← Resumen

Configuración de OmniUDM

OmniUDM se configura a partir de variables de entorno al inicio a través de `config/runtime.exs`, bajo la clave de aplicación `:omniudm`. Cada valor tiene un valor predeterminado incorporado, por lo que el proceso comienza sin entorno establecido; las implementaciones en producción deben establecer al menos los valores de SBI, NRF, UDR, PLMN y `hnet_key_dir`.

Ejemplo de Configuración

```
config :omniudm,
  udr_uri: "http://127.0.0.22:7777",
  sbi_scheme: "http",
  sbi_addr: "127.0.0.12",
  sbi_port: 7777,
  nrf_uri: "http://127.0.0.1:7777",
  mcc: "999",
  mnc: "70",
  prometheus_metrics_port: 9568,
  heartbeat_interval: 10_000,
  hnet_key_dir: "/etc/omniudm/hnet"

config :logger, :default_formatter,
  format: {OmniLogger.JsonFormatter, :format},
  metadata: :all
```

Referencia de Parámetros

Parámetro	Tipo	Requerido	Predeterminado
`udr_uri`	string (URI)	No	`http://127.0.0.22:777`
`sbi_scheme`	string	No	`http`
`sbi_addr`	string (IP)	No	`127.0.0.12`

Parámetro	Tipo	Requerido	Predeterminado
`sbi_port`	integer	No	`7777`
`nrf_uri`	string (URI)	No	`http://127.0.0.1:7777`
`mcc`	string	No	`999`
`mnc`	string	No	`70`
`prometheus_metrics_port`	integer	No	`9568`

Parámetro	Tipo	Requerido	Predeterminado
`heartbeat_interval`	integer (ms)	No	`10000`
`hnet_key_dir`	string (path)	No	`/etc/omniudm/hnet`

Claves de Ajuste Opcionales

Estas claves se leen de la configuración de la aplicación y no se presentan como variables de entorno en `runtime.exs`; configúralas en la configuración si una implementación necesita anular los valores predeterminados.

Parámetro	Tipo	Predeterminado	Descripción
`default_nssai`	map	eMBB / URLLC / mIoT lab slices (ver abajo)	NSSAI de reserva que se devuelve por `GET /{supi}/nssai` cuando la respuesta `am-data` del UDR no lleva un `nssai` explícito. Establecer esto para publicitar los verdaderos slices de la red, incluyendo S-NSSAIs calificados por SD
`nf_capacity`	integer (0-65535)	Predeterminado de la aplicación	Capacidad de procesamiento relativa de esta instancia de NF publicitada en el perfil de NF registrado con el NRF. Los consumidores ponderan la selección de NF por capacidad. Ajustable en tiempo de ejecución a través del endpoint PATCH de configuración OAM (`PATCH /api/oam/config/{id}`); típicamente no tiene una variable de entorno dedicada
`nf_priority`	integer (0-65535)	Predeterminado de la aplicación	Prioridad de selección relativa de esta instancia de NF publicitada en el perfil de NF registrado con el NRF (un valor más bajo es mayor prioridad). Ajustable en tiempo de

Parámetro	Tipo	Predeterminado	Descripción
			ejecución a través del endpoint PATCH de configuración OAM (`PATCH /api/oam/config/{id}`); típicamente no tiene una variable de entorno dedicada

El `default_nssai` de reserva incorporado publicita `defaultSingleNssais` de `sst 1` (y `sst 1 / sd 000001`) y `singleNssais` que cubren `sst 1`, `sst 1 / sd 000001`, `sst 2 / sd 000002` (URLLC), y `sst 3 / sd 000003` (mIoT). Un suscriptor ofrecido un slice que el AMF no está configurado para servir es rechazado con el motivo 5GMM #62, por lo que esta reserva debe coincidir con lo que la red realmente sirve.

El valor es un objeto `Nssai` (TS 29.503 / TS 29.571) con los siguientes subcampos:

Campo	Tipo	Semántica
`defaultSingleNssais`	lista de S-NSSAI	Slices que el UE puede usar *sin* solicitarlos explícitamente - el conjunto predeterminado suscrito que el AMF aplica cuando el UE no solicita NSSAI. Debe ser un subconjunto de `singleNssais`
`singleNssais`	lista de S-NSSAI	El conjunto completo de slices suscritos a los que el UE tiene derecho en este PLMN

Cada entrada de S-NSSAI es un mapa:

Campo	Tipo	Semántica
`sst`	integer (0–255)	Tipo de Slice/Servicio. Valores estandarizados: `1` = eMBB, `2` = URLLC, `3` = mIoT
`sd`	string (6 dígitos hexadecimales)	Diferenciador de Slice opcional que califica el `sst`. Omitir para un slice solo SST; un SST que la red sirve *solo* en forma calificada por SD debe ser listado con su `sd` (una entrada no calificada no coincidirá)

Un S-NSSAI en `defaultSingleNssais` que no esté también presente en `singleNssais`, o un slice aquí que ningún AMF esté configurado para servir, lleva al AMF a rechazar el UE con el motivo 5GMM #62.

Claves de Red de Hogar (`hnet_key_dir`)

`hnet_key_dir` es el directorio que contiene las claves privadas de la Red de Hogar utilizadas para la de-concealment de SUCI del Perfil ECIES A/B. Cada SIM se provisiona con una clave **pública** de la Red de Hogar y su identificador de clave (`home_network_public_key_id`); OmniUDM debe mantener la clave **privada** correspondiente bajo ese mismo identificador.

Los archivos de clave se cargan una vez en el primer uso y se almacenan en caché en memoria. Se tolera un directorio que no existe (se registra una advertencia y la de-concealment de ECIES se desactiva efectivamente - los SUCIs de esquema nulo aún funcionan).

