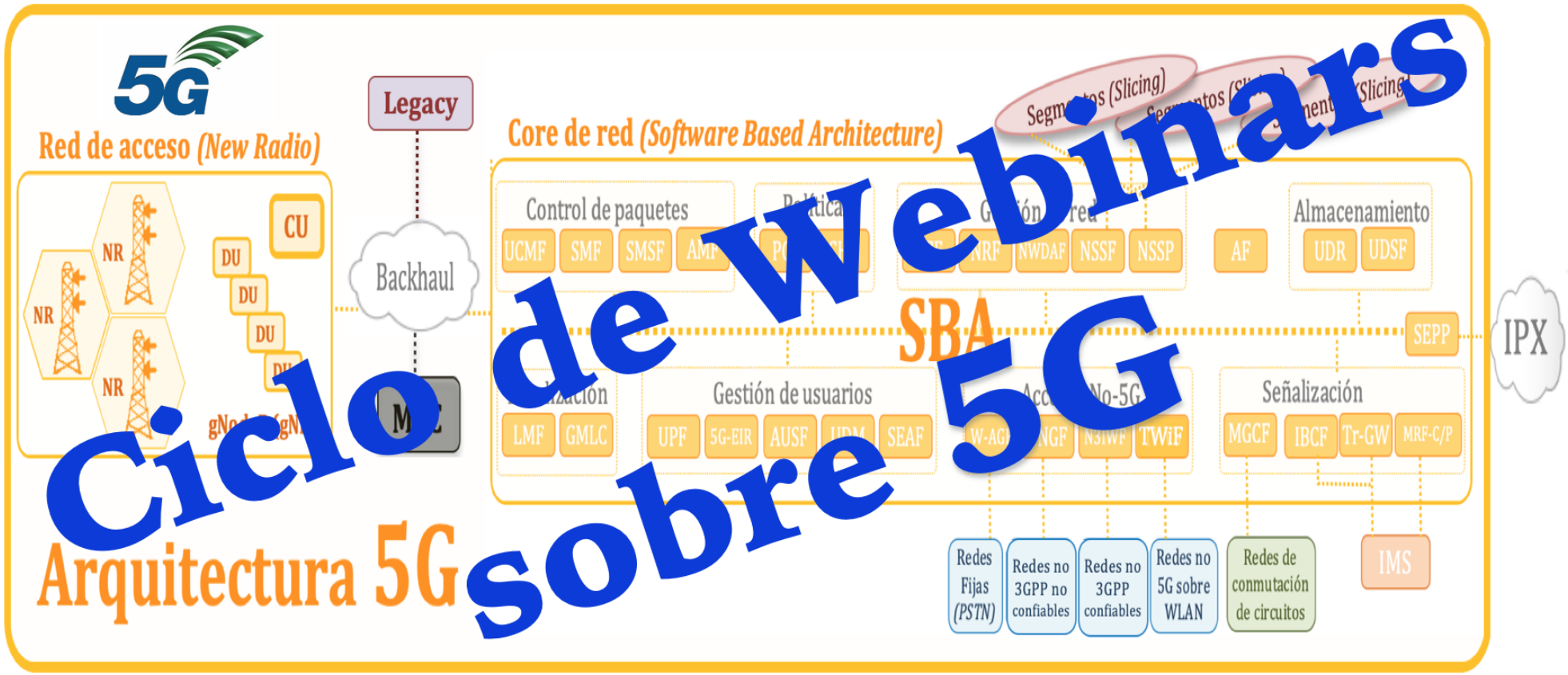
Tema 5: Seguridad en 5G



Ciclo de Webinars sobre 5G

Alejandro Corletti Estrada

acorletti@darFe.es

www.darFe.es

Ciclo de Webinars sobre 5G

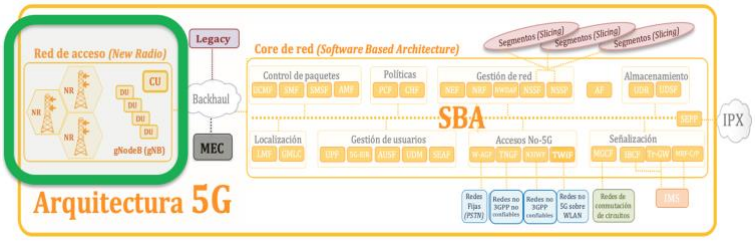
Tema 5: Seguridad en 5G

DESARROLLO DEL CICLO DE WEBINARS

Webinar 1: Presentación y evolución de las tecnologías móviles

Webinar 2: New Radio y gNodeB

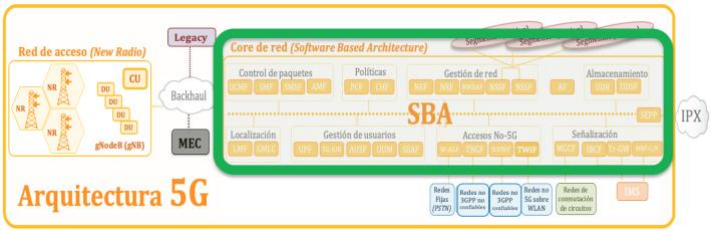
- Descripción de diseño de los gNB
- Open RAN
- Antenas compartidas (RAN Sharing)
- Frecuencias licitadas y asignadas
- Empleo de Cloud



Webinar 3: SBA, MEC y Slicing

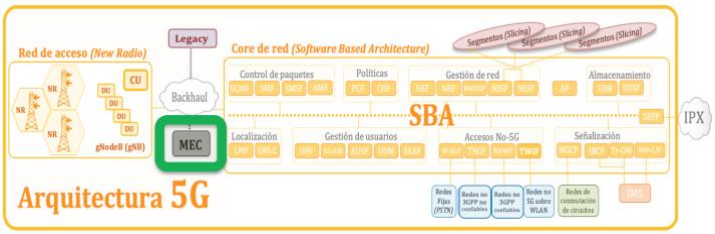
SBA (Core 5G) (Service Based Architecture)

- 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



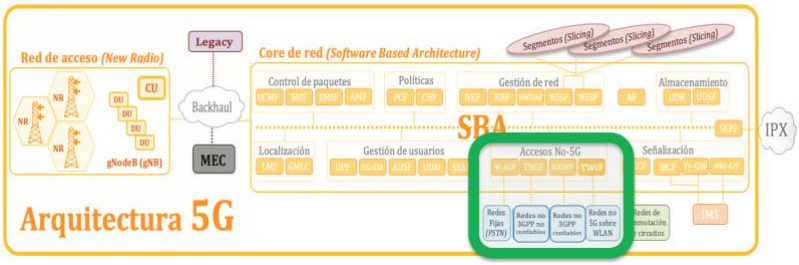
Slicing (Segmentos)

- **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

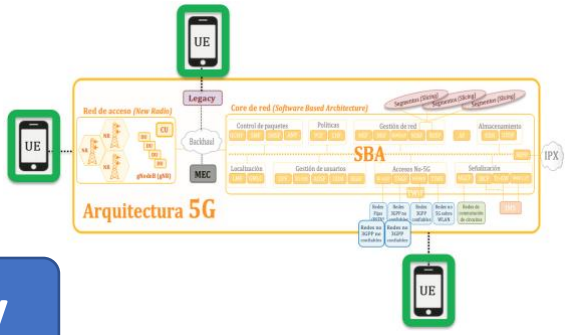
Otros accesos

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



Accesos UE (User Equipment)

