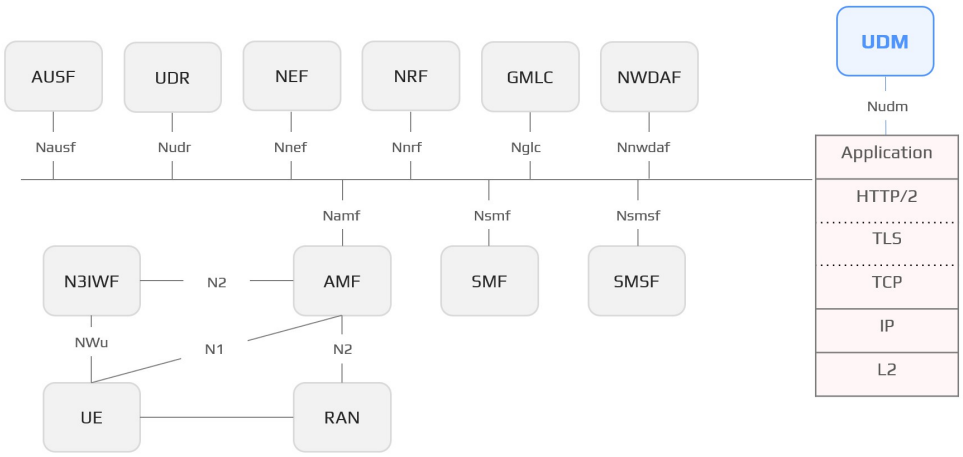
TELCOWARE

5G/LTE Core

UDM

1. Description

UDM(Unified Data Management) is a 5G core solution that offers functions for UE authentication, registration/mobility management, subscription management, and SMS management.



2. Key Features

● Provide Nudm service-based interface to NF Consumers(e.g. AMF, SMF, SMSF, etc.)

· Support Nudm_SubscriberDataManagement service

· Support Nudm_UEContextManagement service

· Support Nudm_UEAuthentication service

· Support Nudm_EventExposure service

● SIDF(Subscriber Identity De-concealing Function)

· Manage Home Network Public Identifier(s) for private/public key pairs

· Support Null-Scheme, Profile A, Profile B

● ARPF(Authentication Credential Repository and Processing Function)

· Support MILENAGE/TUAK algorithm

· Store Long-term key K, home network private key(for SIDF)

· Support 5G-AKA

· Support EAP-AKA' (planned feature: ~24.2Q)

- Support SMS over NAS
- UDM discovery and selection
  - Home Network Identifier of SUCI/SUPI
  - SUCI/GPSI
  - UDM Group ID of the UE's SUPI

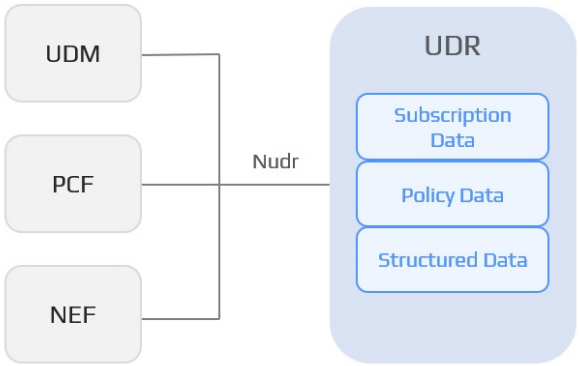
3. Benefits

- Available as Legacy HLR/LTE-HSS integrated system
- Provide Multi-Vendor Interoperability through compliance with 3GPP standards
- Offer customer-specific feature, along with 3GPP standard feature

UDR

1. Description

UDR(Unified Data Repository) enables 5G NF(Network Function) to store and retrieve data, including subscriber data, policy data, structured data, application data.



[Fig. 1] UDR Network Architecture

2. Key Features

● Data management

· Creation/Retrieval/Update/Deletion of resource URI and the related JSON format

· Creation, retrieval, update, and deletion of resource URIs and their related JSON format

● Nudr interface

· HTTP/2 protocol processing

· JSON encoding/decoding

· 3GPP SBI compliant

· Data creation, retrieval, update, and deletion based on NF request

· Subscription/Notification functionality

● Verify authentication and authorization

· NF authentication

· Resource access control for each NF

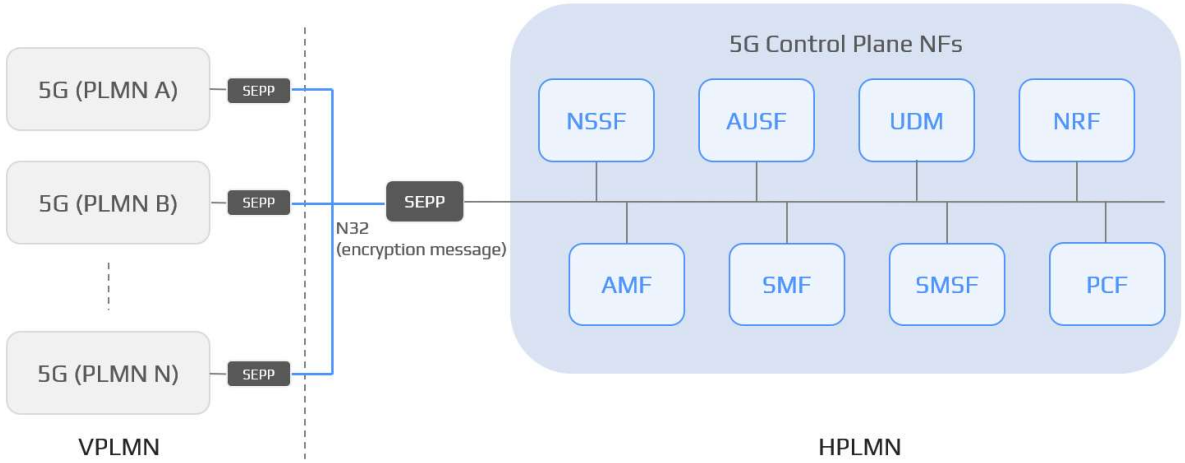
3. Benefits

- Prevent data inconsistency caused by redundant data integration, and reduce overall data size
- Enable to store and retrieve customer-specific data, along with 3GPP standardized data

SEPP

1. Description

SEPP(Security Edge Protection Proxy) serves as a proxy for message filtering, policy, and topology hiding on the Inter-PLMN(Public Land Mobile Network) Control Plan Interface among 5G Core network functions.



[Fig. 1] SEPP Network Architecture

2. Key Features

● N32c Interface (N32 Handshake Procedure)

· Security Capability Negotiation Procedure

· Parameter Exchange Procedure

- Parameter Exchange Procedure for Cipher Suite Negotiation

- Parameter Exchange Procedure for Protection Policy Exchange

· N32-f Context Termination Procedure

· N32-f Error Reporting Procedure

● N32f Interface (Protected Message Forwarding Procedure)

· Support Security Policy TLS

- Forwarding to Peer SEPP

· Support Security Policy PRINS(Protocol for N32 Interconnect Security)

- Identification Protection Policy
- Message Reformatting
- Forwarding to Peer SEPP

· JOSE(JSON Object Signing and Encryption)

- JWE(JSON Web Encryption)
- JWS(JSON Web Signature)

· Topology Hiding

- Create or manage Telescopic FQDN

● TLS Connection Management

· CA (Certification Authority)

- CA Reset and Root CA
- Manage Cross Certificate
- Management of TLS Server and Client Certificates
- Manage TLS Server, Client Certificate
- Manage Certificate and CRL periodically
- LDAP Publish Management

· TLS Wildcard Certificate Processing

● SBI (Service-based Interface)

· Nudm SBI / Nausf SBI / Npcf SBI / Nsmf SBI / Nnrf SBI / Nnssf SBI

3. Benefits

● SEPP, as an important network function within 5G Core, provides security and proxy functions for processing roaming message between Inter-PLMNs.