Nomenclatura de archivos. El identificador de clave y la curva se toman del nombre del archivo. Se aceptan dos convenciones:

Convención	Perfil A (Curve25519)	Perfil B (P-256)
Punto `<id>.<curve>.key`	`1.x25519.key`	`2.secp256r1.key`
Guion `<curve>-<id>.key`	`curve25519-1.key` o `x25519-1.key`	`secp256r1-2.key`

El `<id>` numérico debe coincidir con el `home_network_public_key_id` provisionado en la SIM. Los archivos que no coinciden con un patrón reconocido, y los archivos sin una extensión `.key`, se omiten con una advertencia.

Contenido del archivo. Cada archivo contiene la clave privada en una de tres codificaciones, detectadas automáticamente:

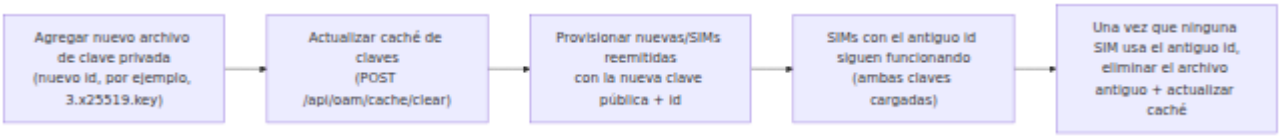
- **PEM** - PKCS#8 (`-----BEGIN PRIVATE KEY-----`) o SEC1 (`-----BEGIN EC PRIVATE KEY-----`). El escalar privado en bruto se extrae automáticamente. Este es el formato de campo recomendado.
- **Hex** - una única cadena codificada en hexadecimales de los bytes de la clave privada en bruto.
- **Raw** - los bytes de la clave privada en bruto tal como están.

Un único archivo de clave corrupto o mal formado se omite (se registra como una advertencia) sin impedir que las otras claves se carguen.

Cómo un identificador de clave se mapea a una SIM. Un SUCI lleva el identificador de clave que la SIM utilizó para ocultar su SUPI: `suci-0-<mcc>-<mnc>-<routing-ind>-<scheme>-<home_nw_pub_key_id>-<scheme_output>`. OmniUDM lee `<home_nw_pub_key_id>` del SUCI y selecciona el archivo de clave privada cuyo `<id>` numérico coincide. Por lo tanto, varios identificadores de clave pueden ser servidos a la vez - un archivo por identificador en uso a través de la propiedad de SIM - y un SUCI cuyo identificador no tiene clave cargada falla con `unknown_home_network_key_id`.

Rotación de una clave de Red de Hogar (sin tiempo de inactividad). Debido a que la de-concealment se basa en el identificador y múltiples

identificadores coexisten, una clave se cambia introduciendo un *nuevo* identificador junto al antiguo en lugar de sobrescribir un archivo en su lugar:



Sobrescribir el archivo para un identificador que aún se usa en SIMs activas rompe la de-concealment para esas SIMs (presentan la antigua clave pública, la verificación MAC falla). Siempre retira un identificador solo después de que cada SIM que lo usa haya sido reprovisionada en uno nuevo.

Cuidado operativo.

- Trata el contenido de `hnet_key_dir` como material secreto altamente sensible - la compromisión de una clave privada de Red de Hogar permite a cualquier parte de-conceal SUCIs para ese identificador de clave. Restringe los permisos de directorio y archivo solo a la cuenta de servicio de OmniUDM.
- La clave privada aquí debe ser la contraparte de la clave pública provisionada en las SIM para el mismo identificador de clave. Una discrepancia causa que la verificación MAC falle y la autenticación sea rechazada.
- Las claves se almacenan en caché después de la primera carga. Después de agregar, reemplazar o eliminar archivos de clave, la caché debe actualizarse (ver la acción de gestión de limpieza de caché OAM, `POST /api/oam/cache/clear`) o el proceso reiniciado para que el cambio surta efecto.

API de Gestión / OAM

Se sirve una API de gestión/OAM HTTPS (puerto predeterminado `8443`, TLS habilitado) para inspección y control operativo. Es separada del listener SBI.

Método	Ruta	Propósito
GET	`/api/status/api`	Estado de la API de gestión
GET	`/api/status/license`	Estado de la licencia
GET	`/api/status/nrf`	Estado del registro NRF
GET	`/api/status/nf`	Resumen del estado de NF
GET	`/api/ue`	Listar contextos UE activos en memoria
GET	`/api/ue/{supi}`	Inspeccionar un solo contexto UE por SUPI
GET	`/api/statistics`	Estadísticas del servicio, incluyendo un conteo en vivo de contextos UE activos en memoria
GET	`/api/oam/config`	Leer configuración efectiva actual
PATCH	`/api/oam/config/{id}`	Actualizar un valor de configuración (también se acepta PUT)
DELETE	`/api/oam/ue_cache/{id}`	Evictar un contexto UE de la caché en memoria
POST	`/api/oam/ue/sdm-notify`	Activar manualmente una notificación de cambio de datos SDM para un SUPI. Envía un `ModificationNotification` a cada `callbackReference` de suscripción SDM activa (por ejemplo, después de cambios de

Método	Ruta	Propósito
		aprovisionamiento fuera de banda)
DELETE	`/api/oam/ue/amf-registration/{id}`	Forzar la desregistración AMF para un UE. Limpia el registro 3GPP AMF almacenado *y* notifica al AMF que sirve en su `deregCallbackUri` para que libere el UE (razón de desregistro `SUBSCRIPTION_WITHDRAWN`); devuelve 404 si el UE no tiene registro AMF
POST	`/api/oam/cache/clear`	Limpiar cachés (incluyendo la caché de claves de Red de Hogar)
POST	`/api/oam/log_level`	Cambiar el nivel de registro en tiempo de ejecución (`{"level": ...}`)
GET	`/api/oam/resources`	Inventario de recursos
GET	`/api/oam/diagnostics`	Instantánea de diagnóstico
POST	`/api/oam/nrf/reregister`	Forzar re-registro con el NRF

