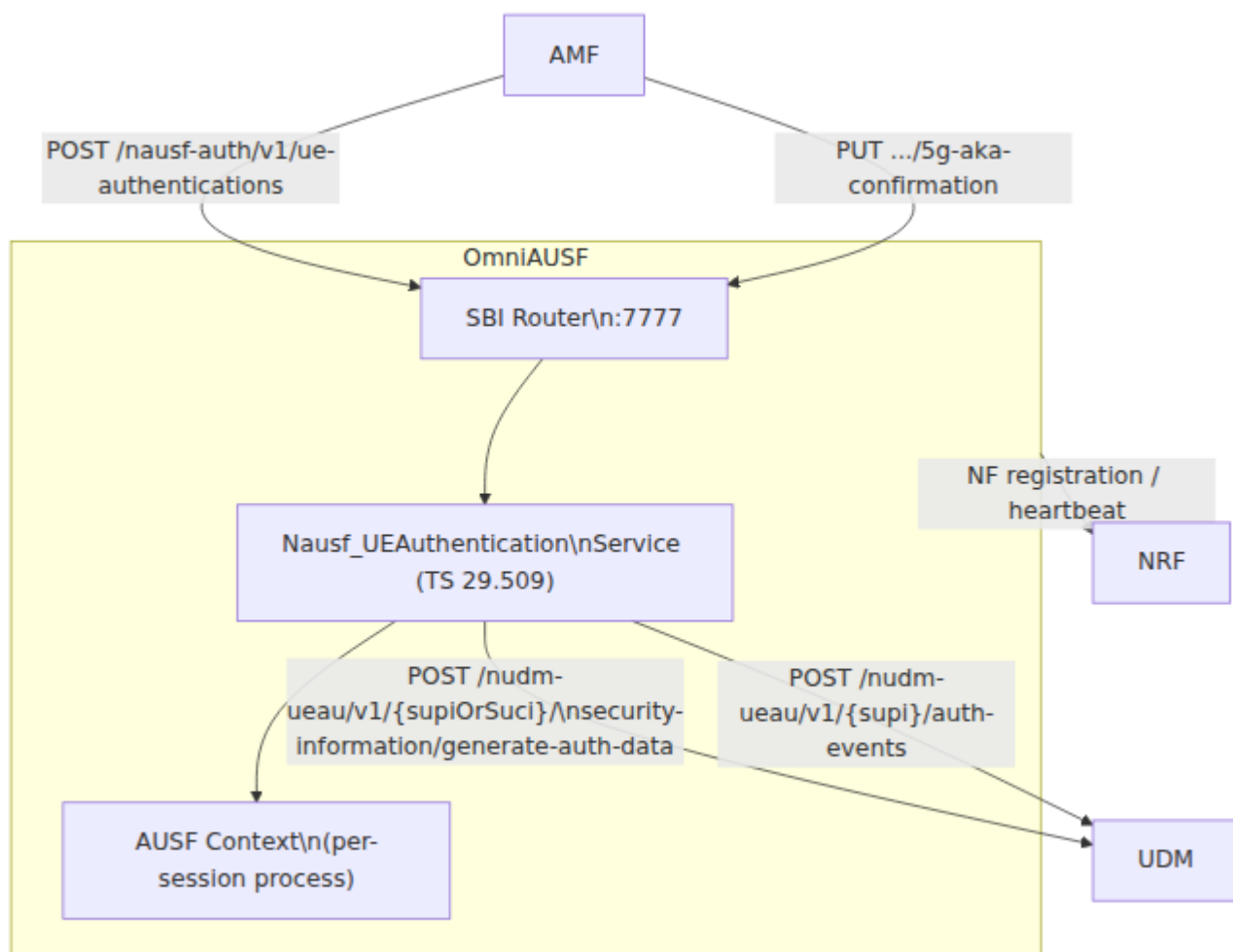


Operaciones de OmniAUSF

1. Visión General del Componente

OmniAUSF es la Función del Servidor de Autenticación (AUSF) independiente para el núcleo 5G de Omnitouch. Orquesta la autenticación 5G-AKA entre el AMF y el UDM, verificando las respuestas de autenticación del UE y derivando claves de sesión. OmniAUSF estaba anteriormente co-localizado dentro de OmniUDM y ahora se despliega como un NF independiente con su propio punto final SBI.

Cada sesión de autenticación es gestionada por un proceso dedicado (proceso-por-sesión-de-autenticación). El contexto de autenticación se mantiene en memoria durante la duración del intercambio de autenticación y se elimina al completarse o fallar.



