

EIR (Registro de Identidad de Equipos)

Descripción general

El HSS incluye un EIR (Registro de Identidad de Equipos) incorporado que proporciona verificación de identidad de equipos para dispositivos móviles. El EIR valida los números IMEI (Identidad Internacional de Equipos Móviles) para determinar si el equipo móvil está autorizado, robado o bajo observación antes de permitir el acceso a la red.

Capacidades clave

- **Interfaz S13:** Verificación de identidad de equipos a través del protocolo Diameter
- **Validación de IMEI:** Verificar la identidad del equipo utilizando IMEI/IMEISV
- **Coincidencia flexible:** Coincidencia de patrones basada en regex para IMEI, IMEISV e IMSI
- **Clasificación de tres niveles:** Soporte para listas blancas, listas negras y listas grises
- **Políticas configurables:** Comportamiento personalizable para equipos desconocidos
- **API REST:** Operaciones CRUD completas para la gestión de reglas EIR

Arquitectura

Interfaz Diameter

Interfaz	ID de aplicación	Par	Propósito
S13	16,777,252	MME/SGSN	Verificación de identidad de equipos

Base de datos de reglas de equipos

El EIR utiliza un sistema de coincidencia basado en reglas flexible:

EIR_RULE		
int	id	PK
string	action	
string	regex	
timestamp	inserted_at	
timestamp	updated_at	

Acciones de regla:

- whitelist - Permitir equipo
- blacklist - Bloquear equipo
- greylist - Monitorear equipo

Patrones Regex: Coincidir con IMEI, IMEISV o IMSI

Valores de estado del equipo

Estado	Código	Significado	Acción en la red
Whitelist	0	Equipo aprobado	Permitir acceso a la red
Blacklist	1	Equipo robado/bloqueado	Denegar acceso a la red
Greylist	2	Equipo bajo observación	Permitir con monitoreo

Interfaz S13

Operaciones soportadas

Solicitud de verificación de identidad de equipo (ECR) / Respuesta de verificación de identidad de equipo (ECA)

Dirección: MME/SGSN → HSS (EIR)

Disparador: MME verifica la identidad del equipo durante el adjunto o la actualización del área de seguimiento

AVPs de solicitud:

- Session-Id
- Origin-Host, Origin-Realm
- Destination-Realm
- Auth-Session-State
- Terminal-Information
 - IMEI (15 dígitos)
 - Software-Version (2 dígitos, opcional)
- User-Name (IMSI, opcional)
- Vendor-Specific-Application-Id

Acciones del EIR:

1. Extraer IMEI, Software-Version (si está presente) e IMSI (si está presente)
2. Si se proporciona IMSI:
 - Validar que el suscriptor existe y está habilitado
 - Actualizar el estado del suscriptor con la información de última vista
3. Intentar la búsqueda del equipo en orden de prioridad:
 - **Coincidencia de IMEISV** (IMEI + Software-Version concatenados)
 - **Coincidencia de IMEI** (solo IMEI)
 - **Coincidencia de IMSI** (si se proporciona en la solicitud)
 - **Política de equipo desconocido** (comportamiento predeterminado configurado)
4. Devolver el estado del equipo

AVPs de respuesta:

- Session-Id (repetido de la solicitud)
- Result-Code: 2001 (éxito)
- Equipment-Status: 0 (whitelist) / 1 (blacklist) / 2 (greylist)

Respuestas de error:

- Experimental-Result: 5422 (equipo/suscriptor no encontrado)
- Experimental-Result: 5012 (error general)

Lógica de coincidencia de equipos

Orden de prioridad

El EIR utiliza una estrategia de búsqueda en cascada para maximizar la flexibilidad de coincidencia:

1. IMEISV (IMEI + Software-Version)
↓ (si no hay coincidencia)
2. IMEI solo
↓ (si no hay coincidencia)
3. IMSI (si se proporciona en la solicitud)
↓ (si no hay coincidencia)
4. Política de equipo desconocido

Algoritmo de coincidencia

Paso 1: Coincidencia de IMEISV

- Concatenar IMEI + Software-Version: "35979139461611" + "08" = "3597913946161108"
- Probar contra todos los patrones regex de reglas EIR
- Devolver acción ("whitelist", "blacklist", "greylist") de la primera regla coincidente

Paso 2: Coincidencia de IMEI (respaldo)

- Usar solo IMEI: "35979139461611"
- Probar contra todos los patrones regex de reglas EIR
- Devolver acción de la primera regla coincidente

Paso 3: Coincidencia de IMSI (respaldo si se proporciona IMSI)

- Usar IMSI de la solicitud: "999999876543210"
- Probar contra todos los patrones regex de reglas EIR
- Devolver acción de la primera regla coincidente
- **Caso de uso:** Bloquear todo el equipo para un suscriptor específico

Paso 4: Política de equipo desconocido (último respaldo)

- Configuración: eir_unknown_equipment_behaviour
- Opciones:
 - :whitelist - Permitir equipo desconocido (permisivo)
 - :blacklist - Bloquear equipo desconocido (restrictivo)

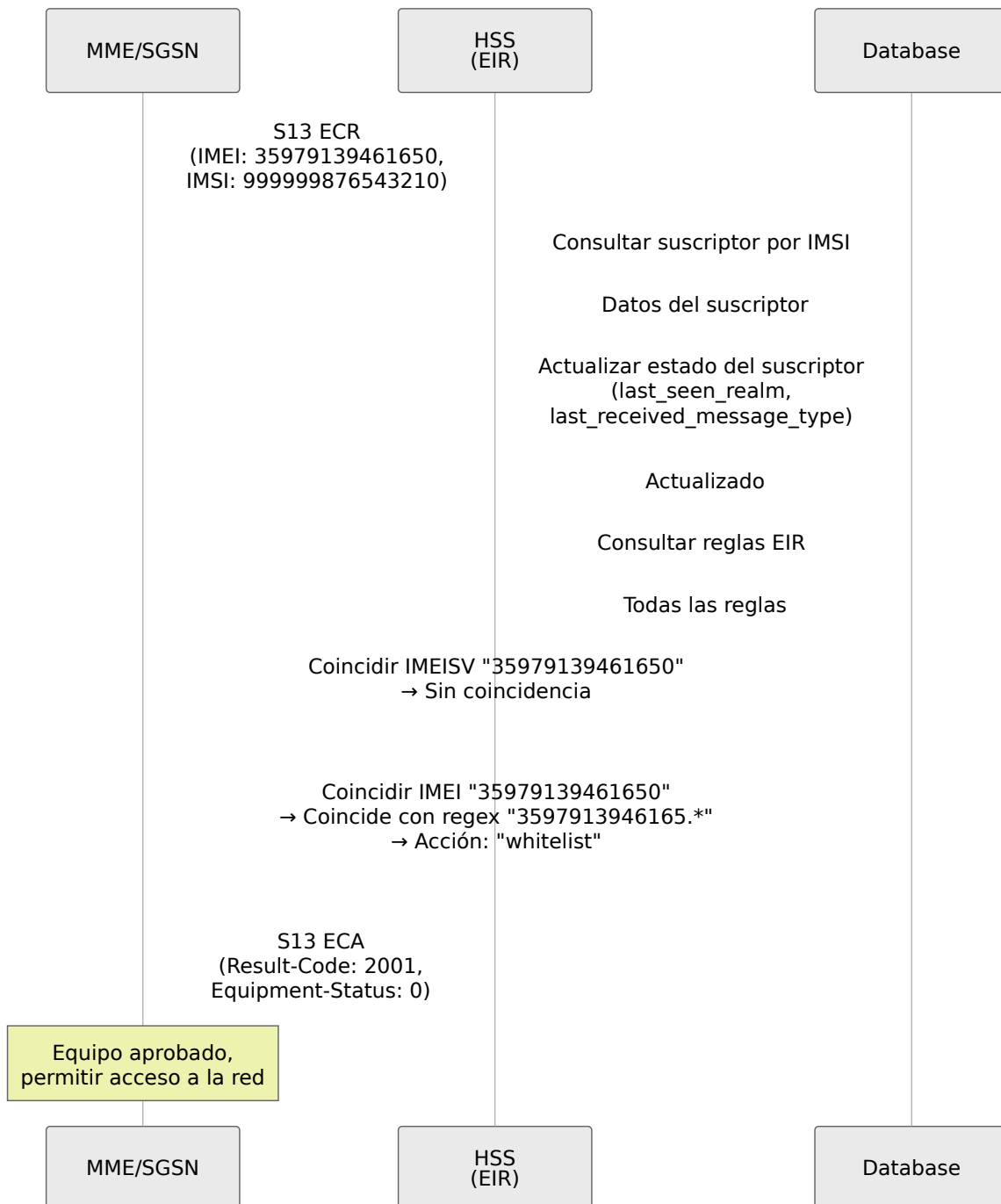
- `:greylist` - Observar equipo desconocido (moderado)
- `:reject_unknown_equipment` - Devolver error 5422 (estricto)

Ejemplos de patrones Regex

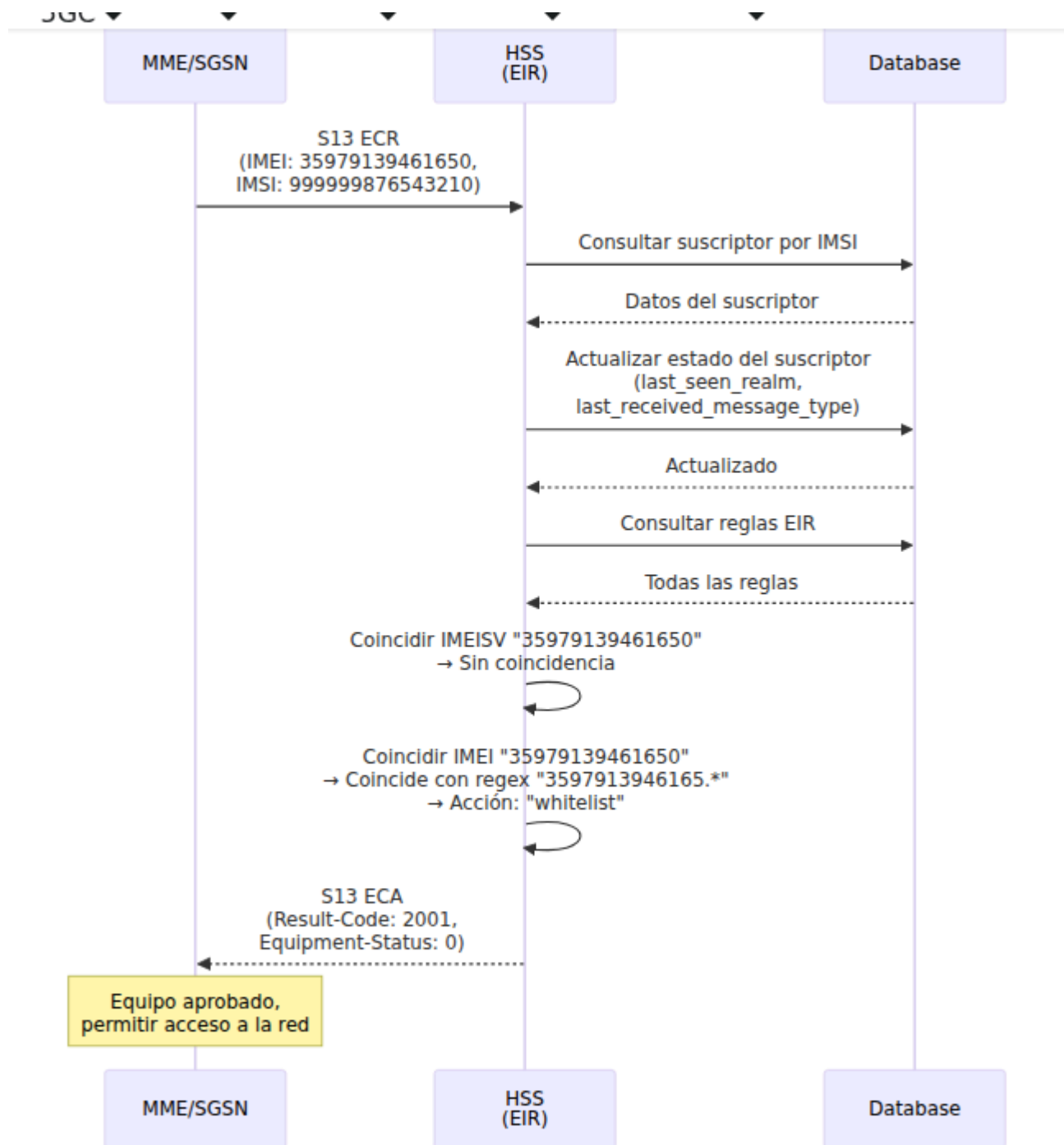
Patrón	Coincide	Caso de uso
<code>"35979139461650"</code>	IMEI exacto	Lista blanca/lista negra de un solo dispositivo
<code>"3597913946165.*"</code>	comodín de prefijo IMEI	Rango de fabricante/modelo
<code>"3597913946161108"</code>	IMEISV exacto	Dispositivo específico con versión de software
<code>"999999876543210"</code>	IMSI	Bloquear todo el equipo para el suscriptor
<code>"359791.*"</code>	comodín TAC	Asignación de todo el tipo de dispositivo

Flujos de mensajes comunes

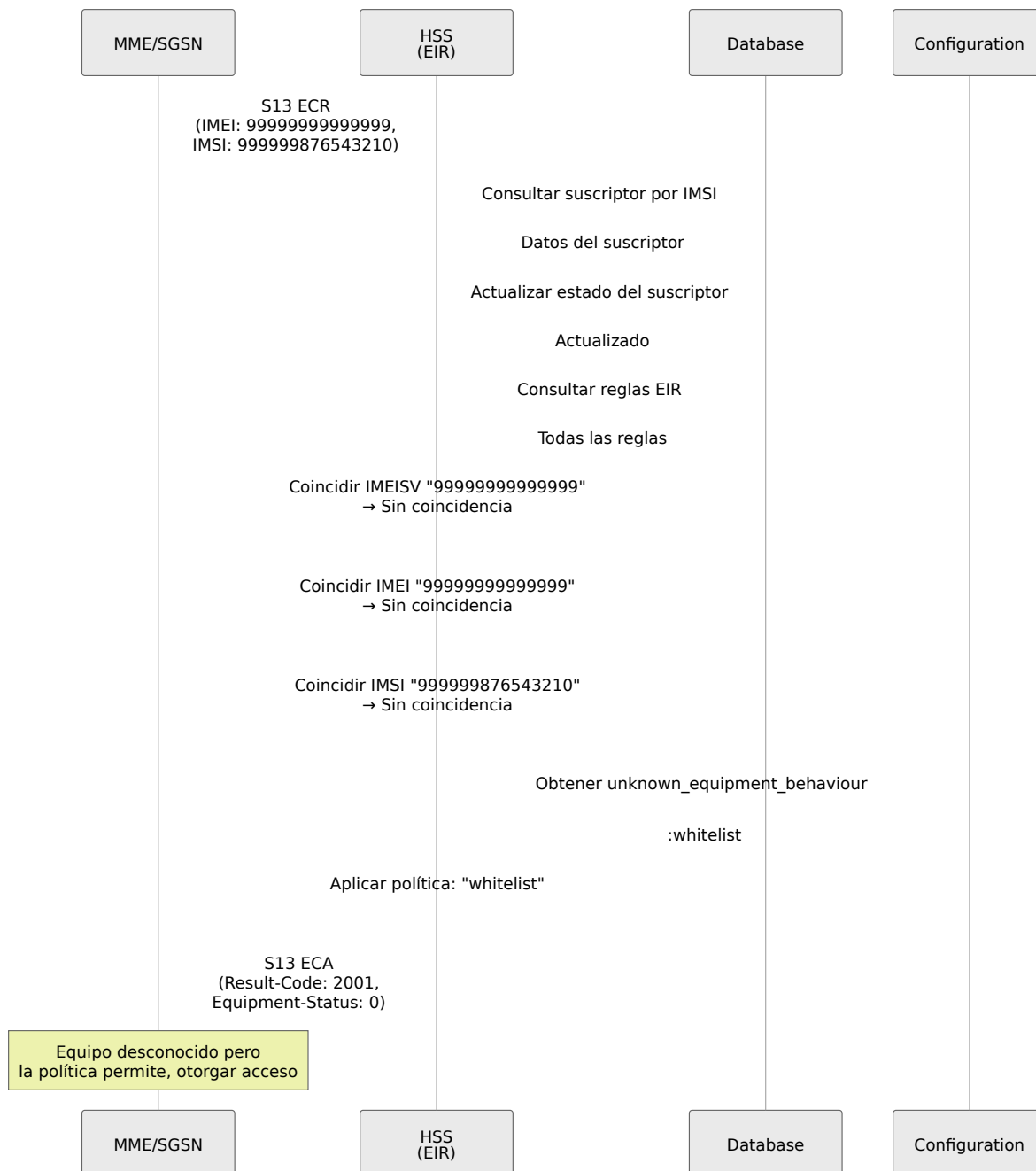
Flujo 1: Verificación de equipo - IMEI conocido en la lista blanca



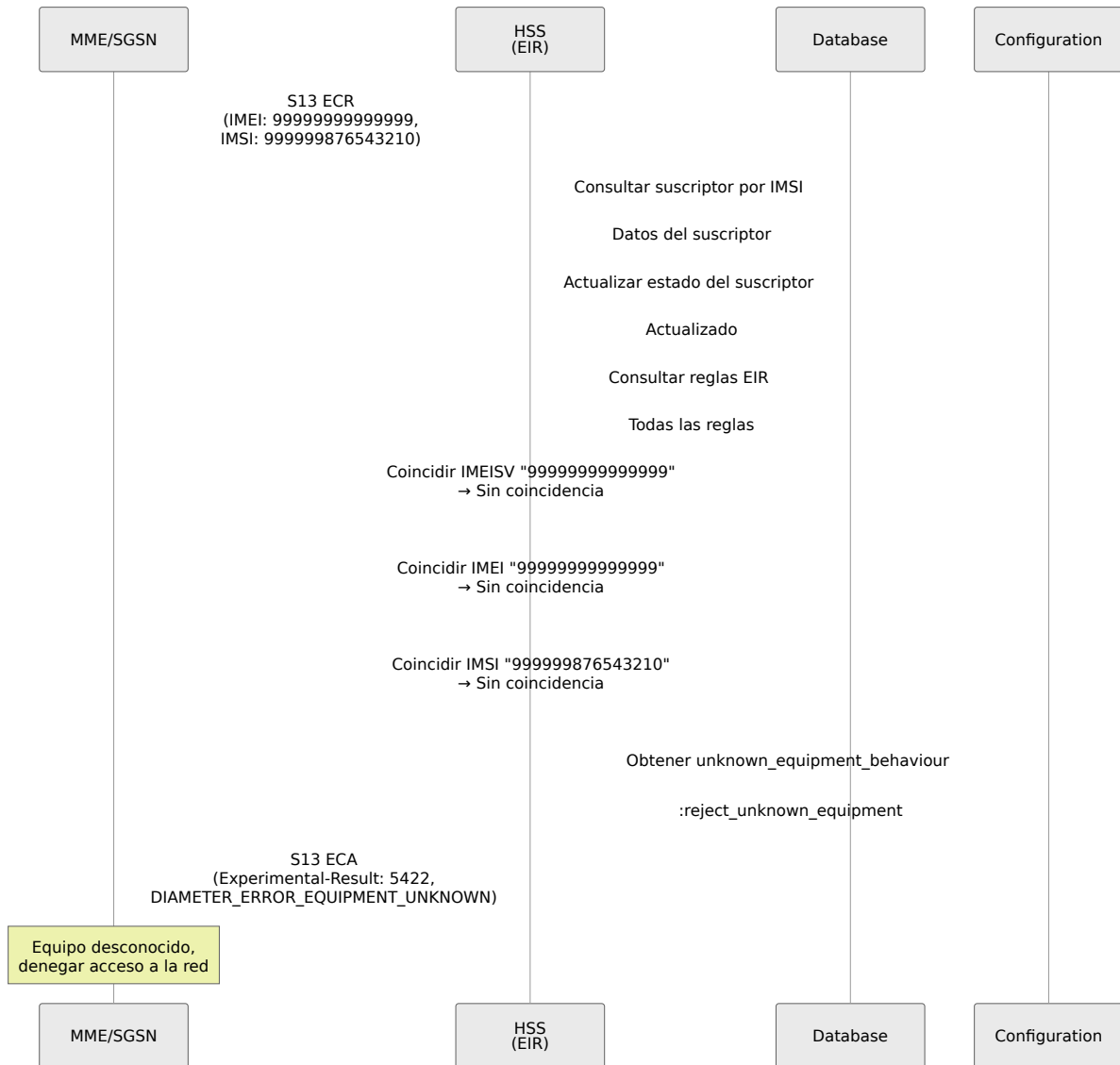
Flujo 2: Verificación de equipo - IMEI en la lista negra (dispositivo robado)



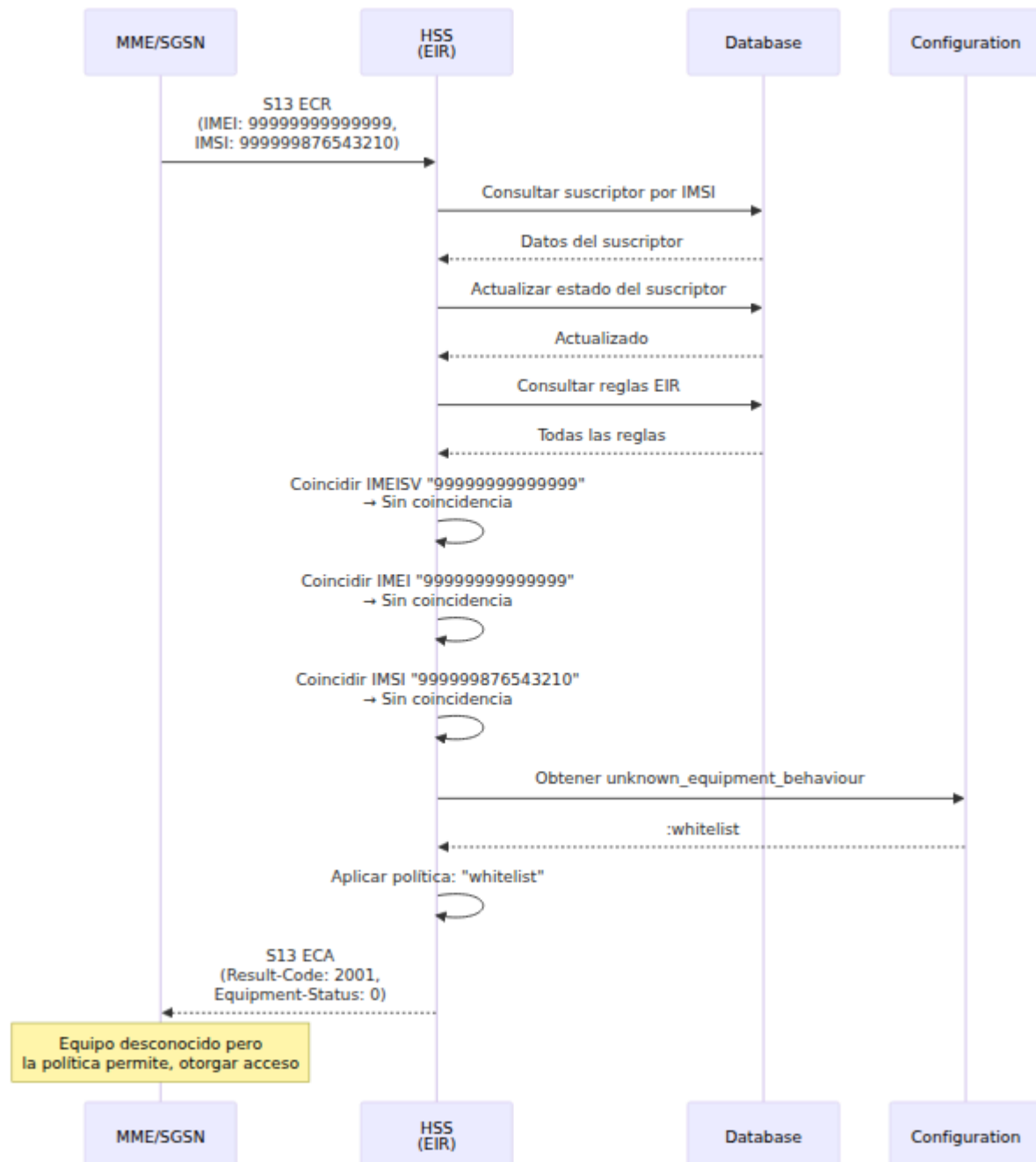
Flujo 3: Verificación de equipo - Equipo desconocido (política de lista blanca)



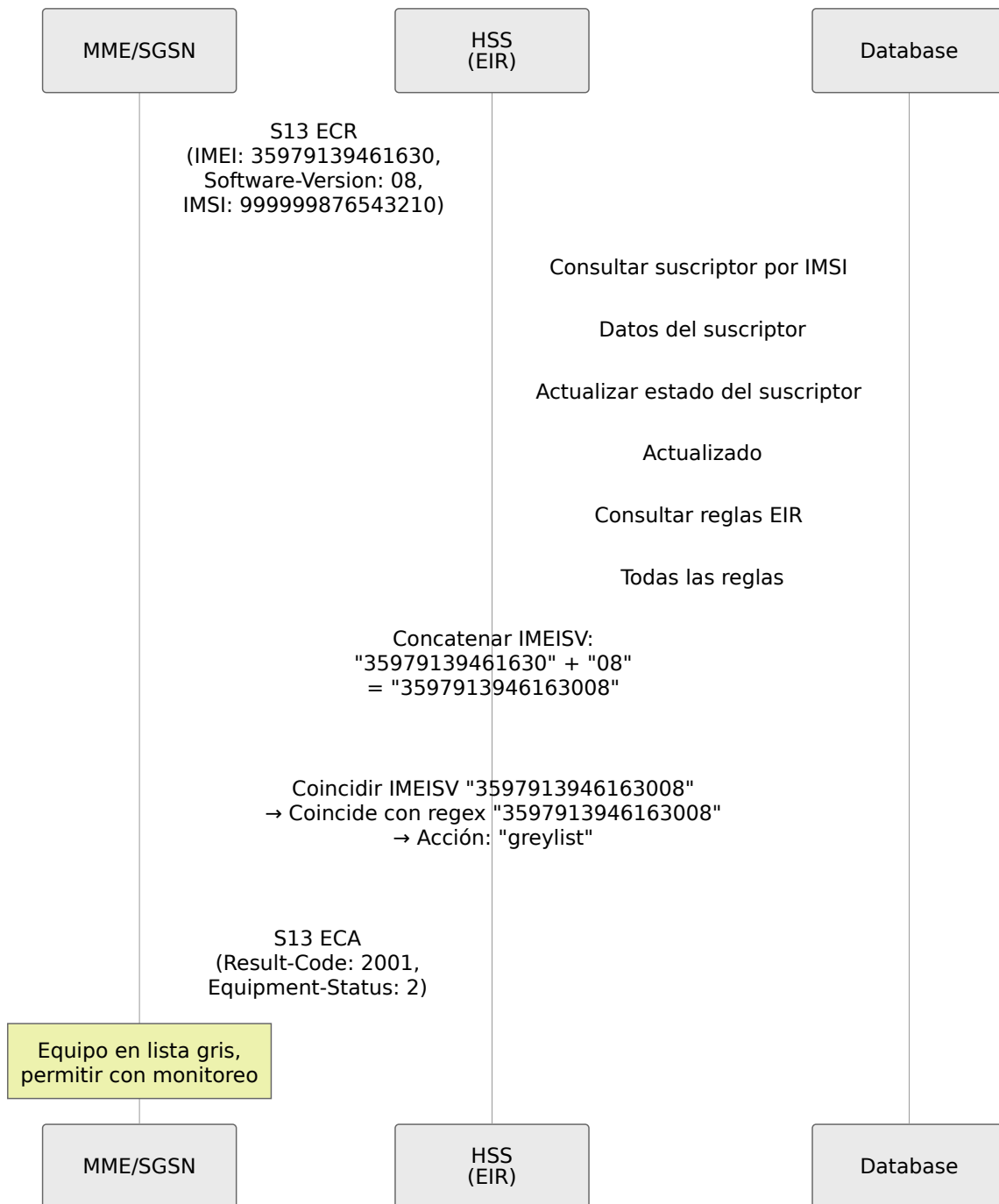
Flujo 4: Verificación de equipo - Equipo desconocido (política de rechazo)



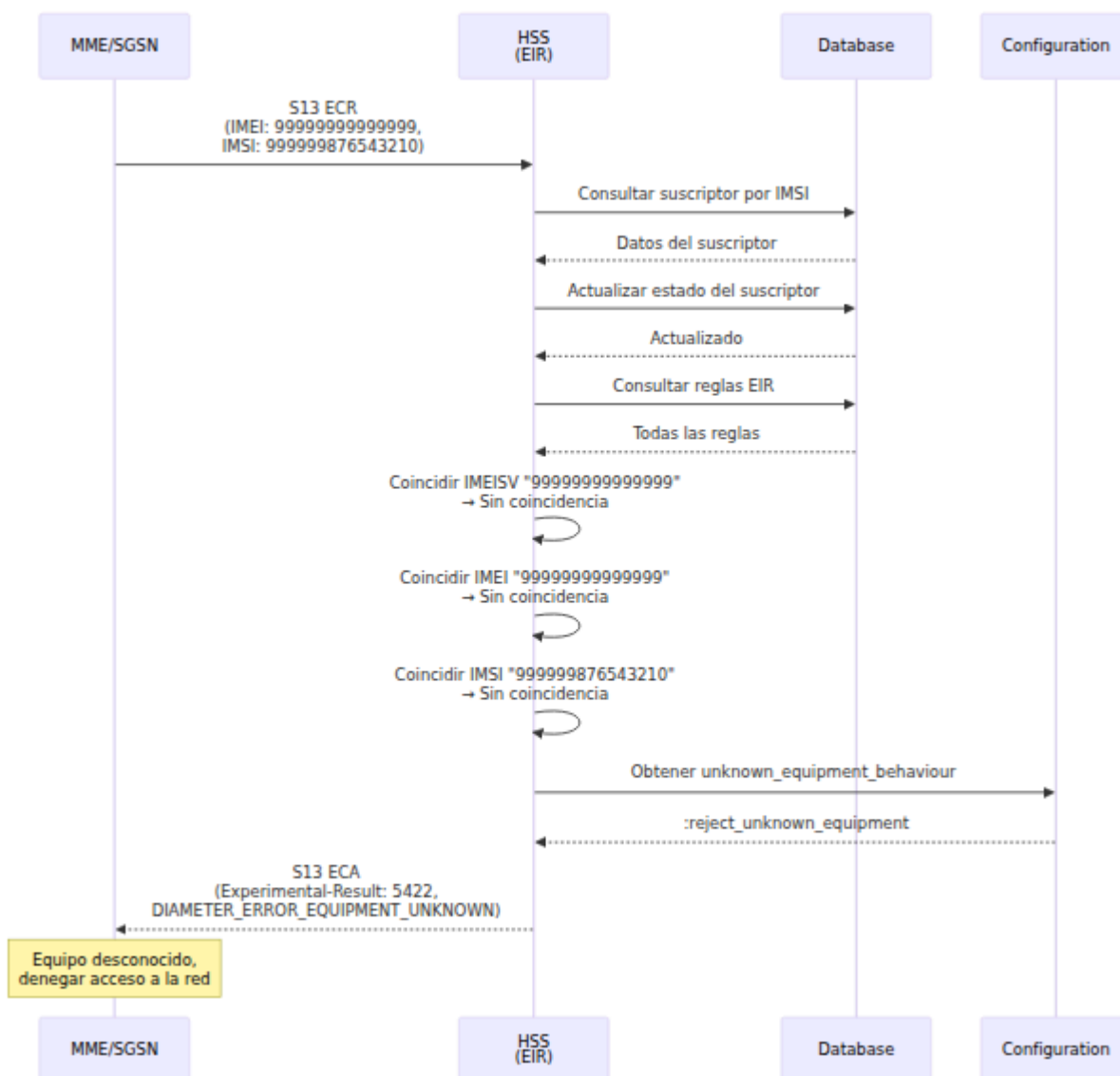
Flujo 5: Verificación de equipo - Suscriptor desconocido



Flujo 6: Verificación de equipo - Coincidencia de IMEISV



Flujo 7: Verificación de equipo - Bloqueo de IMSI



API REST

Gestión de reglas EIR

Ruta base: `/api/eir/rule`

Listar todas las reglas EIR

Solicitud:

```
GET /api/eir/rule
```

Respuesta (HTTP 200):

```
{
  "data": [
    {
      "id": "e7f6a5b4-c3d2-4e1f-8a9b-0c1d2e3f4a5b",
      "action": "whitelist",
      "regex": "3597913946165.*",
      "inserted_at": "2025-01-15T10:30:00Z",
      "updated_at": "2025-01-15T10:30:00Z"
    },
    {
      "id": "f8a7b6c5-d4e3-4f2a-9b0c-1d2e3f4a5b6c",
      "action": "blacklist",
      "regex": "35979139461640",
      "inserted_at": "2025-01-16T14:20:00Z",
      "updated_at": "2025-01-16T14:20:00Z"
    }
  ]
}
```

Obtener regla EIR específica

Solicitud:

```
GET /api/eir/rule/{id}
```

Respuesta (HTTP 200):

```
{
  "data": {
    "id": "e7f6a5b4-c3d2-4e1f-8a9b-0c1d2e3f4a5b",
    "action": "whitelist",
    "regex": "3597913946165.*"
  }
}
```

Crear regla EIR

Solicitud:

```
POST /api/eir/rule
Content-Type: application/json

{
  "action": "blacklist",
  "regex": "35979139461640"
}
```

Validación:

- `action`: Requerido, debe ser "whitelist", "blacklist" o "greylist"
- `regex`: Requerido, debe ser un patrón regex válido, único entre todas las reglas

Respuesta (HTTP 201):

```
{
  "data": {
    "id": "0362b7ab-9bd6-4d8a-8b1a-2f4c6e8d0a1c",
    "action": "blacklist",
    "regex": "35979139461640"
  }
}
```

Respuesta de error (HTTP 400):

```
{
  "errors": {
    "regex": ["ya ha sido tomado"]
  }
}
```

Actualizar regla EIR (parcial)

Solicitud:

```
PATCH /api/eir/rule/{id}
Content-Type: application/json
```

```
{
  "action": "greylist"
}
```

Respuesta (HTTP 200):

```
{
  "data": {
    "id": "0362b7ab-9bd6-4d8a-8b1a-2f4c6e8d0a1c",
    "action": "greylist",
    "regex": "35979139461640"
  }
}
```

Reemplazar regla EIR

Solicitud:

```
PUT /api/eir/rule/{id}
Content-Type: application/json
```

```
{
  "action": "whitelist",
  "regex": "359791394616.*"
}
```

Respuesta (HTTP 200):

```
{
  "data": {
    "id": "0362b7ab-9bd6-4d8a-8b1a-2f4c6e8d0a1c",
    "action": "whitelist",
    "regex": "359791394616.*"
  }
}
```

Eliminar regla EIR

Solicitud:

```
DELETE /api/eir/rule/{id}
```

Respuesta (HTTP 204 No Content)

Configuración

Configuración del servicio Diameter

Aplicación S13 (`config/runtime.exs`):

```
%{  
  application_name: :s13,  
  application_dictionary: :diameter_gen_3gpp_s13,  
  vendor_specific_application_ids: [  
    %{vendor_id: 10415, auth_application_id: 16_777_252}  
  ]  
}
```

Comportamiento de equipo desconocido

Configurar el comportamiento predeterminado para equipos que no coinciden con ninguna regla en `config/runtime.exs`:

Ejemplo:

```
config :hss, :eir,  
  unknown_equipment_behaviour: :whitelist
```

Valores válidos:

- `:whitelist` - Permitir equipo desconocido (predeterminado, permisivo)
- `:blacklist` - Bloquear equipo desconocido (restrictivo)

- `:greylist` - Monitorear equipo desconocido (moderado)
- `:reject_unknown_equipment` - Devolver error Diameter 5422 (estricto)

Casos de uso:

- **Desarrollo/pruebas:** `:whitelist` - Permitir todos los dispositivos
- **Producción (permisivo):** `:whitelist` - Solo bloquear dispositivos conocidos como malos
- **Producción (moderado):** `:greylist` - Registrar dispositivos desconocidos para revisión
- **Producción (estricto):** `:reject_unknown_equipment` - Solo permitir dispositivos registrados

Manejo de errores

Código de resultado	Tipo	Significado	
2001	Éxito	DIAMETER_SUCCESS	Ve eq co
5422	Experimental	DIAMETER_ERROR_EQUIPMENT_UNKNOWN	Su en eq de re
5012	Experimental	DIAMETER_ERROR_UNKNOWN	En pr

Casos de uso

1. Gestión de dispositivos robados

Escenario: Dispositivo reportado como robado

Acción:

```
POST /api/eir/rule
{
  "action": "blacklist",
  "regex": "35979139461640" # IMEI exacto
}
```

Resultado: Dispositivo denegado acceso a la red en el próximo adjunto

2. Lista blanca de fabricantes

Escenario: Pre-aprobar todo el rango de modelos de dispositivos

Acción:

```
POST /api/eir/rule
{
  "action": "whitelist",
  "regex": "359791394.*" # TAC para fabricante/modelo
}
```

Resultado: Todos los dispositivos en el rango TAC aprobados

3. Bloqueo de equipo de suscriptor

Escenario: Bloquear todo el equipo para un suscriptor específico (bloqueo de SIM)

Acción:

```
POST /api/eir/rule
{
  "action": "blacklist",
  "regex": "999999876543210" # IMSI
}
```

Resultado: Cualquier equipo utilizado con esta SIM está bloqueado

4. Lista gris de equipos de prueba

Escenario: Monitorear equipos de prueba en producción

Acción:

```
POST /api/eir/rule
{
  "action": "greylist",
  "regex": "35979139.*" # Rango TAC de equipos de prueba
}
```

Resultado: Equipo permitido pero marcado para monitoreo

5. Control de versión de software

Escenario: Bloquear versión de firmware vulnerable específica

Acción:

```
POST /api/eir/rule
{
  "action": "blacklist",
  "regex": "359791394616.*05" # Rango IMEI + versión de software
  05
}
```

Resultado: Solo se bloquean dispositivos con versión de software "05" en el rango IMEI

Detalles de implementación

Componentes internos

La funcionalidad del EIR se implementa utilizando varios módulos internos:

- **Controlador de protocolo S13** - Procesamiento de mensajes ECR/ECA
- **Motor de coincidencia de equipos** - Coincidencia de IMEI/IMEISV/IMSI basada en regex
- **Base de datos de reglas EIR** - Almacenamiento y búsqueda de patrones
- **Controlador de API REST** - Puntos finales de gestión de reglas

Función de búsqueda de estado del equipo

La búsqueda de estado del equipo sigue esta lógica en cascada:

1. **Coincidencia de IMEISV**: Verificar IMEI + Software-Version concatenados
2. **Coincidencia de IMEI**: Verificar solo IMEI
3. **Coincidencia de IMSI**: Verificar IMSI (si se proporciona)
4. **Equipo desconocido**: Aplicar política predeterminada configurada

Resultados posibles:

- `whitelist` - Equipo permitido
- `blacklist` - Equipo bloqueado
- `greylist` - Equipo bajo observación
- `reject_unknown_equipment` - Rechazo estricto

Consideraciones de seguridad

Privacidad del IMEI

Los números IMEI son identificadores sensibles. El EIR:

- No registra valores IMEI en texto plano por defecto

- Utiliza búsquedas en bases de datos hasheadas (si está configurado)
- Restringe el acceso a la API a administradores autenticados

Orden de reglas

Las reglas EIR se evalúan en orden de base de datos (por ID). Para patrones en conflicto:

```
Regla 1: regex "359791.*" acción "whitelist" (amplio)
Regla 2: regex "35979139461640" acción "blacklist" (específico)
```

Recomendación: Crear reglas específicas antes de comodines amplios para asegurar que la lista negra tenga prioridad.

Limitación de tasa

Considere implementar limitación de tasa en:

- Solicitudes ECR S13 de pares no confiables
- Modificaciones de reglas EIR de la API REST
- Consultas de búsqueda de IMEI para prevenir ataques de enumeración

Documentación relacionada

- [Protocolos Diameter](#) - Especificación del protocolo S13
- [Referencia de API](#) - Documentación completa de la API
- [Arquitectura](#) - Arquitectura general del HSS
- [Guía de operaciones](#) - Procedimientos operativos

Apéndice: Estructura del IMEI

Formato de IMEI (15 dígitos)

35 9791 394616 1

- | | | └ Dígito de verificación (algoritmo de Luhn)
- | | └ Número de serie (6 dígitos)
- | └ FAC (Código de ensamblaje final, 4 dígitos)
- └ TAC (Código de asignación de tipo, 8 dígitos en total incluyendo RBI)
 - | └ RBI (Identificador del organismo de informes, 2 dígitos)
 - └ Fabricante/modelo (6 dígitos)

Formato de IMEISV (16 dígitos)

35 9791 394616 1 08

- | | | | └ Versión de software (2 dígitos)
- └ IMEI (15 dígitos)

Ejemplos de patrones

IMEI/IMEISV	Patrón	Coincide
359791394616108	3597913946161.*	Todos los dispositivos con TAC+FAC+Serial 359791394616*
359791394616140	35979139461614.	Todos los dígitos de verificación para Serial 359791394616141-9
35979139461640	35979139461640	Coincidencia exacta de IMEI
3597913946163008	3597913946163008	Coincidencia exacta de IMEISV (IMEI + SV)

PCRF (Función de Reglas de Políticas y Cargos)

Descripción general

El HSS incluye un PCRF (Función de Reglas de Políticas y Cargos) integrado que proporciona control de políticas y reglas de cargos para sesiones de datos móviles. El PCRF controla las políticas de Calidad de Servicio (QoS), la asignación de ancho de banda y las reglas de cargos para portadoras predeterminadas y dedicadas en redes LTE.