Registro

Configuración	Valor	Descripción
`format`	`{OmniLogger.JsonFormatter, :format}`	Las líneas de registro se emiten como JSON estructurado a través del formateador compartido OmniLogger, adecuado para la ingestión por un agregador de registros
`metadata`	`:all`	Todos los metadatos de registro (incluyendo el contexto de sesión por solicitud como SUPI y procedimiento) se incluyen en cada línea

El nivel de registro en tiempo de ejecución se puede cambiar sobre la marcha a través de la API de Gestión/OAM (`POST /api/oam/log_level`). El material clave (CK/IK/KAUSF/SQN⊕AK) nunca se registra; solo el contexto no secreto como el nombre de la red que sirve y el SUPI de-concealado aparece en los registros.

← Resumen

Métricas de OmniUDM

Las métricas se exponen en formato Prometheus en `prometheus_metrics_port` (por defecto `9568`) en `/metrics`.

Métricas del Servicio UDM

Métrica	Tipo	Etiquetas	De
`omni_udm_auth_requests_count`	contador	`supi`, `result`	Sol vec aut por (`su` `fai`
`omni_udm_auth_vector_generations_total`	contador	`result`	Inte ger de aut por
`omni_udm_auth_result_count`	contador	`supi`, `result`	Eve res aut reg trav `aut` (`re` val `suc` rep
`omni_udm_uecm_registrations_total`	contador	`access_type`	Reg UE trav am acc Tan ruta reg 3GI

Métrica	Tipo	Etiquetas	De
			no inc est cor eti por `acc` (`3g` `nor`
`omni_udm_sdm_queries_total`	contador	`data_type`	Cor dat por dat `dat` `dat` `sel` `nss` `con` `smf` `dat`
`omni_udm_active_ue_contexts_count`	medidor	ninguno	Núr cor act me Em cre elir de UE
`omni_udm_nrf_registration_status`	medidor	`nf_type`	Est reg (`1`

Métrica	Tipo	Etiquetas	De
			reg = r

Consultas Útiles

```
# Tasa de fallos de autenticación en 5 minutos
sum(rate(omni_udm_auth_requests_count{result="failure"}[5m]))
  / sum(rate(omni_udm_auth_requests_count[5m]))

# Tasa de consultas SDM por tipo de dato
sum by (data_type) (rate(omni_udm_sdm_queries_total[5m]))

# Tasa de registro UECM dividida por tipo de acceso (3gpp /
non_3gpp)
sum by (access_type) (rate(omni_udm_uecm_registrations_total[5m]))

# Tasa de fallos en la generación de vectores de autenticación
sum(rate(omni_udm_auth_vector_generations_total{result="failure"}
[5m]))
  / sum(rate(omni_udm_auth_vector_generations_total[5m]))

# Alerta si el UDM no está registrado con el NRF
min(omni_udm_nrf_registration_status) < 1
```

`omni_udm_active_ue_contexts_count` rastrea el número vivo de contextos UE activos en memoria; se actualiza en cada creación y eliminación de contexto UE. Los endpoints OAM `/api/statistics` y `/api/status/nf` informan el mismo conteo a demanda.

Métricas de BEAM VM

Métrica	Tipo	Descripción
`beam_memory_total`	medidor	Memoria total de BEAM (bytes)
`beam_memory_processes`	medidor	Memoria asignada a procesos Erlang
`beam_memory_processes_used`	medidor	Memoria realmente utilizada por procesos
`beam_memory_system`	medidor	Memoria del sistema (ETS, átomos, código)
`beam_memory_atom`	medidor	Memoria total de átomos
`beam_memory_atom_used`	medidor	Memoria de átomos utilizada
`beam_memory_binary`	medidor	Memoria binaria
`beam_memory_code`	medidor	Memoria de código
`beam_memory_ets`	medidor	Memoria de tabla ETS
`beam_processes_count`	medidor	Número de procesos Erlang
`beam_ports_count`	medidor	Número de puertos Erlang
`beam_atom_count`	medidor	Número de átomos
`beam_vm_uptime`	medidor	Tiempo de actividad de la VM (segundos)

← Resumen

Operaciones de OmniUDM

OmniUDM es la función de Gestión Unificada de Datos (UDM) del núcleo 5G de Omnitouch. Presenta la identidad del suscriptor, la suscripción y los datos de contexto al resto del núcleo a través de los servicios estándar de Nudm, respaldando todos los datos autorizados en el Repositorio de Datos Unificado (OmniUDR) a través de `nudr-dr`.

Rol de 3GPP y Referencias de Especificación

Aspecto	Referencia
Rol funcional de UDM en el 5GC	TS 23.501
Servicios de Nudm (SDM / UEAU / UECM)	TS 29.503
Nudr_DataRepository (consumido)	TS 29.504
Esquemas de ocultación y protección de SUCI / SUPI	TS 33.501 §6.12 y Anexo C
Estructura y codificación de SUCI / SUPI	TS 23.003 §2.2B
Autenticación 5G-AKA y jerarquía de claves	TS 33.501 §6.1.3, Anexo A
Codificación de identidad móvil (SUCI/MSIN BCD)	TS 24.501

Interfaces y Puntos de Acceso SBI

OmniUDM registra los siguientes servicios con el NRF y los sirve en el listener SBI (`sbi_scheme://sbi_addr:sbi_port`):

Servicio	Versión	Propósito
`nudm-sdm`	v2	Gestión de datos del suscriptor
`nudm-ueau`	v1	Generación de vectores de autenticación de UE
`nudm-uecm`	v1	Gestión del contexto de UE (registro AMF/SMF)

Todos los datos autorizados del suscriptor y del contexto se leen desde / escriben en OmniUDR a través de `nudr-dr/v2` (ruta base `.../nudr-dr/v2/subscription-data/{ueId}/...`). Todos los cuerpos de solicitud/respuesta son JSON. Los errores se devuelven como `application/problem+json` ProblemDetails.

