Security

Owned by David Cherney DISH •••
Last updated: Jun 26, 2023 • Initializing...

Contents

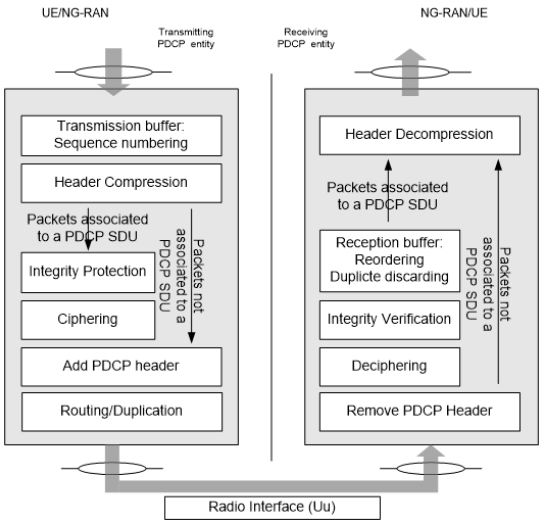
Security for mobile communications is a well developed feild with many facets. Here we will focus on the security features that 5G provides that preceding generations did not provide.

Terminology

Definition: Cyphering is ensuring that transmitted information is readable only to the intended recipient.

Definition: The process of determining if transmitted information is modified between transmission and reception is integrity protection.

Definition: Privacy protection is the ensurement that information about subscribers does not become available to others.



Service data unit treatment of 5G integrity and cyphering systems.

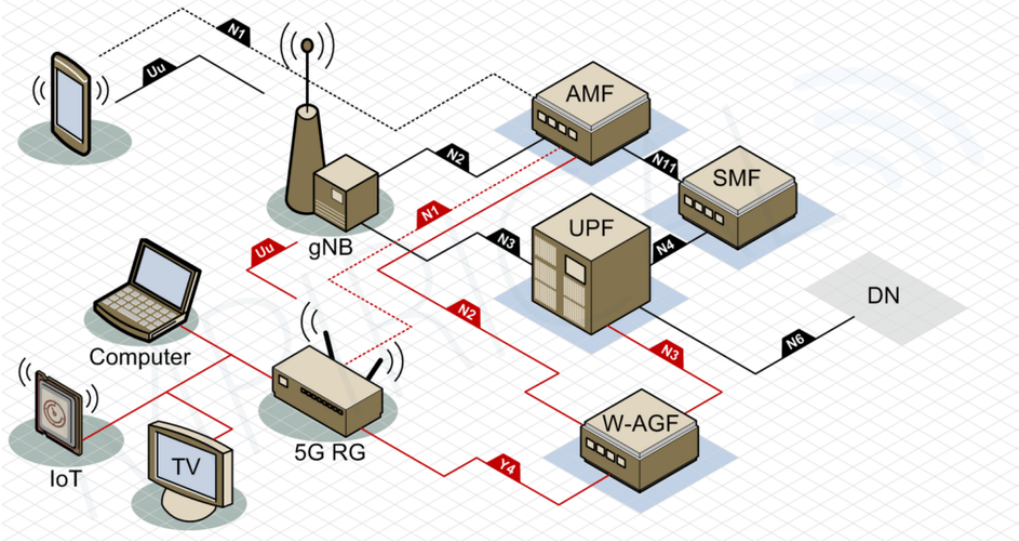
Definition: Primary authentication is authentication of UE with the 5G core network.

Definition: Secondary authentication is authentication of UE with a data network with which it connects through the 5G core.

New in 5G

Access Harmonization

Primary authentication of UE for different access technologies (5G New Radio, WiFi, ethernet over wire) is as consistent as possible in 5G. This is because 5G is designed for a wide range of use cases. In 4G UE authentication to initiate access was designed only for radio access, since any access to the network besides radio access was unusual. In 4G, only the SUPI could be used as the mobile subscriber identity in authentication. Other options are available in 5G. Similarly, in 4G authentication procedures required that the authenticating UE have a USIM. In 5G, authentication can be done with other structures, such as with credentials.