● Offer customer-specific feature, along with 3GPP standard feature

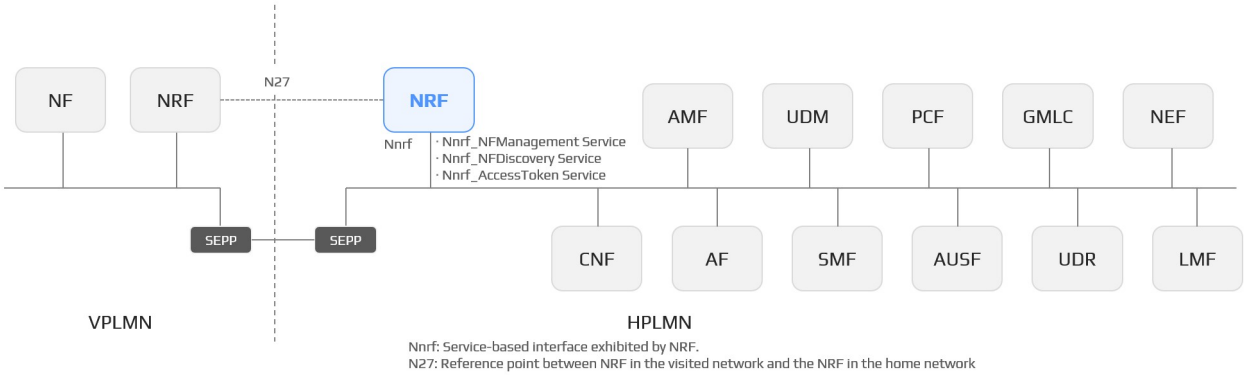
NRF

1. Description

NRF (Network Repository Function) is a component system within the NF (Network Function) Service Framework, defined by 3GPP 5G standards. This infrastructure system supports interconnection between 5G Core NFs by dynamically monitoring the service status and managing interworking information, such as IP addresses and FQDNs.

NRF system, within 3GPP 5G System Architecture, offers the following service functions for NF management via HTTP2-based Nnrf SBI(Service-Based Interface provided by NRF):

- NF Service Registration: Manage 5G Core service information from NF instance
- NF Service Discovery: Provide information about NF instance supporting 5G Core SBI
- Access Token: Offer authentication and authorization tokens for accessing 5G Core service



[Fig. 1] 3GPP 5G System Architecture-based NRF Interconnection Interface

2. Key Features

- NF management service
  - · Manage NF instance information
  - · Process subscription and notification for NF instance information
  - · Provide information for NF instance management
- NF discovery service
  - · Provide NF instance information supporting requested service
- OAuth2 authorization service
  - · Provide access token with valid authentication and authorization for requested service

- Manage NF profile
  - Manage profile information for each NF instance
  - Manage service information for each NF instance
- NF status management
  - Manage NF status based on received HeartBeat message
- Access token management
  - Manage access token issuance information
  - Provide HTTPS-based JWK
- Hierarchical NRF configuration
  - Provide intermediate redirection and forwarding
- HTTP2 interworking
  - Manage IP white list registration
  - Manage FQDN registration for NF using multiple IPs
  - NF interworking TLS setting
  - Control overload
- Roaming
  - Manage multiple HPLMN information
  - Connect roaming NRF through SEPP connection

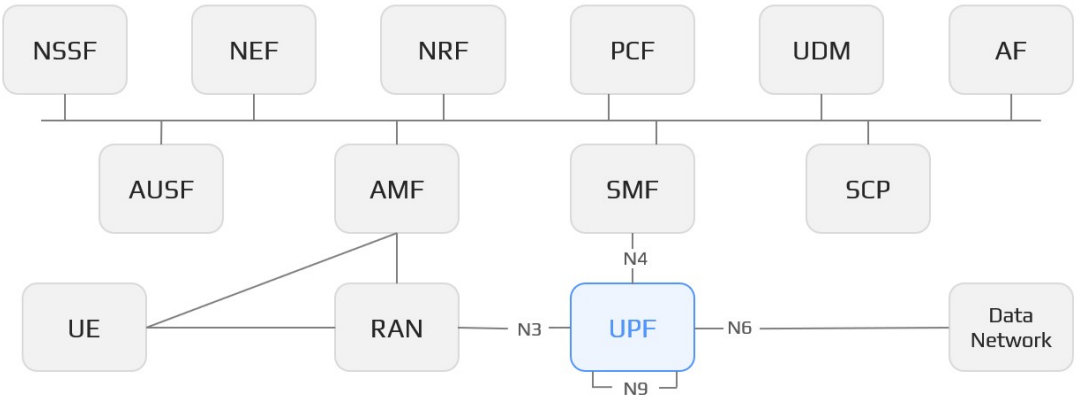
3. Benefits

- Provide optimal interworking NF information through NF RTT monitoring
- Ensure NF instance information integrity through MANO interworking
- Offer DNS-based NF instance interworking information for SBI-unsupported equipment
- Enable NF load balancing selection when providing NF discovery service

UPF

1. Description

UPF(User Plane Function) connects UE and external data network within 5G core network. It interworks with SMF(Session Management Function) to manage PDU(Packet Data Unit) session and facilitate routing and transmission of packet between UE and external data network.



N3 : Reference point between the (R)AN and the UPF
N4 : Reference point between the SMF and the UPF
N6 : Reference point between the UPF and Data Network
N9 : Reference point between two UPFs

2. Key Features

● SMF Interworking

· PFCP (Packet Forwarding Control Protocol) processing

· PFCP Session Management

· PFCP Session Report

● Mobility Anchor Point

· Intra-RAT Handover

· Inter-RAT Handover

· N3 End marker

- Packet Processing
  - GTP En/De-Capsulation
  - GTP Packet Forwarding
  - IP Packet Forwarding

3. Benefits

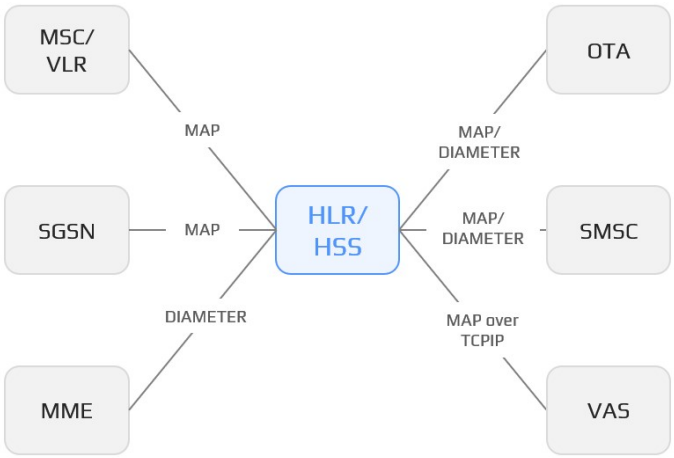
- Support private 5G specialized system Core Node integrated/separated architecture
- Enable high-speed packet processing using DPDK(Data Plane Development Kit)
- Ensure compatibility with 3GPP Release 16-based standards
- Compatible with various virtualized environment(KVM, Bare-Metal, Openstack)

HLR/LTE-HSS

1. Description

HLR(Home Location Register)/HSS(Home Subscriber Server) is a fundamental system in 3G and 4G networks that manages real-time mobile subscriber information, including location, authentication, services, permissions, and additional data. It interworks with MSC/VLR, SGSN, MME, SMSC, OTA, Service Node to provide outgoing/incoming calls, authentication, short messaging, packet transmission, location information, and intelligent network services.