Nudm_UEAuthentication (`nudm-ueau/v1`)

Método	Ruta	Descripción
POST	`/{supiOrSuci}/security-information/generate-auth-data`	Generar un vector de autenticación 5G-AKA. Acepta un SUPI o SUCI; primero oculta SUCI. Requiere `servingNetworkName` y `ausfInstanceId`
POST	`/{supi}/auth-events`	Registrar un evento de resultado de autenticación. Requiere `nfInstanceId`, `success`, `timeStamp`, `authType`, `servingNetworkName`
PUT	`/{supi}/auth-events/{authEventId}`	Actualizar / eliminar un evento de autenticación (el cuerpo de AuthEvent, `authRemovalInd=true` lo elimina)

Nudm_UECM (`nudm-uecm/v1`)

Método	Ruta	Descripción
PUT	`/{supi}/registrations/amf-3gpp-access`	AMF registra acceso 3GPP para un UE
PATCH	`/{supi}/registrations/amf-3gpp-access`	Actualizar parámetros de la inscripción 3GPP AMF almacenada (merge-patch)
GET	`/{supi}/registrations/amf-3gpp-access`	Recuperar la inscripción 3GPP AMF almacenada
PUT	`/{supi}/registrations/amf-non-3gpp-access`	AMF registra acceso no 3GPP para un UE
GET	`/{supi}/registrations/amf-non-3gpp-access`	Recuperar la inscripción no 3GPP AMF almacenada
PUT	`/{supi}/registrations/smf-registrations/{pduSessionId}`	SMF registra un contexto de sesión PDU
DELETE	`/{supi}/registrations/smf-registrations/{pduSessionId}`	SMF desregistra un contexto de sesión PDU

Nudm_SDM (`nudm-sdm/v2`)

Método	Ruta	Descripción
GET	`/{supi}`	GetDataSets - recuperar múltiples conjuntos de datos seleccionados por el parámetro de consulta obligatorio `dataset-names` (separados por comas `AM`, `SM`, `SMF_SEL`, `UEC_SMF`)
GET	`/{supi}/am-data`	Datos de suscripción de acceso y movilidad (consulta opcional `plmn-id`)
GET	`/{supi}/sm-data`	Datos de suscripción de gestión de sesiones (consulta opcional `plmn-id`)
GET	`/{supi}/smf-select-data`	Datos de suscripción de selección de SMF (consulta opcional `plmn-id`)
GET	`/{supi}/nssai`	Datos de suscripción de selección de corte de red
GET	`/{supi}/ue-context-in-smf-data`	Contexto de UE en SMF (sesiones PDU activas): ver nota a continuación
POST	`/{supi}/sdm-subscriptions`	Suscribirse a notificaciones de cambio de datos. Requiere `nfInstanceId`,

Método	Ruta	Descripción
		`callbackReference`, `monitoredResourceUris`
GET	`/{supi}/sdm-subscriptions/{subscriptionId}`	Recuperar una suscripción SDM almacenada
PATCH	`/{supi}/sdm-subscriptions/{subscriptionId}`	Modificar una suscripción SDM (merge-patch)
DELETE	`/{supi}/sdm-subscriptions/{subscriptionId}`	Eliminar una suscripción SDM

Ocultación de SUCI / SUPI

Para proteger la identidad permanente del suscriptor a través del aire, el UE envía un **SUCI** (Identificador Oculto de Suscripción) en lugar del **SUPI** (Identificador Permanente de Suscripción, es decir, `imsi-<IMSI>`). Cuando el AUSF pide a OmniUDM que genere un vector de autenticación para un SUCI, OmniUDM **de-oculta el SUCI al SUPI** antes de que pueda buscar los datos del suscriptor en UDR.

OmniUDM soporta los tres esquemas de protección definidos en TS 33.501 §6.12 / Anexo C:

Esquema	Nombre	Curva / Cripto	¿Requiere clave HNET?
0	Esquema nulo	Ninguno - MSIN está en texto claro	No
1	Perfil ECIES A	Curve25519 (X25519) + AES-128-CTR + HMAC-SHA-256	Sí
2	Perfil ECIES B	secp256r1 / P-256 + AES-128-CTR + HMAC-SHA-256	Sí

Para el **esquema nulo**, el MSIN se transporta en texto claro; se **decodifica en BCD** a partir de la salida del esquema para reconstruir el IMSI (según TS 24.501 - los dígitos MSIN están codificados en BCD, no en hex). Para **Perfil A y Perfil B**, la de-ocultación realiza un ECDH efímero-estático contra la **clave privada de la Red de Hogar** del operador, deriva las claves de cifrado/MAC (ANSI-X9.63-KDF con SHA-256), verifica el MAC, descifra el MSIN oculto y lo decodifica en BCD para reconstruir el IMSI.

