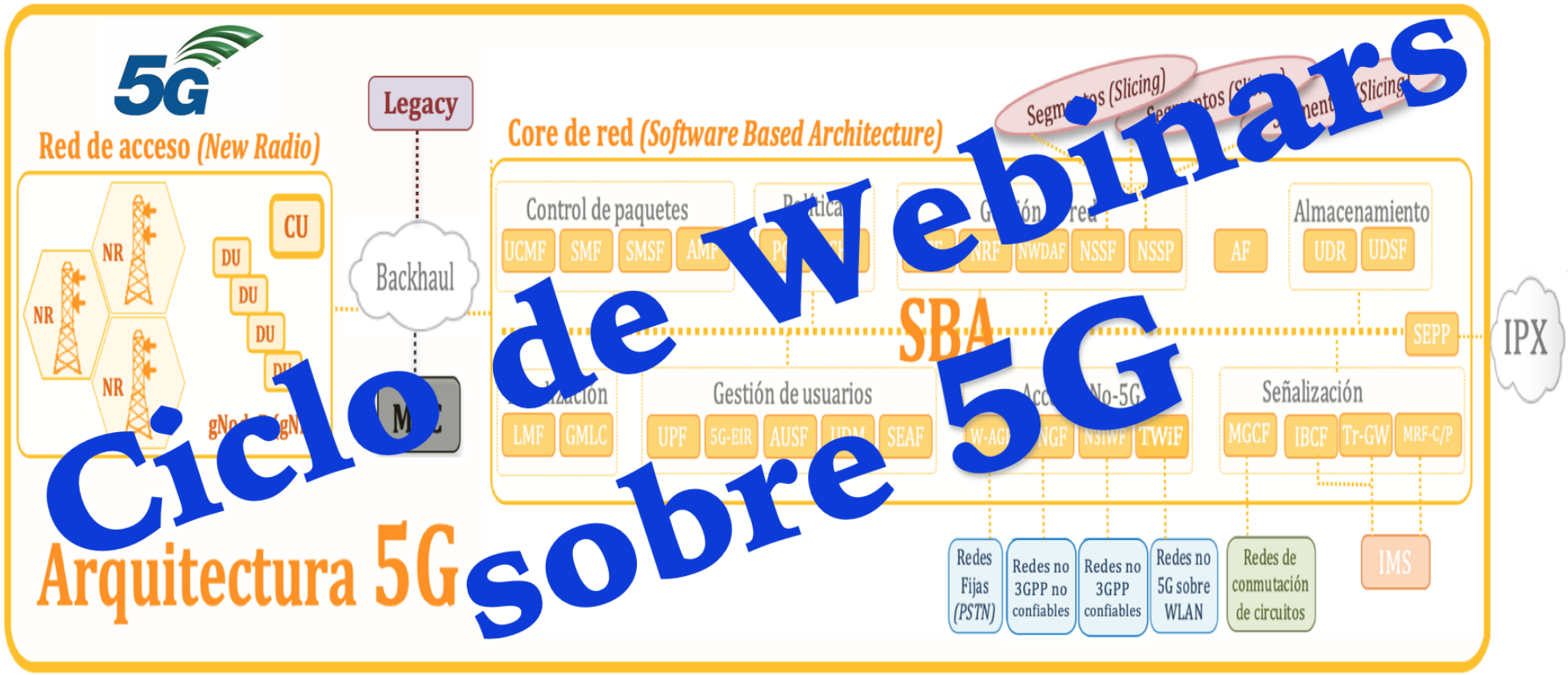
Tema 4: Accesos y autenticación



Ciclo de Webinars sobre 5G

Alejandro Corletti Estrada

acorletti@darFe.es

www.darFe.es

Ciclo de Webinars sobre 5G

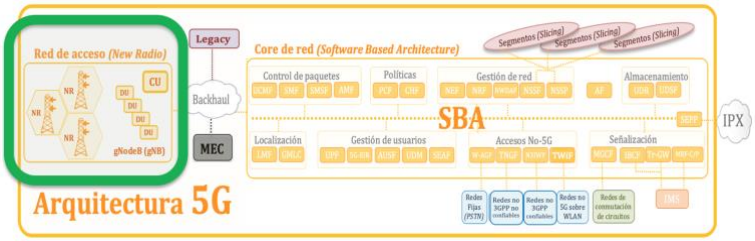
Tema 4: Accesos y autenticación

DESARROLLO DEL CICLO DE WEBINARS

Webinar 1: Presentación y evolución de las tecnologías móviles

Webinar 2: New Radio y gNodeB

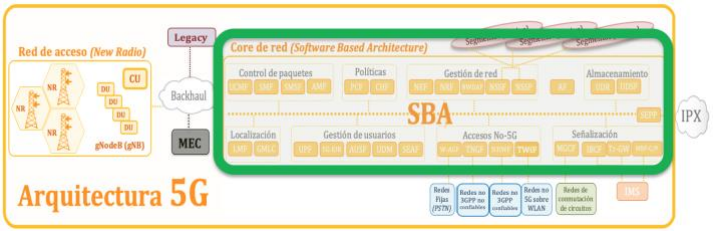
- Descripción de diseño de los gNB
- Open RAN
- Antenas compartidas (RAN Sharing)
- Frecuencias licitadas y asignadas
- Empleo de Cloud



Webinar 3: SBA, MEC y Slicing

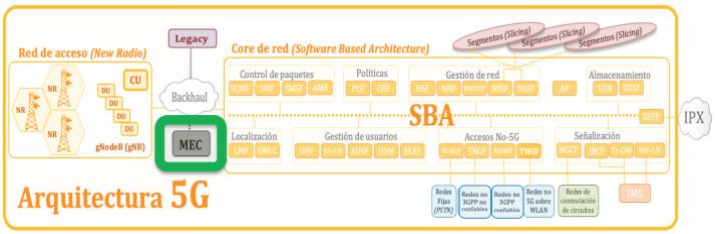
SBA (Core 5G) (Service Based Architecture)

- Descripción
- Funciones de red (NF)
- Security Edge Protection Proxy (SEPP)
- Empleo de Cloud



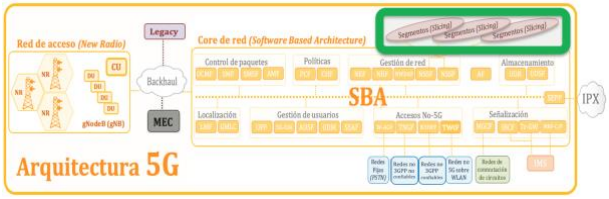
MEC (Multi-access Edge Computing)

- Empleo y detalle de MEC
- Análisis de contratos



Slicing (Segmentos)

- **mMTC**: massive Machine Type Communication - ***IoT***
- **eMBB**: enhanced Mobile Broadband (eMBB) - ***Eventos***
- **URLLC**: Ultra-Reliable Low Latency Communications - ***Salud***
- **V2X**: Vehicle to X - ***Vehículos autónomos***.
- Plantillas GST (Generic network Slice Template)