Capacidades clave

- **Interfaz Gx:** Control de políticas para PGW/PCEF (Gateway de Red de Datos por Paquetes / Función de Ejecución de Políticas y Cargos)
- **Interfaz Rx:** Autorización y QoS para flujos de medios IMS (Subsistema Multimedia IP)
- **Interfaz Sy:** Control del límite de gasto del suscriptor contra un OCS externo - ver [Interfaz Sy](#)
- **Gestión dinámica de políticas:** Actualizaciones de políticas en tiempo real a través de Solicitudes de Reautenticación (RAR)
- **Soporte para VoLTE:** Creación de portadoras dedicadas para llamadas de voz con QoS garantizada
- **Reglas de cargos:** Definir el comportamiento de cargos y perfiles de velocidad utilizando Plantillas de Flujo de Tráfico (TFT)
- **REST API:** Control programático de la ejecución de políticas y gestión de reglas

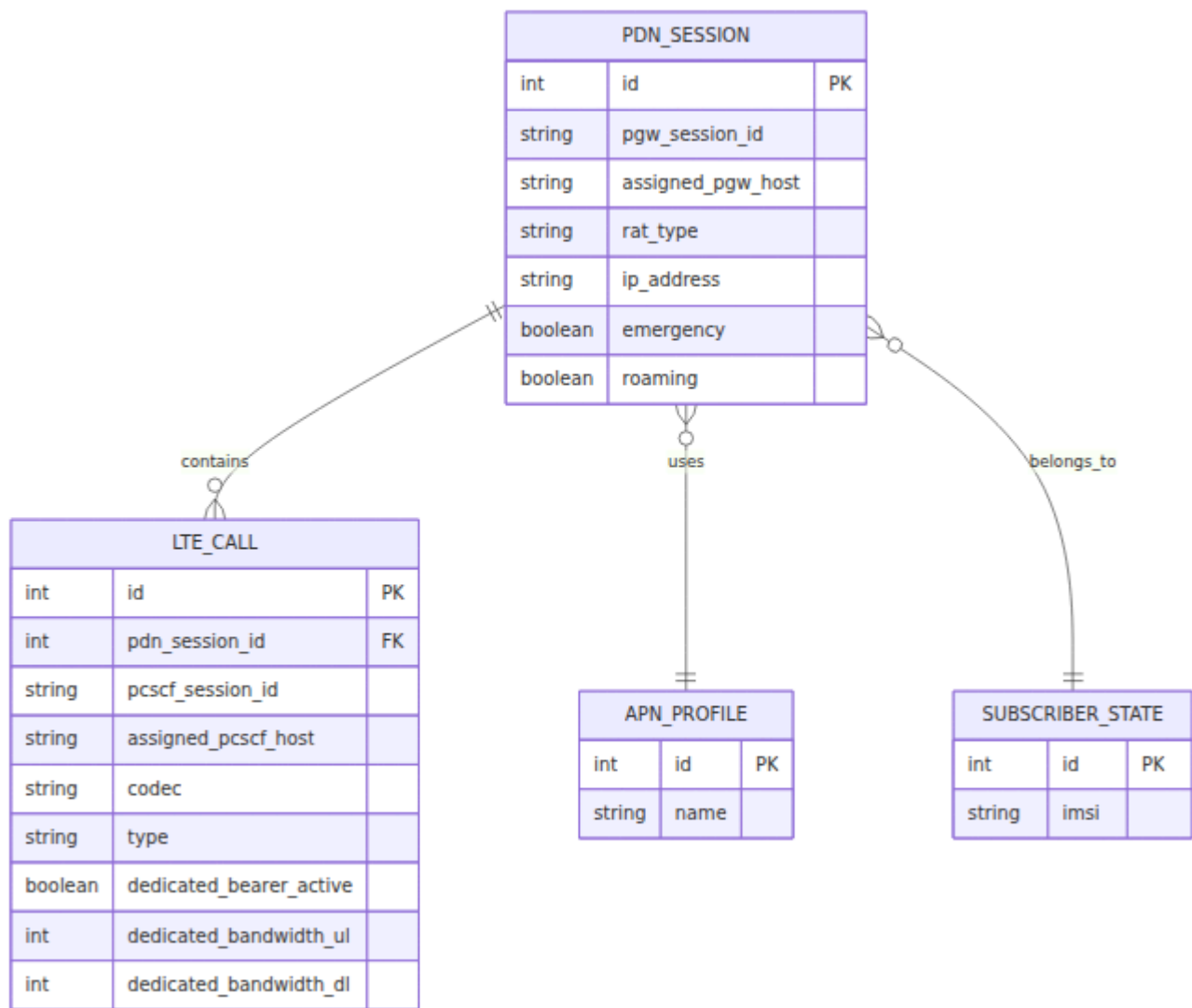
Arquitectura

Interfaces Diameter

Interfaz	ID de Aplicación	Par	Propósito
Gx	16,777,238	PGW (PCEF)	Gestión de sesiones PDN, ejecución de QoS, reglas de cargos
Rx	16,777,236	P-CSCF (AF)	Autorización de medios IMS, reserva de ancho de banda
Sy	16,777,302	OCS	Estado del límite de gasto del suscriptor, política impulsada por el gasto - ver Interfaz Sy

Gestión del estado de sesión

El PCRF mantiene el estado de sesión para conexiones PDN activas y llamadas VoLTE:



Interfaz Gx

Operaciones soportadas

1. Solicitud de Control de Crédito - Inicial (CCR-I)

Disparador: PGW crea una nueva conexión PDN para el suscriptor

AVPs de Solicitud:

- Session-Id
- Origin-Host, Origin-Realm
- Subscription-Id (contiene IMSI)
- Called-Station-Id (nombre de APN)

- IP-CAN-Type (tipo de Red de Acceso a Conectividad IP)
- RAT-Type (Tecnología de Acceso Radio)
- Framed-IP-Address (dirección IP del UE)

Acciones del PCRF:

1. Buscar suscriptor por IMSI
2. Recuperar perfil de APN y configuración de QoS
3. Crear entrada de seguimiento de sesión
4. Construir políticas de QoS a partir del perfil de APN

AVPs de Respuesta:

- Result-Code: 2001 (DIAMETER_SUCCESS)
- QoS-Information (límites de ancho de banda agregados de APN)
- Default-EPS-Bearer-QoS (QCI, ARP, prioridad)
- Bearer-Control-Mode
- Online / Offline (método de carga predeterminado a nivel de sesión - ver [Carga en Línea/ Fuera de Línea a Nivel de Sesión](#))

2. Solicitud de Control de Crédito - Actualización (CCR-U)

Disparador: PGW informa cambios en la sesión (actualización de ubicación, cambio de RAT, etc.)

Acciones del PCRF:

1. Localizar sesión existente por ID de sesión
2. Actualizar parámetros de sesión (tipo de RAT, ubicación, etc.)
3. Devolver políticas actualizadas si es necesario

Respuesta: Result-Code 2001 con actualizaciones de políticas opcionales

3. Solicitud de Control de Crédito - Terminar (CCR-T)

Disparador: PGW termina la conexión PDN

Acciones del PCRF:

1. Localizar sesión por ID de sesión
2. Eliminar sesión y registros de llamada asociados
3. Confirmar la terminación

Respuesta: Result-Code 2001

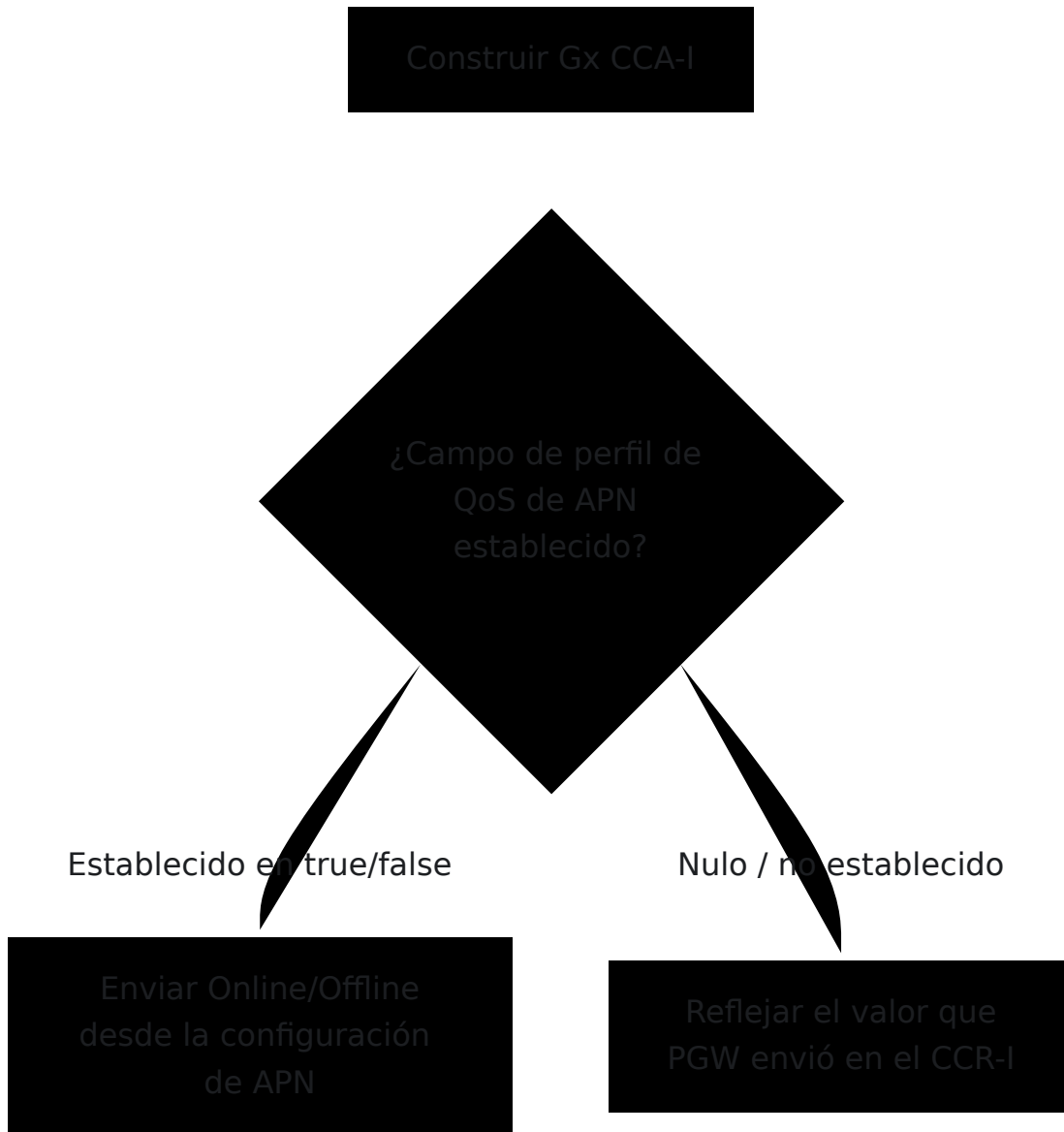
Carga en Línea/Fuera de Línea a Nivel de Sesión

Los AVPs `Online` (AVP 1009) y `Offline` (AVP 1008) enviados en el nivel superior de un Gx CCA-I establecen el **método de carga predeterminado para toda la sesión IP-CAN** (la portadora predeterminada), como se define en [3GPP TS 29.212](#). Esto es distinto del `Online/Offline` por regla que se lleva *dentro* de una Definición de Regla de Carga, que solo rige el tráfico coincidente con esa regla específica.

Por defecto, el PCRF **refleja** los valores que el PGW/PCEF anunció en el CCR-I. El perfil de QoS de APN puede en su lugar **fijar** el método de carga a nivel de sesión, sobrescribiendo el eco. Esto se controla mediante dos campos opcionales en el perfil de QoS de APN:

Campo	Tipo	AVP	Efecto
<code>online_charging_enabled</code>	Booleano	<code>Online</code> (1009)	<code>true</code> → <code>ENABLE_ONLINE (1)</code> , <code>false</code> → <code>DISABLE_ONLINE</code> (0)
<code>offline_charging_enabled</code>	Booleano	<code>Offline</code> (1008)	<code>true</code> → <code>ENABLE_OFFLINE</code> (1), <code>false</code> → <code>DISABLE_OFFLINE</code> (0)

Cada campo se resuelve de forma independiente:



Valores de AVP de Método de Carga (TS 29.212):

AVP	Código	Valor	Nombre	Significado
Online	1009	0	DISABLE_ONLINE	Carga en línea (OCS / Gy) no aplicada a la sesión
Online	1009	1	ENABLE_ONLINE	Carga en línea aplicada - el crédito debe ser otorgado antes de que fluyan los datos
Offline	1008	0	DISABLE_OFFLINE	Carga fuera de línea (CDR / Gz) no aplicada a la sesión
Offline	1008	1	ENABLE_OFFLINE	Carga fuera de línea aplicada - uso registrado para facturación

Cómo funciona: Cuando

`online_charging_enabled`/`offline_charging_enabled` se dejan sin establecer (el valor predeterminado para cada perfil existente), el comportamiento no cambia: el PCRF refleja la solicitud del PGW, por lo que la postura de carga existente de la red se preserva. Establecer cualquiera de los campos obliga a ese modo de carga en cada CCR-I para cualquier APN que use el perfil, independientemente de lo que el PGW anuncie.

Caso de uso: Fijar la carga en línea para un APN prepago (de modo que el PGW deba consultar el OCS incluso si solicitó fuera de línea), o forzar la carga fuera de línea en un APN pospago/IoT para garantizar la generación de CDR. Dado que la configuración reside en el perfil de QoS de APN, se aplica uniformemente a cada APN que haga referencia a ese perfil.

Nota: Esto controla solo el *predeterminado de sesión*. La carga por tráfico sigue estando gobernada por los campos

`online_charging_enabled`/`offline_charging_enabled` en las Reglas de

Carga individuales, que aparecen dentro de los AVPs de Definición de Regla de Carga.

4. Solicitud de Reautenticación (RAR)

Dirección: PCRF → PGW (HSS inicia)

Disparador:

- Configuración de llamada IMS (Rx AAR dispara Gx RAR)
- Terminación de llamada IMS (Rx STR dispara Gx RAR)
- Reautenticación manual a través de REST API

AVPs de RAR:

- Session-Id (ID de sesión PGW)
- Auth-Application-Id: 16,777,238
- Re-Auth-Request-Type (0 = Solo autorizar)
- Charging-Rule-Install/Remove
- QoS-Information (para portadoras dedicadas)

Acciones del PGW: Crear/modificar/eliminar portadoras dedicadas basadas en reglas de carga

Reglas de Carga y Plantillas de Flujo de Tráfico

El PCRF admite la definición de reglas de carga con Plantillas de Flujo de Tráfico (TFT) para controlar:

- **Carga específica de servicio** - Tarifas diferentes para video, juegos, redes sociales, etc.
- **Perfiles de velocidad** - Limitar o priorizar el tráfico que coincide con patrones específicos
- **Políticas basadas en uso** - Aplicar diferentes QoS según el tipo de tráfico o destino

Las reglas de carga pueden ser:

- Instaladas dinámicamente a través de Gx RAR basado en la detección de aplicaciones
- Predefinidas y activadas por condiciones específicas (hora del día, ubicación, cuota)
- Asociadas con TFT utilizando reglas de filtro de paquetes (5-tupla: protocolo, IP de origen/destino, puerto de origen/destino)

Casos de uso comunes:

- **Zero-rating** - Acceso ilimitado a servicios específicos (Spotify, WhatsApp, Facebook) sin consumir cuota de datos
- **Acceso post-cuota** - Permitir portal de autoservicio y sitios de soporte incluso después de que el suscriptor agote la asignación de datos
- **Velocidad por niveles** - Alta velocidad para servicios premium, limitado para contenido estándar
- **Políticas basadas en tiempo** - Streaming ilimitado fuera de pico, priorización en hora pico
- **Políticas de roaming** - Cargos diferentes para uso de datos internacional vs nacional
- **SLA empresariales** - QoS garantizada para aplicaciones críticas para el negocio

Estructura de Política de QoS

QoS de Portadora Predeterminada (del perfil de APN):

```
{
  "QoS-Class-Identifier": 9,           // QCI (9 = portadora
predeterminada)
  "APN-Aggregate-Max-Bitrate-UL": 50000, // kbps
  "APN-Aggregate-Max-Bitrate-DL": 100000, // kbps
  "Allocation-Retention-Priority": {
    "Priority-Level": 8,
    "Pre-emption-Capability": 1,       // Puede preemptar
    "Pre-emption-Vulnerability": 1    // Puede ser preemptado
  }
}
```

QoS de Portadora Dedicada (para VoLTE):

```
{
  "QoS-Class-Identifier": 1,           // QCI 1 = Voz
  Conversacional
  "Max-Requested-Bandwidth-UL": 128000, // bps
  "Max-Requested-Bandwidth-DL": 128000, // bps
  "Guaranteed-Bitrate-UL": 128000,
  "Guaranteed-Bitrate-DL": 128000
}
```

Interfaz Rx

Operaciones soportadas

1. Solicitud AA (AAR) / Respuesta AA (AAA)

Disparador: P-CSCF solicita autorización para sesión de medios IMS (configuración de llamada VoLTE)

AVPs de Solicitud:

- Session-Id (identificador de sesión P-CSCF)
- Subscription-Id (IMSI o URI SIP)
- Media-Component-Description
 - Media-Type (audio, video)
 - Max-Requested-Bandwidth-UL/DL
 - Codec-Data
 - Flow-Description (filtros de paquetes de 5-tupla)
- AF-Application-Identifier

Acciones del PCRF:

1. Buscar suscriptor por IMSI o URI SIP
2. Encontrar sesión IMS activa
3. Extraer parámetros de medios (códec, ancho de banda, reglas de flujo)

4. Crear entrada de seguimiento de llamada
5. **Disparar Gx RAR a PGW** para crear portadora dedicada
6. Esperar respuesta Gx RAA
7. Devolver Rx AAA con resultado de autorización

AVPs de Respuesta:

- Result-Code: 2001 (éxito) o 5063 (servicio no autorizado)

Llamadas de emergencia (SOS), incluidos llamadores no autenticados / sin SIM

Las llamadas de emergencia (`urn:service:sos`) están autorizadas incluso cuando el llamador no es un suscriptor conocido (un dispositivo sin SIM, o un suscriptor en roaming sin credenciales en archivo). Esto es necesario para que las llamadas de emergencia siempre obtengan la QoS correcta (TS 23.167).

Cómo el PCRF reconoce y autoriza un AAR de emergencia:

1. **Detección de emergencia.** La solicitud se trata como de emergencia si **cualquiera** de las `Subscription-Id` es una URI SIP que contiene `sos`, o la `Framed-IP-Address` del AAR se resuelve a una sesión PDN que ya fue creada como una PDN de emergencia por el Gx CCR-I (el lado Gx marca la emergencia por el APN / `Called-Station-Id` que contiene `sos`). El segundo camino es lo que permite que un **invitación** de emergencia **anónima** (sin identidad utilizable) aún sea autorizada.
2. **Resolución del suscriptor.** Buscado por `Subscription-Id`, de lo contrario por `Framed-IP-Address`. Una PDN de emergencia **huérfana** (creada por Gx para un suscriptor desconocido) no tiene suscriptor (`subscriber_state_id: nil`); el AAR toma el camino huérfano en lugar del camino de suscriptor normal.
3. **Perfil de APN SOS.** La QoS de portadora dedicada se toma del perfil de APN SOS (ver "Perfil de APN SOS predeterminado incorporado" a continuación).
4. Un Gx RAR instala la portadora de voz dedicada (QCI 1) en la PDN (huérfana), y el AAA devuelve `2001`.

Nota: una `Framed-IP-Address` solo otorga autorización si se mapea a una PDN que Gx ya creó **como emergencia**. Una solicitud no de emergencia

de un UE no registrado todavía es rechazada en el P-CSCF (nunca llega al PCRF como un AAR de emergencia).

Perfil de APN SOS predeterminado incorporado. La autorización de emergencia ya no depende de que un operador haya pre-provisionado un perfil de APN `sos` en la base de datos. El PCRF resuelve el perfil de APN SOS como:

- un perfil de APN definido por el operador cuyo identificador de APN es `sos`, si existe; de lo contrario
- un **perfil SOS predeterminado incorporado** suministrado por OmniHSS.

El predeterminado incorporado es un perfil transitorio (sin fila de DB, `apn_profile_id: nil` en la PDN huérfana - la columna es nullable) con QoS de emergencia:

Parámetro	Valor
QCI de portadora SOS predeterminada	5
QCI de portadora de voz dedicada	1 (prioridad ARP 2)
Prioridad de Retención de Asignación	1
Capacidad de Preempción	habilitada
Vulnerabilidad a la Preempción	deshabilitada
APN-AMBR UL/DL	10000 kbps

Para sobrescribir estos valores (o para establecer reglas de carga por operador a través de un perfil PCRF), cree un perfil de APN `sos` en la base de datos - tiene prioridad sobre el predeterminado incorporado.

2. Solicitud de Terminación de Sesión (STR) / Respuesta de Terminación de Sesión (STA)

Disparador: P-CSCF termina la sesión IMS (finalización de llamada)

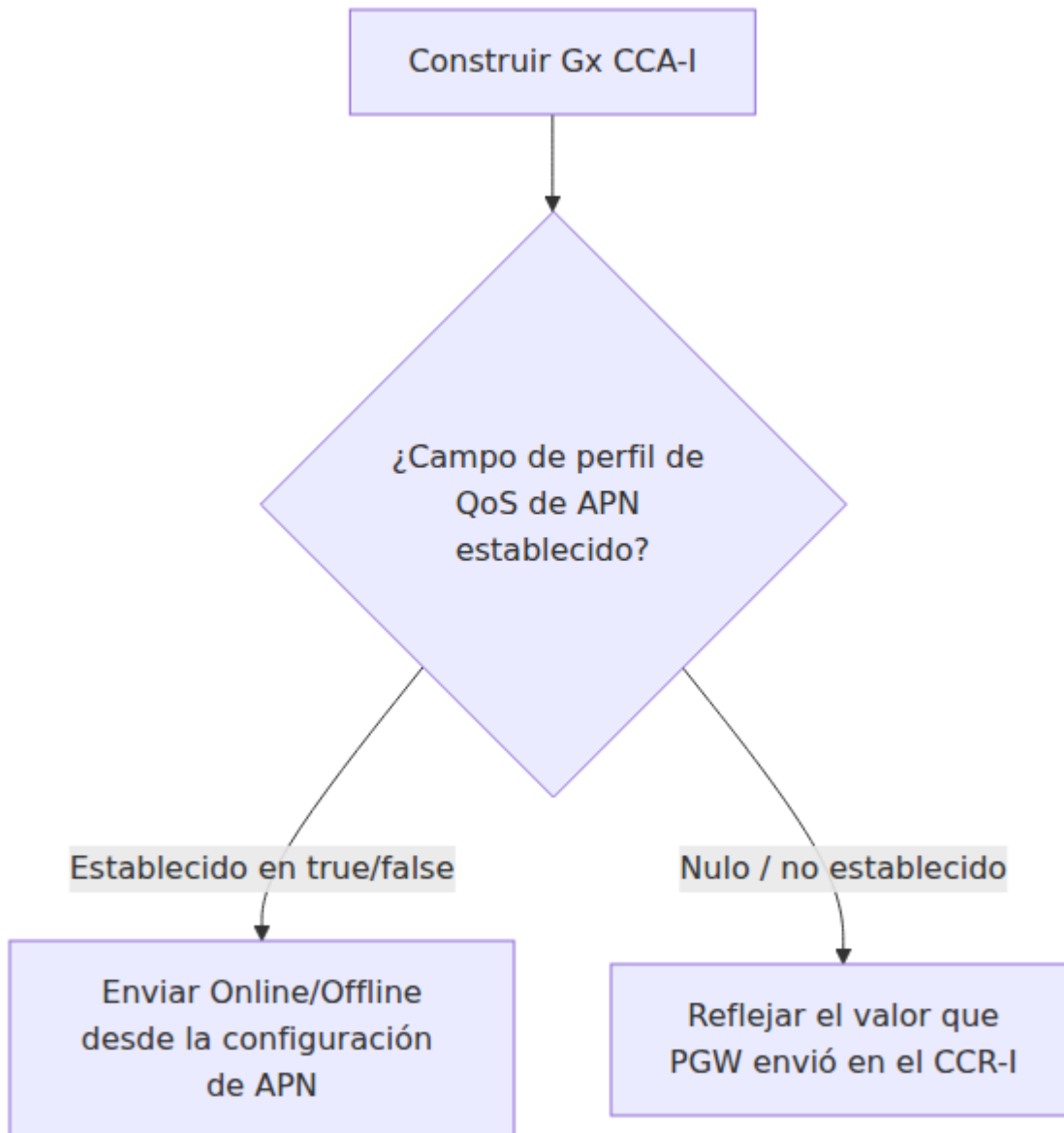
Acciones del PCRF:

1. Localizar sesión de llamada por ID de sesión P-CSCF
2. **Disparar Gx RAR a PGW** para eliminar portadora dedicada
3. Eliminar entrada de seguimiento de llamada
4. Devolver confirmación de STA

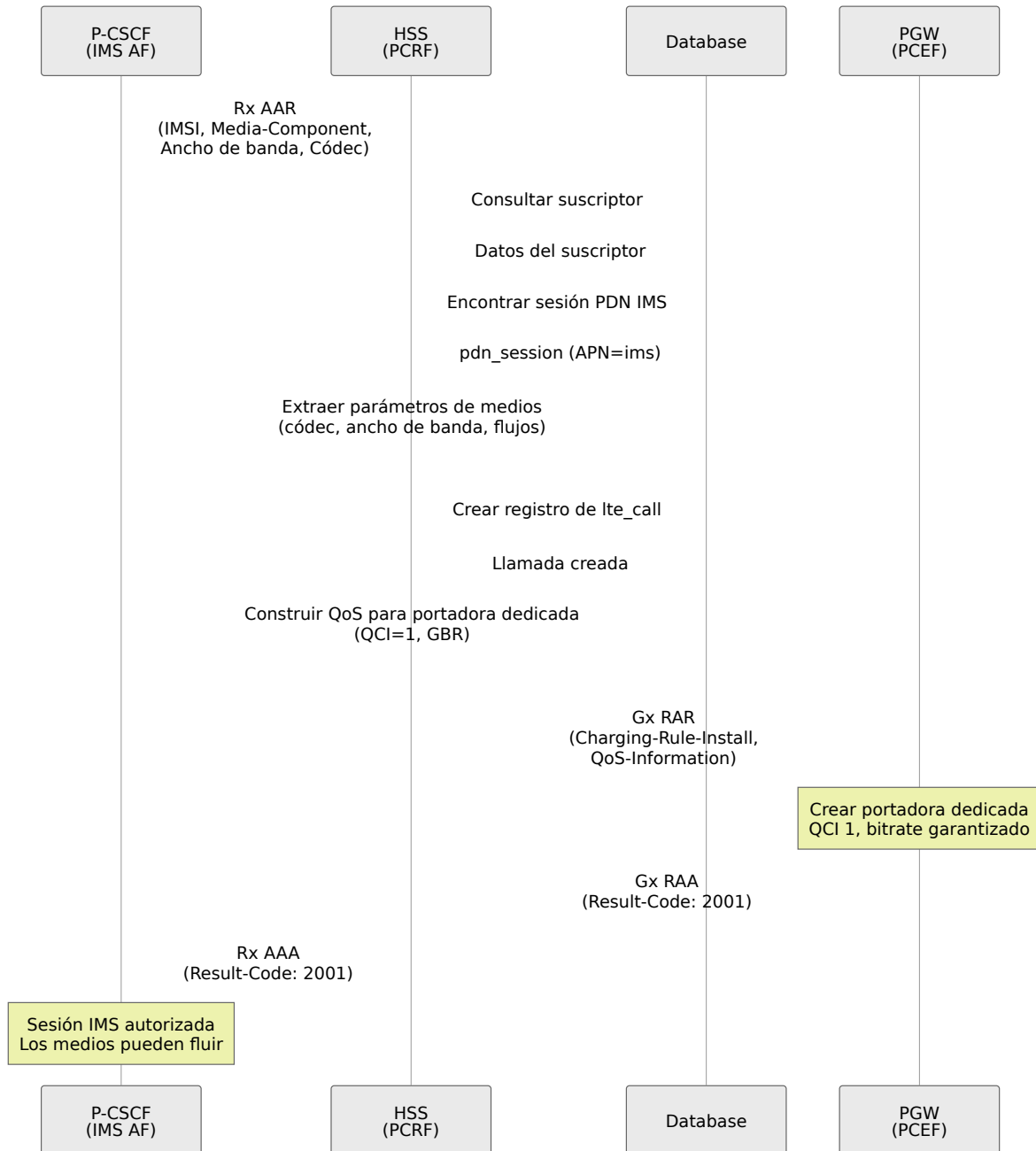
Respuesta: Result-Code 2001

Flujos de Mensajes Comunes

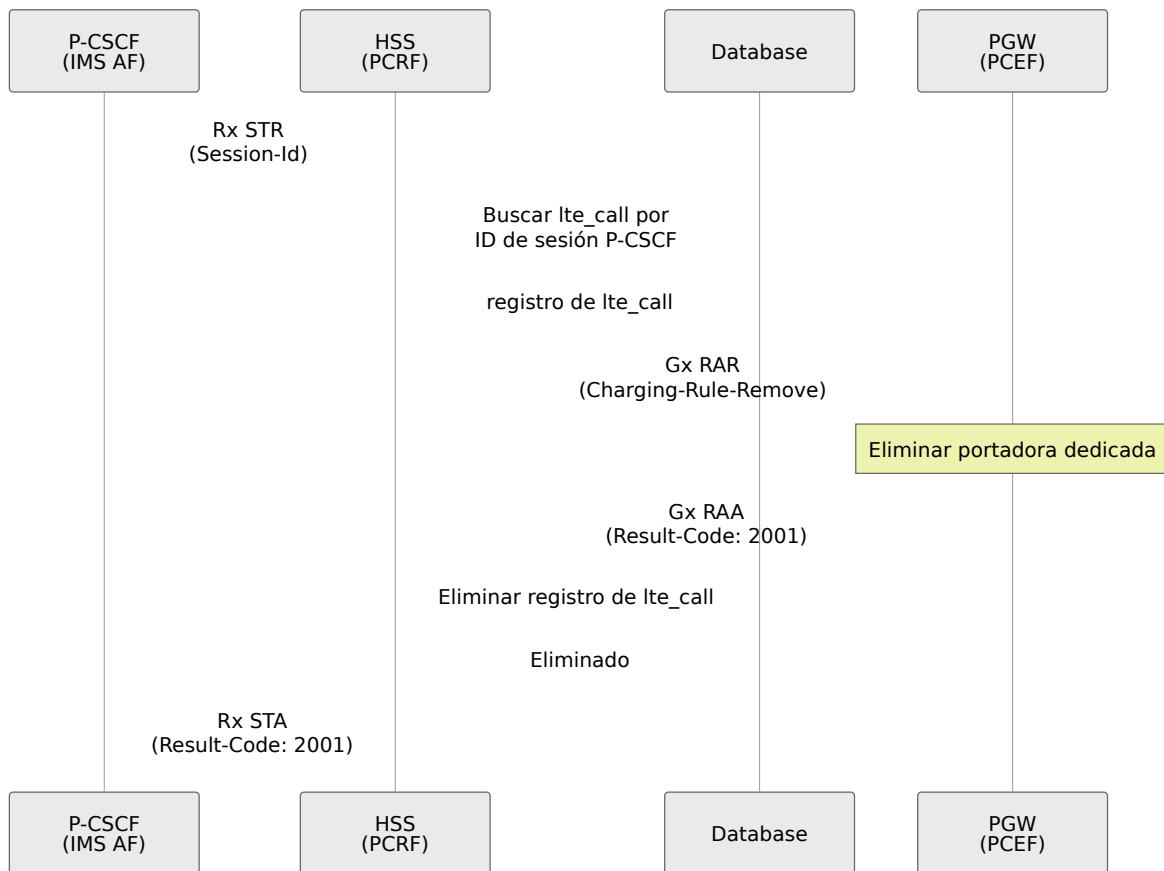
Flujo 1: Establecimiento de Sesión PDN



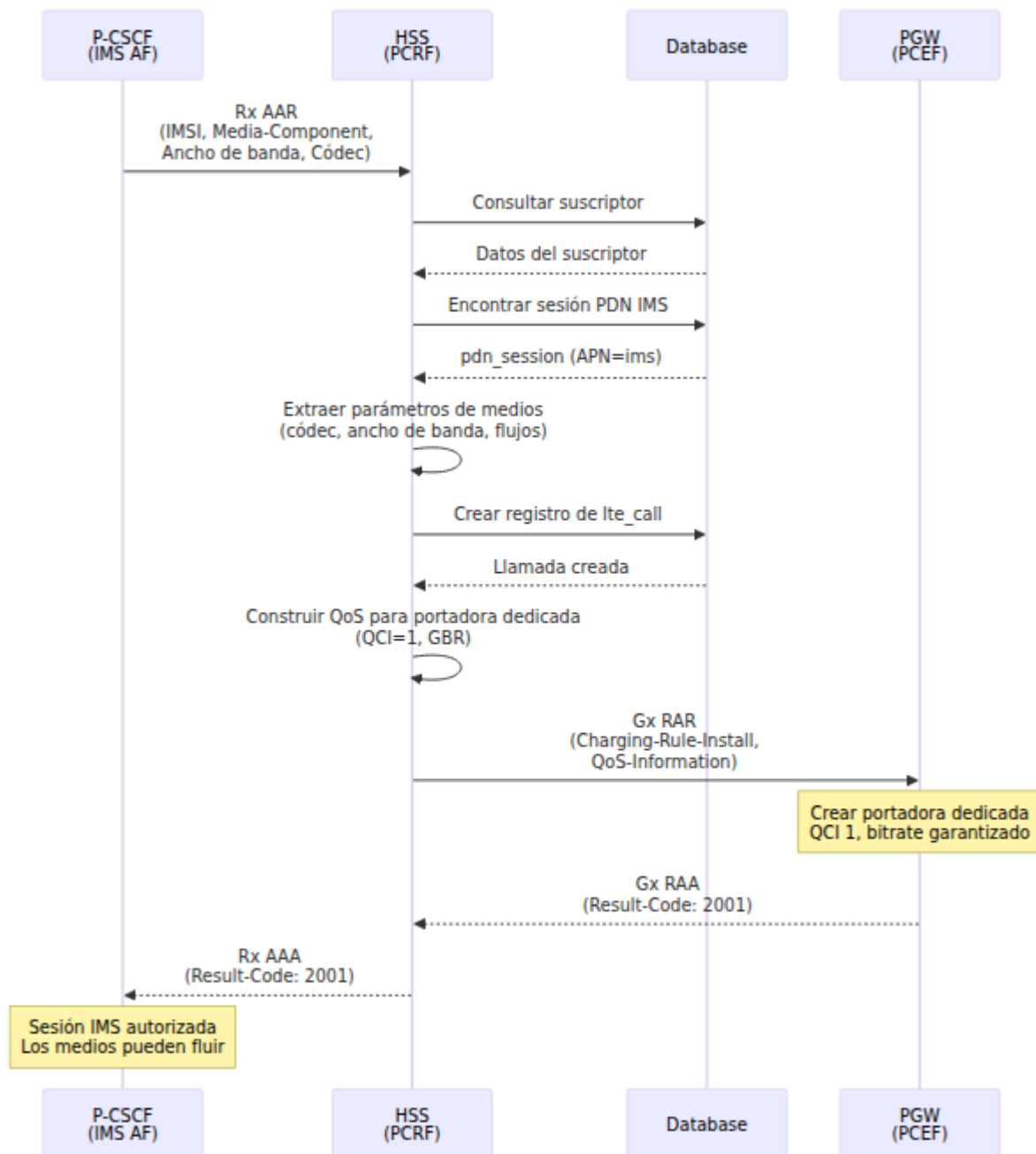
Flujo 2: Configuración de Llamada VoLTE (Rx AAR → Gx RAR)



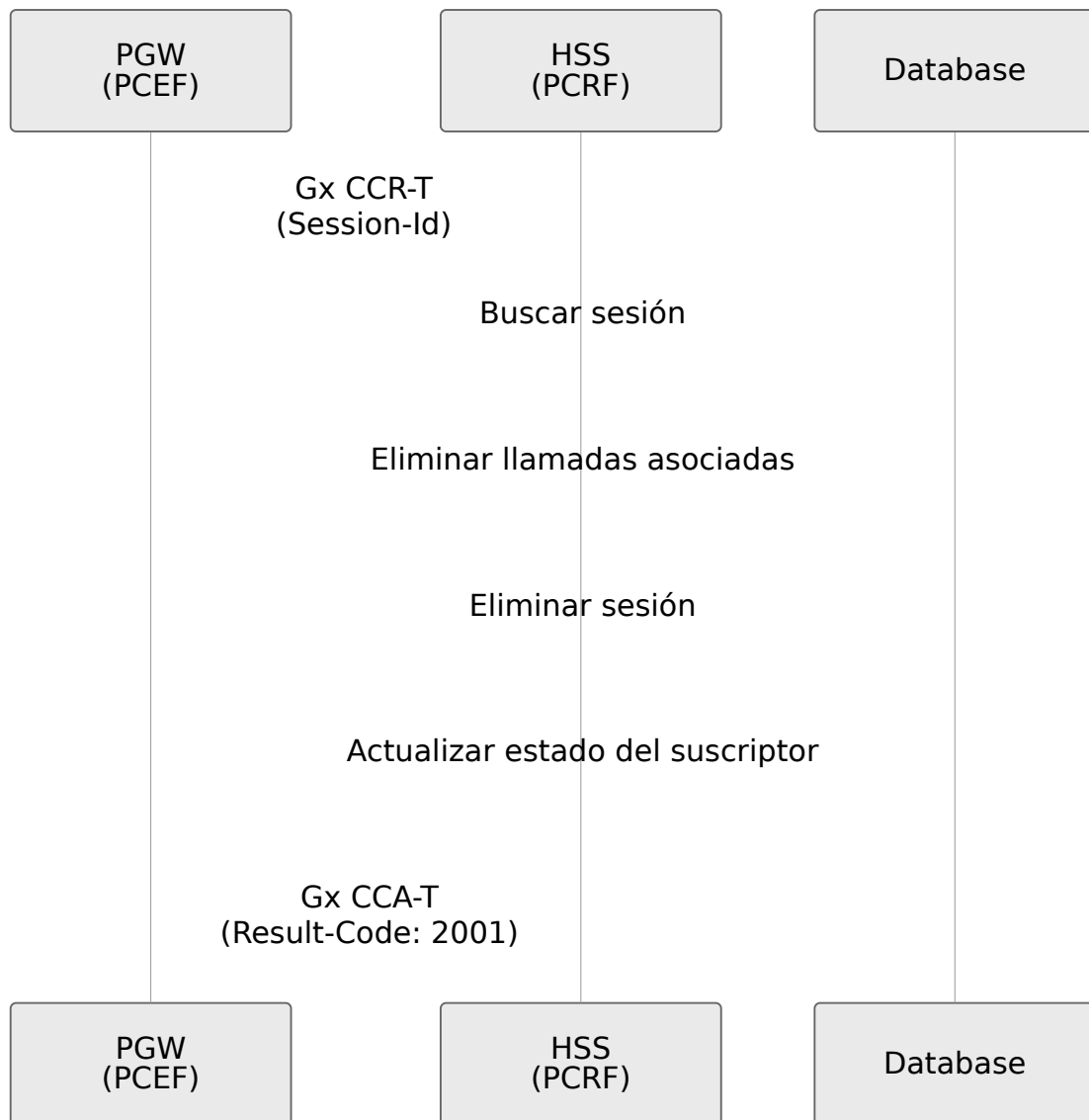
Flujo 3: Terminación de Llamada VoLTE (Rx STR → Gx RAR)



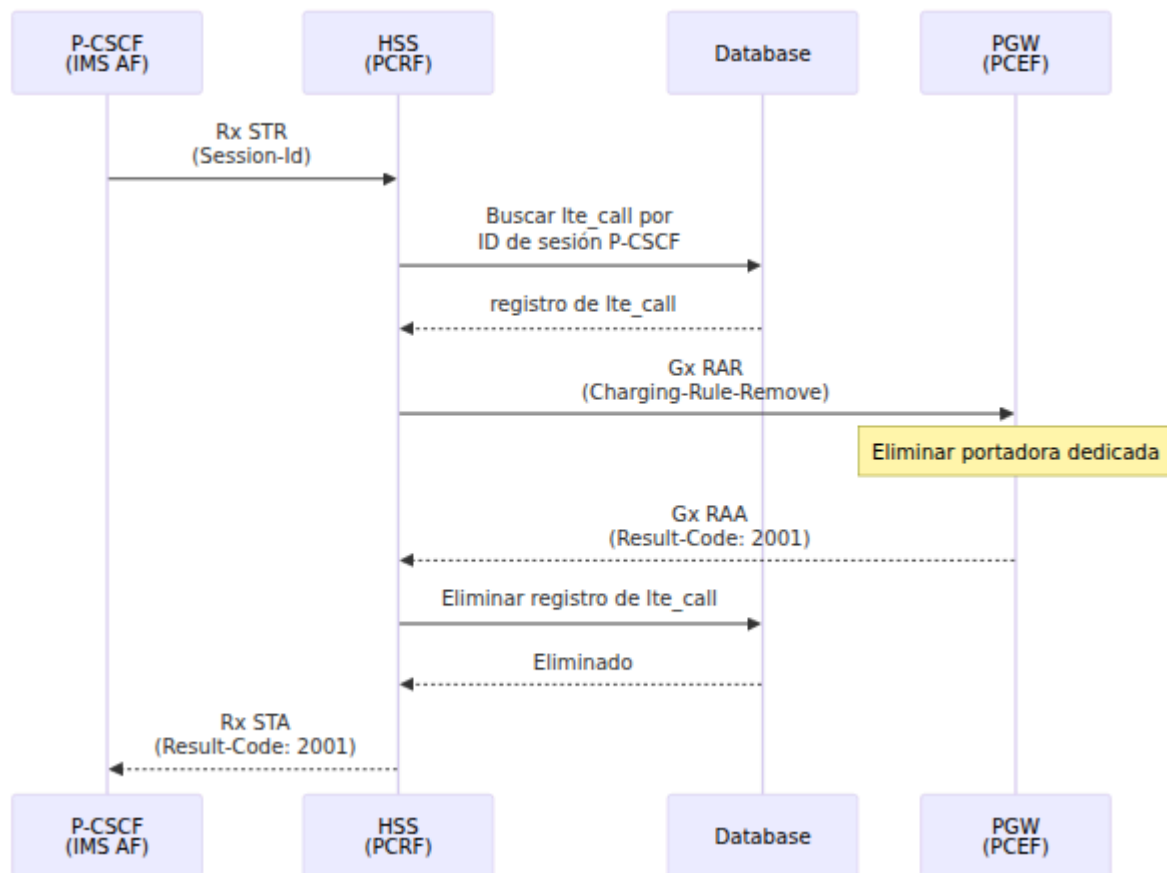
Flujo 4: Actualización de Sesión PDN



Flujo 5: Terminación de Sesión PDN



Flujo 6: Reautenticación Manual a través de REST API



REST API

Endpoint de Reautenticación PCRF

Endpoint: `POST /api/operation/pcrf_re_auth`

Propósito: Disparar manualmente la Solicitud de Reautenticación Gx para refrescar políticas

Cuándo usar: Este endpoint manual se utiliza típicamente para solucionar problemas o forzar la actualización de políticas en suscriptores específicos. Para actualizaciones de políticas de rutina (cambio de perfiles de QoS de APN), el sistema dispara automáticamente reautenticaciones para todas las sesiones afectadas - no se necesita acción manual.