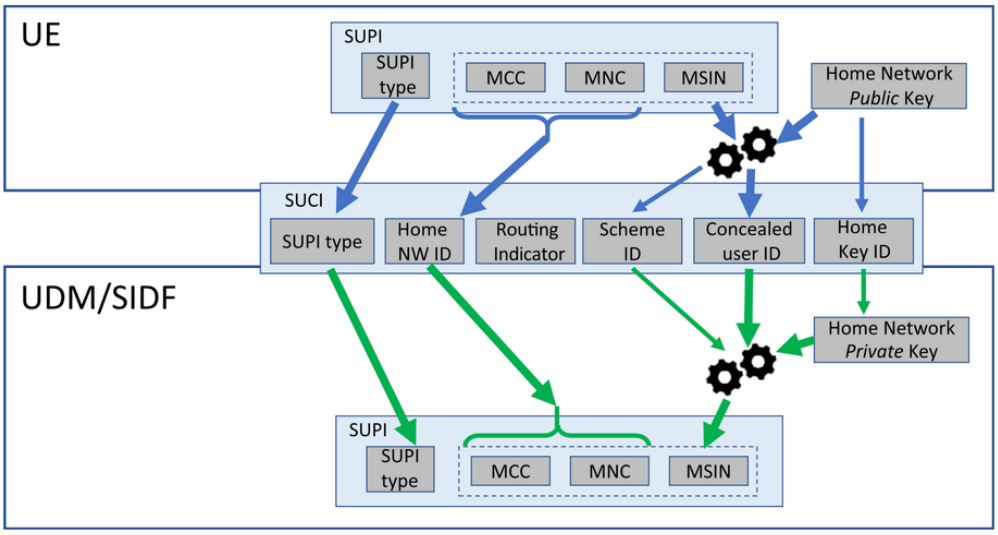


Two access technologies on a single 5G core; a mobile device uses a 5G NR connection, whiles a computer, TV, and IoT device use a 5G residential gateway (5G RG) connection through a wireless access gateway function (W-AGW) that facilitates N2 connection.

In fact, a singe UE can access the core through multiple access technologies in 5G, and to make this process smooth the AUSF keeps the UE's authentication credentials in memory or the sole purpose of serving this possibility.

Concealment of SUPI

The subscriber permanent identity (SUPI) is never exposed in 5G. In 4G there were rare circumstances where UE paging by the network included sending SUPI in plain text. This is an obvious privacy protection problem solved using a public key provided by the home network, so that a visited network can encrypt the SUPI, with the associated private key that can decrypt the SUPI residing in the SIDF.

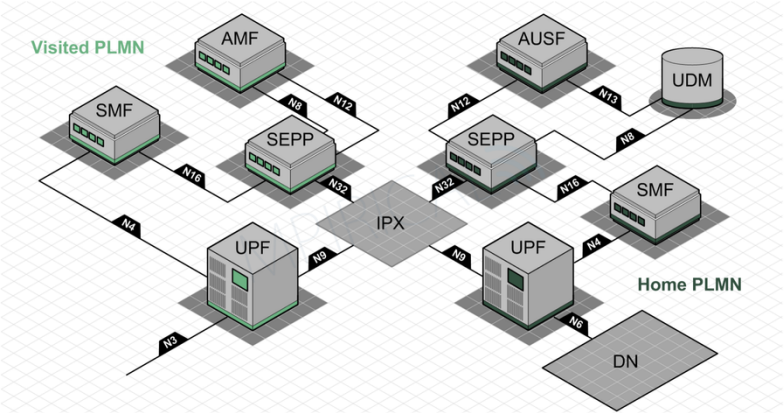


Integrity Protection

Because of the intended use by IoT devices, 3GPP foresaw the importance of integrity protection of user plane communication between UE and gNB.

H and V Authentication

In 4G roaming, the visited PLMN authenticated UE attempting initial registration with the network. 5G introduces the authentication procedure called 5G-AKA (authentication by key agreement) that allows both the visited and the home PLMN to independently authenticate a UE attempting to register in the vPLMN.



Home and visited networks, connected to each other by their security edge protection proxies exchanging packets through a IP exchange (IPX).

Core Initiated Session Security

In 4G the gNB decided upon the ciphering to be used for a UE's user plane data sessions (PDN sessions) at registration. In 5G, at initiation of a PDU session the core dynamically decides upon cyphering and integrity protection to be used. This allows different security setting to be used for different sessions, and gives more security authority to the core.

Initial NAS Messaging Protection

In 4G, the initial message from a UE to the network included some plane text information about the UE and network. In 5G that initial message has lower privacy protection risk.

NRF as SBI Security Agent

Because 5G introduced SBA, new security features were added to ensure secure communication between core network functions. These features are optional, since a private 5G network that accesses only a private data network will not need them.

The NRF can serve as a security agent by acting as a token server. SBA communication then takes on the following procedure.