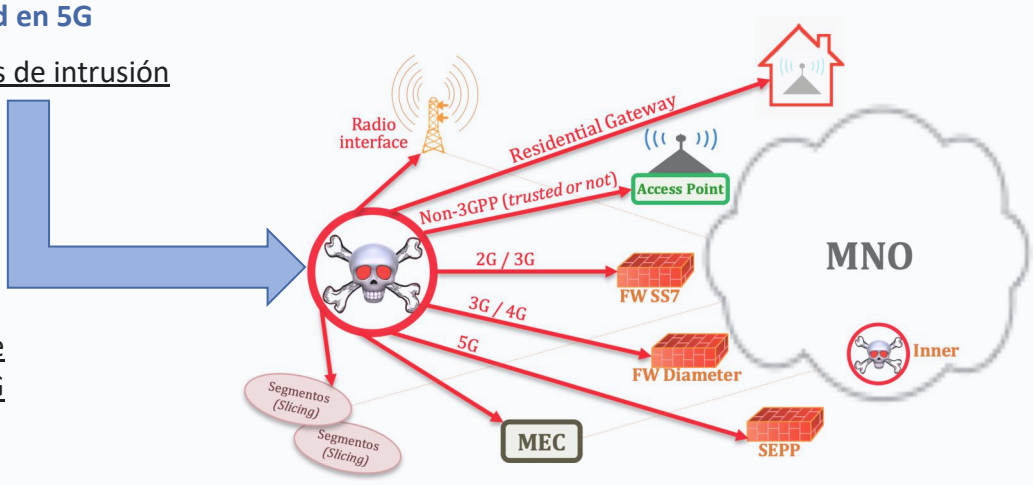
- a. UICC 4G heredado con aplicación USIM
- b. 4G UICC actualizado con la aplicación USIM
- c. 5G UICC con aplicación USIM



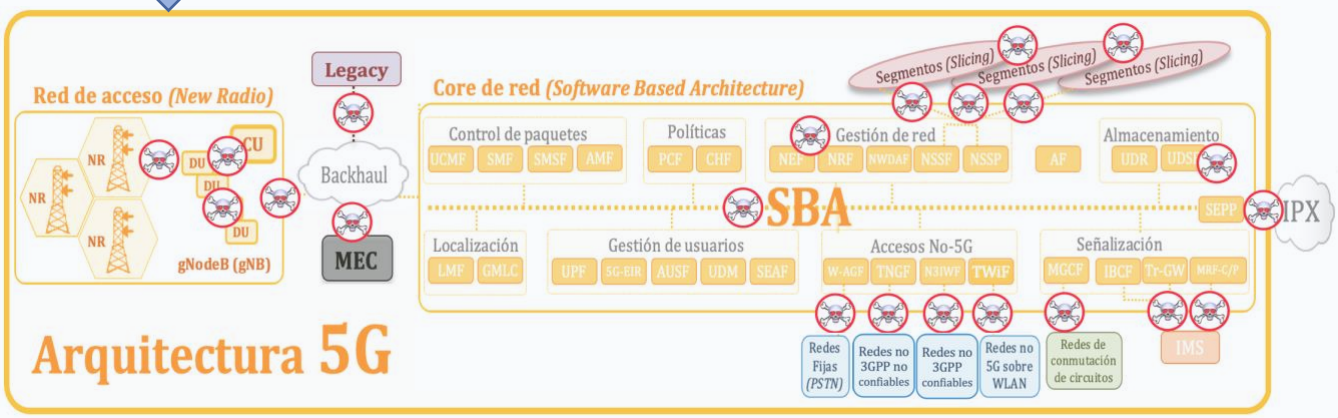
Tema de hoy

Webinar 5: Seguridad en 5G

Vectores de intrusión



Puntos clave de seguridad en 5G



Novedades de seguridad en 5G:

- Autenticación mutua y marco unificado para las diversas tecnologías y dispositivos de acceso 5G.
- A diferencia de LTE, en **5G** existe una segunda autenticación.
- Protección de la privacidad del usuario en la interfaz aire.
- Fortalecimiento de los algoritmos criptográficos.
- Robustecimiento en la gestión y jerarquía de claves.
- Hincapié en evitar ataques tipo "bidding down" o puja hacia abajo.
- Mejor segregación entre planos de control y de usuario.
- Empleo de protocolos nuevos a nivel transporte y aplicación: **APIRestfull**, **JSON**, **DTLS**, **OAuth2, QUIC**.
- Control extendido de la "Home Network" para usuarios de roaming.
- Introducción del **SEPP** (Secure Edge Protection Proxy) como protección de IPX.
- Introducción del **SCP** (Service Communication Proxy) para la seguridad entre funciones de red (NF: Network Function)
- Segmentos (Slicing)
    - Estándar: URLLC – eMBB – V2x – mMTC
    - Otros: MVO, redes privadas, streaming…

Referencias y/o estándares sobre aspectos de seguridad en **5G**

El documento **TS 33.501** presenta una nueva arquitectura de seguridad que incluye:

I. Seguridad de acceso a la red: 3GPP y No3GPP.
II. Seguridad en el dominio de red: Seguridad en plano de usuario y plano de control.
III. Seguridad en el dominio de usuario: Acceso de UE.
IV. Seguridad en el dominio de aplicaciones: intercambio seguro de mensajes.
V. Seguridad en el dominio SBA: Registro, descubrimiento, autorización y protección del SBI.
VI. Seguridad en la visibilidad y configuraciones.

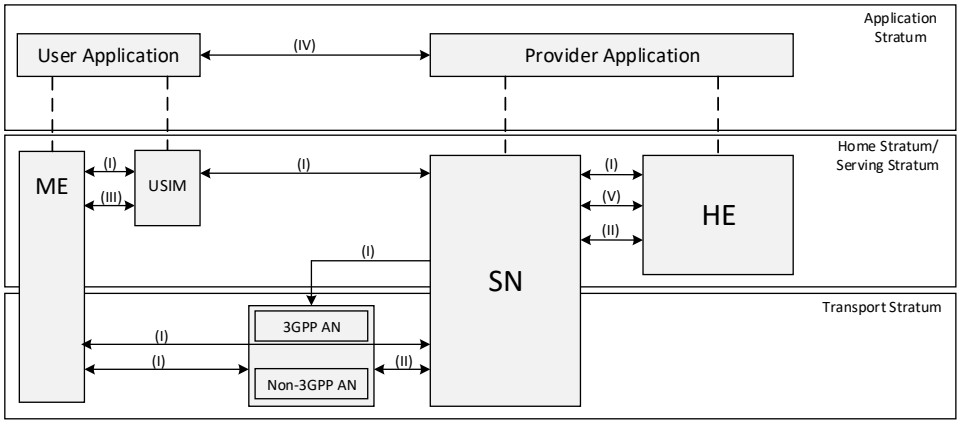


Figure 4-1: Overview of the security architecture, tomada de 3GPP TS 33.501

Jerarquía de claves

Después de una autenticación primaria exitosa entre el **ME** (Mobile Equipement) y la red, se deriva de "**K**" la clave de anclaje específica de la red de servicio (**KSEAF**: serving network specific anchor key).

Esta **KSEAF**, se empleará como anclaje para protección de integridad y confidencialidad (en AS y NAS) en el plano de control y el de usuario (**CP** y **UP**).

Esta jerarquía de claves de 5G incluye:

- K
- Cipher Key (CK)
- Integrity Key (IK)
- KAUSF
- KSEAF
- KAMF
- KNASint
- KNASenc
- KN3IWF,
- KgNB
- KRRCint
- KRRCenc
- KUPint
- KUPenc