HLR/HSS system includes the AUC function for authenticating 3G/4G subscribers. However, AUC function can also be provided as a standalone system.



2. Key Features

● Can apply software in COTS Hardware and various OS environment

● Link with MAP over SIGTRAN for 3G networks and Diameter for 4G networks

· Can select interface, when interworking with server that supports both MAP and Diameter interface such as OTA and SMSC

● Provide all services and features presented in 3GPP standards

· Manage 3G/4G subscriber's location information

· Manage subscriber's UE power status

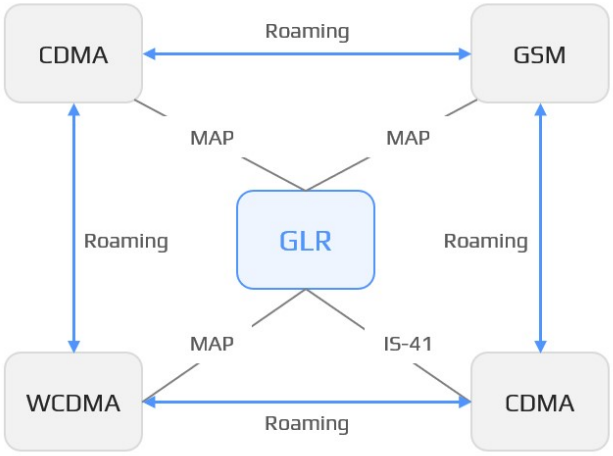
· Manage authority information and additional service settings (including CAMEL profiles)

- Can integrate/separate subscriber's authentication functions
  - MILENAGE algorithm
  - TUAK algorithm
- Compliance with GSM/WCDMA/LTE standard specifications
- Multi-vendor interoperability
- Complete high-availability and geo-redundancy

GLR

1. Description

Telcoware GLR(Gateway Location Register) combines functionalities of HLR and VLR, essential elements in mobile communication network, and includes protocol conversion. GLR serves as a gateway, enabling service between mobile communication operators using different MAP(Mobile Application Part) protocol, such as GSM, ANSI-41, and PDC.



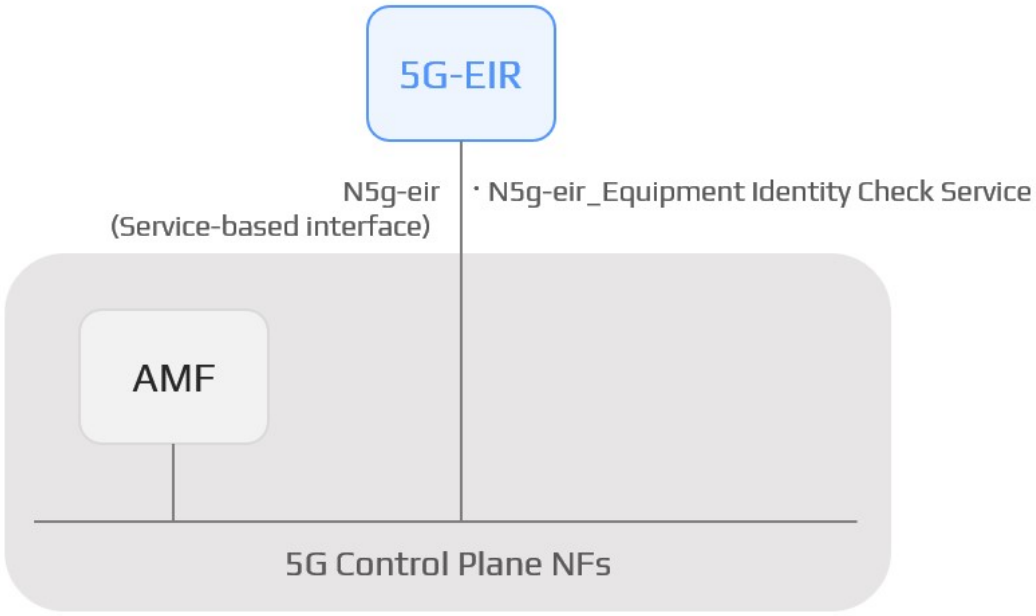
2. Key Features

- MAP protocol conversion (ANSI-41, GSM, PDC, WCDMA)
- Flexible network configuration for CDMA <-> CDMA, CDMA <-> GSM, CDMA <-> WCDMA
- Mobile subscriber number conversion (MIN, IMSI, MSN)
- Seamless automatic roaming services without network changes
- Virtual Home Location Register(HLR) for roaming networks
- Virtual Visitor Location Register(VLR) for home networks
- Unique commercial product in Korea
- Automatic location registration for seamless interworking with multiple networks

5G-EIR

1. Description

5G-EIR(Equipment Identity Register) is a network function that checks PEI(Permanent Equipment Identifier) status, including backlist status.



[Fig. 1] 5G-EIR Network Architecture

2. Key Features

● Device authentication

· Process PEI check requests from AMF(Access and Mobility Management Function)

· Send device status to AMF

● Device capacity notification

· Notify UDM(Unified Data Management) about 5G PEI device capacity

● Arbitrary device change processing

· Handle request for arbitrary device change

● SBI (Service-based Interface) processing

· Manage N5g-eir SBI

● Verify authentication and authorization

· Authenticate NF

· Manage access to NF-specific resource

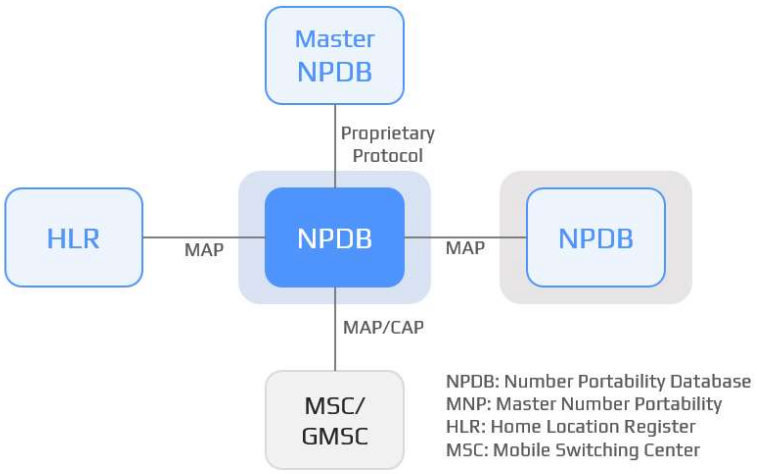
3. Benefits

● Offer service for authentication and handling arbitrary device changes in 5G Core to prevent unauthorized device use based on PEI status

NPDB

1. Description

NPDB(Number Portability Database) is a database system that contains information required to enable number portability in mobile network. (Number portability allows mobile subscribers to change their service provider while keeping the same phone number.)



