployed and run in a distributed, cloud-native manner, which at the same time allows for being extended by new, additional network functions, for example to support location-based services.

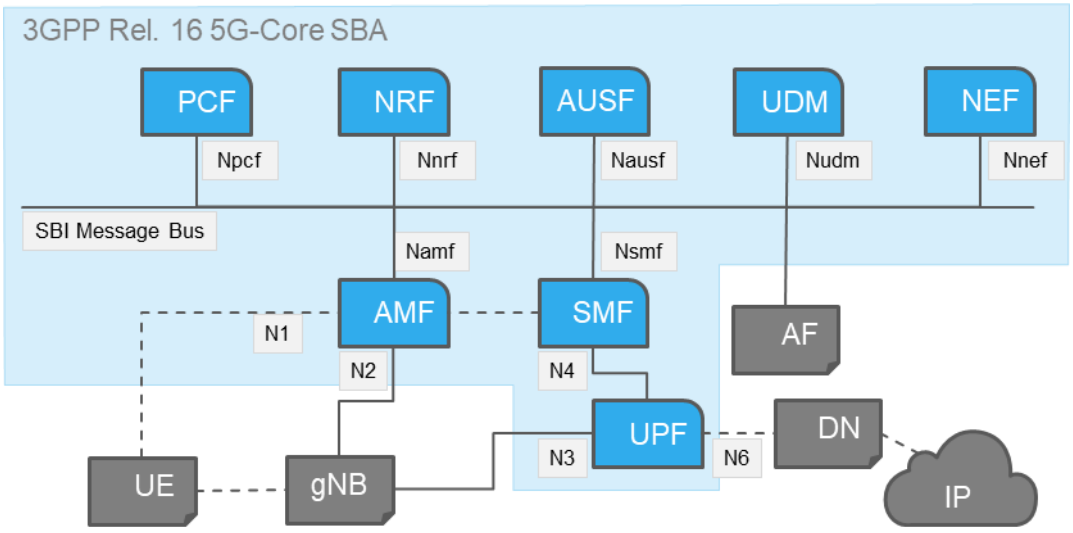

Figure 1: 3GPP 5G Service Based Architecture and Network Functions

The SBA describes of a set of Network Functions (NF) that compose various microservices to manage and control the 5G network and its subscribers. Figure 1 shows most essential network functions of a 5G core, which are marked in blue.

Table 1: 5G-Core Network Functions and Functionality

Network Function (NF)	Description
AMF (Access and Mobility Management Function)	The AMF basically connects the 5G core to the RAN. The communication between a UE/RAN and the core is based on mainly two protocols: NAS and NGAP. Thus, the AMF • is terminating NAS signaling from the RAN/gNB • handles the ciphering and integrity protection of NAS • is in charge of the mobility management • manages the UE connections • provides registration management towards UEs and RAN • does the authentication and authorization for UE access • is managing security contexts The AMF is mandatory for any 5G network core.
SMF (Session Management Function)	The main task of the SMF is to maintain the PDU sessions, and to provide rules for QoS and traffic handling to the UPF via PFCP over the N4 interface, and is in charge of IP address provisioning. It also provides support for data buffering; all session management NAS messages are terminated in the SMF.
NRF (Network Repository Function)	The NRF holds information about available functions and services in the 5G core, and provides this information to NFs upon request and service discovery.
UPF (User Plane Function)	The UPF is in charge of receiving and forwarding the network packets transporting user data. Based on rules, the UPF takes care of correct routing, the forwarding, and setting QoS parameters for data packet flows; for this to work, it inspects the packet header data and applies these rules. The UPF is basically the gateway between an attached data network (or LAN) and one or multiple RANs in a 5G network.
PCF (Policy Control Function)	With the PCF the 5G core has a central function for handling user traffic policy, the rules for the control plane functions of the core, and for providing the required information about subscribers of a 5G network.
UDM (Unified Data Management)	Access authorization and subscriber management is supported by the UDM, e.g. for the AUSF. This includes AKA authentication, authorization for network access, and the management of subscribers and user identification.
UDR (Unified Data Repository)	Note: The UDR is not shown in the diagrams, as it serves closely with the UDM, and serves as converged data store for subscriber information.
AUSF (Authentication Server Function)	The AUSF serves as authentication server for subscribers in a 5G network. UEs trying to access the network, will be handled by the AUSF upon AMF request as part of the registration procedures.
NEF (Network Exposure Function)	The NEF provides multiple exposure services to Application Functions (AF), which allows to access information of various 5G core network functions by external applications in a well-defined manner.