2. Referencias de Rol y Especificación de 3GPP

Aspecto	Referencia
Definición funcional de AUSF	TS 23.501 Sección 6.2.8
Servicio Nausf_UEAuthentication	TS 29.509
Autenticación 5G-AKA	TS 33.501 Sección 6.1.3
Cálculo de HXRES*/HRES*	TS 33.501 Anexo A.5
Derivación de KSEAF	TS 33.501 Anexo A.6
Generación de datos de autenticación UDM	TS 29.503 Sección 5.2.2
Resincronización de SQN	TS 33.102 Sección 6.3.5, TS 33.501 Sección 6.1.3.4

3. Puntos Finales SBI

Todos los puntos finales son HTTP/1.1 con `Content-Type: application/json`.

Nausf_UEAauthentication (TS 29.509)

Método	Ruta	Descripción	Éxito
POST	<code>/nausf-auth/v1/ue-authentications</code>	Iniciar autenticación UE (AMF -> AUSF)	201 Creado
PUT	<code>/nausf-auth/v1/ue-authentications/{authCtxId}/5g-aka-confirmation</code>	Confirmar 5G-AKA (AMF envía RES*)	200 OK

Respuestas de Error

Estado HTTP	Causa	Condición
404	USER_NOT_FOUND	UDM devolvió 404 para el suscriptor
401	AUTHENTICATION_FAILURE	HRES* no coincide con HXRES*
500	SYSTEM_FAILURE	Error interno o UDM inalcanzable

4. Referencia de Configuración

OmniAUSF se configura a través del entorno de aplicación Elixir bajo la clave `:omniausf`.

Ejemplo de Configuración

```
config :omniausf,  
  sbi_scheme: "http",  
  sbi_addr: "127.0.0.19",  
  sbi_port: 7777,  
  nrf_uri: "http://127.0.0.10:7777",  
  udm_uri: "http://127.0.0.12:7777",  
  mcc: "999",  
  mnc: "70",  
  heartbeat_interval: 10_000
```

