5G Advanced (B5G)

5G Advanced evolved User Identities

and

Authentication Architecture

Ike Alisson

2024 - 03 - 12 Rev PA03

Table of Contents

1.5G System enables the ***Creation and Utilization of User-specific Identities*** in order to provide enhanced

- User Experience,
- Optimized Performance, and
- offer Services to Non-3GPP Devices and Human Users.

5G Network settings can be adapted, and Services can be offered to Users according to Users' Needs, which may be different from the Subscription Identifier that is used by the User to establish the Connection.

In 5G, the User to be identified could be

- an **Individual Human User** using **a UE with a certain Subscription** or
- **a Device** behind a Gateway UE (e.g. 5G PIN PEGC or 5G-RG).

Use Cases (UCs) include:

- an Individual Human User, using a UE with a certain Subscription; and
- a Device ("Thing") behind a Gateway UE.

In the context of identity Management something outside a System that needs to be identified in the System is referred to as *"Entity"*. In 3GPP such an Entity is called a "User". A User is not necessarily a Person, it could also be an Application or a Device ("thing").

The Entity is uniquely represented by an Identity in the System. The Identity can dependent on the role of the entity in the System (e.g. which kind of Service is used for which purpose).

As such, a User can have several User identities – e.g. one user identity representing the Professional Role of the (Human) User and another one representing some aspects of her Private life. There is a 1:n relation between User and User Identity.

A User Identity is associated with some pieces of information, which are generally called "attributes". One special form of attributes are "identifiers". The relation between Identity and Identifier is 1:n.

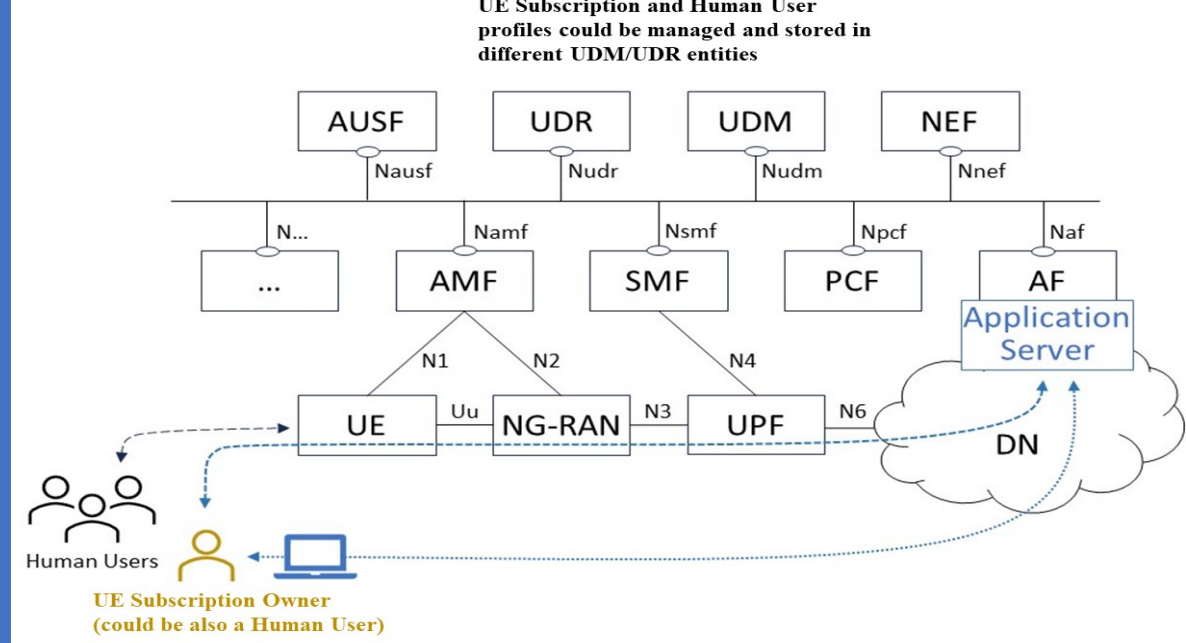


Figure: 3GPP 5G Architecture overview of unique User Identifier for multiple Human Users to use a single UE

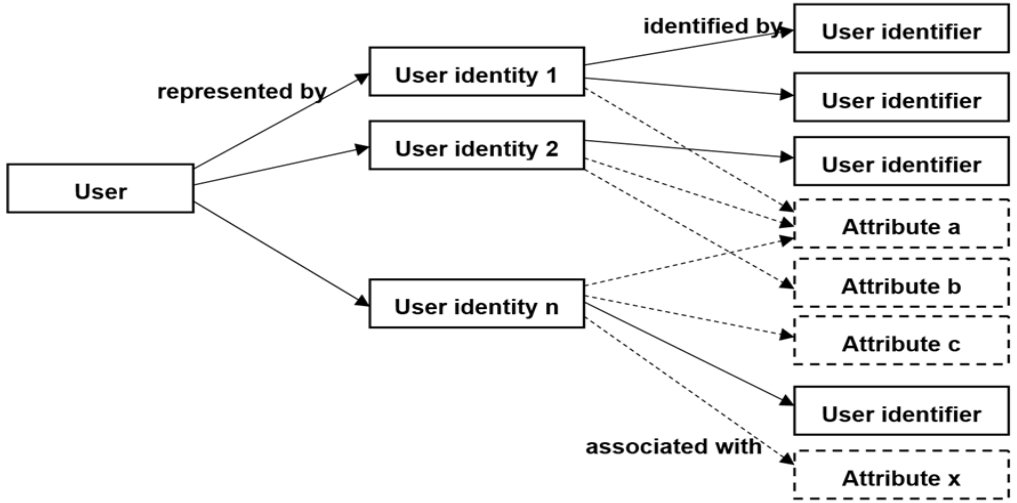


Figure: 3GPP 5G System relation between User, Identities, Identifiers and Attributes

1. The 5G System Architecture, Framework and the QoS Model are specified in 5G System Architecture, 5GS Procedures, 5GS Policy and should be regarded as **the baseline for** this specification.

- Subscriber/Subscription information will not be moved into a User Profile and Information from the User Profile should not be used to override information in a Subscription, e.g., the **Slices and DNNs, that are available to the UE,** do not change based on the **User of the UE**.

- The Subscription is a 5GS Subscription.

- When the User Identifier applies to a Human, only a Single User Identifier is active with a UE Subscription at a given time and it is assumed that the specific User Identifier is associated with all of the UE's traffic during the time that specific User Identifier is active with the UE's Subscription.

NOTE 1: The **Identifier of the Non-3GPP Devices** might not be called a "User Identifier" & a different name might be selected.

NOTE 2: A **User** is considered "active" if ***the associated user identifier has been authenticated and authorized to use a linked subscription to access the 5GS.***

NOTE 3: It is assumed that the ***Non-3GPP Devices*** do not support ***5G-AKA Authentication P***rocedures nor separate NAS connections with the 5GC for each Non-3GPP Device (e.g. like for AUN3 devices).

- The ***User Identifier and any Subscription*** that it links to are assumed to be associated with the same PLMN (e.g. the Operator that manages the User Identifier and the Operator that manages the Subscription is assumed to be the same).

- For the case of ***Non-3GPP device(s) behind a UE or 5G-RG***, how a ***User Identifier*** and any associated credentials are provisioned in a ***Non-3GPP device, UE, or Application*** is out of scope (e.g. the Credentials needed to be provisioned in the Non-3GPP Device by an Operator, Human User, or a 3rd Party).

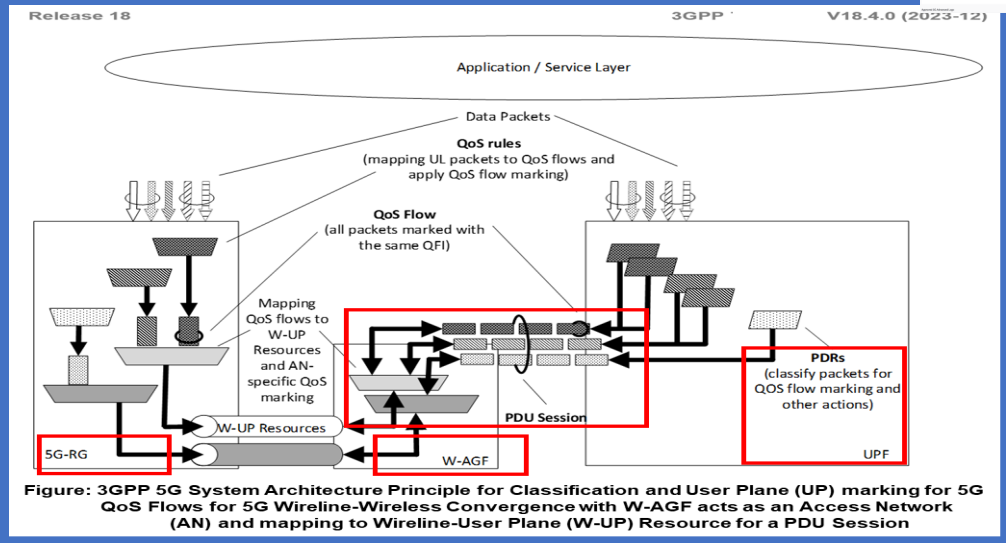


Figure: 3GPP 5G System Architecture Principle for Classification and User Plane (UP) marking for 5G QoS Flows for 5G Wireline-Wireless Convergence with W-AGF acts as an Access Network (AN) and mapping to Wireline-User Plane (W-UP) Resource for a PDU Session

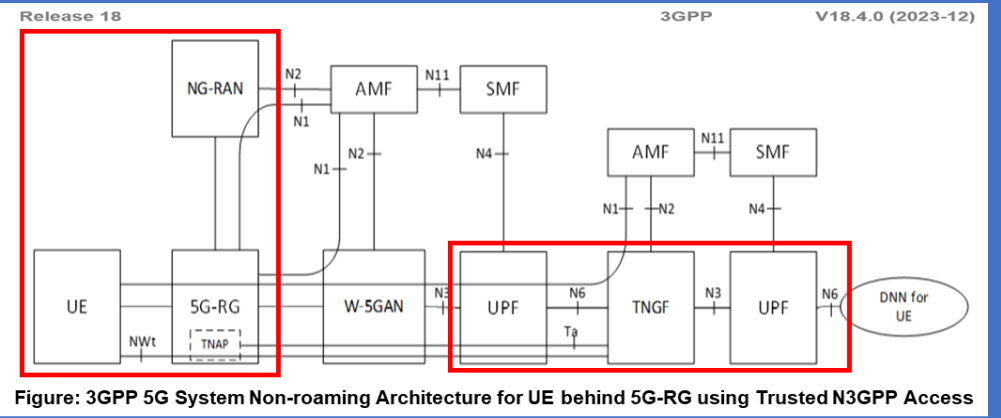


Figure: 3GPP 5G System Non-roaming Architecture for UE behind 5G-RG using Trusted N3GPP Access

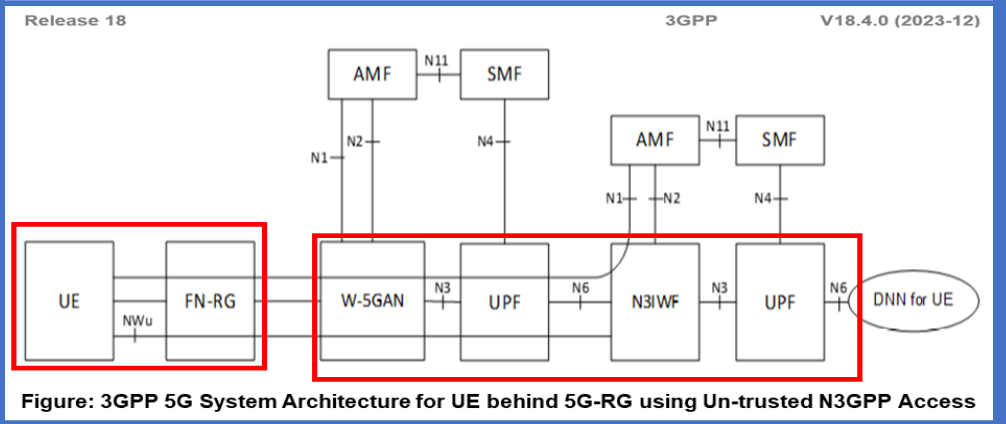


Figure: 3GPP 5G System Architecture for UE behind 5G-RG using Un-trusted N3GPP Access

1. 5G System QoS (Quality of Service) Model

The **5G System Architecture QoS Model** is based on **QoS Flows**. The 5GS QoS Model supports both **QoS Flows** that require *Guaranteed Flow Bit Rate (**GBR QoS Flows**)* and *QoS Flows that do not require Guaranteed Flow Bit Rate (**Non-GBR QoS Flows**).*

*The 5G QoS model also supports Reflective QoS (**RQI**).*

The ***5G QoS Flow is the finest granularity of QoS differentiation in the PDU Session***.

A *QoS Flow ID (**QFI**)* is used to identify a *QoS Flow in the 5G System*. User Plane (UP) traffic with the same QFI within a PDU Session receives the same traffic forwarding treatment (e.g. Scheduling, Admission threshold). ***The QFI is carried in an encapsulation header on N3 (and N9) i.e. without any changes to the E2E Packet Header***.

QFI shall be used for all PDU Session Types. The ***QFI shall be unique within a PDU Session.*** The QFI may be dynamically assigned or might be ***equal to the 5QI.***

Within the 5GS, 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.

Alternative QoS Profile

The Alternative QoS Profile(s) can be optionally provided for a GBR QoS Flow with Notification control enabled. If the corresponding PCC Rule contains the related information, the 5G CN CP shall provide, in addition to the QoS Profile, a Prioritized List of Alternative QoS Profile(s) to the NG-RAN. If the 5G CN CP provides a new prioritized list of Alternative QoS Profile(s) to the NG-RAN (if the corresponding PCC rule information changes), the NG-RAN shall replace any previously stored list with it.

An Alternative QoS Profile represents a combination of QoS parameters PDB, PER, Averaging Window and GFBR to which the application traffic is able to adapt. For delay-critical GBR QoS flows, an Alternative QoS Profile may also include an MDBV.

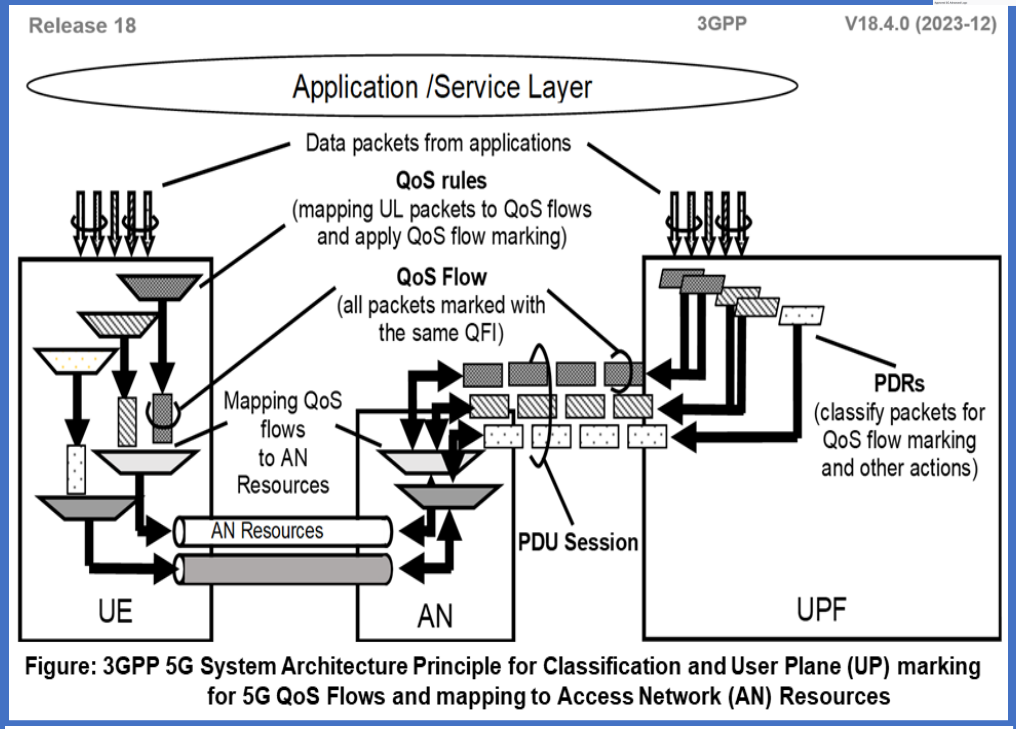


Figure: 3GPP 5G System Architecture Principle for Classification and User Plane (UP) marking for 5G QoS Flows and mapping to Access Network (AN) Resources

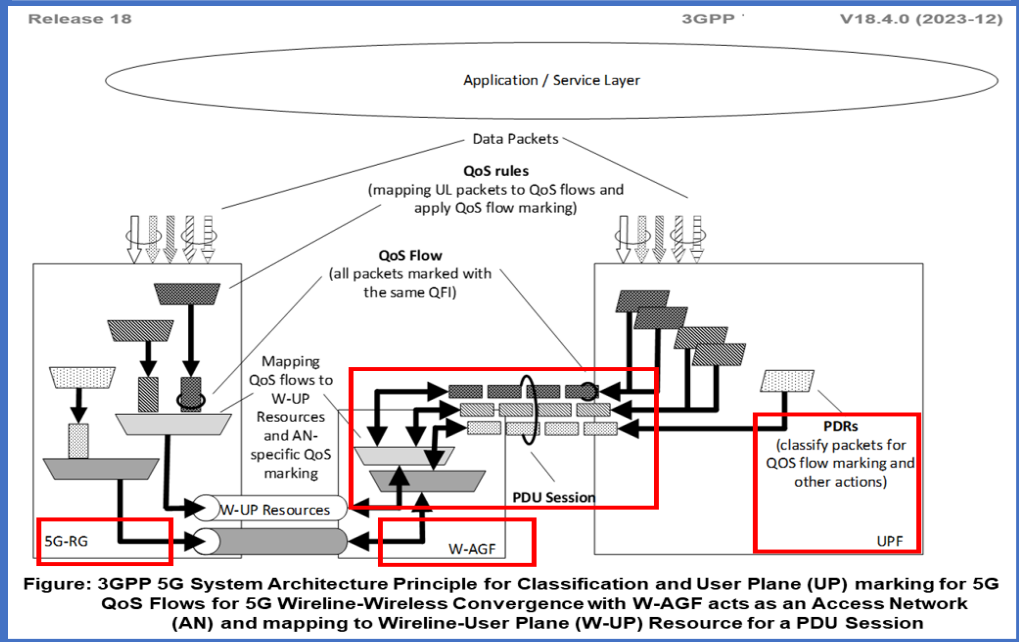


Figure: 3GPP 5G System Architecture Principle for Classification and User Plane (UP) marking for 5G QoS Flows for 5G Wireline-Wireless Convergence with W-AGF acts as an Access Network (AN) and mapping to Wireline-User Plane (W-UP) Resource for a PDU Session

1. 5G System User Identities specified Key Issues (KIs) with Solutions

1. Key Issue #1: Identifying the Human User of a Subscription

This KI focuses on how to support identifying the Human User of a UE's 3GPP Subscription when the Human User access Services via the 5GS using a User Identifier.

2. Key Issue #2: Authentication and Authorization of Users and Restrictions on Users

This KI builds on the identifying Human User case of KI#1 and focuses on How Users are Authenticated and Authorized and How the Network restricts User Identifiers.

3. Key Issue #3: Exposure of User Identity Profile Information (Privacy Identity)

This KI builds on the identifying Human User case of KI #1 and focuses on How User Identifier related Functionality and Information is exposed.

4. Key Issue #4: Identifying Non-3GPP Devices Connecting behind a UE or 5G-RG

This key issue will study whether and how 5G Core Network (5G CN) identifies Individual Non-3GPP Devices connecting behind a UE or 5G-RG and whether and How to provide Policy Control for the Traffic associated with Individual Non-3GPP Devices.

Release 19 3GPP V0.2.0 (2024-03)

Mapping of Solutions to Key Issues

Table : Mapping of Solutions to Key Issues

Solutions				
	<Key Issue #1>	<Key Issue #2>	<Key Issue #3>	<Key Issue #4>
#1	X	X	X	
#2	X			
#3	X	X		
#4	X			
#5	X	X		
#6	X			
#7	X			
#8		X		
#9		X		
#10		X	X	
#11		X	X	
#12		X	X	
#13		X		
#14		X		
#15			X	
#16			X	

1. 5GS User Identifiers selected examples of specified Key Issues (KIs) with different Solutions

Solution: User Identifier linked with a UE Subscription via the Authenticated UE Channel

This Solution addresses KI#1 (linking of User ID).