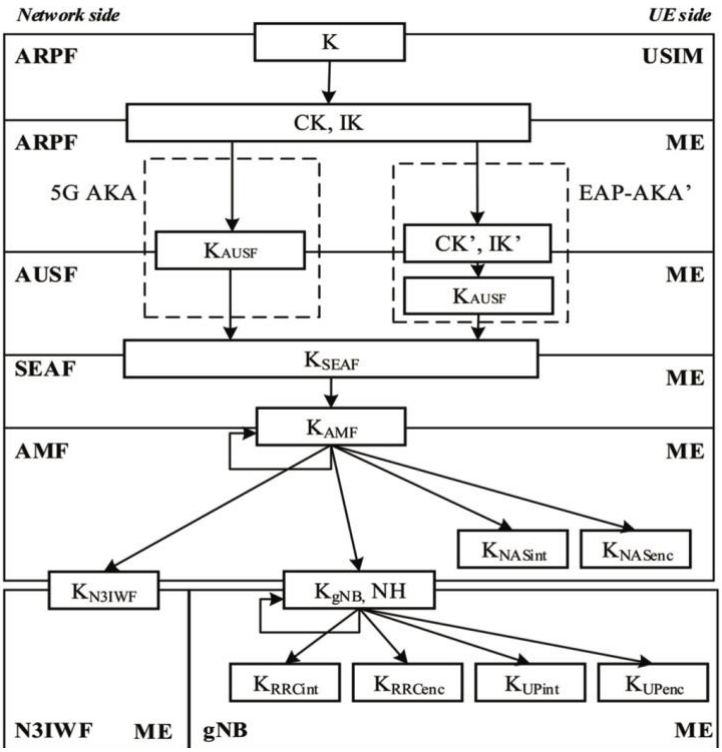


Figure 6.2.1-1: Key hierarchy generation in 5GS, tomada de 3GPP TS 33.501

Acceso a la red y privacidad

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** (User Equipment) debe hacer llegar el identificador permanente de suscripción (**SUPI**: subscription permanent identifier). 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 la generación de claves, cifrando el **SUPI** antes de transmitir utilizando una **clave pública** de la "Home network" que se almacena en el **USIM** (Universal Subscriber Identity Module).

5G se basa en que el identificador de suscripción **SUPI**, por contener información sensible de abonado y de suscripción no debe transferirse en texto claro. Para proporcionar **privacidad**, el **UE** genera y transmite el Identificador oculto de suscripción (**SUCI**: Subscription Concealed Identifier) utilizando un esquema de protección de calve asimétrica, basado en el Esquema de cifrado integrado de curva elíptica (**ECIES**:

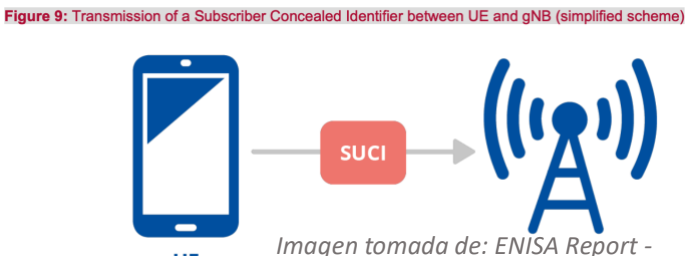


Imagen tomada de: ENISA Report - Security in 5G Specifications.pdf

Elliptic Curve Integrated Encryption Scheme), con la clave pública que se proporcionó de forma segura desde la "home network" del operador.

Únicamente en llamadas de emergencia no autenticadas, no se requiere protección de privacidad.

Hasta 4G, la "Home network" **tenía que confiar en la red visitada** a través de la cual se realizaba la autenticación.

Interfaces F1 y E1

Como ya hemos mencionado en el **Webinar 2**: "**New Radio y gNB**". La comunicación entre **DU** y **CU** se establece mediante la interfaz **F1.** Además, las CU se comunican entre sí a través de la interfaz **E1.** El tráfico transmitido a través de estas interfaces puede transportar datos confidenciales y, por tanto, es un objetivo para los atacantes. Por lo tanto, la especificación exige **confidencialidad**, **integridad** y **anti réplica** para los datos del plano de control intercambiados a través de estas interfaces, aunque se dejan algunas **opcionales** a los operadores, que analizaremos más adelante.

Figure 11: Interfaces between components of the split RAN and 5G Core (simplified scheme)

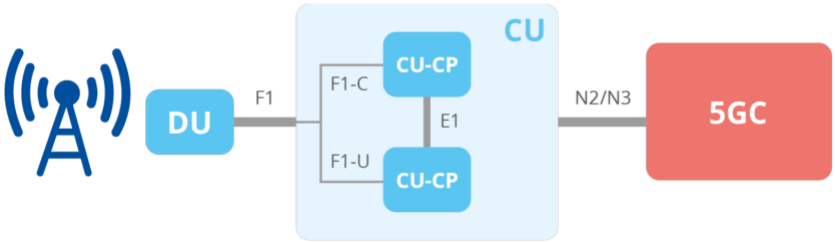


Imagen tomada de: ENISA Report - Security in 5G Specitications.pdf

En las especificaciones de seguridad 3GPP (***TS 33.501**: V17.1.0 "Security architecture and procedures for 5G system" (Release 17 - 2021-03*)), los requisitos para la protección de las interfaces internas de la estación base (**gNB**) que soportan la arquitectura dividida se establecen en la cláusula 5.3.9 y 5.3.10 y los mecanismos de seguridad adicionales se detallan en las Cláusulas 9.8.1 y sub-cláusula 9.8.2, para las interfaces F1 y E1. En ambos casos, el soporte de IPSec es obligatorio. Los requisitos de implementación concretos se proporcionan en la Cláusula 9.1, subcláusula 9.1.2, especificando que el protocolo **IPSec ESP** de acuerdo con **RFC 4303** según lo perfilado por **TS 33.210** (***TS 33.210** V16.4.0 "Technical Specification Group Services and System Aspects;Network Domain Security (NDS); IP network layer security (Release 16 - (2020-07)*) y la autenticación basada en certificados **IKEv2** debe ser usada.

Con respecto a la protección de la interfaz **E1**, que se utiliza para señalizar la transferencia de datos, el requisito simplemente establece que "la interfaz E1 entre CU-CP y CU-UP estará protegida por **confidencialidad**, **integridad** y **anti réplica**" sin enumerar explícitamente más comentarios o exclusiones.

En el mismo Webinar, también comentamos que **5G** separa desde la misma interfaz radio, el **plano de control** y el de **usuario** y **ambos** deben estar securizados.

El uso de un cifrado fuerte para la protección entre el **UE** y la estación base no es nuevo. En las redes **4G** actuales, el

Figure 10: Transmission of user and signalling data between UE and gNB (simplified scheme)

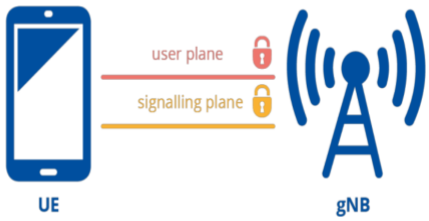


Imagen tomada de: ENISA Report - Security in 5G Specifications.pdf

cifrado del tráfico entre la estación móvil y eNodeB se puede implementar para la protección de la confidencialidad y la integridad de los datos intercambiados entre **UE** y **MME** (MME: Mobility Management Entity). En las redes 5G se aplican requisitos similares. Al igual que en el caso de 4G, algunos de estos requisitos son opcionales. La novedad que viene con **5G** es la protección de la integridad de los datos del plano del usuario, pero esto también es opcional.

La protección de la integridad es **obligatoria** solo para el plano de señalización (señalización RRC y señalización NAS), mientras que es **opcional** para el plano de usuario.

ENISA (European Union Agency For Cybersecurity)

En diciembre de 2018, la UE adoptó un nuevo conjunto de reglas de telecomunicaciones, el Código Europeo de Comunicaciones Electrónicas (**EECC**) 4. Una parte importante del EECC es la protección del consumidor y la seguridad de las comunicaciones electrónicas. El **artículo 40** de la EECC contiene requisitos de seguridad específicos para los proveedores de comunicaciones electrónicas.

ENISA publicó el documento: "**Security in 5G Specificationes (February 2021**)" de **ENISA** que se resumirá a continuación sobre los aspectos claves a considerar:

1.2 FINALIDAD Y OBJETIVOS DEL DOCUMENTO

Una de las medidas técnicas, **TM02** (technical Measure 02 del EEEC), llama a las autoridades pertinentes de los Estados miembros de la UE a que garanticen y evalúen la implementación de las medidas de seguridad en los estándares 5G existentes (específicamente, 3GPP) por parte de los operadores y sus proveedores.

