



[www.layakk.com](http://www.layakk.com)

@layakk

/Rooted<sup>®</sup> CON

# Seguridad 5G

Una introducción a los aspectos más relevantes de la Seguridad de la nueva generación de comunicaciones móviles

José Picó

David Pérez



# Sobre nosotros...



José Picó



David Pérez



Investigación (móviles y otros)

*Red Team*

Laboratorio de Evaluación de Seguridad de Productos TIC  
(en proceso de acreditación por el CCN)

Otros servicios de seguridad



**5G**



# Contenido

Introducción a 5G

Nuevas funcionalidades en  
materia de seguridad

Ataques conocidos contra 5G



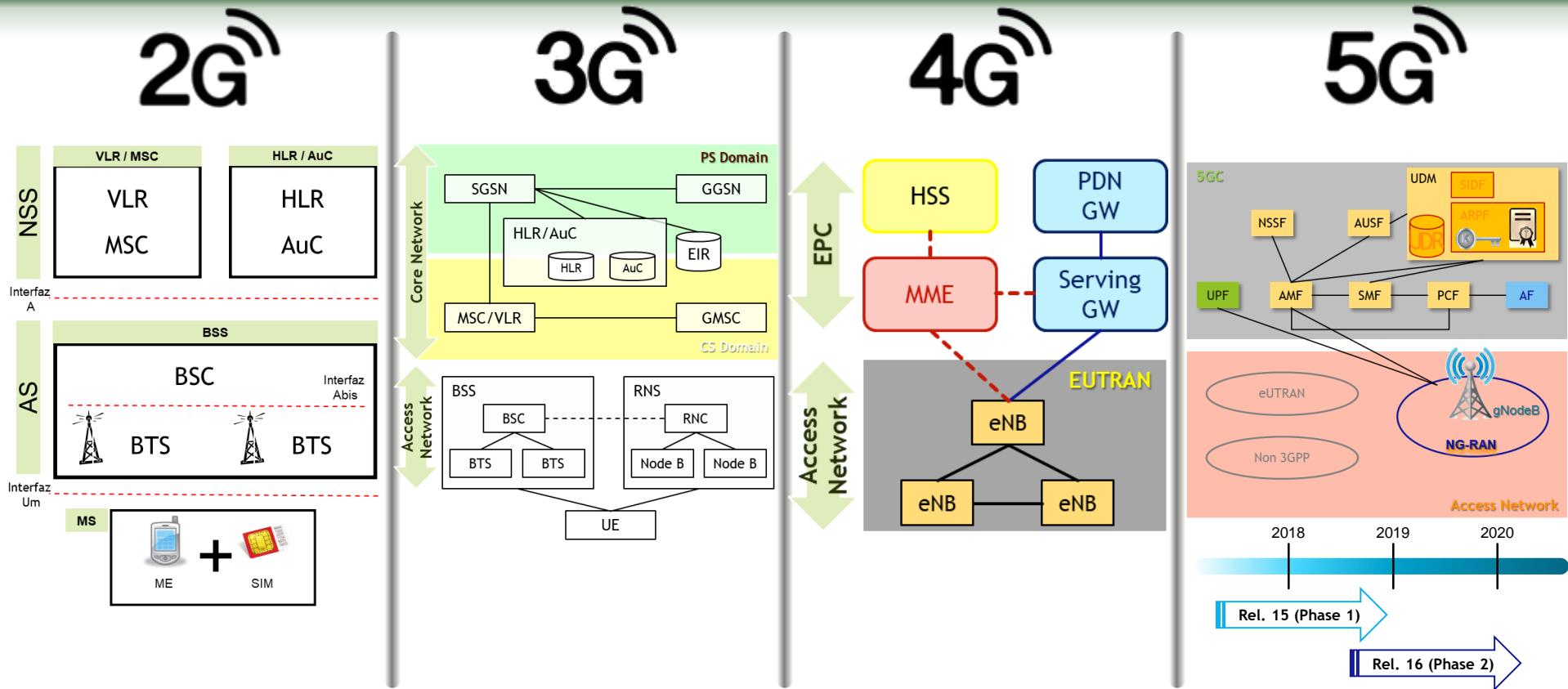
# Contenido

Introducción a 5G

Nuevas funcionalidades en  
materia de seguridad

Ataques conocidos contra 5G

# Las tecnologías móviles



# La tecnología 5G

## OBJETIVOS

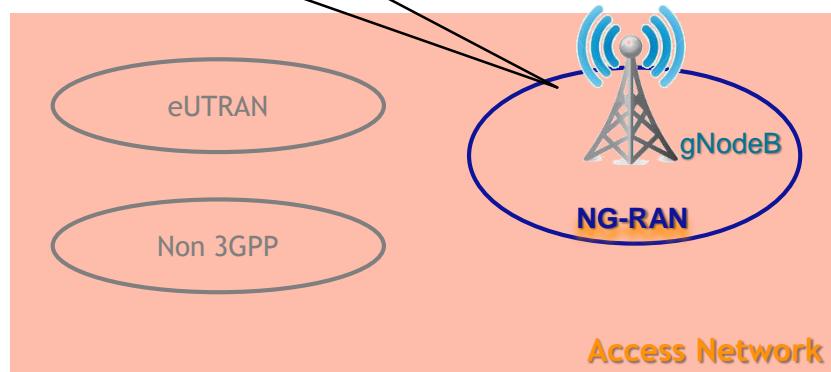
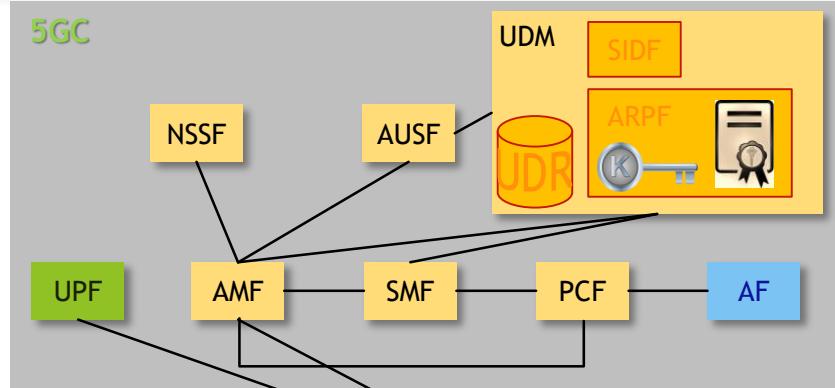
- ▶ Se pretende diseñar un sistema que soporte diferentes tipos de servicio (no sólo “voz y datos”), sino múltiples tipos de dispositivos conectados:
  - ▶ Se habla de  $10^7$  dispositivos
  - ▶ (m)IoT
  - ▶ Drones civiles y militares
  - ▶ Realidad aumentada
  - ▶ Super-automatización industrial
  - ▶ Dispositivos que viajan (y muy rápido) + V2X

# La tecnología 5G

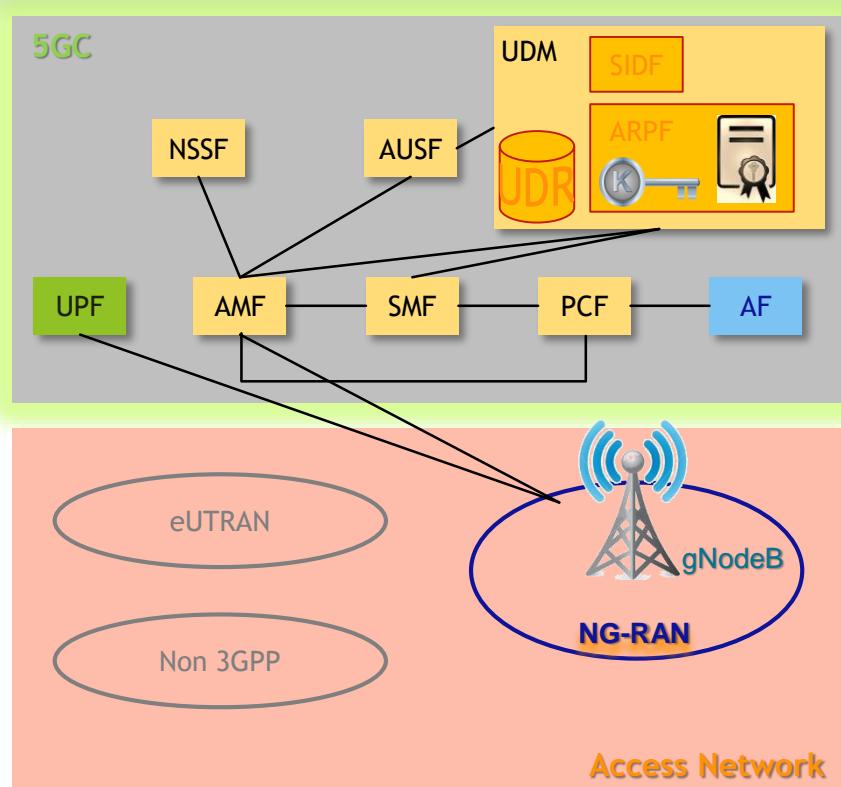
## IMPLICACIONES A NIVEL DE REQUERIMIENTOS



# Arquitectura 5G

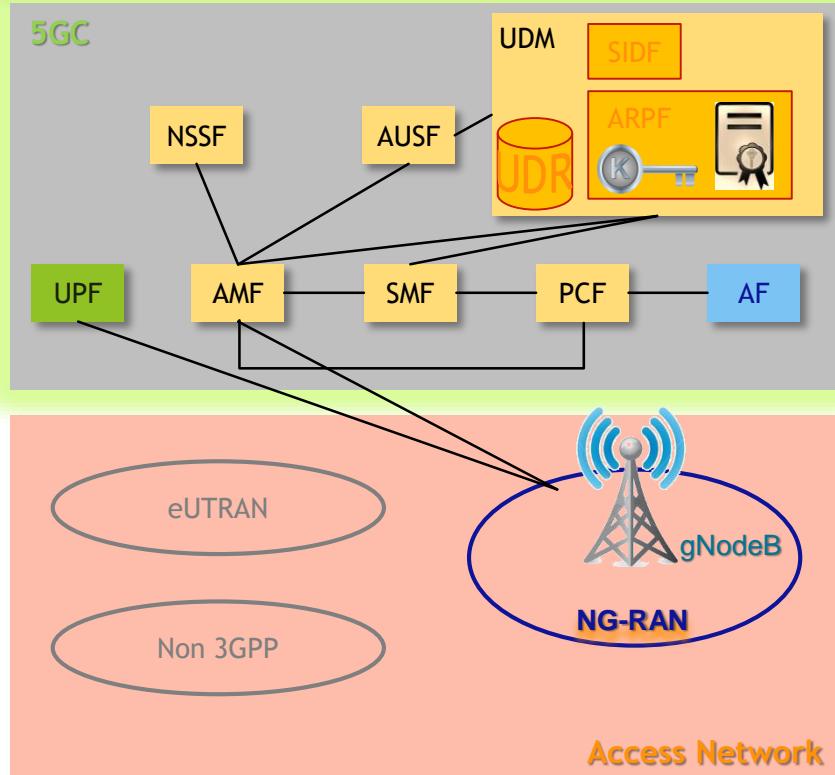


# Arquitectura 5G



- ▶ Ahora no existen componentes, sino **funciones** de red
- ▶ Las funciones de red:
  - ▶ exponen **servicios** mediante SBI (Service-based interfaces)
  - ▶ se diseñan sin estado, separando funciones de computación y funciones de almacenamiento
- ▶ Se soporta la exposición dinámica de capacidades a otros componentes o a otras redes

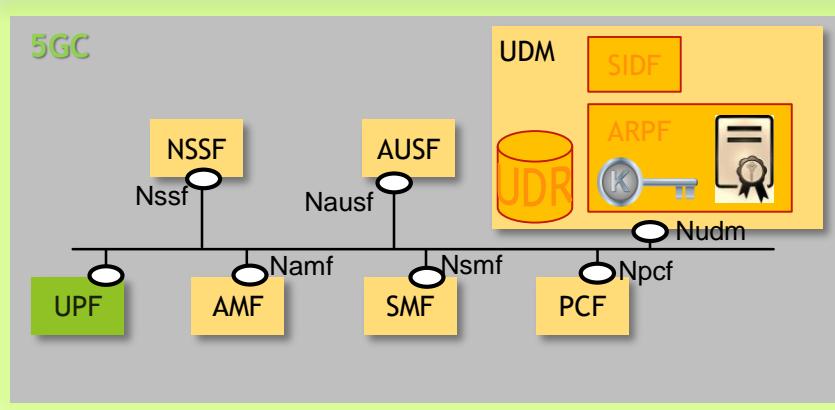
# Arquitectura 5G



## Funciones de Red principales

AMF	Access and Mobility Management Function
SMF	Session Management Function
AUSF	Authentication Server Function
UDM	Unified Data Management
SIDF	Subscription Identifier De-concealing Function
ARPF	Authentication credential Repository and Processing Function

# Arquitectura 5G

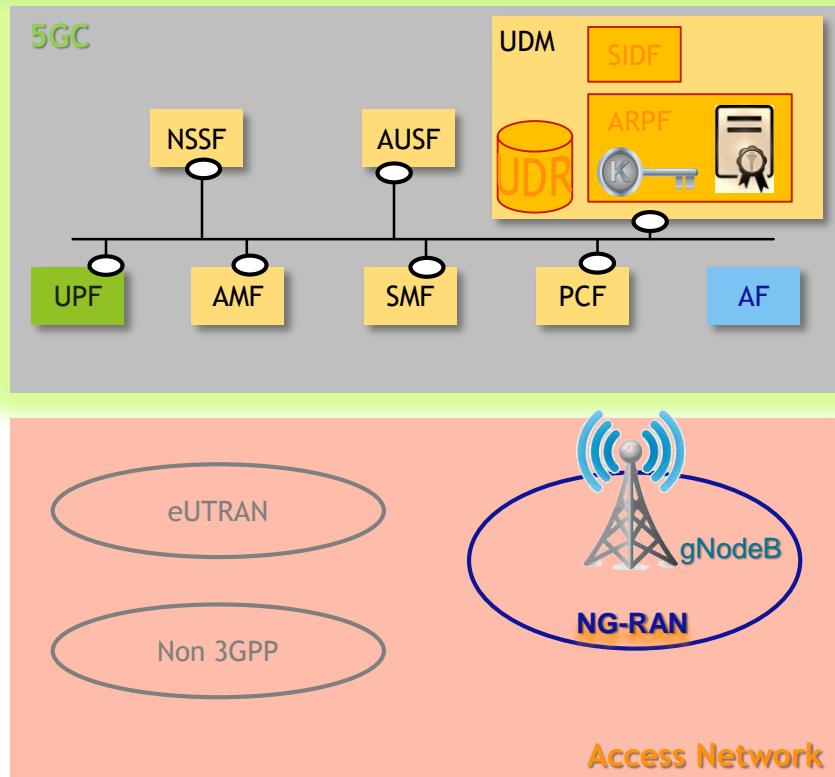


- ▶ SBA (Service-based architecture)

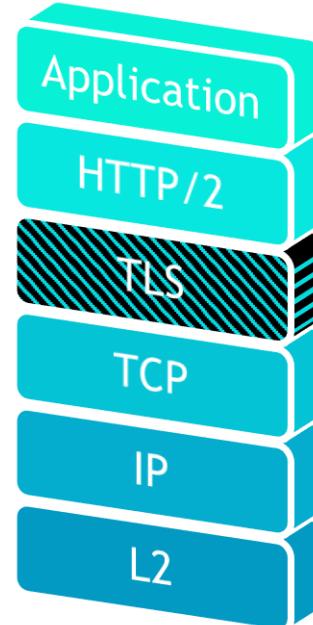


- ▶ Service-based Interfaces:
  - ▶ interface unificado a los servicios ofrecidos por las funciones en el plano de control
  - ▶ existe autenticación y autorización en el acceso al servicio