The Figure illustrates a high level Architecture for the Solution Configuration specification. In this Architecture, the Service Provider (SP) supports the existing OAUTH2 Framework for User ID Provider. ***The SP pre-configures to the MNO with the OAUTH2's Endpoint Address for checking the User ID Verification Information (e.g. OAUTH ID token).***

Using the existing Framework, it can authenticates the User ID and issues the User ID Verification Information after successful User Authentication and delivers it to the User Application, that triggers the UE to start User ID linking procedure by providing the User ID Verification Information received from the ID Provider through the authenticated UE's channel (e.g. NAS channel) **to the 5GC.**

The **5GC verifies the User ID verification Information** received through the Authenticated channel **from the UE *by invoking the pre-configured Endpoint Address of OAUTH2 framework for verifying the User ID Verification Information***.

If the 5GC have checked User ID Verification Information successfully***, the 5GC stores the association between the UE's Subscription information and the UE.***

The association between UE and User ID can be stored in the UDM/UDR as well as UIDF, e.g., the NF (e.g. NEF) in the 5GC can **dynamically update the** associated User ID information into the UDM/UDR for the UE. After this linking procedure is successful, the Application Service can use the User ID to invoke the subsequent NEF service.

User Information Database Function (UIDF) is *a new entity that can store the specific aspects related to a User ID,* e.g. *specific QoS/ or User Plane (UP) relates "settings" for a particular User. The User Profile for a particular User ID also store a reference to the UE Subscription(s) that are linked to the particular User ID.*

After the linking has been performed, UIDF may be updated (by 3rd Party AFs or other Network Functions (NFs)) in order to ***store User specific QoS settings for the User ID.***

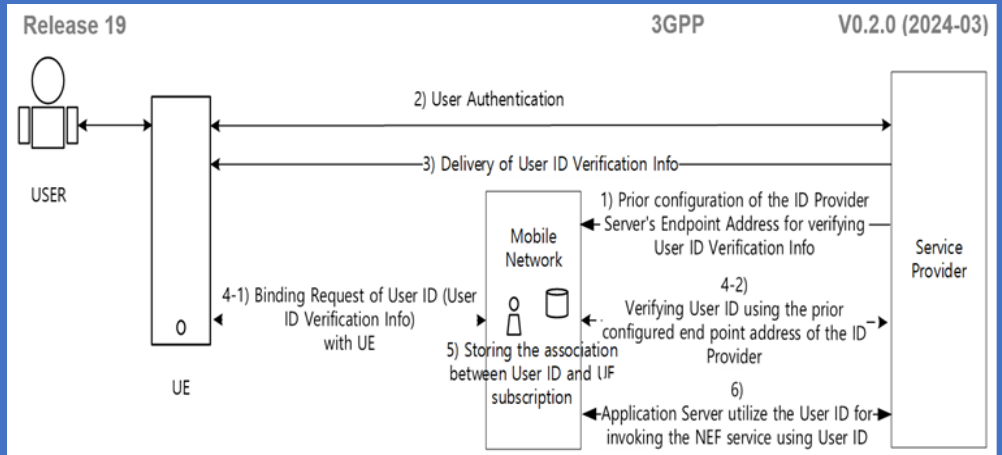


Figure: 3GPP 5G System User Identifier linking with a UE Subscription via the Authenticated UE Channel

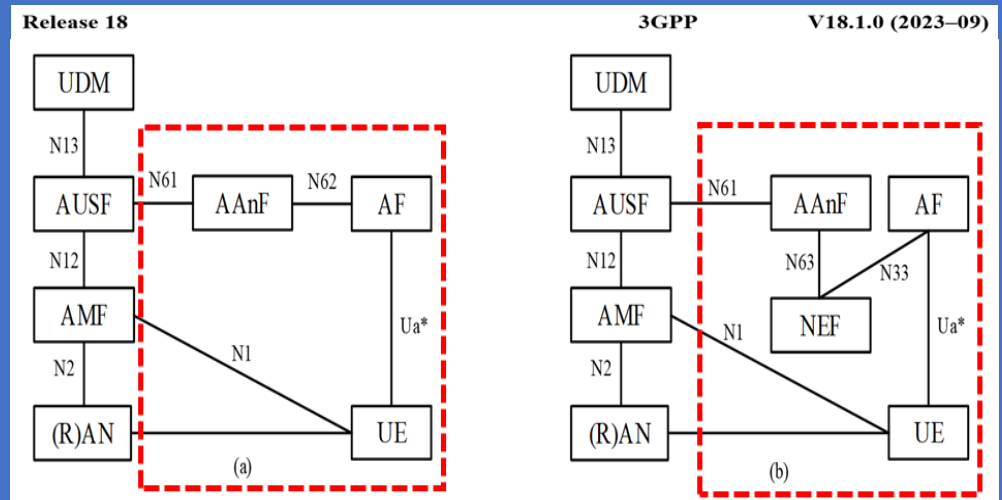


Figure: 5G System Architecture Fundamental Network Model for Authentication and Key Management for Applications (AKMA) Architecture in Reference Point representation for (a) Internal HPLMN AFs and (b) External AFs

Solution: Unique User Identifier for a Human User and how it is used in 3GPP 5GS Procedures to associate the Human User with a UE

This solution addresses KI#2 "Authentication and Authorization of Users and Restrictions on Users".

The solution introduces a *new unique User Identifier* and specifies How the *unique User Identifier* is used in 3GPP Procedures to ***associate a Human User with a UE dynamically.***

This solution is based on dedicated User Profiles for the Human Users and a UE Subscription Profile for the UE (containing a USIM Card). The potential Human Users and the User owning the UE have Individual Contracts with a Single MNO to ensure that the User Profiles and the UE Subscription belongs to the same MNO Domain. The Figure shows how the Solution is embedded in the 3GPP Architecture and provides an overview how Multiple Human Users can use a single UE.

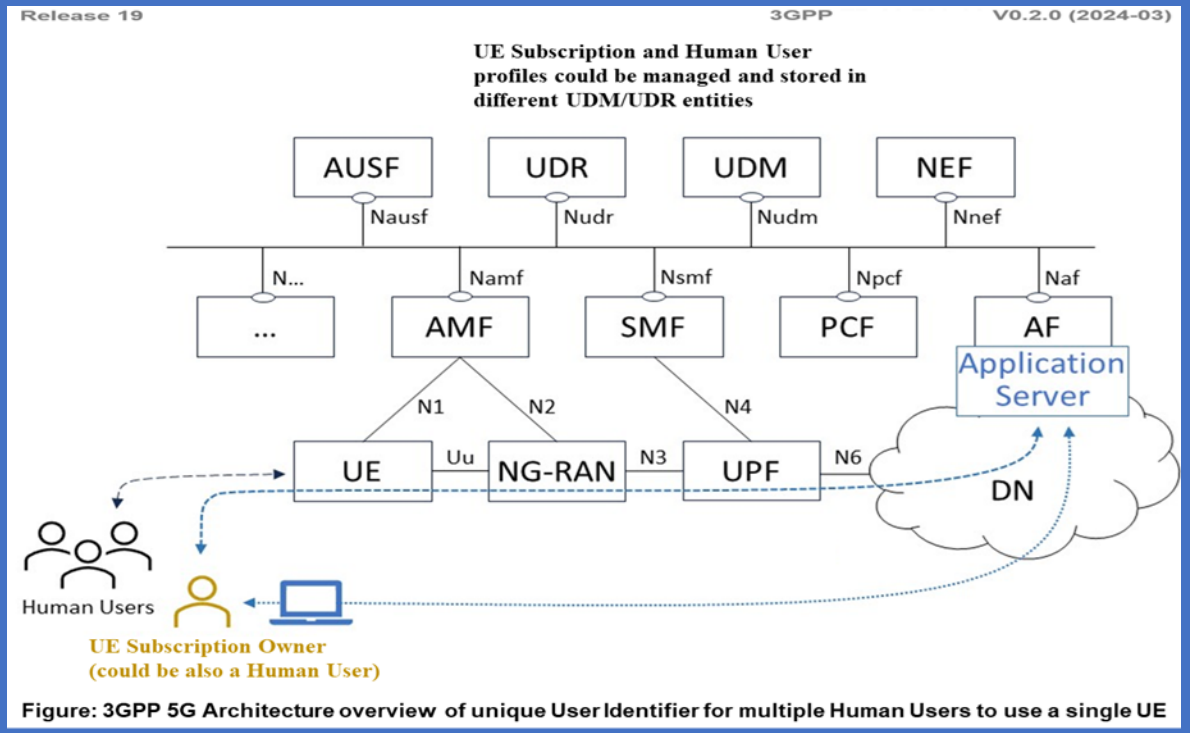


Figure: 3GPP 5G Architecture overview of unique User Identifier for multiple Human Users to use a single UE

When a Human User login to a UE, the UE initiates the registration of the human User to the 5GS via the UE. During the registration the User profile of the Human User is associated with the UE Subscription as follows:

- Only *one (1) Human User Profile is associated with the UE Subscription* at a given time. The ***UE Subscription is dedicated to the USIM Owner,*** who provided the USIM in the UE.

Editor's note: Detailed behaviour when a User initiates a Registration at the UE, but another User with a different User Identifier is already registered is for future Releases. This includes, e. g., the consideration of Security aspects and the decision if UE or CN initiated de-registration is preferred.

- When the MNO allows the association of Multiple Human User(s) with a UE Subscription, a Human User, preferable the one that owns the USIM Card in the UE should be enabled to provide the Information, which Human User is allowed to use the UE. For this purpose, the MNO may limit the Number of potential User Profiles that can be associated to the UE with the UE Subscription.

It is up the MNO to offer Methods to manage potential Human User associations with a UE Subscription, e.g., the respective Information may be part of the Contract Processes and the result is deployed UE Subscription Data and User Profile Data via OAM Services.

Solution: Exposing User Authentication result to 3rd Parties

This Solution addresses KI#2 (Authentication of Users) and KI#3 (Exposure of User Identity Functionality).

The Solution covers the Scenario as per UC for Identity Provisioning to External Services by 3rd Parties.

The UC involves a 3rd Party Entity (e.g. a Bank) requesting for an Authentication Service (or 2nd-Factor Authentication) via the Operator.

Using traditional SMS-OTP for 2nd Factor Authentication could be a ground for Security risk. SMS-OTP solutions are prone to phishing attacks. Whereas using a UE's already established Connection to perform User Authentication, could further provide trust that the User is using its own UE (to which it's User ID was linked securely by the Operator) and using it's own (HPLMN) Network.

The specified Procedures can also be used as a Primary login (and signing up) for 3rd Party Services using Operator's User Identifier.

This enables the Operator to leverage their infrastructure and offer Secure Authentication Solutions to 3rd Party Applications.

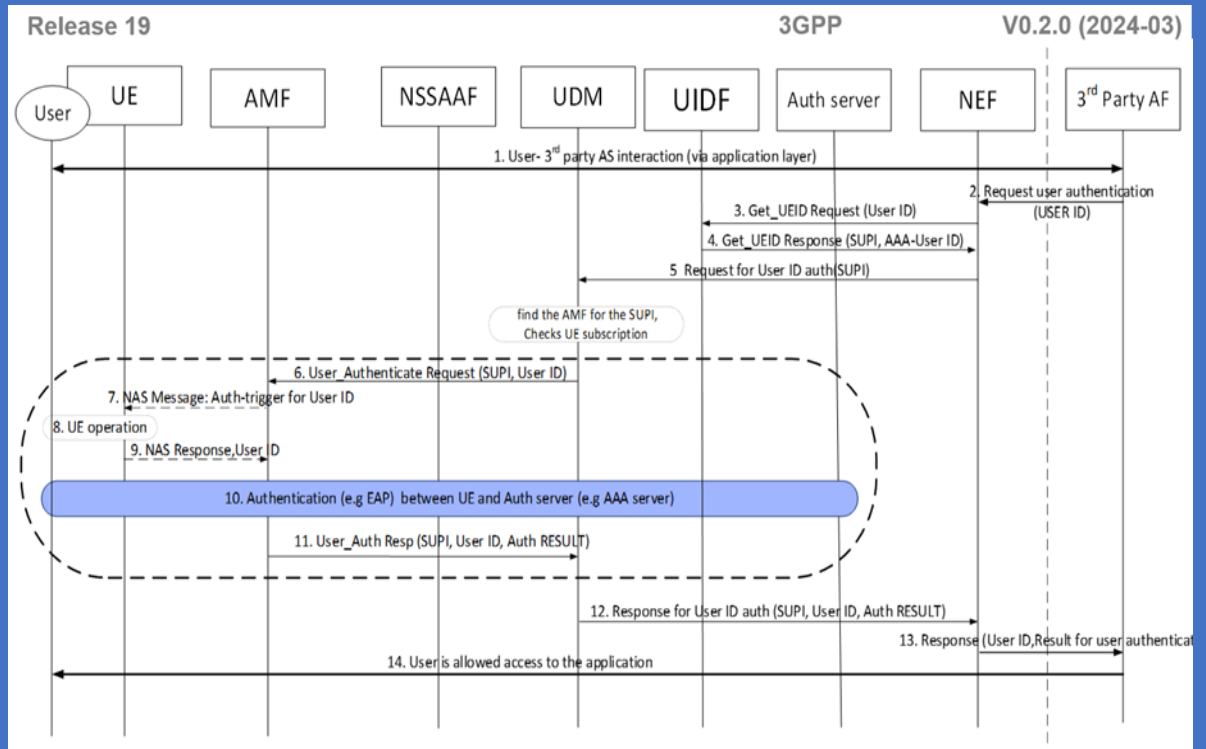


Figure: 3GPP 5G System User Identifier Procedures for 3rd Party Applications requesting User Authentication

Solution: User Identity Profile Server based Control

This Solution addresses KI#2 and KI#3.

The *User Identity Profiles (**UIPs**)* are stored in a UIP Server. The Principles for the UIP Server are as follows:

1. The UIPs can be managed, e.g. created, updated, and removed, by the PLMN Operator.
2. The UIPs can be managed, e.g. created, updated, and removed by Trusted Server (Portal) or by the UE/User, and in such case the PLMN Operator authorizes the Management Operations.
3. All UIP Management Procedures are performed from an Authorized and Authenticated Entity.
4. ***The UIP Information is pushed by the UIP Server to the 5GC, optionally via the NEF.***

The Architecture configurations for Roaming and Non-Roaming are exemplified in the Figures.

The interface between the UE and the Portal is assumed to be an Application Layer Interface.

The Xuips Interface between the UIP Client and the UIP Server is assumed to be on Application Layer and not standardized by 3GPP Architecture.

The Portal is a Trusted Entity from the HPLMN perspective, and can e.g. be managed by the HPLMN Operator or a Trusted Partner.

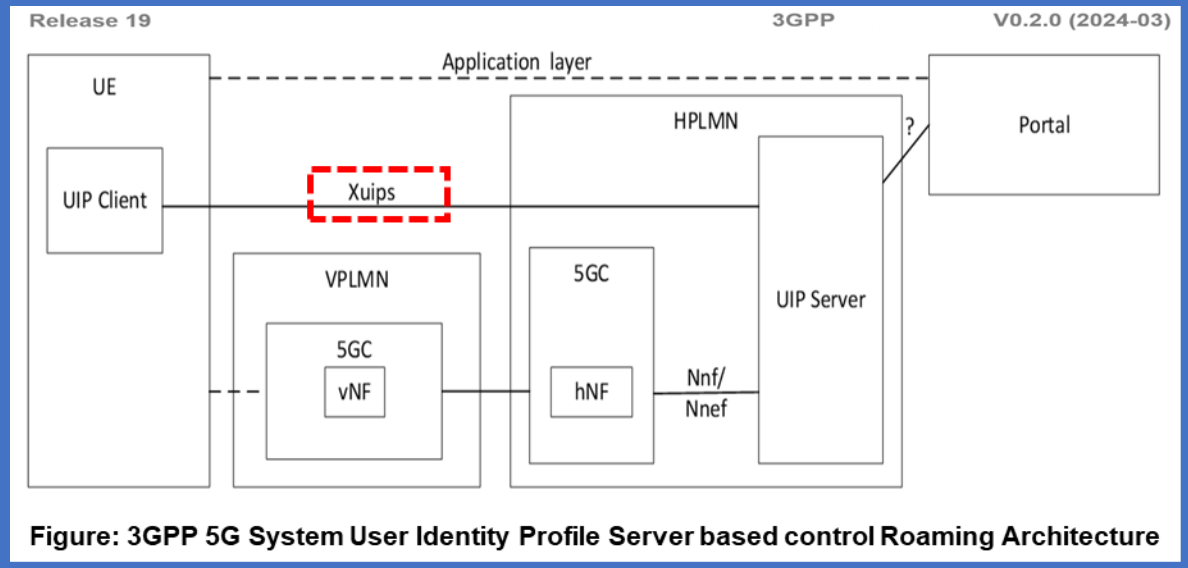


Figure: 3GPP 5G System User Identity Profile Server based control Roaming Architecture

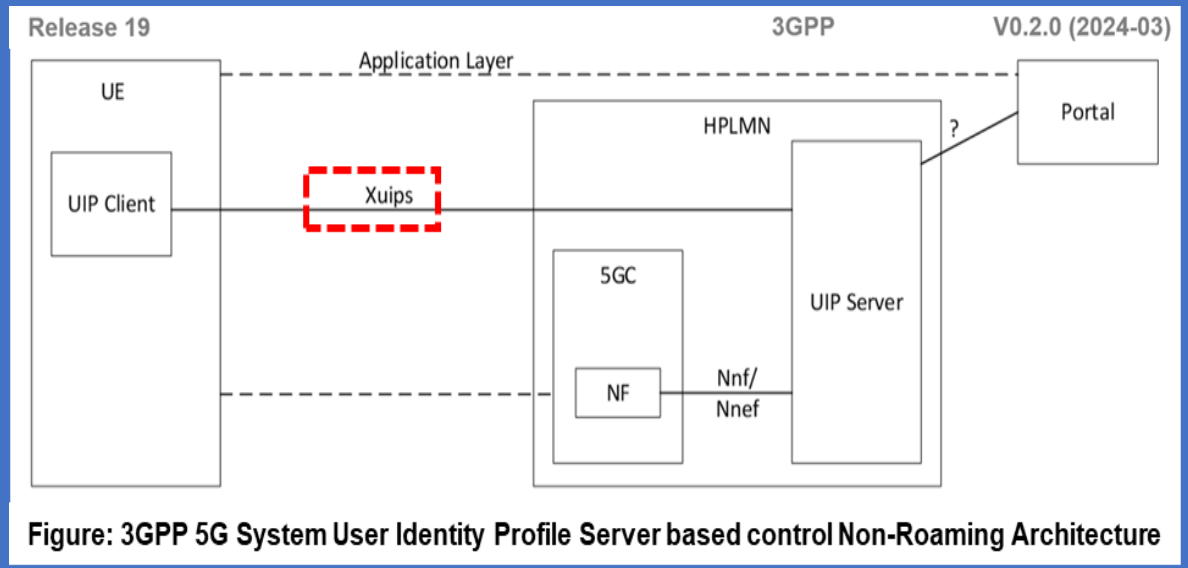


Figure: 3GPP 5G System User Identity Profile Server based control Non-Roaming Architecture

2. 5G System Architecture "Authentication and Key Management for Applications" Capability - 1

3GPP have introduced many novel Security Features in 5G.

One of the "new" Security Features defined is "*Authentication and Key Management for Applications (AKMA)*", to enable Applications to leverage the *Authentication of the UE performed by the PLMN* and to use it *for further Authentication and Authorization by an Application* and to bootstrap the *necessary Application Security Keys to the UE.*

When *a UE registers with the PLMN for the first (1st) time*, the *Network* performs a *Primary Authentication of the UE*.

Only after the *Successful Primary Authentication of the UE*, the *UE is authorized* for additional Network Services.