Cuerpo de Solicitud:

```
{  
  "imsi": "999999876543210",  
  "apn": "ims"  
}
```

Respuesta de Éxito (HTTP 200):

```
{  
  "data": "Solicitud de Reautenticación Gx para 999999876543210  
enviada a pgw.epc.mnc999.mcc999.3gppnetwork.org, Result-Code:  
2001"  
}
```

Respuesta de Error (HTTP 400):

```
{  
  "error": "No se pudo enviar la Solicitud de Reautenticación para  
999999876543210 en APN ims, no se encontró sesión PDN activa"  
}
```

API de Configuración de Políticas

El PCRF recupera políticas de QoS de configuraciones de APN almacenadas en la base de datos. Estas políticas pueden ser creadas y gestionadas a través de la REST API.

Ejecución Automática de Políticas: Cuando actualiza un perfil de QoS de APN (por ejemplo, cambia límites de ancho de banda o QCI), el sistema envía automáticamente Solicitudes de Reautenticación Gx (RAR) a todos los PGWs con sesiones PDN activas que utilizan ese APN. Esto asegura que los cambios de política se apliquen inmediatamente a todos los suscriptores conectados sin intervención manual.

Arquitectura de Políticas

Las políticas se definen a través de una estructura de tres niveles:

```
Identificador de APN → Perfil de QoS de APN → Perfil de APN
    ↓                ↓                ↓
  "internet"      QCI, AMBR, ARP    Vincula ambos
```

1. Crear Identificador de APN

Defina el nombre del APN y el soporte de versión IP.

Endpoint: `POST /api/apn/identifier`

Cuerpo de Solicitud:

```
{
  "apn_identifier": {
    "apn": "internet",
    "ip_version": "ipv4v6"
  }
}
```

Opciones de Versión IP:

- `"ipv4"` - Solo IPv4
- `"ipv6"` - Solo IPv6
- `"ipv4v6"` - Pilas duales (tanto IPv4 como IPv6)
- `"ipv4_or_ipv6"` - La red decide (ya sea IPv4 o IPv6)

Respuesta (HTTP 201):

```
{
  "data": {
    "id": "4fa85f64-5717-4562-b3fc-2c963f66afa6",
    "apn": "internet",
    "ip_version": "ipv4v6"
  }
}
```

Validación:

- `apn`: Requerido, 1-254 caracteres, único
- `ip_version`: Requerido, debe ser una de las cuatro opciones anteriores

Listar Identificadores de APN: `GET /api/apn/identifier`

2. Crear Perfil de QoS de APN

Defina los parámetros de QoS (ancho de banda, QCI, prioridad).

Endpoint: `POST /api/apn/qos_profile`

Cuerpo de Solicitud:

```
{
  "apn_qos_profile": {
    "name": "Internet de Mejor Esfuerzo",
    "qci": 9,
    "allocation_retention_priority": 8,
    "apn_ambr_dl_kbps": 100000,
    "apn_ambr_ul_kbps": 50000,
    "pre_emption_capability": false,
    "pre_emption_vulnerability": true,
    "online_charging_enabled": false,
    "offline_charging_enabled": true
  }
}
```

Parámetros de QoS:

Campo	Tipo	Rango	Descripción
name	string	1-254 chars	Nombre del p (único)
qci	integer	1-254	Identificador Clase de QoS 4 = GBR, 5-9 No-GBR)
allocation_retention_priority	integer	1-15	Nivel de ARP = mayor prioridad)
apn_ambr_dl_kbps	integer	1- 4,294,967,293	Tasa de Bit Máxima Agregada de Descendente (kbps)
apn_ambr_ul_kbps	integer	1- 4,294,967,293	Tasa de Bit Máxima Agregada de Ascendente (kbps)
pre_emption_capability	boolean	true/false	Puede preem portadoras d menor prioric
pre_emption_vulnerability	boolean	true/false	Puede ser preemptado portadoras d mayor prioric
online_charging_enabled	boolean	true/false/null	AVP Online a nivel de sesic

Campo	Tipo	Rango	Descripción
			para el Gx CC null (predeterminado) refleja el valor CCR-I del PGW Ver Carga en Línea/Fuera de Línea a Nivel Sesión
offline_charging_enabled	boolean	true/false/null	AVP Offline nivel de sesión para el Gx CC null (predeterminado) refleja el valor CCR-I del PGW Ver Carga en Línea/Fuera de Línea a Nivel Sesión

Valores comunes de QCI:

- 1 - Voz Conversacional (VoLTE) - GBR, presupuesto de retraso de 100 ms
- 2 - Video Conversacional - GBR, presupuesto de retraso de 150 ms
- 5 - Señalización IMS - No-GBR, presupuesto de retraso de 100 ms
- 9 - Portadora Predeterminada (Internet) - No-GBR, presupuesto de retraso de 300 ms

Respuesta (HTTP 201):

```
{
  "data": {
    "id": "8d8ac610-566d-4ef0-9c22-186b2a5ed793",
    "name": "Internet de Mejor Esfuerzo",
    "qci": 9,
    "allocation_retention_priority": 8,
    "apn_ambr_dl_kbps": 100000,
    "apn_ambr_ul_kbps": 50000,
    "pre_emption_capability": false,
    "pre_emption_vulnerability": true,
    "online_charging_enabled": false,
    "offline_charging_enabled": true
  }
}
```

Listar Perfiles de QoS: GET /api/apn/qos_profile

3. Crear Perfil de APN

Vincule el identificador de APN con un perfil de QoS.

Endpoint: POST /api/apn/profile

Cuerpo de Solicitud:

```
{
  "apn_profile": {
    "name": "Perfil de APN de Internet",
    "apn_identifier_id": "4fa85f64-5717-4562-b3fc-2c963f66afa6",
    "apn_qos_profile_id": "8d8ac610-566d-4ef0-9c22-186b2a5ed793"
  }
}
```

Campos:

- `name`: Nombre del perfil (único), utilizado para referencia
- `apn_identifier_id`: ID de [Crear Identificador de APN](#)
- `apn_qos_profile_id`: ID de [Crear Perfil de QoS de APN](#)

Respuesta (HTTP 201):

```
{
  "data": {
    "id": "a1b2c3d4-e5f6-4a3b-8c2d-1e0f9a8b7c6d",
    "name": "Perfil de APN de Internet",
    "apn_identifier_id": "4fa85f64-5717-4562-b3fc-2c963f66afa6",
    "apn_qos_profile_id": "8d8ac610-566d-4ef0-9c22-186b2a5ed793"
  }
}
```

Restricciones:

- `apn_identifier_id` y `apn_qos_profile_id` deben referenciar registros existentes
- Cada combinación de identificador de APN y perfil de QoS debe ser única

Listar Perfiles de APN: `GET /api/apn/profile`

Ejemplo Completo de Configuración de Políticas

Paso 1: Crear Política de APN IMS (VoLTE)

1. Crear Identificador de APN

```
curl -X POST https://hss.example.com:8443/api/apn/identifier \
-H "Content-Type: application/json" \
-d '{
  "apn_identifier": {
    "apn": "ims",
    "ip_version": "ipv4v6"
  }
}'
```

Respuesta: {"data": {"id": "2c3e4f5a-6b7c-4d8e-9f0a-1b2c3d4e5f6a", ...}}

2. Crear Perfil de QoS (Señalización IMS)

```
curl -X POST https://hss.example.com:8443/api/apn/qos_profile \
-H "Content-Type: application/json" \
-d '{
  "apn_qos_profile": {
    "name": "QoS de Señalización IMS",
    "qci": 5,
    "allocation_retention_priority": 2,
    "apn_ambr_dl_kbps": 5000,
    "apn_ambr_ul_kbps": 5000,
    "pre_emption_capability": true,
    "pre_emption_vulnerability": false
  }
}'
```

Respuesta: {"data": {"id": "7b44a3e0-27cc-4b21-8d7a-3f19e5c2b8d4", ...}}

3. Crear Perfil de APN

```
curl -X POST https://hss.example.com:8443/api/apn/profile \
-H "Content-Type: application/json" \
-d '{
  "apn_profile": {
    "name": "Perfil de APN IMS",
    "apn_identifier_id": "2c3e4f5a-6b7c-4d8e-9f0a-1b2c3d4e5f6a",
    "apn_qos_profile_id": "7b44a3e0-27cc-4b21-8d7a-3f19e5c2b8d4"
  }
}'
```

Respuesta: {"data": {"id": "91c2f3a4-5d6e-4f7a-8b9c-0d1e2f3a4b5c", ...}}

Paso 2: Asignar al Suscriptor

Una vez creado, el perfil de APN se asigna a los suscriptores a través de perfiles EPC. Consulte [Referencia de API](#) para vincular perfiles de APN a suscriptores.

Actualización y Eliminación de Políticas

Actualizar Perfil de QoS:

```
PATCH /api/apn/qos_profile/{id}
PUT /api/apn/qos_profile/{id}
```

Ejemplo - Aumentar Ancho de Banda para Todos los Usuarios:

```
# Actualizar el perfil de QoS para aumentar el ancho de banda
curl -X PATCH
https://hss.example.com:8443/api/apn/qos_profile/8d8ac610-566d-
4ef0-9c22-186b2a5ed793 \
-H "Content-Type: application/json" \
-d '{
  "apn_qos_profile": {
    "apn_ambr_dl_kbps": 150000,
    "apn_ambr_ul_kbps": 75000
  }
}'
```

Qué sucede automáticamente:

1. El perfil de QoS se actualiza en la base de datos
2. El sistema identifica todas las sesiones PDN activas que utilizan APNs vinculados a este perfil de QoS
3. Para cada sesión activa, se envía un Gx RAR al PGW correspondiente
4. Los PGWs actualizan la QoS de la portadora para reflejar los nuevos límites de ancho de banda
5. Todos los suscriptores conectados reciben inmediatamente la política actualizada

Escenario de ejemplo: Si 100 suscriptores están actualmente conectados en el APN "internet" utilizando este perfil de QoS, todos los 100 tendrán sus límites de ancho de banda actualizados a 150 Mbps de descarga / 75 Mbps de subida dentro de segundos de que se complete la llamada a la API.

Nota: Cuando actualiza un perfil de QoS de APN, el sistema **dispara automáticamente la reautenticación** para todas las sesiones PDN activas que utilizan ese APN, aplicando las nuevas políticas de inmediato a los suscriptores conectados. No se requiere reautenticación manual.

Eliminar Recursos:

```
DELETE /api/apn/identifier/{id}
DELETE /api/apn/qos_profile/{id}
DELETE /api/apn/profile/{id}
```

Restricciones de Eliminación:

- No se pueden eliminar identificadores de APN o perfiles de QoS referenciados por perfiles de APN
- No se pueden eliminar perfiles de APN asignados a suscriptores activos

Plantillas de Políticas

Internet de Alta Velocidad (100 Mbps de descarga / 50 Mbps de subida):

```
{
  "apn_qos_profile": {
    "name": "Internet de Alta Velocidad",
    "qci": 9,
    "allocation_retention_priority": 8,
    "apn_ambr_dl_kbps": 100000,
    "apn_ambr_ul_kbps": 50000,
    "pre_emption_capability": false,
    "pre_emption_vulnerability": true
  }
}
```

Internet Premium (500 Mbps de descarga / 100 Mbps de subida):

```
{
  "apn_qos_profile": {
    "name": "Internet Premium",
    "qci": 8,
    "allocation_retention_priority": 5,
    "apn_ambr_dl_kbps": 500000,
    "apn_ambr_ul_kbps": 100000,
    "pre_emption_capability": true,
    "pre_emption_vulnerability": false
  }
}
```

IoT/M2M (Bajo Ancho de Banda):

```
{
  "apn_qos_profile": {
    "name": "IoT M2M",
    "qci": 9,
    "allocation_retention_priority": 10,
    "apn_ambr_dl_kbps": 1024,
    "apn_ambr_ul_kbps": 512,
    "pre_emption_capability": false,
    "pre_emption_vulnerability": true
  }
}
```

Servicios de Emergencia (Mayor Prioridad):


```
{
  "apn_qos_profile": {
    "name": "APN de Emergencia",
    "qci": 5,
    "allocation_retention_priority": 1,
    "apn_ambr_dl_kbps": 10000,
    "apn_ambr_ul_kbps": 10000,
    "pre_emption_capability": true,
    "pre_emption_vulnerability": false
  }
}
```

Configuración

Configuración del Servicio Diameter

Aplicación Gx (`config/runtime.exs`):

```
%{
  application_name: :gx,
  application_dictionary: :diameter_gen_3gpp_gx,
  vendor_specific_application_ids: [
    %{vendor_id: 10415, auth_application_id: 16_777_238}
  ]
}
```

Aplicación Rx (`config/runtime.exs`):

```
%{
  application_name: :rx,
  application_dictionary: :diameter_gen_3gpp_rx,
  vendor_specific_application_ids: [
    %{vendor_id: 10415, auth_application_id: 16_777_236}
  ]
}
```

Parámetros de QoS

Los parámetros de QoS se obtienen de:

- **Portadora Predeterminada:** Configuración de perfil de APN en la base de datos
 - `apn_qos_profile.qci` (Identificador de Clase de QoS)
 - `apn_qos_profile.apn_ambr_ul_kbps` (Tasa de Bit Máxima Agregada Ascendente)
 - `apn_qos_profile.apn_ambr_dl_kbps` (Tasa de Bit Máxima Agregada Descendente)
 - `apn_qos_profile.priority_level` (Prioridad de Retención de Asignación)
- **Portadora Dedicada:** Extraído de la Descripción del Componente de Medios AAR Rx
 - QCI: 1 (Voz Conversacional)
 - Bitrate Garantizado: De los AVPs de Ancho de Banda Máximo Solicitado
 - Filtros de flujo: De los AVPs de Descripción de Flujo

Manejo de Errores

Código de Resultado	Tipo	Significado	Causa
2001	Éxito	DIAMETER_SUCCESS	Solicitud procesada con éxito
5001	Experimental	Usuario no encontrado	IMSI no en la base de datos de suscriptores
5002	Experimental	Sesión no encontrada	La sesión PDN no existe para actualizar/terminar
5063	Experimental	Servicio no autorizado	Autorización de medios IMS denegada

Detalles de Implementación

Gestión de Sesiones

El PCRF rastrea:

- **Sesiones PDN Activas** - Una por APN, por suscriptor
- **Llamadas VoLTE** - Múltiples llamadas por sesión IMS (soporta llamadas en conferencia)
- **Políticas de QoS** - Aplicadas dinámicamente según la configuración de APN
- **Reglas de Carga** - Plantillas de flujo de tráfico y políticas específicas de servicio

Características Avanzadas de Políticas

El PCRF admite control avanzado de políticas, incluyendo:

- **Instalación/eliminación de reglas de carga** a través de la interfaz Gx
- **Coincidencia de Plantillas de Flujo de Tráfico (TFT)** para diferenciación de servicios
- **Perfiles de velocidad dinámicos** basados en la aplicación o tipo de tráfico
- **Políticas conscientes del servicio** activadas por condiciones de red o comportamiento del suscriptor

Contacte a su administrador del sistema para obtener información sobre cómo configurar reglas de carga avanzadas y políticas basadas en TFT.

Documentación Relacionada

- [Interfaz Sy](#) - Control del límite de gasto del suscriptor contra un OCS externo
- [Protocolos Diameter](#) - Especificaciones detalladas de protocolos
- [Referencia de API](#) - Documentación completa de la API
- [Arquitectura](#) - Arquitectura general del HSS
- [Mapeo de Datos](#) - Mapeos de base de datos a AVP Diameter

Manejo de Errores de API

[← Volver a la Referencia de API](#)

Tabla de Contenidos

- [Respuestas de Error Comunes](#)
 - [Flujo de Manejo de Errores](#)
-

Respuestas de Error Comunes

400 Solicitud Incorrecta

```
{  
  "error": "Formato JSON inválido"  
}
```

Causas:

- JSON mal formado
- Campos requeridos faltantes
- Tipos de datos inválidos

404 No Encontrado

```
{  
  "error": "Recurso no encontrado"  
}
```

Causas:

- Suscriptor/perfil/entidad no existe
- ID incorrecto en la URL

422 Entidad No Procesable

```
{
  "errors": {
    "imsi": ["ya ha sido tomado"],
    "key_set_id": ["no existe"]
  }
}
```

Causas:

- Fallos de validación
- Restricciones de base de datos violadas
- Referencias de clave foránea no existen

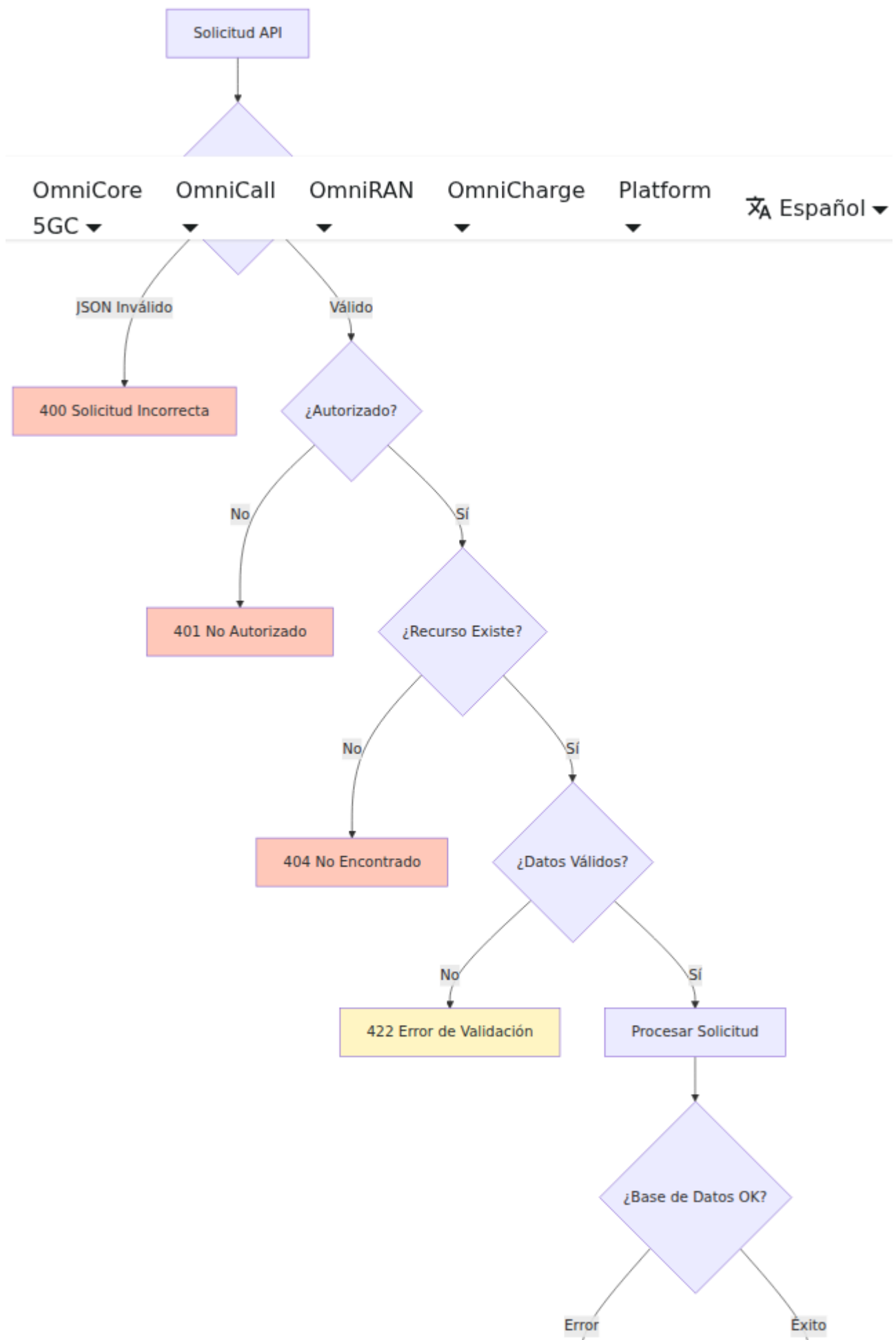
500 Error Interno del Servidor

```
{
  "error": "Error interno del servidor"
}
```

Causas:

- Problemas de conectividad con la base de datos
 - Errores inesperados de la aplicación
-

Flujo de Manejo de Errores



↓
500 Error del Servidor

↓
200/201 Éxito

← [Volver a la Referencia de API](#)

Ejemplos de Uso de la API

[← Volver a la Referencia de la API](#)

Tabla de Contenidos

- [Provisionamiento Completo de Suscriptores](#)
 - [Pre-Provisionamiento de Suscriptores Inactivos](#)
 - [Provisionamiento Completo de IP Estática](#)
-

Provisionamiento Completo de Suscriptores

Este ejemplo demuestra el flujo de trabajo completo para provisionar un nuevo suscriptor desde cero. El proceso implica crear todos los perfiles y componentes requeridos antes de crear el suscriptor.

Requisitos Previos: Este ejemplo utiliza `jq` para el análisis de JSON. Instalar con `apt-get install jq` o `brew install jq`.

Secciones Relacionadas:

- [Gestión de Conjuntos de Claves](#)
- [Perfiles APN](#)
- [Perfiles EPC](#)
- [Gestión de Suscriptores](#)

1. Crear Conjunto de Claves

```
KEY_SET_ID=$(curl -k -X POST
https://hss.example.com:8443/api/key_set \
-H "Content-Type: application/json" \
-d '{
  "ki": "0123456789ABCDEF0123456789ABCDEF",
  "opc": "FEDCBA9876543210FEDCBA9876543210",
  "authentication_algorithm": "milenage",
  "amf": "8000",
  "sqn": 0
}' | jq -r '.response.id')
```

2. Crear Perfil de QoS APN

```
APN_QOS_ID=$(curl -k -X POST
https://hss.example.com:8443/api/apn/qos_profile \
-H "Content-Type: application/json" \
-d '{
  "name": "Default Internet QoS",
  "allocation_retention_priority": 8,
  "apn_ambr_dl_kbps": 50000,
  "apn_ambr_ul_kbps": 25000,
  "pre_emption_capability": true,
  "pre_emption_vulnerability": true,
  "qci": 9
}' | jq -r '.response.id')
```

3. Crear Identificador APN

```
APN_ID=$(curl -k -X POST
https://hss.example.com:8443/api/apn/identifier \
-H "Content-Type: application/json" \
-d '{
  "apn": "internet",
  "ip_version": "ipv4v6"
}' | jq -r '.response.id')
```

4. Crear Perfil APN

```
APN_PROFILE_ID=$(curl -k -X POST
https://hss.example.com:8443/api/apn/profile \
-H "Content-Type: application/json" \
-d '{
  "apn_identifier_id": \"$APN_ID\",
  "apn_qos_profile_id": \"$APN_QOS_ID\",
  "name": \"Internet APN\"
}
```

```

}" | jq -r '.response.id')

# 5. Crear Perfil EPC
EPC_PROFILE_ID=$(curl -k -X POST
https://hss.example.com:8443/api/epc/profile \
-H "Content-Type: application/json" \
-d "{
  \"apn_profiles\": [$APN_PROFILE_ID],
  \"name\": \"Standard Data Plan\",
  \"network_access_mode\": \"packet_only\",
  \"tracking_area_update_interval_seconds\": 600,
  \"ue_ambr_dl_kbps\": 100000,
  \"ue_ambr_ul_kbps\": 50000
}" | jq -r '.response.id')

# 6. Crear Suscriptor
SUBSCRIBER_ID=$(curl -k -X POST
https://hss.example.com:8443/api/subscriber \
-H "Content-Type: application/json" \
-d "{
  \"imsi\": \"001001123456789\",
  \"key_set_id\": \"$KEY_SET_ID\",
  \"epc_profile_id\": \"$EPC_PROFILE_ID\"
}" | jq -r '.response.id')

echo "Suscriptor provisionado con éxito con ID: $SUBSCRIBER_ID"

```

Qué Crea Esto:

Este flujo de trabajo de provisionamiento crea un suscriptor completo con:

1. **Claves criptográficas** ([Conjunto de Claves](#)) - Para autenticación
2. **Perfil de servicio de datos** ([Perfil EPC](#)) - Configuraciones de ancho de banda y acceso a la red
3. **Configuración APN** ([Perfil APN](#)) - Punto de acceso con QoS
4. **Registro de suscriptor** ([Suscriptor](#)) - La entidad de suscriptor real

Próximos Pasos:

- Agregar números de teléfono: Ver [Gestión de MSISDN](#)
- Habilitar servicios de voz: Crear y asignar [Perfil IMS](#)

- Configurar roaming: Crear y asignar [Perfil de Roaming](#)
- Vincular SIM física: Crear y asignar [SIM](#)

Ver También:

- [Documentación Multi-MSISDN](#) - Asignación de múltiples números de teléfono
 - [Documentación de Perfiles](#) - Configuración avanzada de perfiles
-

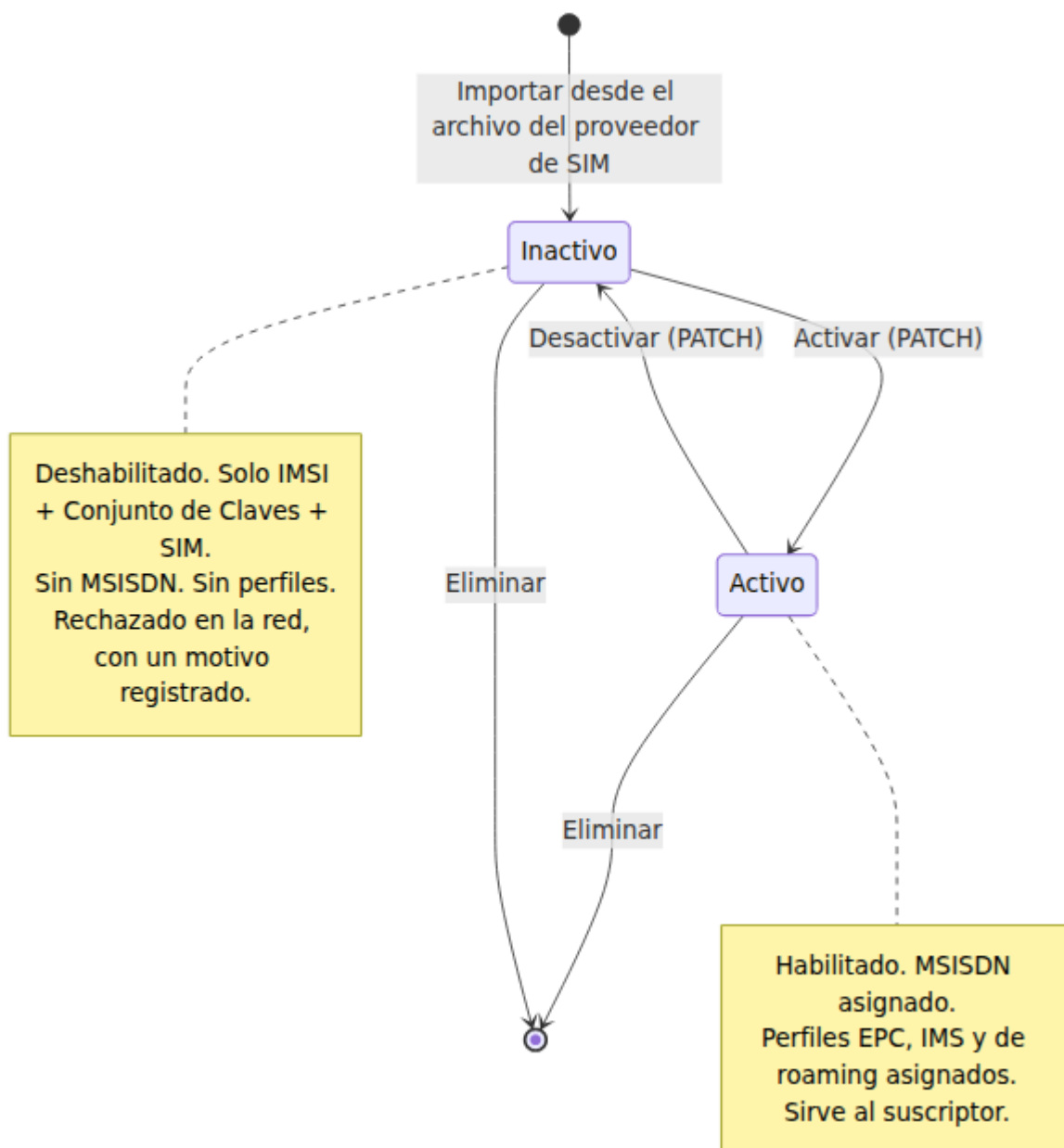
Pre-Provisionamiento de Suscriptores Inactivos

Utilice este flujo de trabajo para cargar suscriptores en masa desde un archivo de salida de proveedor de SIM, y para activar cada suscriptor más tarde. Este es el modelo recomendado para la mayoría de los operadores.

Un suscriptor inactivo solo mantiene su identidad y sus claves de autenticación. Se agrega el número de teléfono y los perfiles de servicio al momento de la activación. Esto coincide con los datos que un proveedor de SIM le envía. El archivo del proveedor de SIM contiene el ICCID, el PIN, los códigos PUK y ADM, y las claves de autenticación (Ki, OPc). El archivo no contiene un número de teléfono ni un plan de servicio.

La base de datos solo necesita el IMSI y el Conjunto de Claves para insertar un Suscriptor. Esto es lo que hace posible un registro inactivo. No significa que los otros objetos sean opcionales para el servicio. Cada objeto es requerido para su propio servicio: el perfil EPC para datos, el perfil IMS y un MSISDN para voz, y una SIM para autenticación. Un suscriptor inactivo no funciona en la red hasta que se le asigne el objeto correspondiente. Se asignan estos objetos cuando el cliente activa el servicio. Debido a que la SIM, el Conjunto de Claves y el Suscriptor son objetos separados, consulte [Conjunto de Claves, SIM y Suscriptor](#).

Ciclo de Vida del Provisionamiento



Paso 1: Importar (crear la SIM, el Conjunto de Claves y un Suscriptor deshabilitado)

Cree un Conjunto de Claves, una SIM y un Suscriptor deshabilitado para cada fila en el archivo del proveedor de SIM. Este ejemplo utiliza `jq` para leer el identificador devuelto de cada respuesta.

1. Crear el Conjunto de Claves desde el archivo del proveedor de SIM (Ki, OPc)

```
KEY_SET_ID=$(curl -k -X POST
https://hss.example.com:8443/api/key_set \
-H "Content-Type: application/json" \
-d '{
  "ki": "0123456789ABCDEF0123456789ABCDEF",
  "opc": "FEDCBA9876543210FEDCBA9876543210",
  "authentication_algorithm": "milenege",
  "amf": "8000",
  "sqn": 0
}' | jq -r '.response.id')
```

2. Crear la SIM desde el archivo del proveedor de SIM (ICCID, PIN/PUK/ADM)

```
SIM_ID=$(curl -k -X POST https://hss.example.com:8443/api/sim \
-H "Content-Type: application/json" \
-d '{
  "iccid": "89440000000000000001",
  "is_esim": false,
  "ind_length": 5
}' | jq -r '.response.id')
```

3. Crear el Suscriptor en un estado deshabilitado.

imsi y key_set_id son requeridos. Vincular la SIM. No agregar MSISDN ni perfiles.

```
SUBSCRIBER_ID=$(curl -k -X POST
https://hss.example.com:8443/api/subscriber \
-H "Content-Type: application/json" \
-d "{
  \"imsi\": \"0010100000000001\",
  \"key_set_id\": \"${KEY_SET_ID}\",
  \"sim_id\": \"${SIM_ID}\",
  \"enabled\": false,
  \"ims_enabled\": false
}" | jq -r '.response.id')
```

Un Suscriptor inactivo es seguro para mantener en la base de datos. El suscriptor no se adjunta, autentica ni registra mientras esté deshabilitado. Si la red consulta a un suscriptor inactivo, el HSS rechaza la solicitud. Consulte [Comportamiento del Suscriptor Inactivo en la Red](#).

Paso 2: Activar (asignar el número y los perfiles, luego habilitar)

Para activar un suscriptor, envíe una solicitud `PATCH`. Agregue el MSISDN, asigne los perfiles y establezca `enabled` en `true`.

```
curl -k -X PATCH
https://hss.example.com:8443/api/subscriber/$SUBSCRIBER_ID \
-H "Content-Type: application/json" \
-d "{
  \"enabled\": true,
  \"ims_enabled\": true,
  \"msisdns\": [\"$MSISDN_ID\"],
  \"epc_profile_id\": \"$EPC_PROFILE_ID\",
  \"ims_profile_id\": \"$IMS_PROFILE_ID\",
  \"roaming_profile_id\": \"$ROAMING_PROFILE_ID\"
}"
```

Una solicitud `PATCH` cambia solo los campos que envía. El IMSI, el Conjunto de Claves y la SIM permanecen como están. Cree el MSISDN y los perfiles primero, o reutilice identificadores existentes. Consulte [Provisionamiento Completo de Suscriptores](#) para saber cómo crear los perfiles.

Paso 3: Desactivar (deshabilitar el suscriptor)

Para desactivar un suscriptor, establezca `enabled` en `false`. El registro del suscriptor y sus datos permanecen en la base de datos.

```
curl -k -X PATCH
https://hss.example.com:8443/api/subscriber/$SUBSCRIBER_ID \
-H "Content-Type: application/json" \
-d '{
  "enabled": false,
  "ims_enabled": false
}'
```

Para eliminar solo la voz IMS y mantener el servicio de datos, establezca `ims_enabled` en `false` y deje `enabled` como `true`.

Comportamiento del Suscriptor Inactivo en la Red

Un suscriptor falla cerrado mientras está inactivo o deshabilitado. El HSS rechaza la solicitud en la interfaz de red. El HSS también escribe un registro de advertencia con el motivo exacto. El motivo es uno de los siguientes:

- El suscriptor está deshabilitado (`enabled` es `false`).
- IMS está deshabilitado para el suscriptor (`ims_enabled` es `false`).
- Un objeto requerido no está asignado aún. Por ejemplo, no hay perfil EPC para un adjunto LTE, o no hay perfil IMS para el registro IMS.

El rechazo utiliza el Código de Resultado Experimental

`DIAMETER_ERROR_USER_UNKNOWN (5001)` en las interfaces S6a y Cx, según [3GPP TS 29.272](#) y [3GPP TS 29.229](#). El registro de advertencia nombra el IMSI y el motivo exacto. El registro le permite distinguir un suscriptor inactivo de un IMSI desconocido.

Provisionamiento Completo de IP Estática

Este ejemplo demuestra el provisionamiento de un suscriptor con una dirección IP estática desde cero.

Escenario: Provisionar un suscriptor de dispositivo IoT que necesita una dirección IPv4 estática en el APN "internet".

```
# Requisitos Previos: jq debe estar instalado (apt-get install jq  
o brew install jq)
```

```
# 1. Crear Conjunto de Claves
```

```
KEY_SET_ID=$(curl -k -X POST  
https://hss.example.com:8443/api/key_set \  
-H "Content-Type: application/json" \  
-d '{  
  "ki": "0123456789ABCDEF0123456789ABCDEF",  
  "opc": "FEDCBA9876543210FEDCBA9876543210",  
  "authentication_algorithm": "milenege",  
  "amf": "8000",  
  "sqn": 0  
}' | jq -r '.response.id')
```

```
# 2. Crear Perfil de QoS APN
```

```
APN_QOS_ID=$(curl -k -X POST  
https://hss.example.com:8443/api/apn/qos_profile \  
-H "Content-Type: application/json" \  
-d '{  
  "name": "IoT Best Effort",  
  "allocation_retention_priority": 8,  
  "apn_ambr_dl_kbps": 10000,  
  "apn_ambr_ul_kbps": 5000,  
  "pre_emption_capability": false,  
  "pre_emption_vulnerability": false,  
  "qci": 9  
}' | jq -r '.response.id')
```

```
# 3. Crear Identificador APN
```

```
APN_ID=$(curl -k -X POST  
https://hss.example.com:8443/api/apn/identifier \  
-H "Content-Type: application/json" \  
-d '{  
  "apn": "internet",  
  "ip_version": "ipv4"  
}' | jq -r '.response.id')
```

```
# 4. Crear Perfil APN
```

```
APN_PROFILE_ID=$(curl -k -X POST  
https://hss.example.com:8443/api/apn/profile \  
-H "Content-Type: application/json" \  
-d "{
```

```
\ "apn_identifier_id\ ": \ "$APN_ID\ ",  
\ "apn_qos_profile_id\ ": \ "$APN_QOS_ID\ ",  
\ "name\ ": \ "IoT Internet APN\  
}" | jq -r '.response.id')
```

5. Crear IP Estática para el APN

```
STATIC_IP_ID=$(curl -k -X POST  
https://hss.example.com:8443/api/epc/static_ip \  
-H "Content-Type: application/json" \  
-d "{  
  \ "apn_profile_id\ ": \ "$APN_PROFILE_ID\  
  \ "ipv4_static_ip\ ": \ "100.64.1.100\  
}" | jq -r '.response.id')
```

6. Crear Perfil EPC

```
EPC_PROFILE_ID=$(curl -k -X POST  
https://hss.example.com:8443/api/epc/profile \  
-H "Content-Type: application/json" \  
-d "{  
  \ "apn_profiles\ ": [$APN_PROFILE_ID],  
  \ "name\ ": \ "IoT Data Plan\  
  \ "network_access_mode\ ": \ "packet_only\  
  \ "tracking_area_update_interval_seconds\ ": 600,  
  \ "ue_ambr_dl_kbps\ ": 10000,  
  \ "ue_ambr_ul_kbps\ ": 5000  
}" | jq -r '.response.id')
```

7. Crear MSISDN (número de teléfono)

```
MSISDN_ID=$(curl -k -X POST  
https://hss.example.com:8443/api/msisdn \  
-H "Content-Type: application/json" \  
-d '{  
  "msisdn": "14155551000"  
}' | jq -r '.response.id')
```

8. Crear Suscriptor con IP Estática

```
SUBSCRIBER_ID=$(curl -k -X POST  
https://hss.example.com:8443/api/subscriber \  
-H "Content-Type: application/json" \  
-d "{  
  \ "imsi\ ": \ "0010019999999999\  
  \ "key_set_id\ ": \ "$KEY_SET_ID\  
  \ "epc_profile_id\ ": \ "$EPC_PROFILE_ID\  
  \ "msisdns\ ": [$MSISDN_ID],
```

```
\ "static_ips\": [$STATIC_IP_ID]
}" | jq -r '.response.id')
```

```
echo "Suscriptor IoT provisionado con éxito!"
echo "  ID del Suscriptor: $SUBSCRIBER_ID"
echo "  IMSI: 001001999999999"
echo "  MSISDN: 14155551000"
echo "  IPv4 Estática: 100.64.1.100 (en APN 'internet')"
```

Qué Crea Esto:

Este flujo de trabajo de provisionamiento crea un suscriptor IoT completo con:

1. **Claves criptográficas** ([Conjunto de Claves](#)) - Para autenticación
2. **Configuración APN** ([Perfil APN](#)) - Punto de acceso "internet"
3. **Asignación de IP Estática** ([IP Estática](#)) - Dirección IPv4 fija 100.64.1.100
4. **Perfil de servicio de datos** ([Perfil EPC](#)) - Límites de ancho de banda optimizados para IoT
5. **Número de teléfono** ([MSISDN](#)) - Para identificación del dispositivo
6. **Registro de suscriptor** ([Suscriptor](#)) - La entidad completa del suscriptor

Resultado:

Cuando este suscriptor se adjunta a la red y se conecta al APN "internet", recibirá la dirección IP estática `100.64.1.100` en lugar de una dirección DHCP dinámica.