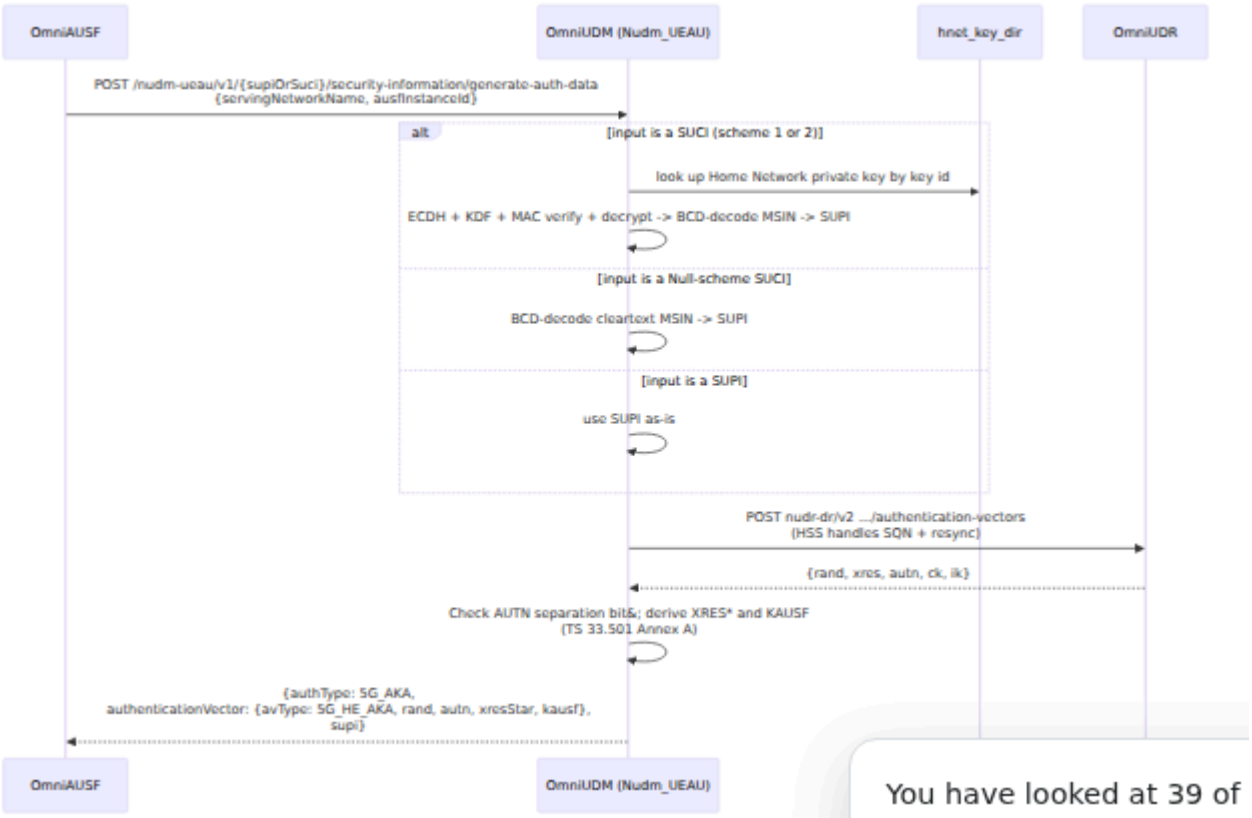
Las claves privadas de la Red de Hogar para Perfil A/B se cargan desde el directorio `hnet_key_dir`. La nomenclatura de archivos, codificaciones y los requisitos de seguridad y actualización de caché están documentados en Configuración → Claves de Red de Hogar (`hnet_key_dir`).

Procedimientos Clave

De-ocultación de SUCI y Generación de Vectores de Autenticación

El AUSF solicita un vector de autenticación; OmniUDM resuelve la identidad (de-ocultando un SUCI si es necesario), solicita un vector al HSS a través de UDR, y luego deriva las claves 5G a partir de él. **Ki/OPc, gestión de SQN y cualquier re-sincronización permanecen en el HSS detrás de UDR** - OmniUDM verifica que el AUTN del HSS lleve el bit de separación 5G (bit 0 de

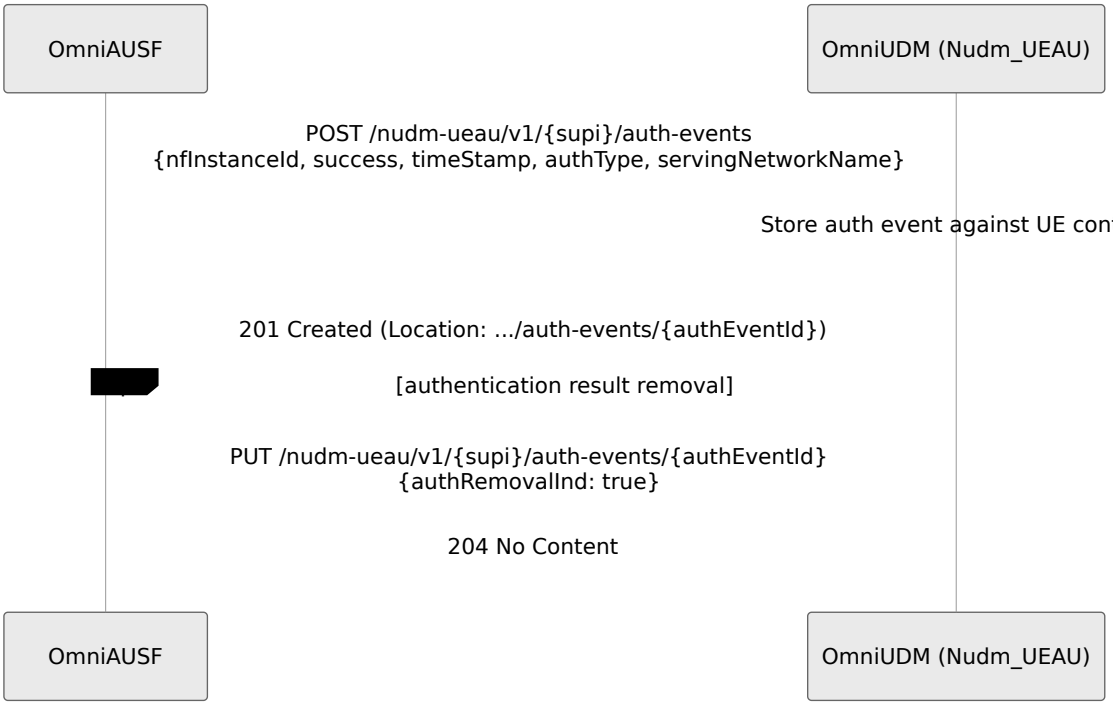
AMF, TS 33.501 §6.1.3.2, tomado de la AMF provisionada del suscriptor) y deriva `XRES*` y `KAUSF` a partir del `xres`, `ck` y `ik` devueltos. Un `resynchronizationInfo` proporcionado por el AUSF se reenvía al HSS a través de UDR.