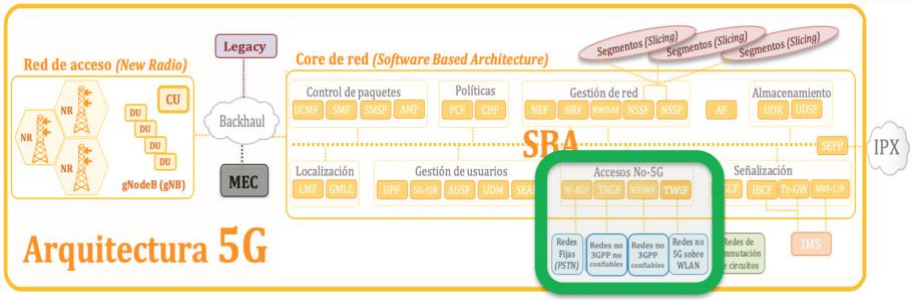


Webinar 4: Accesos y autenticación

Tema de hoy

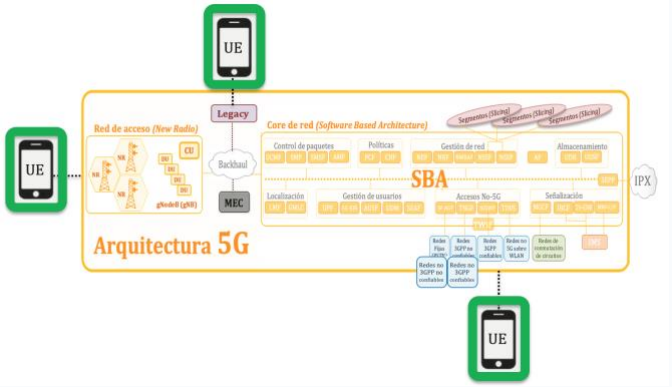
Otros accesos

- Small Cell
- Accesos Non-3GPP Trusted
- Accesos Non-3GPP No Trusted
- Accesos desde red Fija
- FWA



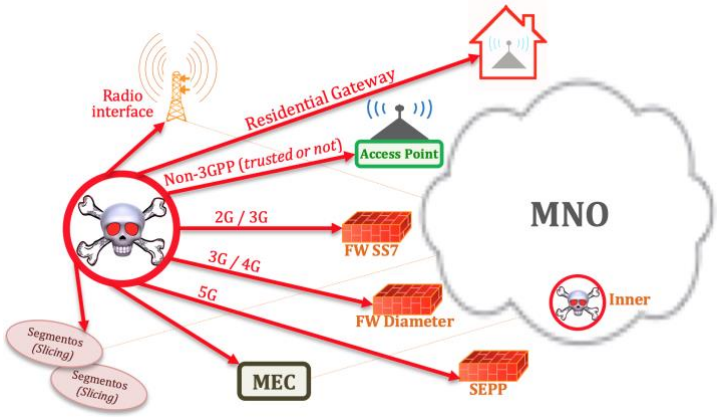
Accesos UE (User Equipment)

- a. UICC 4G heredado con aplicación USIM
- b. 4G UICC actualizado con la aplicación USIM
- c. 5G UICC con aplicación USIM

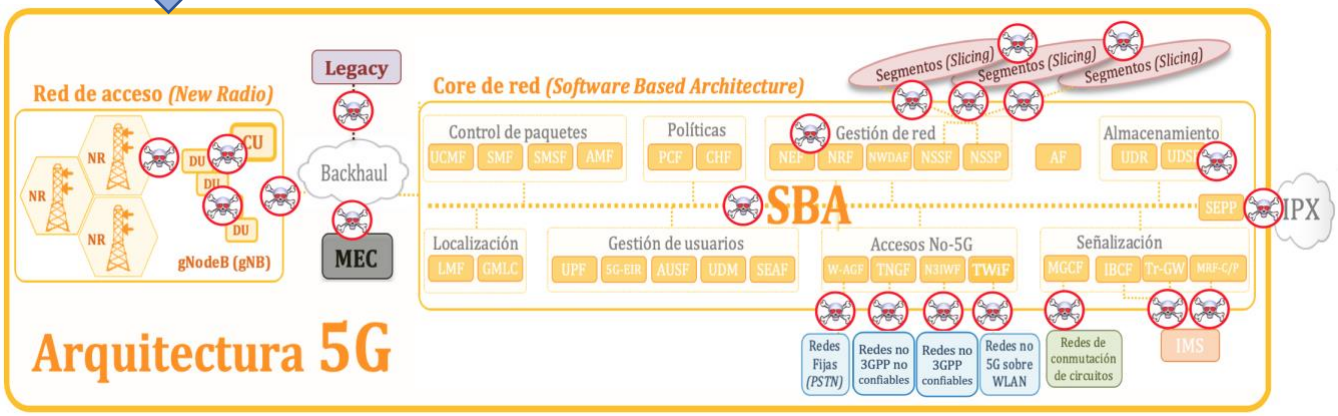


Webinar 5: Seguridad en 5G

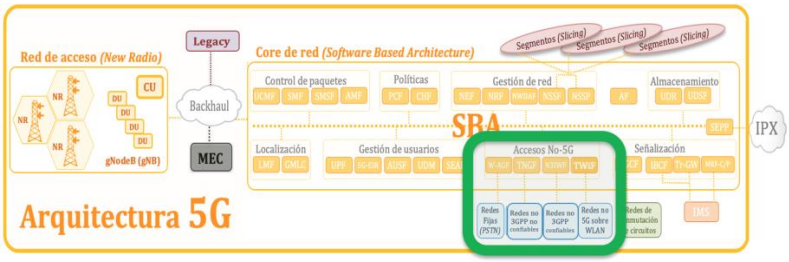
Vectores de intrusión



Puntos clave de seguridad en 5G



Otros accesos



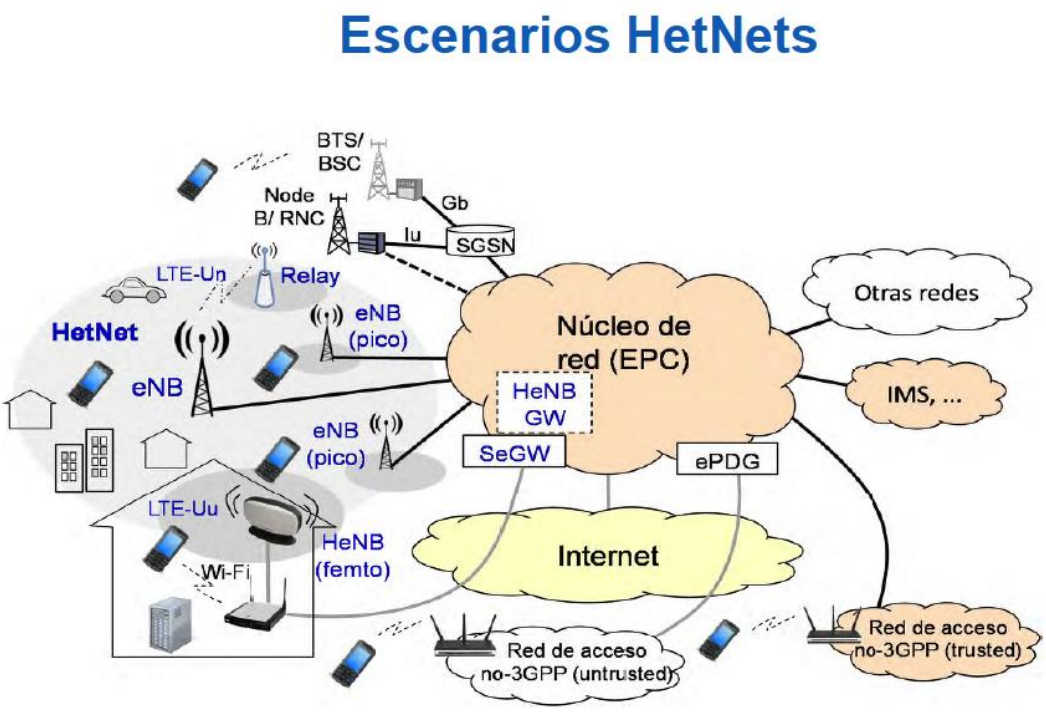
Temas a desarrollar en esta sección.