Próximos Pasos:

- Agregar APNs adicionales con IPs estáticas: Repetir los pasos 2-5 para cada APN
- Habilitar servicios de voz: Crear y asignar [Perfil IMS](#)
- Configurar roaming: Crear y asignar [Perfil de Roaming](#)
- Vincular SIM física: Crear y asignar [SIM](#)

Ver También:

- [Gestión de IP Estática](#) - Documentación detallada sobre IP estática

- [Provisionamiento Completo de Suscriptores](#) - Provisionamiento básico sin IP estática
 - [Documentación Multi-MSISDN](#) - Asignación de múltiples números de teléfono
-

[← Volver a la Referencia de la API](#)

Referencia de la API de OmniHSS

[← Volver a la Guía de Operaciones](#)

Tabla de Contenidos

- [Descripción General de la API](#)
 - [Gestión de Conjuntos de Claves](#)
 - [Gestión de Suscriptores](#)
 - [Datos del Repositorio Sh \(Datos Transparentes\)](#)
 - [Gestión de MSISDN](#)
 - [Gestión de SIM](#)
 - [Gestión de Conjuntos de Claves](#)
 - [Gestión de Perfiles](#)
 - [Gestión de IPs Estáticas](#)
 - [Gestión de Roaming](#)
 - [Gestión de EIR](#)
 - [Estado y Salud](#)
 - [Manejo de Errores](#)
 - [Ejemplos de Uso de la API](#)
-

Descripción General de la API

URL Base

```
https://[hostname]:8443/api
```

Formato de Solicitud

- **Content-Type:** `application/json`
- **Protocolo:** Solo HTTPS
- **Puerto:** 8443 (configurable)

Importante: Todos los puntos finales de la API esperan cargas útiles JSON "planas" sin objetos envolventes.

Formato Correcto:

```
{  
  "name": "value",  
  "field": "value"  
}
```

Formato Incorrecto (No Usar):

```
{  
  "subscriber": {  
    "name": "value",  
    "field": "value"  
  }  
}
```

Ejemplo:

```
# ✓ Correcto  
curl -X POST https://hss.example.com:8443/api/ims/profile \  
  -H "Content-Type: application/json" \  
  -d '{"name": "default", "ifc_template": "..."}'  
  
# x Incorrecto  
curl -X POST https://hss.example.com:8443/api/ims/profile \  
  -H "Content-Type: application/json" \  
  -d '{"ims_profile": {"name": "default", "ifc_template": "..."}}'
```

Formato de Respuesta

Todas las respuestas son JSON con la siguiente estructura:

Respuesta de Éxito:

```
{
  "status": "success",
  "response": { ... }
}
```

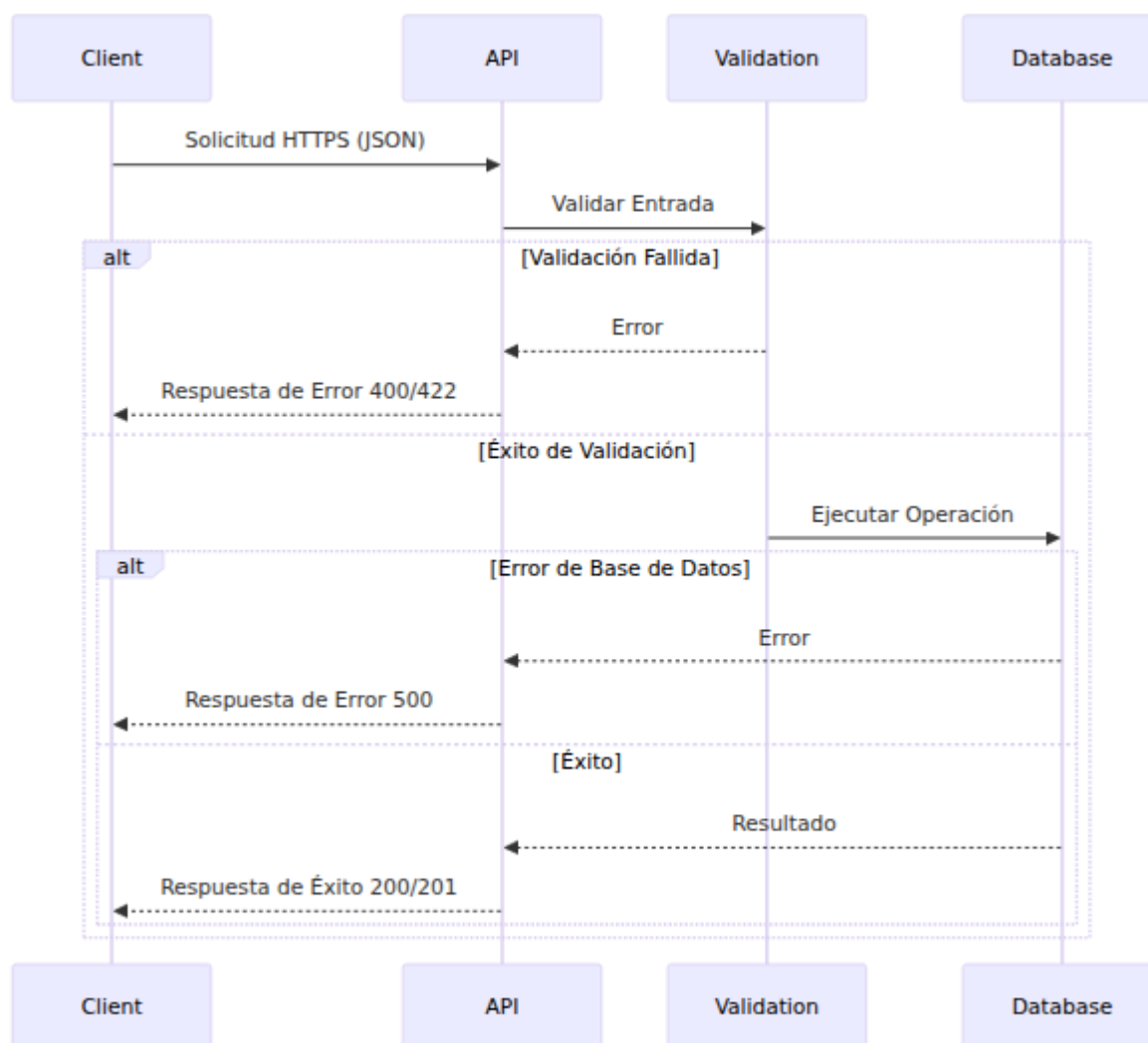
Respuesta de Error:

```
{
  "status": "error",
  "response": {
    "invalid_fields": {
      "field_name": "error message"
    }
  }
}
```

Códigos de Estado HTTP

Código	Significado	Caso de Uso
200	OK	GET, PUT, DELETE exitosos
201	Creado	POST exitoso
400	Solicitud Incorrecta	Datos de entrada inválidos
404	No Encontrado	El recurso no existe
422	Entidad No Procesable	Error de validación
500	Error Interno del Servidor	Error del lado del servidor

Flujo de Solicitud de la API



Gestión de Suscriptores

Listar Suscriptores

Recuperar todos los suscriptores o filtrar por criterios.

Endpoint: GET /api/subscriber

Parámetros de Consulta:

Parámetro	Tipo	Descripción
<code>enabled</code>	booleano	Filtrar por estado habilitado
<code>ims_enabled</code>	booleano	Filtrar por estado habilitado de IMS

Ejemplo de Solicitud:

```
curl -k https://hss.example.com:8443/api/subscriber
```

Ejemplo de Respuesta:

```
{
  "data": [
    {
      "id": "d290flee-6c54-4b01-90e6-d701748f0851",
      "imsi": "001001123456789",
      "enabled": true,
      "ims_enabled": true,
      "sim_id": "3f2504e0-4f89-41d3-9a0c-0305e82c3301",
      "key_set_id": "6ba7b810-9dad-41d1-80b4-00c04fd430c8",
      "epc_profile_id": "e58ed763-928c-4155-bee9-fdbaaadc15f3",
      "ims_profile_id": "7c9e6679-7425-40de-944b-e07fc1f90ae7",
      "roaming_profile_id": "9c858901-8a57-4791-81fe-
4c455b099bc9",
      "custom_attributes": {},
      "inserted_at": "2025-10-15T10:30:00Z",
      "updated_at": "2025-10-15T10:30:00Z"
    }
  ]
}
```

Obtener Suscriptor por ID

Recuperar un suscriptor específico por ID de base de datos.

Endpoint: `GET /api/subscriber/:id`

Parámetros de Ruta:

Parámetro	Tipo	Descripción
id	string (UUID)	ID de base de datos del suscriptor

Ejemplo de Solicitud:

```
curl -k https://hss.example.com:8443/api/subscriber/d290f1ee-6c54-4b01-90e6-d701748f0851
```

Obtener Suscriptor por IMSI

Recuperar un suscriptor por su IMSI.

Endpoint: GET /api/subscriber/imsi/:imsi

Parámetros de Ruta:

Parámetro	Tipo	Descripción	Formato
imsi	string	Identidad Internacional de Suscriptor Móvil	14-15 dígitos

Ejemplo de Solicitud:

```
curl -k https://hss.example.com:8443/api/subscriber/imsi/001001123456789
```

Caso de Uso: Solucionar problemas de un suscriptor específico por su IMSI.

Obtener Suscriptor por MSISDN

Recuperar un suscriptor por su número de teléfono.

Endpoint: GET /api/subscriber/msisdn/:msisdn

Parámetros de Ruta:

Parámetro	Tipo	Descripción	Formato
<code>msisdn</code>	string	Número ISDN de Estación Móvil	1-15 dígitos (E.164)

Ejemplo de Solicitud:

```
curl -k https://hss.example.com:8443/api/subscriber/msisdn/14155551234
```

Caso de Uso: Buscar información del suscriptor cuando solo se tiene su número de teléfono.

Crear Suscriptor

Provisionar un nuevo suscriptor.

Endpoint: `POST /api/subscriber`

Cuerpo de Solicitud:

```
{
  "subscriber": {
    "imsi": "001001123456789",
    "enabled": true,
    "ims_enabled": true,
    "sim_id": "3f2504e0-4f89-41d3-9a0c-0305e82c3301",
    "key_set_id": "6ba7b810-9dad-41d1-80b4-00c04fd430c8",
    "epc_profile_id": "e58ed763-928c-4155-bee9-fdbaaadc15f3",
    "ims_profile_id": "7c9e6679-7425-40de-944b-e07fc1f90ae7",
    "roaming_profile_id": "9c858901-8a57-4791-81fe-4c455b099bc9",
    "custom_attributes": {
      "note": "Suscriptor de prueba"
    }
  }
}
```

Campos Requeridos:

- `imsi` - Debe tener de 14 a 15 dígitos, único
- `key_set_id` - Debe referenciar un [Conjunto de Claves](#) existente
- `epc_profile_id` - Debe referenciar un [Perfil EPC](#) existente

Campos Opcionales:

- `enabled` - Predeterminado: true
- `ims_enabled` - Predeterminado: true
- `sim_id` - Referencia a [SIM](#)
- `ims_profile_id` - Referencia a [Perfil IMS](#) (requerido para servicios IMS)
- `roaming_profile_id` - Referencia a [Perfil de Roaming](#) (requerido para control de roaming)
- `msisdns` - Array de IDs de [MSISDN](#) (números de teléfono)
- `static_ips` - Array de IDs de [IP Estática](#) para asignaciones de APN
- `custom_attributes` - Pares clave-valor personalizados

Ver También:

- [Ejemplo Completo de Provisionamiento de Suscriptores](#) - Flujo de trabajo de extremo a extremo
- [Documentación Multi-MSISDN](#) - Asignación de números de teléfono a suscriptores
- [Gestión de IPs Estáticas](#) - Asignación de IPs estáticas a APNs

Ejemplo de Solicitud:

```
curl -k -X POST https://hss.example.com:8443/api/subscriber \
-H "Content-Type: application/json" \
-d '{
  "subscriber": {
    "imsi": "001001123456789",
    "key_set_id": "6ba7b810-9dad-41d1-80b4-00c04fd430c8",
    "epc_profile_id": "e58ed763-928c-4155-bee9-fdbaaadc15f3"
  }
}'
```

Flujo de Provisionamiento:

Iniciar Provisionamiento

¿Existe el Conjunto de Claves?

No

Error: Conjunto de Claves No Encontrado

Sí

¿Existe el Perfil EPC?

No

Error: Perfil EPC No Encontrado

Sí

¿IMSI Único?

No

Error: El IMSI Ya Existe

Sí

Crear Suscriptor

Estado de Suscriptor Auto-Creado

201 Creado

Actualizar Suscriptor

Modificar un suscriptor existente.

Endpoint: PUT /api/subscriber/:id

Parámetros de Ruta:

Parámetro	Tipo	Descripción
id	string (UUID)	ID de base de datos del suscriptor

Cuerpo de Solicitud:

```
{
  "subscriber": {
    "enabled": false,
    "ims_enabled": false,
    "epc_profile_id": "f47ac10b-58cc-4372-a567-0e02b2c3d479",
    "custom_attributes": {
      "note": "Deshabilitado temporalmente"
    }
  }
}
```

Campos Actualizables:

- enabled - Habilitar/deshabilitar todos los servicios
- ims_enabled - Habilitar/deshabilitar servicios IMS
- sim_id - Cambiar la asignación de SIM
- key_set_id - Cambiar claves criptográficas (¡ten cuidado!)
- epc_profile_id - Cambiar perfil de servicio de datos
- ims_profile_id - Cambiar perfil de servicio de voz
- roaming_profile_id - Cambiar política de roaming
- msisdns - Actualizar números de teléfono asignados al suscriptor
- static_ips - Actualizar asignaciones de IP estática a APNs

- `custom_attributes` - Actualizar datos personalizados

No Actualizable:

- `imsi` - No se puede cambiar el IMSI (eliminar y recrear en su lugar)

Ver También:

- [Gestión de Perfiles](#) - Gestión de perfiles de servicio

Ejemplo de Solicitud:

```
curl -k -X PUT
https://hss.example.com:8443/api/subscriber/d290f1ee-6c54-4b01-
90e6-d701748f0851 \
-H "Content-Type: application/json" \
-d '{
  "subscriber": {
    "enabled": false
  }
}'
```

Casos de Uso:

- Deshabilitar temporalmente al suscriptor: `{"enabled": false}`
- Deshabilitar solo los servicios de voz: `{"ims_enabled": false}`
- Cambiar el perfil de servicio: `{"epc_profile_id": "f47ac10b-58cc-4372-a567-0e02b2c3d479"}` (ver [Perfiles EPC](#))
- Actualizar la política de roaming: `{"roaming_profile_id": "1b671a64-40d5-491e-99b0-da01ff1f3341"}` (ver [Gestión de Roaming](#))

Eliminar Suscriptor

Eliminar un suscriptor del sistema.

Endpoint: `DELETE /api/subscriber/:id`

Parámetros de Ruta:

Parámetro	Tipo	Descripción
id	string (UUID)	ID de base de datos del suscriptor

Ejemplo de Solicitud:

```
curl -k -X DELETE
https://hss.example.com:8443/api/subscriber/d290f1ee-6c54-4b01-
90e6-d701748f0851
```

Advertencia: Esto elimina permanentemente al suscriptor y todos los datos de estado asociados (sesiones PDN, llamadas, etc.). El IMSI puede ser reutilizado después de la eliminación.

Nota: Eliminar un suscriptor NO elimina lo asociado:

- **Conjunto de Claves** - Puede ser reutilizado para otros suscriptores
- **SIM** - Puede ser reasignada a un nuevo suscriptor
- **Perfiles** - Recursos compartidos utilizados por múltiples suscriptores
- **MSISDNs** - Deben ser eliminados por separado si se desea

Cancelar Solicitud de Ubicación (Desconexión Forzada)

Enviar una Solicitud de Cancelación de Ubicación (CLR) para forzar la desconexión de un suscriptor de su MME registrado actualmente.

Endpoint: POST /api/subscriber/cancel_location

Cuerpo de Solicitud:

```
{
  "imsi": "001001123456789"
}
```

Parámetros:

Parámetro	Tipo	Requerido	Descripción
imsi	string	Sí	IMSI del suscriptor a desconectar (14-15 dígitos)

Ejemplo de Solicitud:

```
curl -k -X POST
https://hss.example.com:8443/api/subscriber/cancel_location \
-H "Content-Type: application/json" \
-d '{"imsi": "001001123456789"}'
```

Respuesta de Éxito (200 OK):

```
{
  "data": {
    "message": "Solicitud de Cancelación de Ubicación enviada con éxito",
    "imsi": "001001123456789",
    "destination_host": "mme01.operator.com",
    "destination_realm": "epc.operator.com"
  }
}
```

Respuesta de Error (404 No Encontrado):

```
{
  "error": "Suscriptor no encontrado o no registrado actualmente en ningún MME"
}
```

Comportamiento:

- Envía S6a CLR al MME donde el suscriptor está registrado actualmente (subscriber_state.last_seen_mme)
- Utiliza Cancellation-Type: subscription_withdrawal (forza la desconexión completa)

- Establece CLR-Flags: {s6a_indicator: 1, reattach_required: 1} (el UE debe re-autenticarse)
- Devuelve 404 si el suscriptor nunca se ha registrado o last_seen_mme es nulo
- **Afecta a todos los MSISDNs** asociados con el IMSI (mismo dispositivo físico/SIM)

Casos de Uso:

- **Prevención de Fraude:** Desconectar inmediatamente a un suscriptor sospechoso
- **Terminación de Suscripción:** Forzar cierre de sesión cuando la cuenta está deshabilitada
- **Solución de Problemas:** Limpiar el registro de MME obsoleto para depuración
- **Migración:** Forzar re-autenticación para aplicar nuevas configuraciones de perfil
- **Seguridad:** Desconectar inmediatamente a un suscriptor comprometido

Consideraciones Multi-IMSI:

Al usar CLR con escenarios multi-MSISDN:

1. Múltiples MSISDNs, Un Solo IMSI:

```
// El suscriptor tiene IMSI 001001123456789 con MSISDNs  
["+1234567890", "+9876543210"]  
POST /api/subscriber/cancel_location  
{  
  "imsi": "001001123456789"  
}  
  
// Resultado: Se envió un CLR, ambos MSISDNs afectados (mismo dispositivo)
```

2. Diferentes IMSIs (Dispositivos Diferentes):

```
// Dos suscriptores con el mismo MSISDN pero diferentes IMSIs  
(escenario de portabilidad de número)  
// Suscriptor A: IMSI 001001111111111, MSISDN "+1234567890"  
// Suscriptor B: IMSI 001001222222222, MSISDN "+1234567890"
```

```
POST /api/subscriber/cancel_location  
{  
  "imsi": "001001111111111"  
}
```

```
// Resultado: Solo se desconecta el Suscriptor A, el Suscriptor  
B no se ve afectado
```

Notas Importantes:

- **Basado en IMSI:** CLR siempre se envía por IMSI, no por MSISDN
- **Asíncrono:** CLR se envía de forma asíncrona; la respuesta de éxito significa que se envió el CLR, no que el MME lo procesó
- **Sin validación del estado del MME:** CLR se envía incluso si el MME es inalcanzable (comportamiento estándar de HSS)
- **Idempotente:** Seguro llamar múltiples veces para el mismo IMSI

Documentación Relacionada:

- [Flujo de Protocolo de Solicitud de Cancelación de Ubicación](#)
- [Escenarios Multi-IMSI](#)
- [Arquitectura de la Interfaz S6a](#)

Datos del Repositorio Sh (Datos Transparentes)

Provisionamiento de acceso a los documentos Sh transparentes de un suscriptor (MMTEL-Services, IMS-ODB-Information y otros). Estos son los mismos documentos opacos que un Servidor de Aplicaciones lee y escribe a través de la interfaz Diameter Sh. El acceso es a través de `GET/PUT/DELETE /api/subscriber/repository_data/:imsi`.

Ver [Datos del Repositorio Sh \(Datos Transparentes\)](#) para el modelo de datos, flujos de mensajes, reglas de concurrencia de SequenceNumber y la referencia completa de la API REST.

Gestión de MSISDN

Los MSISDN (números de teléfono) pueden ser asignados a suscriptores para habilitar servicios de voz. Ver [Documentación Multi-MSISDN](#) para detalles sobre la asignación de múltiples números a un solo suscriptor.

Listar MSISDN

Recuperar todos los números de teléfono.

Endpoint: GET /api/msisdn

Ejemplo de Solicitud:

```
curl -k https://hss.example.com:8443/api/msisdn
```

Obtener MSISDN

Recuperar un número de teléfono específico.

Endpoint: GET /api/msisdn/:id

Ejemplo de Solicitud:

```
curl -k https://hss.example.com:8443/api/msisdn/16fd2706-8baf-433b-82eb-8c7fada847da
```

Crear MSISDN

Crear un nuevo número de teléfono.

Endpoint: POST /api/msisdn

Cuerpo de Solicitud:

```
{
  "msisdn": {
    "msisdn": "14155551234"
  }
}
```

Validación:

- Debe tener de 1 a 15 dígitos
- Debe ser único
- Debe seguir el formato E.164 (formato internacional sin el signo +)

Ejemplo de Solicitud:

```
curl -k -X POST https://hss.example.com:8443/api/msisdn \
-H "Content-Type: application/json" \
-d '{
  "msisdn": {
    "msisdn": "14155551234"
  }
}'
```

Asignar MSISDN a Suscriptor

Para asignar un número de teléfono a un suscriptor, necesitas crear un registro de unión. Esto se hace típicamente a través del endpoint de actualización de suscriptor o mediante manipulación directa de la base de datos.

Patrón Multi-MSISDN:

Iniciar Provisionamiento

OmniCore
5GC ▼

OmniCall ▼

OmniRAN ▼

OmniCharge ▼

Platform ▼

🌐 Español ▼

¿Existe el Conjunto de Claves?

No

Error: Conjunto de Claves No Encontrado

Sí

¿Existe el Perfil EPC?

No

Error: Perfil EPC No Encontrado

Sí

¿IMSI Único?

No

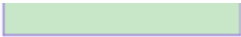
Error: El IMSI Ya Existe

Sí

Crear Suscriptor

Estado de Suscriptor Auto-Creado

201 Creado



Ver [Características Multi-MSISDN y Multi-IMSI](#) para un uso detallado.

Eliminar MSISDN

Eliminar un número de teléfono.

Endpoint: DELETE /api/msisdn/:id

Ejemplo de Solicitud:

```
curl -k -X DELETE
https://hss.example.com:8443/api/msisdn/16fd2706-8baf-433b-82eb-
8c7fada847da
```

Gestión de SIM

Los registros de tarjetas SIM almacenan información física de la tarjeta SIM, incluyendo ICCID, detalles del proveedor, códigos PIN/PUK y claves OTA. Los registros de SIM pueden opcionalmente estar vinculados a [suscriptores](#).

Ver También:

- [Documentación Multi-IMSI](#) - Múltiples suscriptores en una sola SIM física

Listar SIMs

Recuperar todas las tarjetas SIM.

Endpoint: GET /api/sim

Ejemplo de Solicitud:

```
curl -k https://hss.example.com:8443/api/sim
```

Obtener SIM

Recuperar una tarjeta SIM específica.

Endpoint: GET /api/sim/:id

Ejemplo de Solicitud:

```
curl -k https://hss.example.com:8443/api/sim/3f2504e0-4f89-41d3-9a0c-0305e82c3301
```

Crear SIM

Crear un nuevo registro de tarjeta SIM.

Endpoint: POST /api/sim

Cuerpo de Solicitud:

```
{
  "sim": {
    "iccid": "8991101200003204510",
    "sim_vendor": "Gemalto",
    "batch_name": "2025-Q1-Batch-01",
    "is_esim": false,
    "pin1": "1234",
    "pin2": "5678",
    "puk1": "12345678",
    "puk2": "87654321",
    "adm1": "admin-code-1",
    "kic": "0123456789ABCDEF0123456789ABCDEF",
    "kid": "FEDCBA9876543210FEDCBA9876543210"
  }
}
```

Campos Requeridos:

- iccid - 19-20 dígitos, único

Campos Opcionales pero Importantes:

- `sim_vendor` - Nombre del fabricante
- `batch_name` - Para seguimiento
- `is_esim` - Bandera booleana para eSIM
- `pin1`, `pin2` - Códigos PIN del usuario final
- `puk1`, `puk2` - Códigos de desbloqueo de PIN
- `adm1-adm10` - Códigos administrativos
- `kic`, `kid` - Claves de seguridad OTA (cadena hexadecimal)

Ejemplo de Solicitud:

```
curl -k -X POST https://hss.example.com:8443/api/sim \
-H "Content-Type: application/json" \
-d '{
  "sim": {
    "iccid": "8991101200003204510",
    "sim_vendor": "Gemalto"
  }
}'
```

Actualizar SIM

Modificar los datos de la tarjeta SIM.

Endpoint: `PUT /api/sim/:id`

Ejemplo de Solicitud:

```
curl -k -X PUT https://hss.example.com:8443/api/sim/3f2504e0-4f89-
41d3-9a0c-0305e82c3301 \
-H "Content-Type: application/json" \
-d '{
  "sim": {
    "batch_name": "Nombre de Lote Actualizado"
  }
}'
```

Eliminar SIM

Eliminar un registro de tarjeta SIM.

Advertencia: Asegúrate de que ningún suscriptor haga referencia a esta SIM antes de eliminarla.

Gestión de Conjuntos de Claves

Los conjuntos de claves contienen el material criptográfico (Ki, OPC/OP, AMF, SQN) utilizado para la autenticación de suscriptores a través del algoritmo Milenage. Cada **suscriptor** debe referenciar un conjunto de claves.

Ver También:

- **Flujos de Protocolo** - Procedimientos de autenticación utilizando conjuntos de claves

Listar Conjuntos de Claves

Recuperar todos los conjuntos de claves criptográficas.

Endpoint: GET /api/key_set

Ejemplo de Solicitud:

```
curl -k https://hss.example.com:8443/api/key_set
```

Obtener Conjunto de Claves

Recuperar un conjunto de claves específico.

Endpoint: GET /api/key_set/:id

Ejemplo de Solicitud:

```
curl -k https://hss.example.com:8443/api/key_set/6ba7b810-9dad-41d1-80b4-00c04fd430c8
```

Ejemplo de Respuesta:

```
{
  "data": {
    "id": "6ba7b810-9dad-41d1-80b4-00c04fd430c8",
    "ki": "0123456789ABCDEF0123456789ABCDEF",
    "opc": "FEDCBA9876543210FEDCBA9876543210",
    "op": null,
    "amf": "8000",
    "sqn": 0,
    "authentication_algorithm": "milenege",
    "ota_counter": 0
  }
}
```

Crear Conjunto de Claves

Crear un nuevo conjunto de claves criptográficas.

Endpoint: POST /api/key_set

Cuerpo de Solicitud:

```
{
  "key_set": {
    "ki": "0123456789ABCDEF0123456789ABCDEF",
    "opc": "FEDCBA9876543210FEDCBA9876543210",
    "amf": "8000",
    "sqn": 0,
    "authentication_algorithm": "milenege"
  }
}
```

Campos Requeridos:

- `ki` - Clave de 128 bits (32 caracteres hexadecimales)
- Ya sea `opc` O `op` (el OPC puede ser derivado del OP)
- `authentication_algorithm` - Actualmente solo "milenage"

Campos Opcionales:

- `amf` - Predeterminado: "8000"
- `sqn` - Predeterminado: 0
- `ota_counter` - Predeterminado: 0

Formato de Clave:

- Todas las claves son cadenas hexadecimales
- Ki, OPC, OP: 32 caracteres hexadecimales (128 bits)
- AMF: 4 caracteres hexadecimales (16 bits)

Ejemplo de Solicitud:

```
curl -k -X POST https://hss.example.com:8443/api/key_set \
-H "Content-Type: application/json" \
-d '{
  "key_set": {
    "ki": "0123456789ABCDEF0123456789ABCDEF",
    "opc": "FEDCBA9876543210FEDCBA9876543210",
    "authentication_algorithm": "milenage"
  }
}'
```

Advertencia de Seguridad: Los conjuntos de claves contienen material criptográfico altamente sensible. Proteja el acceso a la API en consecuencia.

Actualizar Conjunto de Claves

Modifique un conjunto de claves existente.

Endpoint: `PUT /api/key_set/:id`

Advertencia: Cambiar claves para un **suscriptor** activo causará fallos de autenticación. Solo actualice claves durante ventanas de mantenimiento o para nuevos suscriptores.

Impacto: Las actualizaciones afectan a todos los suscriptores que utilizan este conjunto de claves de inmediato. Los suscriptores activos fallarán en la autenticación en el próximo intento de conexión.

Eliminar Conjunto de Claves

Eliminar un conjunto de claves.

Endpoint: DELETE /api/key_set/:id

Advertencia: Asegúrese de que ningún **suscriptor** haga referencia a este conjunto de claves antes de eliminarlo. Consulte primero a los suscriptores para verificar referencias.

Gestión de Perfiles

Perfiles EPC

Los perfiles EPC (Evolved Packet Core) definen los parámetros del servicio de datos para los suscriptores. Estos perfiles se hacen referencia al crear **suscriptores**.

Listar Perfiles EPC

Endpoint: GET /api/epc/profile

Obtener Perfil EPC

Endpoint: GET /api/epc/profile/:id

Crear Perfil EPC

Endpoint: POST /api/epc/profile

Cuerpo de la Solicitud:

```
{
  "apn_profiles": [],
  "name": "Plan de Datos Estándar",
  "network_access_mode": "packet_only",
  "tracking_area_update_interval_seconds": 600,
  "ue_ambr_dl_kbps": 100000,
  "ue_ambr_ul_kbps": 50000
}
```

Campos:

Campo	Descripción	Unidades	Valores
name	Nombre del perfil	Texto	Id de perfil
ue_ambr_dl_kbps	Límite de ancho de banda de descarga	Kbps	100000
ue_ambr_ul_kbps	Límite de ancho de banda de carga	Kbps	50000
network_access_mode	Tipo de acceso	Cadena	"packet_only" o "ip_only"
tracking_area_update_interval_seconds	Temporizador TAU	Segundos	600
apn_profiles	Lista de IDs de perfil APN	Array	[] o [1, 2, 3]

Ejemplo de Solicitud:


```
curl -k -X POST https://hss.example.com:8443/api/epc/profile \
-H "Content-Type: application/json" \
-d '{
  "apn_profiles": [],
  "name": "Premium 100Mbps",
  "network_access_mode": "packet_only",
  "tracking_area_update_interval_seconds": 600,
  "ue_ambr_dl_kbps": 100000,
  "ue_ambr_ul_kbps": 50000
}'
```

Véase También:

- [Documentación de Perfiles](#) - Guía de configuración detallada de perfiles
- [Provisionamiento Completo de Suscriptores](#) - Uso de perfiles EPC en el aprovisionamiento

Actualizar Perfil EPC

Endpoint: PUT /api/epc/profile/:id

Nota: Los cambios en los perfiles EPC afectan a todos los [suscriptores](#) que utilizan este perfil. Las sesiones activas pueden necesitar ser restablecidas.

Eliminar Perfil EPC

Endpoint: DELETE /api/epc/profile/:id

Advertencia: Asegúrese de que ningún [suscriptor](#) haga referencia a este perfil antes de eliminarlo.

Perfiles IMS

Los perfiles IMS (IP Multimedia Subsystem) definen los parámetros del servicio de voz y los Criterios de Filtro Inicial (IFC) para los suscriptores. Estos perfiles se hacen referencia al crear [suscriptores](#) con servicios IMS habilitados.

Listar Perfiles IMS

Endpoint: GET /api/ims/profile

Crear Perfil IMS

Endpoint: POST /api/ims/profile

Cuerpo de la Solicitud:

```
{
  "name": "VoLTE Estándar",
  "ifc_template": "<IMS-XML-Template-Here>"
}
```

Campos Requeridos:

- `name` - Nombre del perfil (debe ser único)
- `ifc_template` - Plantilla XML IFC (Criterios de Filtro Inicial) con variables de plantilla Liquid

Variables de Plantilla IFC:

La plantilla IFC admite las siguientes variables de plantilla Liquid que se sustituyen dinámicamente:

Variable	Descripción	Valor de Ejemplo
<code>{{ imsi }}</code>	IMSI del suscriptor	001001123456789
<code>{{ msisdns }}</code>	Array de MSISDNs (para bucles)	<code>["14155551234", "14155555678"]</code>
<code>{{ mcc }}</code>	Código de País Móvil	001
<code>{{ mnc }}</code>	Código de Red Móvil	001

Cómo Funciona el Renderizado de Plantillas:

La plantilla IFC se almacena como una **plantilla Liquid** (similar a Jinja2) y se renderiza **dinámicamente** durante las operaciones IMS:

1. **Almacenamiento:** Cuando crea un perfil IMS, la plantilla se almacena tal cual con variables como `{{ imsi }}` y `{% for msisdn in msisdns %}`
2. **Validación:** La API valida la plantilla renderizándola con datos de prueba para asegurar una sintaxis XML válida
3. **Renderizado en Tiempo de Ejecución:** Cuando un suscriptor realiza el registro IMS (MAA/SAA), el HSS:
 - Recupera el perfil IMS del suscriptor
 - Renderiza la plantilla con los datos reales del suscriptor:
 - `{{ imsi }}` → IMSI del suscriptor
 - `{{ msisdns }}` → Números de teléfono del suscriptor
 - `{{ mcc }}` → Código de País Móvil configurado
 - `{{ mnc }}` → Código de Red Móvil configurado
 - Devuelve el XML renderizado al S-CSCF a través de Cx/Diameter

Sintaxis de Plantilla:

```
<!-- Sustitución de variable simple -->
{{ imsi }}

<!-- Bucles para arrays -->
{% for msisdn in msisdns %}
  <MSISDN>{{ msisdn }}</MSISDN>
{% endfor %}

<!-- Combinando variables -->
{{ imsi }}@ims.mnc{{ mnc }}.mcc{{ mcc }}.3gppnetwork.org
```

Ejemplo de Plantilla IFC:

```

<?xml version="1.0" encoding="UTF-8"?>
<IMSSubscription>
<PrivateID>{{ imsi }}@ims.mnc{{ mnc }}.mcc{{ mcc
}}.3gppnetwork.org</PrivateID>
<ServiceProfile>
{% for msisdn in msisdns %}
<PublicIdentity>
<Identity>sip:{{ msisdn }}@ims.mnc{{ mnc }}.mcc{{ mcc
}}.3gppnetwork.org</Identity>
<Extension>
<IdentityType>0</IdentityType>
</Extension>
</PublicIdentity>
<PublicIdentity>
<Identity>tel:{{ msisdn }}</Identity>
<Extension>
<IdentityType>0</IdentityType>
</Extension>
</PublicIdentity>
{% endfor %}
<InitialFilterCriteria>
<Priority>10</Priority>
<TriggerPoint>
<ConditionTypeCNF>0</ConditionTypeCNF>
<SPT>
<ConditionNegated>0</ConditionNegated>
<Group>0</Group>
<Method>REGISTER</Method>
</SPT>
</TriggerPoint>
<ApplicationServer>
<ServerName>sip:as.ims.mnc{{ mnc }}.mcc{{ mcc
}}.3gppnetwork.org</ServerName>
<DefaultHandling>0</DefaultHandling>
</ApplicationServer>
</InitialFilterCriteria>
</ServiceProfile>
</IMSSubscription>

```

Ejemplo de Solicitud (curl):

```
curl -k -X POST https://hss.example.com:8443/api/ims/profile \
-H "Content-Type: application/json" \
-d '{
  "name": "default",
  "ifc_template": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>
<IMSSubscription><ServiceProfile>...</ServiceProfile>
</IMSSubscription>"
}'
```

Ejemplo de Solicitud (Python):

```
import requests

response = requests.post(
    "https://hss.example.com:8443/api/ims/profile",
    json={
        "name": "default",
        "ifc_template": ifc_template_string
    },
    verify=False # Para certificados autofirmados
)
```

Respuesta de Éxito (201 Creado):

```
{
  "status": "success",
  "response": {
    "id": "0f8fad5b-d9cb-469f-a165-70867728950e",
    "name": "default",
    "ifc_template": "<?xml version=\"1.0\" encoding=\"UTF-8\"?
>..."
  }
}
```

Validación:

- La API valida que la plantilla IFC sea un XML válido
- Las variables de plantilla se renderizan con datos de prueba para verificar la sintaxis

- El campo `name` debe ser único y no vacío

Véase También:

- [Documentación de Perfiles](#) - Detalles y ejemplos de la plantilla IFC
- [Flujos de Protocolo](#) - Registro IMS y flujos de llamadas
- [Plantilla IFC Predeterminada](#) - Implementación de referencia

Perfiles APN

Los perfiles APN (Access Point Name) constan de tres componentes que trabajan juntos:

1. **Identificador APN** - Define el nombre del APN y la versión IP
2. **Perfil QoS APN** - Define los parámetros de Calidad de Servicio
3. **Perfil APN** - Combina el identificador y QoS, vinculado a [Perfiles EPC](#)

Consulte la [Documentación PCRF](#) para la configuración detallada de políticas, gestión de QoS y re-autenticación automática. Consulte también la [Documentación de Perfiles](#) para ejemplos de configuración de APN.

Listar Identificadores APN

Endpoint: `GET /api/apn/identifier`

Crear Identificador APN

Endpoint: `POST /api/apn/identifier`

Cuerpo de la Solicitud:

```
{
  "apn": "internet",
  "ip_version": "ipv4v6"
}
```

Valores de Versión IP:

- `ipv4` - Solo IPv4

- "ipv6" - Solo IPv6
- "ipv4v6" - IPv4v6 (doble pila)
- "ipv4_or_ipv6" - IPv4 o IPv6 (elección de red)

Listar Perfiles QoS APN

Endpoint: GET /api/apn/qos_profile

Crear Perfil QoS APN

Endpoint: POST /api/apn/qos_profile

Cuerpo de la Solicitud:

```
{
  "name": "Internet de Mejor Esfuerzo",
  "allocation_retention_priority": 8,
  "apn_ambr_dl_kbps": 50000,
  "apn_ambr_ul_kbps": 25000,
  "pre_emption_capability": false,
  "pre_emption_vulnerability": true,
  "qci": 9
}
```

Listar Perfiles APN

Endpoint: GET /api/apn/profile

Crear Perfil APN

Endpoint: POST /api/apn/profile

Cuerpo de la Solicitud:

```
{
  "apn_identifier_id": "4fa85f64-5717-4562-b3fc-2c963f66afa6",
  "apn_qos_profile_id": "8d8ac610-566d-4ef0-9c22-186b2a5ed793",
  "name": "Perfil APN de Internet"
}
```

Campos Requeridos:

- `apn_identifier_id` - Debe hacer referencia a un **Identificador APN existente**
- `apn_qos_profile_id` - Debe hacer referencia a un **Perfil QoS APN existente**

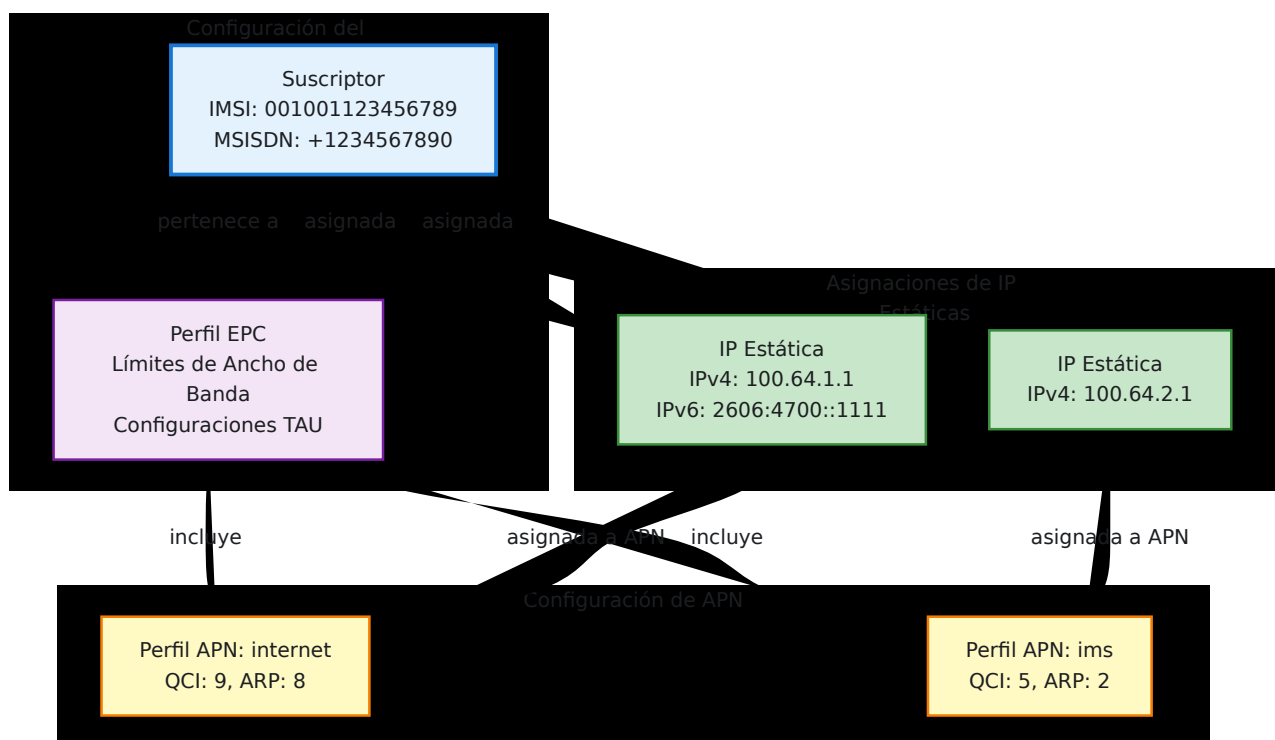
Véase También:

- **Provisionamiento Completo de Suscriptores** - Ejemplo completo que incluye configuración de APN
- **Perfiles EPC** - Los perfiles APN están vinculados a perfiles EPC

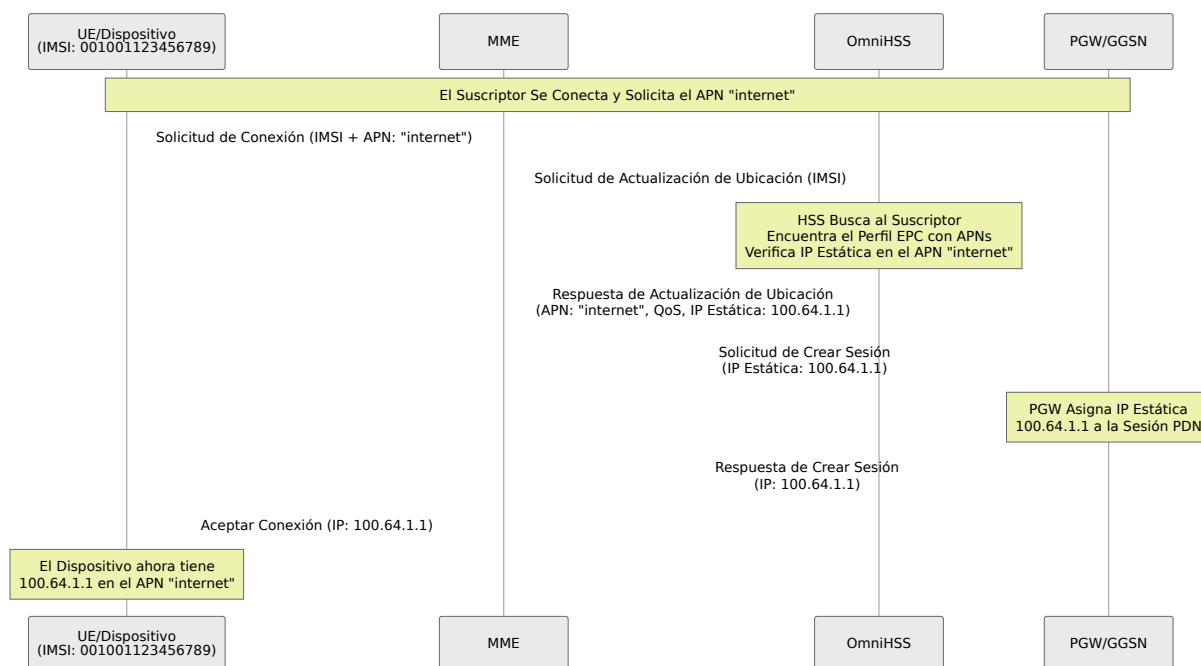
Gestión de IP Estáticas

Las direcciones IP estáticas pueden asignarse a APNs específicos para suscriptores individuales. Esto permite que los suscriptores reciban una dirección IPv4 y/o IPv6 predeterminada al conectarse a un APN en particular, en lugar de recibir una dirección dinámica de un grupo DHCP.