Para mayor comodidad, se proporciona el texto completo del TM02, directamente como se indica en la "Toolbox":

> *"Asegurarse de que los MNO y sus proveedores implementen las medidas de seguridad existentes en los estándares de tecnología 5G relevantes (por ejemplo, 3GPP) y que se utilice como una línea de base de seguridad mínima para los MNO, a fin de garantizar que también las partes opcionales de estos estándares, relevantes para la seguridad, se implementan adecuadamente ".*

Este documento se centra principalmente en la especificación técnica **3GPP TS 33.501**, que es la especificación técnica de seguridad central para redes 5G.

Los acrónimos utilizados en la imagen anterior son los siguientes:

ME=Mobile Equipment

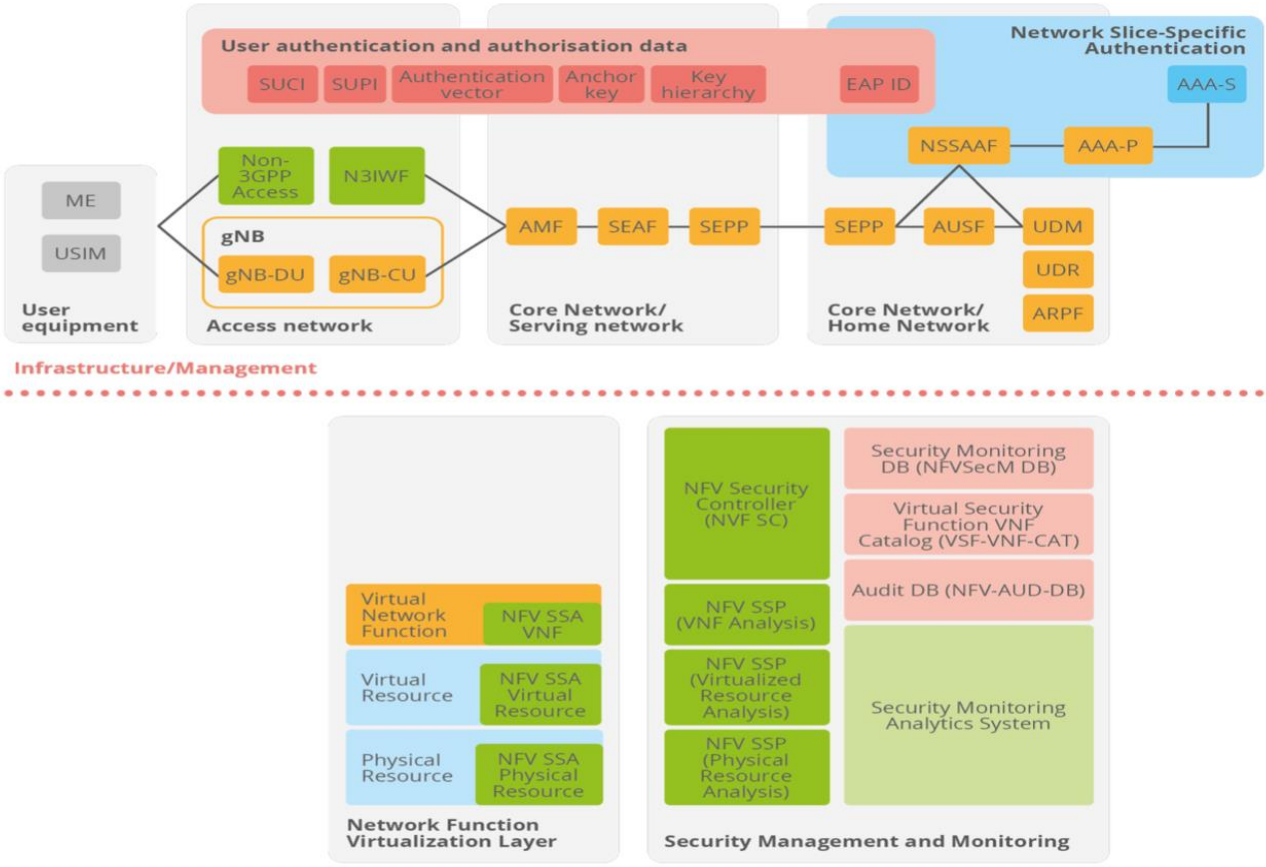
SN=Serving Network

HE=Home environment

Otra vista de la arquitectura de seguridad 5G se presenta y describe en detalle en el panorama de amenazas de **ENISA** para redes 5G (en adelante, "**ETL5G**"). Para completar y facilitar la referencia, incluimos el diagrama arquitectónico de seguridad completo, con la observación de que el alcance de este informe se refiere principalmente a los elementos arquitectónicos por encima de la capa de "infraestructura/administración", mientras que la virtualización de

funciones de red y las capas de administración y monitorización de seguridad no se tratan ampliamente en este informe.

Figure 8: Security architecture zoom-in from the ENISA 5G Threat Landscape 2020



Veamos a continuación los aspectos más relevantes del mismo, que como hemos comentado, se basa en el TS 33.501 de 3GPP.

Protección de la confidencialidad (según: "**Security in 5G Specificationes ENISA**" y **TS 33.501**)

Los requisitos para el uso de la protección de la confidencialidad de los datos de señalización y del usuario en el UE se establecen en la cláusula 5.2.2. Estos mismos requisitos se reflejan efectivamente para el gNB, con respecto a los datos de usuario y la señalización RRC (cláusula 5.3.2) y para la AMF, con respecto a la señalización NAS (cláusula 5.5.1).

En todos los casos, la protección de la confidencialidad tanto del usuario como de los datos de señalización se indica como opcional.

Se indican cuatro algoritmos de cifrado que pueden utilizarse para dicha protección de la confidencialidad, que se explican con más detalle en el anexo D de la especificación. Esos algoritmos son:

- **NEA0**: texto plano sin cifrado (por lo tanto, no ofrece protección)
- **128-NEA1** - Cifrado **SNOW** 3G que permite la retro compatibilidad con redes 3G

- **128-NEA2**: cifrado **AES-128 CTR** que permite la compatibilidad con versiones anteriores de redes 4g-LTE
- **128-NEA3**: basado en el cifrado de flujo **ZUC** que es específico para implementaciones 5G

Según la especificación, el UE tiene que implementar el soporte para los primeros tres algoritmos (NEA0, 128-NEA1 y 128-NEA2), mientras que la implementación del soporte para el cuarto algoritmo (128-NEA3) es **opcional**.

Protección de integridad (según: "**Security in 5G Specificationes ENISA**" y **TS 33.501**)

Los requisitos para la integridad de los datos de señalización y del usuario y la protección anti réplica que se utilizarán en el UE se establecen en la cláusula 5.2.3. Estos mismos requisitos se reflejan efectivamente para el gNB, con respecto a los datos de usuario y la señalización RRC (cláusula 5.3.3) y para la AMF, con respecto a la señalización NAS (cláusula 5.5.2).

Sobre la base de estos requisitos, la protección de la **integridad es obligatoria** solo para el plano de señalización (señalización RRC y señalización NAS), mientras que es **opcional** para el plano de usuario.

Se enumeran cuatro algoritmos de protección de la integridad que pueden utilizarse para dicha protección, que se explican con más detalle en el anexo D de la especificación. Esos algoritmos son:

- **NIA0**: texto plano sin cifrado (por lo tanto, no ofrece protección)
- **128-NIA1** - basado en **SNOW** 3G
- **128-NIA2**: basado en **AES-128** en modo **CMAC**
- **128-NIA3**: basado en **ZUC** de 128 bits

Según la especificación, el UE debe implementar el soporte para los primeros tres algoritmos (NIA0, 128-NIA1 y 128-NIA2), mientras que la implementación del soporte para el cuarto algoritmo (128-NIA3) es **opcional.**

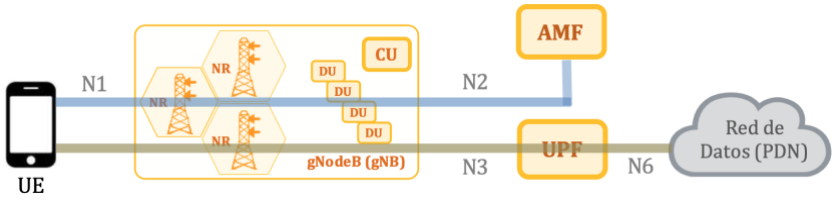
Protección de la instalación y configuración de gNB (según: "**Security in 5G Specificationes ENISA**" y **TS 33.501**)

La cláusula 5.3.4 define los requisitos para la instalación y configuración de gNB, que incluye requisitos sobre cómo los sistemas de operaciones y gestión (O&M) deben instalar y configurar gNB de forma segura. Esencialmente, estos requisitos exigen el uso de **integridad**, **confidencialidad** y protección **anti réplica** para las interfaces entre el sistema O&M y gNB, así como los requisitos para gNB para garantizar que los cambios de software y datos estén autorizados **antes** de la instalación y el uso.