2. Key Features

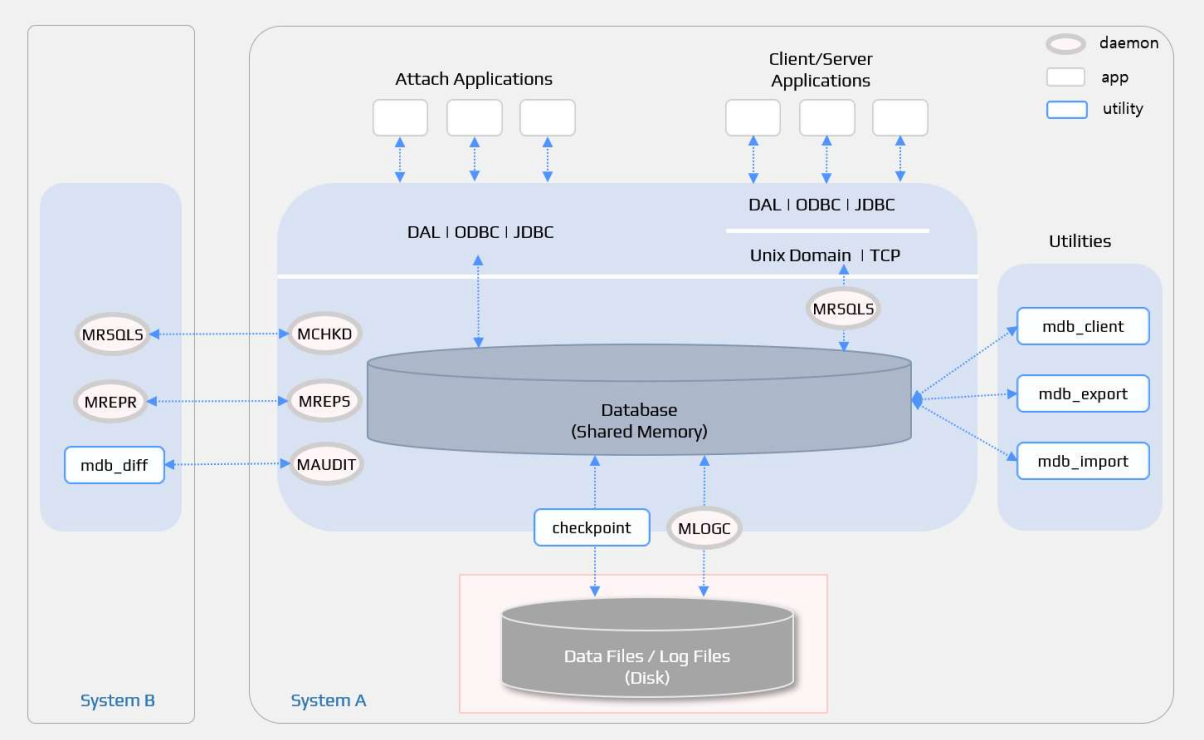
- Manage NPDB subscriber data(subscriber number, routing number, NPDB status, etc.)
- Download, upload, audit, and real-time search for port-in number data
- Process port-in number No.7 call
- Process port-in number TCP/IP call
- Interworking with the NPMF (local-SMS.)

TELCOBASE™

1. Description

Telcobase™ is Main Memory Database Management System (MMDBMS) software that uses memory as the primary data storage and memory management solution. Unlike existing DBMS, where data is stored on disk with memory playing a secondary role, MMDBMS keeps the database in main memory, utilizing the disk for backup purposes.

Telcobase™, functioning as MMDBMS, ensures fast transaction process and minimal resource consumption by directly accessing data residing in memory. Moreover, it offers online backup and real-time replication solutions, making it ideal for high-performance, high-availability system.



2. Key Features

- Basic RDBMS functionality
- Include SQL library
- Support Data backup
- Provide interface for service application development
- High performance and stability

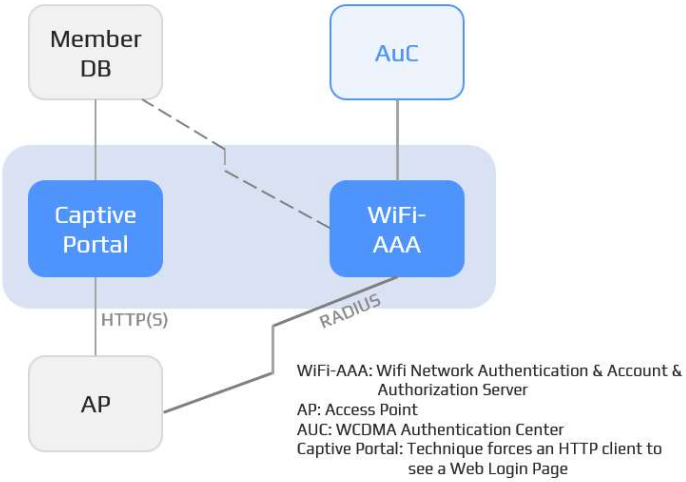
- Various real-time algorithms optimized for the memory space
- Provide a range of real-time algorithm optimized for memory efficiency
- User-friendly interface
- Zero-Downtime services through redundancy
- Network isolation for security with white list access
- redundancy function between heterogeneous OS types
- Cross-platform redundancy
- Support various OS: POSIX Unix, Linux, BSD, etc.

WIFI-AAA

1. Description

WiFi-AAA(WiFi Network Authentication, Authorization, and Accounting Server) authorizes subscriber permission through AP access authentication within WiFi network. The server also handles usage accounting by receiving data(UDR) from AP.

WiFi-AAA is built on RFC 2865 RADIUS and RFC 3748 EAP Base Protocol functionalities. It supports a variey of RADIUS & EAP extensions(RADIUS & EAP Application) and provides a user-friendly web-based interface.



2. Key Features

● Support RADIUS-based EAP Application

· (None-EAP) Automatic MAC-based authentication

· EAP-based security authentication

· USIM-based EAP-AKA authentication

· ID/Password and Certificate-based EAP-PEAP/TTLS authentication

· Billing data processing

● WEB-based Captive Portal authentication

· T world ID/Password authentication

· Resident Registration Number authentication

● Compliance with international standards

· RFC 2716, 2865, 2866, 2868, 3539, 3748, 4187, etc.