3GPP has *specified two (2) Protocols for Primary Authentication*:
- 5G-AKA and
- EAP-AKA'

both of which can *be executed over 3GPP Access and Non-3GPP Access.*

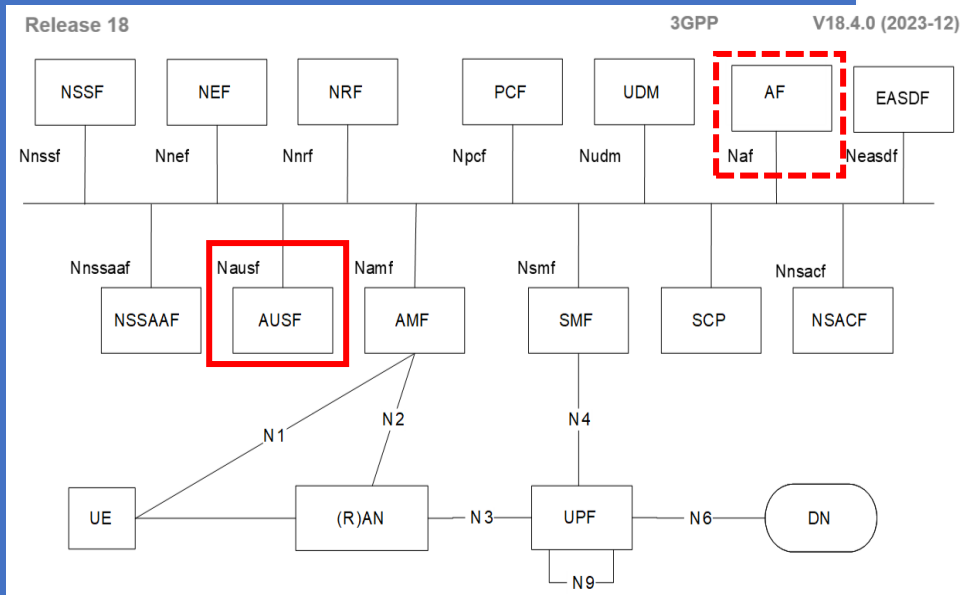


Figure: 5G System Non-roaming Architecture

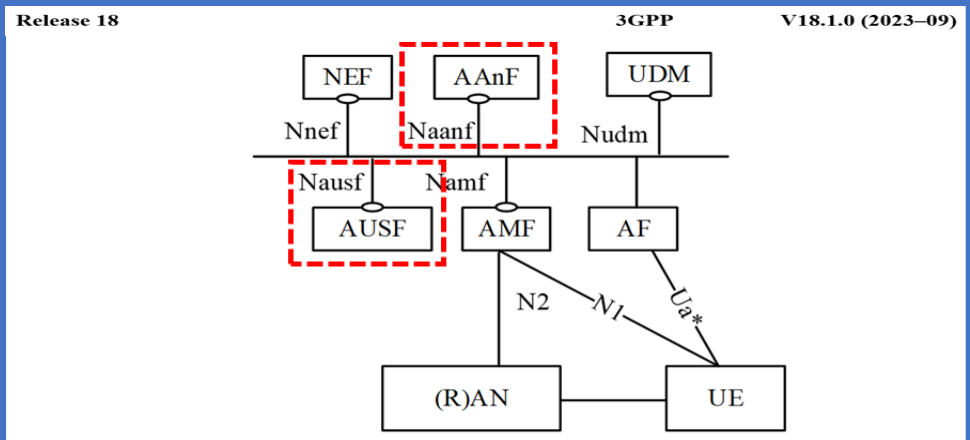


Figure: 5G System Architecture Fundamental Network Model for Authentication and Key Management for Applications (AKMA)

NOTE: The Figure shows the case where *AKMA Anchor Function* (**AAnF**) is deployed as a Stand-alone Function. Deployments can choose to collocate *AAnF* with *AUSF* or with *NEF* according to Operators' deployment Scenarios.

2. 5G System Architecture “Authentication and Key Management for Applications" Capability - 2

In the *Primary Authentication*, the *Subscription Credentials and the shared secret* ***stored in the USIM of the UE*** **and the same** ***stored in the 5G CN Nodes of the Operator Network*** **is verified**.

In 5G, a new Security Network Function (**NF**), Authentication Server Function (**AUSF**) has been introduced in the 5G Core (**5GC**) to manage the ***UE Authentication*** using the **SUCI** or the **SUPI** and to manage the *Root Session Key* ***KAUSF*****.**

The **AUSF** stores the *Root Session Key* **KAUSF** and *further Keys* are derived from *this Key*.

The UE and Network derive further Keys from the ***KAUSF.***

The *availability of the key* ***KAUSF*** *at the* ***AUSF*** *and the* ***UE****,* as a result of the successful *Primary Authentication* has become an advantage since this key *could be used to generate further keys that could be bootstrapped to secure different Applications.*

AKMA Key Hierarchy as specified ***in 5G System Security Domains Architecture*** is shown in the figure(s) on slide(s) 5-9.

From the *Key KAUSF, an AKMA Specific Key* ***KAKMA*** is derived.

To secure Individual Applications, an ***Application Specific Key*** **KAF** is derived from the **KAKMA.**

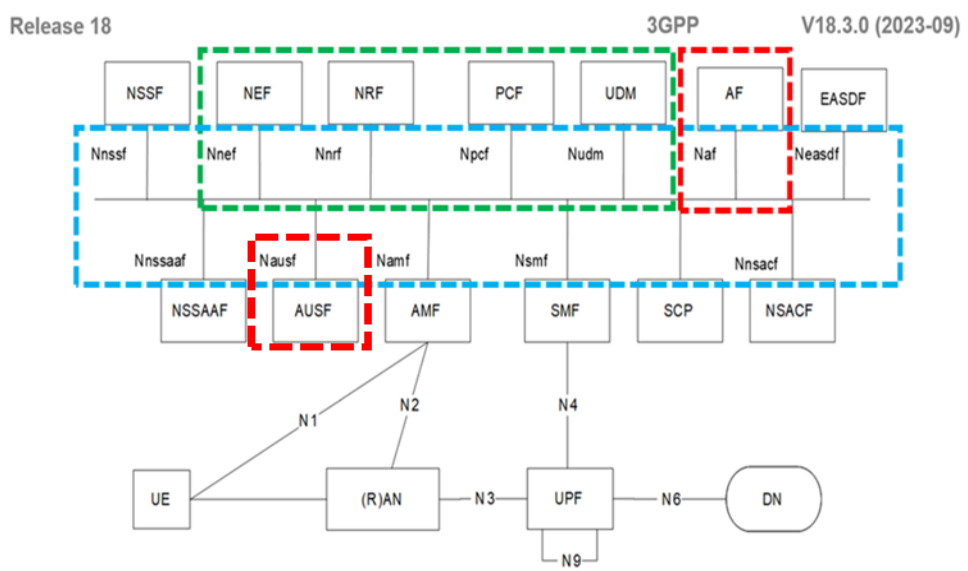


Figure: 5G System Non-Roaming Architecture

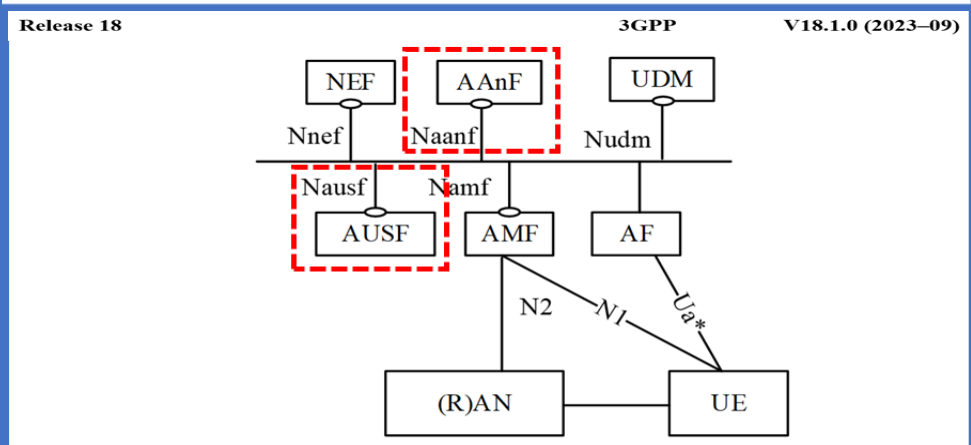


Figure: 5G System Architecture Fundamental Network Model for Authentication and Key Management for Applications (AKMA)

NOTE: The Figure shows the case where *AKMA Anchor Function* (**AAnF**) is deployed as a Stand-alone Function. Deployments can choose to collocate *AAnF* with *AUSF* or with *NEF* according to Operators' deployment Scenarios.

2. 5G System Architecture “Authentication and Key Management for Applications" Capability - 3

5G USIM Service Table Elementary File (EF_{UST})

This *UE USIM Elementary File* indicates *which Services are available*. If a Service *is not indicated as available* in the *USIM,* the ME/UE shall not select this Service.

-Services Contents:

Service n°1:	Local Phone Book
Service n°2:	Fixed Dialling Numbers (FDN)
Service n°3:	Extension 2
Service n°4:	Service Dialling Numbers (SDN)
Service n°5:	Extension3
Service n°6:	Barred Dialling Numbers (BDN)
Service n°7:	Extension4
Service n°8:	Outgoing Call Information (OCI and OCT)
Service n°9:	Incoming Call Information (ICI and ICT)
Service n°10:	Short Message Storage (SMS)
Service n°11:	Short Message Status Reports (SMSR)
Service n°12:	Short Message Service Parameters (SMSP)
Service n°13:	Advice of Charge (AoC)
Service n°14:	Capability Configuration Parameters 2 (CCP2)
Service n°15:	Cell Broadcast Message Identifier
Service n°16:	Cell Broadcast Message Identifier Ranges
Service n°17:	Group Identifier Level 1
Service n°18:	Group Identifier Level 2
Service n°19:	Service Provider Name
Service n°20:	User controlled PLMN selector with Access Technology
Service n°21:	MSISDN
Service n°22:	Image (IMG)
Service n°23:	Support of Localised Service Areas (SoLSA)
Service n°24:	Enhanced Multi-Level Precedence and Pre-emption Service
Service n°25:	Automatic Answer for eMLPP
Service n°26:	RFU
Service n°27:	GSM Access
Service n°28:	Data download via SMS-PP
Service n°29:	Data download via SMS-CB
Service n°30:	Call Control by USIM
Service n°31:	MO-SMS Control by USIM
Service n°32:	RUN AT COMMAND command
Service n°33:	shall be set to '1'
Service n°34:	Enabled Services Table
Service n°35:	APN Control List (ACL)
Service n°36:	Depersonalisation Control Keys
Service n°37:	Co-operative Network List
Service n°38:	GSM security context
Service n°39:	CPBCCH Information
Service n°40:	Investigation Scan
Service n°41:	MexE
Service n°42:	Operator controlled PLMN selector with Access Technology
Service n°43:	HPLMN selector with Access Technology
Service n°44:	Extension 5
Service n°45:	PLMN Network Name
Service n°46:	Operator PLMN List
Service n°47:	Mailbox Dialling Numbers
Service n°48:	Message Waiting Indication Status
Service n°49:	Call Forwarding Indication Status
Service n°50:	Reserved and shall be ignored
Service n°51:	Service Provider Display Information
Service n°52	Multimedia Messaging Service (MMS)
Service n°53	Extension 8
Service n°54	Call control on GPRS by USIM
Service n°55	MMS User Connectivity Parameters
Service n°56	Network's indication of alerting in the MS (NIA)
Service n°57	VGCS Group Identifier List (EF_{VGCS} and EF_{VGCSS})
Service n°58	VBS Group Identifier List (EF_{VBS} and EF_{VBSS})
Service n°59	Pseudonym
Service n°60	User Controlled PLMN selector for I-WLAN access
Service n°61	Operator Controlled PLMN selector for I-WLAN access
Service n°62	User controlled WSID list
Service n°63	Operator controlled WSID list
Service n°64	VGCS security
Service n°65	VBS security
Service n°66	WLAN Reauthentication Identity
Service n°67	Multimedia Messages Storage
Service n°68	Generic Bootstrapping Architecture (GBA)
Service n°69	MBMS security
Service n°70	Data download via USSD and USSD application mode
Service n°71	Equivalent HPLMN
Service n°72	Additional TERMINAL PROFILE after UICC activation
Service n°73	Equivalent HPLMN Presentation Indication
Service n°74	Last RPLMN Selection Indication
Service n°75	OMA BCAST Smart Card Profile
Service n°76	GBA-based Local Key Establishment Mechanism
Service n°77	Terminal Applications
Service n°78	Service Provider Name Icon
Service n°79	PLMN Network Name Icon
Service n°80	Connectivity Parameters for USIM IP connections
Service n°81	Home I-WLAN Specific Identifier List
Service n°82	I-WLAN Equivalent HPLMN Presentation Indication
Service n°83	I-WLAN HPLMN Priority Indication
Service n°84	I-WLAN Last Registered PLMN
Service n°85	EPS Mobility Management Information
Service n°86	Allowed CSG Lists and corresponding indications
Service n°87	Call control on EPS PDN connection by USIM
Service n°88	HPLMN Direct Access
Service n°89	eCall Data
Service n°90	Operator CSG Lists and corresponding indications
Service n°91	Support for SM-over-IP
Service n°92	Support of CSG Display Control
Service n°93	Communication Control for IMS by USIM
Service n°94	Extended Terminal Applications
Service n°95	Support of UICC access to IMS
Service n°96	Non-Access Stratum configuration by USIM
Service n°97	PWS configuration by USIM
Service n°98	RFU
Service n°99	URI support by UICC
Service n°100	Extended EARFCN support
Service n°101	ProSe
Service n°102	USAT Application Pairing
Service n°103	Media Type support
Service n°104	IMS call disconnection cause
Service n°105	URI support for MO SHORT MESSAGE CONTROL
Service n°106	ePDG configuration Information support
Service n°107	ePDG configuration Information configured
Service n°108	ACDC support
Service n°109	Mission Critical Services
Service n°110	ePDG configuration Information for Emergency Service supp
Service n°111	ePDG configuration Information for Emergency Service confi
Service n°112	eCall Data over IMS
Service n°113	URI support for SMS-PP DOWNLOAD as defined in
Service n°114	From Preferred
Service n°115	IMS configuration data
Service n°116	TV configuration
Service n°117	3GPP PS Data Off
Service n°118	3GPP PS Data Off Service List
Service n°119	V2X
Service n°120	XCAP Configuration Data
Service n°121	EARFCN list for MTC/NB-IOT UEs
Service n°122	5GS Mobility Management Information
Service n°123	5G Security Parameters
Service n°124	Subscription identifier privacy support
Service n°125	SUCI calculation by the USIM
Service n°126	UAC Access Identities support
Service n°127	Control plane-based steering of UE in VPLMN
Service n°128	Call control on PDU Session by USIM
Service n°129	5GS Operator PLMN List
Service n°130	Support for SUPI of type NSI or GLI or GCI
Service n°131	3GPP PS Data Off separate Home and Roaming lists
Service n°132	Support for URSP by USIM
Service n°133	5G Security Parameters extended
Service n°134	MuD and MiD configuration data
Service n°135	Support for Trusted non-3GPP access networks by USIM
Service n°136	Support for multiple records of NAS security context storage for multiple registration
Service n°137	Pre-configured CAG information list
Service n°138	SOR-CMCI storage in USIM
Service n°139	5G ProSe
Service n°140	Storage of disaster roaming information in USIM
Service n°141	Pre-configured eDRX parameters
Service n°142	5G NSWO support
Service n°143	PWS configuration for SNPN in USIM
Service n°144	Multiplier Coefficient for Higher Priority PLMN search via NG-RAN satellite access
Service n°145	K_{AUSF} derivation configuration
Service n°146	Network Identifier for SNPN (NID)
Service n°147	5MBS UE pre-configuration
Service n°148	UE configured for using "Operator controlled signal threshold per access technology"

Release 18 3GPP V18.2.0 (2023-09)

Table: USIM Service Table Elementary File (EF_{UST})

Identifier: '6F38'	Structure: transparent	Mandatory
SFI: '04'		
File size: X bytes, (X ≥ 1)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Services n°1 to n°8	M	1 byte
2	Services n°9 to n°16	O	1 byte
3	Services n°17 to n°24	O	1 byte
4	Services n°25 to n°32	O	1 byte
etc.			
X	Services n°(8X-7) to n°(8X)	O	1 byte

2. 5G System Architecture "Authentication and Key Management for Applications" Capability - 4

In the UE *Primary Authentication*, the *Subscription Credentials and the shared secret stored in the USIM of the UE* and the same *stored in the 5G CN Nodes of the Operator Network* is verified.

In **5G**, *a new Security Network Function (NF)*, Authentication Server Function (**AUSF**) has been introduced in the 5G Core (**5GC**) to manage the *UE Authentication* using the **SUCI** or the ***SUPI*** and to manage the Root Session Key **KAUSF.**

The **AUSF** stores the Root Session Key **KAUSF** and further Keys are derived from this Key. *The UE and Network derive further Keys from the **KAUSF.***

The availability of the key ***KAUSF*** at the AUSF and the **UE**, as a result of the successful *Primary Authentication* has become an advantage since this key could be used to generate further keys that could be bootstrapped to secure different applications. The Key Hierarchy as specified in the 5G System Architecture is shown below.

From the *Key KAUSF*, an *AKMA Specific Key **KAKMA*** is derived.
To secure Individual Applications, an Application Specific Key **KAF** is derived from the ***KAKMA*.**

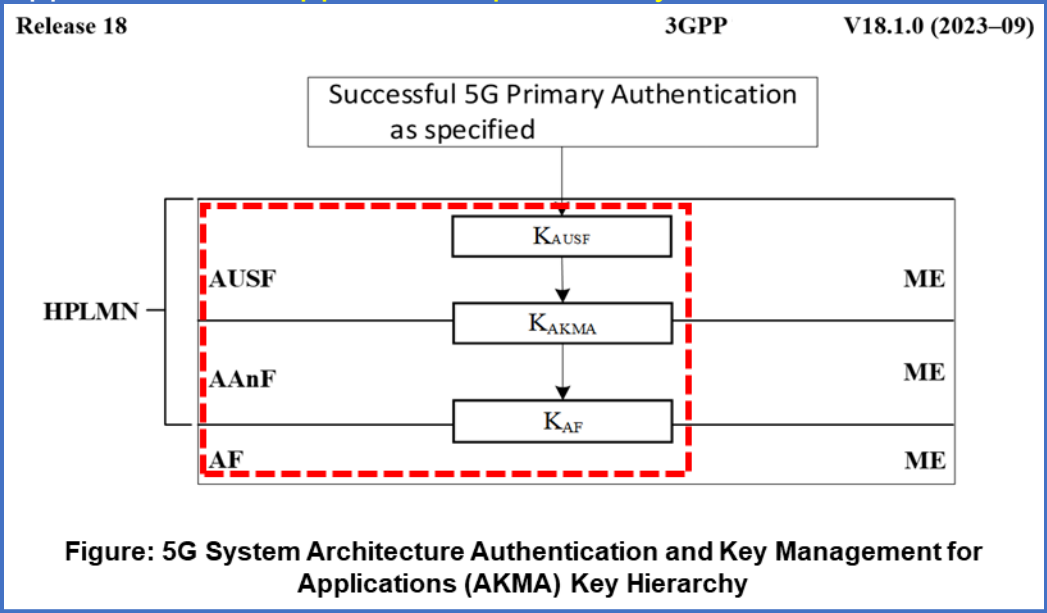


Figure: 5G System Architecture Authentication and Key Management for Applications (AKMA) Key Hierarchy

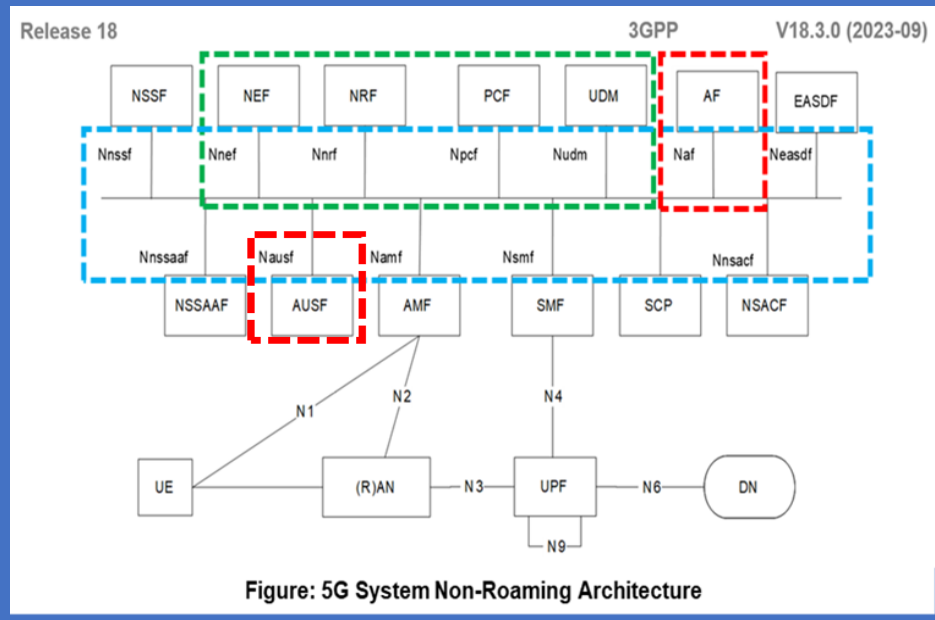


Figure: 5G System Non-Roaming Architecture

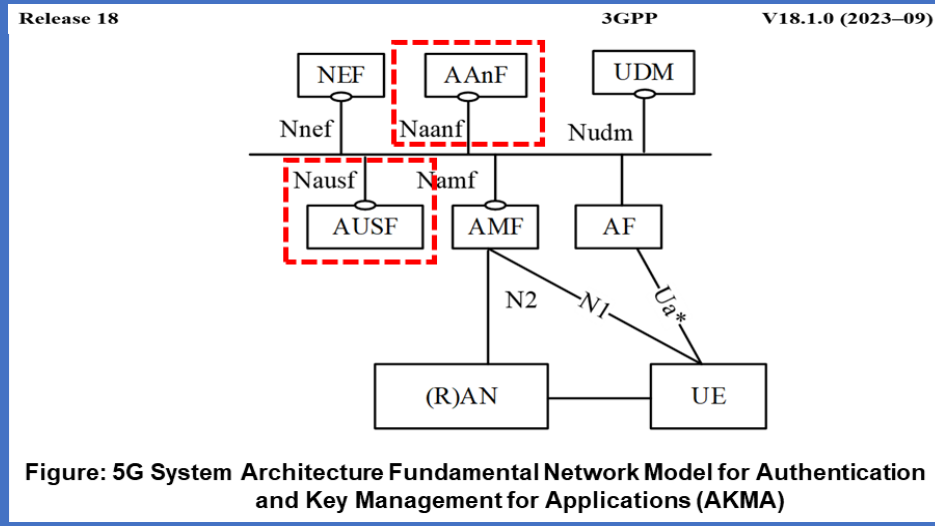


Figure: 5G System Architecture Fundamental Network Model for Authentication and Key Management for Applications (AKMA)

NOTE: The Figure shows the case where *AKMA Anchor Function* (**AAnF**) is deployed as a Stand-alone Function. Deployments can choose to collocate *AAnF* with *AUSF* or with *NEF* according to Operators' deployment Scenarios.