# Arquitectura 5G



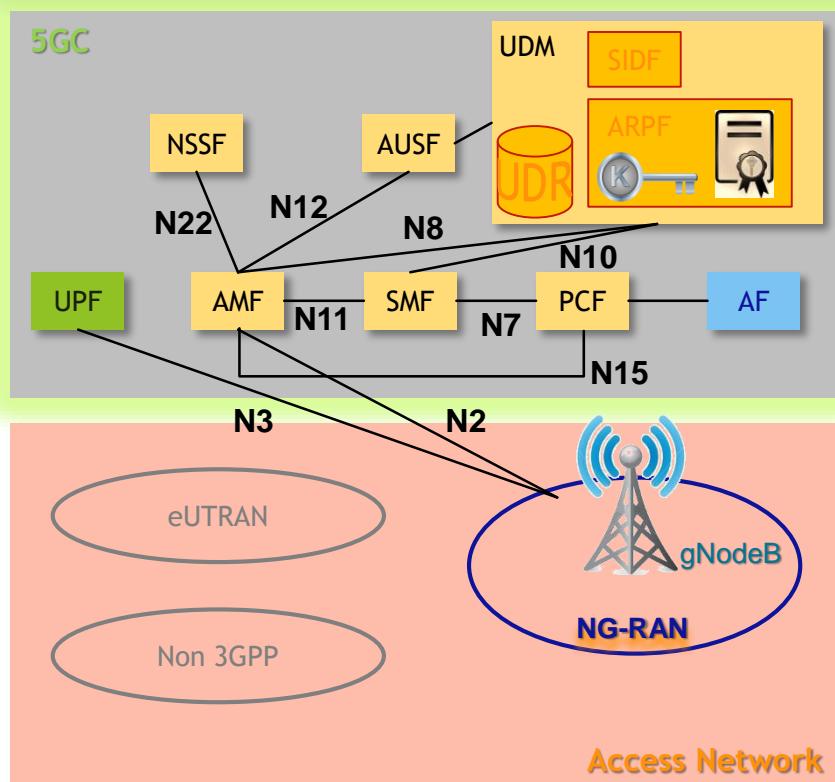
► Service-based Interfaces



- Autenticación mutua
- Cifrado

Pila de protocolos SBI

# Arquitectura 5G



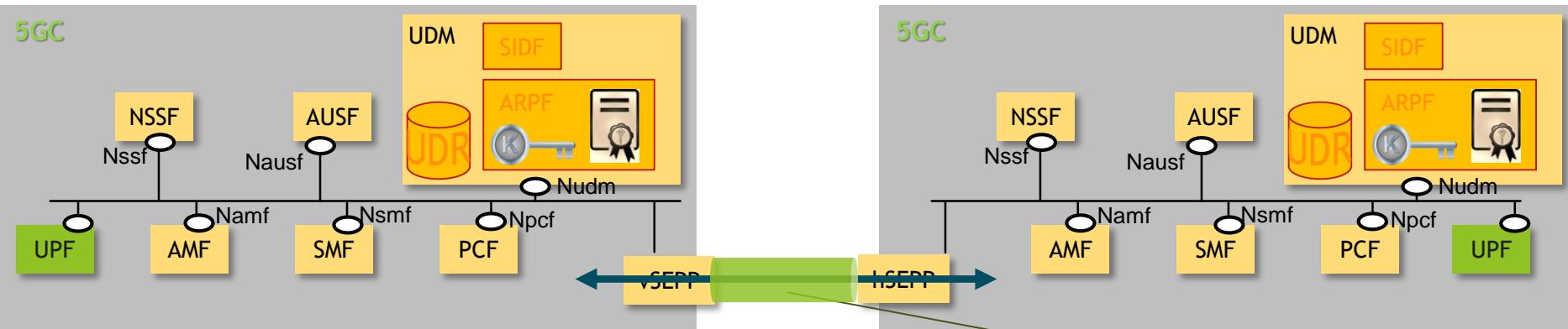
Reference points

≡

Especificación de interfaces entre  
funciones

# Arquitectura 5G

## Interconexión

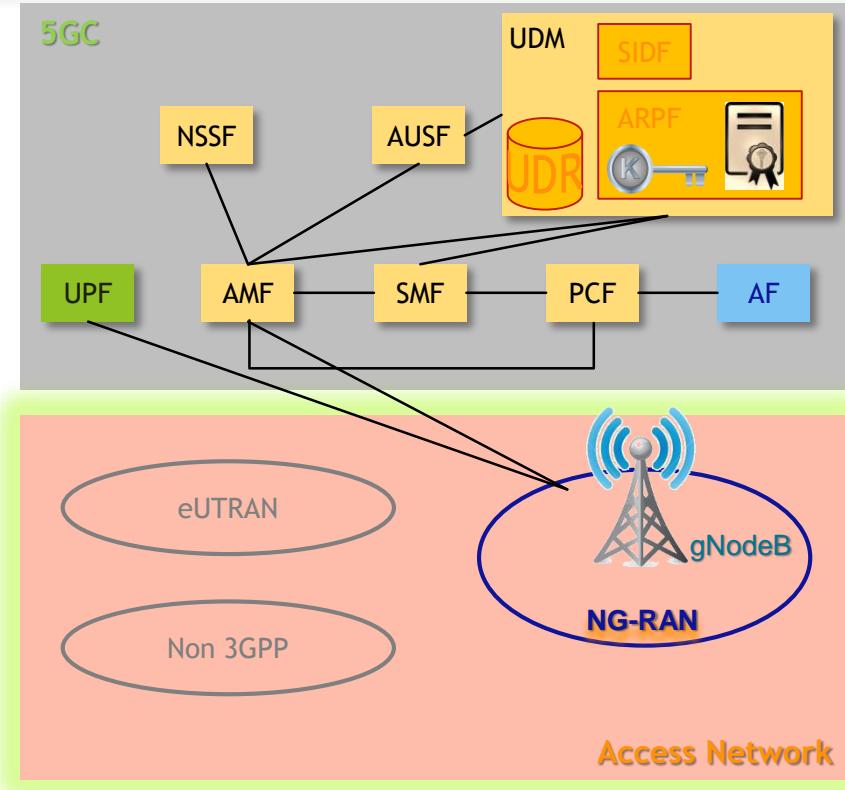


### SEPP (Security Edge Protection Proxy):

- Actúa como *proxy* no transparente para las comunicaciones en el plano de control entre redes
- Como *reverse proxy* proporciona un punto de acceso único a las funciones de red internas

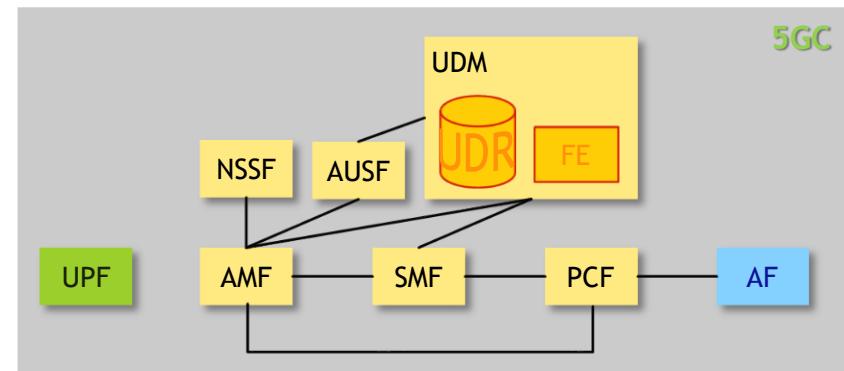
- Autenticación mutua
- Cifrado

# Arquitectura 5G

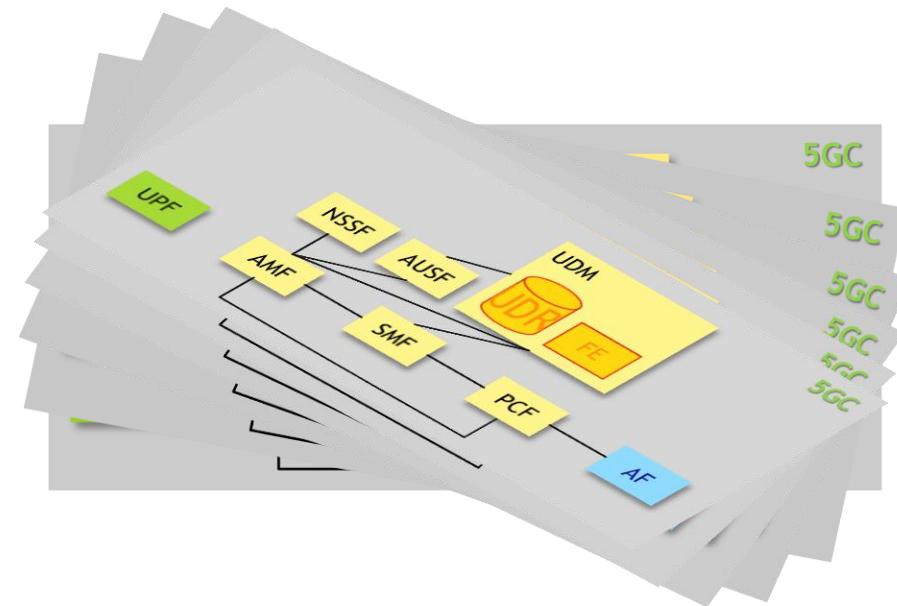


- ▶ Tecnologías soportadas en la red de acceso:
  - ▶ NG-RAN (New Generation Radio Access Network ≡ 5G Radio)
  - ▶ eUTRAN (Evolved Universal Terrestrial Radio Access Network ≡ LTE radio)
  - ▶ Non-3GPP: cualquier otra tecnología de acceso, considerada como no confiable por la red 5G