- Small Cell
- Accesos Non-3GPP Trusted
- Accesos Non-3GPP No Trusted
- Accesos desde red Fija
- FWA (Fixed Wireless Access)

Small Cell

"Small Cells" son antenas de menor cobertura, por medio de lo que se denominan "**pico, micro** y **femto cells**" que se comercializan para empresas y también para descongestión de las celdas convencionales (también llamadas Macro cells).

Con la idea de small cell, da origen al concepto de accesos heterogéneos o **HetNets**, pueden existir algunos "confiables" y otros "no confiables". Los primeros simplemente son aquellos en los que el operador 3GPP confía en la seguridad de la red o dispositivo que está accediendo a su Core y los segundos como, una red "no confiable" pueden ser, por ejemplo, el uso de una WLAN (Wireless LAN) en un café público o un aeropuerto para conectarse al servicio de red privada (o VPN) de su empresa.



A continuación se desarrolla con más detalle los accesos NO 3GPP:

Uno de los principales objetivos logrados en 5G, luego de las **Release 15** y **16**, es definir todas las posibilidades de acceso existentes al día de hoy sobre la red telefónica conmutada y las redes Wireless hacia el core de 5G (**5GC**). Este objetivo aplica tanto para las redes definidas por 3GPP como para las que no.

5G permite un marco unificado de autenticación para redes 5G, anteriores, WLAN (Wireless LAN), fijas, confiables y no confiables. Veremos que las cataloga como redes 3GPP y No 3GPP. Existe:

- una autenticación primaria cuyo objetivo es la autenticación mutua entre el **UE** y la **red**, y la provisión de material de codificación que pueda utilizarse en los procedimientos de seguridad posteriores entre el equipo de usuario y la red de servicio.
- Una autenticación secundaria que permite al operador delegar la autorización a un tercero.

El protocolo de autenticación principal o nativo para 5G es **5G-AKA** (Authentication and Key Agreement Scheme), pero permite el empleo de:

- **EAP-AKA** (Extensible Authentication Protocol - *RFC-4187*) desarrollado por 3GPP y es compatible con EAP (*RFC-3748*).
- **EAP-AKA'**: (*RFC-5448*) es el nuevo método adoptado en 5G para un uso más amplio de EAP.

La adopción del marco EAP en 5G significa que es posible que otros métodos además de EAP-AKA', como **EAP-TLS** (Extensible Authentication Protocol-Transport Layer Security, que como se trata en este texto, se utiliza para implementaciones aisladas.

Cuando se utiliza **EAP** (por ejemplo, EAP-AKA o EAP-TLS), la autenticación EAP se realiza entre el **UE** (un EAP *peer*) y el **AUSF** (Authentication Server Function - un *servidor EAP*) a través de **SEAF** (Security Anchor Function que funciona como una *pasarela EAP del autenticador*).

Si analizamos desde el punto de vista de su grado de avance, en la **Release 15** se introdujo el soporte para acceso no confiable no 3GPP (Untrusted non-3GPP) disponible desde 4G. Luego en la **Release 16** se introdujo el soporte para el acceso confiable no 3GPP (trusted non-3GPP) y el acceso por cable (red fija).

En esta Release 16, el core 5G admite conectividad a **W-5GAN** (Wireline -5G Access Network) a través de una función de puerta de enlace llamada **W-AGF** (Wireline Access Gateway Function).

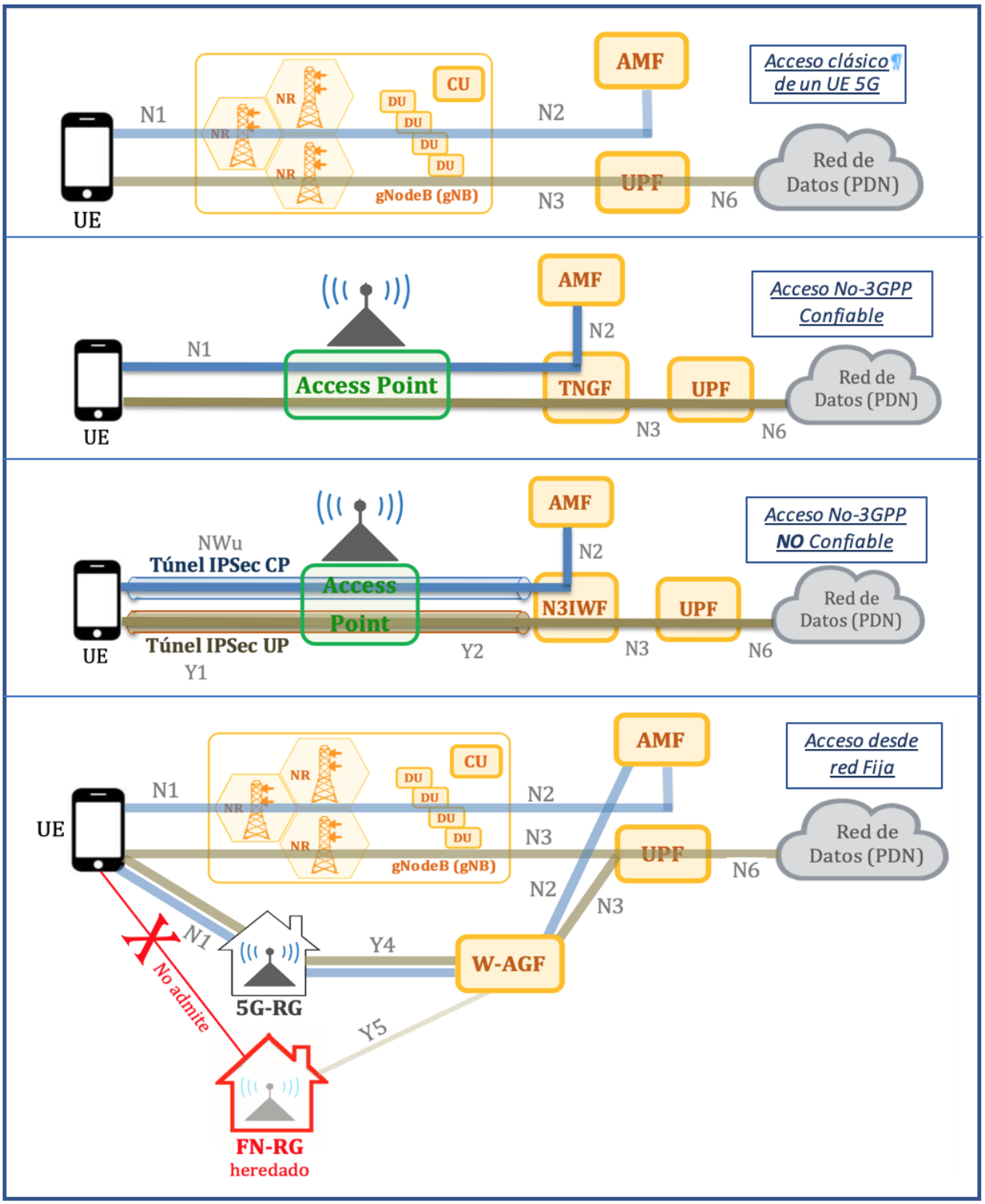
El **W-AGF** como veremos en las imágenes que siguen, puede ser alcanzado por dos tipos de Gateway residenciales (**RG**: Residential Gateway)