Arquitectura:

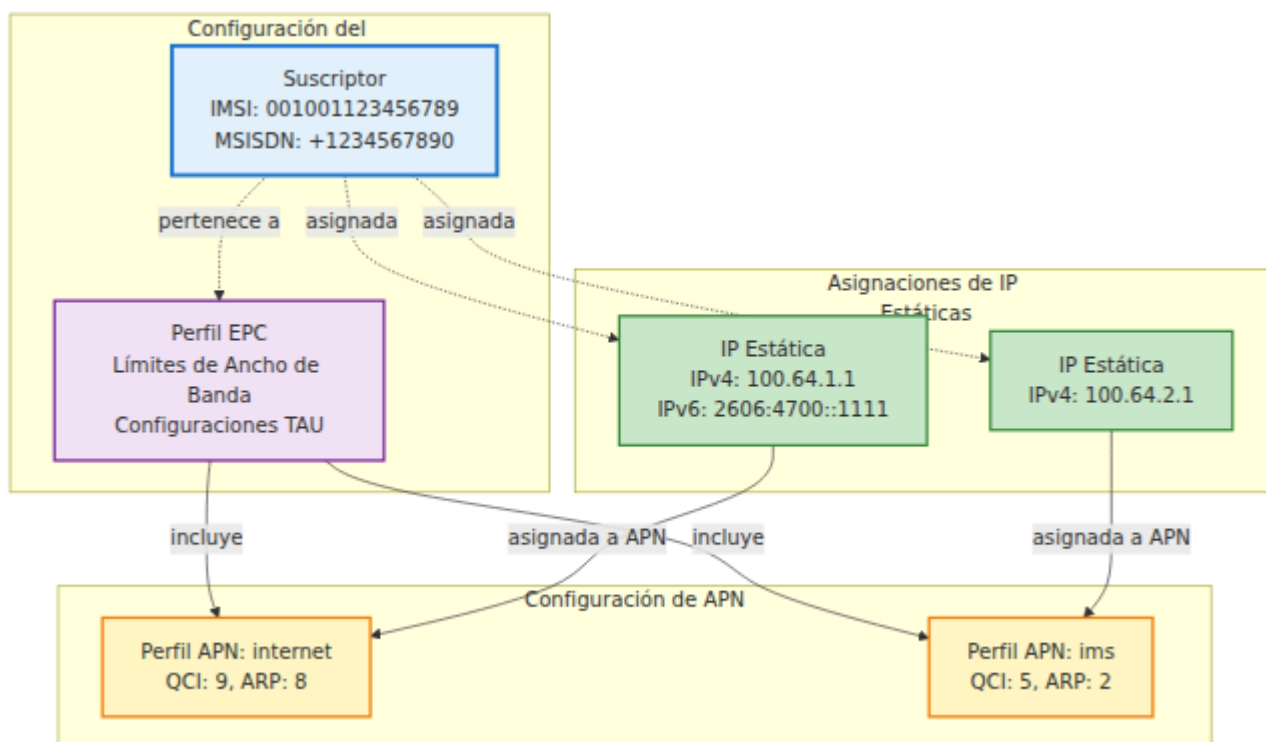


Flujo de Datos Cuando el Suscriptor se Conecta:



Respuesta de Actualización de Ubicación - Mapeo de Datos de Configuración de APN:

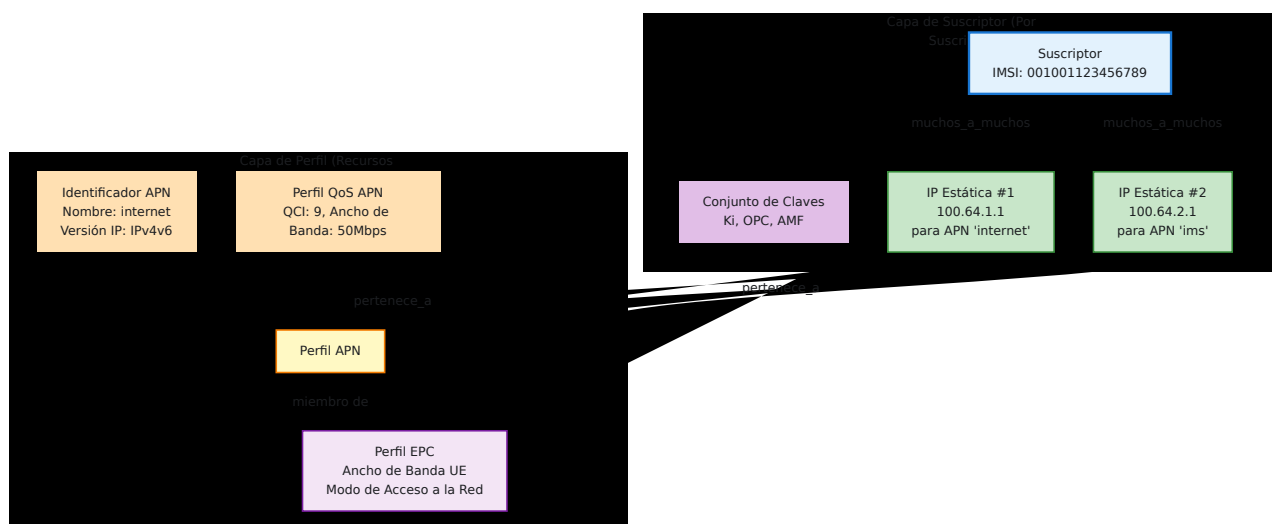
Este diagrama muestra exactamente de dónde proviene cada campo en el AVP de Configuración de APN de la Respuesta de Actualización de Ubicación S6a en la base de datos:



Observaciones Clave:

1. **Identificador de Contexto:** Índice secuencial (0, 1, 2...) para cada APN en el perfil
2. **Selección de Servicio:** Proviene directamente de `apn_identifier.apn` (por ejemplo, "internet", "ims")
3. **Tipo de PDN:** Codificado a partir de `apn_identifier.ip_version` (ipv4=0, ipv6=1, ipv4v6=2, ipv4_or_ipv6=3)
4. **Parámetros QoS:** Todos provienen de la tabla `apn_qos_profile`
5. **Ancho de Banda AMBR:** Los valores se multiplican por 1000 (conversión de kbps a bps)
6. **Dirección-IP-Servida:** Solo se incluye si existe una IP estática para esta combinación de suscriptor+APN
 - Proceso de búsqueda: `subscriber.static_ips` → filtrar por `apn_profile_id` → extraer IPs
 - Compatibilidad de versión IP verificada contra `apn_identifier.ip_version`
7. **VPLMN-Dirección-Dinámica-Permitida:** Codificado a 0 (no permitido) - obliga al uso de IP estática si se proporciona

Jerarquía de Relaciones:



Conceptos Clave:

- **Asignación por APN:** Cada IP Estática está vinculada a un **Perfil APN específico**
- **Una IP por APN por Suscriptor:** Un suscriptor solo puede tener una asignación de IP estática por APN

- **Soporte IPv4 e IPv6:** Las IP estáticas pueden ser solo IPv4, solo IPv6 o de doble pila
- **Unicidad Global de IP:** Cada dirección IP debe ser globalmente única en **todos** los registros de IP estáticas en el sistema
 - La misma dirección IPv4 o IPv6 no puede asignarse a múltiples suscriptores (incluso en diferentes APNs)
 - Esto previene conflictos de enrutamiento y ambigüedad de direcciones IP
 - Se aplica mediante índices únicos en la base de datos en los campos `ipv4_static_ip` y `ipv6_static_ip`
- **Relación Muchos a Muchos:** Los suscriptores y las IP estáticas están vinculados a través de una tabla de unión

Casos de Uso:

- Direcciones IP fijas para dispositivos IoT
- Alojamiento de servidores en dispositivos móviles (requiere IP estática para conexiones entrantes)
- Aplicaciones heredadas que requieren direcciones IP específicas
- Enrutamiento de políticas de red basado en IP de origen
- Cumplimiento normativo que requiere seguimiento de direcciones IP

Listar IPs Estáticas

Recuperar todas las asignaciones de IP estáticas.

Endpoint: `GET /api/epc/static_ip`

Ejemplo de Solicitud:

```
curl -k https://hss.example.com:8443/api/epc/static_ip
```

Ejemplo de Respuesta:

```
{
  "data": [
    {
      "id": "c56a4180-65aa-42ec-a945-5fd21dec0538",
      "apn_profile_id": "a1b2c3d4-e5f6-4a3b-8c2d-1e0f9a8b7c6d",
      "ipv4_static_ip": "100.64.1.1",
      "ipv6_static_ip": "2606:4700:4700::1111",
      "apn_profile": {
        "id": "a1b2c3d4-e5f6-4a3b-8c2d-1e0f9a8b7c6d",
        "name": "Perfil APN de Internet",
        "apn_identifier": {
          "apn": "internet",
          "ip_version": "ipv4v6"
        }
      },
      "inserted_at": "2025-11-15T10:30:00Z",
      "updated_at": "2025-11-15T10:30:00Z"
    }
  ]
}
```

Obtener IP Estática

Recuperar una asignación de IP estática específica.

Endpoint: GET /api/epc/static_ip/:id

Parámetros de Ruta:

Parámetro	Tipo	Descripción
id	string (UUID)	ID de base de datos de IP estática

Ejemplo de Solicitud:

```
curl -k https://hss.example.com:8443/api/epc/static_ip/c56a4180-65aa-42ec-a945-5fd21dec0538
```

Crear IP Estática

Crear una nueva asignación de IP estática para un APN.

Endpoint: POST /api/epc/static_ip

Cuerpo de la Solicitud:

```
{
  "static_ip": {
    "apn_profile_id": "a1b2c3d4-e5f6-4a3b-8c2d-1e0f9a8b7c6d",
    "ipv4_static_ip": "100.64.1.1",
    "ipv6_static_ip": "2606:4700:4700::1111"
  }
}
```

Campos Requeridos:

- `apn_profile_id` - Debe hacer referencia a un **Perfil APN** existente
- Al menos uno de `ipv4_static_ip` O `ipv6_static_ip` debe ser especificado

Campos Opcionales:

- `ipv4_static_ip` - Dirección IPv4 (notación decimal con puntos)
- `ipv6_static_ip` - Dirección IPv6 (notación estándar)

Validación del Formato IP:

- IPv4: Formato estándar decimal con puntos (por ejemplo, `100.64.1.1`)
- IPv6: Formato estándar hexadecimal separado por dos puntos (por ejemplo, `2606:4700:4700::1111`)
- Tanto las direcciones IPv4 como IPv6 deben ser **globalmente únicas en todos los registros de IP estáticas**
 - Esto previene conflictos de direcciones IP en la red
 - La misma IP no puede ser asignada a múltiples suscriptores, incluso en diferentes APNs
 - Esta es una restricción a nivel de base de datos impuesta por índices únicos

Opciones de Configuración:

Configuración	IPv4	IPv6	Ejemplo
Solo IPv4	✓	-	<code>{"ipv4_static_ip": "100.64.1.1"}</code>
Solo IPv6	-	✓	<code>{"ipv6_static_ip": "2606:4700:4700::1111"}</code>
Dual Stack	✓	✓	Ambos campos especificados

Ejemplos de Solicitudes:

IP Estática Solo IPv4:

```
curl -k -X POST https://hss.example.com:8443/api/epc/static_ip \
-H "Content-Type: application/json" \
-d '{
  "static_ip": {
    "apn_profile_id": "a1b2c3d4-e5f6-4a3b-8c2d-1e0f9a8b7c6d",
    "ipv4_static_ip": "100.64.1.1"
  }
}'
```

IP Estática Solo IPv6:

```
curl -k -X POST https://hss.example.com:8443/api/epc/static_ip \
-H "Content-Type: application/json" \
-d '{
  "static_ip": {
    "apn_profile_id": "b2c3d4e5-f6a7-4b1c-9d2e-3f4a5b6c7d8e",
    "ipv6_static_ip": "2606:4700:4700::1111"
  }
}'
```

IP Estática Dual Stack:

```
curl -k -X POST https://hss.example.com:8443/api/epc/static_ip \
-H "Content-Type: application/json" \
-d '{
  "static_ip": {
    "apn_profile_id": "a1b2c3d4-e5f6-4a3b-8c2d-1e0f9a8b7c6d",
    "ipv4_static_ip": "100.64.1.1",
    "ipv6_static_ip": "2606:4700:4700::1111"
  }
}'
```

Respuesta de Éxito (201 Creado):

```
{
  "data": {
    "id": "c56a4180-65aa-42ec-a945-5fd21dec0538",
    "apn_profile_id": "a1b2c3d4-e5f6-4a3b-8c2d-1e0f9a8b7c6d",
    "ipv4_static_ip": "100.64.1.1",
    "ipv6_static_ip": "2606:4700:4700::1111",
    "inserted_at": "2025-11-15T10:30:00Z",
    "updated_at": "2025-11-15T10:30:00Z"
  }
}
```

Ver También:

- [Asignar IP Estática a Suscriptor](#) - Cómo vincular esto a un suscriptor
- [Perfiles APN](#) - Gestión de configuraciones APN

Actualizar IP Estática

Modificar una asignación de IP estática existente.

Endpoint: PUT /api/epc/static_ip/:id

Parámetros de Ruta:

Parámetro	Tipo	Descripción
id	string (UUID)	ID de base de datos de IP estática

Cuerpo de Solicitud:

```
{
  "static_ip": {
    "ipv4_static_ip": "100.64.1.2",
    "ipv6_static_ip": "2606:4700:4700::1112"
  }
}
```

Campos Actualizables:

- ipv4_static_ip - Cambiar dirección IPv4
- ipv6_static_ip - Cambiar dirección IPv6
- apn_profile_id - Cambiar asignación APN

No Actualizable:

- id - Clave primaria (solo lectura)

Advertencia: Cambiar la dirección IP para un suscriptor activo afectará su próxima conexión PDN. Las sesiones PDN activas continuarán utilizando la IP antigua hasta que se desconecten y se reconecten.

Ejemplo de Solicitud:

```
curl -k -X PUT
https://hss.example.com:8443/api/epc/static_ip/c56a4180-65aa-42ec-
a945-5fd21dec0538 \
-H "Content-Type: application/json" \
-d '{
  "static_ip": {
    "ipv4_static_ip": "100.64.1.2"
  }
}'
```


Eliminar IP Estática

Eliminar una asignación de IP estática.

Endpoint: DELETE /api/epc/static_ip/:id

Parámetros de Ruta:

Parámetro	Tipo	Descripción
id	string (UUID)	ID de base de datos de IP estática

Ejemplo de Solicitud:

```
curl -k -X DELETE
https://hss.example.com:8443/api/epc/static_ip/c56a4180-65aa-42ec-
a945-5fd21dec0538
```

Comportamiento:

- Elimina la asignación de IP estática
- NO afecta el **Perfil APN** (el APN sigue disponible para otros suscriptores)
- Los suscriptores que utilizan esta IP estática recibirán IPs dinámicas en la próxima conexión
- La dirección IP se vuelve disponible para reutilización después de la eliminación

Advertencia: Si un suscriptor está utilizando activamente esta IP estática, eliminarla hará que reciba una IP dinámica en su próxima conexión PDN. Asegúrese de que los suscriptores estén desconectados o envíe una **Solicitud de Cancelación de Ubicación** antes de eliminar.

Asignar IP Estática a Suscriptor

Para asignar una IP estática a un suscriptor, debe asociar el registro de IP Estática con el **Suscriptor** durante la creación o actualización.

Patrón de Asignación:

1. **Crear la IP Estática** (ver [Crear IP Estática](#))
2. **Asignar al Suscriptor** utilizando el campo `static_ips`

Crear Suscriptor con IP Estática:

```
# Paso 1: Crear IP estática para el APN "internet"
STATIC_IP_ID=$(curl -k -X POST
https://hss.example.com:8443/api/epc/static_ip \
-H "Content-Type: application/json" \
-d '{
  "static_ip": {
    "apn_profile_id": "a1b2c3d4-e5f6-4a3b-8c2d-1e0f9a8b7c6d",
    "ipv4_static_ip": "100.64.1.1",
    "ipv6_static_ip": "2606:4700:4700::1111"
  }
}' | jq -r '.data.id')

# Paso 2: Crear suscriptor con IP estática asignada
curl -k -X POST https://hss.example.com:8443/api/subscriber \
-H "Content-Type: application/json" \
-d "{
  \"subscriber\": {
    \"imsi\": \"001001123456789\",
    \"key_set_id\": \"6ba7b810-9dad-41d1-80b4-00c04fd430c8\",
    \"epc_profile_id\": \"e58ed763-928c-4155-bee9-fdbaaadc15f3\",
    \"static_ips\": [$STATIC_IP_ID]
  }
}"
```

Actualizar Suscriptor Existente con IP Estática:

```
curl -k -X PUT
https://hss.example.com:8443/api/subscriber/d290f1ee-6c54-4b01-
90e6-d701748f0851 \
-H "Content-Type: application/json" \
-d '{
  "subscriber": {
    "static_ips": ["c56a4180-65aa-42ec-a945-5fd21dec0538",
"5a8f9c3e-2d4b-4e6f-8a1b-3c5d7e9f0a2b"]
  }
}'
```

Múltiples IPs Estáticas (Diferentes APNs):

Un suscriptor puede tener múltiples IPs estáticas siempre que cada una sea para un APN diferente:

```
# Crear IP estática para el APN "internet"
INTERNET_IP=$(curl -k -X POST
https://hss.example.com:8443/api/epc/static_ip \
-H "Content-Type: application/json" \
-d '{
  "static_ip": {
    "apn_profile_id": "a1b2c3d4-e5f6-4a3b-8c2d-1e0f9a8b7c6d",
    "ipv4_static_ip": "100.64.1.1"
  }
}' | jq -r '.data.id')

# Crear IP estática para el APN "ims"
IMS_IP=$(curl -k -X POST
https://hss.example.com:8443/api/epc/static_ip \
-H "Content-Type: application/json" \
-d '{
  "static_ip": {
    "apn_profile_id": "b2c3d4e5-f6a7-4b1c-9d2e-3f4a5b6c7d8e",
    "ipv4_static_ip": "100.64.2.1"
  }
}' | jq -r '.data.id')

# Asignar ambos al suscriptor
curl -k -X POST https://hss.example.com:8443/api/subscriber \
-H "Content-Type: application/json" \
-d "{
  \"subscriber\": {
    \"imsi\": \"001001123456789\",
    \"key_set_id\": \"6ba7b810-9dad-41d1-80b4-00c04fd430c8\",
    \"epc_profile_id\": \"e58ed763-928c-4155-bee9-
fdbaaadc15f3\",
    \"static_ips\": [$INTERNET_IP, $IMS_IP]
  }
}"
```

Reglas de Validación:

- ✓ **Permitido:** Múltiples IPs estáticas para diferentes APNs
- ✗ **Rechazado:** Múltiples IPs estáticas para el mismo APN

Ejemplo de Error - APN Duplicado:

```
# Esto FALLARÁ si ambas IPs estáticas hacen referencia al mismo APN
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "imsi": "001001123456789",
      "static_ips": ["c56a4180-65aa-42ec-a945-5fd21dec0538",
"5a8f9c3e-2d4b-4e6f-8a1b-3c5d7e9f0a2b"]
    }
  }'

# Respuesta de Error:
{
  "errors": {
    "static_ips": [
      "las ips estáticas por apn por suscriptor deben ser únicas.
por ejemplo, un suscriptor no puede ser asignado a la ip estática
100.64.1.1 para internet y también 100.64.1.2 para internet"
    ]
  }
}
```

Ver También:

- [Crear Suscriptor](#) - Aprovisionamiento de suscriptores
- [Actualizar Suscriptor](#) - Modificación de la configuración del suscriptor
- [Ejemplo Completo de Aprovisionamiento de IP Estática](#) - Flujo de trabajo de extremo a extremo

Gestión de Roaming

Los perfiles de roaming controlan si los suscriptores pueden acceder a datos y servicios IMS en redes visitadas. Los perfiles se asignan a [suscriptores](#) y consisten en reglas coincidentes por MCC/MNC.

Listar Perfiles de Roaming

Endpoint: GET /api/roaming/profile

Crear Perfil de Roaming

Endpoint: POST /api/roaming/profile

Cuerpo de Solicitud:

```
{
  "roaming_profile": {
    "name": "Solo Operadores de EE. UU.",
    "data_action_if_no_rules_match": "deny",
    "ims_action_if_no_rules_match": "deny",
    "roaming_rules": []
  }
}
```

Valores de Acción:

- "allow" - Permitir
- "deny" - Denegar

Acciones Predeterminadas:

- data_action_if_no_rules_match - Acción cuando ninguna regla de roaming coincide
- ims_action_if_no_rules_match - Acción predeterminada específica de IMS

Listar Reglas de Roaming

Endpoint: GET /api/roaming/rule

Crear Regla de Roaming

Endpoint: POST /api/roaming/rule

Cuerpo de Solicitud:

```
{
  "roaming_rule": {
    "name": "Permitir AT&T",
    "mcc": "310",
    "mnc": "410",
    "data_action": "allow",
    "ims_action": "allow"
  }
}
```

Campos:

- `mcc` - Código de País Móvil (3 dígitos)
- `mnc` - Código de Red Móvil (2-3 dígitos)
- `data_action` - "allow" o "deny" servicios de datos
- `ims_action` - "allow" o "deny" servicios IMS/voz

Ver También:

- [Documentación de Roaming](#) - Configuración detallada y ejemplos
- [Flujos de Protocolo](#) - Cómo funciona el control de roaming en los flujos de Diameter

Gestión de EIR

OmniHSS funciona como un Registro de Identidad de Equipos (EIR) a través de la interfaz Diameter S13. Las reglas de EIR controlan el acceso de dispositivos basado en patrones IMEI.

Ver [Documentación de EIR](#) para la verificación detallada de identidad de equipos, flujos de interfaz S13 y validación de IMEI.

Listar Reglas de EIR

Endpoint: GET /api/eir/rule

Crear Regla de EIR

Endpoint: POST /api/eir/rule

Cuerpo de Solicitud:

```
{
  "eir_rule": {
    "name": "Bloquear iPhone 6",
    "imei_regex": "^35[0-9]{6}0[0-9]{7}$",
    "action": 1
  }
}
```

Campos:

- `name` - Nombre descriptivo para la regla
- `imei_regex` - Expresión regular para coincidir números IMEI
- `action` - Lista blanca (0), Lista negra (1) o Lista gris (2)

Valores de Acción:

- 0 - Lista blanca (permitir)
- 1 - Lista negra (denegar)
- 2 - Lista gris (permitir pero rastrear)

Casos de Uso:

- Bloquear dispositivos robados (lista negra de IMEIs específicos)
- Restringir tipos de dispositivos (lista negra por patrón TAC)
- Permitir solo dispositivos aprobados (patrón de lista blanca con denegación por defecto)

Ver También:

- [Flujos de Protocolo](#) - Flujo de interfaz S13 y verificación de EIR
 - [Descripción General de la Arquitectura](#) - Función EIR de OmniHSS
-

Documentación Adicional

Para más información, consulte la siguiente documentación:

- [Estado y Salud](#) - Puntos finales de verificación de salud de la API
 - [Manejo de Errores](#) - Errores comunes y solución de problemas
 - [Ejemplos de Uso de la API](#) - Flujos de trabajo de aprovisionamiento completos
-

[← Volver a la Guía de Operaciones](#) | [Siguiente: Panel de Control →](#)

Estado y Salud de la API

[← Volver a la Referencia de la API](#)

Estado del Sistema

Verifique si la API está respondiendo.

Endpoint: `GET /api/status`

Ejemplo de Solicitud:

```
curl -k https://hss.example.com:8443/api/status
```

Ejemplo de Respuesta:

```
{  
  "status": "ok"  
}
```

Caso de Uso: Verificación de salud para balanceadores de carga y sistemas de monitoreo.

[← Volver a la Referencia de la API](#)

Visión General de la Arquitectura de OmniHSS

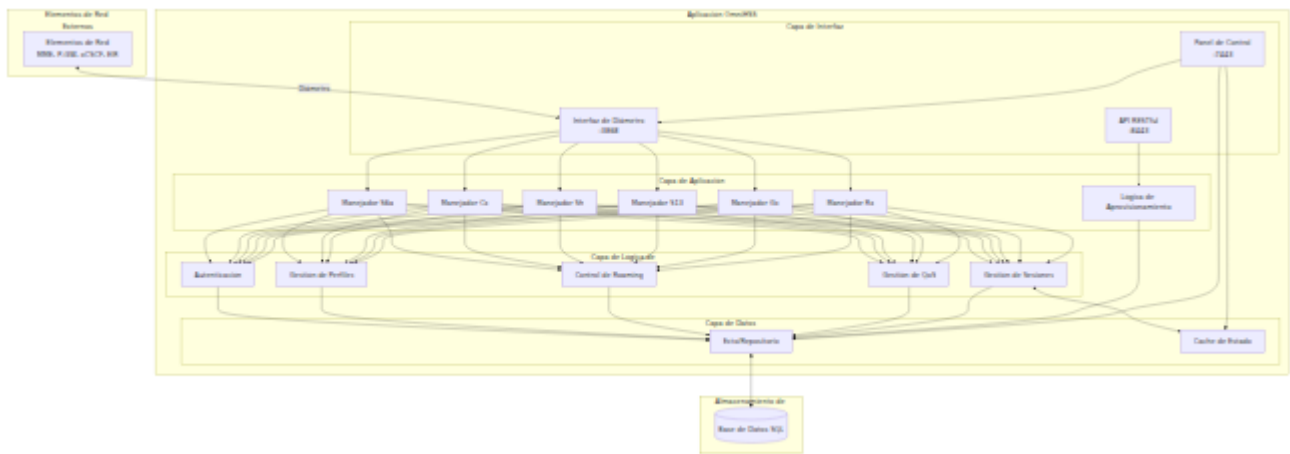
[← Volver a la Guía de Operaciones](#)

Tabla de Contenidos

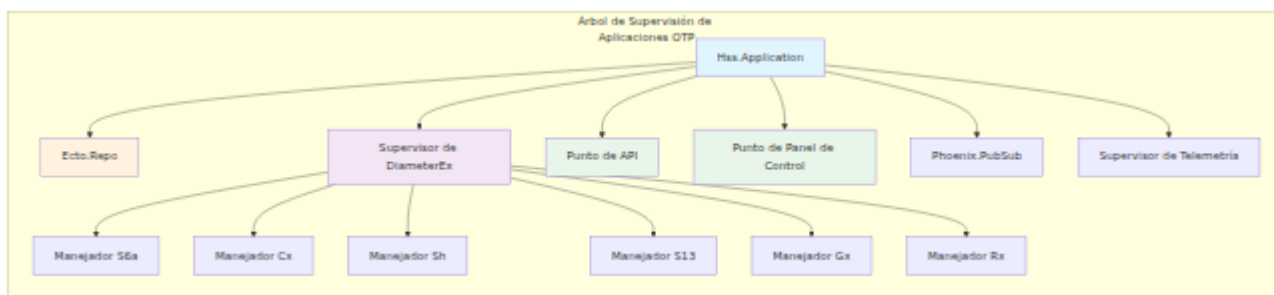
- [Visión General del Sistema](#)
 - [Arquitectura de Componentes](#)
 - [Pila de Diámetro](#)
 - [Capa de Aplicación](#)
 - [Capa de Datos](#)
 - [Interfaces Externas](#)
 - [Arquitectura de Despliegue](#)
-

Visión General del Sistema

OmniHSS está construido sobre Elixir y la plataforma Erlang/OTP, proporcionando un sistema altamente concurrente y tolerante a fallos diseñado para cargas de trabajo de telecomunicaciones. La arquitectura sigue un enfoque por capas con una clara separación de preocupaciones.



1. **Se registra en DiameterEx** - Se suscribe a IDs de Aplicación de Diámetro específicos
2. **Valida Solicitudes** - Extrae AVPs, valida el estado del suscriptor
3. **Procesa Lógica de Negocios** - Llama a los módulos de lógica de negocios apropiados
4. **Construye Respuestas** - Construye mensajes de respuesta de Diámetro con AVPs
5. **Maneja Errores** - Devuelve códigos de resultado de Diámetro apropiados



Pila de Diámetro

Configuración del Servicio de Diámetro

OmniHSS configura un único servicio de Diámetro con múltiples aplicaciones soportadas:

Servicio de Diámetro:
:omnitouch_hss

S6a
ID de App: 16777251

S13
ID de App: 16777252

Cx
ID de App: 16777216

Sh
ID de App: 16777217

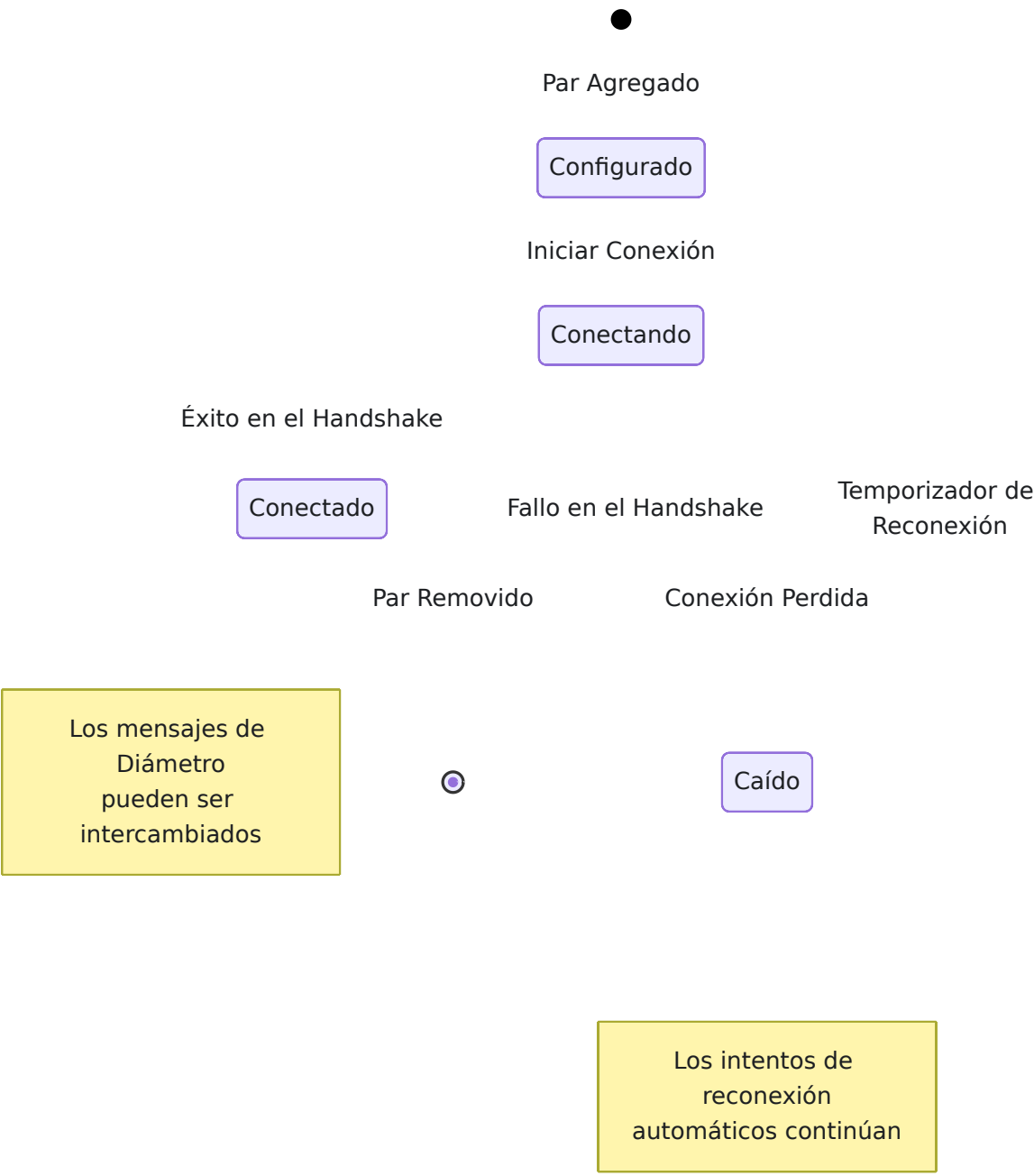
Gx
ID de App: 16777238

Rx
ID de App: 16777236

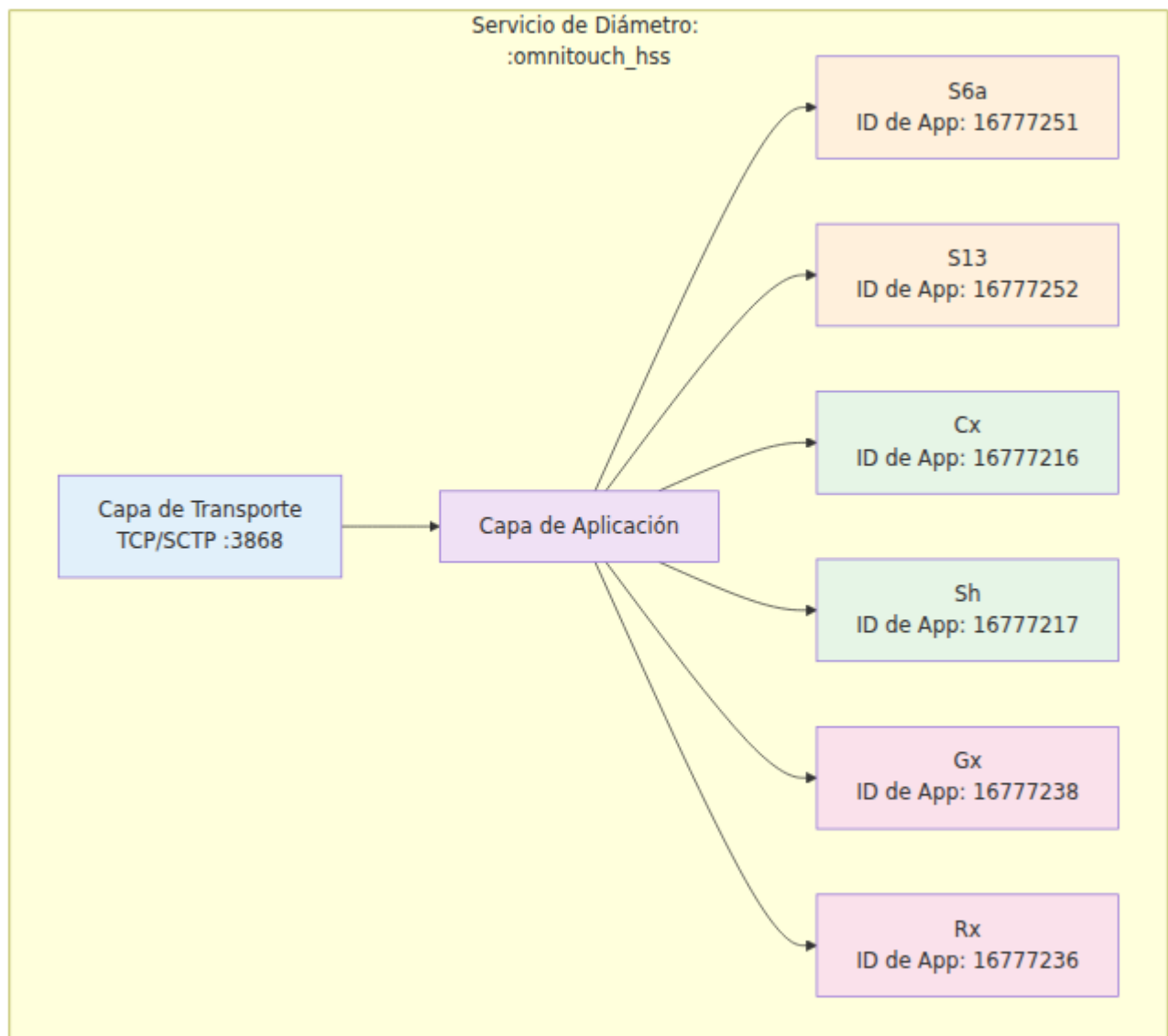
Capa de Transporte
TCP/SCTP :3868

Capa de Aplicación

Gestión de Conexiones de Pares



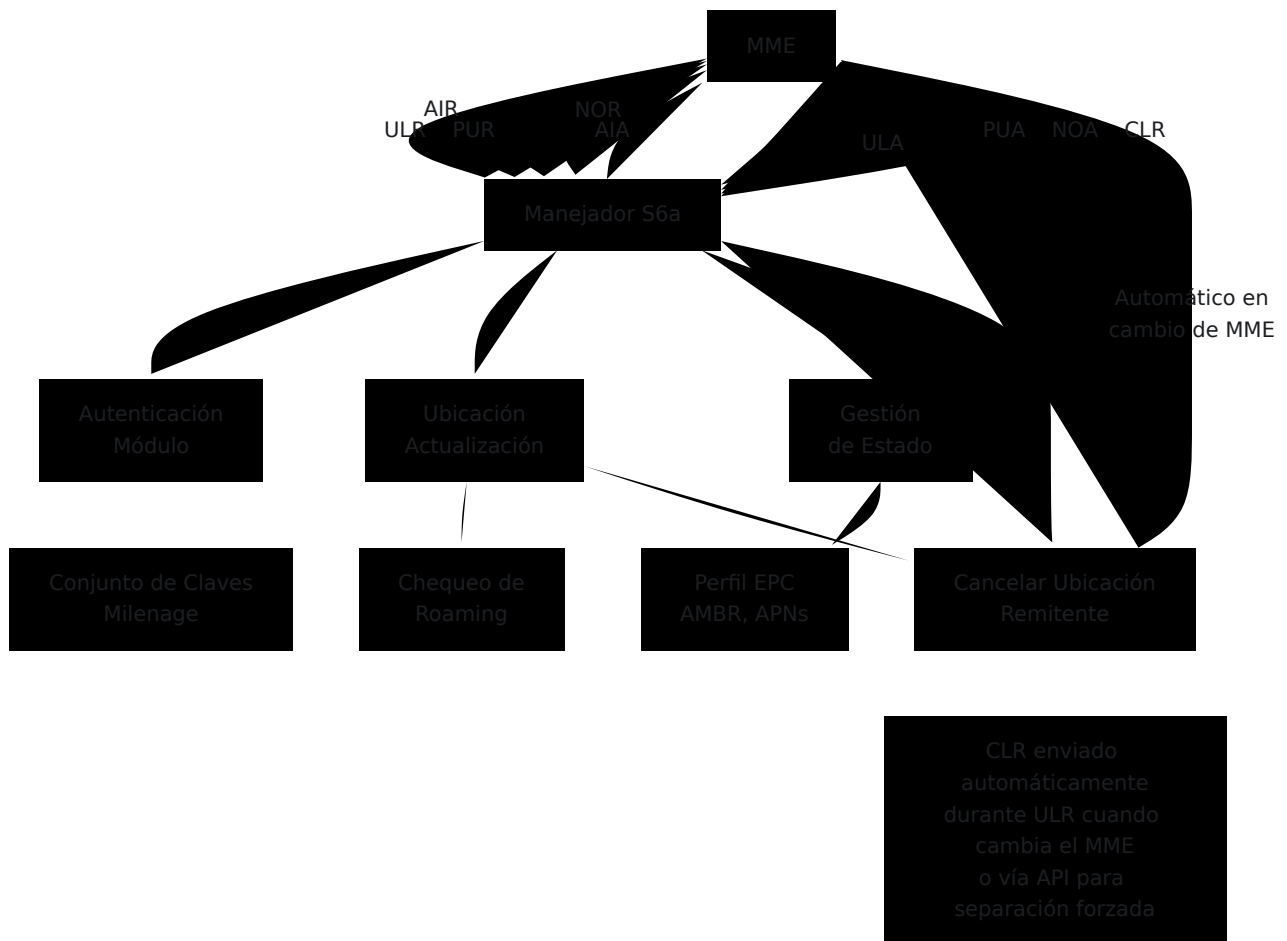
Flujo de Mensajes de Diámetro



Capa de Aplicación

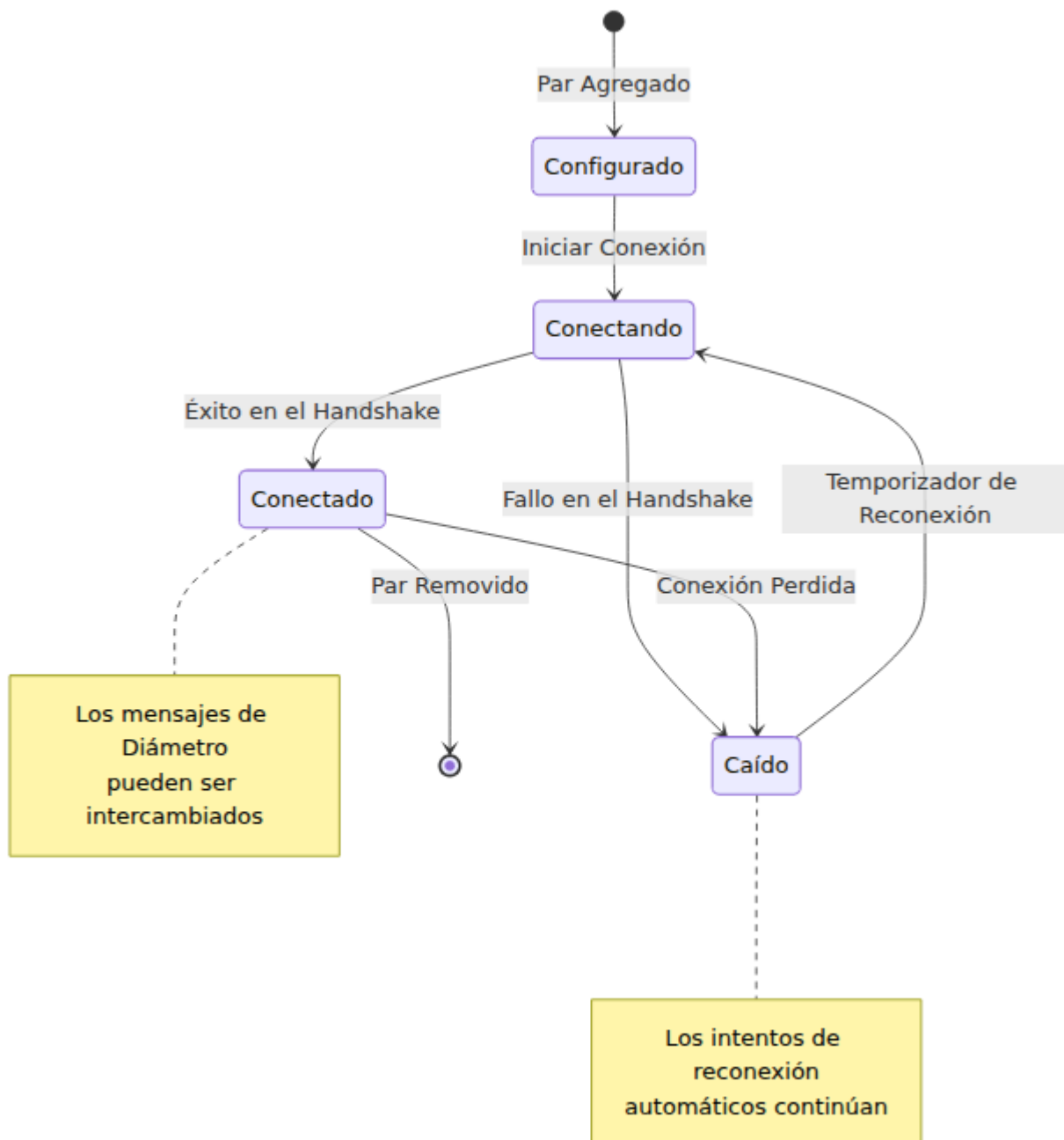
Interfaz S6a (LTE/EPC)

Maneja la autenticación y la gestión de movilidad para redes LTE.