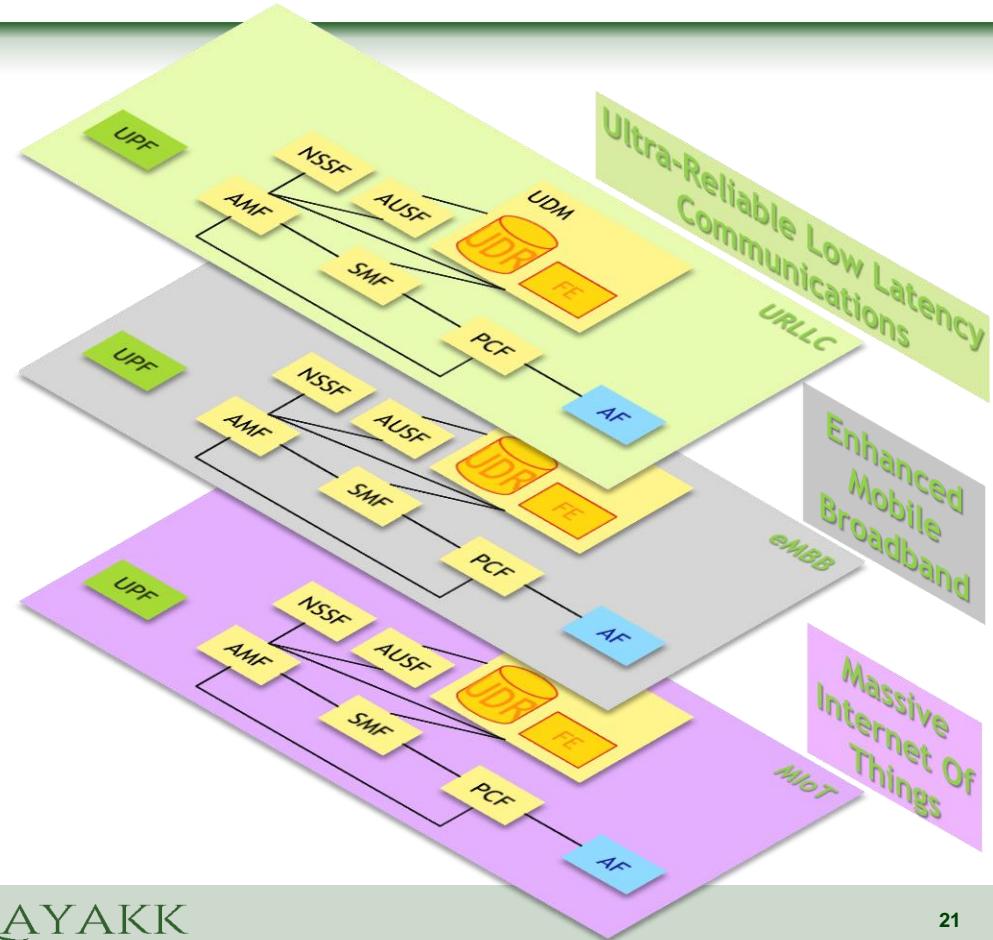
# Network Slicing



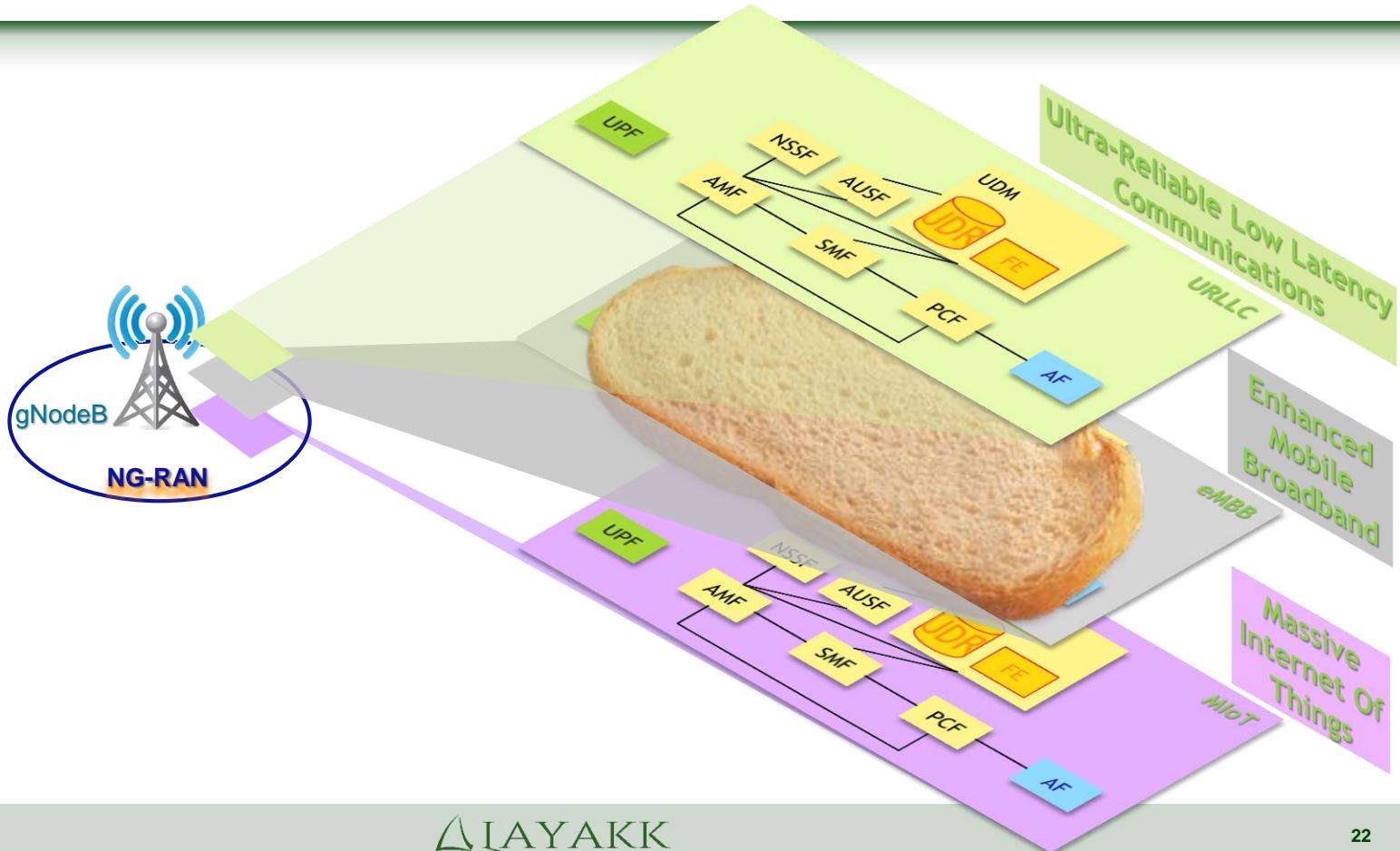
# Network Slicing



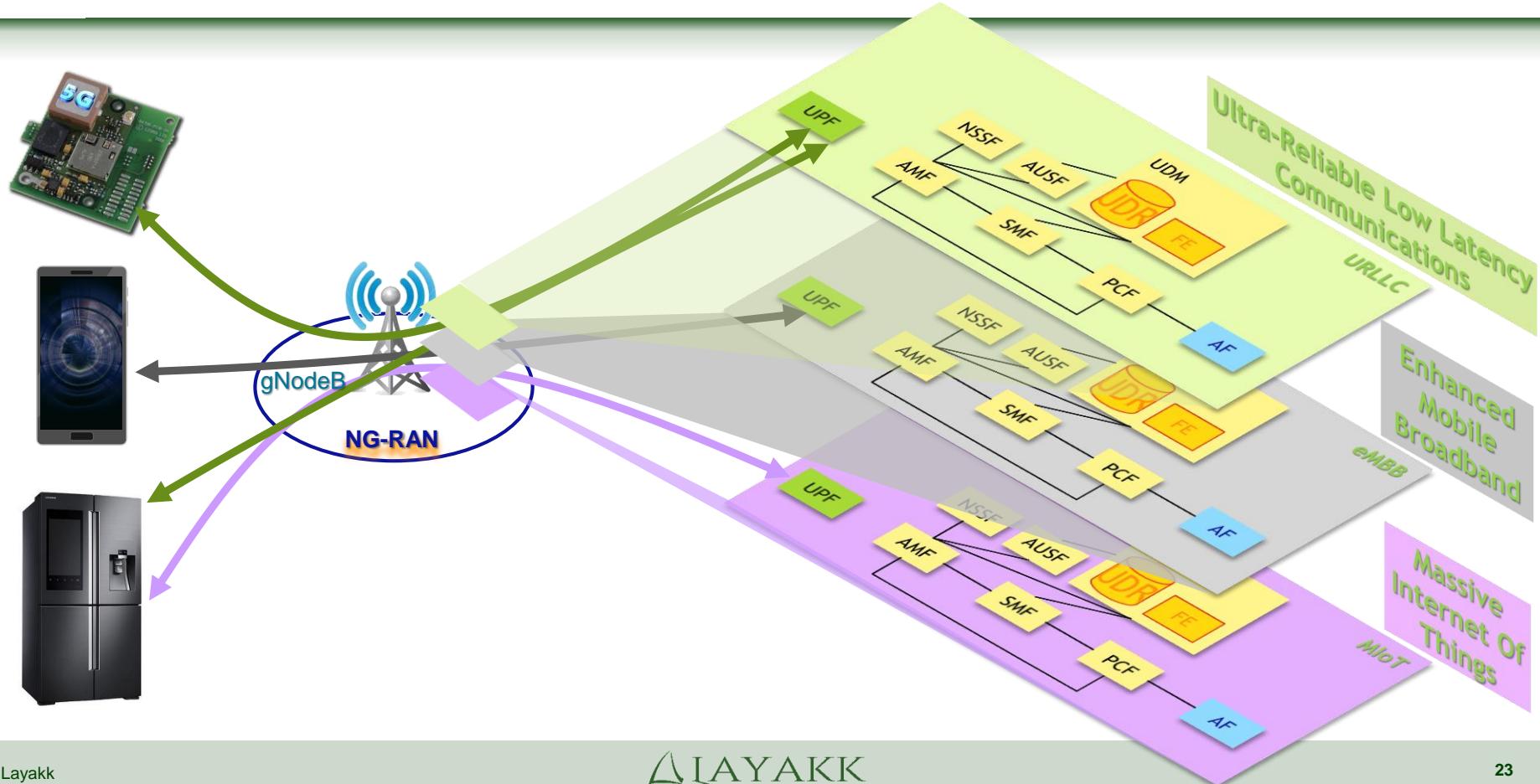
# Network Slicing



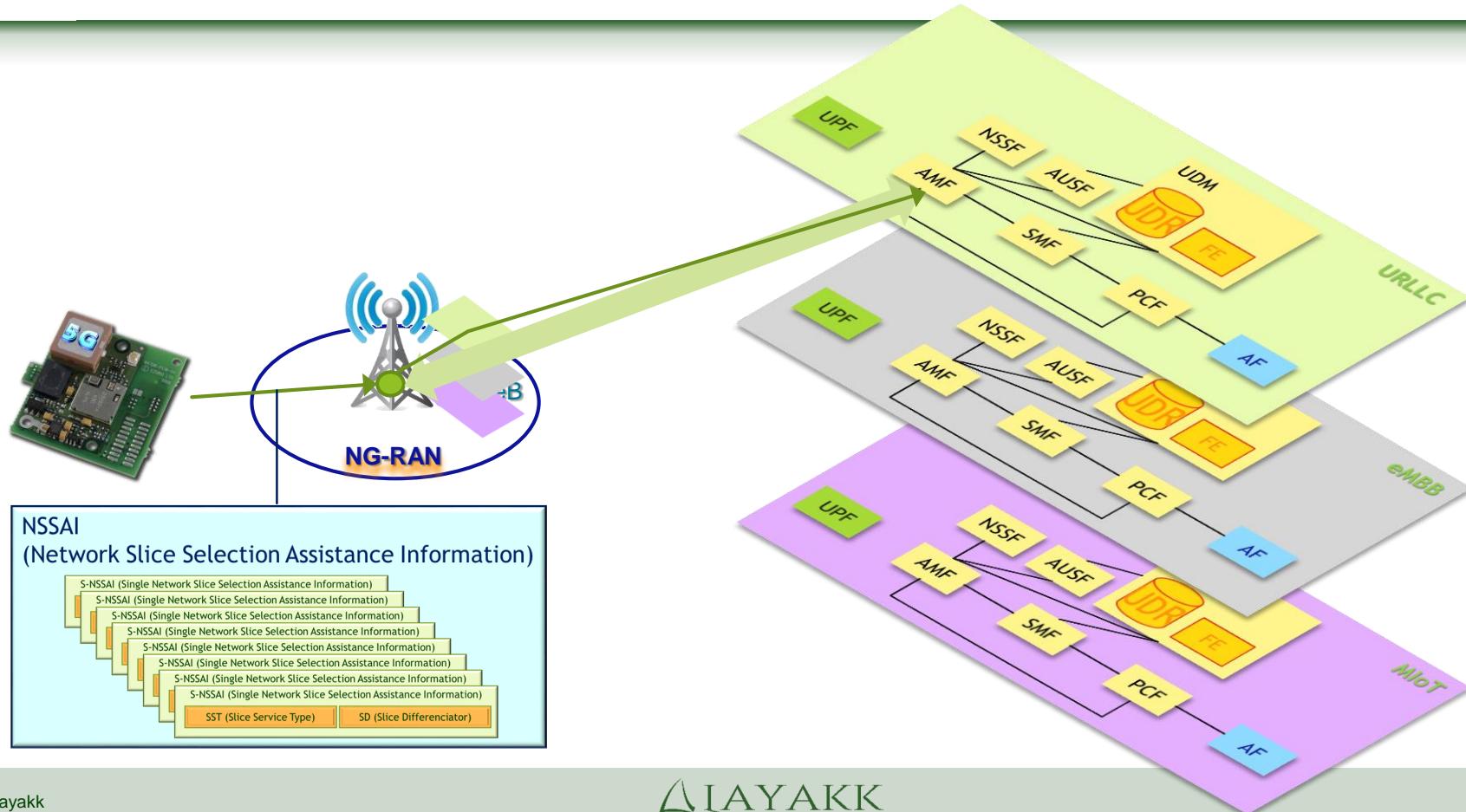
# Network Slicing



# Network Slicing



# Network Slicing



# Software Defined Network

## ► Funciones soportadas:

- ▶ *provisioning de network slices*: creación, modificación y finalización de cualquier NSI (*Network Slice Instance*)
- ▶ definición dinámica de recursos de red
- ▶ monitorización y detección de la red (fallos, disponibilidad, rendimiento)
- ▶ gestión de logs

## ► Diferentes modelos de gestión

- ▶ Network Slicing as a Service (NSaaS)
- ▶ Network Slicing como parte de la infraestructura propia del Operador





# Contenido

Introducción a 5G

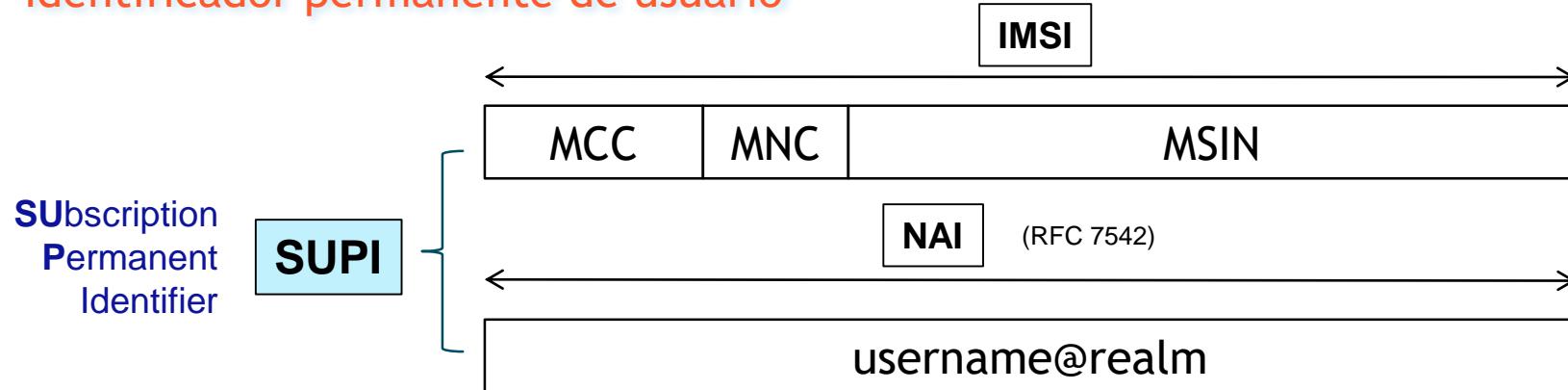
Nuevas funcionalidades en  
materia de seguridad

Ataques conocidos contra 5G

# Protección de la identidad

# Protección de la identidad

## Identificador permanente de usuario



- ▶ Información sensible, pues identifica al usuario y puede usarse para diversos fines maliciosos, tales como geolocalización, suplantación de usuarios, denegación de servicio, etc.

# Protección de la identidad

## Identificador temporal de usuario

**5G-GUTI**

5G Globally Unique Temporary UE Identity

**5G-GUTI**



GUAMI (Globally Unique AMF identifier)

5G-TMSI

MCC

MNC

AMF Identifier

## Identificador temporales derivados (formas cortas del 5G-GUTI)

**S-TMSI**

**5G-S-TMSI**

# Protección de la identidad

## Identificador de usuario encubierto

**SUCI****SUbscription Concealed Identifier**

- ▶ Contiene el SUPI cifrado:
  - ▶ con una clave pública pre-suministrada por el operador, almacenada en la USIM
  - ▶ utilizando uno de los esquemas de protección soportados



El identificador de usuario (SUPI) **NUNCA** se envía directamente (se envía en su lugar el SUCI)



El UE utilizará el “null-scheme” en los siguientes casos:

- En llamadas de emergencia
- **Si la Home Network ha configurado que debe usarse ese esquema**
- **Si la Home Network no ha provisionado la clave pública necesaria**

Dependiente  
del operador

# Autenticación

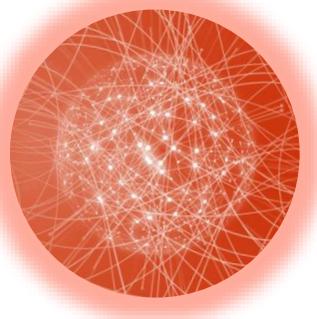
# Autenticación

## Agentes

UE



SERVING  
NETWORK



HOME NETWORK



Ref.: <https://simalliance.org/wp-content/uploads/2018/12/What-is-a-3GPP-R15-5G-SIM-card-20-11-2018-FINAL.pdf>

# Autenticación

## Mecanismos de autenticación

### 5G-AKA

- Actualización 5G del mecanismo clásico 3gPP de autenticación
- Soporte obligado para dispositivos 5G

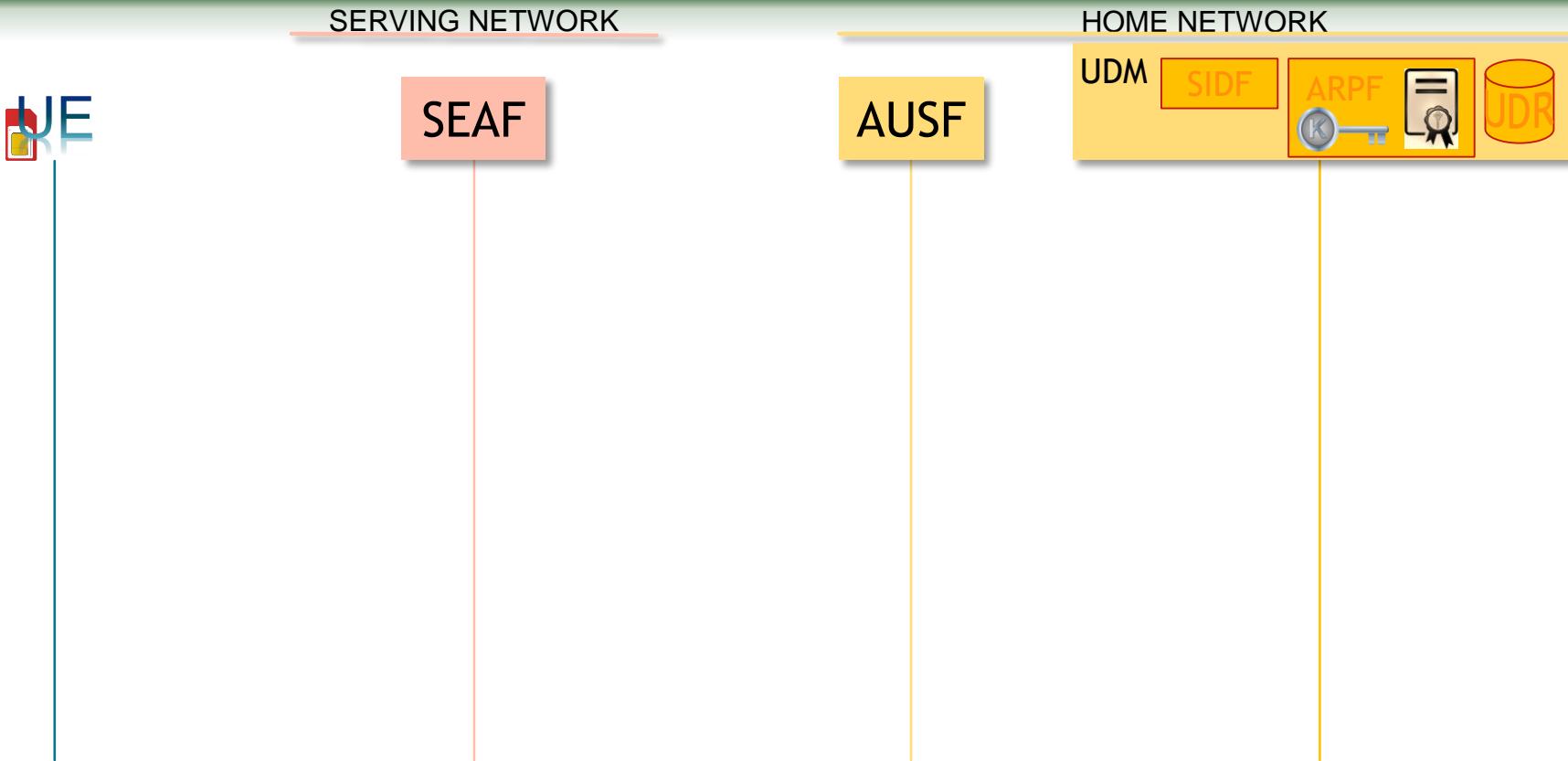
### EAP-AKA'

- Extiende EAP-AKA (3G) con:
  - Inclusión del *serving network name* en la derivación de claves
  - Uso de SHA256 en lugar de SHA1
  - Actualización para prevenir ataques *bidding down*
  - Soporte obligado para dispositivos 5G

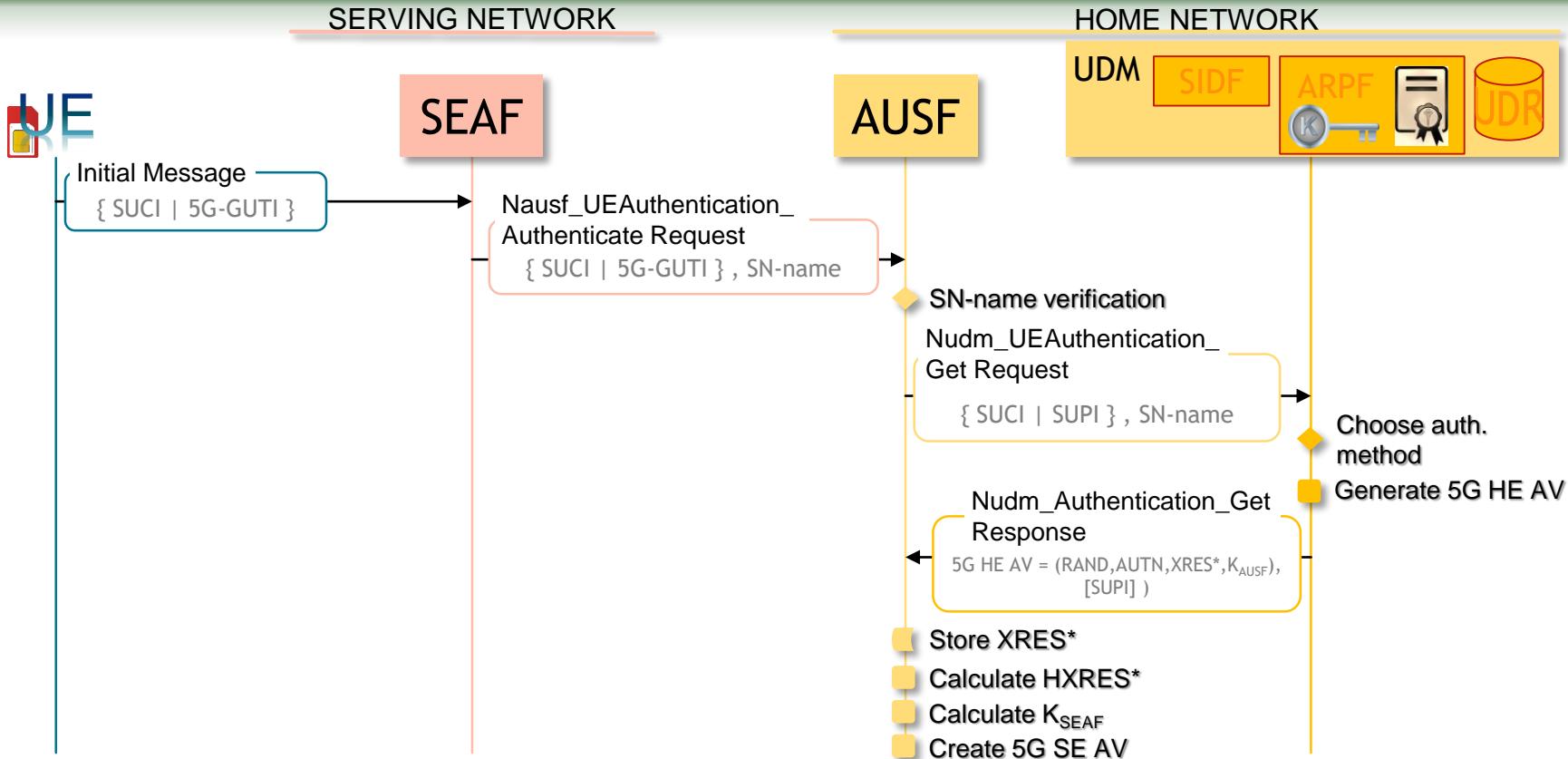
### EAP Adicionales

- Permitidos para autenticación en *redes privadas* (redes aisladas de las redes públicas) que usan tecnología 5G
- Rel.15 sólo define EAP-TLS como mecanismo adicional soportados