- **FN-RG** (FN-RG: Fixed Network-RG): Gateway que NO soportan el acceso del móvil 5G en la interfaz N1. Se trata de dispositivos heredados de tecnologías anteriores, es decir cualquiera de los Puntos de acceso WiFi que tenemos actualmente en nuestros domicilios y que no permitan a futuro su actualización por software.
- **5G-RG:** Gateway que SÍ soportan el acceso del móvil 5G en la interfaz N1. Nuevos puntos de acceso domiciliarios que permitirán la conexión en la interfaz N1 con el 5GC. El **5G-RG** se conecta al core 5G como si fuera un UE

Cuando la autenticación se realiza en redes de acceso no 3GPP NO confiable, se requiere una nueva entidad llamada **N3IWF** (Non-3GPP Interworking Function, que requiere un servidor VPN para permitir que el **UE** acceda al **core 5G** a través de **túneles IPsec**. Una vez creado el túnel IPSec, el UE puede utilizar uno de los métodos de autenticación primarios 5G para autenticarse en el 5GC. Si el UE no es 5G, no podrá autenticarse en el 5GC a través de

la red de acceso que no es de confianza, ya que es posible que no admita las capacidades necesarias para descubrir el N3IWF o para establecer un túnel IPsec con N3IWF, esto difiere de una acceso a través de una red de confianza, pues a pesar que el UE no sea 5G en este caso sí está contempladas estrategias de acceso compatibles.

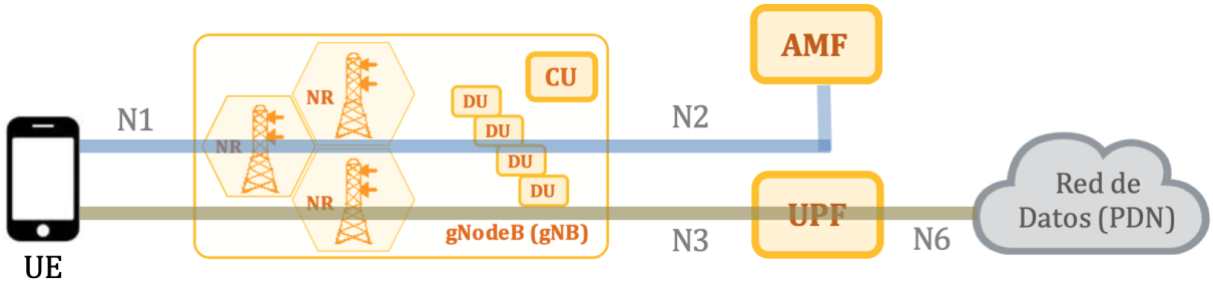
A continuación se presentan en forma de imágenes, los diferentes tipos de accesos que permite el 5GC. En primer lugar, presentaremos todas las imágenes reunidas para poder observar en detalle las diferencias, y luego se presenta caca una de ellas con una breve explicación particular de cada caso.



Como se puede apreciar en todas las imágenes anteriores, la pieza clave es el **AMF** (Access and Mobility Management Function). Entre sus principales funciones están la gestión del registro, la gestión de la conexión, la gestión de movilidad y gestionar varios aspectos relacionados con la seguridad y la autorización de los accesos. AMF ya era parte de la funcionalidad de MME en EPC, es decir en 4G.

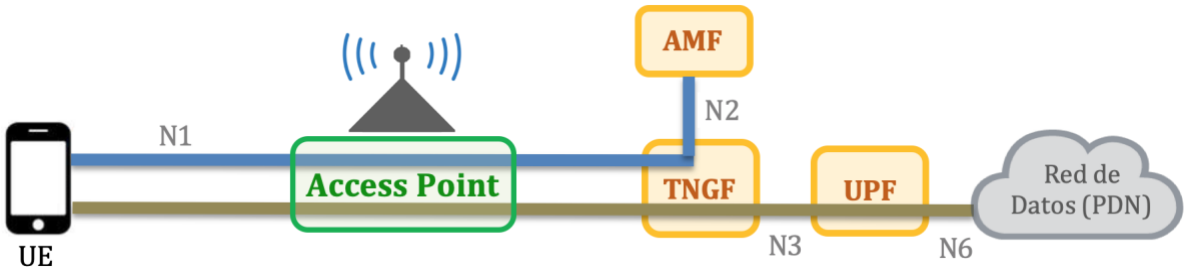
Las interfaces N2 y N3 son interfaces que conectan 5G-AN con **AMF** (Access and Mobility Function) y con la **UPF** (User Plane Function), respectivamente. Transportan señales sensibles y datos del plano del usuario entre la red de acceso y el núcleo (core 5G).

1) Acceso clásico de un UE 5G:



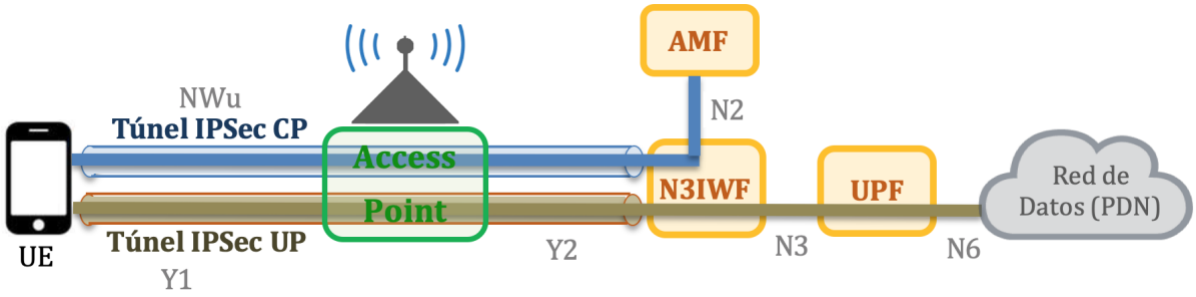
Se trata de la forma normal en la que un móvil 5G se autentica y conecta a la red.

2) Acceso No-3GPP Confiable:



En este caso, podemos ver cómo el UE se conecta a través de una WLAN a través de un Access Point (administrado por la operadora, por eso es "confiable"), el dispositivo que desempeña las funciones de acceso es el **TNGF** (Trusted Non-3GPP Gateway).