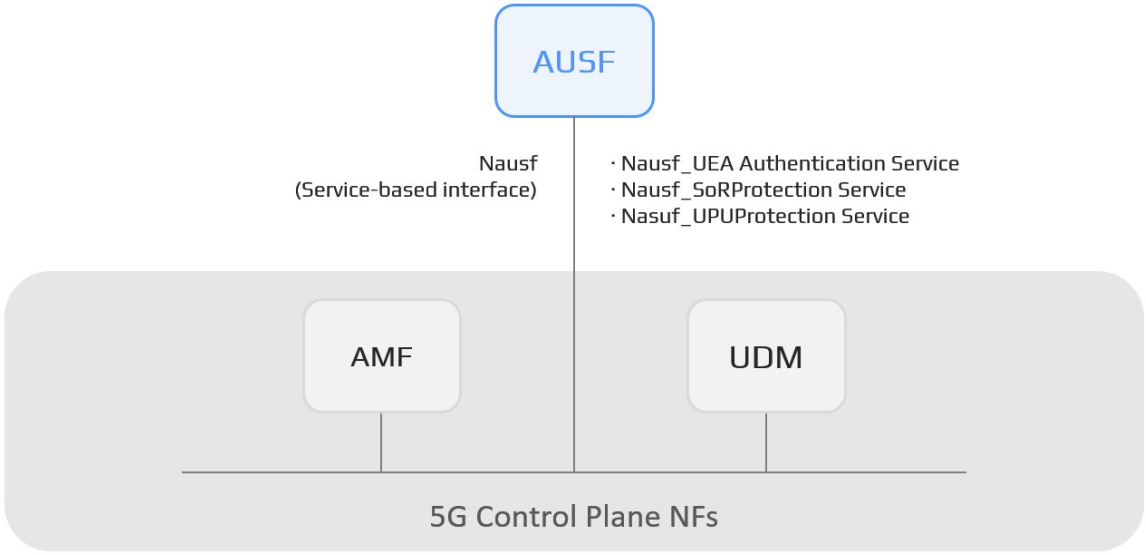
· 3GPP 33.102

AUSF

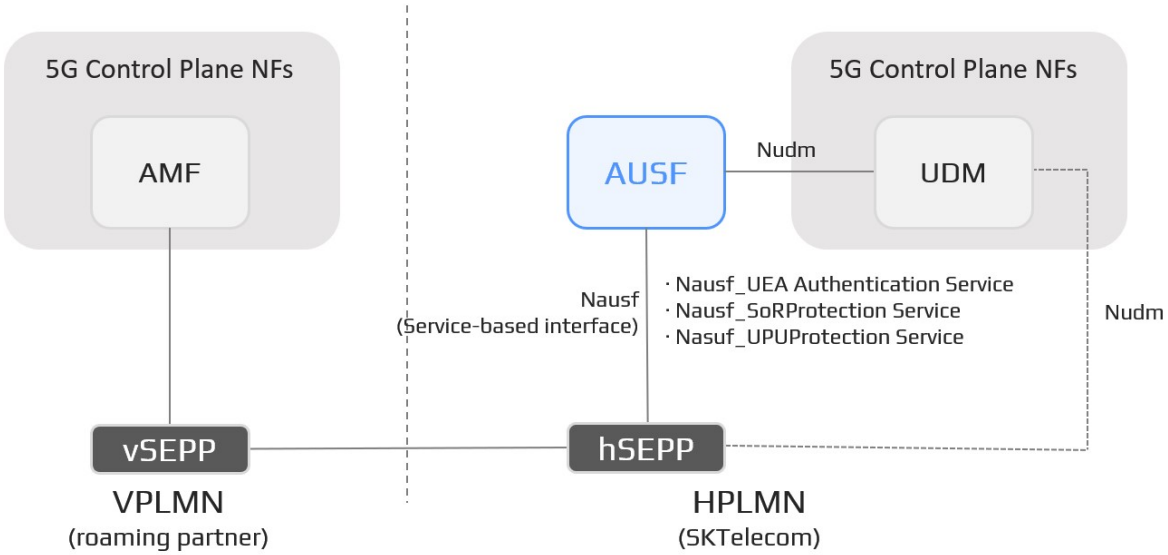
1. Description

AUSF(Authentication Server Function) supports authentication for both 3GPP and non-3GPP access.

AUSF interworks with UDM(Unified Data Management) and AMF(Access and Mobility Management Function) through SBI(Service-based Interface) and offers its service to UDM/AMF.



[Fig. 1] AUSF Non-Roaming Architecture



[Fig. 2] AUSF Roaming Architecture

2. Key Features

● Verify authentication and authorization

· Generate 5G authentication vector

- Convert 5G HEAV(Home Environment Authentication Vector) received from UDM into 5G SEAV(Serving Environment Authentication Vector) and Kseaf, then send them to SEAF

- Store XRES* for authentication confirmation

· Authentication Verification

- Verify AV upon receiving authentication confirmation message

- Compare and verify UE's RES* with stored XRES*

- Send authentication result to UDM

● EAP server function

· Functions as EAP server for non-3GPP access authentication

● SBI(Service-based Interface) processing

· Provide Nausf SBI

· Process Nudm SBI

3. Benefits

● AUSF, as an essential NF(Network Function) in 5G Core, provides fundamental authentication function for both 3GPP and non-3GPP access.

● Offer customer-specific feature, along with 3GPP standard feature (e.g. various AUSF deployment based on client network configuration, etc.)

NSSF

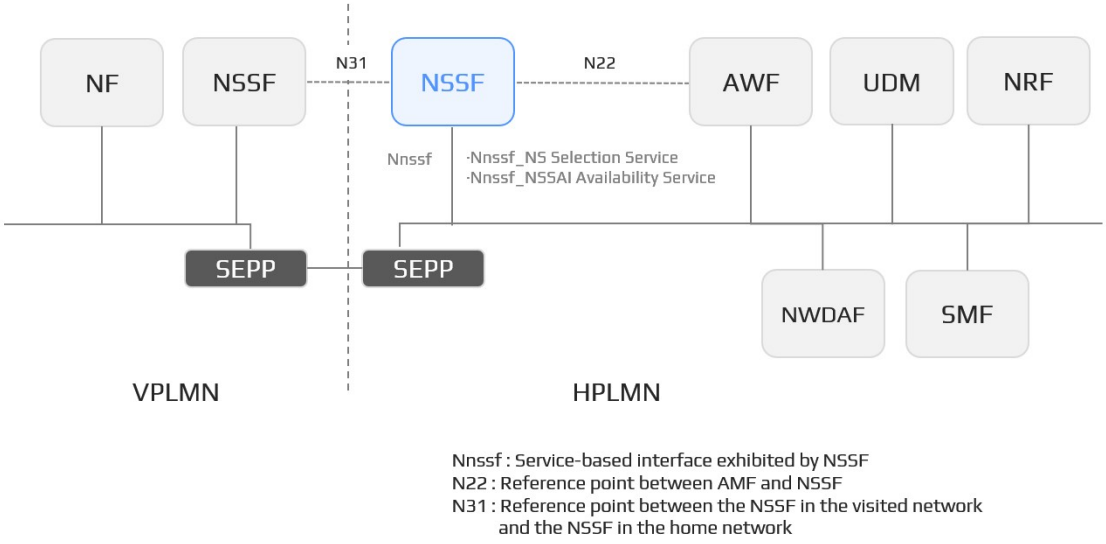
1. Description

NSSF(Network Slicing Selection Function) system selects the best network slice available for user's requested service in diverse 5G environment, and it provides optimal AMF(Access Management Function) or AMF Set information to support authorized service.

To provide slice selection, NFSSF system utilizes HTTP-2 based Nnssf SBI(Service-based interface exhibited by NSSF) within 3GPP 5G System Architecture to process the following service:

● NS(Network Slice) Selection: Provide user the right Network Slice information

● NSSAI(Network Slice Selection Assistance Information) Availability: Manage serviceable S-NSSAI information in access network



[Fig. 1] 3GFF 5G System Architecture-based NSSF Interconnection Interface

2. Key Features

● NS selection service

· Decide allowed NSSAI

· Decide AMF set or candidate AMF list

· Decide network slice instance

· Process configured NSSAI mapping

- NSSAI Availability Service
  - Manage S-NSSAI support information for each TAI
  - Process subscription to and notification of S-NSSAI support information for each TAI
- NS data management
  - Manage network slice(S-NSSAI) information
  - Manage network slice instance information
  - Manage NF(AMF, NRF) information including network slice instance
  - Manage AMF NSSAI availability information
- NS selection standard management
  - Manage network selection information for each tracking area
  - Manage HPLMN NSSAI mapping information for each PLMN
  - Manage rejected NSSAI information for each PLMN
  - Manage rejected NSSAI information for each tracking area
- NS status management
  - Acquire “load level” information of “network slice instance” through interworking with NWDAF
- NRF interworking
  - Register NSSF Profile data
  - Update NSSF status periodically
- Authentication and authorization monitoring
  - Request NRF interworking access token issuance
  - Validate NSSF service request access token
  - Validate access token
- Hierarchical NSSF configuration
  - Provide intermediate redirection and forwarding
- HTTP2 interworking
  - Register and manage IP in white-list