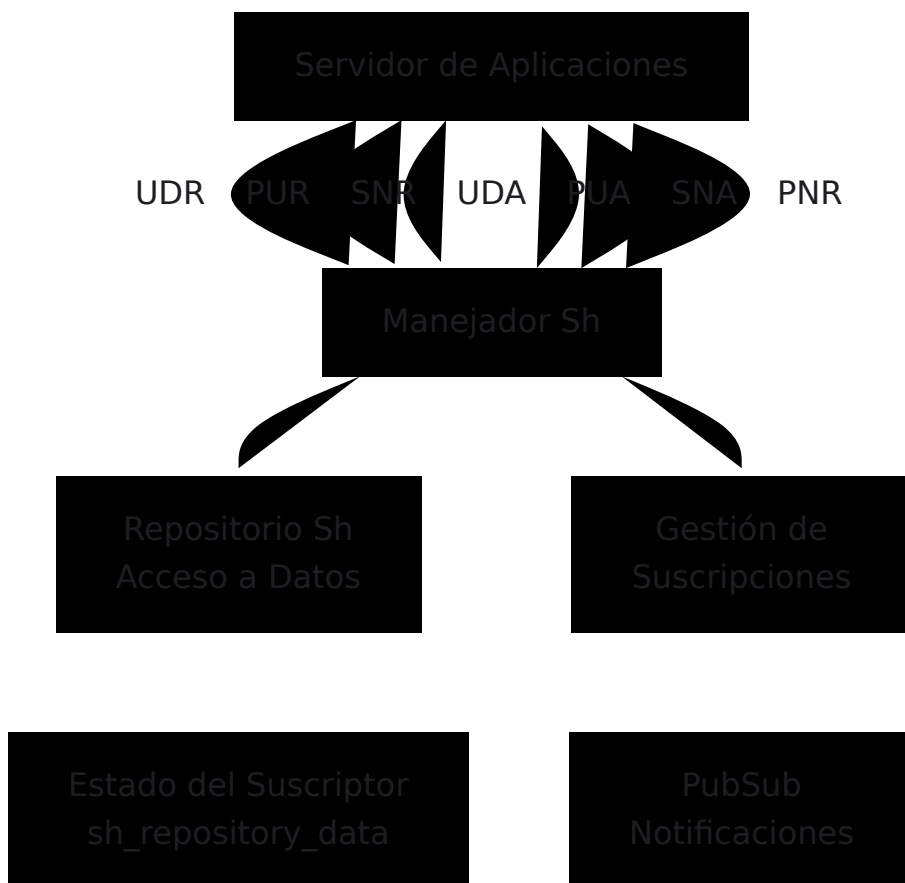
Interfaz Cx (IMS)

Maneja el registro y la autenticación de IMS.



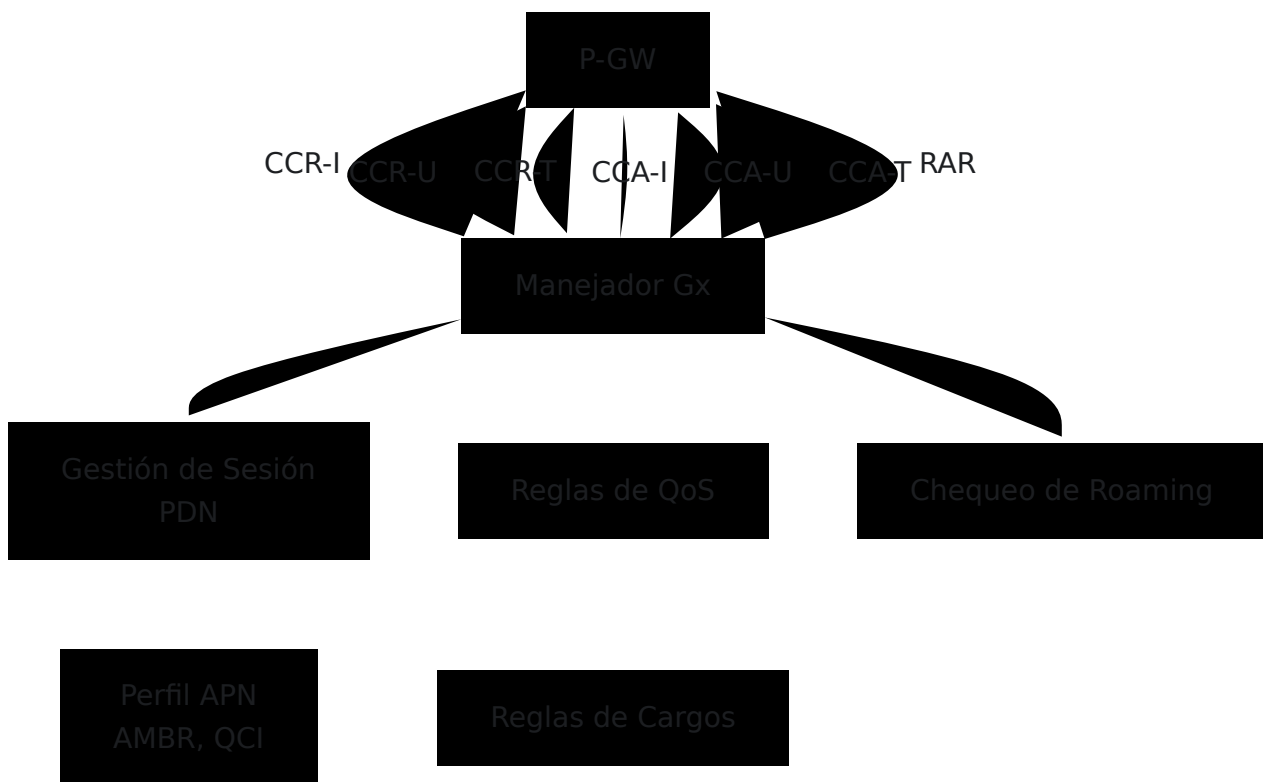
Interfaz Sh (Datos de Perfil IMS)

Proporciona a los servidores de aplicaciones IMS acceso a los datos del perfil del suscriptor.



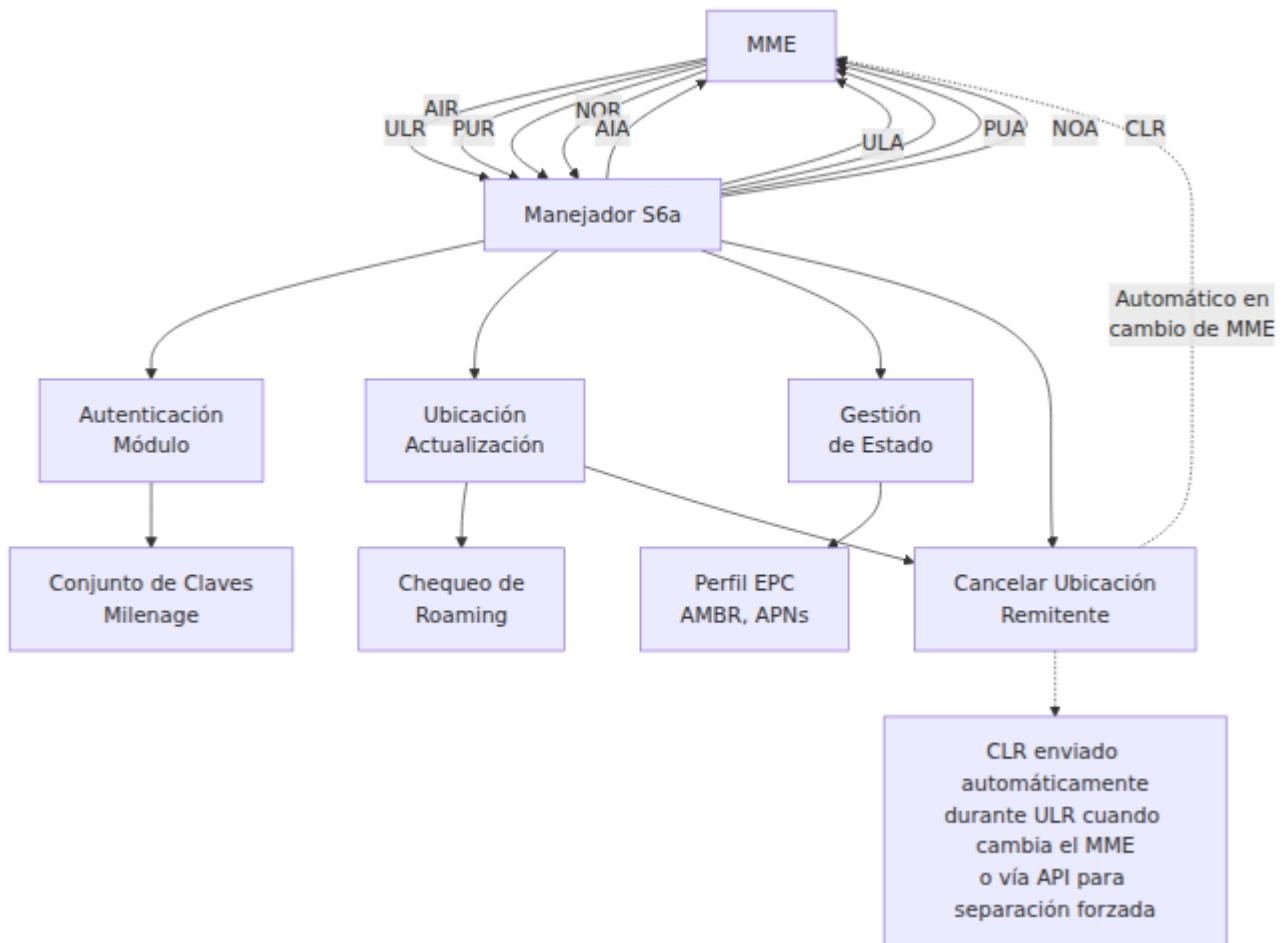
Interfaz Gx (Control de Políticas)

Gestiona el control de políticas y cargos para sesiones de datos. **Ver Documentación de PCRF** para más detalles.



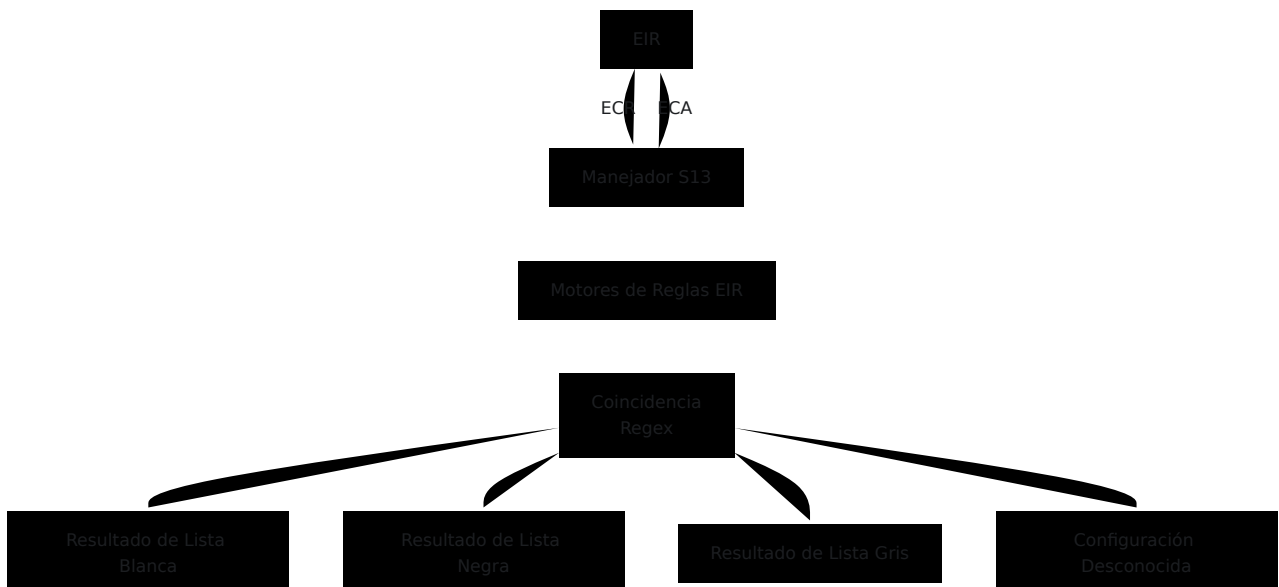
Interfaz Rx (Medios IMS)

Controla la política de medios IMS y los portadores dedicados para VoLTE. **Ver Documentación de PCRF para más detalles.**



Interfaz S13 (EIR)

Valida el IMEI del dispositivo contra las reglas de identidad del equipo. **Ver Documentación de EIR para más detalles.**



Capa de Datos

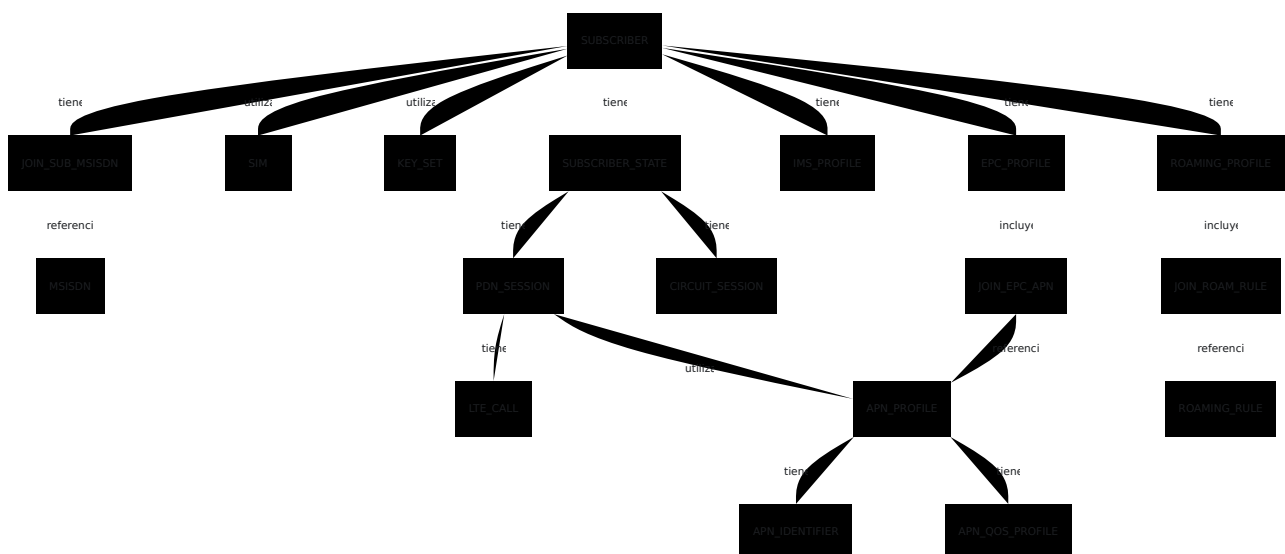
Backend de Base de Datos

OmniHSS utiliza **PostgreSQL** como su backend de base de datos y **Ecto** como su capa de abstracción de base de datos. Todas las tablas utilizan claves primarias UUID para identificación única global en todos los sitios.

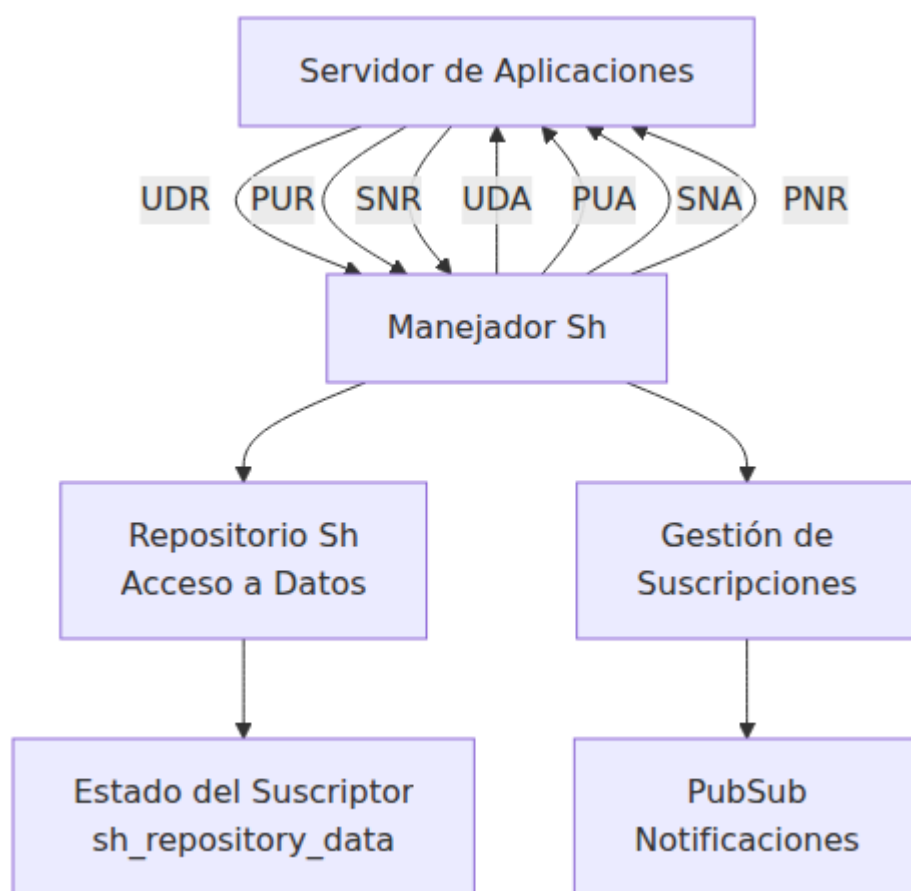
Para despliegues en múltiples sitios, OmniHSS utiliza la replicación lógica bidireccional de PostgreSQL. Cada sitio opera como un primario de lectura/escritura independiente con replicación asíncrona basada en WAL entre sitios.

Ver [Replicación de Base de Datos](#) para la configuración y operaciones de replicación en múltiples sitios.

Visión General del Esquema de Base de Datos



Patrón de Repositorio Ecto



Estrategia de Consulta Optimizada

Cada procedimiento de Diámetro utiliza consultas optimizadas que precargan solo las asociaciones necesarias:

Solicitud de Diámetro

Tipo de Procedimiento

S6a AIR

Consulta: suscriptor
+ conjunto_de_claves
+ perfil_de_roaming

Datos Mínimos
Respuesta Rápida

S6a ULR

Consulta: suscriptor
+ perfil_epc + apns
+ estado_del_suscriptor

Datos Moderados
Información de Perfil

Cx SAR

Consulta: suscriptor
+ perfil_ims
+ msisdns

Datos IMS Completos
Perfil Completo

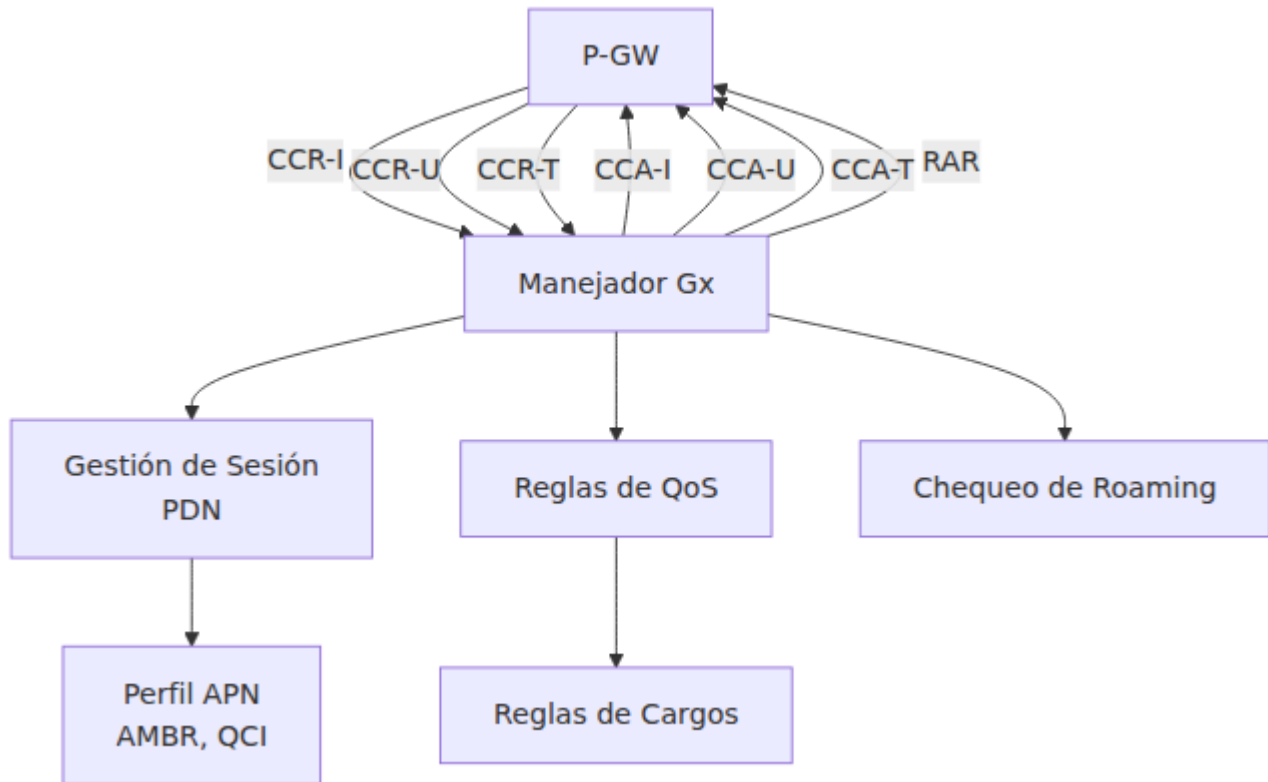
Cx CCR-I

Consulta: suscriptor
+ perfil_apn + qos
+ estado_del_suscriptor

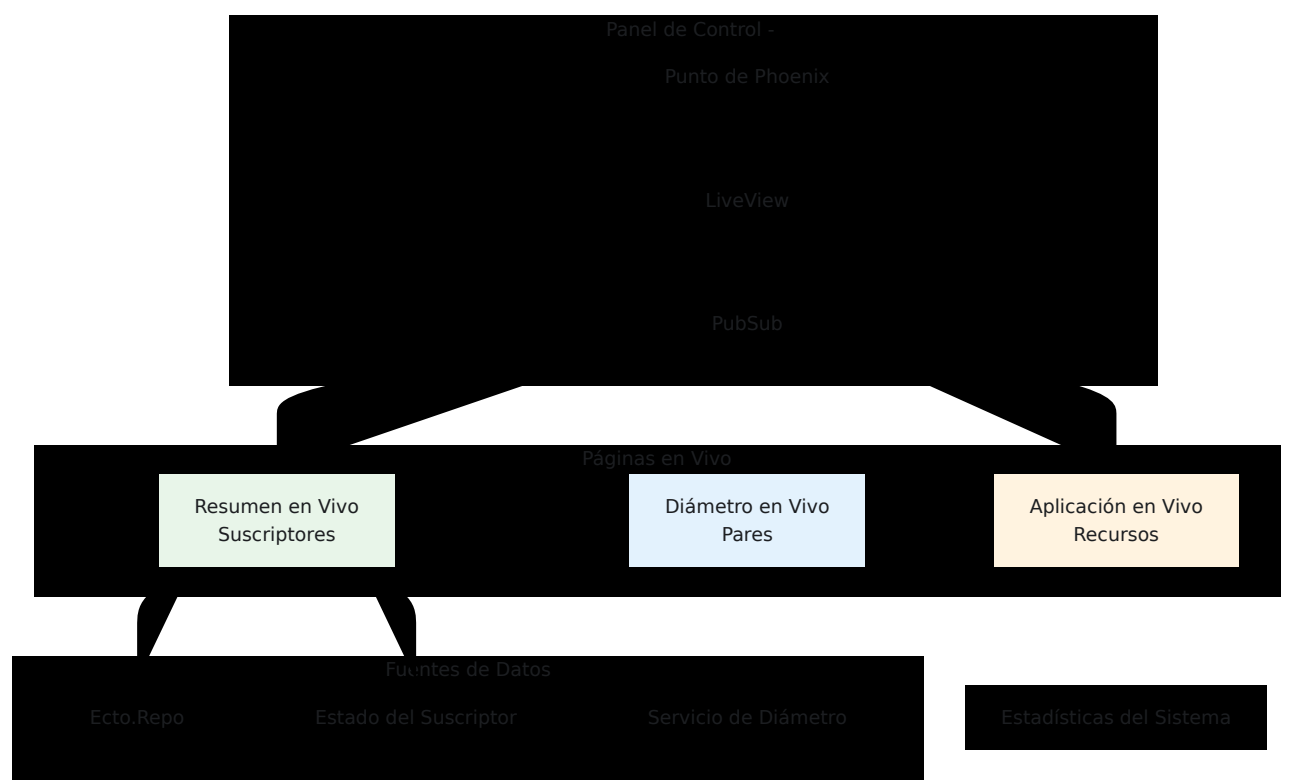
Datos de Sesión
Reglas de QoS

Interfaces Externas

Arquitectura de API

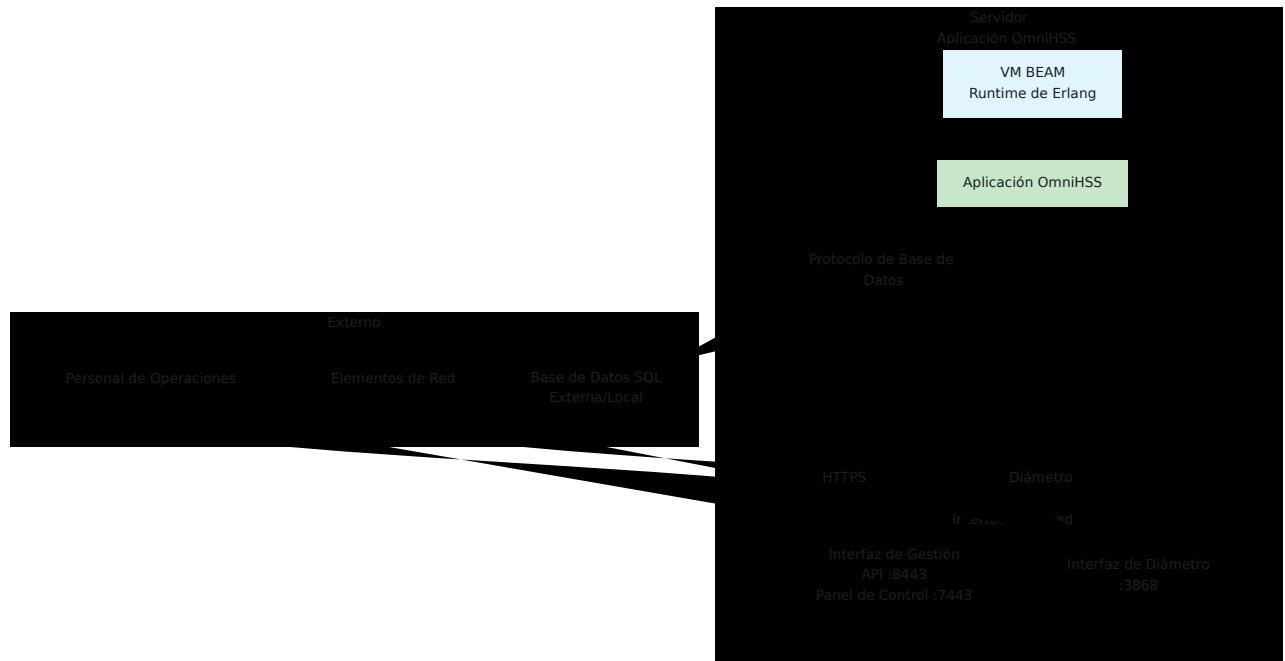


Arquitectura del Panel de Control



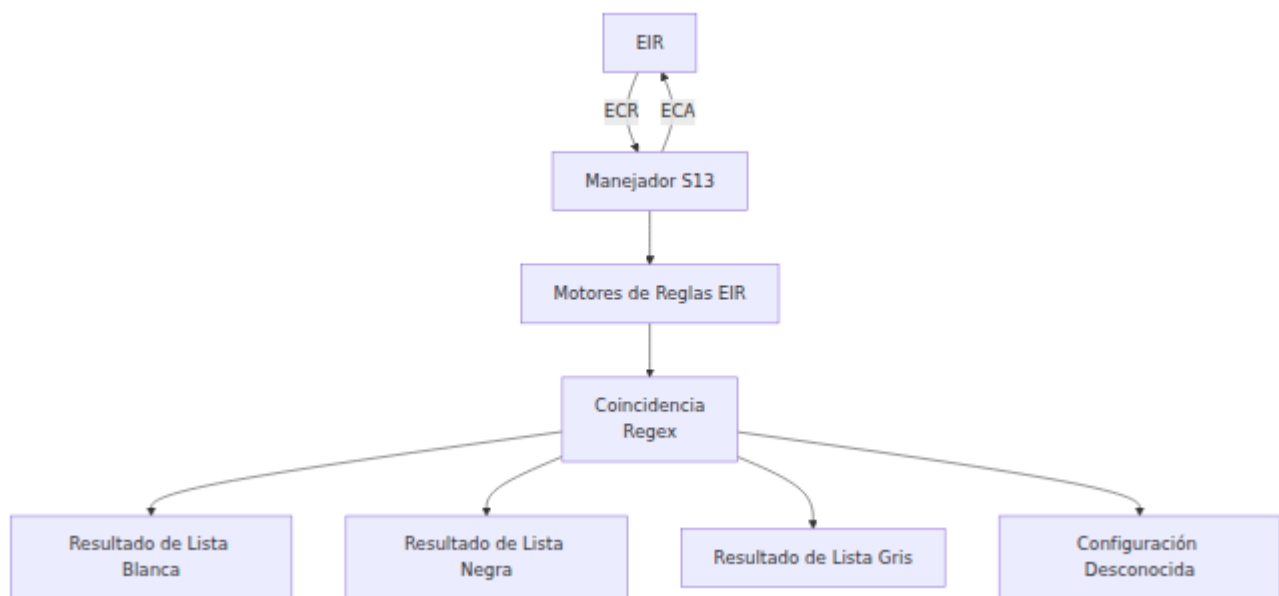
Arquitectura de Despliegue

Despliegue en Nodo Único



Despliegue HA en Múltiples Sitios (Replicación Lógica)

Para despliegues de alta disponibilidad a través de sitios geográficos, OmniHSS utiliza la replicación lógica bidireccional de PostgreSQL. Cada sitio tiene una base de datos independiente de lectura/escritura.



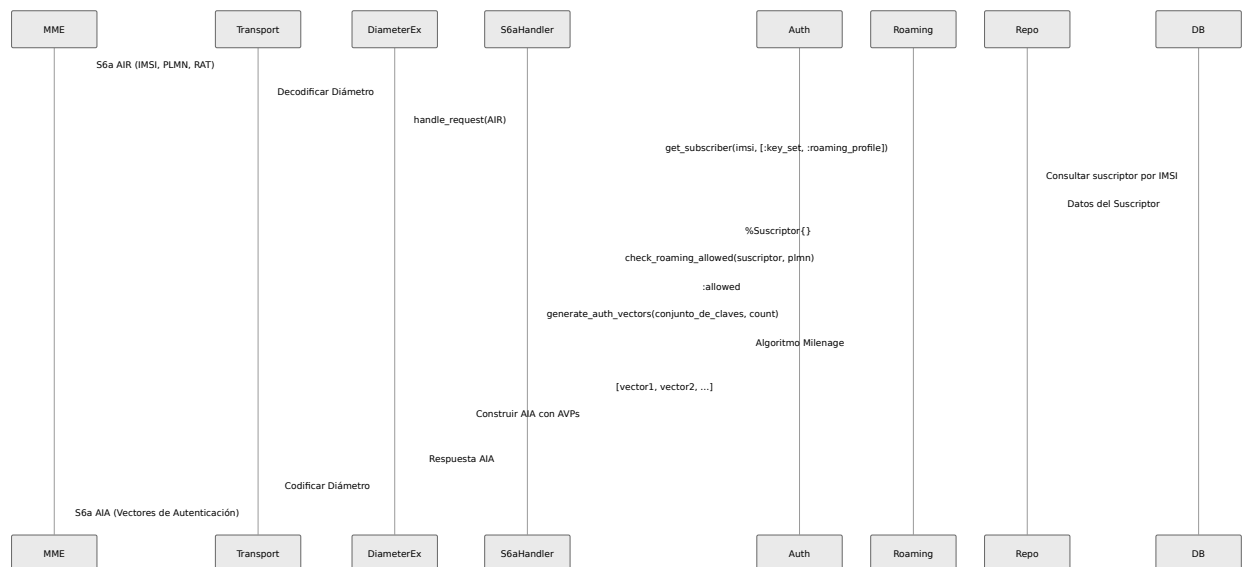
Características Clave:

- **Ambos Sitios Lectura/Escritura:** Las escrituras locales son instantáneas, nunca bloqueadas por el sitio remoto
- **Replicación Asíncrona:** Los cambios fluyen a través de WAL. La replicación no añade penalización de latencia de escritura
- **Tolerante a Particiones:** Ambos sitios continúan operando si se cae el enlace intersitios. Las colas WAL se mantienen localmente y se recuperan al restaurar
- **Sin Quorum:** No se requiere un número mínimo de nodos. Funciona de manera idéntica con un sitio o muchos
- **Claves Primarias UUID:** IDs globalmente únicos eliminan conflictos entre sitios

Ver **Replicación de Base de Datos** para configuración y operaciones detalladas.