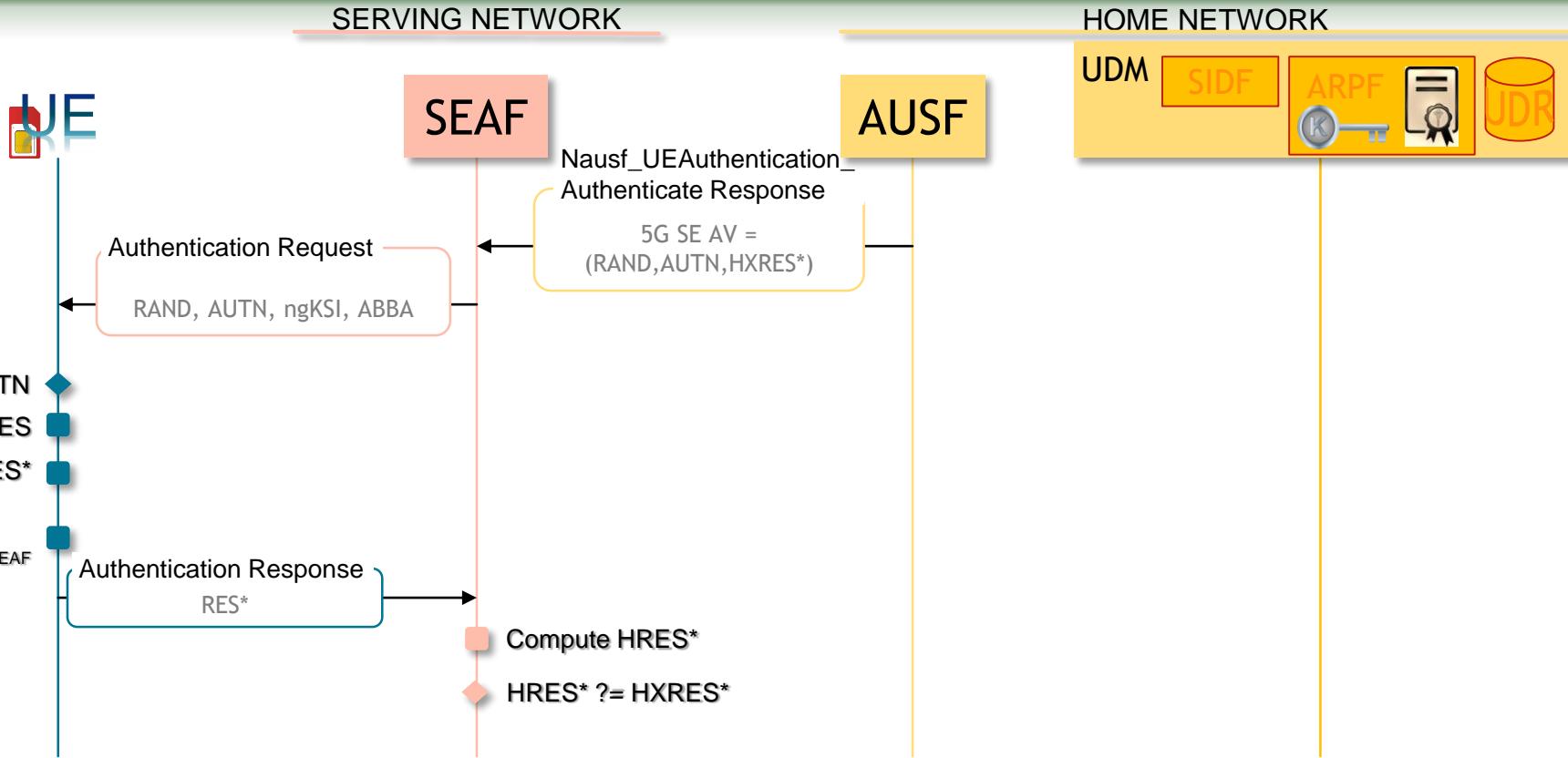
# 5G AKA (I)



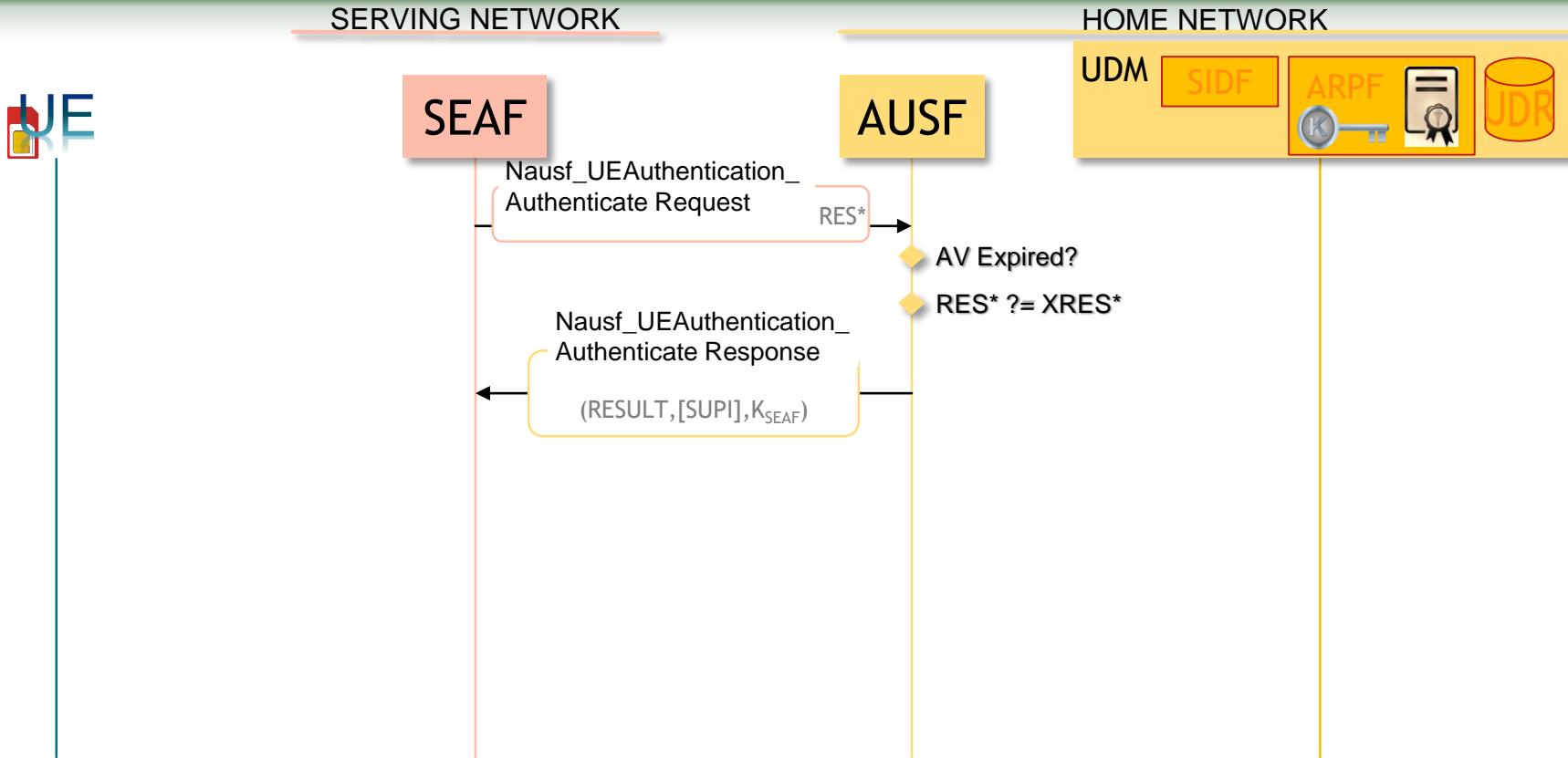
# 5G AKA (I)



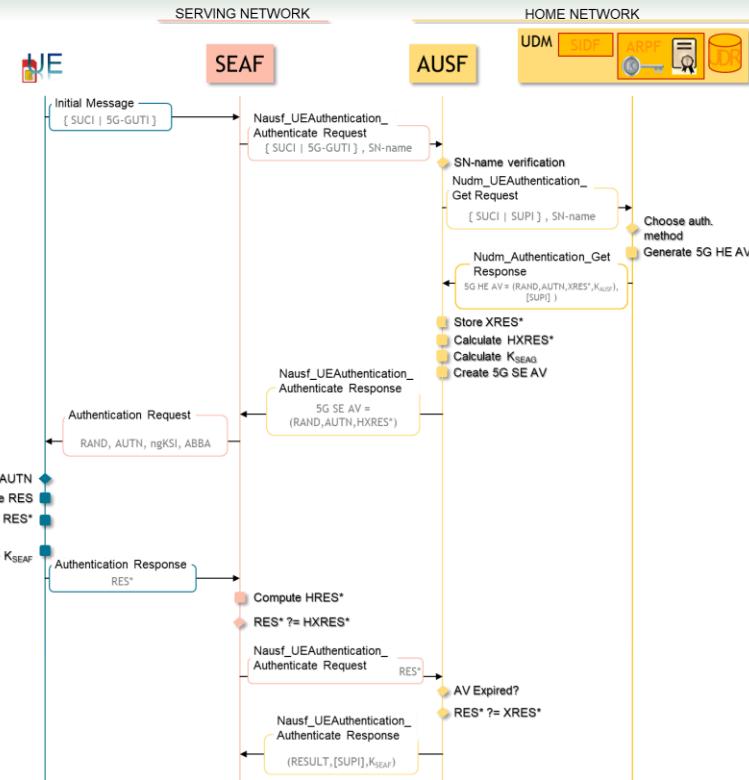
# 5G AKA (II)



## 5G AKA (III)

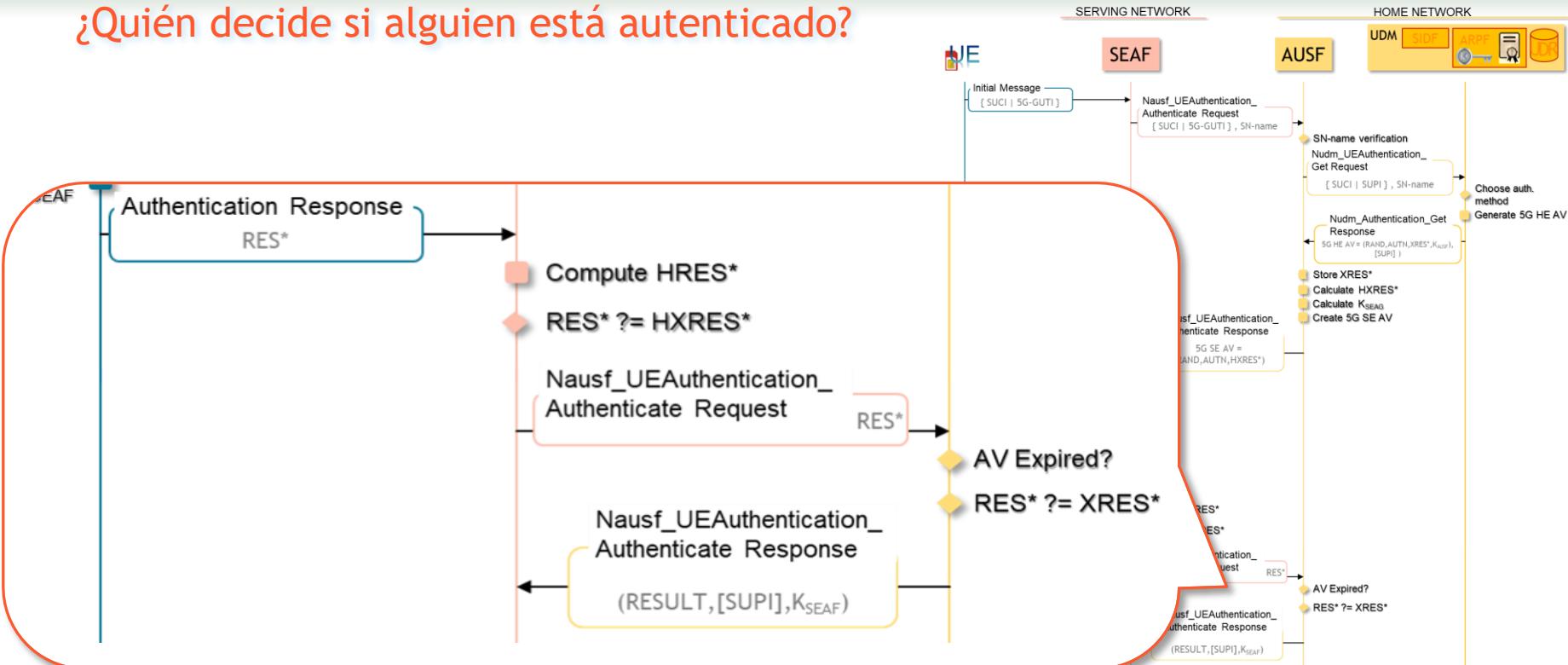


# Autenticación AKA



# Autenticación AKA

¿Quién decide si alguien está autenticado?