- Manage FQDN registration of NF that uses multiple IPs
- Configure TLS interworking for each NF
- Overload control

● Roaming

- Manage multiple HPLMN information
- Interwork with roaming NSSF through SEPP interconnection

3. Benefits

● Provide optimal AMF information for network slice

● Enable network slice selection for roaming network

● Support 5G NF RTT monitoring

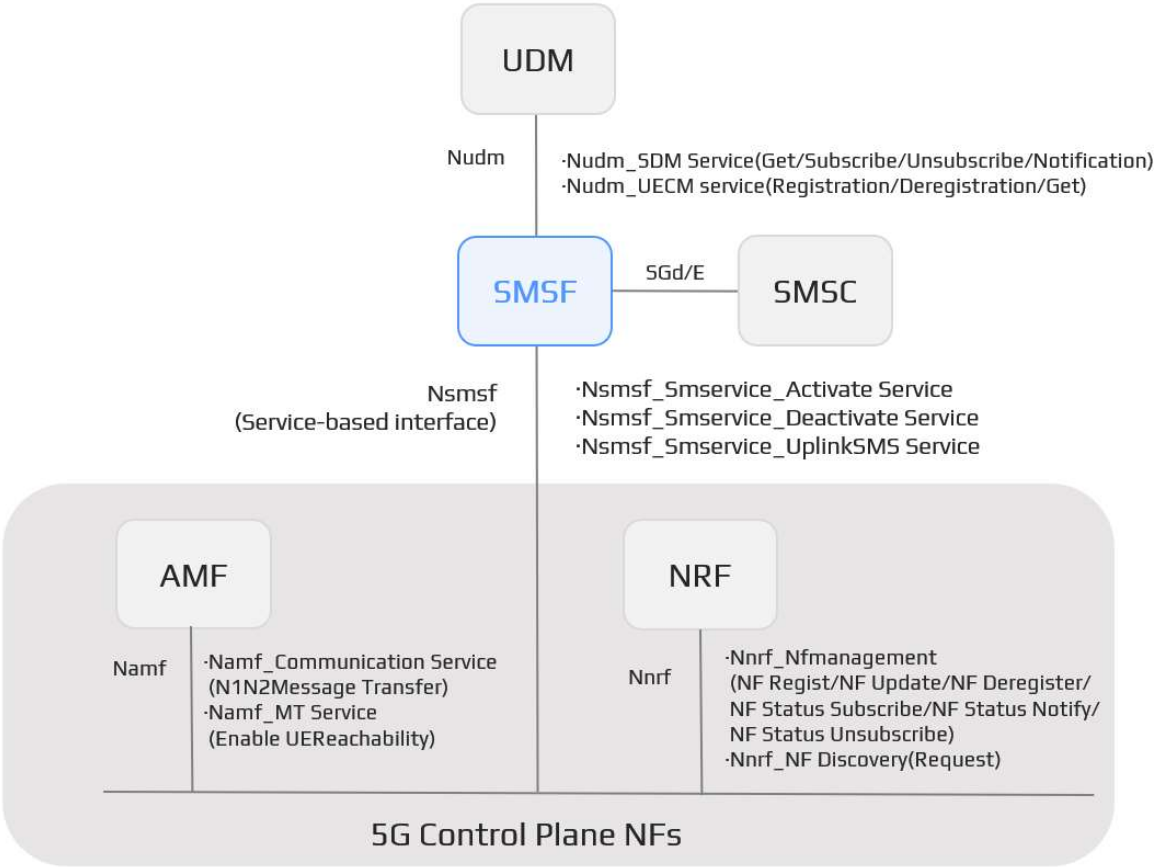
● Support NSI load balancing during NS selection service provision

SMSF

1. Description

SMSF is a system essential for offering SMS over NAS via AMF. SMSF connects with existing legacy network's SMCS for storing and forwarding SMS using SGd interface. It also interfaces with AMF and UDM, both part of 5G control plane network function, through service-based interface to provide SMS MO/MT service using SMS over NAS method.

- SMSF(Short Message Service Function)
- AMF(Access and Mobility Management Function)
- UDM(Unified Data Management)
- MO(Mobile Originating)/MT(Mobile Terminating)



[Fig. 1] SMSF Network Architecture

2. Key Features

● Subscription Information Management

· Generate/Delete subscriber context via Nsmsf_SMService_Active/Deactivate

· Manage SMS Management Subscription data via Nudm_SDM_Get

● SBI (Service-based Interface) processing

· Process Namf SBI / Nudm SBI / Nnrf SBI / Nsmsf SBI

● SGd Interface (DIAMETER) processing

· Process OFR/A(MO-Forward-Short-Message-Request/Answer)

· Process TFR/A(MT-Forward-Short-Message-Request/Answer)

● Roaming processing

· Manage SEPP interworking

· Manage PLMN information

● Database function

· DB backup and recovery

· Monitor DBMS(Telcobase)

● Support virtualization

· MANO interworking-based automation(Scaling, migration, reboot, rebuild, evacuation, etc.)

· Alarm/fault/performance information interworking

● OAM

· Manage virtual H/W and S/W status, Process alarm

· Manage and monitor connection node and resource status

· Logging

· Statistics

· MMC via CLI command or GUI

· Trace

· NMS interworking

3. Benefits

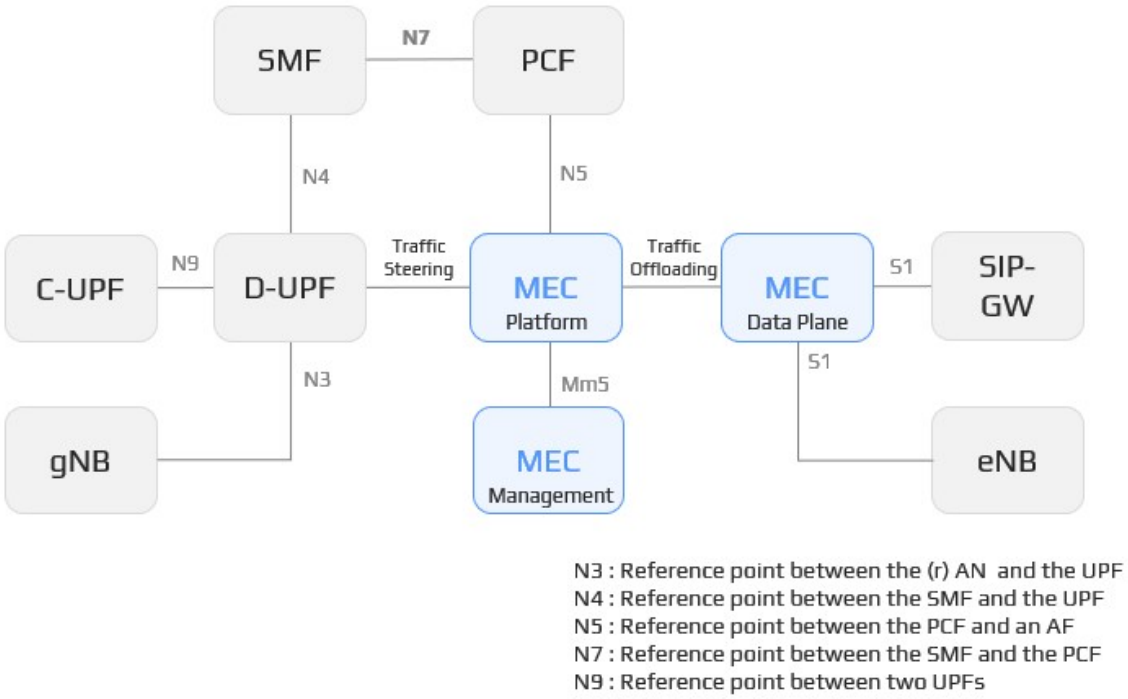
- Interwork with legacy SMS feature to offer SMS service upon 5G Core adoption
- Offer customer-specific feature, along with 3GPP standard feature

MEC

1. Description

MEC(Multi-Access Edge Computing) is a solution that optimizes processing of services with ultra-low latency and high bandwidth characteristics by distributing Core function from centralized 4G/5G network to the edge.