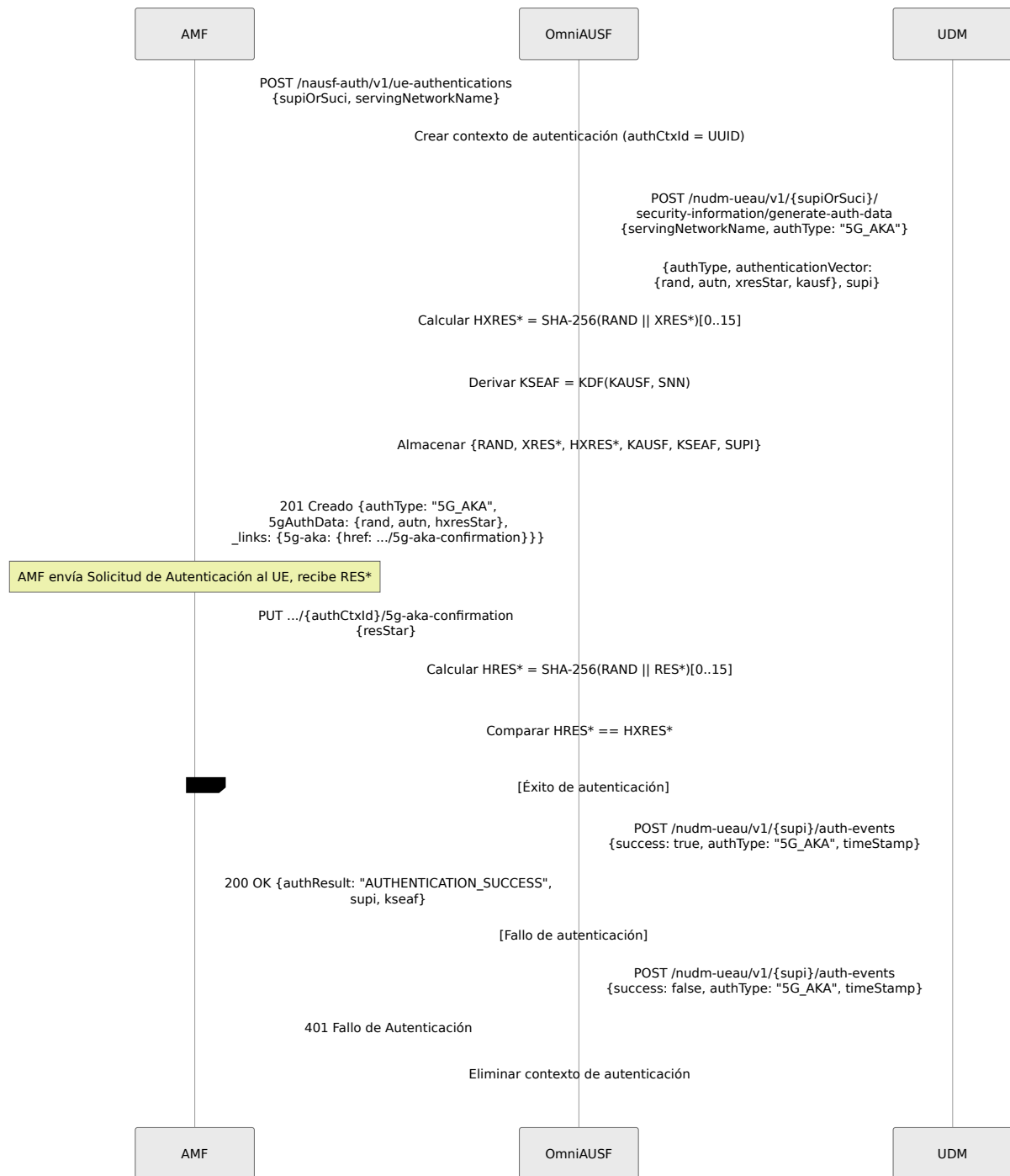
Tabla de Parámetros

Parámetro	Tipo	Por Defecto	Descripción
sbi_scheme	cadena	"http"	Esquema URL para el servicio HTTP SBI
sbi_addr	cadena	"127.0.0.19"	Dirección IP a la que se vincula el servidor HTTP SBI
sbi_port	entero	7777	Puerto TCP en el que escucha el servidor HTTP SBI
nrf_uri	cadena	"http://127.0.0.10:7777"	URI base del NRF para el registro NF y latido
udm_uri	cadena	"http://127.0.0.12:7777"	URI base del UDM para la generación de vectores de autenticación y almacenamiento de eventos de autenticación
mcc	cadena	"999"	Código de País Móvil para el PLMN que presta servicio

Parámetro	Tipo	Por Defecto	Descripción
mnc	cadena	"70"	Código de Red Móvil para el PLMN que presta servicio
heartbeat_interval	entero (ms)	10000	Intervalo en que OmniAUS envía solicitud PATCH de latencia NRF

5. Procedimientos Clave

5.1 Flujo de Autenticación 5G-AKA



6. Métricas de Prometheus

Métricas de AUSF

Métrica	Tipo	Etiquetas	Descripción
<code>omni_ausf.auth.count</code>	contador	<code>result</code>	Total de operaciones de autenticación (iniciadas/éxito/fallo)
<code>omni_ausf.nrf.registration.status</code>	gauge	<code>nf_type</code>	Estado de registro NRF (1=registrado, 0=no)
<code>omni_ausf.active_contexts.count</code>	gauge	--	Número de contextos de autenticación UE AUSF activos

Métricas de BEAM VM

Métrica	Tipo	Descripción
<code>beam.memory.total</code>	gauge	Memoria total de BEAM en bytes
<code>beam.memory.processes</code>	gauge	Memoria utilizada por procesos Erlang
<code>beam.memory.system</code>	gauge	Memoria del sistema (ETS, átomos, código)
<code>beam.processes.count</code>	gauge	Número de procesos Erlang
<code>beam.vm.uptime</code>	gauge	Tiempo de actividad de la VM en segundos

7. Limitaciones Conocidas

ID	Área	Descripción
AUSF-1	Estado en memoria	Los contextos de autenticación se almacenan solo en memoria. El estado se pierde al reiniciar el proceso. Las sesiones de autenticación activas fallarán al reiniciar el AUSF; el AMF debe reiniciar la autenticación
AUSF-2	EAP-AKA'	Solo se admite 5G-AKA. El método de autenticación EAP-AKA' (TS 33.501 Sección 6.1.3.1) no está implementado
AUSF-3	Reenvío de resincronización	El AUSF no maneja de forma independiente <code>resynchronizationInfo</code> ; lo pasa al UDM. El AMF debe incluir <code>resynchronizationInfo</code> en la solicitud de autenticación inicial

8. Solución de Problemas

La autenticación falla con 404 Usuario No Encontrado

El UDM devolvió 404 para el suscriptor. Confirme:

1. `udm_uri` es accesible desde el host de OmniAUSF.
2. El IMSI del suscriptor existe en el backend de UDM/UDR/HSS.
3. El SUCI presentado por el AMF está correctamente formateado.

La autenticación falla con 401 Fallo de Autenticación

El AUSF calculó HRES* a partir del RES* recibido y no coincidió con el HXRES* almacenado. Esto indica que las credenciales del UE (Ki, OPc) no coinciden con las del backend, o que el RAND/AUTN se corrompió en tránsito.

UDM inalcanzable (500 Error Interno)

Verifique la configuración de `udm_uri` y la conectividad de red. El AUSF registra `AUSF auth failed for {supiOrSuci}: {reason}` en caso de fallo de comunicación con el UDM.

Contexto de autenticación no encontrado en la confirmación

El `authCtxId` en la solicitud PUT no coincide con ningún contexto activo. Los contextos se eliminan después de una confirmación exitosa o fallida, y se pierden al reiniciar el AUSF. El AMF debe reiniciar la autenticación.