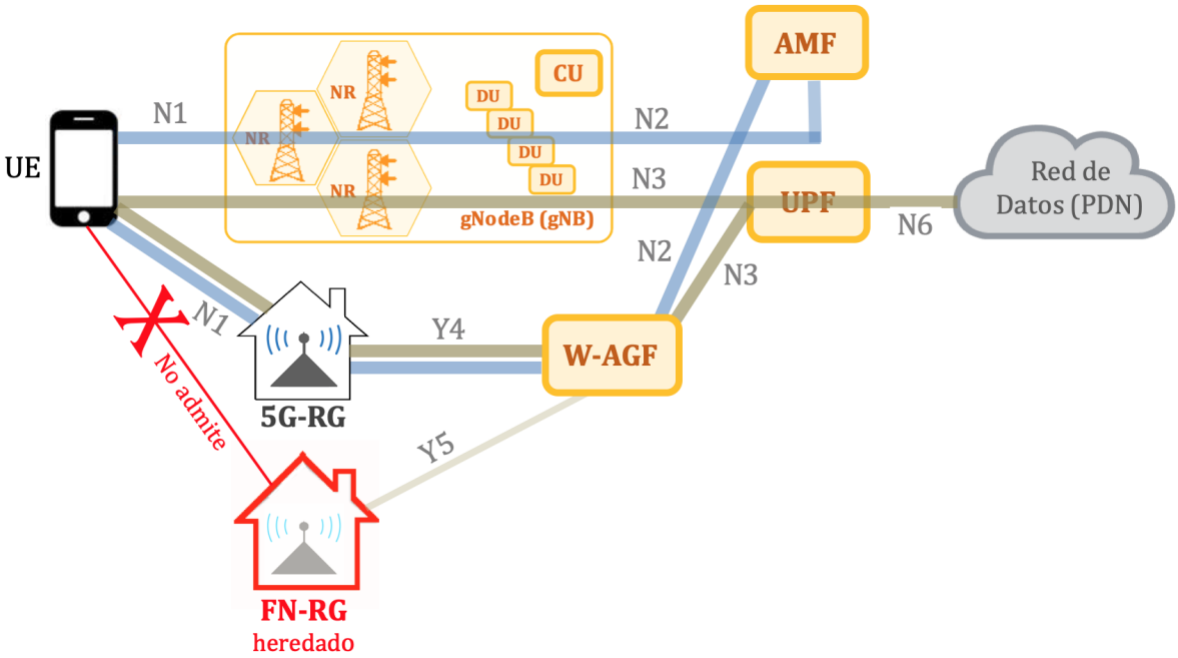
3) Acceso No-3GPP NO Confiable:



En este caso, podemos ver cómo el UE se conecta a través de una WLAN a través de un Access Point (No administrado por la operadora, por eso es " No confiable"), el

dispositivo que desempeña las funciones de acceso es el **N3IWF** (Non-3GPP Inter-Working Function). En este caso, como la interfaz WLAN no es confiable, deben crearse dos túneles IPSec entre el UE y el N3IWF que es un servidor de **VPN** (Virtual Private Network). Este tipo de túneles (con IPSec u otras tecnologías) son los que se emplean en casi todos los casos para accesos remotos seguros (por ejemplo para el teletrabajo). En este caso, primero se realiza la asociación de seguridad para el plano de control (**CP**) y sobre la seguridad de este, luego se realiza el segundo túnel para el plano de usuario (**UP**).

4) Acceso desde la red fija:



En el caso de los accesos desde un "Residencial Gateway" (RG), como se aprecia en la imagen anterior, este dispositivo puede ser de nueva generación, es decir un "router 5G" nuevo (**5G-RG**) instalado en mi domicilio y/o empresa, el cuál ya presenta la posibilidad de conexión vía 5G desde el UE, o puede ser a través del "router" que tenía instalado en mi domicilio y/o empresa que aún no soporta 5G. En esta caso, el móvil no puede conectarse vía 5G, por supuesto que si ese router tiene capacidad WiFi (como casi todos los actuales), cualquier móvil 3G, 4G o 5G podrá conectarse si se habilita la opción "WiFi" desde el UE, pero debe quedar claro que este enlace aire NO es a través de la tecnología 5G, sino la que tengo desde hace años por WiFi (Protocolo **IEEE 802.11x**).

En este caso y en el anterior, el acceso de estos RG al core de 5G se realiza como si los mismos fueran UE 5G convencionales, pasando por el W-AGF.

El acceso a la red requiere autenticación del suscriptor, que se realiza mediante un mecanismo de autenticación primario en el sistema 5G. Para que la red pueda identificar al abonado, el UE debe enviar el identificador permanente de suscripción (**SUPI**: subscription permanent identifier, en 5G). Este identificador de suscripción permanente se enviaba en texto plano hasta 4G, lo que provocó varios ataques relacionados con la privacidad.

En **5G**, la privacidad se logra, incluso antes de la autenticación y el acuerdo de claves, cifrando el SUPI antes de transmitir utilizando una clave pública de la "Home Network" que se almacena en la USIM.

Para proporcionar privacidad, el **UE** genera y transmite el Identificador oculto de suscripción (**SUCI**: Subscription Concealed Identifier) utilizando un esquema de protección por medio de algoritmos de curva elíptica (**ECIES**: Elliptic Curve Integrated Encryption Scheme), con la clave pública mencionada.

A continuación, y solo a título de ejemplo para poder observar las diferencias, se presenta una comparativa sobre el proceso de autenticación por medio de **EAP-AKA** y **EAP-AKA'** de acuerdo a lo que establecen sus respectivas RFCs.