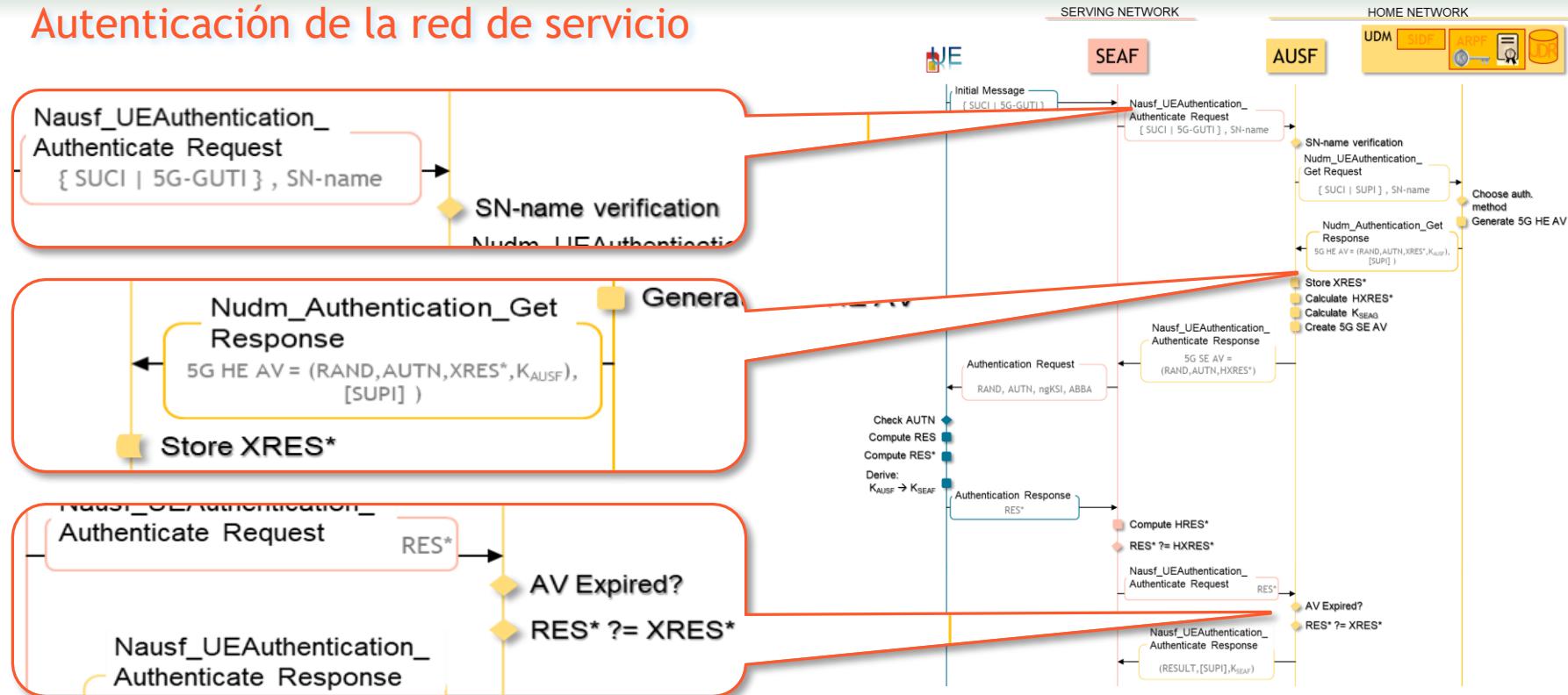
# Control de la HOME NETWORK

El nuevo AKA *facilita* establecer mecanismos de control de fraude, pero no supone una protección *per-se*

- ▶ Ejemplo: impedir que una red registre un AMF asociado a un UE que no está realmente presente en la red
- ▶ Implementarlo se deja a criterio del operador
- ▶ La Release 15 sugiere mecanismos para ello:
  - ▶ El UDM debe autorizar cada nuevo procedimiento de red sobre UE, basándose en el estado de autentación del UE

# Autenticación AKA

## Autenticación de la red de servicio



# EAP-AKA

## Roles



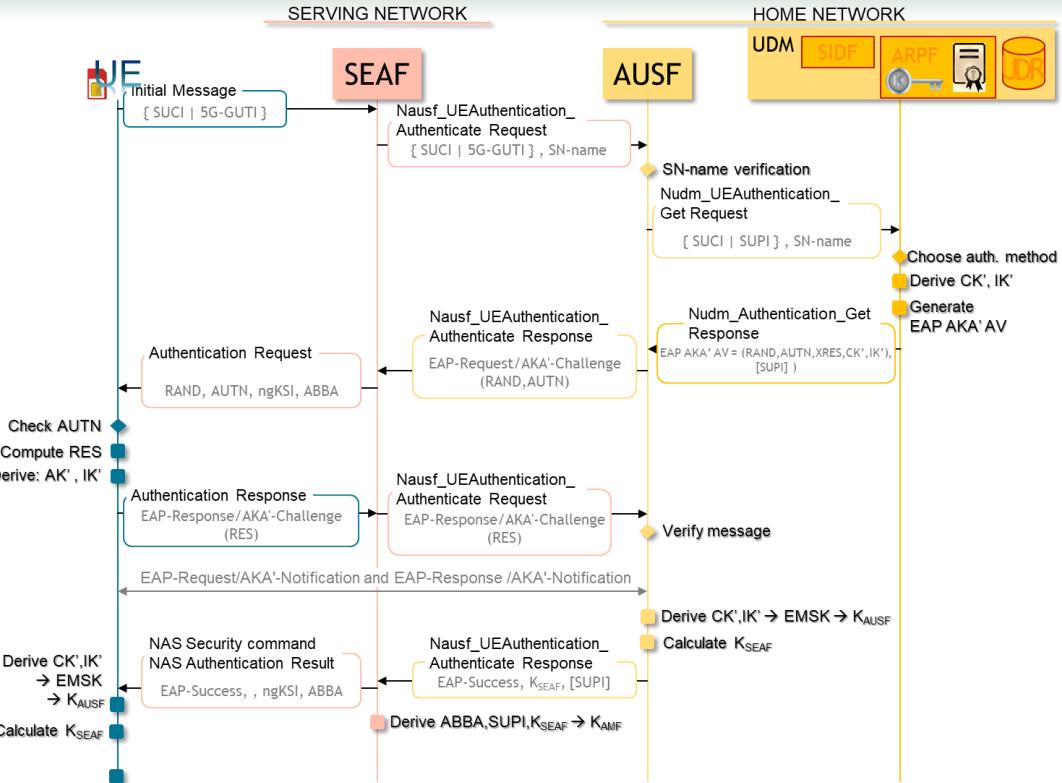
Peer

**SEAF**

Authenticator  
(pass-through)

**AUSF**

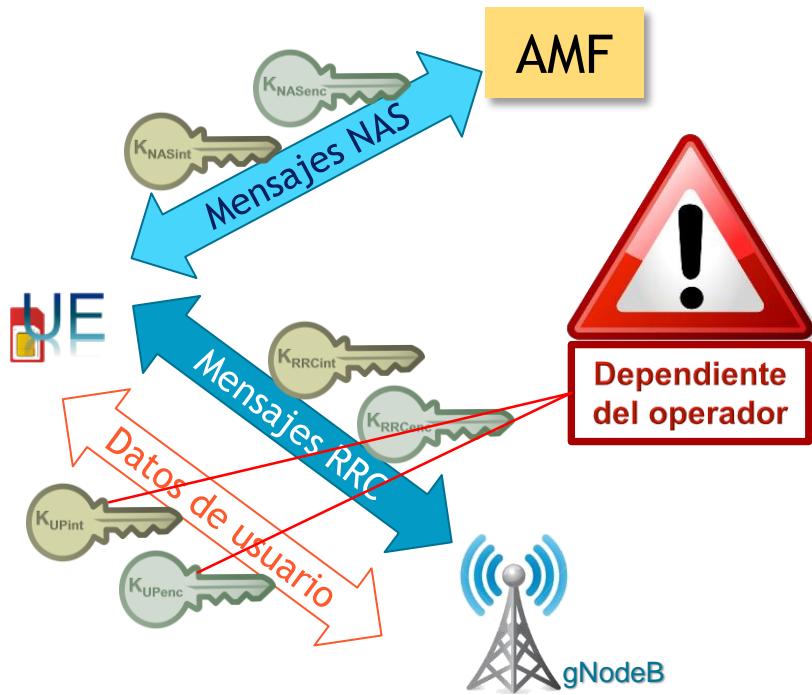
Backend  
Authentication  
server



# Protección de la información

# Protección de la información

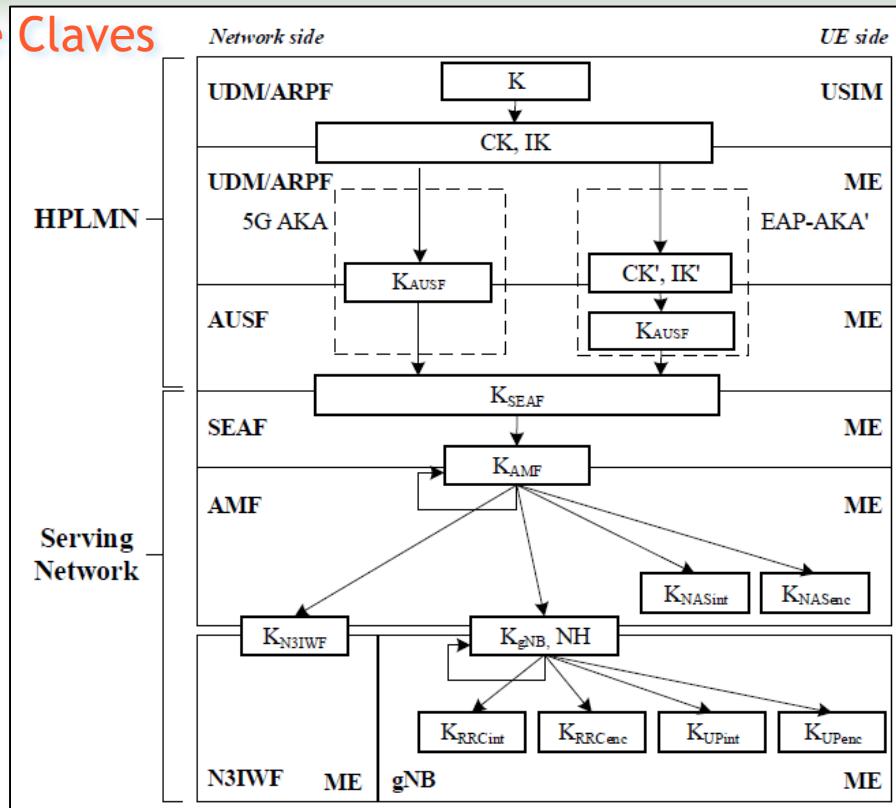
## Gestión de Claves



- ▶ Algoritmos de cifrado e integridad:
  - ▶ NEA0 = NIA0 = Null ciphering algorithm
  - ▶ NEA1 = NIA1 = 128-bit SNOW 3G based algorithm
  - ▶ NEA2 = NIA2 = 128-bit AES based algorithm
  - ▶ NEA3 = NIA3 = 128-bit ZUC based algorithm

# Protección de la información

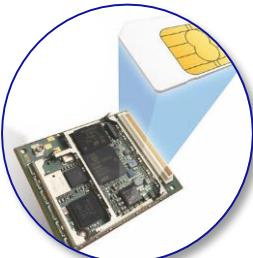
## Derivación de Claves



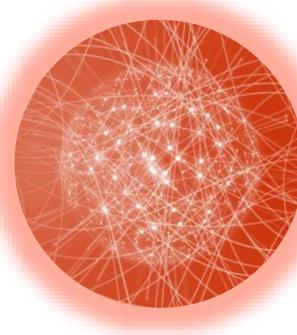
# Autenticación AKA

¿Quién decide si se cifran en el interfaz radio las comunicaciones de usuario?

UE



SERVING  
NETWORK



HOME NETWORK



# Autenticación AKA

¿Quién decide si se cifran en el interfaz radio las comunicaciones de usuario?

SERVING  
NETWORK

*“Local SMF can override the confidentiality option in the UP security policy received from the home SMF based on:*

- *regulatory requirements*
- *roaming agreement*
- *its local policy ”*

HOME NETWORK

*“The SMF shall provide UP security policy for a PDU session (...) [It] shall indicate whether UP confidentiality and/or UP integrity protection shall be activated or not (...)"*



*Non-3GPP access*

# Security for non-3gpp access

## Autenticación

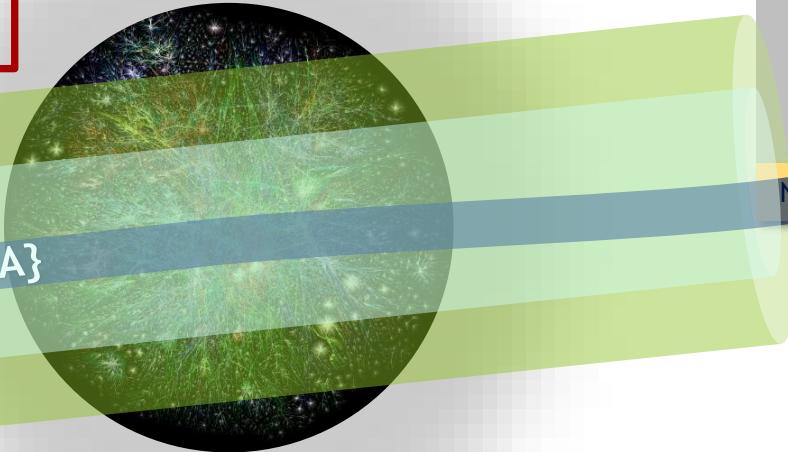
(optional)  
N3IWF  
Operator  
Certificate



IPSec IKEv2

EAP-5G

{EAP-AKA | 5G-AKA}



Untrusted network



# Contenido

Introducción a 5G

Nuevas funcionalidades en  
materia de seguridad

Ataques conocidos contra 5G

# IMSI Catching tradicional

# IMSI catching tradicional (hasta 4G)

## User identification by a permanent identity [TS 33.401]

The user identification mechanism should be invoked by the serving network whenever the user cannot be identified by means of a temporary identity (GUTI). In particular, it should be used when the serving network cannot retrieve the IMSI based on the GUTI by which the user identifies itself on the radio path.

The mechanism described in figure 6.1.3-1 allows the identification of a user on the radio path by means of the permanent subscriber identity (IMSI).

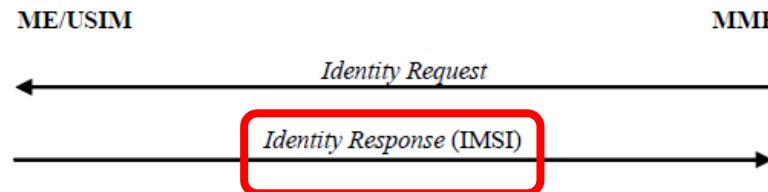
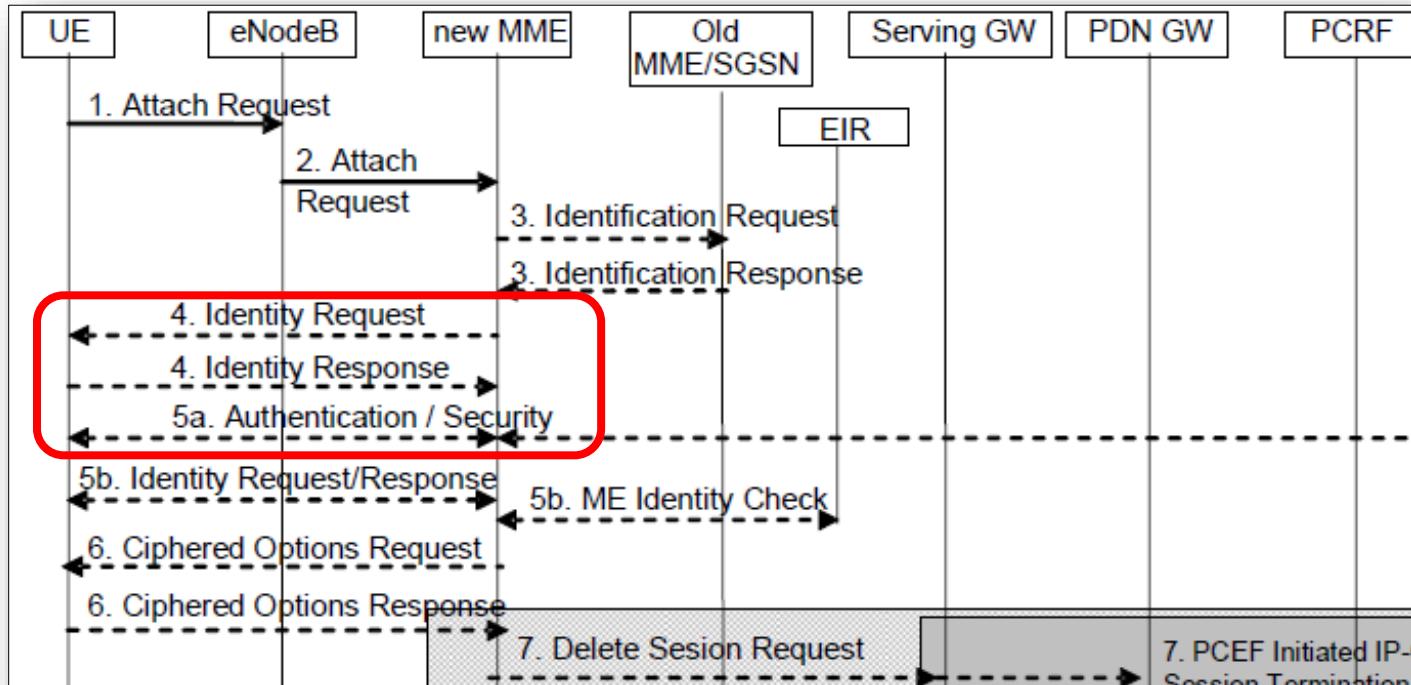


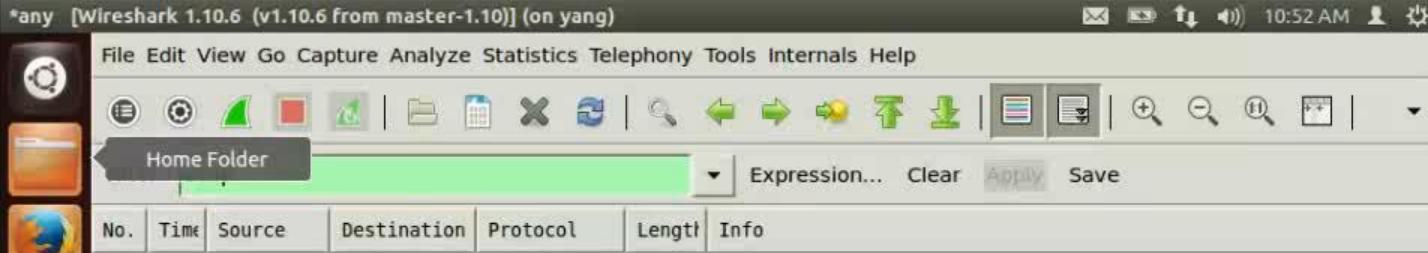
Figure 6.1.3-1: User identity query

The mechanism is initiated by the MME that requests the user to send its permanent identity. The user's response contains the IMSI in cleartext. This represents a breach in the provision of user identity confidentiality.