2. 5G System Architecture “Authentication and Key Management for Applications" Capability - 5

AKMA Key Hierarchy

The Key Hierarchy includes the following keys:
- K_{AUSF},
- K_{AKMA},
- K_{AF}.

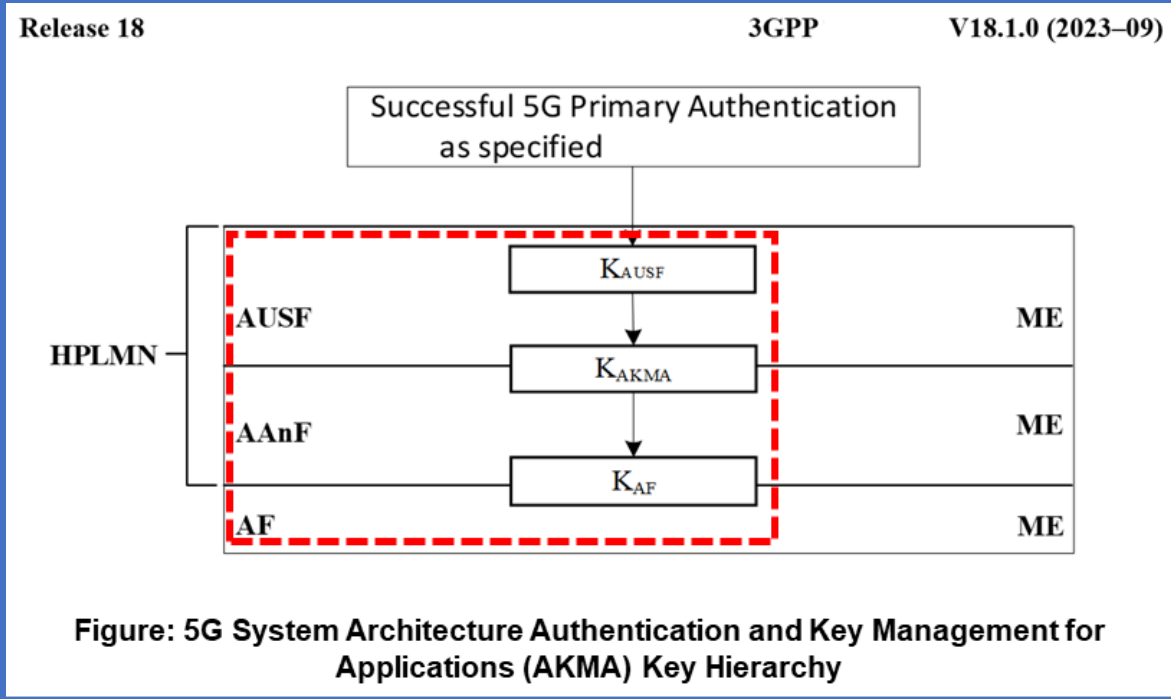


Figure: 5G System Architecture Authentication and Key Management for Applications (AKMA) Key Hierarchy

K_{AUSF} is generated by *AUSF* as specified in 5G System Architecture

Keys for AAnF: K_{AKMA} is a key derived by ME and AUSF from K_{AUSF}.

Keys for AF: K_{AF} is a key derived by ME and AAnF from K_{AKMA}.

K_{AKMA} and K_{AF} are derived according to the procedures specified.

AKMA Key Lifetimes

The K_{AKMA} and A-KID are valid until the next successful Primary Authentication is performed (implicit lifetime), in which case the *K_{AKMA} and A-KID are replaced.*

AKMA Application Keys K_{AF} shall use explicit lifetimes based on the Operator's Policy.

The lifetime of *K_{AF}* shall be sent by the *AAnF* as described. In case that *a new AKMA Anchor Key K_{AKMA}* is established, the *AKMA Application Key K_{AF} can continue to be used* for the duration of the current Application Session or until its lifetime expires, whichever comes first.

When the *K_{AF} lifetime expires, a new AKMA Application Key is established based on the current AKMA Anchor Key K_{AKMA}.*

NOTE: When the K_{AF} lifetime expires and the K_{AKMA} has not changed in AAnF, the AKMA Application Key which is established based on the current AKMA Anchor Key K_{AKMA} is not a new one.

In 4G, 3GPP defined the *Generic Bootstrapping Architecture* (**GBA**) to bootstrap keys to secure the Application between the *UE* and an Application Server (*AS),* after *Authenticating the UE using **LTE-AKA Protocol**.*

A similar approach is taken in AKMA, but **because of the *5G Core Service-based Architecture (SBA*), the AKMA Architecture becomes entirely different compared to 4G LTE EPS Generic Bootstrapping Architecture (GBA).**

A New Logical Entity, called the *AKMA Anchor Function* (**AAnF**) has been introduced to support the *AKMA feature.*

From the ***KAUSF, the AUSF*** generates *AKMA key KAKMA* and sends it to the *AKMA Anchor function AAnF.*

When UE tries to connect to an *Application Server (AS)*, the UE provides the **AKMA** *Temporary Identifier* to the *Application Server (**AS**)*.

Based on this Temporary Identifier, the *Application Server (**AS**)* interacts with ***the AAnF*** to receive the *Specific Session Key KAF and UE Identifier.*

The AF can use Received Session Key KAF or further derive the Keys based on the Session Key KAF to secure the Communication between the UE and the Application Server (AS).

Thus, AKMA provides a reliable Framework for Applications to authenticate the UE and secure the Communication between the UE and the Application Server (AS), leveraging the highly secure HPLMN based Primary Authentication.

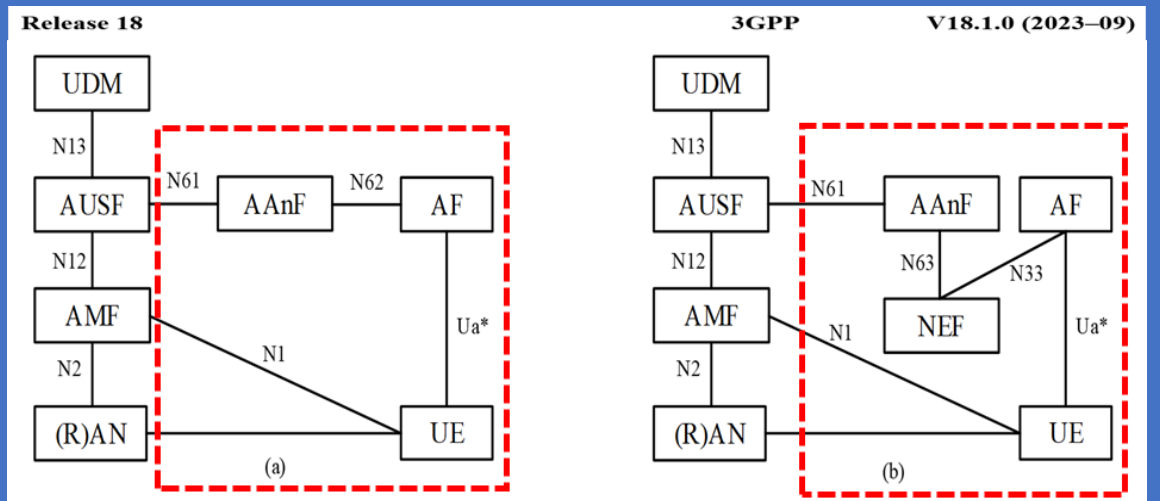


Figure: 5G System Architecture Fundamental Network Model for Authentication and Key Management for Applications (AKMA) Architecture in Reference Point representation for (a) Internal HPLMN AFs and (b) External AFs

Please note, <u>there is no separate authentication of the UE to support AKMA Functionality</u>. Instead, *AKMA re-uses the 5G Primary Authentication Procedure* for the sake of Implicit Authentication for AKMA Services. The Figure above shows:

(a) where the *Application Function (AF) is within the 5GC and part of the PLMN*, whereas

(b) provides the scenario where Application Function (AF) is outside the 5GC and the Application Function (AF) interacts with AKMA Anchor Function (AAnF) via the *Network Exposure Function (**NEF**)*.

2. 5G System Architecture “Authentication and Key Management for Applications" Capability - 7

The Figure illustrates the 5G System Architecture Security Domains:

- *Network Access Security (I):* the Set of Security Features that enable a UE to authenticate and access services via the Network securely, *including the 3GPP Access and Non-3GPP Access, and in particularly, to protect against attacks on the (radio) interfaces.* In addition, it includes the *Security Context delivery from SN to AN* for the Access Security.

- *Network Domain Security (II):* the Set of Security Features that enable Network Nodes to securely exchange Signalling Data and User Plane (UP) Data.

- *User Domain Security (III):* the Set of Security Features that secure the User Access to ME

- *Application Domain Security (IV):* the Set of Security Features that enable Applications in the *User Domain and in the Provider Domain* to exchange messages securely. Application domain security is out of scope of the present document.

- *SBA domain security (V):* the Set of Security Features that enables *Network Functions (NFs) of the SBA Architecture* to securely communicate within the serving Network Domain and with other Network Domains . Such *Features include Network Function Registration, Discovery, and Authorization Security Aspects, as well as the Protection for the Service-Based Interfaces (SBIs)*.

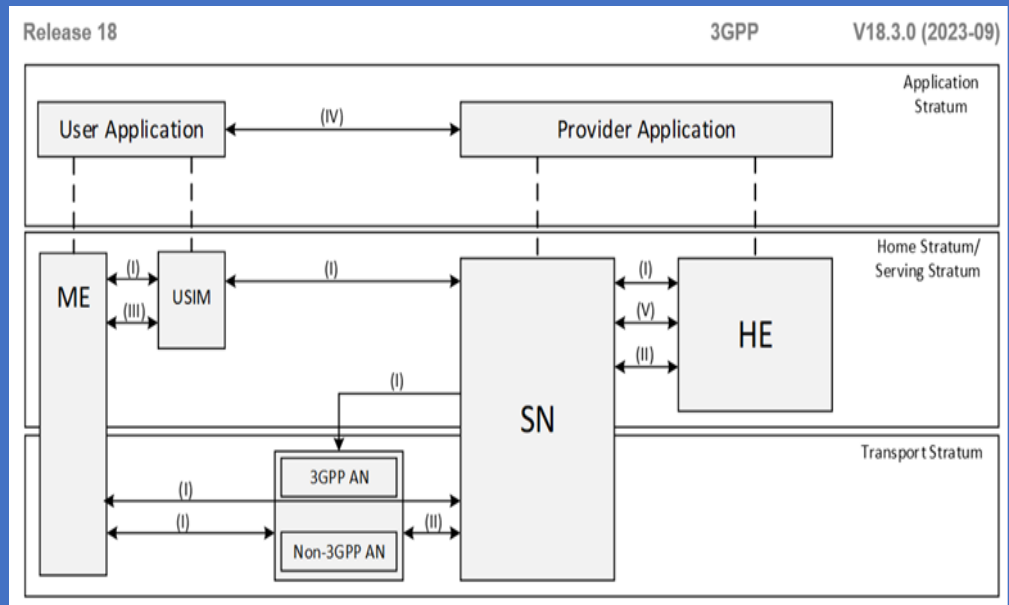


Figure: 5G System Security Domains Architecture Overview

5G SBA Domain Security is a New Security Feature compared to the 4G (the Evolved Packet System) and the Evolved Packet Core (4G EPC), and the Security Procedures performed within the Evolved Packet System (EPS) including the Evolved Packet Core (EPC) and the Evolved UTRAN (E-UTRAN).

- *Visibility and Configurability of Security (VI):* the Set of Features that enable the User to be informed whether a Security Feature is in Operation or not.

NOTE: The Visibility and Configurability of Security is not shown in the Figure.

2. 5G System Architecture “Authentication and Key Management for Applications" Capability - 8

The Figure illustrates the ***5G System Security Architecture*** Key Hierarchy Generation:
Requirements on 5GC and NG-RAN related to keys are described in clause. The following describes the Keys of the Key Hierarchy Generation in a 5GS in detail:
The keys related to Authentication include the following keys: K, CK/IK. In case of EAP-AKA', the keys CK', IK' are derived from CK, IK as specified in clause.
The Key Hierarchy includes the following keys: KAUSF, KSEAF, KAMF, KNASint, KNASenc, KN3IWF, KgNB, KRRCint, KRRCenc, KUPint and KUPenc.

Keys for AUSF in Home Network:

- KAUSF is a key derived by ME and AUSF from CK', IK' in case of EAP-AKA', CK' and IK' is received by AUSF as a part of transformed AV from ARPF; or,
- by ME and ARPF from CK, IK in case of 5G AKA, KAUSF is received by AUSF as a part of the 5G HE AV from ARPF.
- KSEAF is an anchor key derived by ME and AUSF from KAUSF. KSEAF is provided by AUSF to the SEAF in the serving network.

Key for AMF in serving network:

- KAMF is a key derived by ME and SEAF from KSEAF. KAMF is further derived by ME and source AMF when performing horizontal key derivation.

Keys for NAS signalling:

- KNASint is a key derived by ME and AMF from KAMF, which shall only be used for the protection of NAS signalling with a particular integrity algorithm.
- KNASenc is a key derived by ME and AMF from KAMF, which shall only be used for the protection of NAS signalling with a particular encryption algorithm.

Key for NG-RAN:

- KgNB is a key derived by ME and AMF from KAMF. KgNB is further derived by ME and source gNB when performing horizontal or vertical key derivation. The KgNB is used as KeNB between ME and ng-eNB.

Keys for UP traffic:

- KUPenc is a key derived by ME and gNB from KgNB, which shall only be used for the protection of UP traffic with a particular encryption algorithm.
- KUPint is a key derived by ME and gNB from KgNB, which shall only be used for the protection of UP traffic between ME and gNB with a particular integrity algorithm.

Keys for RRC signalling:

- KRRCint is a key derived by ME and gNB from KgNB, which shall only be used for the protection of RRC signalling with a particular integrity algorithm.
- KRRCenc is a key derived by ME and gNB from KgNB, which shall only be used for the protection of RRC signalling with a particular encryption algorithm.

Intermediate keys:

- NH is a key derived by ME and AMF to provide forward security as described.
- KNG-RAN * is a key derived by ME and NG-RAN (i.e., gNB or ng-eNB) when performing a horizontal or vertical key derivation as specified and using a KDF as specified.
- KAMF' is a key that can be derived by ME and AMF when the UE moves from one AMF to another during inter-AMF mobility as specified and using a KDF as specified.

Key for the non-3GPP access:

- KN3IWF is a key derived by ME and AMF from KAMF for the non-3GPP access. KN3IWF is not forwarded between N3IWFs.

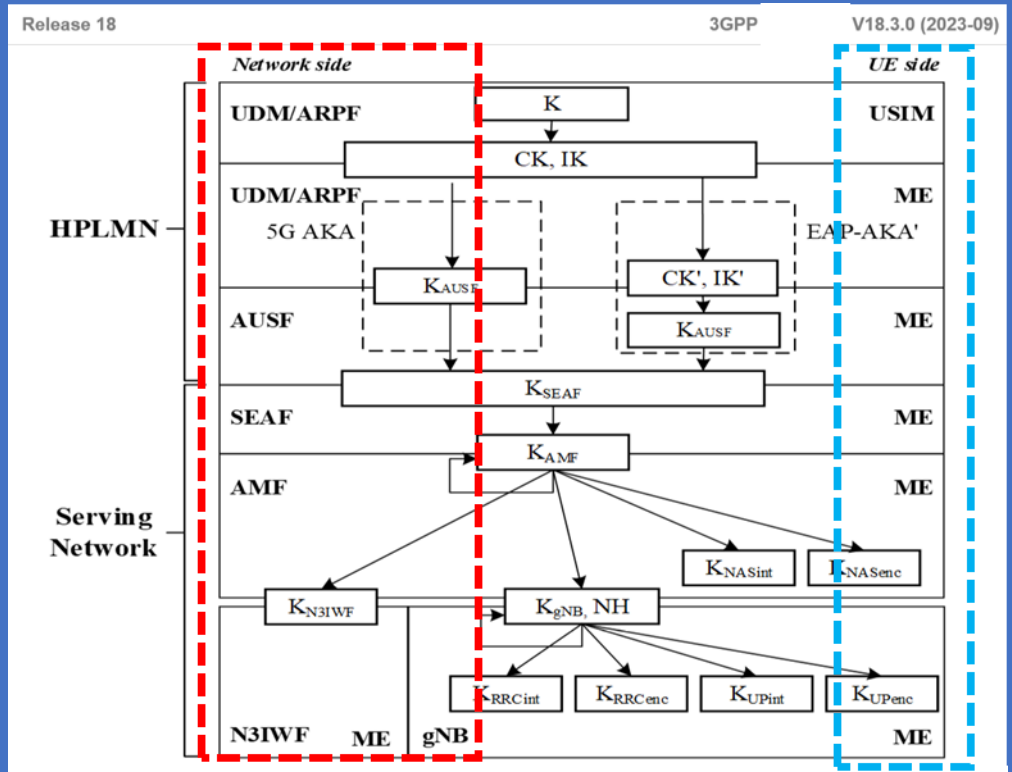


Figure: 5G System Security Architecture Key Hierarchy Generation

NOTE 1: The Key Hierarchy for Stand-alone Non-Public Networks (SNPNs) when an Authentication Method other than 5G AKA or EAP-AKA' is used..

2. 5G System Architecture “Authentication and Key Management for Applications" Capability - 9

The Figure shows the dependencies between the different keys, and how they are derived from the Network Nodes point of view.

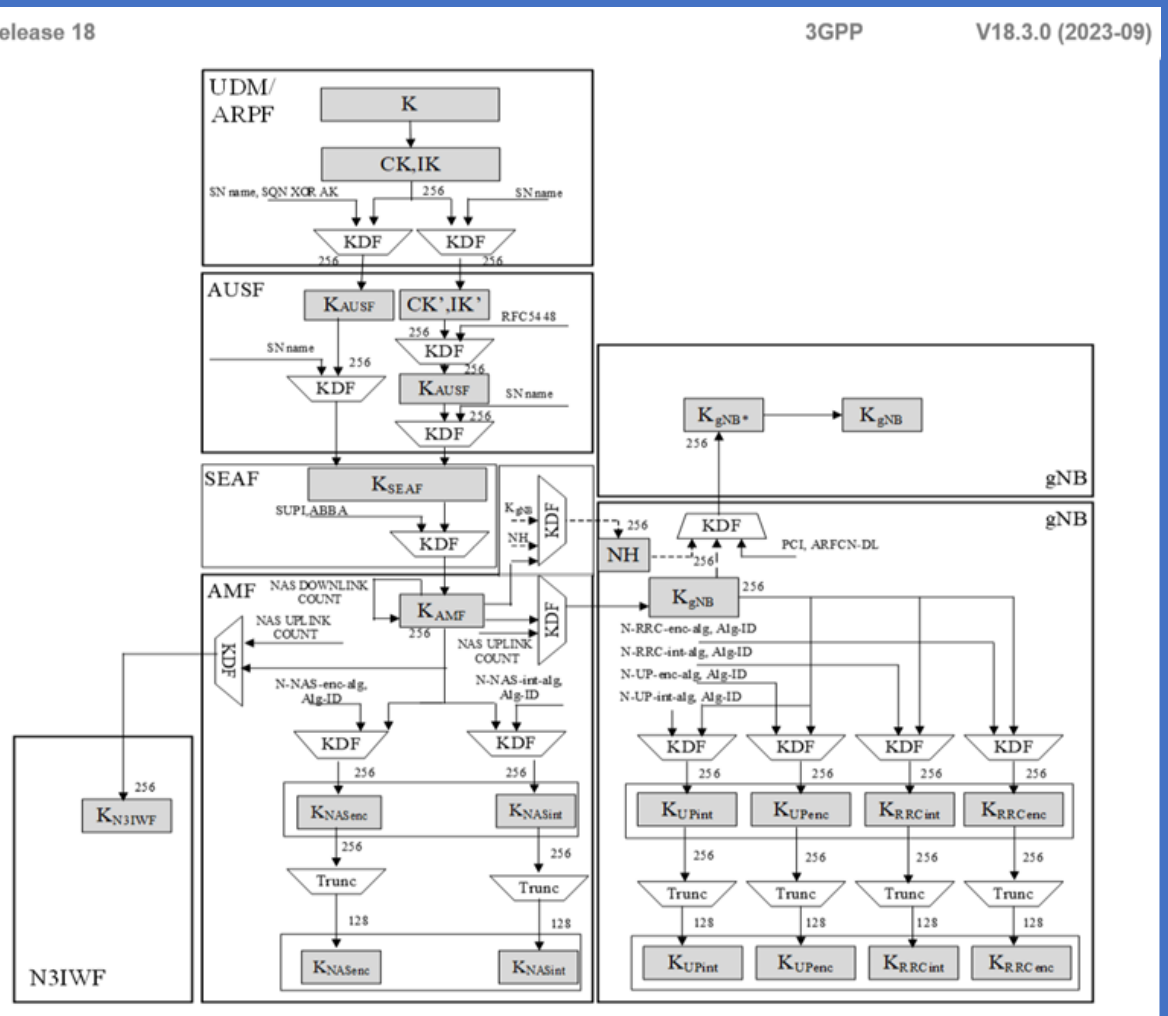


Figure: 5G System Security Architecture Key Distribution and Key Derivation Scheme for 5G for Network Nodes

For every Key in a Network Entity, there is a corresponding Key in the UE. The Figure shows the corresponding relations and derivations as performed in the UE.