Ejemplo de Flujo de Proceso: Autenticación

Este ejemplo muestra el flujo completo para una solicitud de autenticación:



Principios Arquitectónicos Clave

1. Tolerancia a Fallos

- Los árboles de supervisión de Erlang/OTP reinician automáticamente los procesos fallidos
- Los manejadores de Diámetro aislados previenen fallos en cascada
- Agrupamiento de conexiones de base de datos con reconexión automática

2. Concurrencia

- Cada solicitud de Diámetro se maneja en su propio proceso
- No hay estado compartido entre los manejadores de solicitudes
- Agrupamiento de conexiones de base de datos para consultas paralelas

3. Modularidad

- Cada aplicación de Diámetro en un módulo separado
- Clara separación entre la interfaz, la lógica de negocios y las capas de datos
- Algoritmos de autenticación intercambiables

4. Rendimiento

- Consultas de base de datos optimizadas con precarga selectiva
- Transferencia de datos mínima para cada tipo de procedimiento
- Agrupamiento de conexiones y keepalive

5. Observabilidad

- Monitoreo en tiempo real a través del Panel de Control
- Registro estructurado en toda la aplicación
- Seguimiento del estado de pares de Diámetro
- Seguimiento del estado del suscriptor con marcas de tiempo

[← Volver a la Guía de Operaciones](#) | [Siguiente: Configuración →](#)

Guía de Configuración de OmniHSS

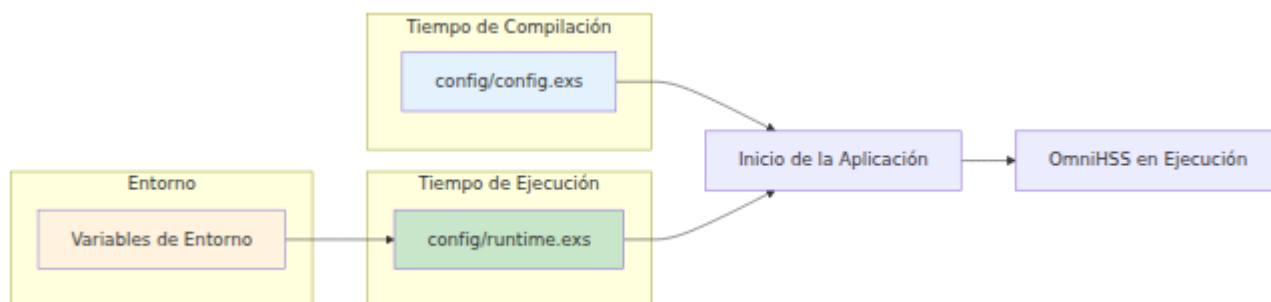
[← Volver a la Guía de Operaciones](#)

Tabla de Contenidos

- [Descripción General del Archivo de Configuración](#)
 - [Configuración del Cliente de Licencias](#)
 - [Configuración en Tiempo de Ejecución](#)
 - [Configuración de la Base de Datos](#)
 - [Configuración de Diameter](#)
 - [Configuración de la Red](#)
 - [Configuración del PLMN de Inicio](#)
 - [Configuración del Núcleo HSS](#)
 - [Configuración de IMS](#)
 - [Configuración de EIR](#)
 - [Configuración de la API y del Panel de Control](#)
 - [Flujo de Trabajo de Configuración](#)
-

Descripción General del Archivo de Configuración

OmniHSS utiliza dos archivos de configuración principales:



config/config.exs (Tiempo de Compilación)

Contiene la configuración estática que no cambia entre entornos:

- Configuración de la página del Panel de Control
- Configuración del punto final de la API
- Configuración de telemetría

config/runtime.exs (Tiempo de Ejecución)

Contiene la configuración específica del entorno que cambia por implementación:

- Parámetros de conexión a la base de datos
- Configuración de pares de Diameter
- Configuración del PLMN de inicio
- Selección de S-CSCF de IMS
- Vínculos de interfaz de red

Configuración del Cliente de Licencias

El Cliente de Licencias valida la licencia HSS con un servidor de licencias remoto:


```
# config/runtime.exs

config :license_client,
  # Puntos finales de la API del servidor de licencias (lista para
  conmutación por error)
  license_server_api_urls:
  ["https://license.example.com:8443/api"],

  # Nombre de la organización licenciada
  licensee: "Su Nombre de Organización",

  # Identificador del producto
  product_name: "omnihss"
```

Parámetros de Configuración de Licencia:

Parámetro	Descripción	Requerido	Ejem
license_server_api_urls	Lista de URLs del servidor de licencias	Sí	["https://10.0.0.1:8443/api"]
licensee	Nombre de la organización en la licencia	Sí	"ACME Telecom"
product_name	Identificador del producto para la licencia	Sí	"omnihss"

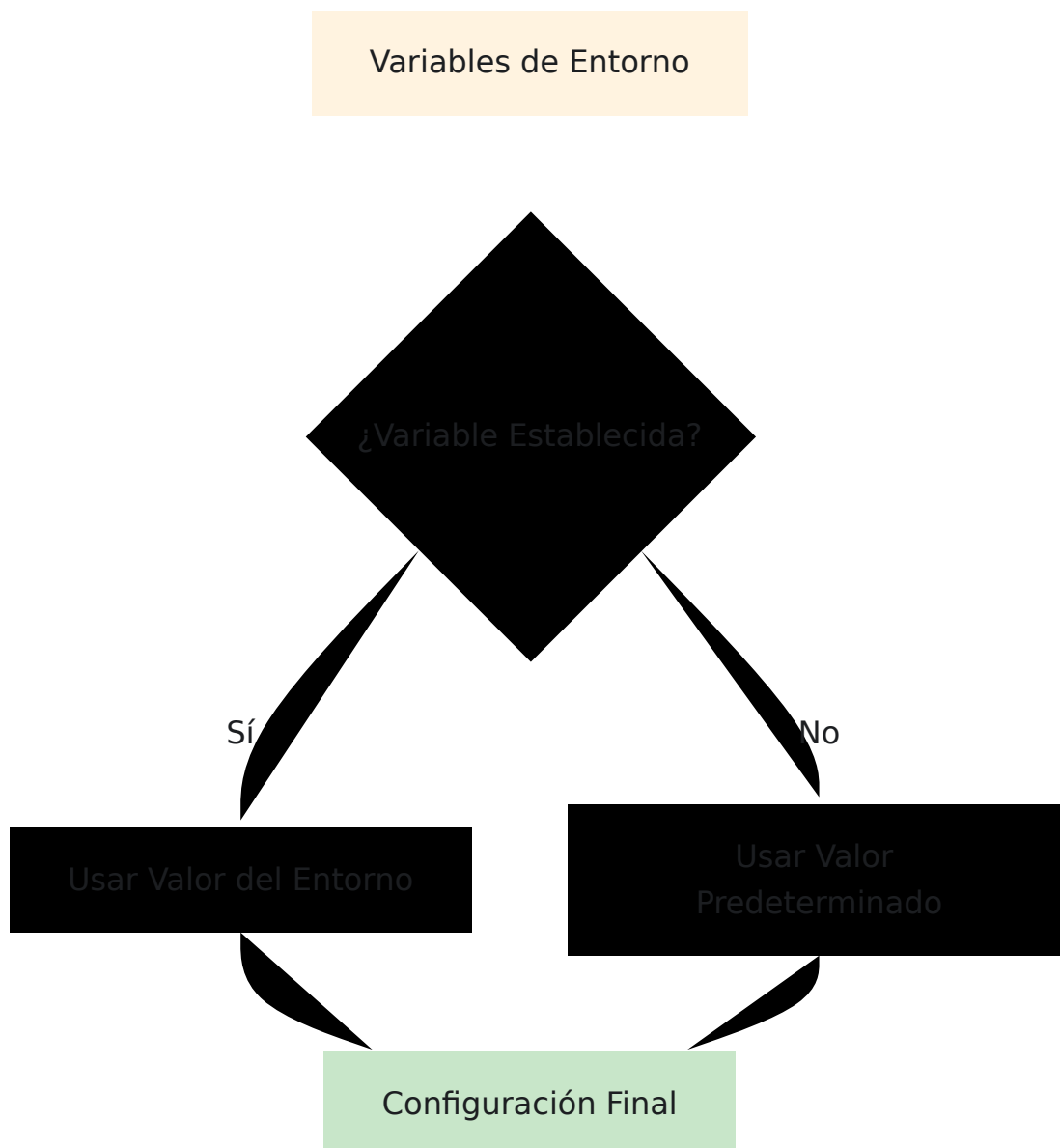
Notas Importantes:

- El servidor de licencias debe ser accesible desde HSS
- Utilice HTTPS para la validación segura de licencias
- Múltiples URLs proporcionan capacidad de conmutación por error

- La validación de la licencia ocurre al inicio y periódicamente

Configuración en Tiempo de Ejecución

Prioridad de Configuración



Patrón de Variables de Entorno

OmniHSS sigue este patrón para la configuración:

- Los nombres de las variables de entorno están en MAYÚSCULAS con guiones bajos
 - Los valores predeterminados se proporcionan en runtime.exs
 - Las credenciales de la base de datos deben usar variables de entorno en producción
-

Configuración de la Base de Datos

Configuración Básica de la Base de Datos

```
# config/runtime.exs

config :hss, Hss.Repo,
  # Parámetros de conexión a la base de datos
  username: System.get_env("DATABASE_USERNAME", "root"),
  password: System.get_env("DATABASE_PASSWORD", "password"),
  hostname: System.get_env("DATABASE_HOSTNAME", "localhost"),
  database: System.get_env("DATABASE_NAME", "omnihss"),

  # Configuración del grupo de conexiones
  pool_size:
    String.to_integer(System.get_env("DATABASE_POOL_SIZE", "20")),

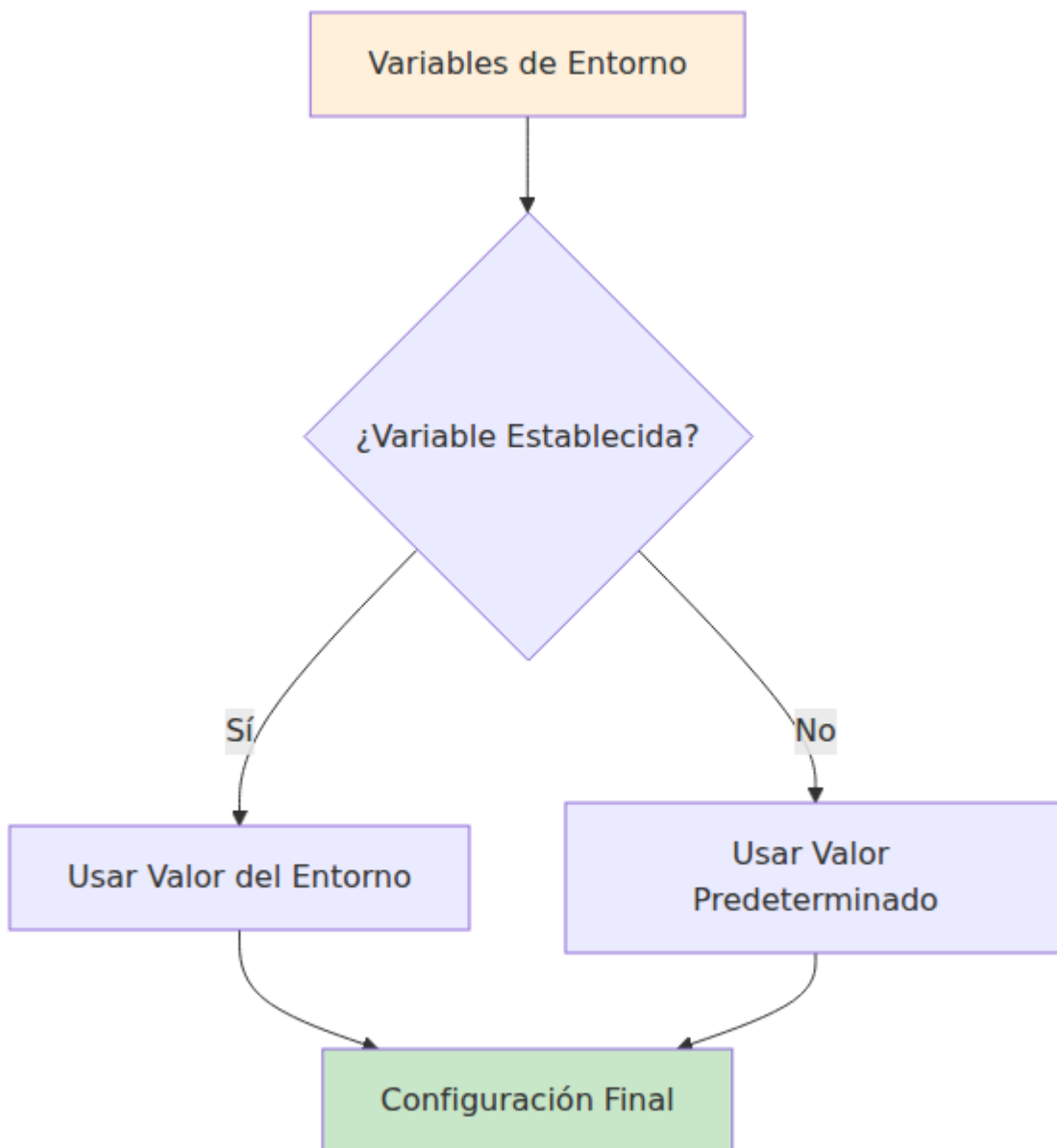
  # Timeouts (en milisegundos)
  timeout: 15_000,
  connect_timeout: 15_000,

  # Opciones adicionales
  show_sensitive_data_on_connection_error: false
```

Parámetros de Configuración de la Base de Datos

Parámetro	Descripción	Predeterminado	Recomendación
<code>username</code>	Nombre de usuario de la base de datos SQL	<code>"root"</code>	Usar usuario dedicado en producción
<code>password</code>	Contraseña de la base de datos SQL	<code>"password"</code>	Usar contraseña fuerte, almacenar en variable de entorno
<code>hostname</code>	Nombre del servidor de la base de datos SQL	<code>"localhost"</code>	Usar FQDN o IP en producción
<code>database</code>	Nombre de la base de datos	<code>"omnihss"</code>	Mantener predeterminado a menos que haya múltiples instancias
<code>pool_size</code>	Tamaño del grupo de conexiones	<code>20</code>	Ajustar según la carga (10-50 típico)

Ajuste del Tamaño del Grupo



Directrices:

- Comience con 20 conexiones
- Monitoree los errores de "timeout del grupo de conexiones"
- Aumente en 10 si ocurren timeouts bajo carga normal
- Cada conexión utiliza ~4MB de memoria
- Demasiadas conexiones pueden degradar el rendimiento de la base de datos SQL

Ejemplo: Configuración de la Base de Datos en Producción

```
# config/runtime.exs - Ejemplo de producción

config :hss, Hss.Repo,
  username: System.fetch_env!("DATABASE_USERNAME"),      #
  password: System.fetch_env!("DATABASE_PASSWORD"),      #
  hostname: System.get_env("DATABASE_HOSTNAME",
    "db.internal.example.com"),
  database: System.get_env("DATABASE_NAME", "omnihss"),
  port: String.to_integer(System.get_env("DATABASE_PORT",
    "5432")),
  pool_size:
    String.to_integer(System.get_env("DATABASE_POOL_SIZE", "30")),
  ssl: true,
  ssl_opts: [
    cacertfile: "/etc/ssl/certs/postgres-ca.pem",
    verify: :verify_peer
  ]
```

Configuración de Diameter

Configuración del Servicio Diameter

```
# config/runtime.exs

diameter_config = %{
  service_name: :omnitouch_hss,

  # Vínculo de red
  listen_ip: System.get_env("DIAMETER_LISTEN_IP", "10.7.25.186"),
  listen_port:
    String.to_integer(System.get_env("DIAMETER_LISTEN_PORT", "3868")),

  # Identidad de Diameter
  host: System.get_env("DIAMETER_HOST", "omnihss"),
  realm: System.get_env("DIAMETER_REALM",
    "epc.mnc001.mcc001.3gppnetwork.org"),

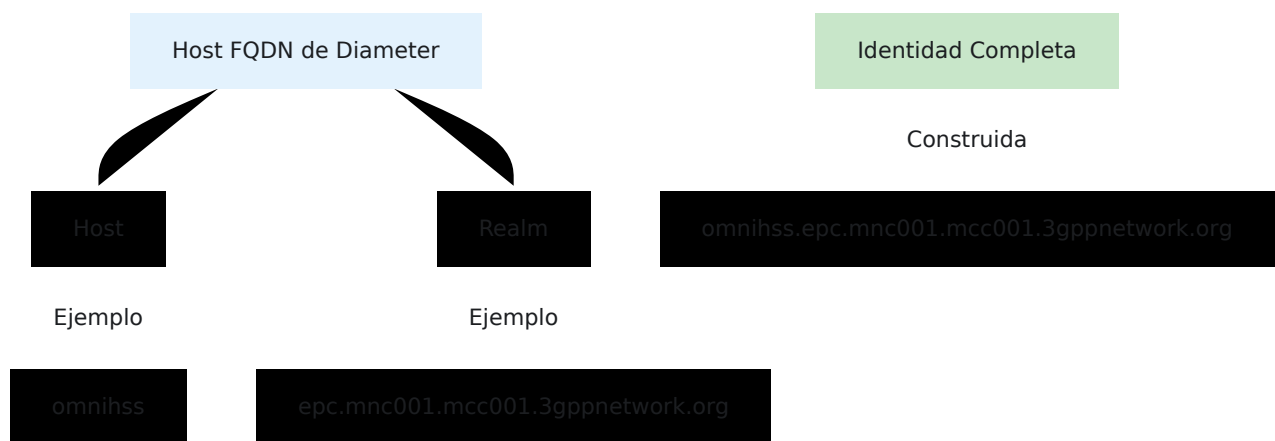
  # Identificación del producto
  product_name: "OmniHSS",
  vendor_id: 10415, # 3GPP
  supported_vendor_ids: [5535, 10415],

  # Configuración del protocolo
  request_timeout: 5000,

  # Configuración de pares
  peers: [
    # Agregar configuraciones de pares aquí
  ]
}

config :hss, :diameter, diameter_config
```

Configuración de la Identidad de Diameter



Directrices:

- **Host:** Nombre corto del HSS (por ejemplo, "omnihss", "hss01")
- **Realm:** Realm de Diameter que coincide con su PLMN (por ejemplo, "epc.mnc001.mcc001.3gppnetwork.org")
- **Identidad Completa:** Construida como `{host}.{realm}`

Agregar Pares de Diameter

Configuración de Pares Estáticos (Modo Conectar)


```
# config/runtime.exs

peers: [
  # Ejemplo de Par MME
  %{
    host: "mme01.epc.mnc001.mcc001.3gppnetwork.org",
    realm: "epc.mnc001.mcc001.3gppnetwork.org",
    ip: "10.7.25.100",
    port: 3868,
    transport: :sctp, # o :tcp
    applications: [:s6a]
  },

  # Ejemplo de Par P-GW
  %{
    host: "pgw01.epc.mnc001.mcc001.3gppnetwork.org",
    realm: "epc.mnc001.mcc001.3gppnetwork.org",
    ip: "10.7.25.101",
    port: 3868,
    transport: :sctp,
    applications: [:gx]
  },

  # Ejemplo de Par I-CSCF
  %{
    host: "icscf01.ims.mnc001.mcc001.3gppnetwork.org",
    realm: "ims.mnc001.mcc001.3gppnetwork.org",
    ip: "10.7.25.102",
    port: 3868,
    transport: :tcp,
    applications: [:cx]
  }
]
```

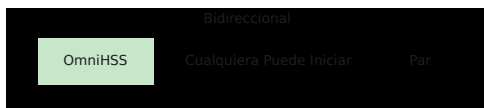
Modo Solo Escuchar

Para entornos donde los pares inician conexiones al HSS:

```
# config/runtime.exs

diameter_config = %{
  # ... otra configuración ...
  peers: [] # Vacío - aceptar solo conexiones entrantes
}
```

Modos de Conexión de Pares de Diameter



Selección del Protocolo de Transporte

Transporte	Ventajas	Desventajas	Recomendación
SCTP	Multi-streaming, mejor detección de fallos	Requiere soporte del kernel, configuración del firewall	Preferido para Diameter
TCP	Soporte universal, reglas de firewall más simples	Flujo único, detección de fallos más lenta	Usar si SCTP no está disponible

Configuración de la Red

Configuración del PLMN de Inicio

El PLMN de inicio identifica a su operador de red:

```
# config/runtime.exs

config :hss, :home_plmn, %{
  mcc: System.get_env("HOME_PLMN_MCC", "001"), # Código de País
  mnc: System.get_env("HOME_PLMN_MNC", "001")   # Código de Red
}

Móvil
```

Configuración del Núcleo HSS

Estos ajustes controlan el comportamiento y las características del HSS:

```
# config/runtime.exs

config :hss,
  # Repositorios Ecto para operaciones de base de datos
  ecto_repos: [Hss.Repo],

  # CLR (Cancel Location Request) en cambio de MME
  send_clr_on_mme_change: true,

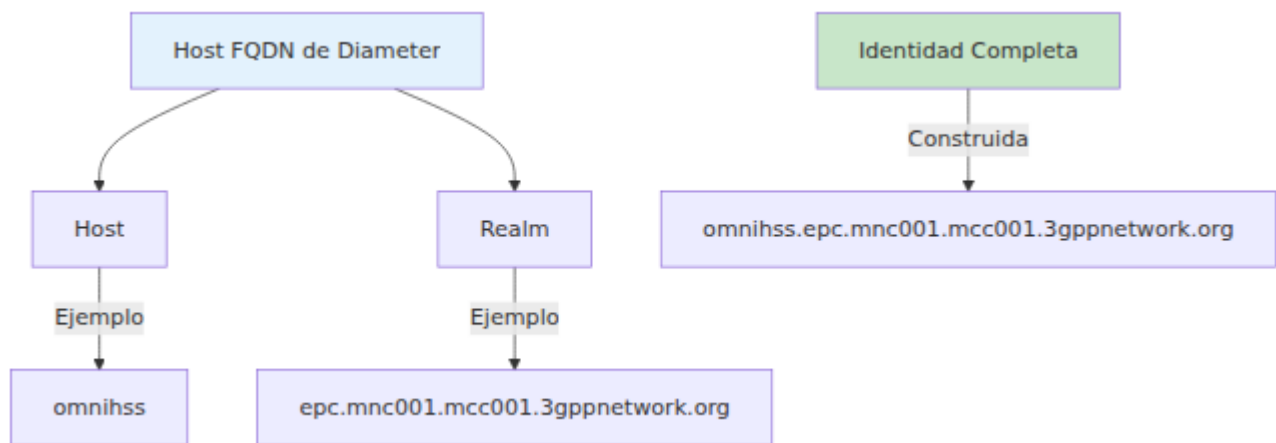
  # Detener el servicio Diameter durante fallos de base de datos
  stop_diameter_on_database_failure: true,

  # Configuración de aplicación de licencia
  license_enforced: true,
  license_module: LicenseClient
```

Parámetros del Núcleo HSS:

Parámetro	Descripción	Predeterminado
<code>ecto_repos</code>	Lista de repositorios Ecto utilizados por la aplicación	<code>[Hss.Repo]</code>
<code>send_clr_on_mme_change</code>	Enviar Cancel Location Request cuando el suscriptor cambia de MME	<code>true</code>
<code>stop_diameter_on_database_failure</code>	Deshabilitar el servicio Diameter si la base de datos se vuelve no disponible	<code>true</code>
<code>license_enforced</code>	Habilitar la aplicación de licencia	<code>true</code>
<code>license_module</code>	Módulo que maneja las verificaciones de licencia	<code>LicenseClient</code>

Formato del Código PLMN



Ejemplos:

- AT&T (EE. UU.): MCC=310, MNC=410
- Verizon (EE. UU.): MCC=311, MNC=480
- Vodafone (Reino Unido): MCC=234, MNC=15
- Red de Prueba: MCC=001, MNC=01

Vínculo de la Interfaz de Red

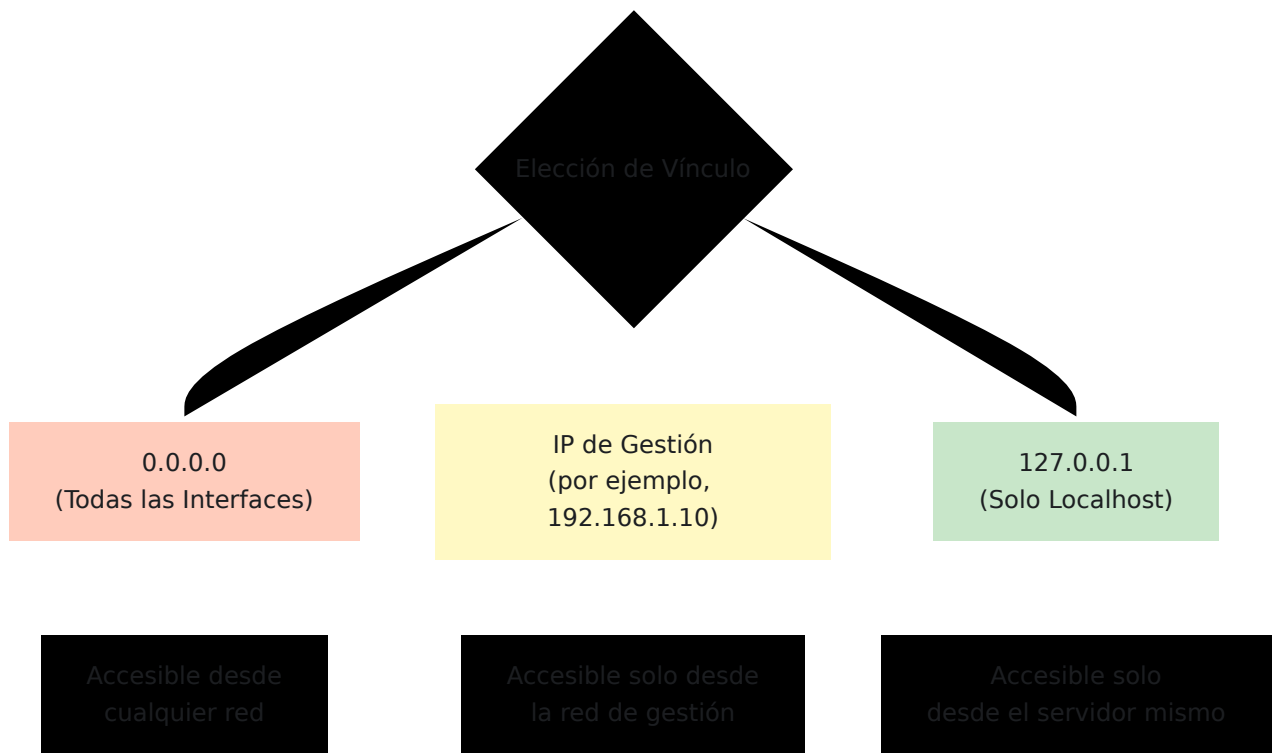
```
# config/runtime.exs

# Interfaz Diameter
listen_ip: System.get_env("DIAMETER_LISTEN_IP", "0.0.0.0"), #
Todas las interfaces
# 0 interfaz específica:
# listen_ip: "10.7.25.186",

# Interfaz API
config :hss, HssWeb.Api.Endpoint,
  http: [
    ip: {0, 0, 0, 0}, # Todas las interfaces
    port: 8443
  ]

# Interfaz del Panel de Control
config :hss, HssWeb.ControlPanel.Endpoint,
  http: [
    ip: {0, 0, 0, 0}, # Todas las interfaces
    port: 7443
  ]
```

Opciones de Vínculo de Interfaz:



Configuración de IMS

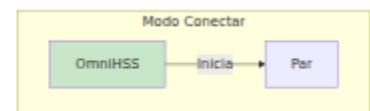
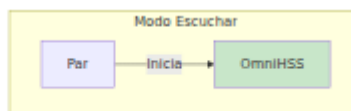
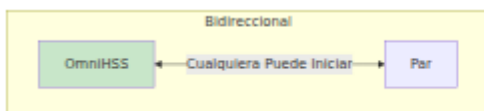
Configuración de Selección de S-CSCF

```
# config/runtime.exs

config :hss, :ims, %{
  scscf: %{
    # Método de selección: :random_peer o :round_robin
    selection_method: :random_peer,

    # Lista de pares S-CSCF disponibles
    peers: [
      %{
        host:
        "sip:scscf01.ims.mnc001.mcc001.3gppnetwork.org:5060",
        capabilities: [] # Opcional: coincidencia de capacidades
      },
      %{
        host:
        "sip:scscf02.ims.mnc001.mcc001.3gppnetwork.org:5060",
        capabilities: []
      }
    ]
  }
}
```

Métodos de Selección de S-CSCF



Métodos de Selección:

Método	Descripción	Caso de Uso
<code>: random_peer</code>	Selecciona aleatoriamente un S-CSCF	Distribución de carga uniforme
<code>: round_robin</code>	Asigna S-CSCF de manera secuencial	Distribución predecible

Configuración del Realm de IMS

Típicamente, IMS utiliza un realm separado del EPC:

```
# Realm EPC
"epc.mnc001.mcc001.3gppnetwork.org"

# Realm IMS
"ims.mnc001.mcc001.3gppnetwork.org"
```

Configuración de EIR

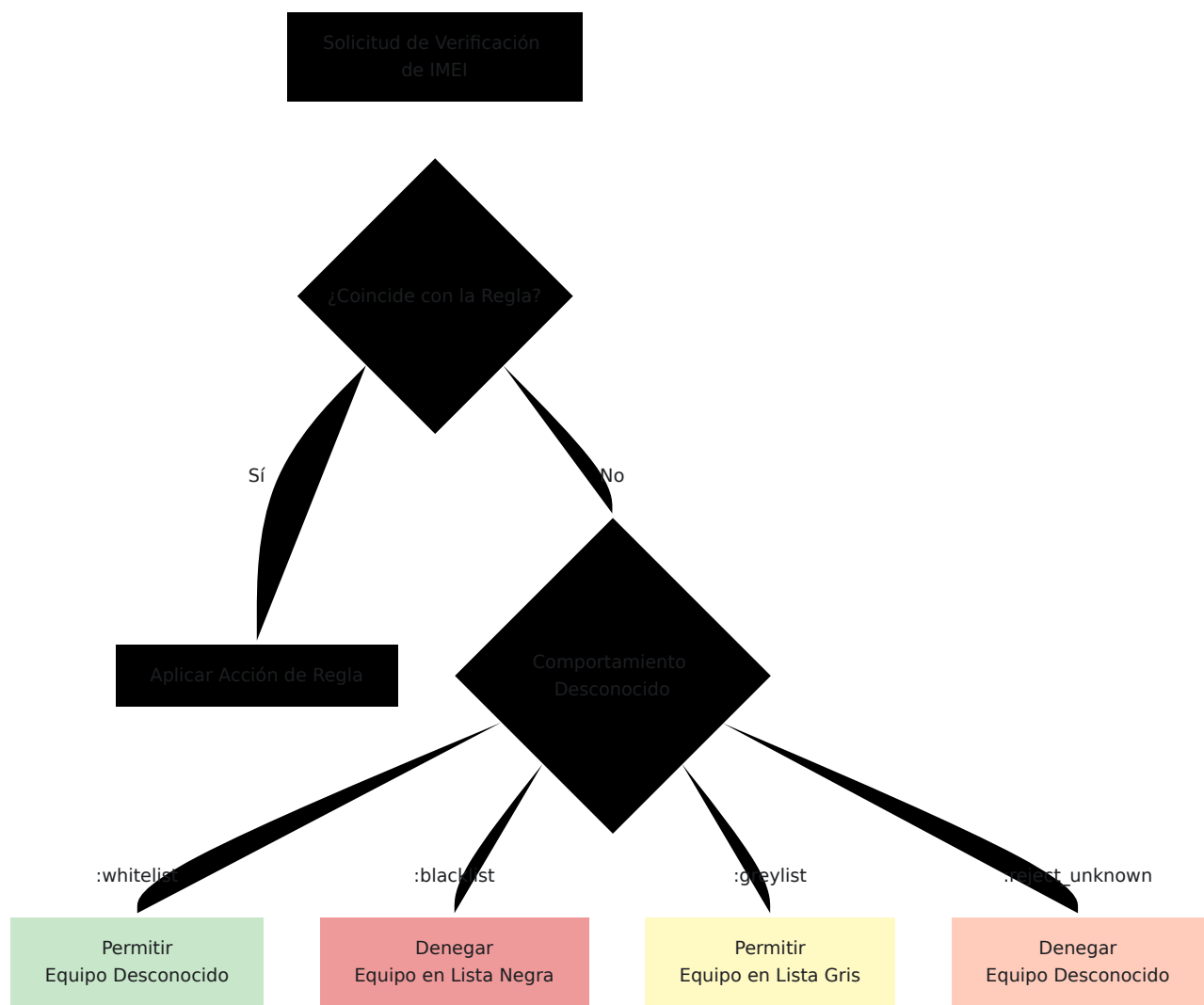
Consulte la [Documentación de EIR](#) para obtener detalles completos sobre la verificación de identidad del equipo.

Configuración del Registro de Identidad del Equipo

```
# config/runtime.exs

config :hss, :eir, %{
  # Comportamiento para equipos desconocidos (sin regla
  # coincidente)
  unknown_equipment_behaviour: :whitelist
  # Opciones:
  #   :whitelist - Permitir equipos desconocidos
  #   :blacklist - Bloquear equipos desconocidos
  #   :greylist - Rastrear pero permitir equipos desconocidos
  #   :reject_unknown_equipment - Rechazar con código de resultado
  # específico
}
```

Comportamiento de Equipos Desconocidos



Opciones de Comportamiento:

Opción	Resultado	Caso de Uso
:whitelist	Permitir todos los IMEI desconocidos	Red abierta, pruebas
:blacklist	Bloquear todos los IMEI desconocidos	Seguridad moderada
:greylist	Permitir pero rastrear IMEI desconocidos	Modo de monitoreo
:reject_unknown_equipment	Rechazar con código específico	Alta seguridad

Recomendación: Comience con :whitelist durante las pruebas, pase a :greylist para el monitoreo en producción, luego :blacklist para una seguridad estricta.

Configuración de la API y del Panel de Control

Configuración del Punto Final de la API

```
# config/config.exs

config :hss, HssWeb.Api.Endpoint,
  url: [host: "localhost"],
  render_errors: [view: HssWeb.ErrorView, accepts: ~w(json)],
  pubsub_server: Hss.PubSub,

# Configuración de HTTPS
https: [
  port: 8443,
  cipher_suite: :strong,
  certfile: "priv/cert/omnitouch.crt",
  keyfile: "priv/cert/omnitouch.pem"
]
```

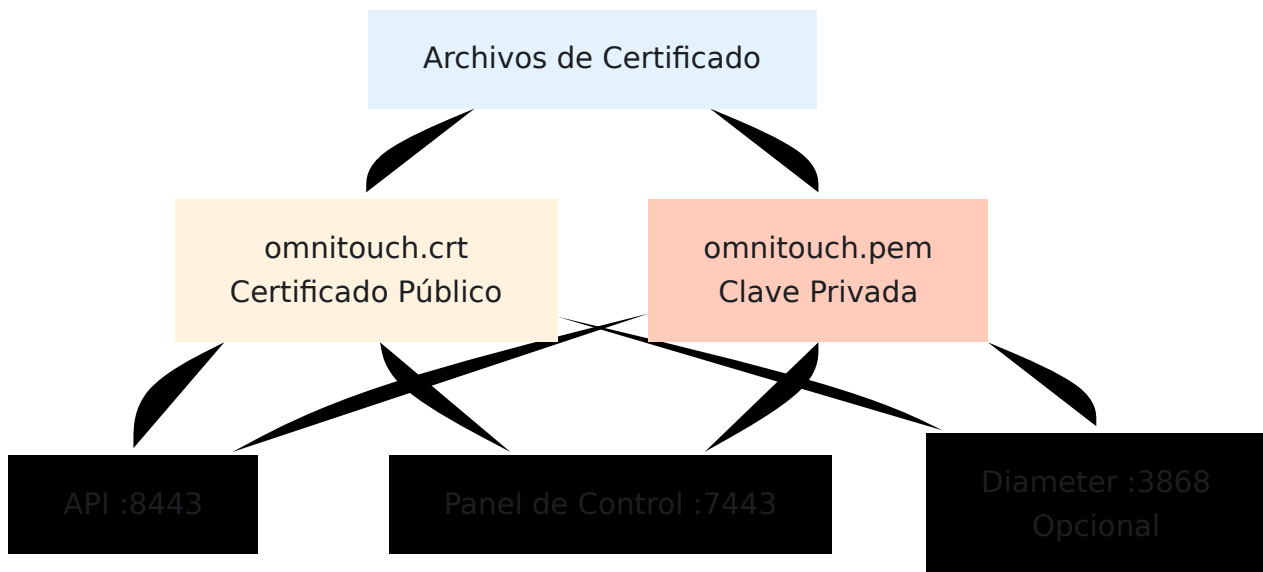
Configuración del Panel de Control

```
# config/config.exs

config :hss, HssWeb.ControlPanel.Endpoint,
  url: [host: "localhost"],
  render_errors: [view: HssWeb.ErrorView, accepts: ~w(html json)],
  pubsub_server: Hss.PubSub,
  live_view: [signing_salt: "some-secret"],

# Configuración de HTTPS
https: [
  port: 7443,
  cipher_suite: :strong,
  certfile: "priv/cert/omnitouch.crt",
  keyfile: "priv/cert/omnitouch.pem"
]
```

Configuración del Certificado TLS



Requisitos del Certificado:

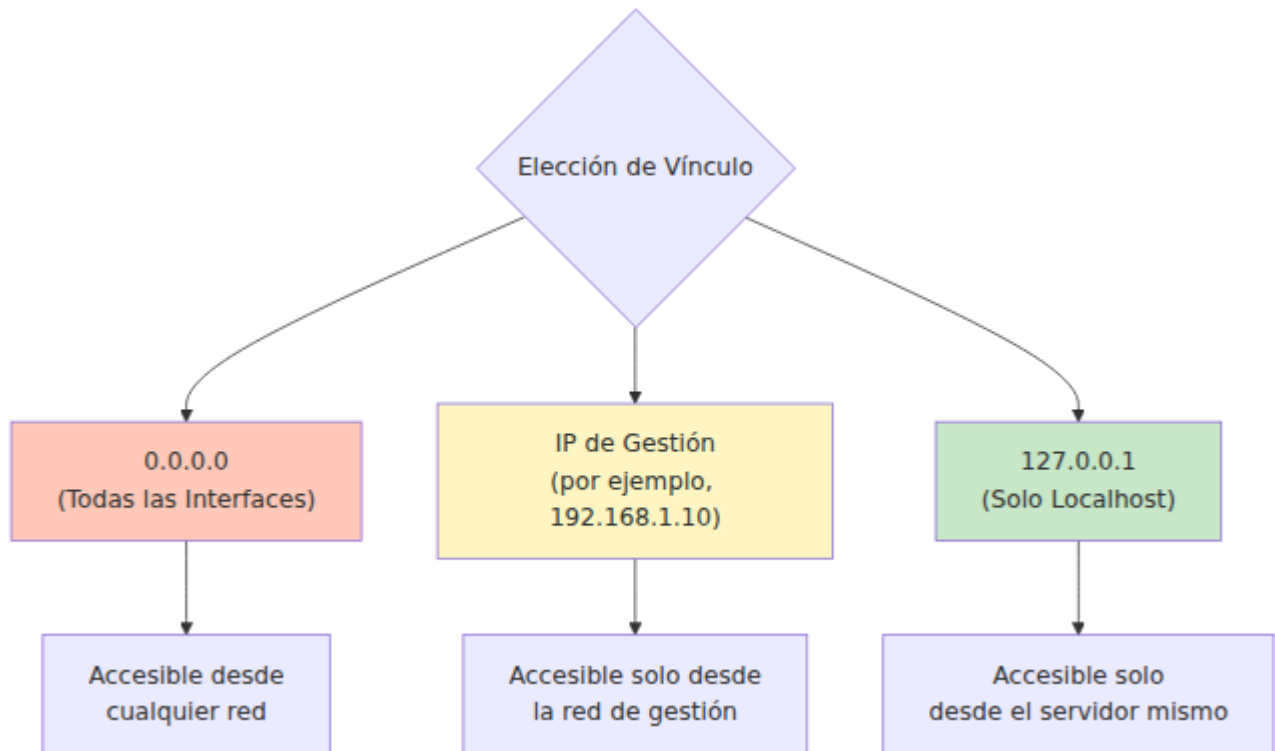
- Certificado X.509 válido
- Clave privada coincidente
- Incluir certificados intermedios si es necesario
- CN o SAN debe coincidir con el nombre de host

Para Producción:

```
https: [  
  port: 8443,  
  cipher_suite: :strong,  
  certfile: System.get_env("TLS_CERT_FILE",  
    "/etc/ssl/certs/omnihss.crt"),  
  keyfile: System.get_env("TLS_KEY_FILE",  
    "/etc/ssl/private/omnihss.key"),  
  cacertfile: System.get_env("TLS_CA_FILE", "/etc/ssl/certs/ca-  
    bundle.crt")  
]
```

Flujo de Trabajo de Configuración

Configuración Inicial de Despliegue



Lista de Verificación de Configuración

Configuración Esencial

- ☐ Conexión a la base de datos (nombre de host, credenciales)
- ☐ PLMN de Inicio (MCC, MNC)
- ☐ Host y realm de Diameter
- ☐ IP y puerto de escucha de Diameter
- ☐ Certificados TLS para API y Panel de Control
- ☐ Configuración del cliente de licencias (URLs del servidor, licensee, product_name)
- ☐ Ajustes del núcleo HSS (send_clr_on_mme_change, stop_diameter_on_database_failure)

Integración de Elementos de Red

- ☐ Pares de Diameter configurados (si se utiliza el modo conectar)
- ☐ Reglas de firewall permiten tráfico de Diameter (puerto 3868)
- ☐ Reglas de firewall permiten tráfico HTTPS (puertos 7443, 8443)
- ☐ Resolución DNS para identidades de Diameter

Configuración de IMS (si se utilizan funciones de IMS)

- ☐ Lista de pares S-CSCF configurada
- ☐ Método de selección de S-CSCF elegido
- ☐ Realm de IMS configurado

Configuración Opcional

- ☐ Comportamiento de EIR configurado
- ☐ Tamaño del grupo de base de datos ajustado
- ☐ Vínculo de interfaz de red restringido

Verificación de la Configuración

Después de modificar la configuración:

1. Verificación de Sintaxis:

Verifique los registros en busca de errores de carga de configuración

2. Acceso al Panel de Control:

Acceda a `https://[nombre de host]:7443`
Verifique que se cargue la página de Resumen

3. Acceso a la API:

```
curl -k https://[nombre de host]:8443/api/status
```

4. Estado de Diameter:

Verifique la página de Diameter en el Panel de Control
Verifique las conexiones de pares

5. **Conectividad de la Base de Datos:**

Verifique el Panel de Control para datos de suscriptores
O conéctese directamente a la base de datos SQL

Ejemplo Completo de Configuración en Tiempo de

Ejecución

```
# config/runtime.exs - Ejemplo completo de producción
```

```
import Config
```

```
#
```

```
=====
```

```
# CONFIGURACIÓN DE LA BASE DE DATOS
```

```
#
```

```
=====
```

```
config :hss, Hss.Repo,
```

```
  username: System.fetch_env!("DATABASE_USERNAME"),
```

```
  password: System.fetch_env!("DATABASE_PASSWORD"),
```

```
  hostname: System.get_env("DATABASE_HOSTNAME", "db.omnihss.internal"),
```

```
  database: System.get_env("DATABASE_NAME", "omnihss"),
```

```
  port: String.to_integer(System.get_env("DATABASE_PORT", "5432")),
```

```
  pool_size: String.to_integer(System.get_env("DATABASE_POOL_SIZE", "10")),
```

```
  timeout: 15_000,
```

```
  connect_timeout: 15_000,
```

```
  ssl: true,
```

```
  ssl_opts: [
```

```
    cacertfile: "/etc/ssl/certs/postgres-ca.pem",
```

```
    verify: :verify_peer
```

```
  ]
```

```
#
```

```
=====
```

```
# CONFIGURACIÓN DEL CLIENTE DE LICENCIAS
```

```
#
```

```
=====
```

```
config :license_client,
```

```
  license_server_api_urls: [System.get_env("LICENSE_SERVER_URL",
```

```
"https://license.example.com:8443/api")],
```

```
  licensee: System.get_env("LICENSE_ORGANIZATION", "Su Organización"),
```

```
  product_name: "omnihss"
```

```
#
```

```
=====
```

```
# CONFIGURACIÓN DEL PLMN DE INICIO Y DEL NÚCLEO HSS
```

```
#
```

```
=====
```

```

config :hss,
  ecto_repos: [Hss.Repo],
  home_plmn: %{
    mcc: System.get_env("HOME_PLMN_MCC", "001"),
    mnc: System.get_env("HOME_PLMN_MNC", "001")
  },
  send_clr_on_mme_change: true,
  stop_diameter_on_database_failure: true,
  license_enforced: true,
  license_module: LicenseClient

#
=====
# CONFIGURACIÓN DE DIAMETER
#
=====
diameter_config = %{
  service_name: :omnitouch_hss,
  listen_ip: System.get_env("DIAMETER_LISTEN_IP", "10.7.25.186"),
  listen_port: String.to_integer(System.get_env("DIAMETER_LISTEN_PORT", "3868")),
  host: System.get_env("DIAMETER_HOST", "omnihss01"),
  realm: System.get_env("DIAMETER_REALM", "epc.mnc001.mcc001.3gppnetwork.org"),
  product_name: "OmniHSS",
  vendor_id: 10415,
  supported_vendor_ids: [5535, 10415],
  request_timeout: 5000,
  peers: [
    %{
      host: "mme01.epc.mnc001.mcc001.3gppnetwork.org",
      realm: "epc.mnc001.mcc001.3gppnetwork.org",
      ip: "10.7.25.100",
      port: 3868,
      transport: :sctp,
      applications: [:s6a]
    }
  ]
}

config :hss, :diameter, diameter_config

#
=====

```

```
# CONFIGURACIÓN DE IMS
```

```
#
```

```
=====
config :hss, :ims, %{
  scscf: %{
    selection_method: :random_peer,
    peers: [
      %{host: "sip:scscf01.ims.mnc001.mcc001.3gppnetwork.org:5060"},
      %{host: "sip:scscf02.ims.mnc001.mcc001.3gppnetwork.org:5060"}
    ]
  }
}
```

```
#
```

```
=====
# CONFIGURACIÓN DE EIR
#
=====
config :hss, :eir, %{
  unknown_equipment_behaviour: :whitelist
}
```

```
#
```

```
=====
# CONFIGURACIÓN DEL PUNTO FINAL DE LA API
#
=====
config :hss, HssWeb.Api.Endpoint,
  http: [ip: {0, 0, 0, 0}, port: 8443],
  https: [
    port: 8443,
    cipher_suite: :strong,
    certfile: System.get_env("TLS_CERT_FILE", "/etc/ssl/certs/omnihss"),
    keyfile: System.get_env("TLS_KEY_FILE", "/etc/ssl/private/omnihss"),
  ],
  url: [host: System.get_env("API_HOST", "api.omnihss.internal"), port: 8443]
```

```
#
```

```
=====
# CONFIGURACIÓN DEL PUNTO FINAL DEL PANEL DE CONTROL
#
=====
config :hss, HssWeb.ControlPanel.Endpoint,
```

```
http: [ip: {0, 0, 0, 0}, port: 7443],
https: [
  port: 7443,
  cipher_suite: :strong,
  certfile: System.get_env("TLS_CERT_FILE", "/etc/ssl/certs/omnihss"),
  keyfile: System.get_env("TLS_KEY_FILE", "/etc/ssl/private/omnihss"),
],
url: [host: System.get_env("CP_HOST", "hss.omnihss.internal"), port
```

[← Volver a la Guía de Operaciones](#) | [Siguiente: Relaciones de Entidad](#) →

Guía del Panel de Control de OmniHSS

[← Volver a la Guía de Operaciones](#)

Tabla de Contenidos

- [Descripción General del Panel de Control](#)
 - [Acceso al Panel de Control](#)
 - [Página de Resumen](#)
 - [Página de Diámetro](#)
 - [Página de Aplicación](#)
 - [Página de Configuración](#)
 - [Navegación e Interfaz](#)
-

Descripción General del Panel de Control

El Panel de Control de OmniHSS es una interfaz de monitoreo basada en la web que proporciona visibilidad en tiempo real del estado del sistema, la actividad de los suscriptores y la conectividad de Diámetro. Construido con Phoenix LiveView, se actualiza automáticamente sin requerir recargas de página.