- MEC Platform: Execute ME app and API GW function to support MEC service
- MEC Management: Manage MEC configuration and operation via MEC Portal
- MEC Data Plane: Handle traffic offloading based on DNS query



[Fig. 1] MEC Network Architecture

2. Key Features

- MEC Data Routing
  - Control L3 between UE and ME app
- TOF (Traffic Offload Function)
  - Apply filter condition for certain type of traffic flow(TOF Rule)
  - TOF Type (Breakout / Inline / Tap / Info)
  - TOF Rule (Enable / Disable)
  - LBS (Load Balancing Service) with weight
- Packet Processing
  - UP/Down Link Traffic Processing
  - En/De-Capsulation
- MEC Service
  - Offer a variety of service including RNIS, Zone, Subscriber Info, etc.
  - Connect to 3rd-party PaaS service

3. Benefits

- Automated Lifecycle Mgmt & Configuration
- Flow-based routing based on various TOF(Traffic Offload Function) corresponding to S1/SGi.
- Provide configurable DNS based on REST API
- Include built-in weighted LBS(Load Balancing Service)
- Support various virtualization environment including KVM, Bare-Metal, Openstack, K8S

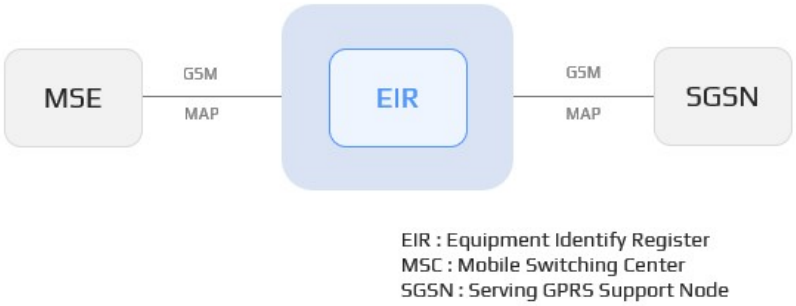
EIR

1. Description

Telcoware WCDMA EIR(Equipment Identity Register) is a system within WCDMA network responsible for storing and managing IMEI(International Mobile Station Equipment Identity) number.

MSC(Mobile Switching Center) or SGSN(Serving GPRS Supporting Node) sends IMEI status confirmation message to EIR via MAP(Mobile Application Part). EIR queries database for IMEI's status and sends result back to MSC or SGSN. If IMEI is in normal status(white-listed), call continues; if it's abnormal(black-listed due to stolen device), call is terminated.

In this way, EIR is used to detect stolen or unauthorized mobile device on network and restrict its usage.



EIR : Equipment Identify Register
MSC : Mobile Switching Center
SGSN : Serving GPRS Support Node

2. Key Features

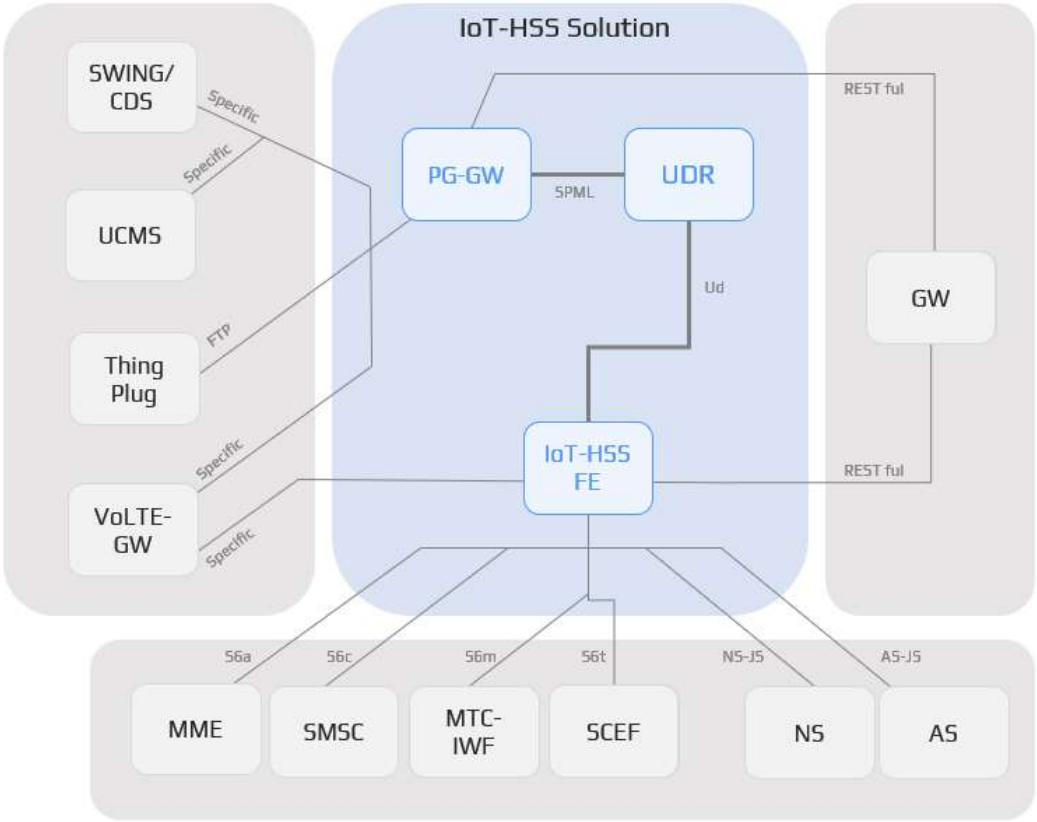
- Call processing with MSC and SGSN
- List management
  - White List: IMEI with allowed network access
  - Black List: IMEI with denied network usage
  - Gray list: IMEI with uncertain status, such as temporary issue
- Implicit IMEI List
- IMEI management by range
  - Manage list by range, along with individual IMEI
- Multi-IMEI management: Allow for duplicate IMEI information
- Add, Change, or Delete IMEI in each list

- IMEI list inquiry: View entire IMEI list or search by condition like model or vendor
- Additional list management: include institution, model, and valid reason code list
- Support standard SQL function and interface

IOT-HSS SOLUTION

1. Description

IoT-HSS Solution is a dedicated HSS solution based on 3GPP UDC(User Data Convergence) architecture. It is designed to manage LoRa device and LTE-based MTC/IoT device, comprising UDR(User Data Repository), PG-FE(Provisioning Gateway Front-end), and IoT-HSS FE.