Keys in the USIM: The USIM shall store the same long-term key K that is stored in the ARPF. During an authentication and key agreement procedure, the USIM shall generate key material from K that it forwards to the ME. If provisioned by the home operator, the USIM shall store the Home Network Public Key used for concealing the SUPI.

Keys in the ME: The ME shall generate the KAUSF from the CK, IK received from the USIM. The generation of this key material is specific to the authentication method and is specified in.. When 5G AKA is used, the generation of RES* from RES shall be performed by the ME. The UE shall store the latest KAUSF or replace the old KAUSF with the latest KAUSF, after successful completion of the latest primary authentication . If the USIM supports 5G parameters storage, KAUSF shall be stored in the USIM. Otherwise, KAUSF shall be stored in the non-volatile memory of the ME. In case 5G AKA is used as an authentication method, upon receiving the valid NAS Security Mode Command message from the AMF (to take the corresponding partial context derived from the newly generated KAUSF into use), the UE shall consider the performed primary authentication as successful and the UE shall store the newly generated KAUSF as the latest KAUSF or replace the old KAUSF with the latest KAUSF.
In case of any key generating EAP method in the present document (EAP-AKA', EAP-TLS in

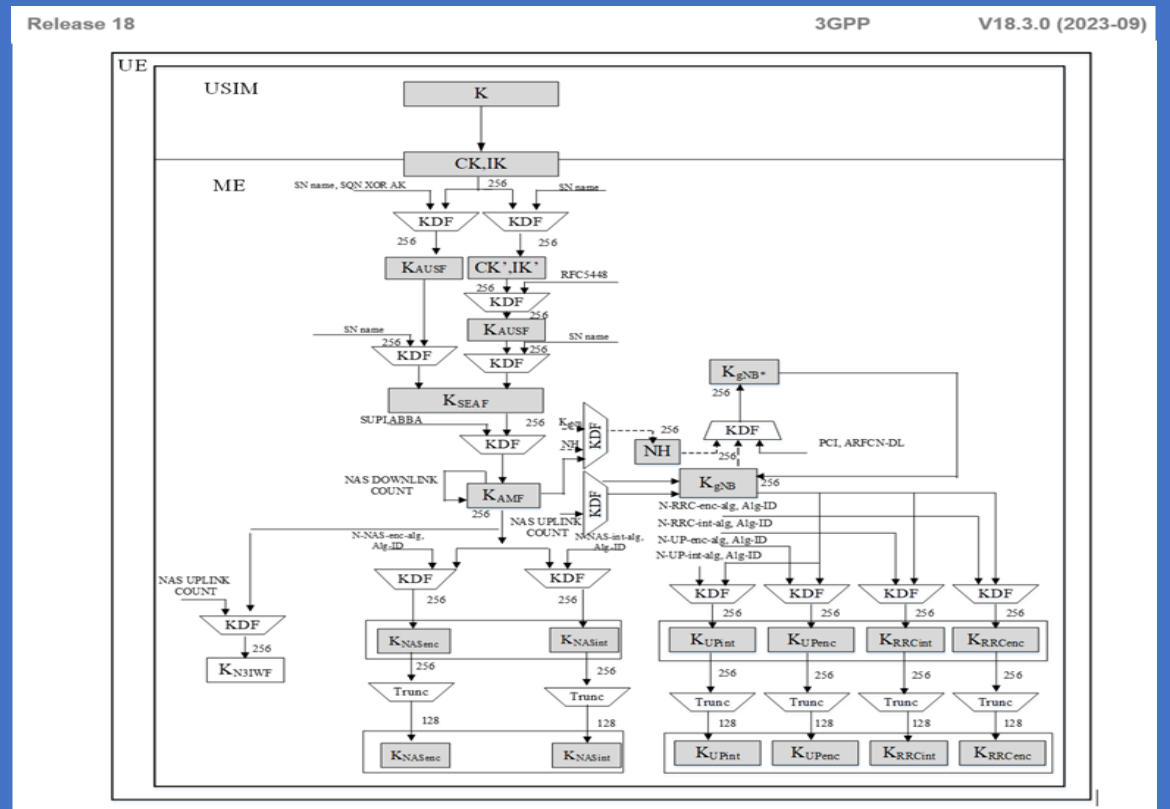


Figure: 5G System Security Architecture Key Distribution and Key Derivation Scheme for 5G for the UE

2. 5GS support for Unified Access Control for UE Access Identities and UE Access Categories - 10

Depending on Operator's Policies, Deployment Scenarios, Subscriber Profiles, and Available Services, different criterion will be used in determining which Access attempt should be allowed or blocked when congestion occurs in the 5G System.

These different criteria for **Access Control** are associated with **Access Identities and Access Categories**. The 5GS will provide a Single Unified Access Control where Operators Control Accesses based on these two (2).

In **Unified Access Control**, each Access attempt is categorized into one (1) or more of the Access Identities and one of the Access Categories.

Based on the Access Control Information applicable for the corresponding Access Identity and Access Category of the access attempt, the **UE performs a test whether the actual access attempt can be made or not.**

The **Unified Access Control** supports extensibility to allow inclusion of *additional Standardized Access Identities and Access Categories* and supports flexibility to allow operators to define Operator-defined Access Categories using their own criterion (e.g. *Network Slicing, Application, and Application Server).*

NOTE: *When a **UE is configured for EAB** (Extended Access Barring) according to 5GS Service Accessibility, the **UE is also configured for Delay Tolerant Service for 5G System**.*

The Unified Access Control Framework shall be applicable both to *UEs accessing the 5G CN* using *E-UTRA* and to UEs accessing the *5G CN using NR.*

The Unified Access Control Framework shall be **applicable to UEs in**
- RRC Idle,
- RRC Inactive, and
- RRC Connected
at the time of initiating a new access attempt (e.g. New Session Request).

Table: 5G System support for Unified Access Control Access Identities

Access Identity number	UE configuration
0	UE is not configured with any parameters from this table
1 (NOTE 1)	UE is configured for Multimedia Priority Service (MPS).
2 (NOTE 2)	UE is configured for Mission Critical Service (MCS).
3	UE for which Disaster Condition applies (note 4)
4-10	Reserved for future use
11 (NOTE 3)	Access Class 11 is configured in the UE.
12 (NOTE 3)	Access Class 12 is configured in the UE.
13 (NOTE 3)	Access Class 13 is configured in the UE.
14 (NOTE 3)	Access Class 14 is configured in the UE.
15 (NOTE 3)	Access Class 15 is configured in the UE.

NOTE 1: Access Identity 1 is used by UEs configured for MPS, in the PLMNs where the configuration is valid. The PLMNs where the configuration is valid are HPLMN, PLMNs equivalent to HPLMN, and visited PLMNs of the home country.
Access Identity 1 is also valid when the UE is explicitly authorized by the network based on specific configured PLMNs inside and outside the home country.
NOTE 2: Access Identity 2 is used by UEs configured for MCS, in the PLMNs where the configuration is valid. The PLMNs where the configuration is valid are HPLMN or PLMNs equivalent to HPLMN and visited PLMNs of the home country. Access Identity 2 is also valid when the UE is explicitly authorized by the network based on specific configured PLMNs inside and outside the home country.
NOTE 3: Access Identities 11 and 15 are valid in Home PLMN only if the EHPLMN list is not present or in any EHPLMN. Access Identities 12, 13 and 14 are valid in Home PLMN and visited PLMNs of home country only. For this purpose, the home country is defined as the country of the MCC part of the IMSI.
NOTE 4: The configuration is valid for PLMNs that indicate to potential Disaster Inbound Roamers that the UEs can access the PLMN. See clause 6.31.

Table: 5G System support for Unified Access Control Access Categories

Access Category number	Conditions related to UE	Type of access attempt
0	All	MO signalling resulting from paging
1 (NOTE 1)	UE is configured for delay tolerant service and subject to access control for Access Category 1, which is judged based on relation of UE's HPLMN and the selected PLMN.	All except for Emergency, or MO exception data
2	All	Emergency
3	All except for the conditions in Access Category 1.	MO signalling on NAS level resulting from other than paging
4	All except for the conditions in Access Category 1.	MMTEL voice (NOTE 3)
5	All except for the conditions in Access Category 1.	MMTEL video
6	All except for the conditions in Access Category 1.	SMS
7	All except for the conditions in Access Category 1.	MO data that do not belong to any other Access Categories (NOTE 4)
8	All except for the conditions in Access Category 1	MO signalling on RRC level resulting from other than paging
9	All except for the conditions in Access Category 1	MO IMS registration related signalling (NOTE 5)
10 (NOTE 6)	All	MO exception data
11-31		Reserved standardized Access Categories
32-63 (NOTE 2)	All	Based on operator classification

NOTE 1: The barring parameter for Access Category 1 is accompanied with information that define whether Access Category applies to UEs within one of the following categories:
a) UEs that are configured for delay tolerant service;
b) UEs that are configured for delay tolerant service and are neither in their HPLMN nor in a PLMN that is equivalent to it;
c) UEs that are configured for delay tolerant service and are neither in the PLMN listed as most preferred PLMN of the country where the UE is roaming in the operator-defined PLMN selector list on the SIM/USIM, nor in their HPLMN nor in a PLMN that is equivalent to their HPLMN.
When a UE is configured for EAB, the UE is also configured for delay tolerant service. In case a UE is configured both for EAB and for EAB override, when upper layer indicates to override Access Category 1, then Access Category 1 is not applicable.
NOTE 2: When there are an Access Category based on operator classification and a standardized Access Category to both of which an access attempt can be categorized, and the standardized Access Category is neither 0 nor 2, the UE applies the Access Category based on operator classification. When there are an Access Category based on operator classification and a standardized Access Category to both of which an access attempt can be categorized, and the standardized Access Category is 0 or 2, the UE applies the standardized Access Category.
NOTE 3: Includes Real-Time Text (RTT).
NOTE 4: Includes IMS Messaging.
NOTE 5: Includes IMS registration related signalling, e.g. IMS initial registration, re-registration, and subscription refresh.
NOTE 6: Applies to access of a NB-IoT-capable UEto a NB-IOT cell connected to 5GC when the UE is authorized to send exception data.

Annex 1. 5G Advanced specified 5G System Capabilities on User Identifiers in 3GPP 5G Advanced Rel-19 - 1

5G System enhancement foresees to cover the preliminary assessed UCs including:
- One (1) or more Users (i.e., Humans) sharing one (1) UE,
- One (1) or more Users (i.e., Devices) behind one (1) GW UE, and
- One (1) or more Users (i.e., Gaming Applications) running on the same UE and each is treated as a different User.

Support for the identification of Non-3GPP Devices that communicate via a GW UE may also enable UCs such as the deployment of a 5G Mobile VPN that is managed by the network.

A 5G Mobile VPN that can provide a secure and reliable connection between an Enterprise's equipment, which includes:

- Non-3GPP Devices and
- UE(s), and
- Authorized UEs that are located off-premises.

Support for associating a User Identifier with traffic of a UE may enable Charging and *Service differentiation by an RG's Home Network Operator for Users whose UE(s) or Non-3GPP Device(s) connect to the 5GC via the RG.*

The User Identity Profile Information is used to authenticate & authorize Accessing Information from the User Profile and *to authenticate and authorize users, including API Exposure of User Identity Functionality (e.g. Exposure of the Content of the User Profile, Exposure of Authorization/Authentication Results, and linking a User Identity with a Subscription).*

TSG SA Meeting #SP-101
11 - 15 September 2023, Bangalore, India

Source: InterDigital Inc.
Title: New Study on Enhancement of Usage of User Identifiers in the 5G System
Document for: Approval
Agenda Item: 6.4.2

3GPP™ Work Item Description

Title: Study on the Enhancement of Usage of User Identifiers in the 5G System

Potential target Release: Rel-19

Impacts

Affects:	UICC apps	ME	AN	CN	Others (specify)
Yes		x		x	
No					
Don't know	x		x		x

Other related Work Items and dependencies

Other related Work /Study Items (if any)		
Unique ID	Title	Nature of relationship
	Study on a Layer for User Centric Identifiers and Authentication	*SA1 study on requirements for User Identifiers*
	User Identities and Authentication	*SA1 normative work on requirements for User Identifiers*
	Study on Personal IoT Networks	*SA1 study on Personal IoT Networks*
	Personal IoT and Residential Networks	*SA1 normative work on Personal IoT Networks; requirements for User Identifiers apply to Personal IoT Networks*
	Study on Personal IoT Networks	*SA2 study on Personal IoT Networks*
	Personal IoT Networks	*SA2 normative work on Personal IoT Networks*

Annex 1. 5G PINs and 5G CPNs (Customer Premises Networks) - 2

5G Personal IoT Networks (PINs) and 5G Customer Premises Networks (CPNs) provide local connectivity between UEs and/or Non-3GPP Devices.

The *5G CPN* via *an eRG*, or *5G PIN Elements (PINEs) via a PIN Element with Gateway Capability (**PEGC**)* can provide *access to 5G Network Services for the UEs and/or Non-3GPP Devices* on the CPN or PIN.

5G CPNs and5G PINs have in common that, in general, they are:
- owned, Installed and/or (at least partially) Configured by a Customer of a Public Network Operator.

A Customer Premises Network (CPN) is a Network located within
- a Premises (e.g. a Residence, Office or Shop).
- via an evolved Residential Gateway (eRG), the CPN provides connectivity to the 5G Network. The eRG can be connected to the 5G Core Network via wireline, wireless, or hybrid access.
- A *Premises Radio Access Station* (**PRAS**) is a Base Station installed in a CPN. Through the PRAS, UEs can get Access to the CPN and/or 5G Network Services.

The **PRAS** can be configured to use
- Licensed,
- Unlicensed, or
- Both Frequency bands.

Connectivity between the **eRG** and the **UE**, **non-3GPP Device**, or **PRAS** can use any suitable **Non-3GPP Technology** (e.g. **Ethernet, optical, WLAN).**

A Personal IoT Network (PIN) consists of **PIN Elements (PINEs)** that communicate using PIN
- "Direct Connection" or
- "Direct Network Connection

and is managed locally using a *PIN Element (PINE) with Management Capability (PEMC).*

Examples of 5G PINs include Networks of Wearables and Smart Home / Smart Office Equipment.

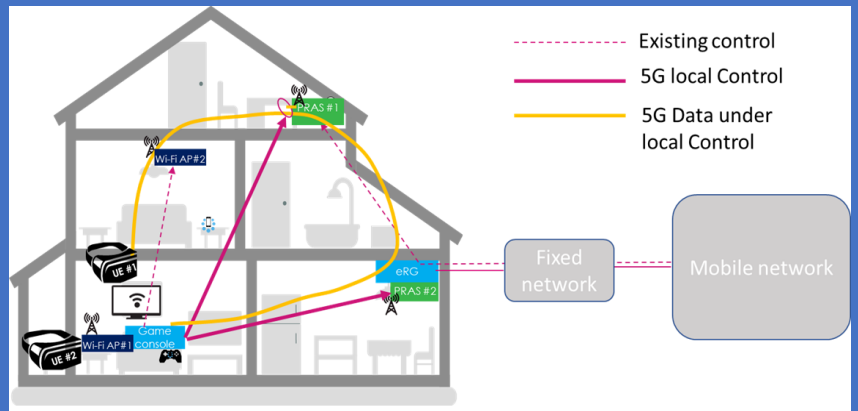


Figure: 5G Local Control of Premise Radio Access Stations (PRASs) for UE to access CPN Device

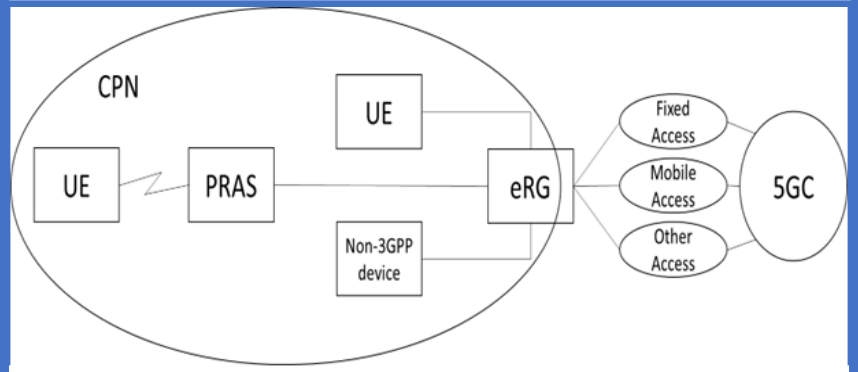
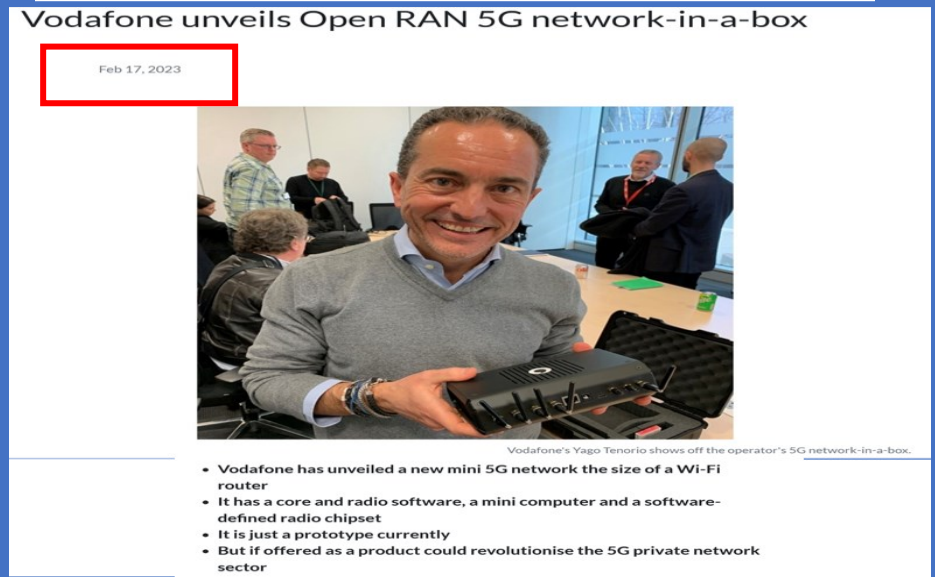


Figure: Customer Premises Network (CPN) connected to 5GC



Personal IoT Network: A configured and managed group of PIN Element that are able to communicate each other directly or via PIN Elements with Gateway Capability (PEGC), communicate with 5G network via at least one PEGC, and managed by at least one PIN Element with Management Capability (PEMC).

PIN Element (PINE): A UE or Non-3GPP device that can communicate within a PIN (via PIN "direct" connection, via PEGC, or via PEGC and 5GC), or outside the PIN via a PEGC and 5GC.

PIN Element with Gateway Capability: A PIN Element with the ability to provide connectivity to & from the 5G Network for other PIN Elements, or to provide "relay" for the communication between PIN Elements.

PIN Element with Management Capability: A PIN Element with capability to manage the PIN.

NOTE: A PIN Element can have both PIN Management Capability and Gateway Capability.

PINE-to-PINE communication: communication between two PINEs which may use PINE-to-PINE direct communication or PINE-to-PINE indirect connection.

PINE-to-PINE direct connection: the connection between two PIN Elements without PEGC, any 3GPP RAN or core network entity in the middle.