La misma cláusula también indica que el mecanismo de inscripción de certificados (como se especifica en TS 33.310) debe ser compatible con gNB, sin embargo, la decisión sobre el uso real de este mecanismo de inscripción se deja a criterio de los operadores y, por lo tanto, puede considerarse **opcional.**

Interfaces N2 y N3 (según: "**Security in 5G Specificationes ENISA**" y **TS 33.501**)

Las interfaces **N2** y **N3** (también mostradas en la figura anterior) son interfaces que conectan 5G-AN con **AMF** (Access and Mobility Function) y con la **UPF** (User Plane Function), respectivamente.



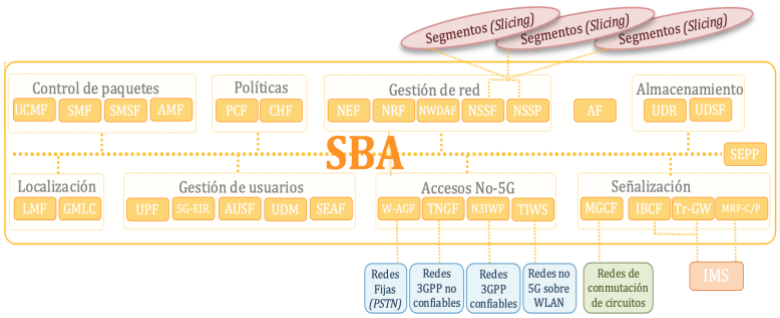
Transportan señales sensibles y datos del plano del usuario entre la red de acceso y el núcleo (core), lo que significa que pueden ser el objetivo de atacantes. Por lo tanto, en la especificación de seguridad 3GPP (TS 33.501), los requisitos de **confidencialidad**, **integridad** y protección anti réplica el transporte de datos del plano de control y de usuario sobre interfaces N2 y N3 se definen en las cláusulas 9.2 y 9.3, respectivamente.

En ambos casos también existe un requisito para implementar la autenticación basada en certificados **IPsec ESP** e **IKEv2**, como se especifica en la subcláusula 9.1.2 de la especificación. Además, la cláusula 9.2 también requiere el soporte de **DTLS** (como se especifica en RFC 6083: "*Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP))*" y se refiere a los perfiles de seguridad para la implementación y el uso de DTLS como se define en la cláusula 6.2 de TS 33.210, aclarando también que el uso de DTLS para la seguridad de la capa de transporte no descarta el uso de otra protección de capa de red, enfatizando la ventaja de **IPSec** en términos de proporcionar ocultación de topología.

Dicho todo esto, vale la pena señalar que en ambos casos, para N2 y para interfaz N3, hay notas dentro de las respectivas cláusulas que dicen que el uso de soluciones criptográficas para proteger N2/N3 **es decisión del operador**.

Protección SBA (según: "**Security in 5G Specificationes ENISA**" y **TS 33.501**)

SBA es esencialmente un marco en el que el plano de control de 5G y los repositorios de datos se implementan mediante un conjunto de funciones de red (**NF**: Net. Functions) interconectadas.



Estas funciones de red se conectan por medio de interfaces basadas en servicios (**SBI**: Service Based Interfaces) a través de un bus de mensajes SBI que implementa **API RESTful** sobre **HTTP/2**.

Desde el punto de vista de la seguridad, dicha comunicación requiere la protección de **confidencialidad** e **integridad** de los mensajes intercambiados, así como un fuerte mecanismo de **autenticación** y **autorización**.

En las especificaciones de seguridad 3GPP (TS 33.501), los requisitos para la seguridad del core de red se definen en la cláusula 5.9. En la sección 13 de la especificación técnica se proporciona una descripción más detallada de los procedimientos y aspectos de seguridad y se hace referencia a ellos en las secciones siguientes.

Otro documento de especificación que es importante es **TS 33.122**, que define los aspectos de seguridad del marco de API común (**CAPIF**: common API framework) para las API de 3GPP. CAPIF se introduce con el propósito de estandarizar la funcionalidad expuesta a través de las API. Esta especificación define varios requisitos de seguridad comunes, relacionados principalmente con la autenticación y autorización, pero también relacionados con el ocultamiento de topología.

Protección en la capa de red o transporte (según: "**Security in 5G Specificationes ENISA**" y **TS 33.501**)

La descripción de los requisitos para los mecanismos de protección en la capa de transporte se proporciona en la Cláusula 13.1. En resumen, las **NF** admitirán **certificados** de cliente y servidor y **TLS**, que está previsto que se utilice para la protección del transporte, mientras que **NDS/IP** se puede utilizar para la protección de la capa de red.

Al observar la posible opcionalidad de la solicitud para usar TLS, puede valer la pena notar que, aunque la cláusula 13.1.0 establece explícitamente que "todas las NF deben admitir TLS", el uso real de **TLS** para la protección del transporte parece **no estar tan estrictamente definido**. En cambio, la cláusula especifica que "**TLS** se utilizará para la protección del transporte dentro de una PLMN a menos que la seguridad de la red se proporcione por otros medios". Esto puede crear un espacio para introducir vulnerabilidades si "**por otros medios**" incluye una protección más débil que la proporcionada por TLS.

Autorización (según: "**Security in 5G Specificationes ENISA**" y **TS 33.501**)

La descripción de los requisitos para la autorización del acceso al servicio **NF** se proporciona en la sección 13.4. El marco de autorización especificado (en las cláusulas 13.4.1 y 13.4.1.0) es el marco **OAuth 2.0** como se especifica en RFC 6749. Los tokens de acceso serán **tokens web JSON** como se describe en RFC 7519 y estarán protegidos con firmas digitales o códigos de autenticación de mensajes (**MAC**: Message Authentication Codes) basado en **JSON Web Signature (JWS)** como se describe en RFC 7515.

Figure 12: Secure communication between network functions in 5G core SBA (simplified scheme)

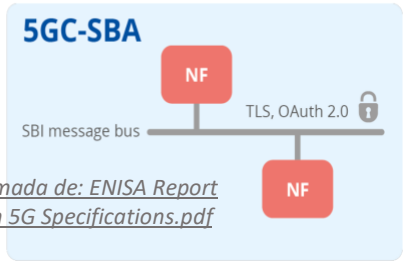


Imagen tomada de: ENISA Report Security in 5G Specifications.pdf

Ocultación de topología (según: "**Security in 5G Specificationes ENISA**" y **TS 33.501**)

El ocultamiento de topología es una característica de seguridad importante que protege las direcciones de los elementos de la red y puede prevenir los ataques destinados al acceso no autorizado o para la interrupción del servicio de la red.

La cláusula 5.9.2.1 de TS 33.501 incluye varios requisitos para el registro, descubrimiento y autorización del servicio SBA, uno de los cuales establece que "el descubrimiento y el registro basados en el servicio NF **podrán** ocultar la topología de los **NF** disponibles/admitidos" entre diferentes dominios de confianza, por ejemplo, entre NF en "home" y NF en la red visitada. Otros requisitos relacionados con la ocultación de topología para la ocultación de topología para API expuestas también se definen en la sección 4.2. del TS 33.122.