# IMSI catching tradicional (hasta 4G)

User identification by a permanent identity [TS 33.401]





No.	Time	Source	Destination	Protocol	Length	Info

# IMSI catching tradicional ¿5G?



# IMSI catching tradicional ¿5G?

## 6.12.4 Subscription identification procedure

3GPP TS 33.501 V15.3.1 (2018-12)

The subscriber identification mechanism may be invoked by the serving network when the UE cannot be identified by means of a temporary identity (5G-GUTI). In particular, it should be used when the serving network cannot retrieve the SUPI based on the 5G-GUTI by which the subscriber identifies itself on the radio path.

The mechanism described in figure 6.12.4-1 allows the identification of a UE on the radio path by means of the SUCI.

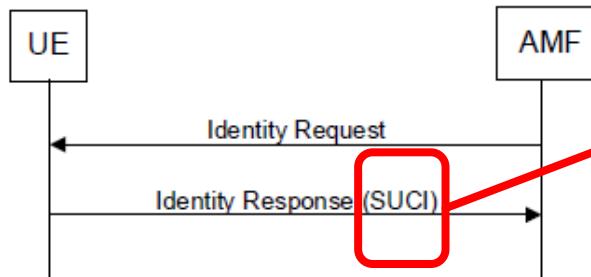


Figure 6.12.4-1: Subscription identifier query

The UE shall calculate a fresh SUCI from SUPI using the Home Network Public Key, and respond with Identity Response carrying the SUCI. The UE shall implement a mechanism to limit the frequency at which the UE responds with a fresh SUCI to an Identity Request for a given 5G-GUTI.

NOTE 1: If the UE is using any other scheme than the null-scheme, the SUCI does not reveal the SUPI.

SUCI  
SUbscription  
Concealed  
Identifier

Dependiente  
del operador

# IMSI catching tradicional ¿5G?

Funcionalidades de Seguridad

## Protección de la identidad

### Identificador de usuario encubierto

SUCI

SUbscription Concealed Identifier

► Contiene el SUPI cifrado:

- con una clave pública pre-suministrada por el operador, almacenada en la USIM.
- utilizando uno de los esquemas de protección soportados



El identificador de usuario (SUPI) **NUNCA** se envía directamente (se envía en su lugar el SUCI)

El UE utilizará el "null-scheme" en los siguientes casos:

- En llamadas de emergencia
- Si la Home Network ha configurado que debe usarse ese esquema
- Si la Home Network no ha provisionado la clave pública necesaria

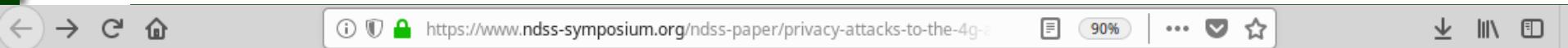
Dependiente  
del operador



Dependiente  
del operador

# ToRPEDO, IMSI-Cracking

ToRPEDO = TRacking via Paging mEssage DistributiOn attack



 NDSS About NDSS Sponsorship Previous Events

NDSS 2019 Attend Programme Submissions Committees



## Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information

Syed Rafiul Hussain (Purdue University), Mitziu Echeverria (University of Iowa), Omar Chowdhury (University of Iowa), Ninghui Li (Purdue University), Elisa Bertino (Purdue University)

**NDSS 2019**

26th Annual Network and Distributed System Security Symposium  
San Diego, California

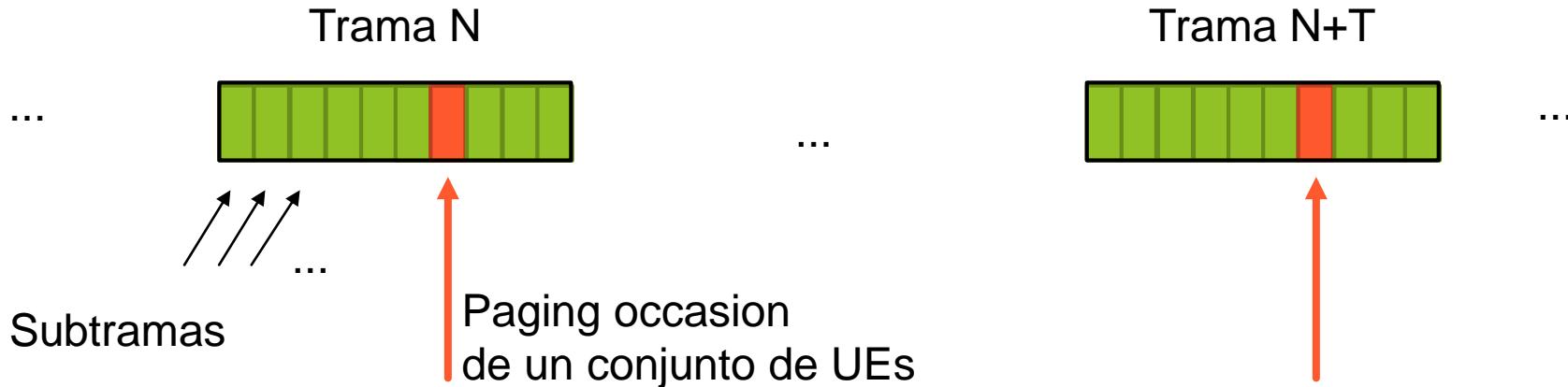
24 – 27 February 2019

(Investigación realizada en 2018)

# ToRPEDO (5G y 4G)

## Paging occasion

- ▶ Los *paging* para cada UE suceden en momentos concretos periódicos (*paging occasion*) que dependen de los 10 bits menos significativos del IMSI



# ToRPEDO (5G y 4G)

ToRPEDO = TRacking via Paging mEssage DistributiOn attack

- ▶ Los *paging* para cada UE suceden en momentos concretos periódicos (*paging occasion*) que dependen de los 10 bits menos significativos del IMSI
- ▶ Lanzando llamadas silenciosas (menos de 10) a un número víctima se pueden observar los *paging occasion* (PO) y si hay un PO que claramente incrementa sus pagings con cada llamada, se determina:
  - que la víctima está presente en la zona
  - cuál es su PO (en qué momentos escucha por si hay pagings para él)
  - 7 bits de su IMSI (no son 10 por diferencias de codificación, decimal vs. BCD)
- ▶ Funcionaría aunque el TMSI cambiara continuamente y fuera completamente aleatorio

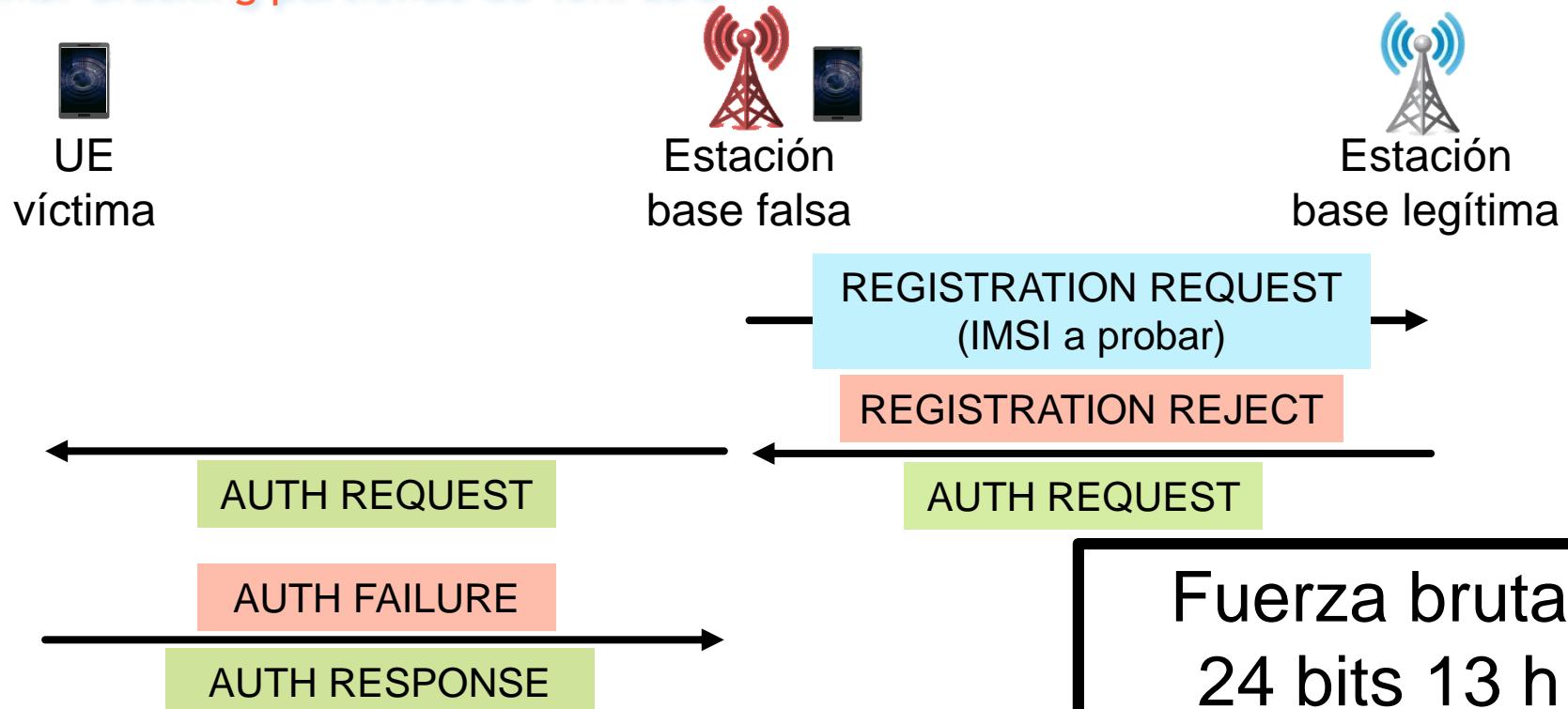
# IMSI-Cracking (5G y 4G)

## IMSI-Cracking partiendo de ToRPEDO

- ▶ Un IMSI en USA tiene 49 bits (similar en el resto del mundo)
- ▶ Los primeros 18 bits representan el pais y el operador
  - ▶ Quedan 31 bits desconocidos
- ▶ ToRPEDO obtiene los últimos 7 bits del IMSI
  - ▶ Quedan 24 bits desconocidos
- ▶ Con un ataque de fuerza bruta sobre los 24 bits desconocidos se puede obtener el resto del IMSI en menos de 13 horas
  - ▶ Registration\_request a la red real con IMSI de prueba (registration\_reject/auth\_request)
  - ▶ Reenvío de los auth\_request al UE víctima (auth\_failure/auth\_response)

# IMSI-Cracking (5G y 4G)

## IMSI-Cracking partiendo de ToRPEDO



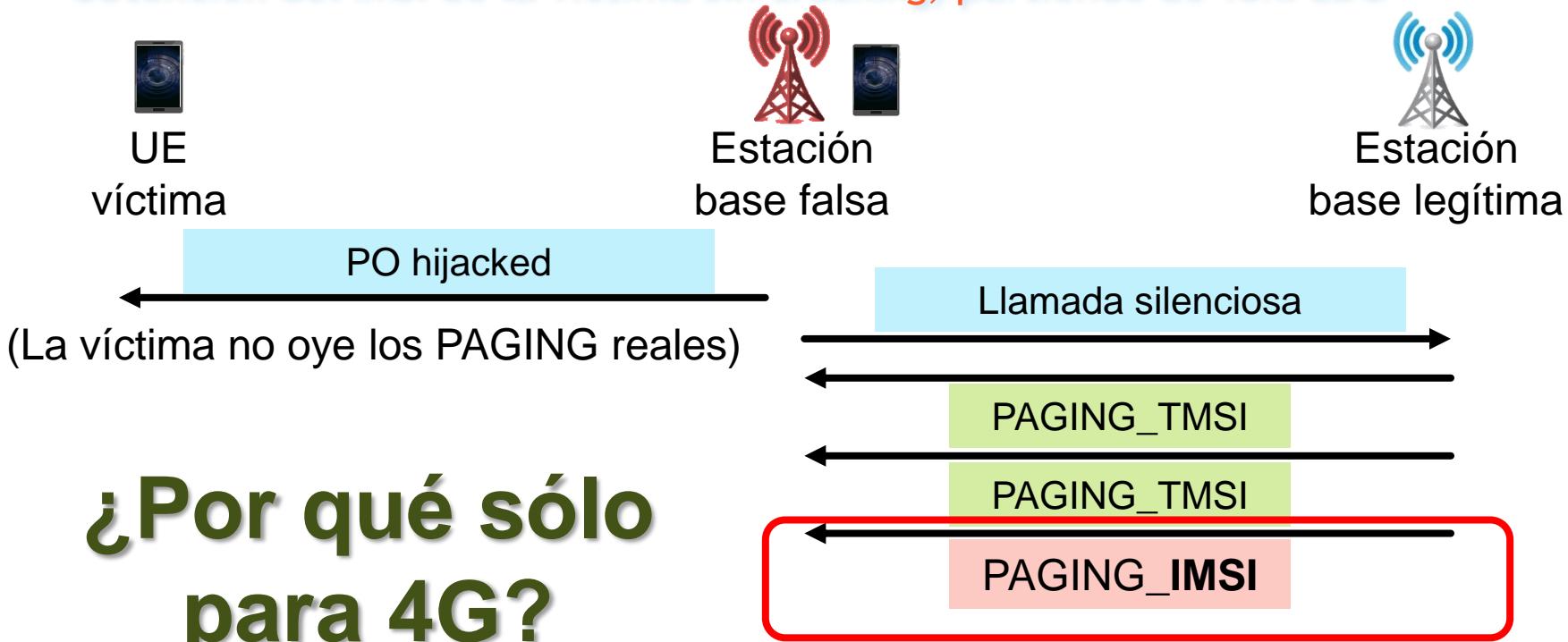
## ... y PIERCER para 4G

### Obtención del IMSI de la víctima sin cracking, partiendo de ToRPEDO

- ▶ El atacante emite con estación base falsa durante los PO de la víctima, evitando que ésta oiga los paging messages de la red real
- ▶ El atacante lanza llamadas silenciosas
- ▶ La red hace paging usando el TMSI... pero cuando no responde pasa a hacer paging usando el IMSI
- ▶ El atacante captura esos mensajes de paging con el IMSI de la víctima

# ... y PIERCER para 4G

Obtención del IMSI de la víctima sin cracking, partiendo de ToRPEDO



# ... y PIERCER para 4G

Obtención del IMSI de la víctima sin cracking, partiendo de ToRPEDO

## Paging message

4G

```
PagingUE-Identity ::= CHOICE {  
    s-TMSI,  
    imsi,  
    ...,  
    ng-5G-S-TMSI-r15,  
    fullI-RNTI-r15  
}
```

3GPP TS 36.331 V15.4.0 (2018-12)

5G

```
PagingUE-Identity ::= CHOICE {  
    ng-5G-S-TMSI,  
    i-RNTI,  
    ...  
}
```

3GPP TS 38.331 V15.3.0 (2018-09)

# ... y PIERCER para 4G

Obtención del IMSI de la víctima sin cracking, partiendo de ToRPEDO

4G



5G



# Inciso: GSMA CVD

## Coordinated Vulnerability Disclosure

The screenshot shows a web browser window with the URL <https://www.gsma.com/aboutus/workinggroups/working-groups/fraud-security-group/mobile-security-research-hall-fame>. The page features the GSMA logo and a navigation menu with links to About, What We Do, Membership, Services, Events, and News. A search bar is also present.

## Working Groups

Home > Fraud and Security Group

### Fraud and Security Group

Network Equipment Security Assurance Scheme

Security Algorithms

Security Advice for Mobile Phone Users

IMEI Database

Stolen Phone Checking

Security Accreditation Scheme

## Mobile Security Research Hall of Fame

Welcome to the GSMA Mobile Security Research Hall of Fame

# GSMA CVD

## Coordinated Vulnerability Disclosure

CVD-2018	0014	Elisa Bertino	Purdue University <a href="https://www.cs.purdue.edu/homes/bertino/">https://www.cs.purdue.edu/homes/bertino/</a>
CVD-2018	0014	Omar Chowdhury	University of Iowa <a href="http://homepage.divms.uiowa.edu/~comarhaider/">http://homepage.divms.uiowa.edu/~comarhaider/</a>
CVD-2018	0014	Mitziu Echeverria	University of Iowa
CVD-2018	0014	Syed Rafiul Hussain	Purdue University <a href="https://relentless-warrior.github.io/">https://relentless-warrior.github.io/</a>
CVD-2018	0014	Ninghui Li	Purdue University <a href="https://www.cs.purdue.edu/homes/ninghui/">https://www.cs.purdue.edu/homes/ninghui/</a>

## ToRPEDO, IMSI-Cracking (CONT.)

PO depende de...