PINE-to-PINE indirect connection: the connection between two PIN Elements via PEGC or via UPF.

PINE-to-PINE routing: the traffic is routed by a PEGC between two PINEs, the two PINEs direct connect with the PEGC via non-3GPP access.

PINE-to-Network routing: the traffic is routed by a PEGC between PINE and 5GS, the PINE direct connects with the PEGC via non-3GPP access separately.

Network local switch for PIN: the traffic is routed by UPF(s) between two PINEs, the two PINEs direct connect with two PEGCs via non-3GPP access separately.

Abbreviations

PIN	Personal IoT Networks
PINE	PIN Element
PEGC	PIN Elements with Gateway Capability
PEMC	PIN Elements with Management Capability
P2P	PINE-to-PINE
P2N	PINE-to-Network
NLSP	Network Local Switch for PIN

Note 1: The AF relies on PIN signaling between the PINE/PEGC/PEMC and the PIN AF, which is transferred via UP transparently to the 5G System, to determine the need for a QoS modification.

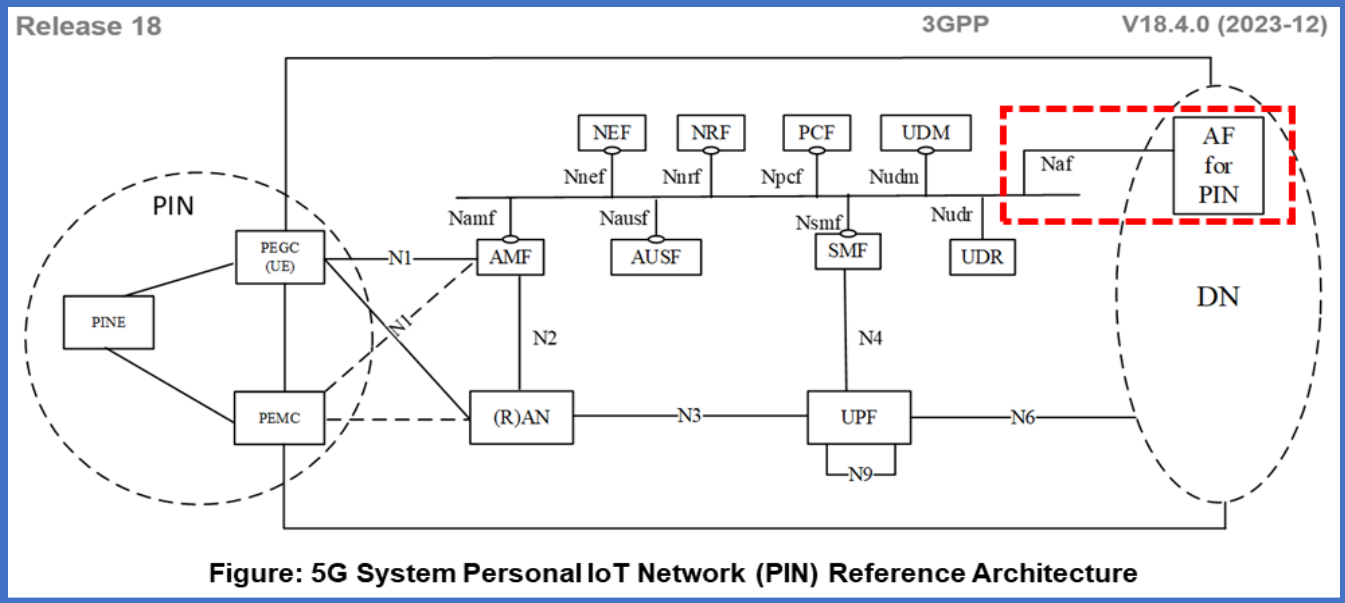


Figure: 5G System Personal IoT Network (PIN) Reference Architecture

Annex 1. 5G PINs (Personal IoT Networks) - Network & Application Layers enhancements - 4

5G **Personal IoT Network (PIN)** in **5G System Core Network (CN)** consists of:

- 1 (one) or more Devices providing Gateway/Routing Functionality known as **the PIN Element with Gateway Capability (PEGC)**, and

- 1 (one) or more Devices providing PIN Management Functionality known as the **PIN Element with Management Capability (PEMC)** to manage the Personal IoT Network; and

- Device(s) called the PIN Elements (PINEs).
  A PINE can be a non-3GPP Device

The 5G PIN Service can also have an AF for PIN. The PIN AF can be deployed by MNO or by an Authorized Third (3rd) Party.

When the 5G PIN AF is deployed by 3rd Party, the interworking with 5GS is performed via the 5GS CN NEF.

With 5GS PIN - DN Communication, the PEMC and PEGC communicates with the 5G PIN Application Server (AS) at the Application Layer over the User Plane UP).

The 5G PIN ***PEGC and PEMC*** can communicate with each other via:
- 5GS **PIN "Direct Communication** using 3GPP Access (e.g. PC5) or Non-3GPP Access (e.g. Wi-Fi, BT) or via
- **5GS PIN "Indirect Communication" using a PDU Session in the 5GS.**

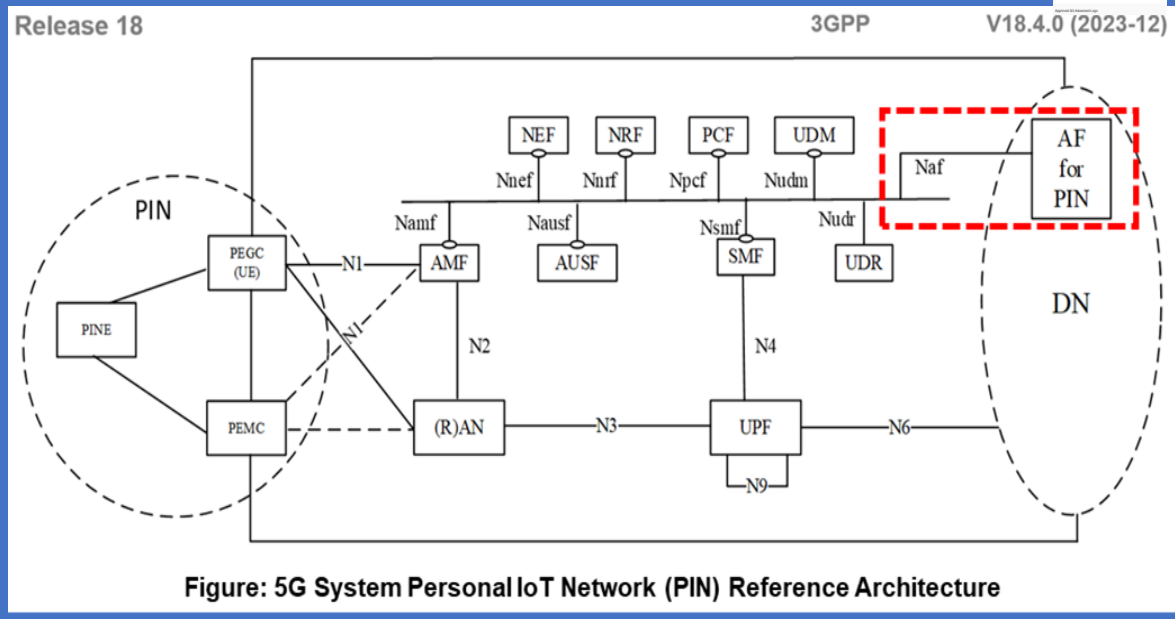


Figure: 5G System Personal IoT Network (PIN) Reference Architecture

The PIN can also have a PIN Application Server (AS) that includes an AF (Application Function) functionality.

The AF can be deployed by Mobile Operator or by an Authorized Third (3rd) Party.

When the AF is deployed by 3rd Party, the interworking with 5GS is performed via the NEF.

The PEMC and PEGC communicates with the PIN Application Server (AS) at the Application Layer over the User Plane. The PEGC and PEMC can communicate with each other via "Direct" Communication

Only a 3GPP UE can act as PEGC and/or PEMC.

5G System Session Management and Traffic Routing for 5G PIN

The 5G System Architecture specified for PINs:

- 5GS Session Management Principles

- 5GS QoS Model

- 5GS User Plane (UP) Management

are **applicable to 5G PIN-DN Communication and PIN-Indirect Communication.**

With the support of the 5G PIN PEGC registered to 5G Network, the PIN Elements (PINEs) have Access to the 5G Network Services and communicate with other PINEs within the 5G PIN or with the DN via 5G CN.

A 5G PIN PEGC is capable to support multiple PINs. For each 5G PIN, a dedicated DNN/S-NSSAI shall be configured.

For a 5G PIN PEGC registered in the 5GS, the 5GS supports the provisioning of URSP rules that include a PIN ID as Traffic Descriptor. URSP rules with a PIN ID in the Traffic Descriptor are sent to the UE based on the information provided from an 5G PIN AF as specified in the 5G System Architecture Procedures and 5G System Architecture Policy and Charging Control delivery.

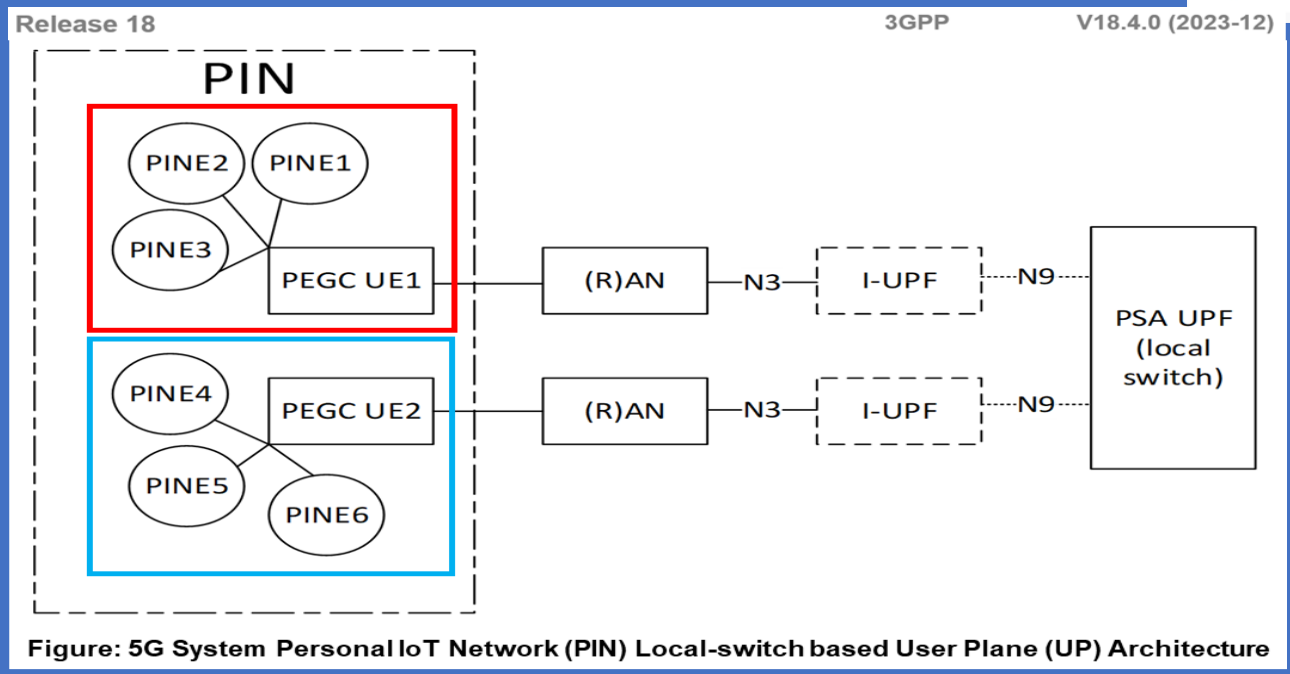


Figure: 5G System Personal IoT Network (PIN) Local-switch based User Plane (UP) Architecture

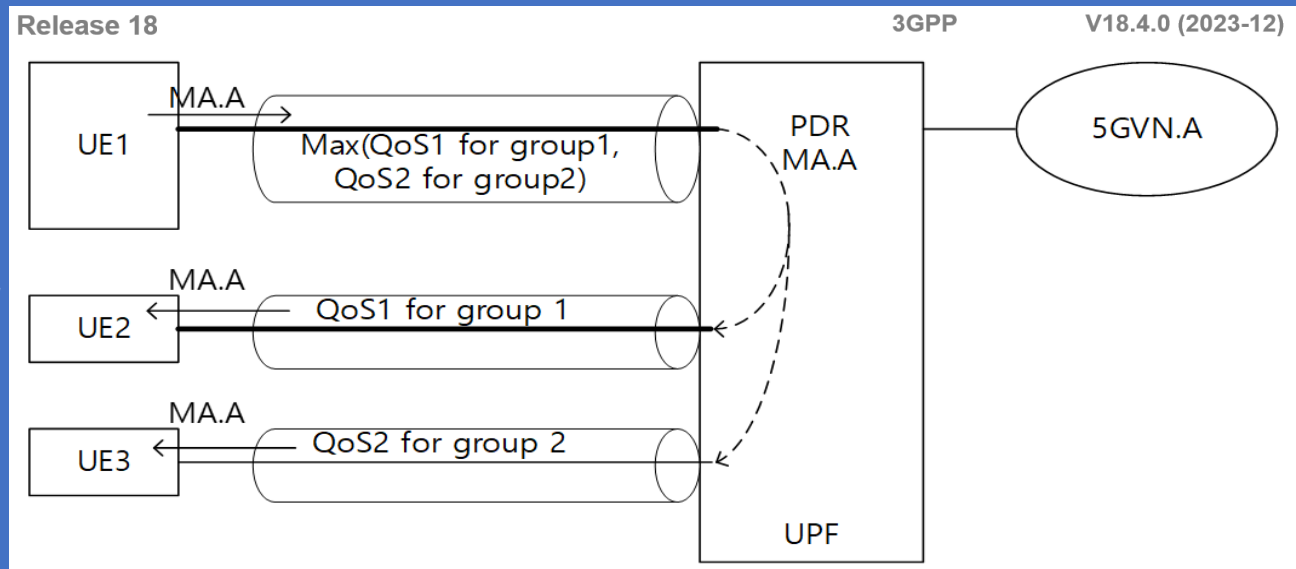


Figure: 5G System Architecture PDU Session targeting a predefined Group formed of multiple Sub-Groups

Annex 2: 5G Ambient IoT - 1

A new kind of IoT Service for the Vertical industries will be enabled by combining *Ambient-power enabled IoT with Cellular (5G) Networks*.

In 5G, various IoT Technologies, as eMTC, NB-IoT, & RedCap have been developed to fulfil the increasing demand from Verticals.

These IoT Technologies *aimed to achieved Low Cost, Low Power & Massive Connections to meet Requirements of many Applications*.

The deployment of huge number of IoT Devices, has pushed up ***the Maintenance Costs, including both Labor & Battery Costs.***

However, there are UCs & Applications that can benefit from an ***IoT Technology that requires Less Power & has Lower Cost than previous IoT Technologies.***

Improvements can be made where *Maintenance-Free Devices are required (e.g. where the Devices are inaccessible & it is not possible to replace the Device Battery) or for Devices in extreme Environmental conditions. Ultra-low Complexity, very Small Device Size/Form factor (e.g. Thickness of mm), Longer Life Cycle, etc. are required for some UCs.*

Ambient IoT is a Technology to fulfil these Market Requirements.

Ambient IoT Device is an *IoT Device powered by Energy harvesting*, being either Battery-less or with limited Energy Storage Capability (e.g. using a Capacitor). The Energy is provided through the Harvesting of Radio Waves, Light, Motion, Heat, or any other Power Source that could be seen suitable. *An Ambient IoT Device has Low Complexity, Small Size & Lower Capabilities & Lower Power Consumption than previously defined 3GPP IoT Devices (e.g. NB-IoT/eMTC Devices). Ambient IoT Devices can be Maintenance Free & can have Long Life Span (e.g. more than 10 years).*

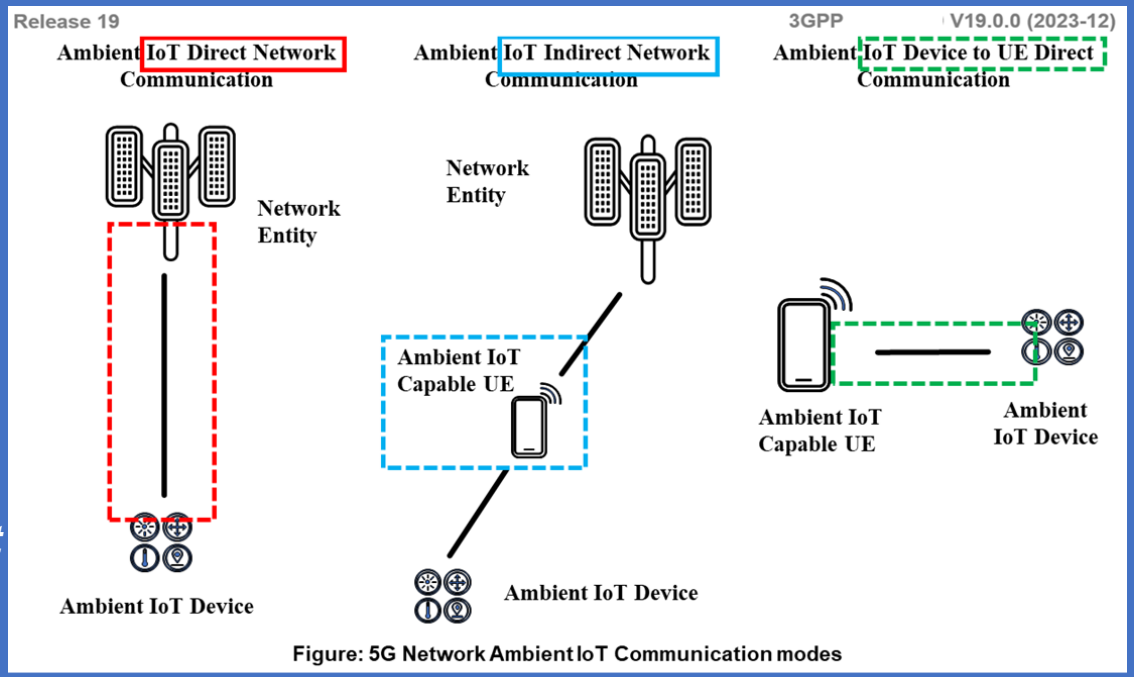


Figure: 5G Network Ambient IoT Communication modes

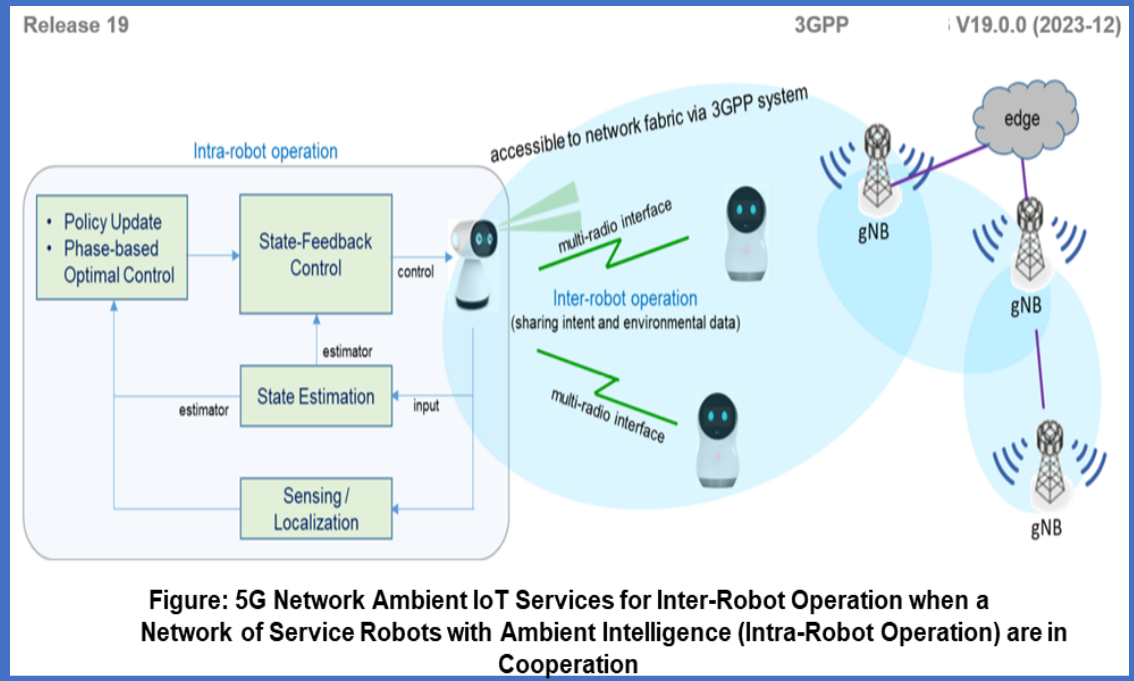


Figure: 5G Network Ambient IoT Services for Inter-Robot Operation when a Network of Service Robots with Ambient Intelligence (Intra-Robot Operation) are in Cooperation

Annex 2: 5G Ambient IoT - 2 5G IoT Communication Modes - 2

Ambient IoT devices are expected to be able to communicate with the 5G Network and/or Ambient IoT capable UE using the one (1) or more of the following Communication modes:

A) Ambient IoT Direct Network Communication:

Communication between the Ambient IoT device & 5G network with no UE conveying information between the Ambient IoT Device & the 5G network.