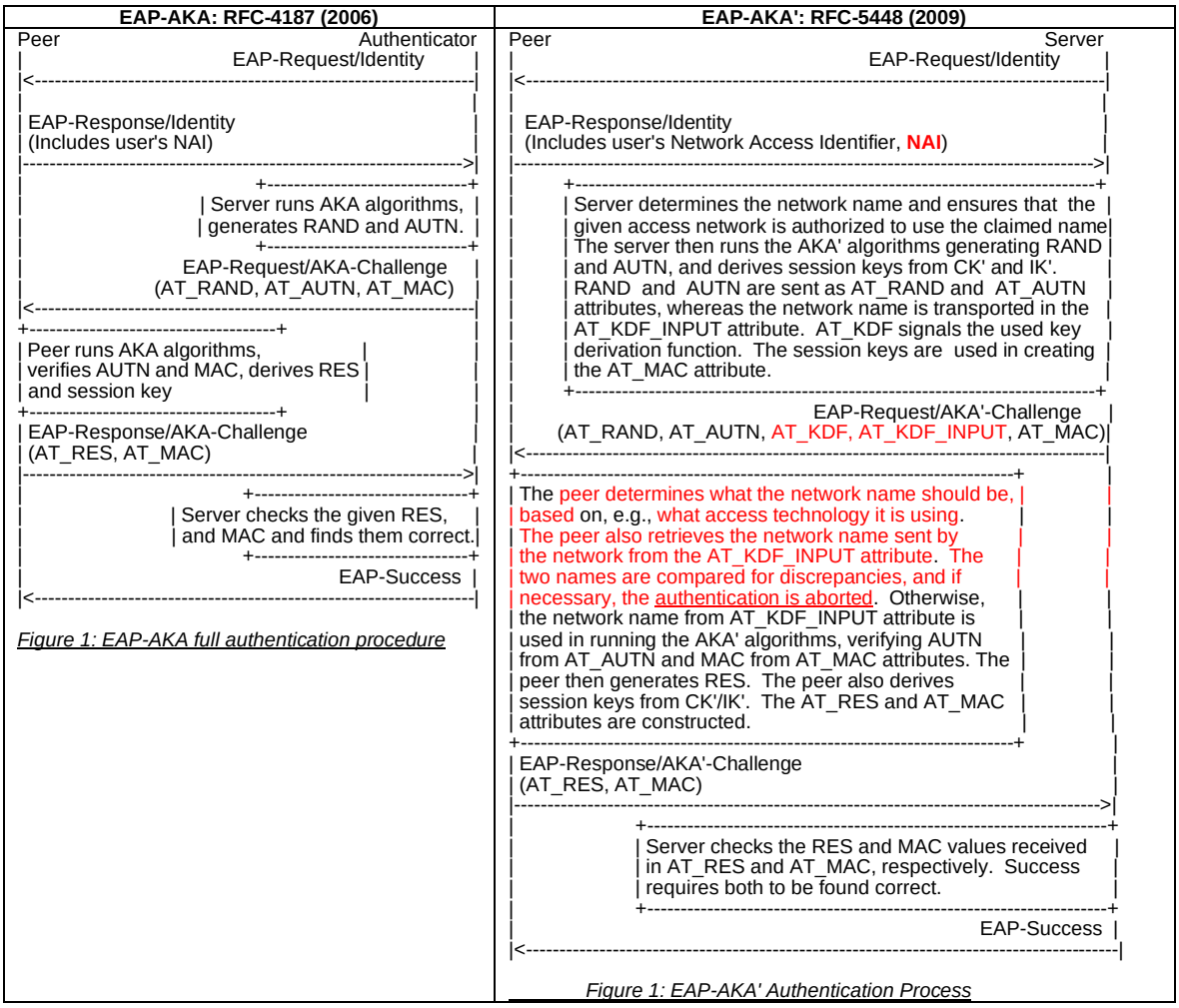


Figure 1: EAP-AKA full authentication procedure

Figure 1: EAP-AKA' Authentication Process

FWA (Fixed Wireless Access)

FWA es una conexión que proporciona acceso primario de banda ancha a través de equipos de instalaciones del cliente (**CPE**: customer premises equipment) habilitados para redes móviles de área amplia inalámbrica.

Para expresar su función de forma sencilla, en realidad la tecnología de FWA es como que da solución alternativa al viejo tema de la "última milla", es decir ese acceso de cobre con que nacieron todos los teléfonos fijos del mundo y que hoy se está reemplazando por fibra óptica.

Como bien se sabe, para poder ofrecer el ancho de banda que las sociedades del primer mundo (o en vías) exigen hoy en día, se están desplegando diferentes tecnologías de fibra óptica que gracias a las tecnologías **GPON** (Giga Passive Optical Network) y a las multiplexaciones por división de onda (**WDM**: Wavelength Division Multiplexing) permiten hoy, lo que se suele llamar **FTTx** (Fiber To The "X", siendo X = Builiding, Home, Curb, Premise, etc.).

Con cualquiera de estas tecnologías, se acerca la fibra todo lo posible al usuario final.

El tema que entra en discusión ahora es que el acceso de usuario, en vez de llevárselo dentro de su casa o empresa, se puede ofrecer mediante una antena que facilite el acceso a la red de 5G lo suficientemente cercana como para que obtenga por aire, una ancho de banda similar a la fibra óptica.

Se debe tener especialmente en cuenta que los usuarios domiciliarios, cada vez exigen más movilidad y se está prescindiendo de las líneas fijas, con lo que:

¿Sigue siendo necesario invertir la enorme cantidad de recursos necesarios para llegar con fibra óptica hasta los hogares?

NOTA: *Mucho cuidado con esta idea*, pues si la relación de: "*distancia y ancho de banda*", es la oportuna… se pueden evitar muchos (*muchísimos*) metros de instalación de Fibra óptica, es decir se reduce la inversión o se bajan costes.

Aquí entra en juego la batalla "**FTTx vs. FWA**" que a cualquier operadora de telecomunicaciones debe importarle en extremo. Como se verá en las líneas que siguen las estimaciones de gasto de capital por suscriptor que indica **GSMA** son **$ 500-$ 1000 para FTTx** versus **$ 100-$ 400 para FWA**, lo cual es un argumento muy convincente a favor de FWA.

Análisis del documento: "THE 5G GUIDE A REFERENCE FOR OPERATORS"

https://www.gsma.com/wp-content/uploads/2019/04/The-5G-Guide_GSMA_2019_04_29_compressed.pdf

punto 3.6 The FWA opportunity

- El acceso inalámbrico fijo **FWA** es un subproducto del exceso de capacidad de eMBB y permite a los operadores abordar oportunidades de banda ancha nuevas y existentes.
- Hay **cuatro casos** de uso claros de FWA:
  - banda ancha para los no conectados
  - banda ancha para competir con alternativas fijas
  - backhaul de respaldo de banda ancha
  - estación base.

Muy IMPORTANTE

- FWA también es importante por otras razones estratégicas:
  - un incentivo adicional para profundizar la capilaridad de la fibra
  - para impulsar la cartera de productos para los operadores solo de telefonía móvil

- o para evitar que los nuevos participantes de FWA distorsionen el mercado.

- La GSMA ha mapeado las oportunidades de FWA para 160 países: mercados del océano azul, mercados del océano rojo y mercados del desierto.
- Si bien la oportunidad de FWA varía considerablemente según las geografías, siempre hay "oasis" potenciales de oportunidades.

Punto 3.6.1 FWA productos y servicios

FWA ofrece un enlace inalámbrico que proporciona conectividad a objetos que están estacionarios o con cierta movilidad (nomadic).

FWA no es una idea nueva, pero 5G FWA se posiciona mucho mejor que los intentos anteriores de implementar servicios similares a FWA utilizando tecnologías inalámbricas patentadas (por ejemplo, LMDS, iBurst), tecnologías celulares alternativas (por ejemplo, WiMAX y WiFi) y tecnologías celulares predeterminadas (por ejemplo, 3G, 4G).

Muchos operadores esperan implementar 5G FWA a principios de la era 5G para proporcionar banda ancha en regiones rurales/suburbanas, o para proporcionar una alternativa de precio competitivo a la banda ancha fija. Esta oportunidad existe, pero de ninguna manera es universalmente accesible para los operadores en todos los mercados. Como tal, 5G FWA debe verse como una oportunidad que depende en gran medida de las realidades locales.

Hay cuatro productos FWA principales que los operadores pueden ofrecer a nivel mundial, como se muestra en la figura siguiente. Además, dado que la oportunidad de FWA no es universal, esta sección enmarca la discusión en función de los diferentes escenarios de mercado en términos de atractivo para FWA.