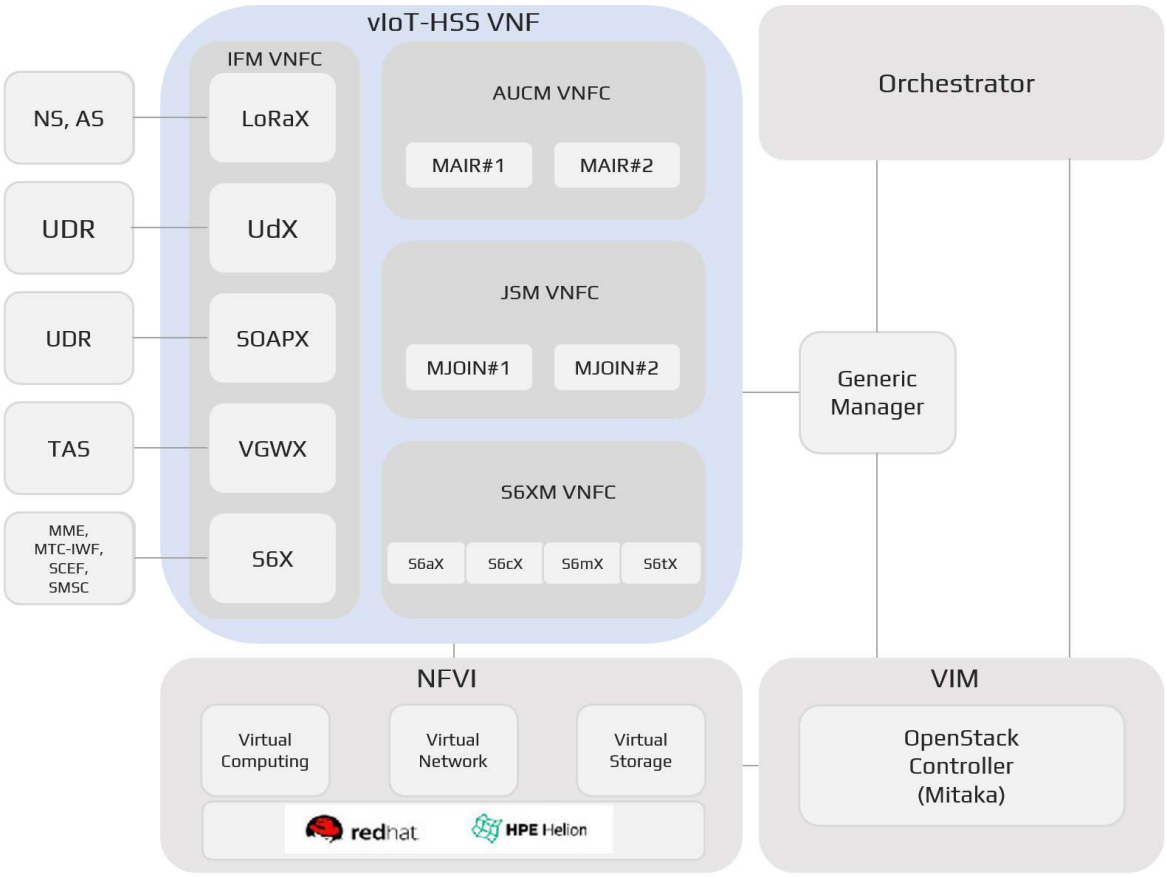


[Fig. 1] IoT-HSS solution components

- HSS system for the IoT-HSS FE – IoT device service
- Relay system between PG-FE – customer's self-care system and UDR (protocol conversion, etc.)
- Integrated DB server system for the UDR – UDC network

2. Key Features

IoT-HSS FE and PG-FE systems in IoT-HSS Solution are structured with NFV(Network Function Virtualization) architecture.



[Fig. 2] NFV-based IoT-HSS FE structure

- LTE authentication
  - Create and transmit LTE authentication vector
- LTE mobility management
  - Manage LTE location registration
  - Transfer and synchronize EPS subscription
  - Manage overseas roaming
  - SMS in MME
  - Manage rate plan
- SMS Outgoing/Incoming
  - SMS outgoing/incoming
  - SMS pending, Alert

- MONTE (Monitoring Enhancements)
  - Monitoring Configuration
  - Monitoring Report
  - NIDD(Non-IP Data Delivery) Configuration
- LoRa Device OTA Activation
  - Integrity protection through MIC check
  - Create and transfer session key for each MAC version
- LoRa device subscriber profile management
  - Transfer profile during join/rejoin
  - Synchronize profile via SOAP notification

3. Benefits

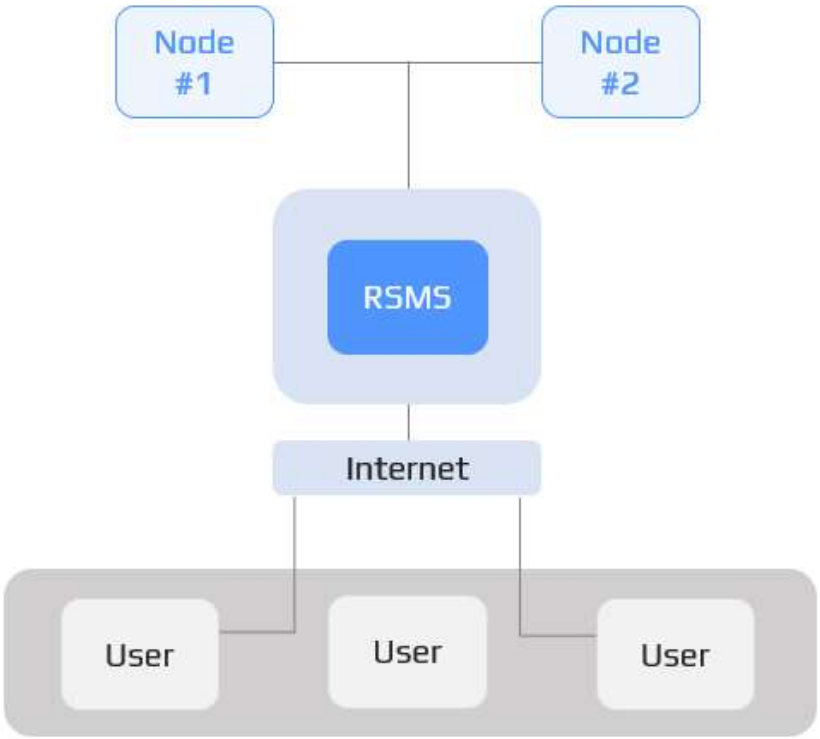
- Manage integrated subscriber for IoT device(LoRa, eMTC)
- Enhance flexibility through virtualization-based architecture
- Large-capacity subscriber service based on UDC architecture

RSMS

1. Description

Telcoware RSMS(Roaming Signal Monitoring System) captures message exchanged between network node using SS7 protocol, facilitated by SS7 monitoring cable.

RSMS decodes collected message and offers various function such as data analysis, message history based on data exchange, and statistical data. It allows for management of monitored network node and provide service for subscriber.



2. Key Features

- Decode and analyze all CDMA and WCDMA messages
- Web-based user tool
- Real-time message analysis
- Various statistics
- Message capturing between network nodes. No overload.

- Interworking with all nodes that use SS7 protocol
- Manage history based on file and database
- Manage message
- Store, manage, and analyze raw data from MTP2 message to MAP message
- Web access to analyzed raw data
- Strong data trace through user-centered service