B) Ambient IoT Indirect Network Communication:

Communication between the Ambient IoT Device & the 5G Network where there is an Ambient IoT capable UE helping in conveying Information between the Ambient IoT Device & the 5G Network.

C) Ambient IoT Device to UE Direct Communication:

Communication between an Ambient IoT Device & an Ambient IoT capable UE with no Network Entity in the middle.

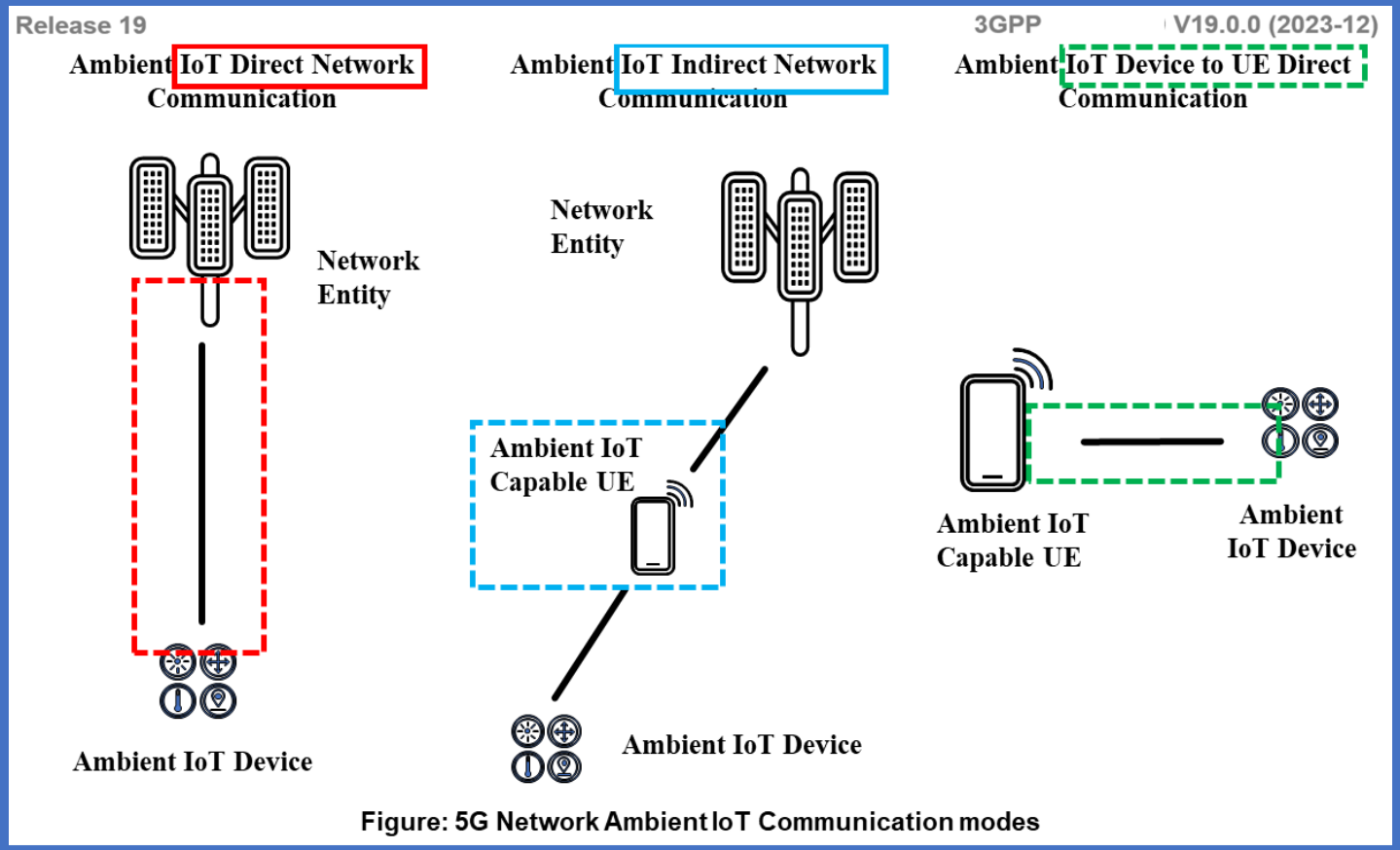


Figure: 5G Network Ambient IoT Communication modes

Ambient IoT Device is an IoT Device powered by energy harvesting, being either:

A) Battery-less or with

B) Limited Energy Storage Capability (e.g. using a Capacitor) and the energy is provided through the harvesting of Radio Waves, Light, Motion, Heat, or any other Power Source that could be seen suitable.

C) Low Complexity, Small Size & lower Capabilities & lower Power Consumption than previously defined 3GPP IoT Devices (e.g. NB-IoT/eMTC Devices)

D) Maintenance Free & can have long *Life Span, e.g. more than 10 years*

Annex 3: 5G Advanced System Factory of the Future (FF) Application Layer Architecture (FFAPP)- 1

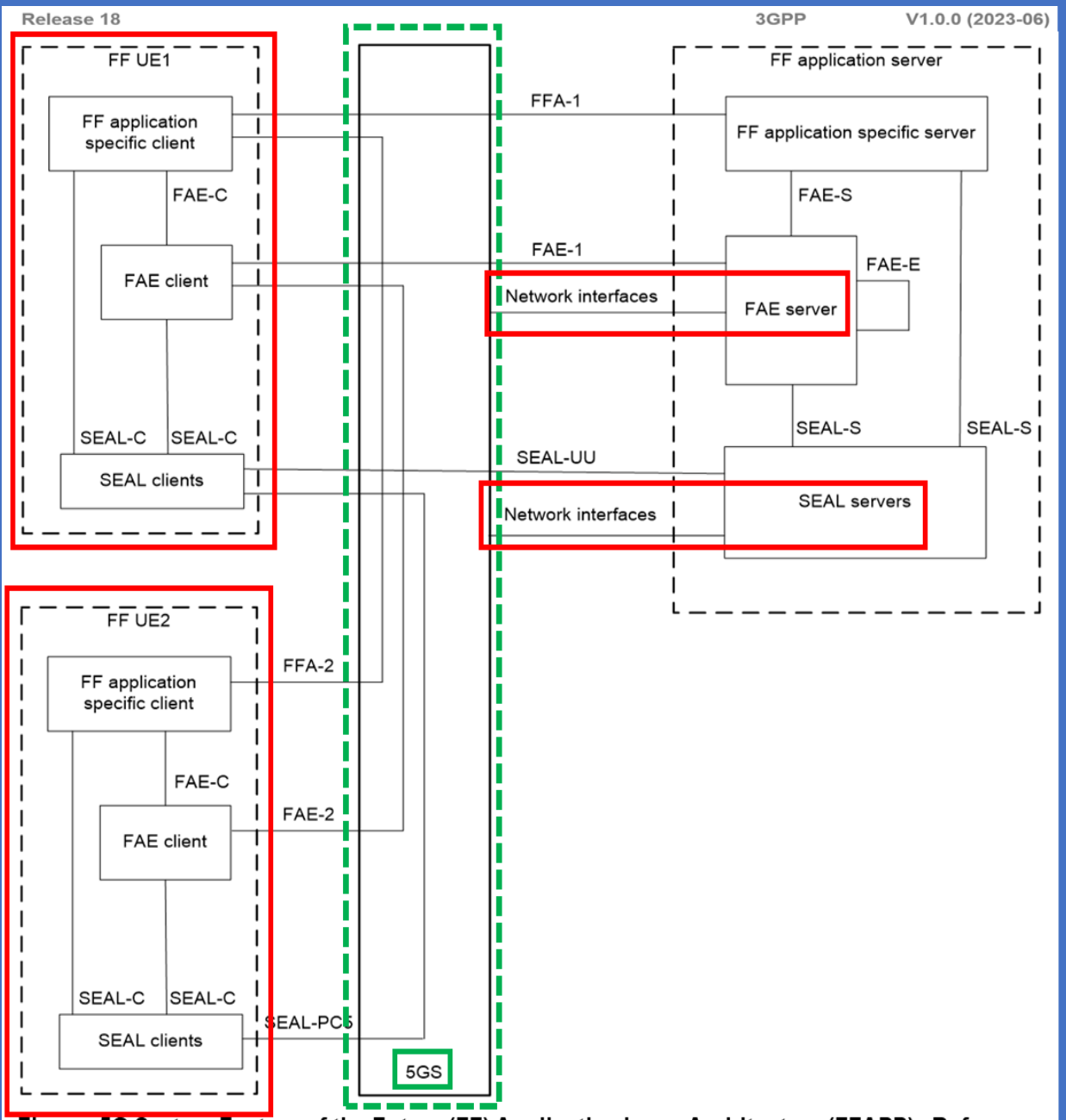


Figure: 5G System Factory of the Future (FF) Application Layer Architecture (FFAPP) - Reference Point representation

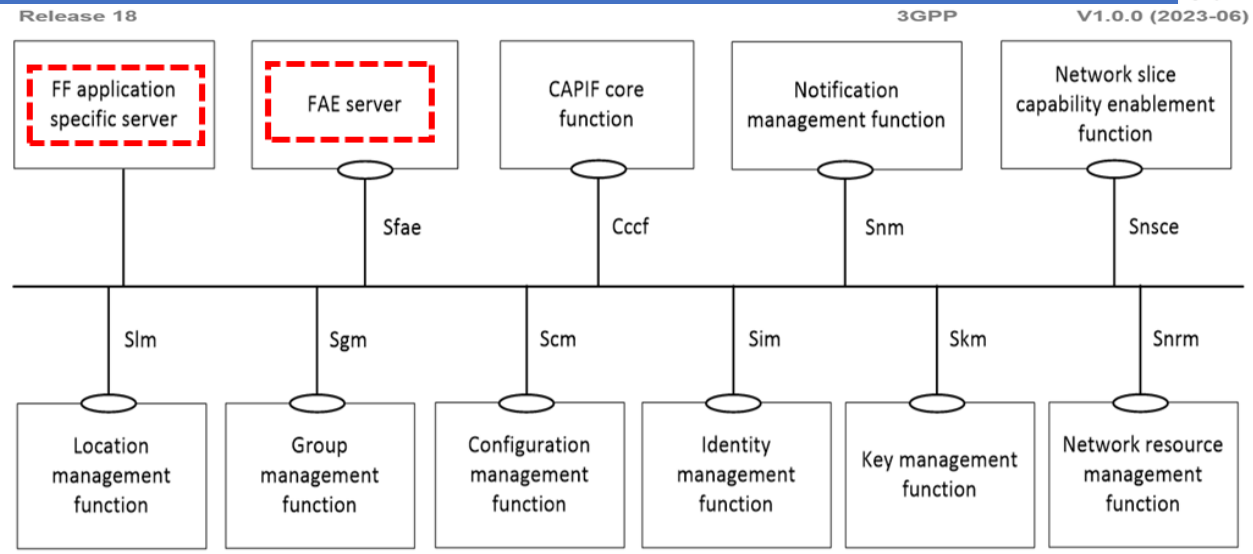


Figure: 5G System Factory of the Future (FF) Application Layer Architecture - Service-based Representation

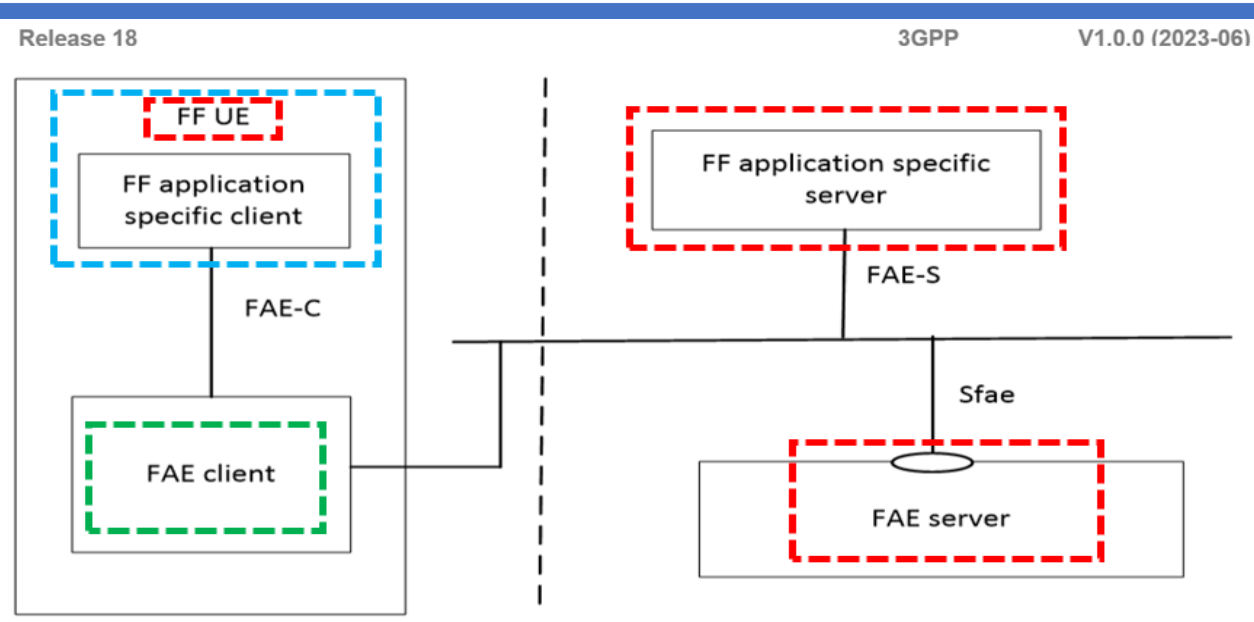


Figure: 5G System Factory of the Future (FF) Architecture Application Layer Reference Point Representation

The ***Distributed Deployment is where Multiple FF Application Enabler (FAE) and Service Enabler Application Layer (FAE+SEAL) Servers*** are deployed either in the:

- Factory of the Future (FF) Operator Domain or in the

- PLMN Operator Domain.

The Distributed Deployment of the ***FAE*** (*FF Application Enabler*) + ***SEAL*** (*Service Enabler Application Layer*) ***Servers*** provide
- Geographical Coverage or
- Support Multiple PLMN Operator Domains in a Geographical Location.

The FAE+SEAL Servers interconnect via FAE-E+SEAL-E and the FAE-S+SEAL-S Reference Points are used for interaction between FF Application Specific Server and the FAE+SEAL Server.

The Figure illustrates the Deployment of FAE+SEAL Servers in Multiple PLMN Operator Domain and provide FAE+SEAL Capabilities to the FF Application Specific Server deployed in the FF Operator domain.

The FF Application Specific Server connects via FAE-S+SEAL-S to the FAE+SEAL Servers.

The Figure illustrates the Deployment of *Multiple FAE+SEAL Servers* deployed in Multiple PLMN Operator Domains. The FF Application Specific Server connects via OP1 FAE-S+SEAL-S to the OP2 FAE+SEAL Server.

The interconnection between FAE+SEAL Servers are via FAE-E+SEAL-E and support the FF Applications for the FF UEs connected to the FAE+SEAL Servers in Multiple PLMN Operator Domains.

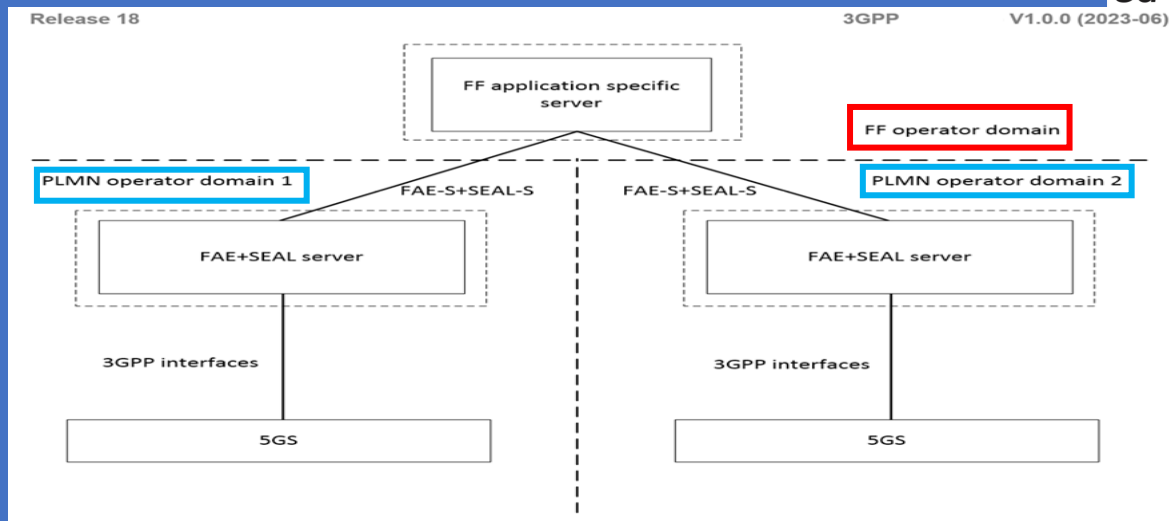


Figure: 5G System Factory of the Future (FF) Application Layer Architecture (FFAPP) deployment of FAE+SEAL Servers in Multiple PLMN Operator Domain without Interconnection between FAE+SEAL Servers

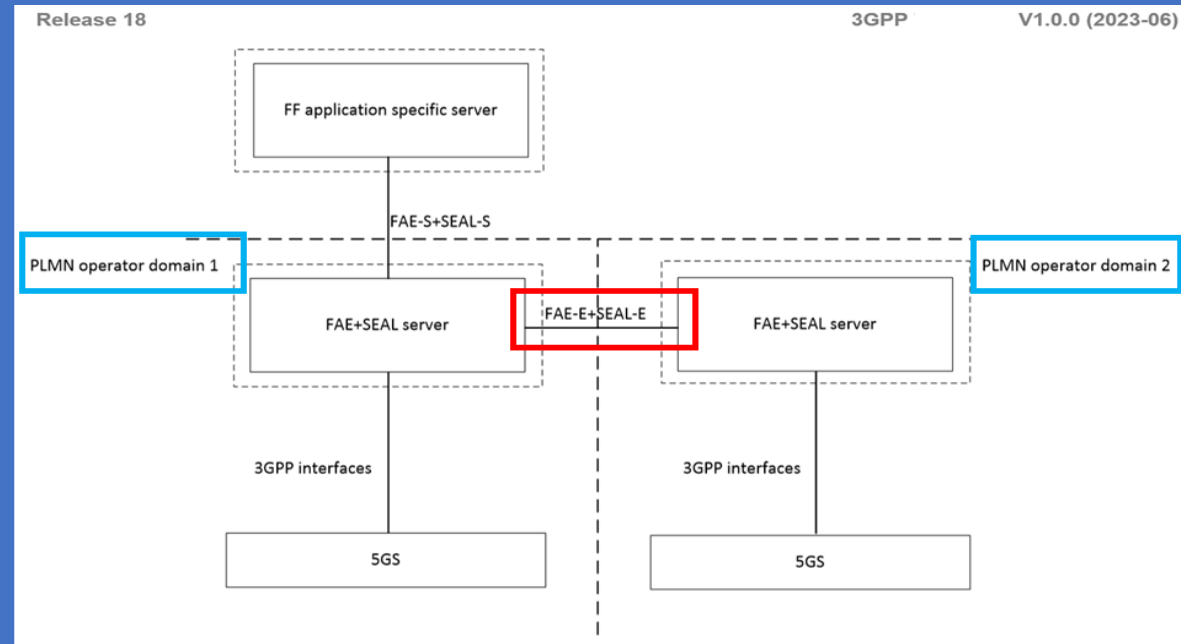


Figure: 5G System Factory of the Future (FF) Application Layer Architecture (FFAPP) deployment of FAE+SEAL Servers in Multiple PLMN Operator Domain with Interconnection between FAE+SEAL Servers

Annex 3: 5G System Factories of the Future (FF) Use Cases Service Requirements for Cyber-Physical Control Applications in Vertical Domains - 3

The Manufacturing Industry is currently subject to a Fundamental Change, which is often referred to as the "Fourth (4th) Industrial Revolution" or simply "Industry 4.0".

The Main Goals of Industry 4.0 are, among others, the improvement of Flexibility, Versatility, Resource Efficiency, Cost Efficiency, Worker Support, and Quality of Industrial Production and Logistics. These Improvements are important for addressing the needs of increasingly volatile and Globalized Markets.

A major Enabler for all this, is Cyber-Physical Production Systems, that are based on a Ubiquitous and Powerful Connectivity, Communication, and Computing Infrastructure.