1. When a SBA consumer (client) that we will call NF1 wishes to send a service request to a SBA producer (server) we will call NF2, first NF1 asks NRF for a security token.
2. If the NRF recognizes NF1 as a authenticated and authorized NF, then the NRF gives NF1 a security token.
3. NF1 then sends it's service request to NF2, including the token in the request.
4. NF2 checks the validity of the security token using either (I'd like a more detailed description of this step)
    a. a public key from the NRF
    b. a shared key with the NRF
5. If the token is validated by NF2 then NF2 provides the requested service to NF1.

To avoid self reference to the security token service, the services that the NRF provides do not require a security token:

- NF registration
- NF discovery
- NF service discovery
- token request

Slicing Security

Since network slicing is new in 5G, security pertaining to slicing is also new to 5G.

Slice Concealing

Transmitting the identifier of a slice (S-NSSAI) is considered a security risk; a malicious actor could gather information about the topology of the slice and which UE access the slice. Thus is is always transmitted with encryption and integrity protection over N1. Over N2 UE, use is made of two lists of slices for a UE; elements of one list can be sent in plain text over N2 wile the other can not. This should allow flexibility.

NF Slice Assignment

Network functions are also given a list of slices on which they are authorized to function, in accordance with the security principle of least privilege.

Secondary Authentication to a Slice

To enable IoT use cases to have high security, after primary authentication onto the network a second authentication onto a slice can be performed. This is to be handled by a dedicated network function called the network slice specific authentication and authorization function (NSSAAF). The authentication server for this process need not reside in the core; the NSSAAF may access an external server to authenticate the UE onto the slice.

Slice Admission Control

To further enable IoT use cases, the ability for an application function to monitor the number of UE and PDU sessions on a slice has been created. This has been done through a new function called the network slice admission control function (NSACF). Security measures to make sure the AF does not learn too much about the network have been put in place.

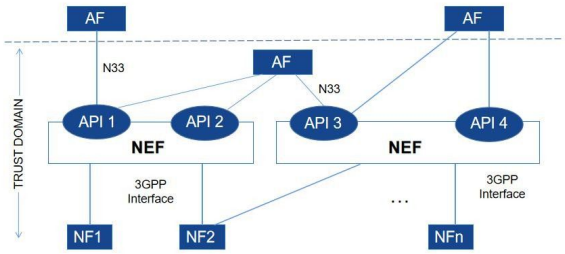
That concludes the list of new security features in 5G.

NEF Security

Recall that NEF exposes information about from the core to application functions (AFs) and facilitates AFs updating policy and charging control information in the core. Clearly it is important to have tight security on which application functions have these abilities.

3GPP recognizes that some application functions might be trusted functions in the operator's domain, and for these it requires only "implicit authentication" of AFs. For AFs outside the operator domain, authentication must be explicit and must use TLS client and server credentials.

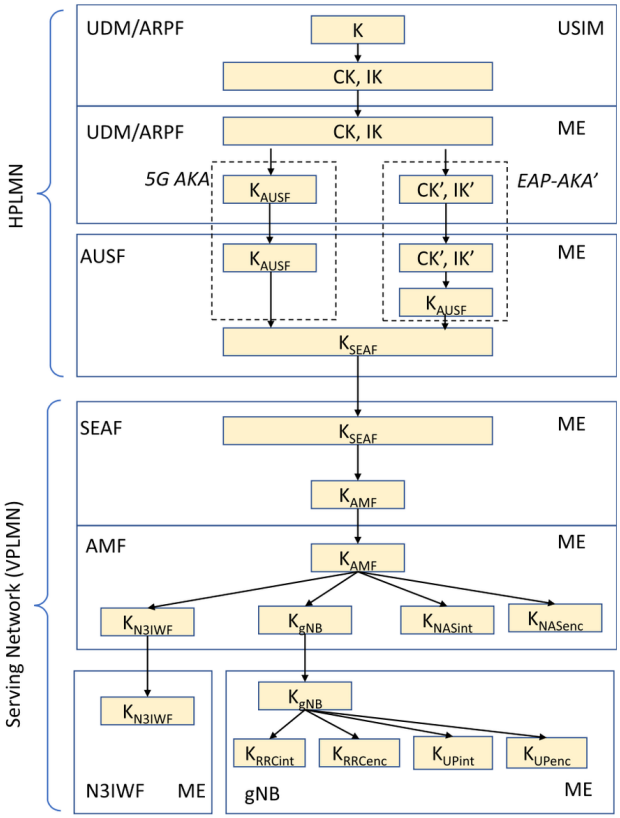
Further, after authentication, the NEF maintains authority to authorize the AF to send requests.