Requisitos de almacenamiento seguro para **UE** (según: "**Security in 5G Specificationes ENISA**" y **TS 33.501**)

Para el **UE**, en las especificaciones de seguridad 3GPP (TS 33.501), los requisitos para el almacenamiento seguro y el procesamiento de las credenciales de suscripción se definen en la cláusula 5.2.4. Están relacionados con la protección de la **integridad** y la **confidencialidad** de las claves y credenciales de suscripción, para lo cual es **obligatorio** el uso de un componente de hardware seguro resistente a la manipulación.

Más adelante, en la sección 6.2, se dan los procedimientos relacionados con la jerarquía de claves, la derivación de claves y el esquema de distribución.

Dentro de esa sección, hay una cláusula 6.2.2.2 que incluye procedimientos para manejar claves. Por ejemplo, para la clave pública de la "home network" que se utiliza para ocultar el **SUPI**, se especifica que se almacenará en el **USIM**. Sin embargo, el almacenamiento de KAUSF en el USIM es opcional y también se define la posibilidad de que esta clave también se almacene en una memoria no volátil (dependiendo de la capacidad del UE). Dada la importancia de esta clave, en el último caso existe una dependencia de seguridad de si existe protección y/o cifrado en las ubicaciones de la memoria para garantizar que no se pueda acceder a ellas mediante intentos no autorizados.

Requisitos de almacenamiento seguro para **gNB** (según: "**Security in 5G Specificationes ENISA**" y **TS 33.501**)

Para gNB, los requisitos para el manejo de claves se definen en la cláusula 5.3.5. La cláusula enfatiza la importancia de proteger las claves almacenadas en **gNB**, como el material del llaveros de claves de sesión que también contiene claves a largo plazo utilizadas para la autenticación y la configuración de asociaciones de seguridad. Estos requisitos especifican que cualquier parte de la implementación de gNB que almacene o procese claves en texto sin cifrar **debe estar protegida contra ataques físicos**. Sin embargo, no se dan especificaciones con respecto al tipo y nivel requerido de tal protección. La alternativa indicada es que toda la entidad se coloque en una ubicación físicamente segura y que las claves se procesen en un requisito seguro, que se define en la cláusula 5.3.8. Esto incluye los requisitos para admitir el almacenamiento seguro de datos sensibles, la ejecución segura de funciones sensibles y la ejecución de partes sensibles del proceso de arranque, así como para el control de acceso a dicho entorno.

Requisitos de almacenamiento seguro para **5GC** (según: "**Security in 5G Specificationes ENISA**" y **TS 33.501**)

La cláusula 5.8.1 define requisitos genéricos sobre la Gestión Unificada de Datos (**UDM** Unified Data Management), que incluyen requisitos para las claves a largo plazo utilizadas para los procesos de configuración de asociaciones de seguridad y autenticación. Se especifica que estas claves estarán protegidas contra **ataques físicos** y nunca dejarán desprotegido el entorno de seguridad del Repositorio y Función de Procesamiento de Credenciales de Autenticación/UDM (**ARPF**: Authentication credential Repository and Processing Function). Al mismo tiempo, sin embargo, la cláusula no entra en los detalles de los mecanismos de seguridad para la protección de las credenciales de suscripción en ARPF o Repositorio Unificado de Datos (**UDR**: Unified Data

Repository), ni para la transferencia de dichas credenciales entre ARPF y UDR, indicando que son "**Dejados a la implementación**".

Cuando se trata de la protección de la **Clave Privada** de la "home network", que es el elemento crítico para la eliminación del ocultamiento de **SUCI**, la cláusula 5.8.2 (Requisitos relacionados con la privacidad del suscriptor para UDM y SIDF) incluye el requisito de que la clave debe estar protegida de ataques en la UDM. Al mismo tiempo, sin embargo, la cláusula 6.2.2 (esquema de derivación y distribución de claves) y su subcláusula 6.2.2.1 (claves en entidades de red) también incluyen la siguiente disposición: "El ARPF posee la clave privada de la "home network" que es utilizado por el SIDF para desenmascarar el SUCI y reconstruir el SUPI. La generación y el almacenamiento de este material clave está fuera del alcance del documento".

Propiedades del segmento y atributos de seguridad.

El Grupo de Red de GSMA (**NG**: Network Group) especificó la Plantilla de Segmento Genérica (**GST**: Generic Slice Template) en su especificación NG.116. El GST es un conjunto de características para un tipo de segmento o servicio. Es un conjunto genérico de atributos obligatorios y opcionales. Esos atributos están relacionados con el rendimiento, la tolerancia al retardo, el espectro de radio, etc. NG.116 v2.0 también contiene los siguientes atributos relacionados con la seguridad, que se centran principalmente en el aislamiento físico y lógico/virtual. NG.116 divide el aislamiento en los siguientes 2 tipos principales:

Aislamiento físico

- Aislamiento de procesos y subprocesos
- Aislamiento de la memoria física
- Aislamiento de la red física

Aislamiento lógico

- Aislamiento de recursos virtuales: un segmento de red tiene acceso a un rango específico de recursos que no se superpongan con otros segmentos de la red (por ejemplo, aislamiento de la máquina virtual)
- Aislamiento de red: la función de red está dedicada al segmento y al cliente vertical, pero los recursos virtuales son compartidos.
- Aislamiento de inquilinos/servicios: los datos verticales del cliente están aislados de otros verticales, pero son virtuales los recursos y las funciones de la red son compartidos.

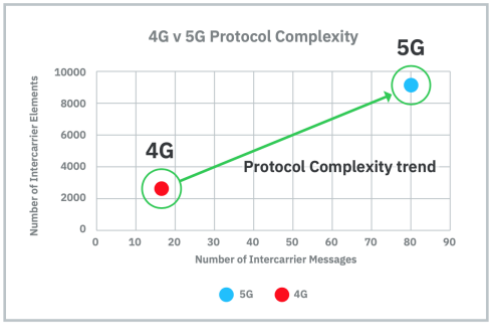
Es importante señalar que el documento NG.116 tiene una vista de extremo a extremo, es decir, no cubre escenarios donde parte de la infraestructura es virtual y parte de las funciones de red son nodos físicos, o donde algunos nodos son compartidos y otros están dedicados a un segmento. Esto significa que no proporciona diferentes políticas para diferentes nodos, sino solo de un extremo a otro para todo el segmento. Queda por ver si los MNO siempre implementarán un escenario de corte completo de extremo a extremo.

El TS 33.501 establece también una nueva figura que es el **SCP** (Service Communication Proxy), el cual participa en escenarios de comunicación indirecta de forma "**opcional**" por parte del MNO, proporcionando de protección entre las NF (Network Functions).

Desafíos de seguridad debido a una mayor complejidad

5G proporciona una gran cantidad de funciones y servicios adicionales a las tecnologías anteriores. Según el documento: "**AMS_Slicing_Security_in_5G_Core_Networks_Whitepaper_1.00.pdf"** de Addpatativa Mobile:

- Hay 4,7 veces más tipos de **comandos** (mensajes) que se pueden enviar entre MNO a través de 5G, en comparación con 4G.
- Más de 3,4 veces más elementos de información (**atributos**) enviados entre MNO a través de 5G, en comparación con 4G.



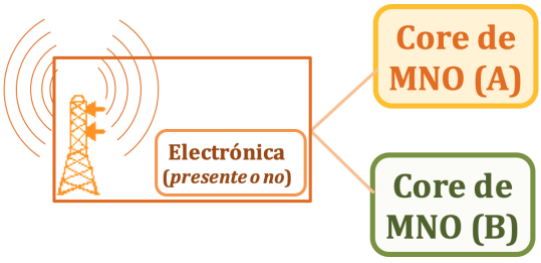
AdaptiveMobile Research: 4G v 5G Complexity

Esto muestra una tendencia de complejidad muy clara entre 4G y 5G. Según estas métricas, 5G es varias veces más complejo. Tiene implicaciones de seguridad obvias porque todos y cada uno de estos comandos deben ser inspeccionados y muchos elementos aprobados para evitar que se envíen actividades ilegales o no deseadas hacia y desde una red. Esto se vuelve más difícil cuanto más comandos y tipos de elementos de información se reciben.