The Infrastructure interconnects People, Machines, Products, and all kinds of other Devices in a flexible, secure and consistent manner.

Several different Application Areas can be distinguished:

Release 19 3GPP V19.1.0 (2023-09)

Table: 5G System Factories of the Future selected Use Cases mapping to Cyber-Physical Control Application areas (rows) in Vertical Domains

	Motion control	Control-to-control	Mobile control panels with safety	Mobile robots	Remote access and maintenance	Augmented reality	Closed-loop process control	Process monitoring	Plant asset management
Factory automation	X	X		X					
Process automation				X			X	X	X
HMIs and Production IT			X			X			
Logistics and warehousing		X		X					X
Monitoring and maintenance					X				

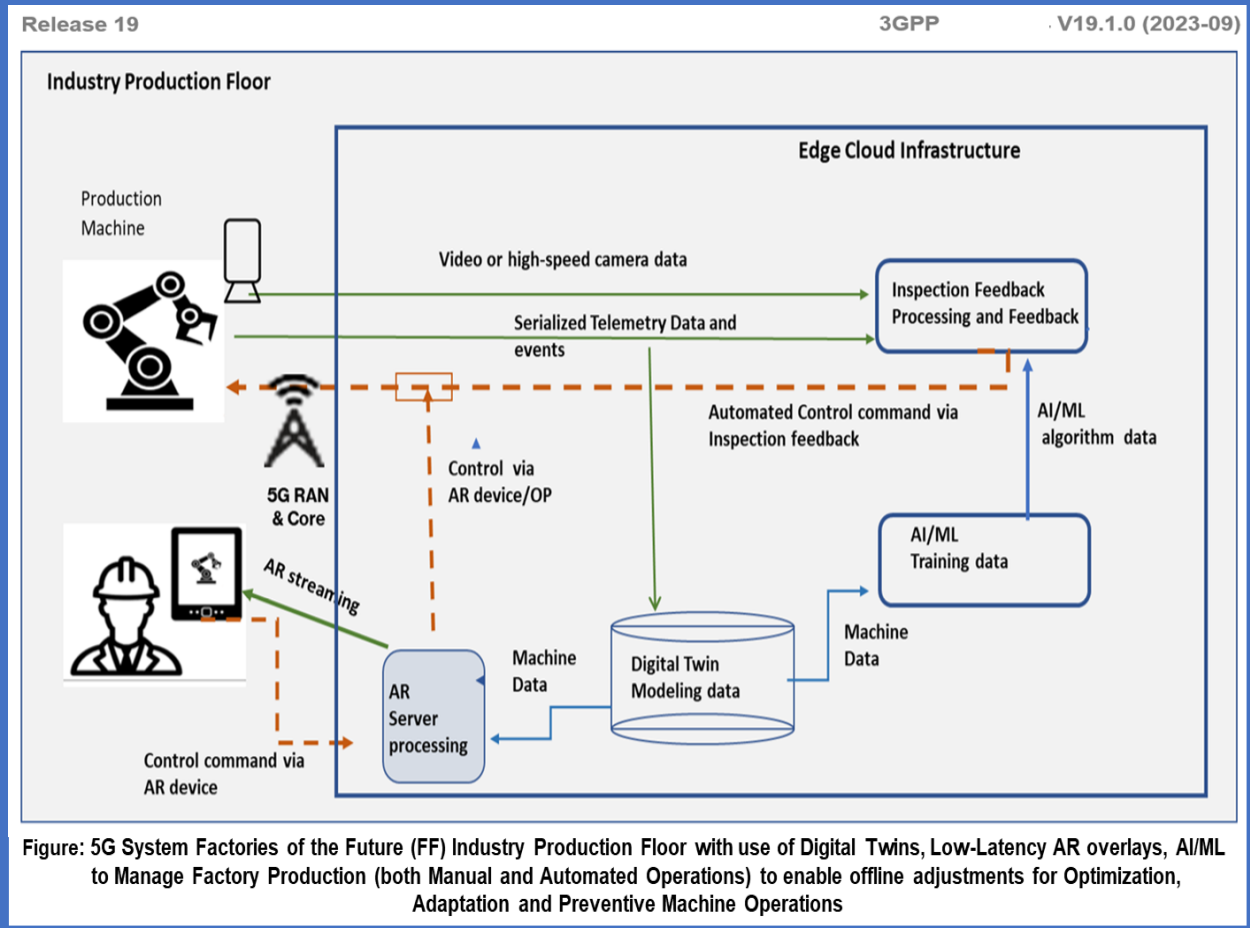


Figure: 5G System Factories of the Future (FF) Industry Production Floor with use of Digital Twins, Low-Latency AR overlays, AI/ML to Manage Factory Production (both Manual and Automated Operations) to enable offline adjustments for Optimization, Adaptation and Preventive Machine Operations

3GPP RAN Rel-16 progress and Rel-17 potential work areas

July 18, 2019

https://www.3gpp.org/news-events/2058-ran-rel-16-progress-and-rel-17-potential-work-areas

Slide 7

Release 16 progressing towards completion

- 5G V2X
  - Targeting advanced use cases beyond LTE V2X
- Industrial IoT and URLLC enhancements
  - Adding 5G NR capabilities for full wired Ethernet replacement in factories: Time Sensitive networking, etc... with high reliability
- 5G NR operation in unlicensed bands
  - Includes both Licensed Assisted Access (LAA), as well as Standalone Unlicensed operation
- System improvements and enhancements
  - Positioning
  - MIMO enhancements
  - Power Consumption improvements

 7

Annex 3. Year 2023: 5G System Factory of the Future Service Requirements for Cyber-Physical Control Applications in Vertical Domains *Wired Links replaced with Wireless Links with Use Cases (Ucs) Traffic (Periodic & A-Periodic) Service Requirements - 5*

In a "traditional" Factory, the Production Environment is "fixed". Machines that are co-operating are connected via cable (***wireline***), typically using an Industrial Ethernet Technology like PROFINET. In order ***to increase flexibility in the Production set-up, the Wired Links are replaced with Wireless Links.***

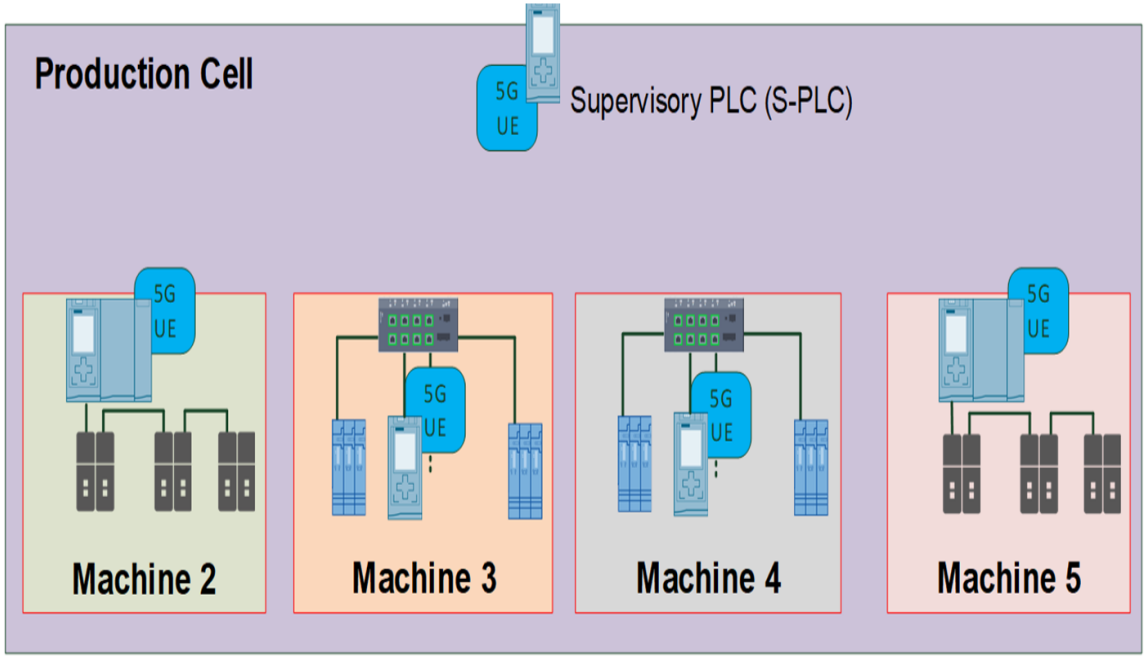


Figure: 5G System Factory of the Future (FF) Service Requirements for Cyber-Physical Control Applications in Vertical Domains example of Four (4) Cooperating Machines with Wireless Connection based on Time-Sensitive Networking (TSN) Profile for Industrial Automation

Table: 5G System Factories of the Future selected Use Cases Traffic (Periodic & A-Periodic) Service Performance Requirements for Wired to Wireless Link Replacement

Use case #	Characteristic parameter			Influence quantity					
	Communication service availability: target value [%]	Communication service reliability: mean time between failures	End-to-end latency: maximum	Data rate [Mbit/s]	Transfer interval	Survival time	UE speed	# of UEs	Service area (note 1)
1 (periodic traffic)	99.999 9 to 99.999 999	~ 10 years	< transfer interval value	50	≤ 1 ms	3 x transfer interval	stationary	2 to 5	100 m x 30 m x 10 m
1 (aperiodic traffic)	99.999 9 to 99.999 999	~ 10 years	< transfer interval value	25	≤ 1 ms (note 2)		stationary	2 to 5	100 m x 30 m x 10 m
2 (periodic traffic)	99.999 9 to 99.999 999	~ 10 years	< transfer interval value	250	≤ 1 ms	3 x transfer interval	stationary	2 to 5	100 m x 30 m x 10 m
2 (aperiodic traffic)	99.999 9 to 99.999 999	~ 10 years	< transfer interval value	500	≤ 1 ms (note 2)		stationary	2 to 5	100 m x 30 m x 10 m

NOTE 1: Length x width x height.
NOTE 2: Transfer interval also applies for scheduled aperiodic traffic

Use Case (UC) 1*: In the case of the 100Mbit/s Link Replacement, 50% Periodic Traffic and 25% A-Periodic Traffic are assumed.*
Use Case (UC) 2*: In the case of the 1Gbit/s Link Replacement, 25% Periodic Traffic and 50% A-Periodic Traffic are assumed.*

Two (2) or more Machines (typically 4 or 5) cooperate with each other during production. In order to replace the Cables, each Machine is equipped with one (1) UE, connected to the Controller (shown in the Figure above). The Cooperating Machine's Communication can be divided into two (2) types.

A) Periodic Traffic and B) A-Periodic Traffic. Both types are scheduled, therefore the A-Periodic Traffic is also adhering to the transfer interval. The Traffic Requirements are from the point of view of the UE and give the Maximum Aggregate Traffic of all Links. Meaning, the Traffic per Link can change according to the Number of Cooperating Machines, but the Total Traffic at the UE cannot exceed the given values.

Annex 4. Mobile Networks to evolve from:

a Design that offers "Best-effort Services

to

a Design that offers Performance and User Experience Guarantees

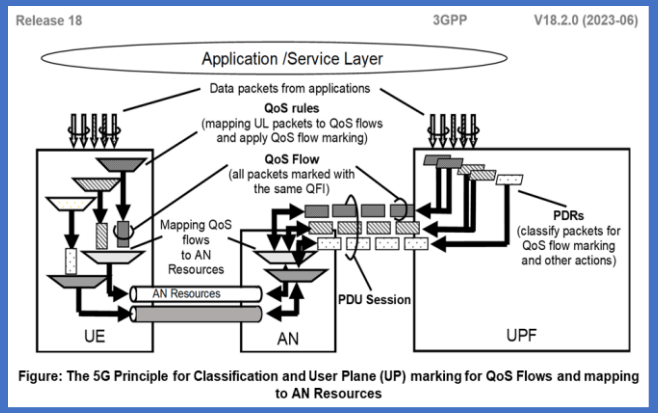


Figure: The 5G Principle for Classification and User Plane (UP) marking for QoS Flows and mapping to AN Resources

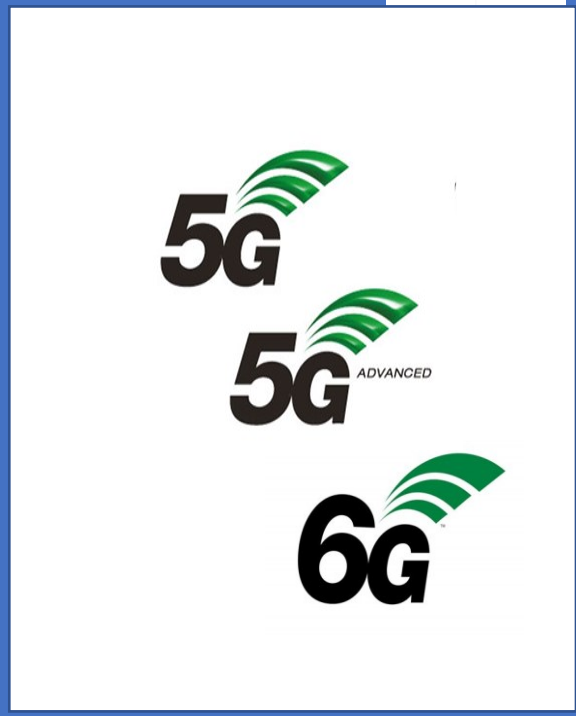
Capabilities related to e.g.:

When a *Multi-access* (**MA**) **PDU Session** is established, the Network may provide the UE with *Measurement Assistance Information* to enable the UE in determining which measurements shall be performed over both Accesses, as well as whether measurement reports need to be sent to the Network.

Measurement Assistance Information shall include the addressing information of *a* ***Performance Measurement Function*** **(PMF) in the UPF, the UE can send PMF protocol messages** incl.:

- Messages to allow for *Round Trip Time* (**RTT**) Measurements: the "*Smallest Delay*" steering mode is used or when either "*Priority-based*", "*Load-Balancing*" or "**Redundant**" steering mode is used with RTT threshold value being applied;
- Messages to allow for *Packet Loss Rate* (**PLR**) measurements, i.e. when steering mode is used either "*Priority-based*", "*Load-Balancing*" or "*Redundant*" steering mode is used with **PLR** threshold value being applied;
- Messages for reporting Access Availability/Un-availability by the UE to the UPF.
- Messages for sending **UE-assistance Data** to **UPF.**
- Messages for sending "*Suspend Traffic Duplication*" and "*Resume Traffic Duplication*" from **UPF** to **UE** to "suspend" or "resume" traffic duplication as defined in **5GS Architecture**.

=>



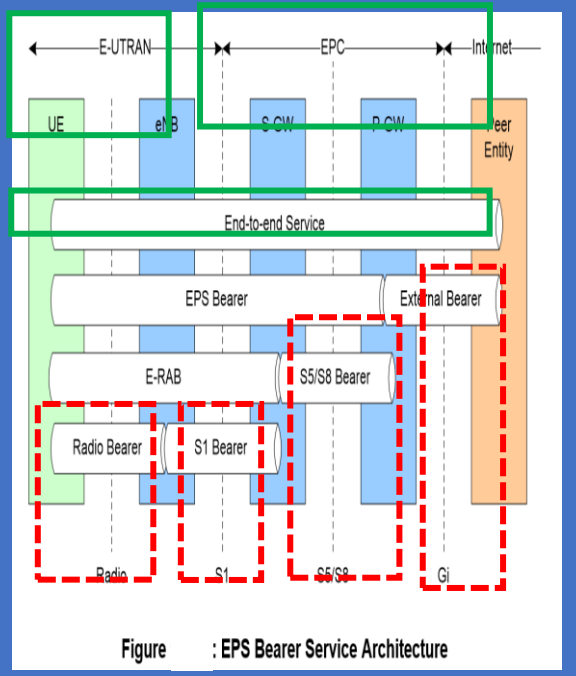


Figure : EPS Bearer Service Architecture

=>

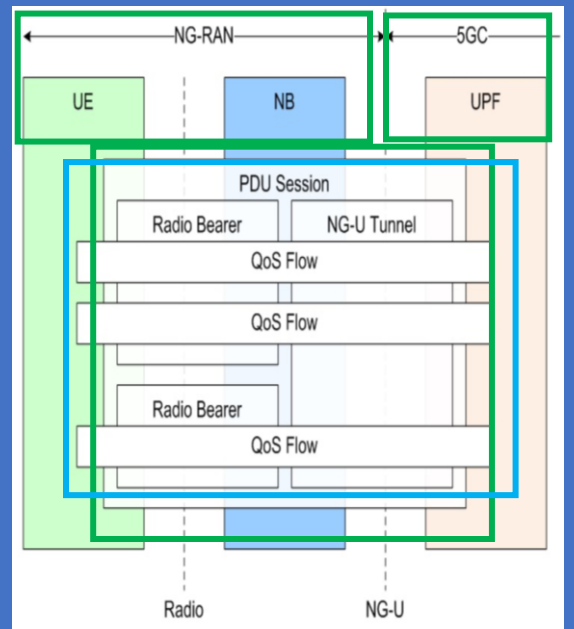
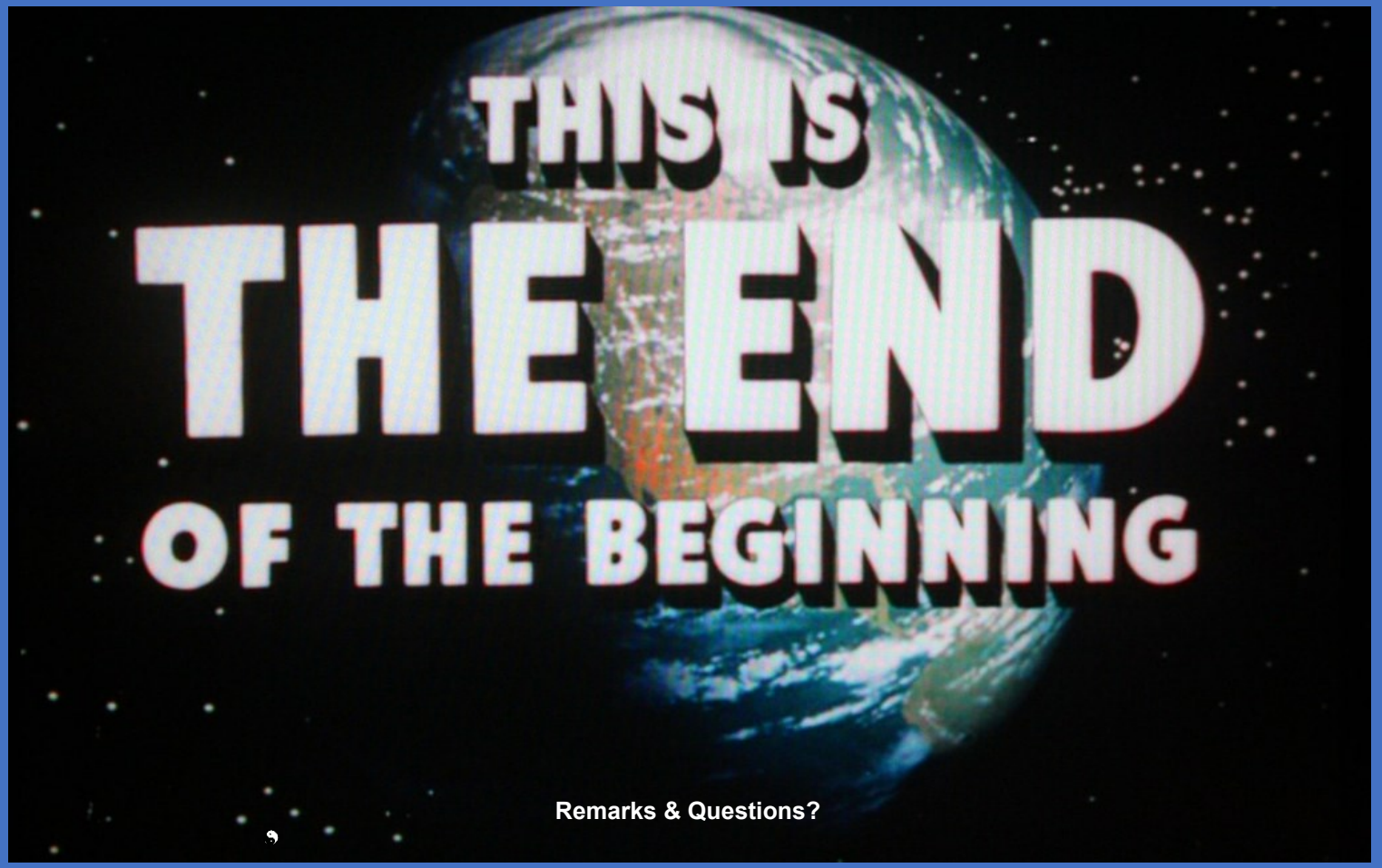


Figure: 5G CN NG-RAN Bearer Services QoS Architecture


THIS IS
THE END
OF THE BEGINNING
Remarks & Questions?