Los fallos de de-ocultación devuelven HTTP 403 (`Fallo de De-ocultación de SUCI`), un esquema de protección no soportado devuelve HTTP 501, un suscriptor faltante o deshabilitado devuelve HTTP 404 (`USER_NOT_FOUND`), y un vector HSS inválido (incluyendo un AUTN sin el bit de separación) o una generación de vector HSS fallida devuelve HTTP 500.

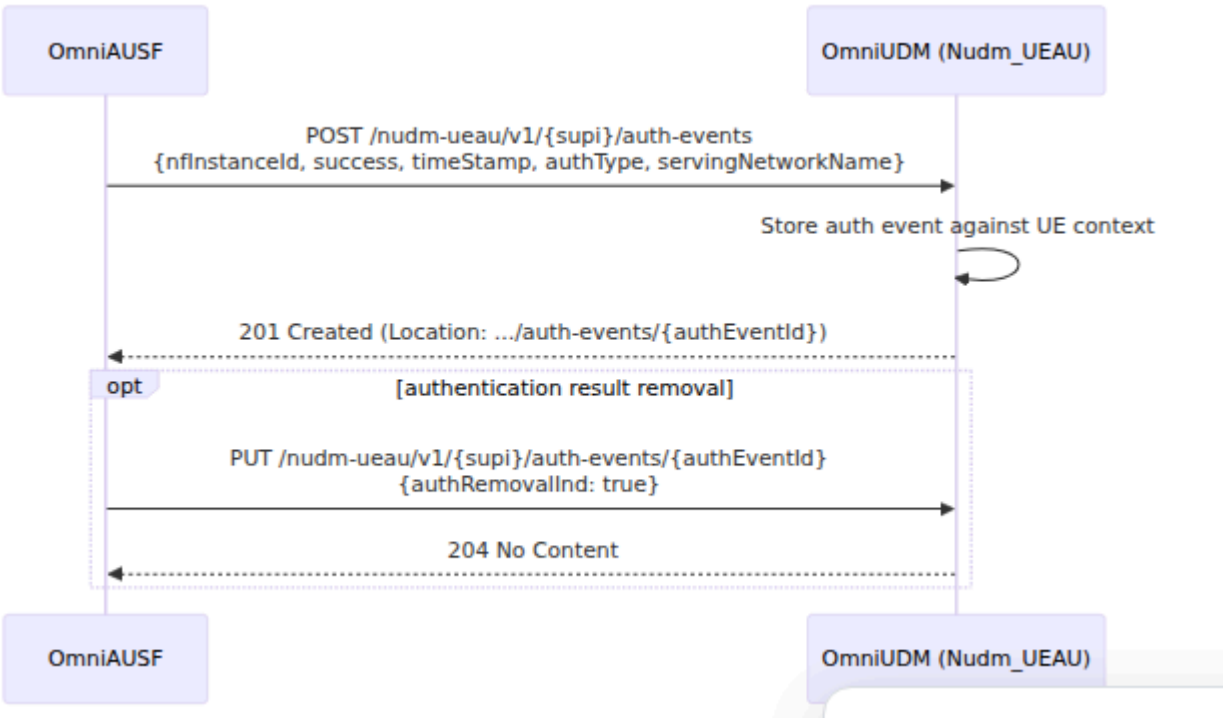
Registro de Evento de Resultado de Autenticación

Después de que el AUSF completa la autenticación, registra el resultado. OmniUDM almacena el evento contra el contexto de UE y devuelve una `Location` para el evento creado; el AUSF puede más tarde `PUT` un `AuthEvent` con `authRemovalInd=true` para eliminarlo (204 No Content).



Recuperación de Datos del Suscriptor SDM (`sm-data`)

Después del registro, el AMF/SMF recupera los datos de suscripción. OmniUDM actúa como proxy de la solicitud hacia UDR, añadiendo el PLMN de servicio, y devuelve la respuesta de UDR. Para `sm-data`, un único objeto UDR se envuelve en un array según TS 29.503 `SmSubsData`.