## 3GPP TS 38.304 V15.0.0 (2018-06)

PF, PO are determined by the following formulae:

SFN for the PF is determined by:

$$(\text{SFN} + \text{PF\_offset}) \bmod T = (\text{T div N}) * (\text{UE\_ID mod N})$$

Index ( $i_s$ ), indicating the start of a set of PDCCH monitoring occasions

$$i_s = \text{floor}(\text{UE\_ID}/\text{N}) \bmod \text{Ns}; \text{ where, } \text{Ns} = \max(1, \text{nB}/\text{T})$$

UE\_ID: IMSI mod 1024

## 3GPP TS 38.304 V15.1.0 (2018-09)

PF, PO are determined by the following formulae:

SFN for the PF is determined by:

$$(\text{SFN} + \text{PF\_offset}) \bmod T = (\text{T div N}) * (\text{UE\_ID mod N})$$

Index ( $i_s$ ), indicating the start of a set of PDCCH monitoring occasions

$$i_s = \text{floor}(\text{UE\_ID}/\text{N}) \bmod \text{Ns}$$

UE\_ID: 5G-S-TMSI mod 1024

PO depende de...

## 3GPP TS 38

PF, PO are determined by

SFN for the PF is de

(SFN + PF\_offset)

Index ( $i_s$ ), indicatin

$i_s = \text{floor}(\text{UE}_$

(Suponiendo que el 5G-S-TMSI cambie continuamente)

(2018-09)

UE\_ID:



\_ID mod N)

CH monitoring occa

od 1024

# IMSI-Cracking (5G y 4G)

## IMSI-Cracking partiendo de ToRPEDO

- ▶ Sin ToRPEDO: Es IMSI-Cracking completo (31 bits en lugar de 24)
- ▶ El tiempo necesario crece exponencialmente



# Ataques de trazabilidad

Saber si un usuario es el mismo que otro visto antes

# #1 : Basin et al.

## Mensaje de fallo

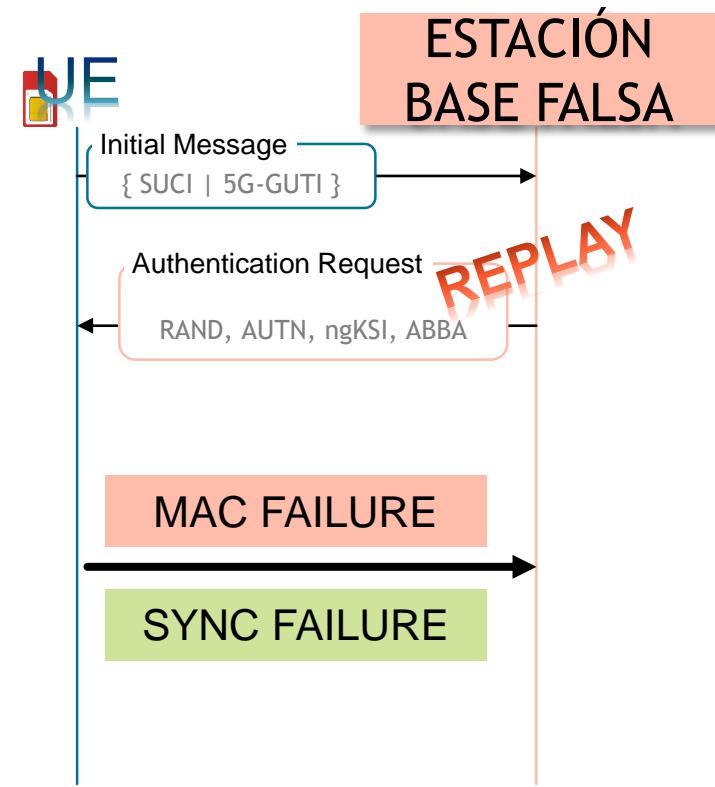
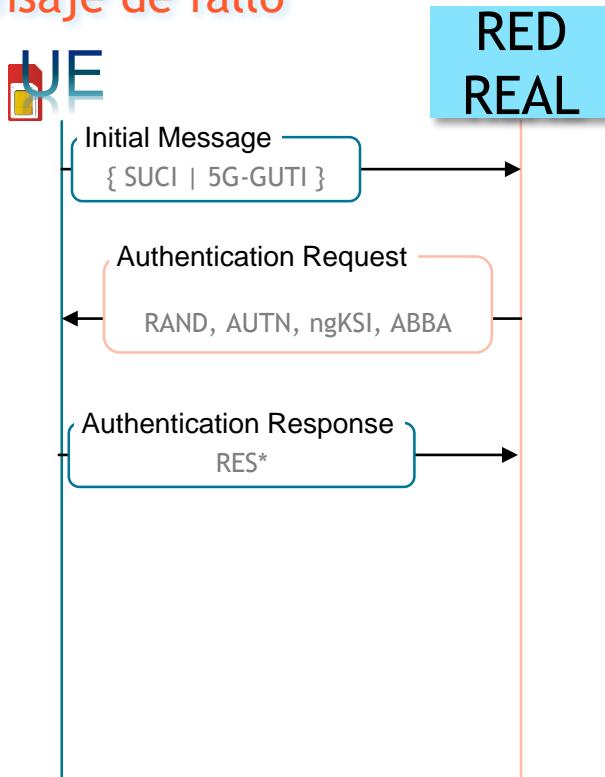
- ▶ 5G AKA proporciona privacidad del SUPI, pero no protección contra reenvío de mensajes
- ▶ El atacante observa y almacena un intercambio de mensajes 5G AKA de un UE de interés.
- ▶ Luego hace replay de esos mensajes hacia un UE para averiguar si es el mismo que el observado anteriormente:
  - ▶ Si es el mismo: SYNCHRONIZATION FAILURE
  - ▶ Si NO es el mismo: MAC FAILURE

2018

D. Basin, I. Dreier, L. Hirschi, S. Radomirović, R. Sasse and V. Stettler  
**A Formal Analysis of 5G Authentication**

## #1 : Basin et al.

## Mensaje de fallo



## #2 : Fouque et al.

### Reenvío de IMSI cifrado

- ▶ 5G AKA proporciona privacidad del SUPI, pero no protección contra reenvío de mensajes
- ▶ El atacante observa y almacena el mensaje inicial de identificación de un UE de interés en su diálogo 5G AKA normal
- ▶ Cuando quiere averiguar si un UE es el mismo que el observado anteriormente, captura su mensaje de identificación inicial (impide que llegue a la red real), lo reemplaza por el capturado antes, y deja continuar el diálogo:
  - ▶ Si es el mismo: el UE aceptará la respuesta de la red
  - ▶ Si NO es el mismo: MAC FAILURE

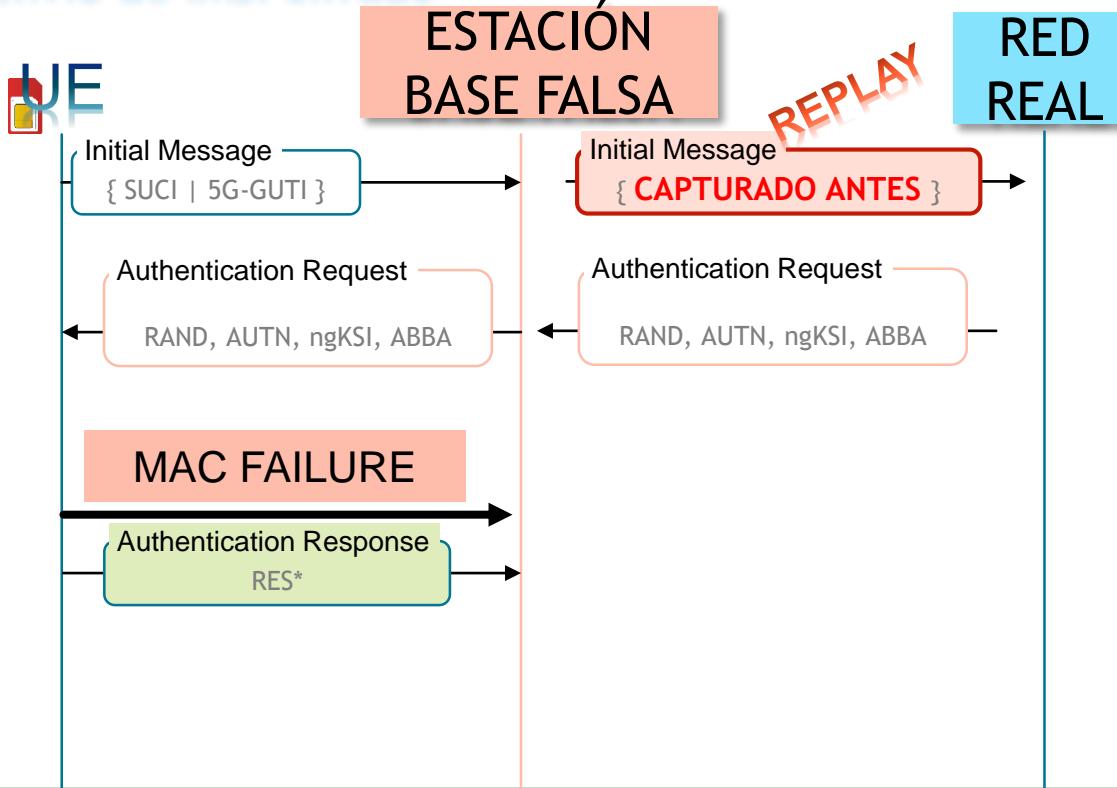
2018

P. Fouque, C. Onete, and B. Richard, "Achieving better privacy for the 3gpp AKA protocol," *PoPETs*, vol. 2016, no. 4, pp. 255–275, 2016.

Adrien Koutsos  
The 5G-AKA Authentication Protocol Privacy

## #2 : Fouque et al.

## Reenvío de IMSI cifrado



# #3 : Borgaonkar et al.

## Obtención del número de secuencia SQN

- ▶ El SQN de la HN para cada UE se incrementa con cada generación de challenge de autenticación para él
- ▶ El SQN del UE se incrementa con cada autenticación exitosa
- ▶ Cuando UE y HN se desincronizan, el UE envía un mensaje SYNCH FAILURE con el parámetro AUTS, que contiene el SQN del UE anonimizado con la clave AK (que solo depende del challenge y de la clave precompartida del usuario)
- ▶ El atacante obtiene varios challenge de la HN haciéndose pasar por la víctima (IMSI, TMSI o SUCI)
- ▶ Reenviando esos challenges varias veces a la víctima es capaz de obtener el SQN del UE
- ▶ Comparando con valores de SQN obtenidos anteriormente puede inferir:
  - ▶ Si es el mismo UE observado antes
  - ▶ Cuánta actividad ha realizado en ese tiempo

 sciendo Proceedings on Privacy Enhancing Technologies 2019

Ravishankar Borgaonkar, Lucca Hirschi\*, Shinjo Park, and Altaf Shaik

New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols

## Otro inciso: Análisis formales

Herramientas de validación de seguridad de protocolos

# Pruebas formales de seguridad de protocolos

## ► Método simbólico o Dolev-Yao

- El atacante controla la red. Puede ver, manipular y generar cualquier mensaje en la red siguiendo unas reglas fijas.
- Herramientas: **TAMARIN**, DEEPSEC, PROVERIF

## ► Método computacional

- El atacante también controla la red pero no está limitado a reglas fijas, sino que es modelado como máquinas de Turing
- Herramientas: CRYPTOVERIFY

## ► Método Bana-Comon

- El atacante puede hacer cualquier cosa excepto lo que se configure en reglas fijas.

2018

Adrien Koutsos

The 5G-AKA Authentication Protocol Privacy

# Tamarin Prover

The screenshot shows a web browser window with the URL <https://tamarin-prover.github.io>. The page content is identical to the one shown above, featuring the Tamarin Prover logo, navigation links, and the main text about the tool.

## Tamarin Prover

The Tamarin prover is a security protocol verification tool that supports both falsification and unbounded verification in the symbolic model. Security protocols are specified as multiset rewriting systems and analysed with respect to (temporal) first-order properties and a message theory that models Diffie-Hellman exponentiation and exclusive-or (XOR), combined with a user-defined rewriting theory that has the Finite Variant Property, which includes subterm-convergent theories.

## About / Core team:

[David Basin](#), [Cas Cremers](#), [Jannik Dreier](#), [Simon Meier](#), [Ralf Sasse](#), [Benedikt Schmidt](#)

Tamarin is a collaborative effort: see the [manual](#) for a more extensive overview of its development and additional contributors.

Current maintainers: [Cas Cremers](#), [Jannik Dreier](#), [Ralf Sasse](#)

# Tamarin Prover

Theory: Artificial \* +

127.0.0.1:3001/thy/trace/30/overview/proof/Characterize\_Fin/\_/Step1/Step1/Reveal\_key

Running TAMARIN 1.3.0 Index Download Actions » Options »

**Proof scripts**

```

theory Artificial begin
  Message theory
  Multiset rewriting rules (5)
  Raw sources (7 cases, deconstructions complete)
  Refined sources (7 cases, deconstructions complete)

  lemma Characterize_Fin:
    exists-trace "∃ k S #i. Fin( S, k ) @ #i"
    simplify ✘
    solve( St( S, k ) ▷ #i )
    case Step1
      solve( !KU( ~n ) @ #vk )
    case Step1
      solve( !KU( ~n.1 ) @ #vk.1 )
        case Reveal_key
          SOLVED // trace found
    qed
  qed
  qed

  lemma Fin_unique:
    all-traces

```

**Visualization display**

Constraint System is Solved

Constraint system

# Tamarin Prover

- ▶ Utilizado por Basin et al. para modelar y analizar 5G-AKA.
  - ▶ Modelan la comunicación con 3 elementos (UE - SN - HN)
  - ▶ Encuentran **AUTOMÁTICAMENTE** el ataque de trazabilidad descrito antes (replay de mensajes hacia el UE: SYNCH\_FAILURE/MAC\_FAILURE)
  - ▶ También encuentran **AUTOMÁTICAMENTE** una race condition en los mensajes intercambiados entre SN y HN: una sesión puede acabar asignada a otro usuario

2018

D. Basin, J. Dreier, L. Hirschi, S. Radomirović, R. Sasse and V. Stettler

**A Formal Analysis of 5G Authentication**

# Tamarin Prover

- ▶ Utilizado también por Cremers y Dehnel-Wild para modelar y analizar 5G-AKA.
  - ▶ Modelan la comunicación con 4 elementos (UE - SN - AUSF - ARPF) en lugar de 3
  - ▶ Además de verificar los hallazgos de Basin et al...
  - ▶ También encuentran **AUTOMÁTICAMENTE** una race condition en los mensajes intercambiados entre AUSF y ARPF en la HN: una sesión puede acabar asignada a otro usuario

Component-Based Formal Analysis of 5G-AKA:  
Channel Assumptions and Session Confusion

Cas Cremers

CISPA Helmholtz Center for Information Security, Germany  
[cremers@cispa.saarland](mailto:cremers@cispa.saarland)

Martin Dehnel-Wild

Department of Computer Science, University of Oxford  
[martin@dehnelwild.co.uk](mailto:martin@dehnelwild.co.uk)

# Problemas pendientes respecto a estaciones base falsas

# Technical Report

3GPP TR 33.809 V0.2.0 (2019-02)

*Technical Report*

**3rd Generation Partnership Project;  
Technical Specification Group Services and System Aspects;  
Study on 5G Security Enhancement against False Base Stations  
(Release 16)**