Private 5G

Private 5G allows enterprises to deploy and operate their own, dedicated and secure 5G network to implement their own applications, services, or innovative use cases. With the help of non-public 5G

networks (5G campus networks), the enterprise is able to protect their critical infrastructure, develop and maintain their own processes, and ensure data privacy, because the data transported over private 5G networks never has to leave the private infrastructure.

Multiple choices exist to deploy private 5G networks. Locally deployed 5G networks are operated from local on-premise standalone servers or private cloud systems, including also local container environments. Such basic on-premise setup is shown in Figure 2.

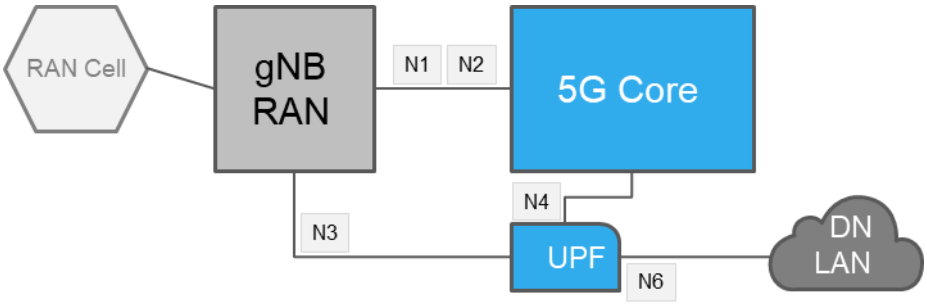

Figure 2: Basic private 5G on-premise campus network

A hybrid setup on the other hand allows for operating the Radio Access Network (RAN) and a decoupled UPF locally, as depicted in Figure 3. The hybrid deployment ensures that user data never leaves the enterprises network, and at the same time is using a 5G-core that is deployed on a remote cloud service or data center. The core is connected to UPF and RAN, respectively the gNB using encrypted and secure VPN tunnels.

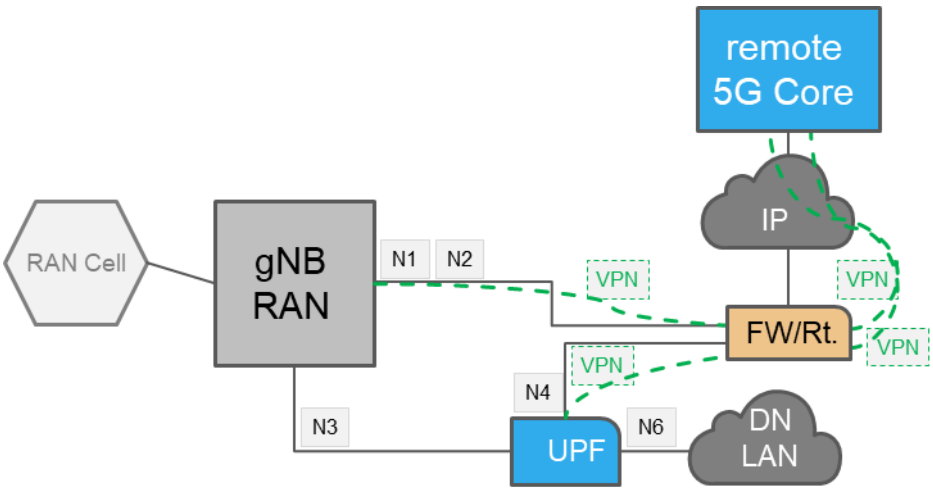

Figure 3: Hybrid 5G network: local gNB and UPF connected to remote 5G core (CUPS secenario)

The hybrid deployment of a private 5G network is potentially the easiest approach; user-traffic is private and secure, the 5G core runs cloud-based 5G, and get the a basic deployment just requires a local small-cell gNB and a UPF; this is the Control and User Plane Separation (CUPS) scenario along with a remotely hosted 5G core.

5GaaS

Provided the deployment possibilities and the modular software architecture of the 5G-Core, a general fast and easy deployment option for a 5G-Core as a Service arises. This 5GaaS aims to provide all necessary software components in a cloud environment, that can be utilized fast and easy from anywhere in the world with a plug-&-play like integration. However, 5G RAN (hardware) is still required for such a setup. The 5GaaS is a 5G-Core running as a cloud service with all necessary functionalities, connecting to the gNB via the Internet over a pre-defined and securely encrypted IP connection and establishes a N2 authentication with the gNB and then realizing connectivity featuring the N1, N3, N4 and N6 Interfaces. In order to improve latency, Control and User Plane Separation (CUPS) allows the user plane function to be separated from the cloud deployment, thus enabling the UPF to be run on a dedicated server at the customer side.