FWA PRODUCT OFFERINGS FOR OPERATORS

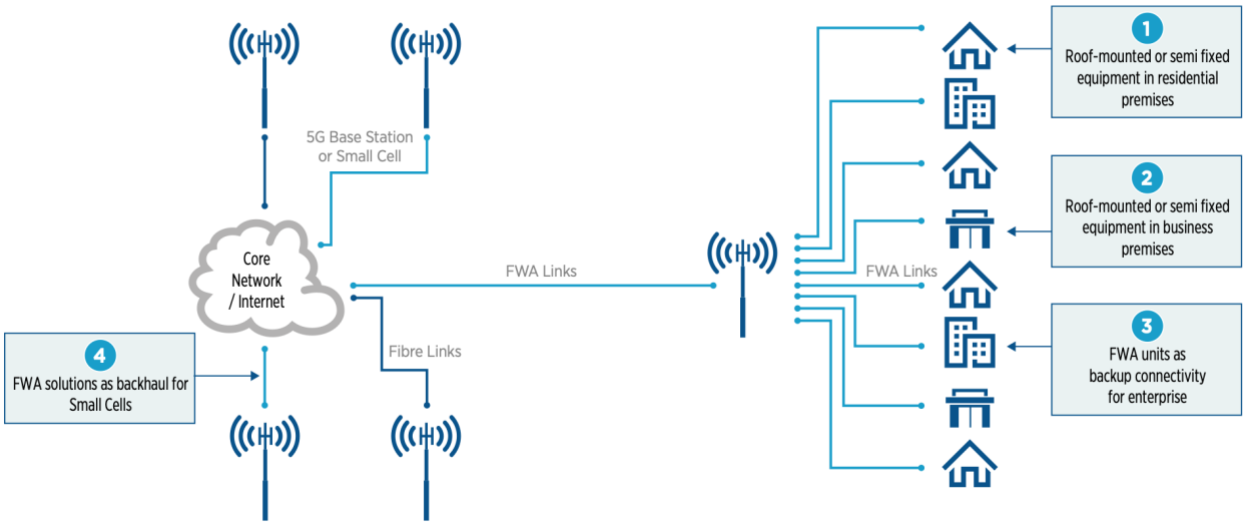


Imagen tomada del documento: THE 5G GUIDE A REFERENCE FOR OPERATORS

(1) Equipos fijos o semi fijos en locales residenciales

(2) Equipos fijos o semi fijos en locales comerciales

(3) Unidades FWA como conectividad de respaldo para empresas

(4) Soluciones FWA como backhaul para Small Cells

3.6.1.1 Banda ancha para los desconectados

Los operadores pueden abordar las demandas de banda ancha:

- instalaciones que no estaban conectadas anteriormente o que solo están conectadas con banda ancha de cobre/DSL heredada
- demandas de banda ancha de tiempo limitado (por ejemplo, estacionales)
- demandas de IoT.

Para los operadores de telefonía móvil, FWA es una oportunidad para las soluciones como backhaul para ingresar a nuevos mercados de banda ancha, obteniendo acceso a nuevos grupos de valor.

Para muchos operadores fijos/móviles con el compromiso de proporcionar servicios de banda ancha de alta velocidad a instalaciones rurales y suburbanas, FWA ofrece una economía de costos competitiva en comparación con las implementaciones FTTx totalmente nuevas, especialmente en regiones en desarrollo donde la baja penetración de la fibra y las costosas obras civiles para la densificación de la fibra favorecen la conectividad inalámbrica.

Dos conceptos nuevos que se comenzaron a emplear sobre los tendidos de telecomunicaciones son:

- Brownfield: Zonas donde ya hay instalaciones de voz y/o datos sobre cables de cobre.

- **Greenfield:** Zonas de nueva o reciente construcción, donde aún no existe cobre.

FWA ES UNA ALTERNATIVA DE MENOR COSTO QUE GREENFIELD FTTX

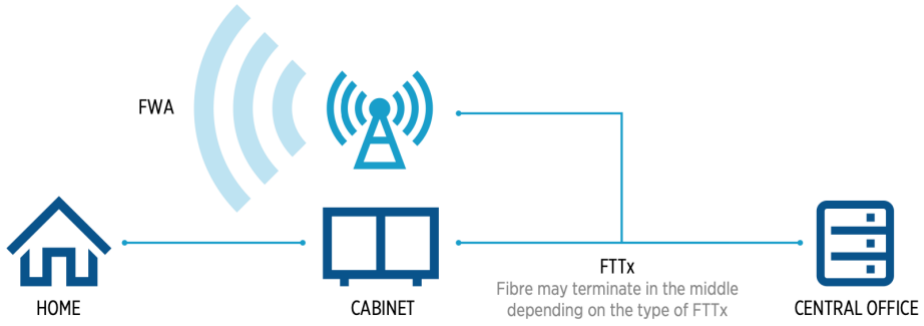
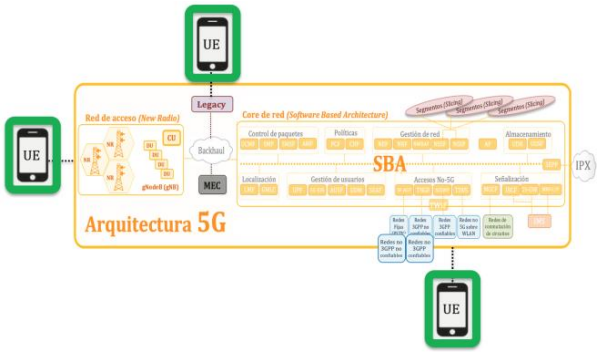


Imagen tomada del documento: THE 5G GUIDE A REFERENCE FOR OPERATORS

UE (User Equipment)



Temas a desarrollar en esta sección.

- a. UICC 4G heredado con aplicación USIM
- b. 4G UICC actualizado con la aplicación USIM
- c. 5G UICC con aplicación USIM

Antes de entrar en detalle sobre la tecnología 5G, recordemos brevemente que las USIM actuales tienen incorporados tres algoritmos criptográficos que provienen desde GSM:

- **A3**: Autentificación de la tarjeta SIM ante la red.
- **A5**/0, A5/1, A5/2 y A5/3: Algoritmos de cifrado de voz entre el teléfono y la estación base GSM.
- **A8**: Algoritmo de generación de clave para los algoritmos A5.

Estos procedimientos de manejo de claves critpográficos han sufrido diferentes tipos de ataques, cuyos resultados son la obtención de claves de usuario, la intercepción y falsificación de llamadas, la obtención de información y localización del UE, ataques del hombre del medio, negación de servicio, etc.

A lo largo de los años que lleva la telefonía móvil, han ido mejorando la fortaleza criptográfica de los mismos, pero hasta 4G inclusive hay aspectos que debían ser mejorados, en particular lo referido a ataques del hombre del medio e integridad.

En el Capítulo "1.2. La red móvil" del libro: "Seguridad en Redes" puede ampliarse este tema.

La seguridad 3GPP tiene un fuerte enfoque en el escenario de ataque, en el que, solo el equipo de usuario autorizado (UE) puede acceder y utilizar los servicios proporcionados por un determinado segmento de red. A tal efecto, **3GPP TS 29.531** define una función de selección de segmento de red (**NSSF**: Network Slice Selection Function), que contiene la **NSSAI** (Network Slice Selection Assistance Information). Este NSSAI es esencialmente una lista de identidades de segmentos, es decir, es una lista de S-NSSAI. Un caso de uso vertical común es que un UE tendría acceso a una red de datos específica, como una red privada o una red empresarial. La información de suscripción de los **UE** para cada segmento también contendría diferentes Nombres de red de datos (**DNN**: Data Network Names) que identifican las redes de datos a los que los UE pueden acceder y que pertenecerían a "sus" segmentos.

Los **DNN** son el equivalente 5G de los nombres de puntos de acceso (**APN**: Access Point Names) para 4G, y para implementaciones verticales, estas podrían ser la red de la empresa o una red privada específica. Un **UE** está preconfigurado o provisto con un **NSSAI** predeterminado, que podemos recordar que es un grupo de **S-NSSAI** (Single- **NSSAI**) de su "Home network".