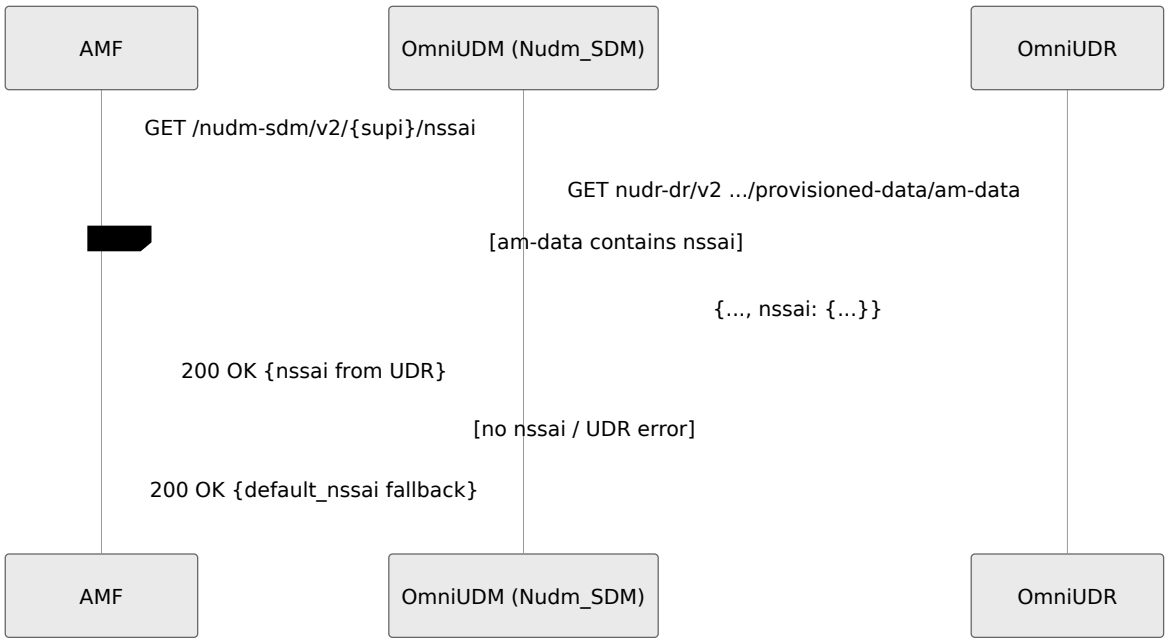


Los flujos `am-data`, `smf-select-data` y GetDataSets (`GET /{supi}`) siguen el mismo patrón de proxy contra UDR. GetDataSets ensambla solo los conjuntos de datos solicitados que puede resolver, omitiendo cualquier que falle. `nssai` se deriva de la respuesta `am-data` de UDR (ver más abajo).

> **UE-context-in-SMF devuelve contexto de sesión PDU en vivo.** `GET /{supi}/ue-context-in-smf-data` y el conjunto de datos `UEC_SMF` en GetDataSets devuelven los contextos de sesión PDU activos del UE según lo informado por el SMF a través del procedimiento de registro SMF Nudm_UECM. Cada registro SMF almacenado se proyecta en el mapa `pduSessions` (indexado por ID de sesión PDU) según TS 29.503. El mapa está vacío (`{"pduSessions": {}}`) solo cuando el UE no tiene registros SMF genuinos.

Recuperación de NSSAI con Recaída por Defecto

`GET /{supi}/nssai` recupera `am-data` de UDR y extrae el `nssai` embebido. Si UDR devuelve `am-data` sin un `nssai`, o si la búsqueda en UDR falla, OmniUDM devuelve la recaída configurable `default_nssai` para que el AMF siempre reciba una lista de cortes.



La recaída `default_nssai` debe coincidir con los cortes que la red realmente sirve - un suscriptor al que se le ofrece un corte que el AMF no está configurado

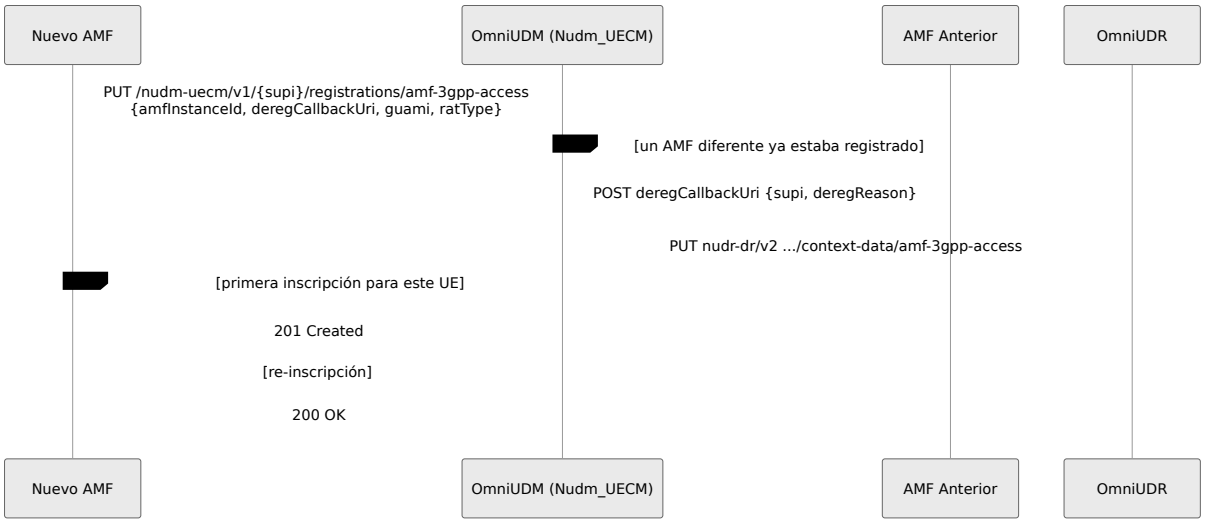
para servir es rechazado con la causa 5GMM #62. Ver Configuración → Claves de Ajuste Opcionales.

Notificaciones de Cambio SDM

Los suscriptores con una suscripción SDM activa son notificados de cambios posteriores: OmniUDM POSTea una `ModificationNotification` a la `callbackReference` de cada suscripción (asíncronamente) cuando los recursos monitoreados cambian. También se puede activar manualmente una notificación para un SUPI a través de la API de Gestión/OAM.