In the hosted cloud, the 5G-Core is deployed using Kubernetes containers for easy scalability and shall support multi-tenancy. However, this solution can also run on-premise either deployed on bare metal, within virtual machines, or a self-hosted container environment.

With the 5GaaS service running in the cloud a license for a 5G-Core can be easily obtained, and connection establishment is immediately possible by defining protected IP endpoints (VPN) for the UPF and gNB interfaces.

GeniusCore

Introduction to GeniusCore

The GeniusCore is a 5G-SA core software solution that provides a cloud native implementation of the 3GPP standards-defined 5G Core (5G NGC or 5GC) for 5G-SA (Stand-Alone) 5G private networking. It comprises of a defined set of network functions and interfaces for using the GeniusCore for the deployment of private 5G networks, so called campus networks.

Due to its nature, the GeniusCore can be used for private 5G-SA networks only; any legacy or 4G support is not provided, and interworking with other or older generations of 3GPP networks is not in the scope of the GeniusCore solution.

For detailed insights and KPI analysis GeniusCore will provide proactive, real-time analysis of all message traffic including NGAP/NAS and also PFCP messages and HTTP requests and responses through APIs (Application Programming Interface), respectively in graphical dashboards for the user.

For that, GeniusCore is also integrated with cloud native monitoring tools, such as OpenTelemetry, Prometheus and Grafana, allowing for real time analysis and visualization of the 5G network, alerting, and investigation for troubleshooting.

Architecture: Network Functions and Interfaces

The 5G Service Based Architecture (SBA) is connecting a set of Network Functions (NFs) with each other over the Service Based Interface (SBI) the using HTTP/2 over TCP as defined by 3GPP.

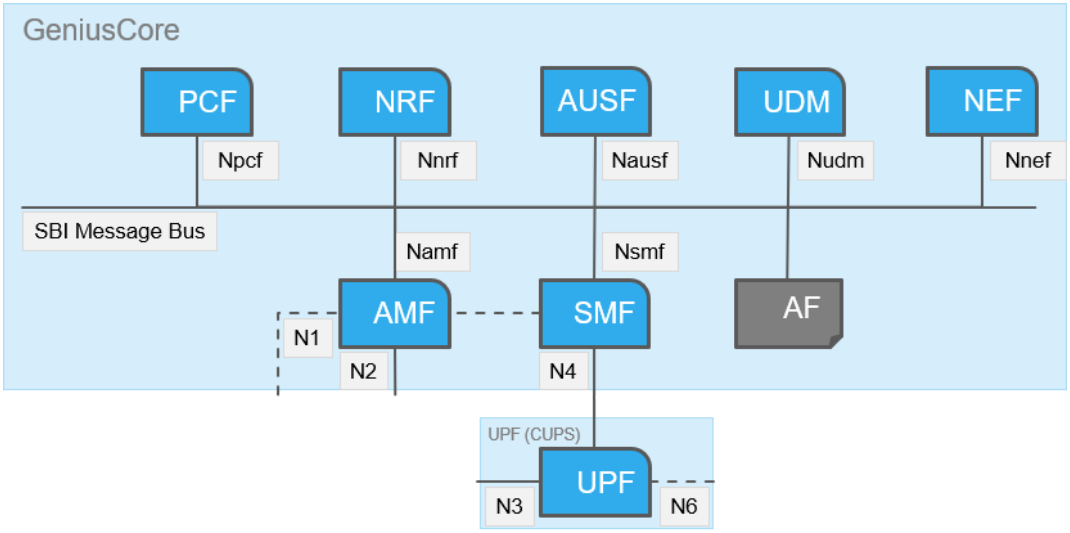

Figure 4: 5G Service Based Architecture and Network Functions

Supported Network Functions

The GeniusCore 5G-Core implements the NFs listed in the Table 2; the detailed description with NF functionality is given in Table 1 on page 5 above.

Table 2: GeniusCore Network Functions

NF	Name	Status	Annotation
AMF	Access and Mobility Management Function	implemented	no roaming support
SMF	Session Management Function	implemented	Single SMF
UPF	User Plane Function	implemented	support for CUPS
PCF	Policy Control Function	implemented	
NRF	Network Repository Function	implemented	
AUSF	Authentication Server Function	implemented	5G-AKA authentication
UDM	Unified Data Management	implemented	
UDR	Unified Data Repository	implemented	dedicated dockerized database
NEF	Network Exposure Function	implemented	NEF exposure service for SMF
AF	Application Function	in devel.	will allow NEF access by AF