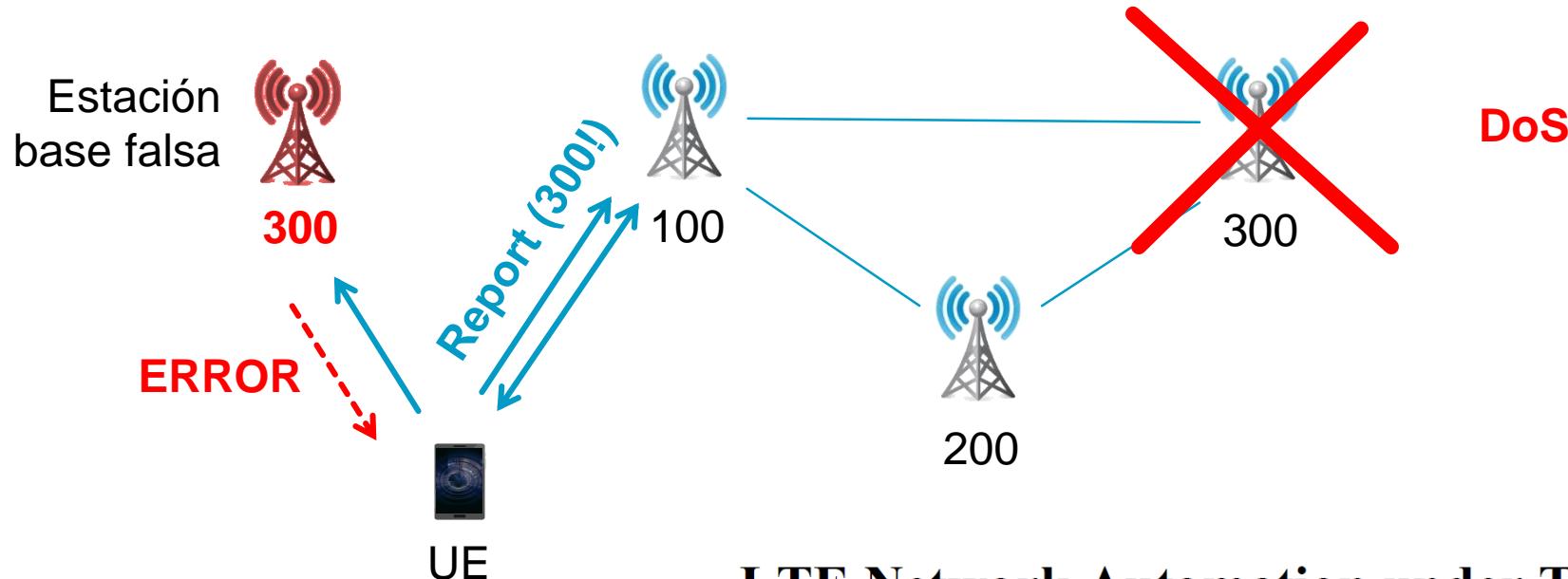


# Problemas pendientes de resolución respecto a estaciones base falsas

- ▶ Problema 1: Seguridad de mensajes unicast sin protección (RRC y NAS)
- ▶ Problema 2: Protección de información del Sistema (SI)
- ▶ Problema 3: Detección de estaciones base falsa cercanas
- ▶ Problema 4: Protección frente a envenamiento de SON
- ▶ Problema 5: Protección frente a authentication relay
- ▶ Problema 6: Resistencia frente a inhibición de radiofrecuencia

# Envenenamiento de SON

SON = Self Organized Network

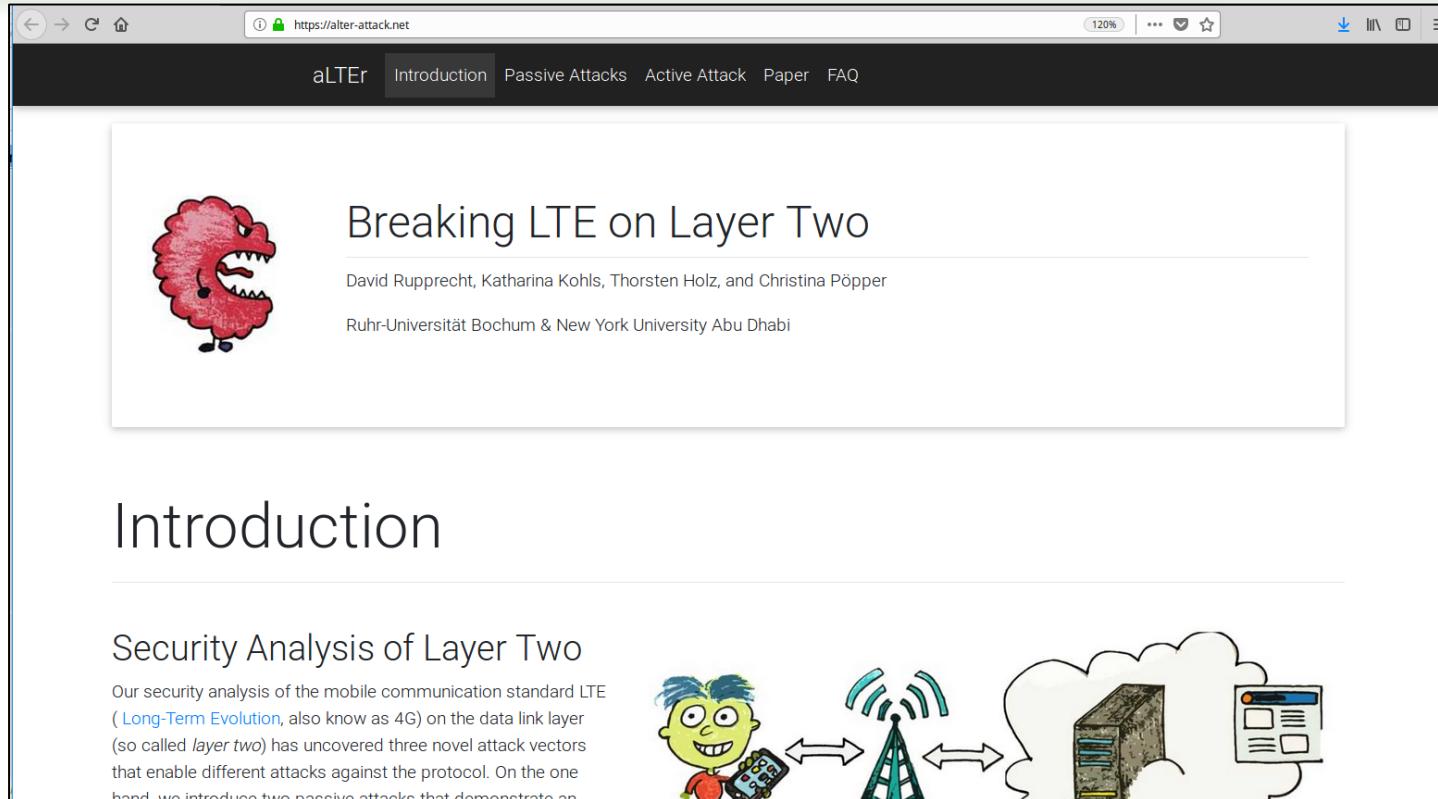


**LTE Network Automation under Threat**  
Altaf Shaik\*, Ravishankar Borgaonkar

# aLTEr ATTACK

No afecta a 5G... ¿o sí?

# aLTEr attack (<https://alter-attack.net>)



The screenshot shows the homepage of the [aLTEr attack](https://alter-attack.net) website. The URL is visible in the browser's address bar. The page features a navigation bar with links to "aLTEr", "Introduction", "Passive Attacks", "Active Attack", "Paper", and "FAQ". The main content area has a white background with a red cartoon monster icon on the left. The title "Breaking LTE on Layer Two" is centered above a horizontal line. Below the title, the authors' names are listed: David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper. The institutions involved are Ruhr-Universität Bochum & New York University Abu Dhabi. The "Introduction" section is currently selected, indicated by a larger font size. Below it, the "Security Analysis of Layer Two" section is described, mentioning three novel attack vectors against the LTE protocol. To the right of this text is a cartoon illustration showing a green-skinned character with blue hair holding a smartphone, connected by arrows to a cellular tower and a server in a cloud, with a computer monitor displaying a webpage.

## Introduction

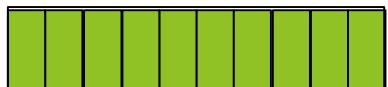
### Security Analysis of Layer Two

Our security analysis of the mobile communication standard LTE (Long-Term Evolution, also known as 4G) on the data link layer (so called *layer two*) has uncovered three novel attack vectors that enable different attacks against the protocol. On the one hand, we introduce two passive attacks that demonstrate an

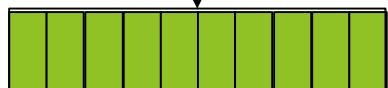
# aLTEr attack (<https://alter-attack.net>)

Manipulación de ciphertext en AES-CTR (AES en counter mode)

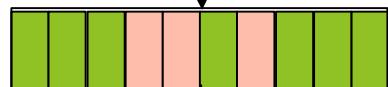
PLAINTEXT - p



CIPHERTEXT - c



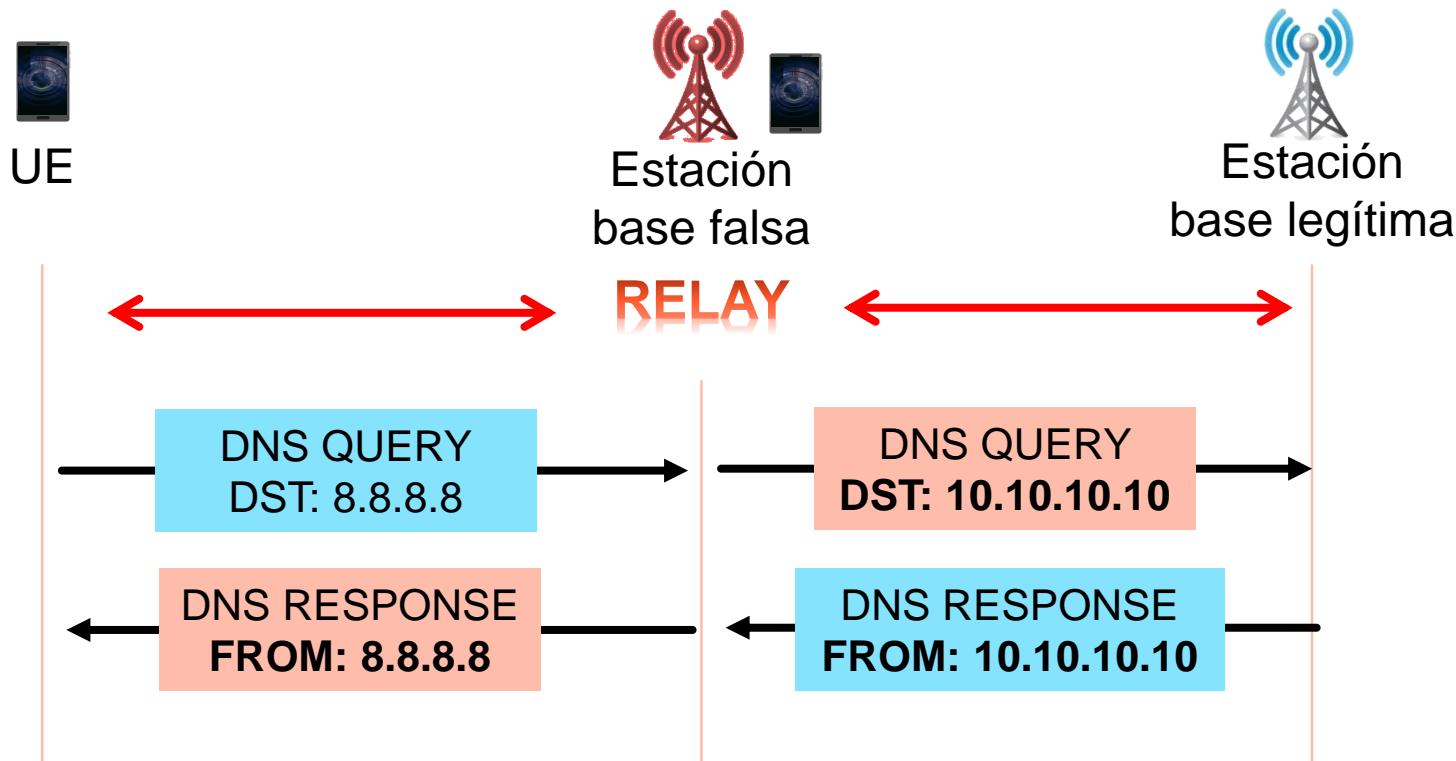
CIPHERTEXT – c'



PLAINTEXT – p'

# aLTEr attack (<https://alter-attack.net>)

PoC



# ¿Podría afectar aLTEr a 5G?



# ¿Protección de integridad para datos de usuario?

► En 5G sí, pero... es opcional, así que:



## Ataques de señalización

¿Es SBA más seguro que de SS7 y DIAMETER?

# ¿Es SBA más seguro que SS7 o DIAMETER?

Release 15 9 3GPP TS 29.500 V15.3.0 (2019-03)

## 5 Protocols Over Service Based Interfaces

### 5.1 Protocol Stack Overview

The protocol stack for the service based interfaces is shown on Figure 5.1-1.

The diagram shows a vertical stack of protocol layers. From top to bottom, the layers are: Application, HTTP/2, TLS, TCP, IP, and L2. A dashed horizontal line separates the TLS layer from the TCP layer.

**Figure 5.1-1: SBI Protocol Stack**

The service based interfaces use HTTP/2 protocol (see subclause 5.2) with JSON (see subclause 5.4) as the application layer serialization protocol. For the security protection at the transport layer, all 3GPP NFs shall support TLS and TLS shall be used within a PLMN if network security is not provided by other means, as specified in 3GPP TS 33.501 [17].



# ¿Es SBA más seguro que SS7 o DIAMETER?

VULNERABILIDADES PUBLICADAS:

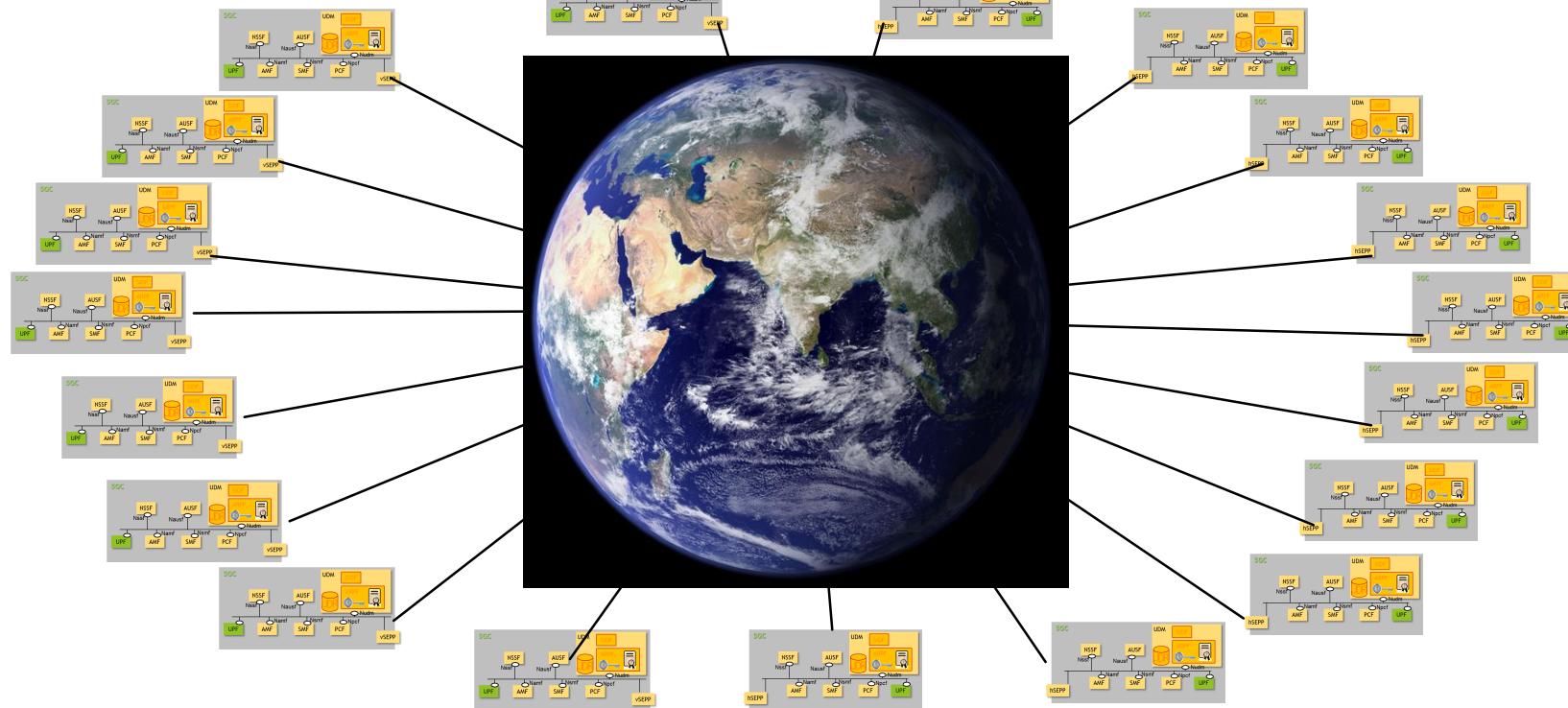
# ¿Es SBA más seguro que SS7 o DIAMETER?

## Modelo de confianza



# ¿Es SBA más seguro que SS7 o DIAMETER?

## Modelo de confianza



**5G**





[www.layakk.com](http://www.layakk.com)

@layakk

¡Gracias!

/Rooted<sup>®</sup> CON

# Seguridad 5G

Una introducción a los aspectos más relevantes de Seguridad de la nueva generación de comunicaciones móviles

José Picó

David Pérez