Con todas las nuevas funciones y servicios de red en 5G, el roaming y la interacción heredada se volverán bastante complejos. La configuración será clave, pero asumir que los MNO siempre configurarán todo correctamente es peligroso, especialmente porque saber qué es "correcto" puede no ser posible. Un aspecto destacado en esta sección es el segmento y la configuración, y la capacidad de los segmentos para hacer más de lo que deberían.

Seguridad en RAN Sharing.

Este es uno de los temas más importantes de compartir. Tanto en el tipo pasivo, como activo es necesario contemplar un conjunto de medidas que no pueden ser dejadas de lado.



En RAN Sharing pasivo, el principal control es en la parte física, donde se deberá tener en cuenta un riguroso procedimiento de control de acceso y de ser posible de segmentación física de los recursos de la otra operadora. Es un tema muy frecuente, encontrar en centrales y gabinetes de comunicaciones, el empleo de jaulas, pasillos y hasta accesos diferentes a las instalaciones de personal externo. Por otro lado, también se debe gestionar adecuadamente la supervisión y monitorización de estos accesos y medidas para evitar anomalías o fallos en momentos críticos, y en caso de producirse, contar con las alarmas y mecanismos adecuados de respuesta.

En RAN Sharing activo, el tema es más complicado pues se está abriendo el acceso lógico (y seguramente también físico) a personal que es externo a la operadora, y en la mayoría de los casos competencia.

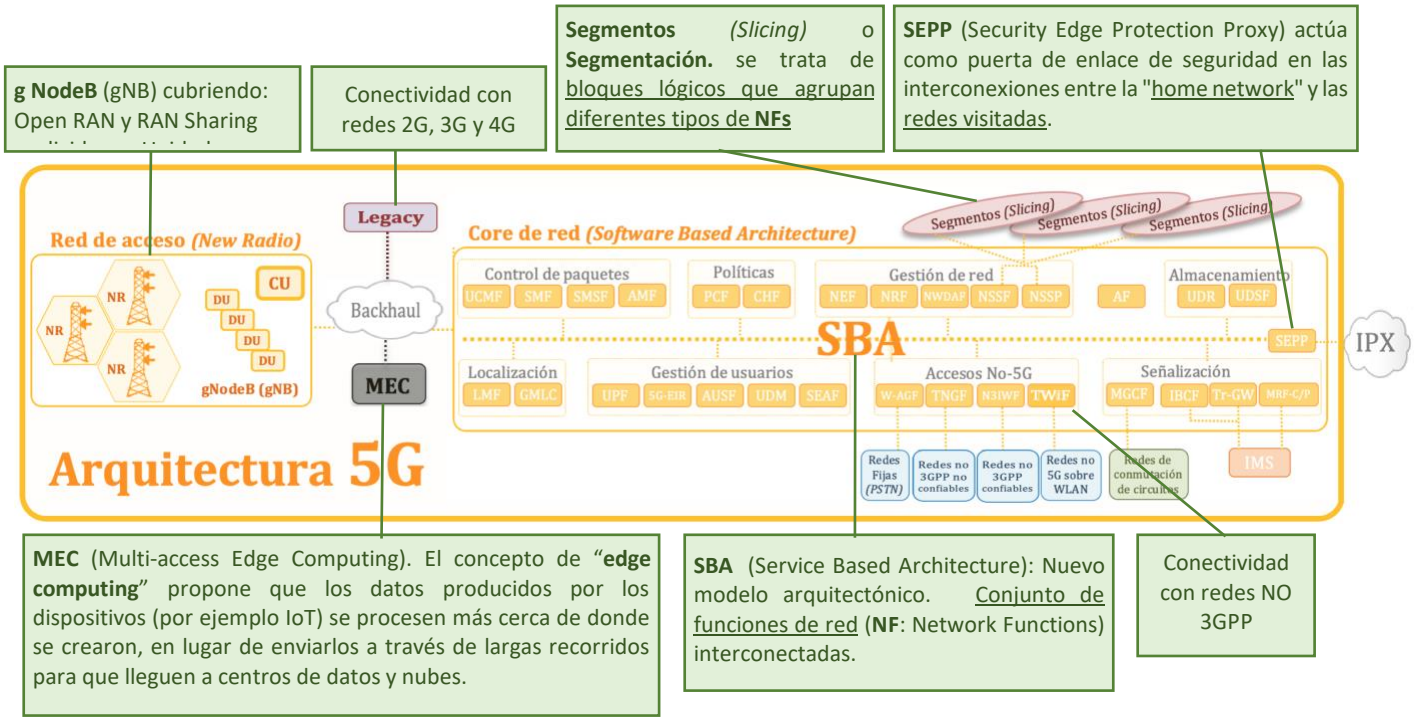
Los controles a considerar deberían ser al menos:

- Robustos procedimientos de gestión de accesos y gestión de usuarios.
- Adecuada segmentación de entornos.
- Supervisión, control y monitorización de actividad.

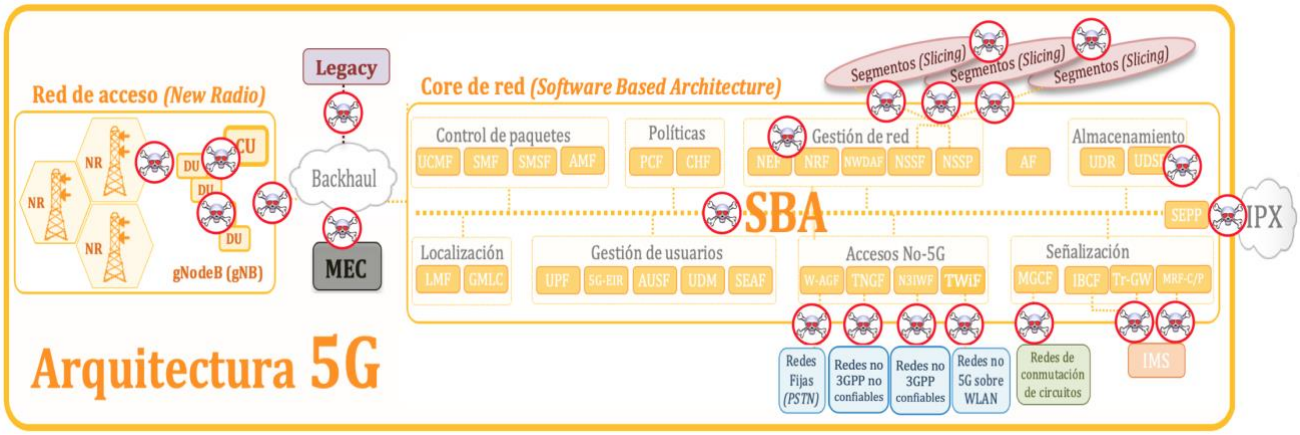
- Estricto empleo de roles y perfiles en las herramientas de Operación y mantenimiento. Control sobre escalado de privilegios y empleo de cuentas con atributos especiales.
- Empleo de un buen sistema de gestión y correlación de Logs.
- Desarrollo y prácticas sobre técnicas forenses.

Aspectos básicos de seguridad sobre la arquitectura 5G.