Registro AMF UECM y Movilidad

Cuando un UE se registra, el AMF se registra a sí mismo para ese UE en OmniUDM. Si un AMF diferente fue registrado previamente, OmniUDM notifica la `deregCallbackUri` del viejo AMF para que pueda liberar el UE, luego persiste la nueva inscripción en UDR.



Los IEs obligatorios se validan según TS 29.503: el registro 3GPP de AMF requiere `amfInstanceId`, `deregCallbackUri`, `guami`, `ratType`; el registro SMF requiere `smfInstanceId`, `pduSessionId`, `singleNssai`, `plmnId`, y el cuerpo `pduSessionId` debe coincidir con la ruta (una discrepancia devuelve `MANDATORY_IE_INCORRECT`). Los IEs faltantes devuelven HTTP 400.

← Resumen

Solución de problemas de OmniUDM

La autenticación falla con 404 Usuario no encontrado

OmniUDM resolvió la identidad, pero UDR no devolvió ninguna suscripción de autenticación. Confirme que `udr_uri` sea accesible, que OmniUDR pueda acceder a la base de datos de suscriptores y que el IMSI esté provisionado. Para una entrada de SUCI, confirme que la deconstrucción produjo el IMSI esperado (verifique la línea de registro "De-concealed SUCI to ...").

La autenticación falla con 403 Fallo en la deconstrucción de SUCI

OmniUDM no pudo deconstruir el SUCI. El campo de detalle nombra la causa específica:

- `unknown_home_network_key_id` - no se ha cargado ninguna clave privada para el identificador de clave del SUCI. Confirme que existe un archivo de clave para ese `home_network_public_key_id` en `hnet_key_dir` y que sigue una convención de nomenclatura reconocida, y que la caché de claves se ha actualizado desde que se agregó el archivo.
- `ecies_mac_verification_failed` - la clave privada cargada no coincide con la clave pública en la SIM (clave incorrecta o intercambiada), o el SUCI está dañado. Verifique el par de claves provisionadas en las SIM contra la clave privada desplegada para ese identificador.
- `ecies_profile_a_scheme_output_too_short` / `ecies_profile_b_scheme_output_too_short` - la salida del esquema SUCI está truncada / mal formada.

- `invalid_suci_format` - la cadena SUCI no está bien formada.

La autenticación falla con 501 Esquema de protección no soportado

El SUCI utilizó un esquema de protección diferente de 0 (Nulo), 1 (Perfil A) o 2 (Perfil B). Solo se admiten estos tres.

La autenticación falla con 500 Error interno

Los campos del vector HSS (`rand`/`xres`/`ck`/`ik`/`autn`) estaban ausentes, no eran hexadecimales válidos o tenían la longitud incorrecta; el AUTN carecía del bit de separación 5G; o falló la generación del vector HSS. La línea de registro `Invalid auth key material ... separation_bit_not_set` significa que el AMF provisionado del suscriptor en el conjunto de claves HSS no tiene su bit superior establecido (use `8000`). De lo contrario, verifique el conjunto de claves del suscriptor en el HSS y que OmniUDR pueda acceder al HSS.

`am-data` / `sm-data` / `smf-select-data` devuelve 404 No encontrado

La búsqueda de UDR falló para ese conjunto de datos. Confirme que los datos provisionados del suscriptor existen en UDR para el PLMN que sirve, que `mcc`/`mnc` (o el `plmn-id` de la solicitud) coincidan con la forma en que se provisionaron los datos, y que `udr_uri` sea accesible.

UE rechazado por AMF con causa 5GMM #62 (sin slice soportado)

El NSSAI servido al AMF no incluye un slice que el AMF esté configurado para servir. Si el `am-data` de UDR del suscriptor no lleva `nssai`, OmniUDM devuelve el fallback `default_nssai` - establezca `default_nssai` (o provisione `nssai` en UDR) para que coincida con los slices reales de la red, incluidos los S-NSSAIs calificados por SD.

Contexto de UE o registro no presente después del reinicio

El estado de ejecución por UE (contexto de autenticación, registros AMF/SMF, suscripciones SDM) se mantiene en un almacén de contexto en memoria y se reconstruye mediante re-registro; los datos del suscriptor autoritativos persisten en OmniUDR. Después de un reinicio, AMF/SMF se re-registran en la siguiente actualización de registro periódica, restablecimiento de sesión PDU o ciclo de encendido de UE. Si falta un registro específico antes de lo esperado, active la actualización de registro del NF consumidor en lugar de esperar el temporizador periódico.

Notificación de cambio de datos SDM no recibida

Confirme que la URI `callbackReference` de la suscripción sea accesible desde el host de OmniUDM. Las notificaciones se envían de forma asíncrona; busque advertencias "SDM notification to ... failed". Se puede activar manualmente una notificación para un SUPI a través de la API de Gestión/OAM (`POST /api/oam/ue/sdm-notify`).

Después de cambiar las claves de la red de hogar, la deconstrucción

aún utiliza la clave antigua

Las claves de la red de hogar se almacenan en caché en memoria después de la primera carga. Cárguelas de nuevo a través de la acción de gestión OAM (`POST /api/oam/hnet/reload`) después de agregar o reemplazar archivos de clave en `hnet_key_dir`; la respuesta informa la cantidad de claves cargadas y sus identificadores de clave. No se requiere reinicio del proceso.

UDM no es descubrible por otros NFs

Verifique `omni_udm_nrf_registration_status`. Si es `0`, confirme que `nrf_uri` sea accesible y que el latido sea exitoso; la API de gestión OAM ofrece una acción de re-registro NRF (`POST /api/oam/nrf/reregister`).