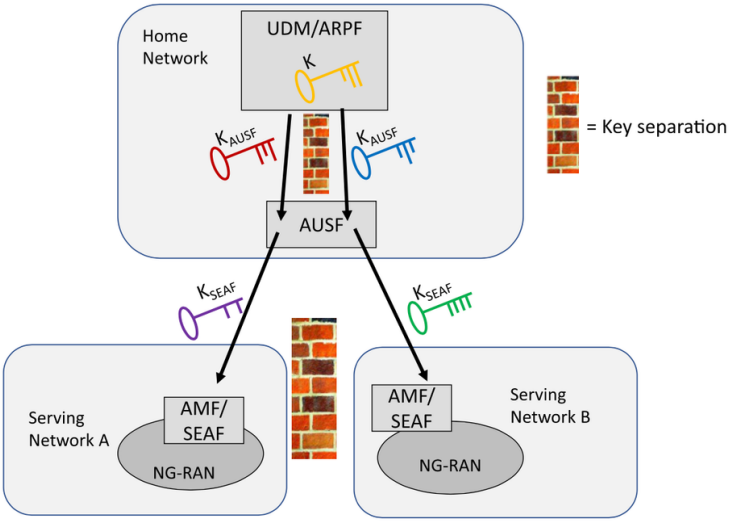
Key Hierarchy

In 5G, keys for authentication, integrity protection, and cyphering are well separated; a malicious actor who discovers a key for one purpose can not use it for another purpose. The keys are derived from a long term-key stored in the UE's USIM and the core's UDR. The derivations are slightly different for the two primary authentication procedures, 5G AKA and EAP-AKA' (extensible application protocol authentication by key agreement prime.) The derived keys are for the following purposes:

- home AUSF authentication
- visited SEAF authentication
- visited AMF authentication
- N3IWF authentication
- gNB authentication
- gNB encryption
- gNB integrity protection
- user plane encryption
- user plane integrity protection



This family structure of keys facilitates many other security aspects. For example, it enables giving different keys to the same UE in different visited networks so that the identity of the UE is not revealed by the same key appearing in two visited networks.



Lawful Intercept

While 3GPP specifications do not require any specific structures for enabling law enforcement to intercept messages, the specifications to say that the capacity to comply with laws must be built in to all functions, and that the capacity must be able to facilitate narrow data collection through methods that ensure privacy protection.

An example setup option for lawful intercept is presented below. It involves a few network functions and module that can be included in a core to facilitate lawful intercept (LI).

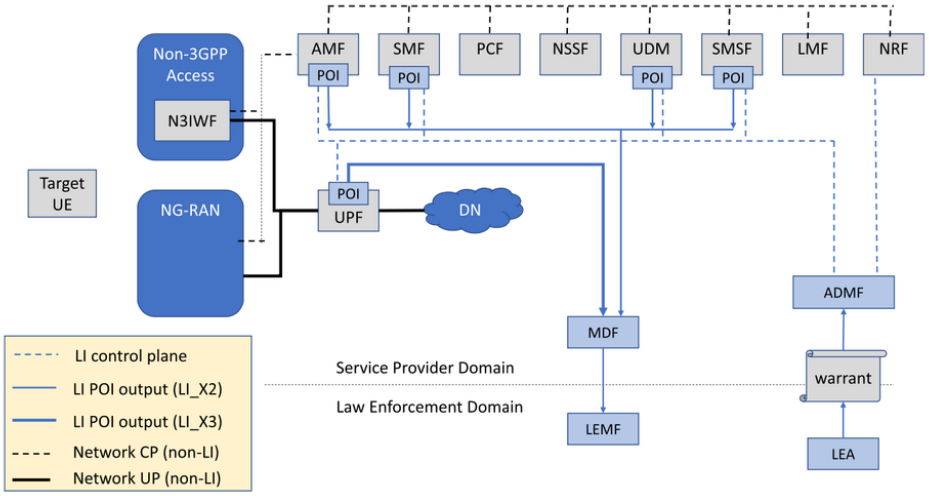


Fig. 8.13 High level LI architecture.

In steps:

1. The law enforcement agency (LEA) obtains a warrant.
2. That warrant allows passing of access setting to the administration function (ADMF). The ADMF manages the LI system in the following sense;
3. The ADMF queries the NRF for the NFs the LEA has been authorized to intercept data from.
4. Using this list, the ADMF accesses the point of intercept (POI) modules that are built into the NFs. In particular, the ADMF inserts new rules into the POI modules about reporting specific kinds of usage for specific UE or subscribers.
5. The reports from the POI are sent to the mediation delivery function (MDF), which is an aggregation point for intercepted data within the core.
6. The MDF then sends the aggregated reports to the law enforcement monitoring facility (LEMF) located outside the core and in the law enforcement domain.

The requirements and implementations of LI vary widely between the nations that are signatories of the ITU.