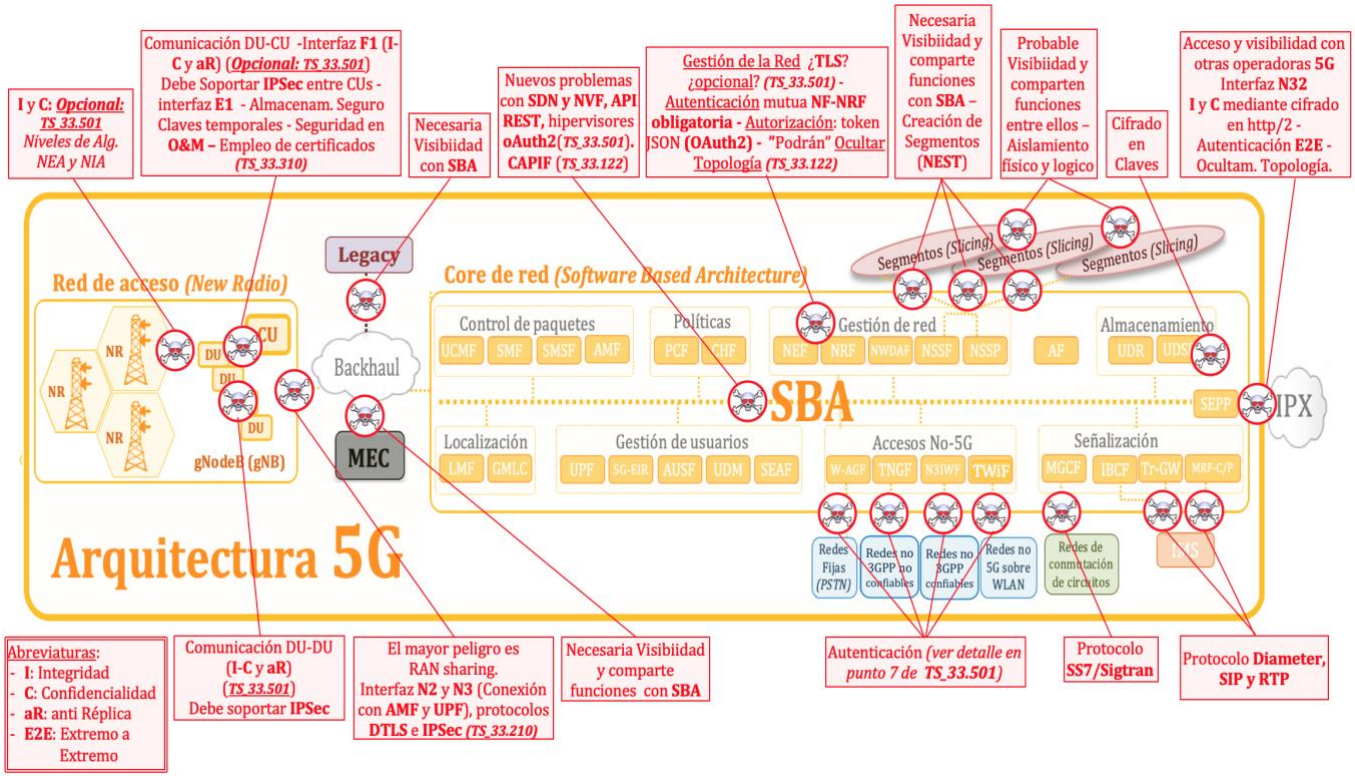
Volvamos a nuestro mapa de la arquitectura de 5G.



En esta arquitectura, podemos definir los siguientes puntos clave.



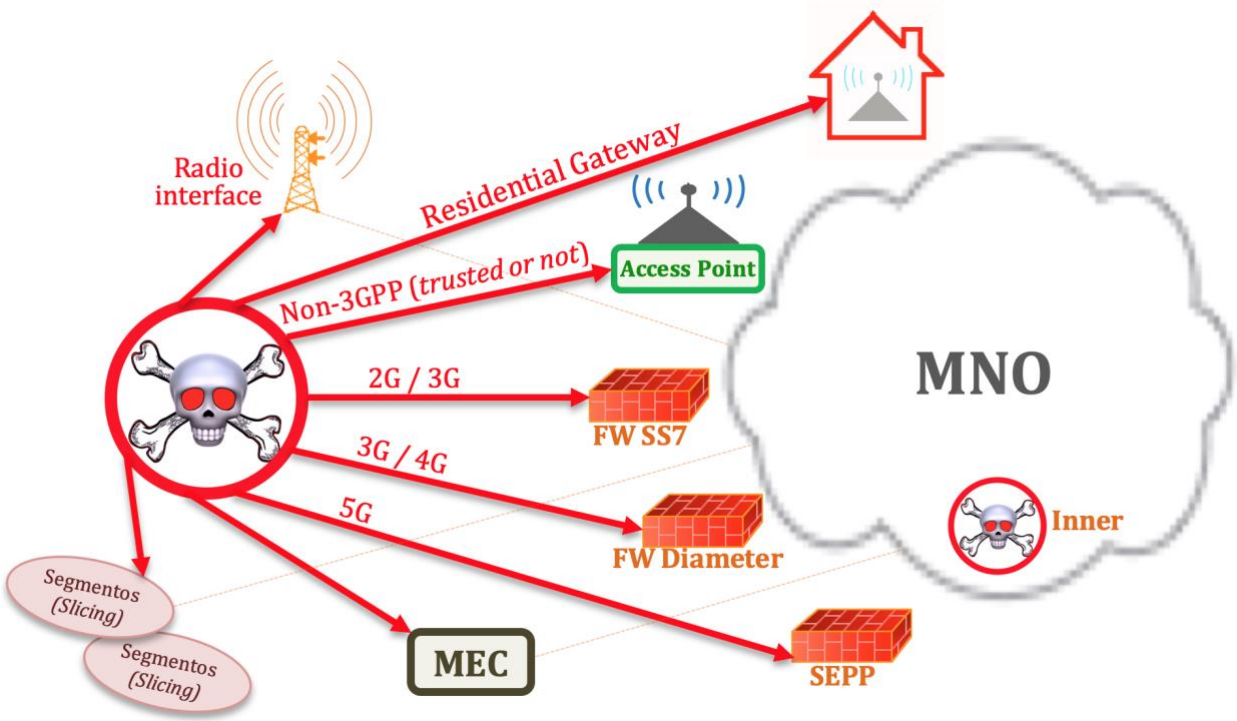
Cada uno de ellos se puede asociar con las referencias que hemos ido desarrollando a lo largo del presente documento.



Vectores de intrusión

A lo largo de la evolución de las redes móviles, se ha ido aprendiendo mucho acerca de medidas de seguridad, y del mismo modo los intrusos fueron mejorando sus estrategias de ataques. En 2G el punto de partida fue la facilidad que "regalaba" el algoritmo A5/0 que no cifraba los datos de usuario con lo que la interfaz radio ofrecía servido en bandeja la escucha e intercepción del mismo.

Con la tecnología 5G, como hemos ido desarrollando, se estima que hay una mejora substancial desde el punto de vista de la seguridad, pero aún quedan varios vectores de ataque, tal cual presentamos en la imagen que sigue.



Como suele suceder con cualquier red o sistema, el mayor peligro, y quien puede causar daños verdaderamente grandes, es el usuario interno que tiene un grado de visibilidad que, en general, es superior a cualquier persona que se encuentra fuera del perímetro de esa organización. Dentro de este perímetro interior, por supuesto que habrá roles, perfiles y usuarios que a medida que escalan privilegios pueden potencialmente más peligrosos.

Como se ha mencionado también, con 5G se abren dos nuevos vectores de ataque con la introducción de MEC y Slicing, pues estamos abriendo nuestro “Backhaul” hacia desconocidos.

Los puntos de acceso WiFi, confiables y no confiables son ahora también dos nuevas vías de aproximación, como así también la seguridad mejor o peor que podamos configurar en los “Residencial Gateway”.

El tráfico roaming a través de la red IPX (que incluye a más de 2000 actores en el mundo), debería estar controlado a través de los SEPP, es otro nuevo desafío en la configuración adecuada del acceso al SBA.

Por último los problemas heredados de SS7 y/o Diameter de las generaciones anteriores, de una forma u otra son posibilidades de intrusión y/o ataques hacia este nuevo escenario. Este último, tal vez sea uno de los principales focos de atención que deban prestar as operadoras de telecomunicaciones, pues tanto SS7 como Diameter siguen presentando serios problemas de seguridad y cualquier nodo comprometido de esas arquitecturas ya son una puerta de entrada a 5G.