Un UE puede utilizar servicios de varios segmentos, por ejemplo, una red privada o Internet. Si el **UE** está en roaming, la red "Home" puede tener la NSSAI para la red visitada ya configurada en ella. Si no existe dicha lista, se utiliza el NSSAI de la red "Home". Si el UE tiene configurada la NSSAI para la red visitada, que la red visitada no reconoce, entonces la red visitada puede actualizar los segmentos NSSAI permitidos con un mapeo de sus propios S-NSSAI correspondientes (identidades de segmento), por ejemplo, basado en SST. Las interacciones en torno a la seguridad de roaming específico de cada segmento han sido definidas recientemente por GSMA en NG.113.

La identidad del segmento **S-NSSAI** es la piedra angular clave para autenticar y autorizar el acceso del UE a un segmento. Hay dos tipos de mecanismos para controlar el acceso de UE a un segmento:

- Acceso simple al segmento realizado durante el registro del UE.
- Segmento de acceso específico que requiere un paso de autenticación adicional (por ejemplo, para el acceso a la Intranet de una red privada).

El primero se basa únicamente en la autenticación de red "normal" y las identidades de segmento (S-NSSAI), y también es el método utilizado cuando un UE está en roaming.

El segundo está destinado a utilizar autenticación adicional mediante el Protocolo de autenticación extensible (**EAP**: Extensible Authentication Protocol). Un caso de uso típico para los mecanismos de autenticación adicionales sería que una empresa desea tener un paso de autenticación adicional antes de que un UE pueda acceder a la red empresarial y, por lo tanto, exista un servidor de autenticación para la autenticación EAP

UICC y USIM

El concepto de **SIM** (subscriber Identity Module) nace con 2G como la tarjeta inteligente (Smart Card) que se emplea en los equipos de telefonía móviles y representa el software y hardware embebidos en esta tarjeta.

Por razones de seguridad, a partir de la tecnología **3G** se separa el software del hardware dando origen al concepto de **USIM** (Universal SIM), este USIM es parte de las aplicaciones de software que residen físicamente en ese hardware que ahora llamaremos **UICC** (Universal Integrated Circuit Card)

Estas tarjetas USIM, como todos los diseños de telefonía móvil, se van regulando a través de las diferentes "Releases" (versiones) que genera 3GPP. Nos interesa tomar como punto de partida la conocida "**Release 99+"** que introduce varias mejoras de seguridad para las USIM, las cuáles permiten inclusive la integración con las redes 5G, aunque esto no habilita aún la máxima seguridad que se busca con 5G. Las tarjetas anteriores al Release 99+ **NO** son compatibles con 5G.

Otro concepto importante relacionado con las USIM compatibles con el Rel-99+ es que algunas permiten su actualización vía Over-the-air (**OTA**) y otras no. Las que lo permiten, facilitan el cálculo del **SUCI** (Subscription Concealed Identifier) que como su nombre lo indica

"oculta" (Concealed) el identificador de usuario en la interfaz radio (generando privacidad del subscriptor). Las que NO permiten actualizaciones vía OTA, lo que hacen es un cálculo llamado "null-scheme" (Esquema nulo), que en realidad es ficticio y **NO** oculta el **SUPI** en la interfaz aire.

Tengamos en cuenta que los factores clave que busca 5G son: Integridad, Autenticación, confidencialidad, privacidad y anti réplica.

Ya hemos hablado en párrafos anteriores del **SUPI** (Subscription Permanent Identifier), el cual NUNCA debería salir del **UE** (User Equipment). El tratamiento de este SUPI, puede ejecutarse de dos formas:

- Heredado del **IMSI**.
- Nuevo de 5G **NAI** (Network Access Identifier)

Además, 5G proporciona al menos dos métodos de autenticación y acuerdo de clave (AKA: Authentication and Key Agreement) para acceder a la red.

- **5G AKA** (evolución del método de autenticación en 4G).
- **EAP-AKA'** (Extensible Authentication Protocol-AKA: método adoptado en 5G para un uso de EAP, incorpora el Serving Network Name:SNN,y fuerza el empleo de SHA256)

Los dos anteriores son de soporte obligado en dispositivos 5G, pero a su vez habilita también otras opciones como por ejemplo **EAP-TLS** (EAP-Transport Layer Security).

Analicemos con más detalle el **SUPI**. El mismo se especifica en el TS_23.501, en el punto 5.9.2 "Subscription Permanent Identifier". En este documento, de forma similar al IMSI de tecnologías anteriores, para redes 5G se establece que "Se asignará un SUPI 5G único a nivel mundial a cada suscriptor en el sistema 5G y se proporcionará en el UDM/UDR (Unified Data Management/Unified Data Repository)".

El SUPI puede contener:

- una IMSI según se define en **TS 23.003**, o
- un identificador específico de la red, (NSI: Network Specific Identifier) utilizado para redes privadas como se define en **TS 22.261**.
- un GLI (Global Line Identifier) y un identificador de operador del operador 5GC, utilizado para soportar FN-BRG, como se describe con más detalle en **TS 23.316**.
- un GCI /Global Cable Identifier) y un identificador de operador del operador 5GC.

Para habilitar escenarios de itinerancia, el SUPI deberá contener la dirección de la home network. Para el interfuncionamiento con el **EPC** (Evolved Packet Core - Core de 4G), el SUPI asignado al UE siempre se basará en un IMSI para permitir que el UE presente un IMSI al EPC.

El **TS_33.501**, a partir de los puntos 5.2 "Requirements on the UE" y 5.3 "Requirements on the gNB" se describen con todo detalle el uso de mecanismos de cifrado entre el UE y la red en la interfaz aire, incorporando nuevos métodos para evitar los problemas detectados en las generaciones anteriores.

Los dispositivos y/o funciones que participarán en todo este proceso son:

- **AMF** (Access and Mobility Management Function)
- **SEAF** (security anchor function): Provee la función de autenticación, vía AMF a la red de servicio.
- **UDM/ARPF** (Unified Data Management/Authentication credential Repository and Processing Function(ality))
- **UDR** (Unified Data Repository)
- **SIDF** (Subscription identifier de-concealing function): Vuelve a descifrar el SUPI desde el SUCI
- **AUSF** (Authentication server function) Controla la autenticación para redes 3GPP y No 3GPP. Informa al UDM si la autenticación del subscriptor fue exitosa o no.

El mismo documento en su punto 6.1 "Primary authentication and key agreement" describe el propósito de esta autenticación primaria como la autenticación mutua entre la red y el UE y la provisión del material de claves necesarios para ser usados a posteriori. Este material, da como resultado la clave de "anclaje" **K_{SEAF}** provista por el **AUSF** de la "home network". Más claves pueden ser derivadas luego de **K_{SEAF}** sin la necesidad de una nueva autenticación. Esta clave **K_{SEAF}** se deriva de una clave intermedia llamada **K_{AUSF}**

Presentación del Documento: "**3GPP R15 5G SIM Card: A Definition**"

Tarjetas SIM.

Si bien la **UICC 5G** permite que un dispositivo se autentique en la red 5G, tiene algunas capacidades adicionales, definidas para diferentes esquemas de implementación 5G.

SIMalliance ha identificado tres tipos diferentes asociados de 5G UICC:

- SIM de transición: proporciona las capacidades mínimas para autenticarse en la red, pero no aprovecha el beneficio de la capacidad del core 5G.
- SIM 5G: aprovecha toda la potencia de 5G. Es la que recomienda SIMalliance, ya que existe una compatibilidad total con versiones anteriores y es la SIM más preparada para el futuro.

  SIM de bajo consumo: optimizado para casos de uso de IoT de bajo consumo en los que se pueden utilizar NB-IoT y LTE.