Características Clave

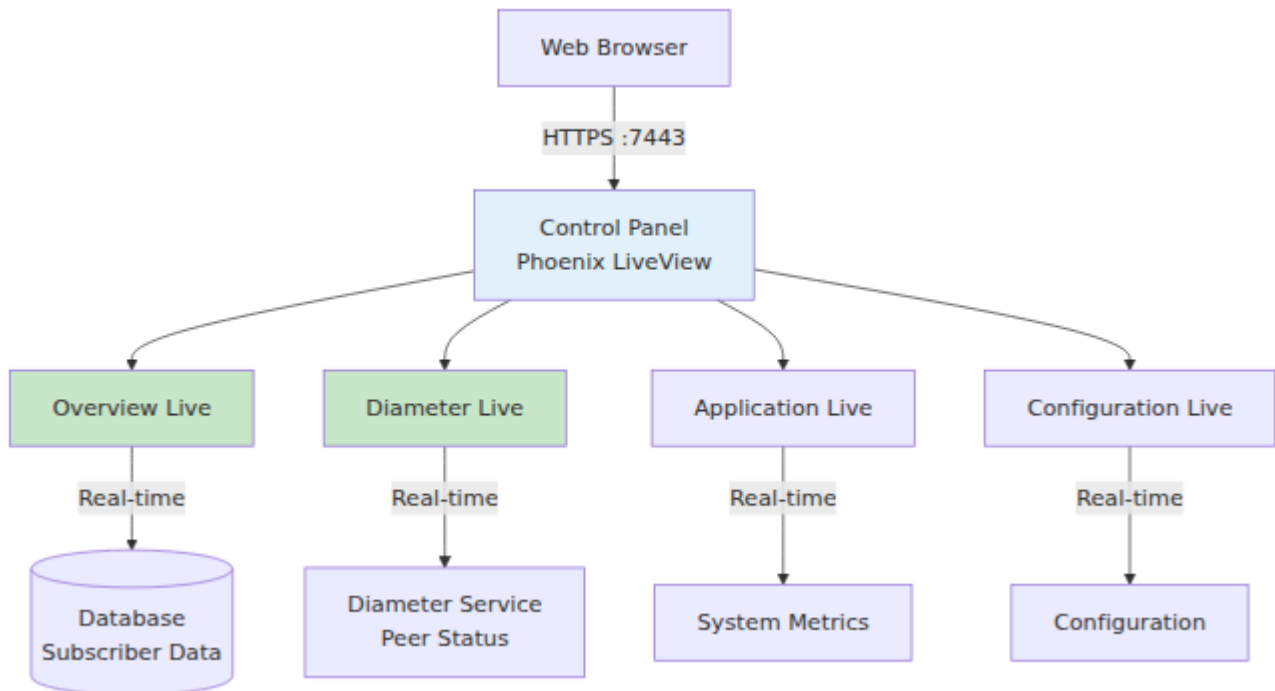
- **Actualizaciones en Tiempo Real** - Se actualiza automáticamente cada segundo
- **Monitoreo de Suscriptores** - Ver suscriptores activos y su estado actual
- **Estado de Diámetro** - Monitorear conexiones de pares en tiempo real

- **Recursos del Sistema** - Rastrear el rendimiento de la aplicación
- **Visor de Configuración** - Inspeccionar la configuración en tiempo de ejecución

Información de Acceso

URL: `https://[hostname]:7443`
Protocolo: Solo HTTPS
Puerto: 7443 (configurable)
Certificado: Configurado en `config/config.exs`

Arquitectura del Panel de Control



Acceso al Panel de Control

Acceso Inicial

1. Abre un navegador web
2. Navega a `https://[hostname]:7443`

3. Acepta el certificado TLS (si es autofirmado)
4. Se te presentará la página de Resumen por defecto

Advertencias de Certificado TLS

Si se utilizan certificados autofirmados, los navegadores mostrarán advertencias de seguridad. Esto es esperado para implementaciones internas.

Para Producción: Utiliza certificados firmados por una Autoridad de Certificación de confianza.

Requisitos de Red

- **El puerto 7443** debe ser accesible desde tu red de gestión
- **HTTPS** es obligatorio - HTTP no es compatible
- **Las reglas del firewall** deben permitir tráfico al puerto 7443

Compatibilidad del Navegador

El Panel de Control utiliza tecnologías web modernas (LiveView, WebSockets):

- Chrome/Chromium (recomendado)
- Firefox
- Safari
- Edge

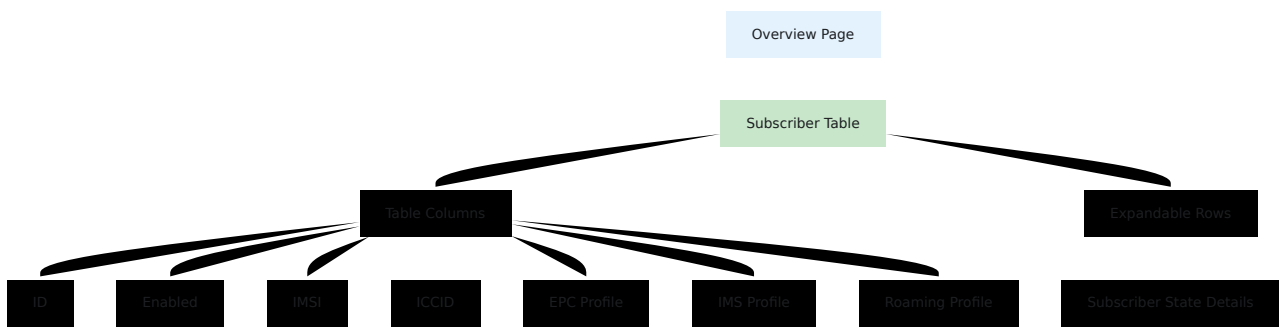
Nota: Internet Explorer no es compatible.

Página de Resumen

URL: `https://[hostname]:7443/overview`

La página de Resumen muestra todos los suscriptores y su información de estado en tiempo real.

Diseño de la Página



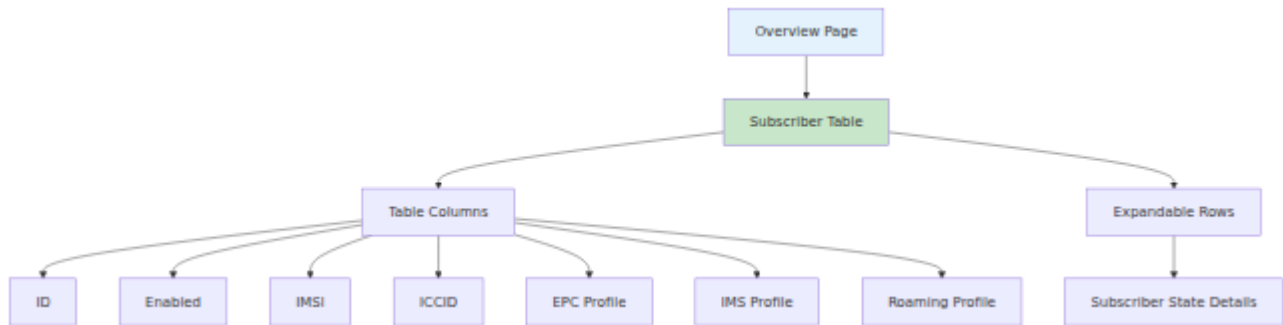
Columnas de la Tabla

Columna	Descripción	Valores
ID	ID de base de datos del suscriptor	Cadena (UUID)
Enabled	Estado del servicio	✓ (habilitado) / ✗ (deshabilitado)
IMSI	Identidad de Suscriptor Móvil Internacional	14-15 dígitos
ICCID	ID de la tarjeta SIM	19-20 dígitos o "N/A"
EPC Profile	Nombre del perfil de servicio de datos	Nombre o ID del perfil
IMS Profile	Nombre del perfil de servicio de voz	Nombre del perfil, ID, o "N/A"
Roaming Profile	Nombre de la política de roaming	Nombre del perfil, ID, o "N/A"

Detalles de Filas Expandibles

Haz clic en cualquier fila para expandir y ver el estado detallado del suscriptor:

Información de Ubicación



Campos:

- **MCC** - Código de País Móvil (3 dígitos)
- **MNC** - Código de Red Móvil (2-3 dígitos)
- **TAC** - Código de Área de Seguimiento
- **Cell ID** - Identificador de la celda de servicio
- **eNodeB ID** - Identificador de la estación base
- **ECI** - Identificador de Celda E-UTRAN

Información de Red

Campos:

- **Último MME Visto** - Nombre de host del MME de servicio actual
- **Último Reino Visto** - Reino de Diámetro del MME
- **Tipo de RAT** - Tecnología de Acceso Radio (por ejemplo, "E-UTRAN" para LTE)
- **Último Visto En** - Marca de tiempo del último mensaje de Diámetro

Información de IMS

Campos:

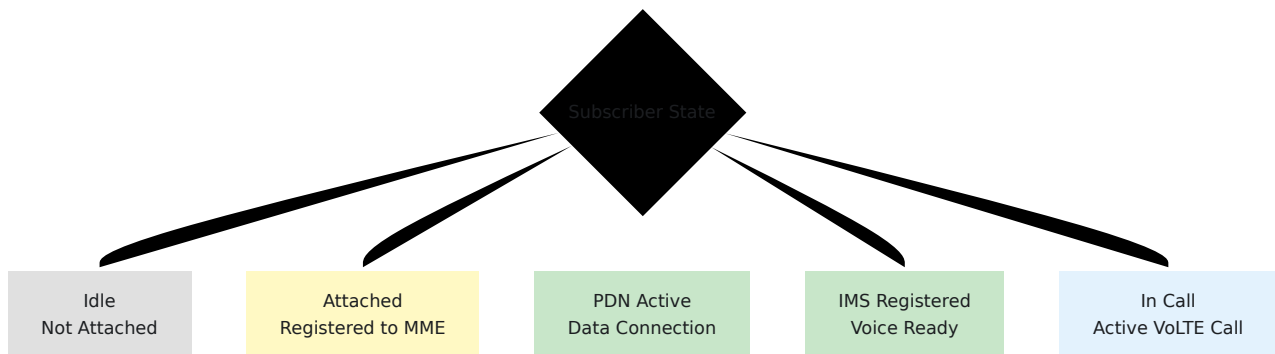
- **S-CSCF Asignado** - URI SIP S-CSCF actualmente asignado
- **Identidad Pública IMS** - URI SIP (por ejemplo, sip:**+14155551234@ims.example.com**)
- **Último P-CSCF Visto** - Último P-CSCF que contactó al HSS
- **Último I-CSCF Visto** - Último I-CSCF que contactó al HSS

Información de Sesión

Campos:

- **Sesiones PDN** - Número de conexiones de datos activas
- **Llamadas Activas** - Número de llamadas VoLTE activas

Indicadores de Estado



Cómo identificar el estado:

- **Idle:** Sin información de ubicación, sin MME
- **Attached:** Último MME Visto presente, información de ubicación disponible
- **PDN Active:** Conteo de sesiones PDN > 0
- **IMS Registered:** S-CSCF Asignado presente
- **In Call:** Conteo de llamadas activas > 0

Auto-Actualización

La página de Resumen se actualiza automáticamente **cada 1 segundo** para mostrar actualizaciones en tiempo real.

Indicadores visuales:

- Nuevos datos aparecen sin recarga de página
- Las marcas de tiempo se actualizan en tiempo real
- No se necesita actualización manual

Casos de Uso

1. Monitorear Suscriptores Activos

- Ver qué suscriptores están actualmente adjuntos
- Comprobar la red de servicio actual (para roaming)
- Verificar el estado de registro IMS

2. Resolución de Problemas

- Verificar que el suscriptor esté habilitado
- Comprobar la marca de tiempo del último visto (¿el suscriptor responde?)
- Confirmar asignaciones de perfil
- Ver información de ubicación actual

3. Monitoreo de Capacidad

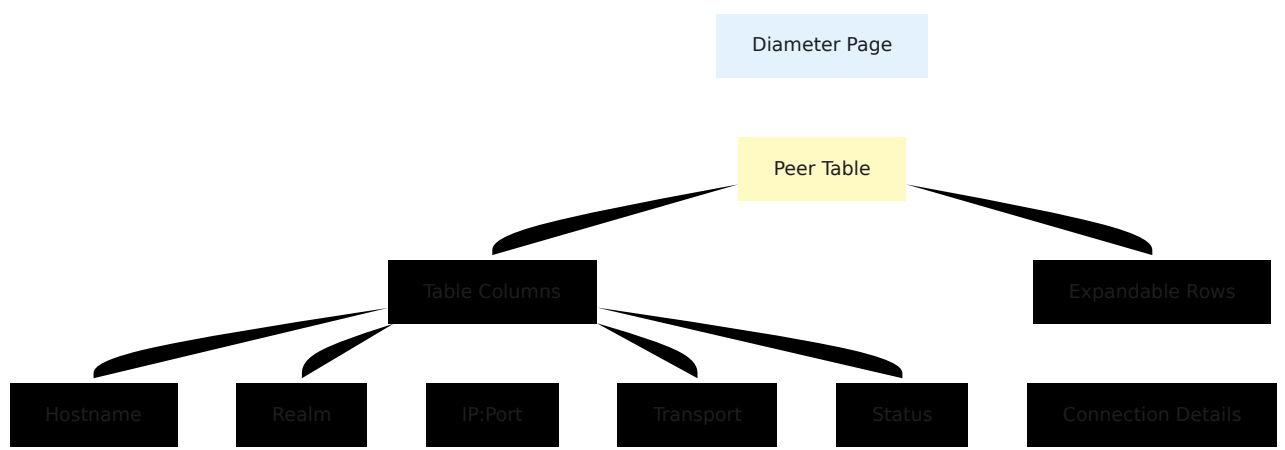
- Contar el total de suscriptores adjuntos
- Monitorear conteos de sesiones PDN
- Rastrear llamadas VoLTE activas

Página de Diámetro

URL: `https://[hostname]:7443/diameter`

La página de Diámetro muestra el estado en tiempo real de todas las conexiones de pares de Diámetro.

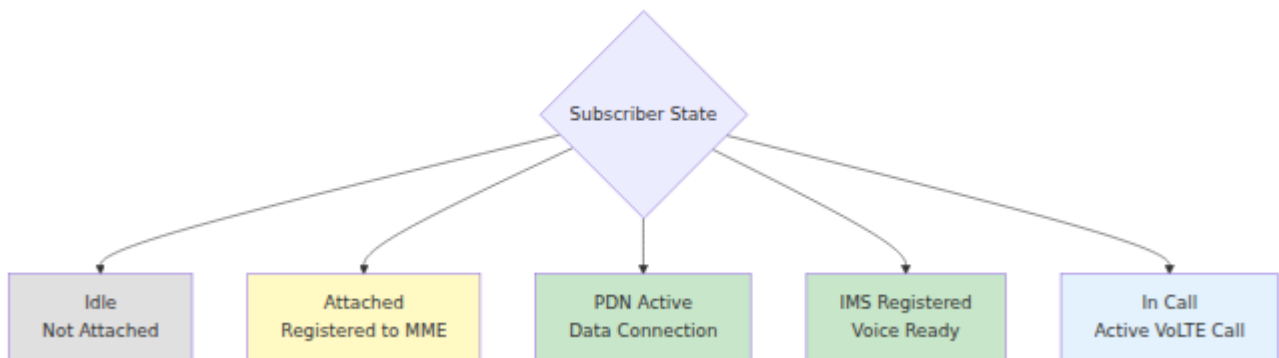
Diseño de la Página



Columnas de la Tabla

Columna	Descripción	Valores
Hostname	Nombre de host del par de Diámetro	FQDN
Realm	Reino de Diámetro	Nombre de dominio
IP:Port	Dirección de red	Dirección IP y puerto
Transport	Protocolo de transporte	TCP o SCTP
Status	Estado de la conexión	Conectado / Desconectado

Estado de la Conexión



Detalles de Filas Expandibles

Haz clic en cualquier par para ver información adicional:

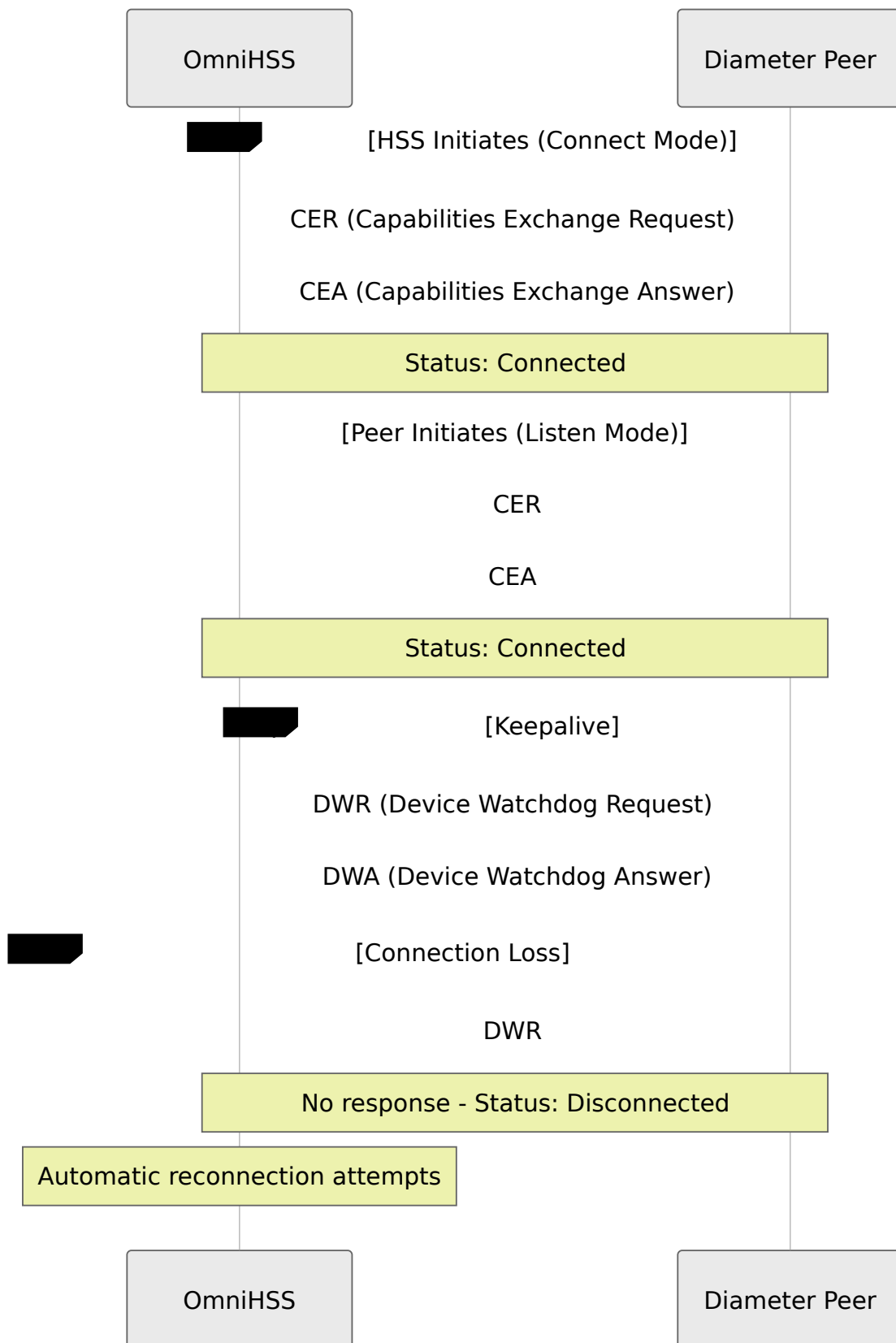
Información de Conexión:

- **Tipo de Conexión** - Iniciada por HSS o par
- **Nombre del Producto** - Identificación del producto del par
- **IDs de Aplicación** - Aplicaciones de Diámetro soportadas

Ejemplos de ID de Aplicación:

- 16777251 - S6a (MME)
- 16777238 - Gx (P-GW)
- 16777216 - Cx (I-CSCF, S-CSCF)
- 16777217 - Sh (Application Server)
- 16777236 - Rx (P-CSCF)
- 16777252 - S13 (cliente EIR, si es externo)

Flujo de Conexión de Pares



Auto-Actualización

La página de Diámetro se actualiza automáticamente **cada 1 segundo**.

Casos de Uso

1. Verificar Conectividad

- Asegurarse de que todos los pares esperados estén conectados
- Identificar pares desconectados de inmediato
- Monitorear conexiones inestables

2. Resolución de Problemas

- Comprobar si el par es accesible
- Verificar el protocolo de transporte (TCP vs SCTP)
- Confirmar que los IDs de aplicación coincidan con las expectativas
- Identificar qué lado inició la conexión

3. Planificación de Capacidad

- Contar el total de pares conectados
- Monitorear la estabilidad de la conexión
- Planificar capacidad adicional para pares

Problemas Comunes

El Par Muestra Desconectado

Posibles Causas:

1. Problema de conectividad de red
2. El par está caído o reiniciándose
3. Firewall bloqueando tráfico
4. Desajuste de configuración de Diámetro
5. Problema de certificado (si se utiliza TLS)

Pasos de Resolución de Problemas:

1. Comprobar conectividad de red: `ping [peer-ip]`
2. Verificar que el puerto sea accesible: `telnet [peer-ip] 3868`
3. Comprobar reglas del firewall
4. Revisar registros del HSS en busca de mensajes de error
5. Verificar que la configuración de Diámetro del par coincida con el HSS

El Par Se Conecta y Desconecta Repetidamente

Posibles Causas:

1. Inestabilidad de la red
2. Desajuste de tiempo de espera de keepalive
3. Problemas de recursos en el par
4. Desajuste de aplicación de Diámetro

Pasos de Resolución de Problemas:

1. Comprobar estabilidad de la red
2. Revisar temporizadores de keepalive en ambos lados
3. Comprobar recursos del sistema del par
4. Verificar que los IDs de aplicación coincidan en ambos lados

Página de Aplicación

URL: `https://[hostname]:7443/application`

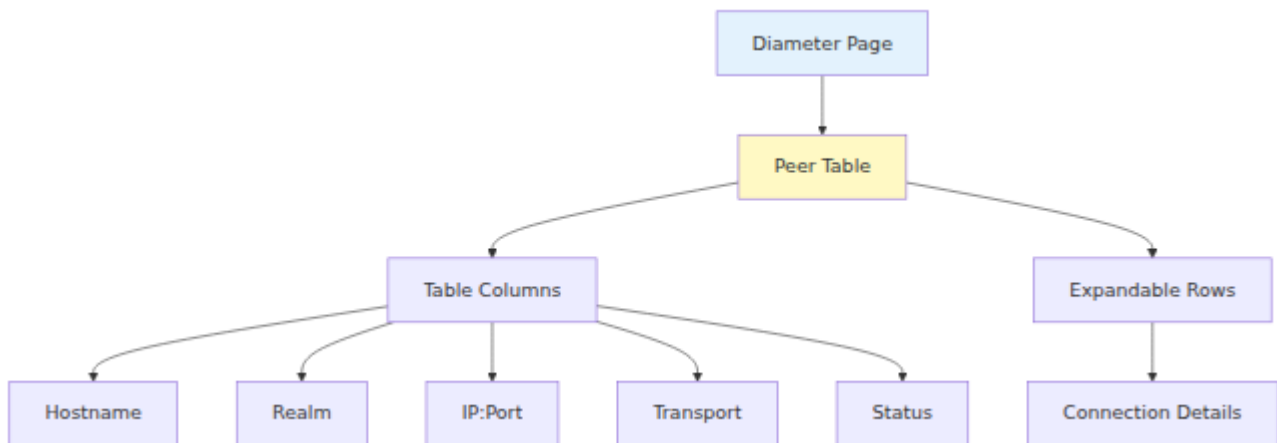
La página de Aplicación proporciona información de monitoreo a nivel de sistema y uso de recursos.

Características

- **Información de Procesos** - Conteo de procesos de la VM de Erlang y memoria
- **Memoria del Sistema** - Memoria total y utilizada

- **Tiempo de Actividad de la Aplicación** - Cuánto tiempo ha estado funcionando OmniHSS
- **Versión de la VM de Erlang** - Información de la versión de tiempo de ejecución

Métricas Clave



Casos de Uso

1. Monitoreo de Salud

- Verificar que la aplicación esté en funcionamiento
- Comprobar fugas de memoria (aumento de memoria con el tiempo)
- Monitorear el crecimiento del conteo de procesos

2. Planificación de Capacidad

- Rastrear tendencias de uso de memoria
- Planificar escalado basado en el conteo de procesos
- Verificar recursos del sistema adecuados

3. Resolución de Problemas

- Identificar agotamiento de recursos
 - Comprobar si es necesario reiniciar
 - Verificar la versión de la VM de Erlang
-

Página de Configuración

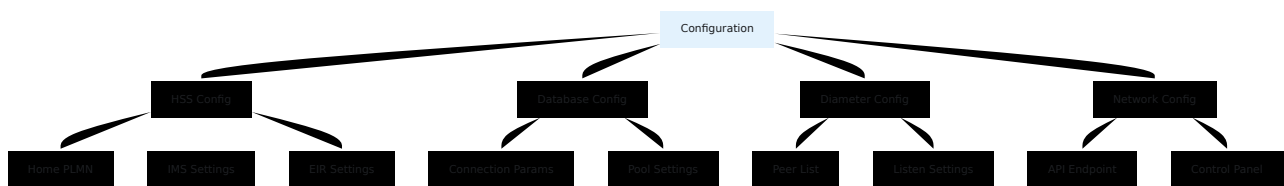
URL: `https://[hostname]:7443/configuration`

La página de Configuración muestra la configuración actual en tiempo de ejecución de OmniHSS.

Características

- **Ver Configuración** - Inspeccionar todos los parámetros de configuración
- **Buscar Configuración** - Encontrar configuraciones específicas
- **Variables de Entorno** - Ver valores resueltos

Categorías de Configuración



Casos de Uso

1. Verificación de Configuración

- Verificar que se apliquen los ajustes de runtime.exs
- Confirmar parámetros de conexión de base de datos
- Comprobar la configuración de pares de Diámetro

2. Resolución de Problemas

- Identificar desajustes de configuración
- Verificar que las variables de entorno estén configuradas correctamente
- Comparar configuración esperada vs real

3. Documentación

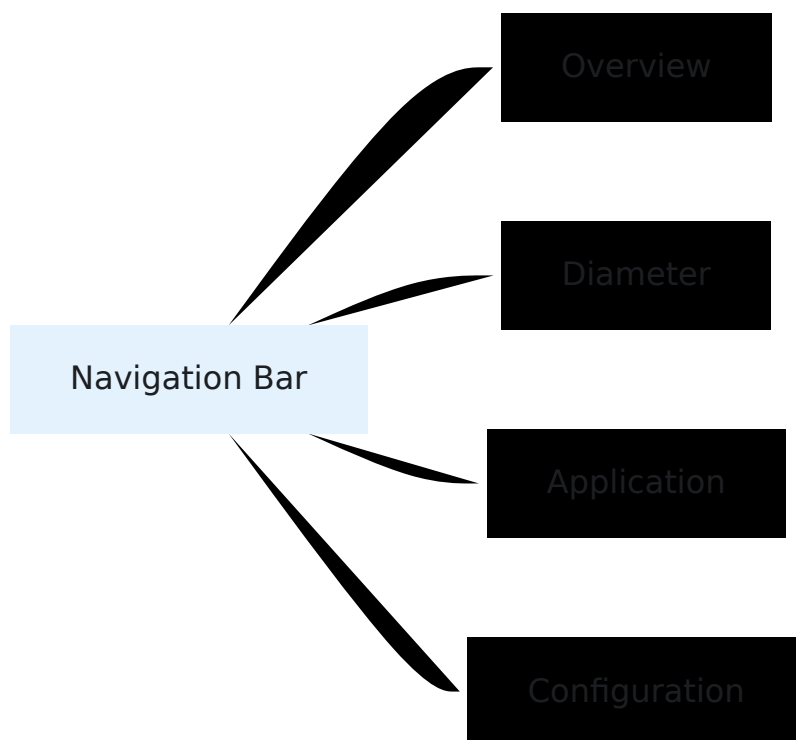
- Exportar la configuración actual para documentación

- Compartir la configuración con el equipo de soporte

Nota de Seguridad: La página de configuración puede mostrar información sensible (contraseñas de base de datos, claves). Restringir el acceso adecuadamente.

Navegación e Interfaz

Barra de Navegación Superior



La navegación siempre es visible en la parte superior de la página para un acceso rápido.

Atajos de Teclado

El Panel de Control no implementa atajos de teclado personalizados. Los atajos estándar del navegador funcionan:

- **Ctrl+R / F5** - Actualización manual de la página (aunque la auto-actualización hace esto innecesario)

- **Ctrl+F** - Buscar en la página
- **Ctrl+T** - Abrir nueva pestaña (para múltiples páginas)

Monitoreo en Múltiples Pestañas

Puedes abrir múltiples páginas del Panel de Control en pestañas separadas del navegador para monitoreo simultáneo:

Configuración de Ejemplo:

- Pestaña 1: Página de Resumen (monitorear suscriptores)
- Pestaña 2: Página de Diámetro (monitorear conectividad)
- Pestaña 3: Página de Aplicación (monitorear recursos)

Todas las pestañas se actualizarán automáticamente de forma independiente.

Diseño Responsivo

El Panel de Control está optimizado para navegadores de escritorio. Los navegadores móviles son compatibles, pero pueden requerir desplazamiento horizontal para las tablas.

Resolución Recomendada: 1920x1080 o superior para una visualización cómoda.

Mejores Prácticas de Monitoreo

Operaciones Diarias

1. Inicio de Turno

- Abrir la página de Resumen del Panel de Control
- Verificar que el número esperado de suscriptores esté adjunto
- Comprobar la página de Diámetro - todos los pares conectados

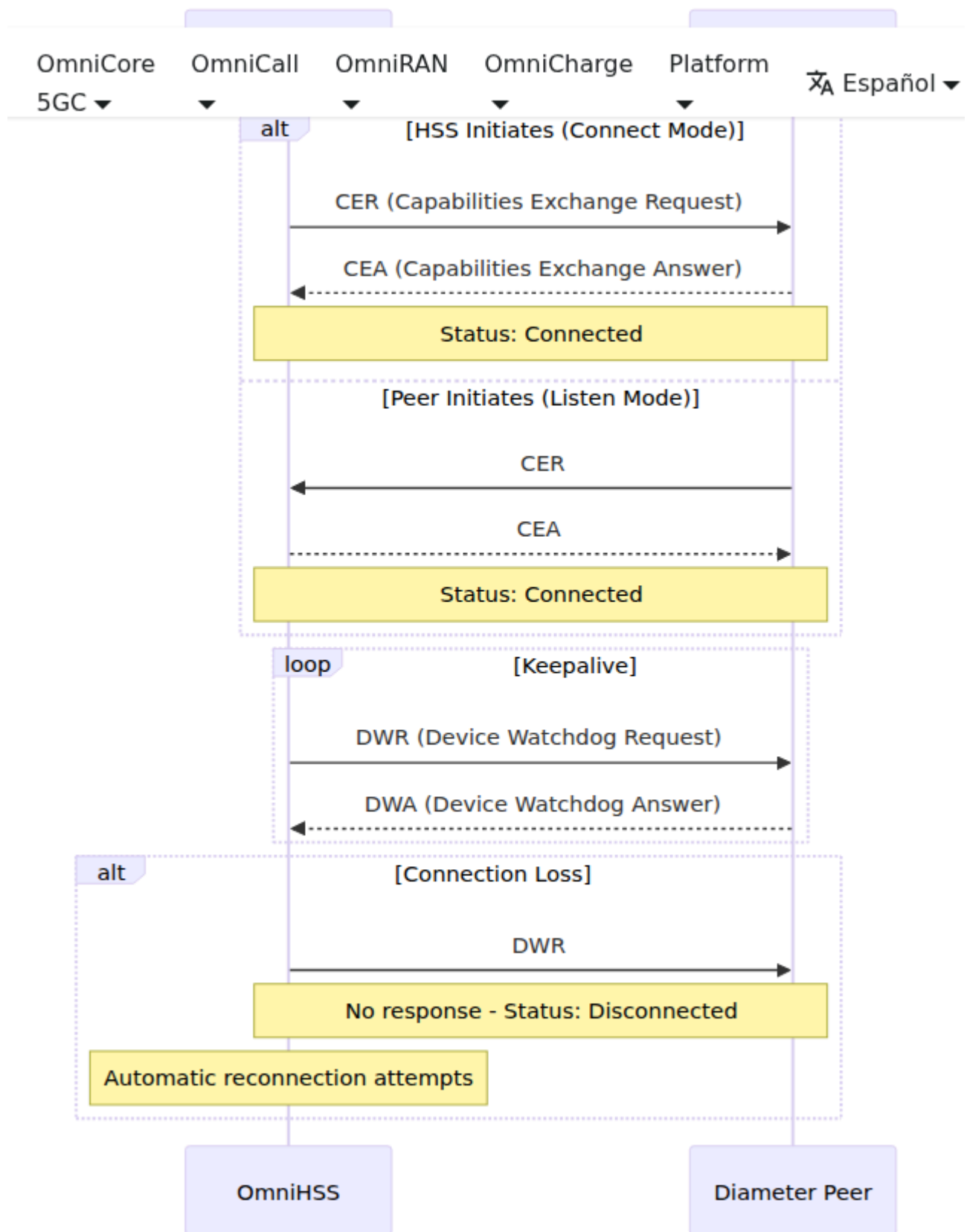
2. Durante el Turno

- Mantener la página de Resumen abierta para monitoreo en tiempo real
- Estar atento a cambios de estado inusuales
- Monitorear pares desconectados en la página de Diámetro

3. Fin de Turno

- Verificar que el sistema esté estable
- Comprobar la página de Aplicación para tendencias de uso de recursos
- Documentar cualquier anomalía

Flujo de Trabajo para Resolución de Problemas



Umbrales de Alerta

Establecer umbrales de monitoreo para alertas proactivas:

Métrica	Advertencia	Crítica
Pares de Diámetro Desconectados	1 par	2+ pares o par crítico
Uso de Memoria	> 80%	> 90%
Fallos de Autenticación de Suscriptores	> 5%	> 10%
Conteo de Procesos	> 80% del límite	> 95% del límite

[← Volver a la Guía de Operaciones](#) | [Siguiente: Métricas y Monitoreo](#) →

Replicación de Base de Datos

[← Volver a la Guía de Operaciones](#)

Tabla de Contenidos

- [Descripción General](#)
 - [Cómo Funciona](#)
 - [Arquitecturas de Despliegue](#)
 - [Referencia de Configuración](#)
 - [Gestión de Pares](#)
 - [Monitoreo](#)
 - [Solución de Problemas](#)
-

Descripción General

OmniHSS utiliza **PostgreSQL** con **replicación lógica bidireccional** para despliegues de alta disponibilidad en múltiples sitios. Cada sitio opera como un primario independiente de lectura/escritura. No hay un maestro único ni réplicas de solo lectura.

Características Clave

- **Ambos Sitios Lectura/Escritura:** Cada sitio tiene una base de datos primaria completa. Las escrituras locales son instantáneas independientemente de la calidad del enlace intersitios.
- **Replicación Asíncrona:** Los cambios se replican a través del Registro de Escritura Adelantada (WAL) de PostgreSQL. Ninguna escritura se bloquea esperando que un sitio remoto reconozca.

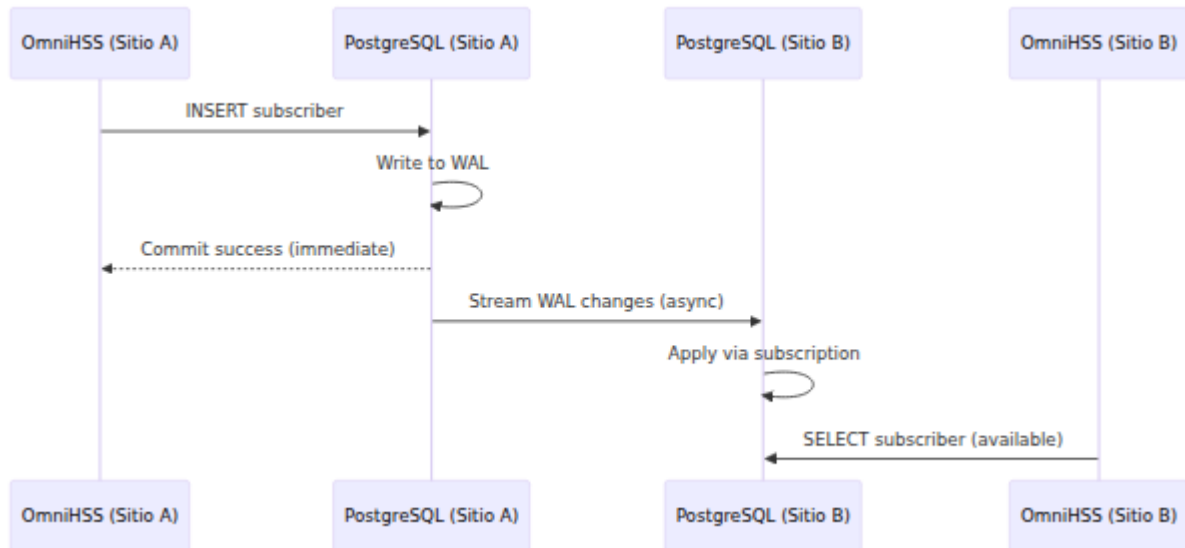
- **Tolerante a Particiones:** Si el enlace intersitios se cae, ambos sitios continúan operando de forma independiente. Los segmentos de WAL se acumulan localmente y se reproducen automáticamente cuando el enlace se recupera.
- **No se Requiere Quórum:** A diferencia de los enfoques de clúster sincrónicos, no hay concepto de quórum. Un despliegue de un solo sitio opera de manera idéntica a un despliegue de múltiples sitios.
- **Claves Primarias UUID:** Todos los registros utilizan claves primarias UUIDv4, eliminando colisiones de ID entre sitios sin coordinación.

Cómo Esto Se Diferencia de la Replicación Sincrónica

	Sincrónica	Replicación Lógica Asincrónica
Latencia de escritura	Bloqueada por el nodo más lento	Solo local: sub-milisegundos
Fallo de enlace	El sitio minoritario se vuelve de solo lectura	Ambos sitios continúan lectura/escritura
Quórum necesario	Sí (mayoría de nodos)	No
Consistencia de datos	Fuerte (todos los nodos idénticos)	Eventual (breve retraso de replicación)
Adecuado para enlaces satelitales	No (la latencia afecta el rendimiento de escritura)	Sí (WAL se acumula y se pone al día)

Cómo Funciona

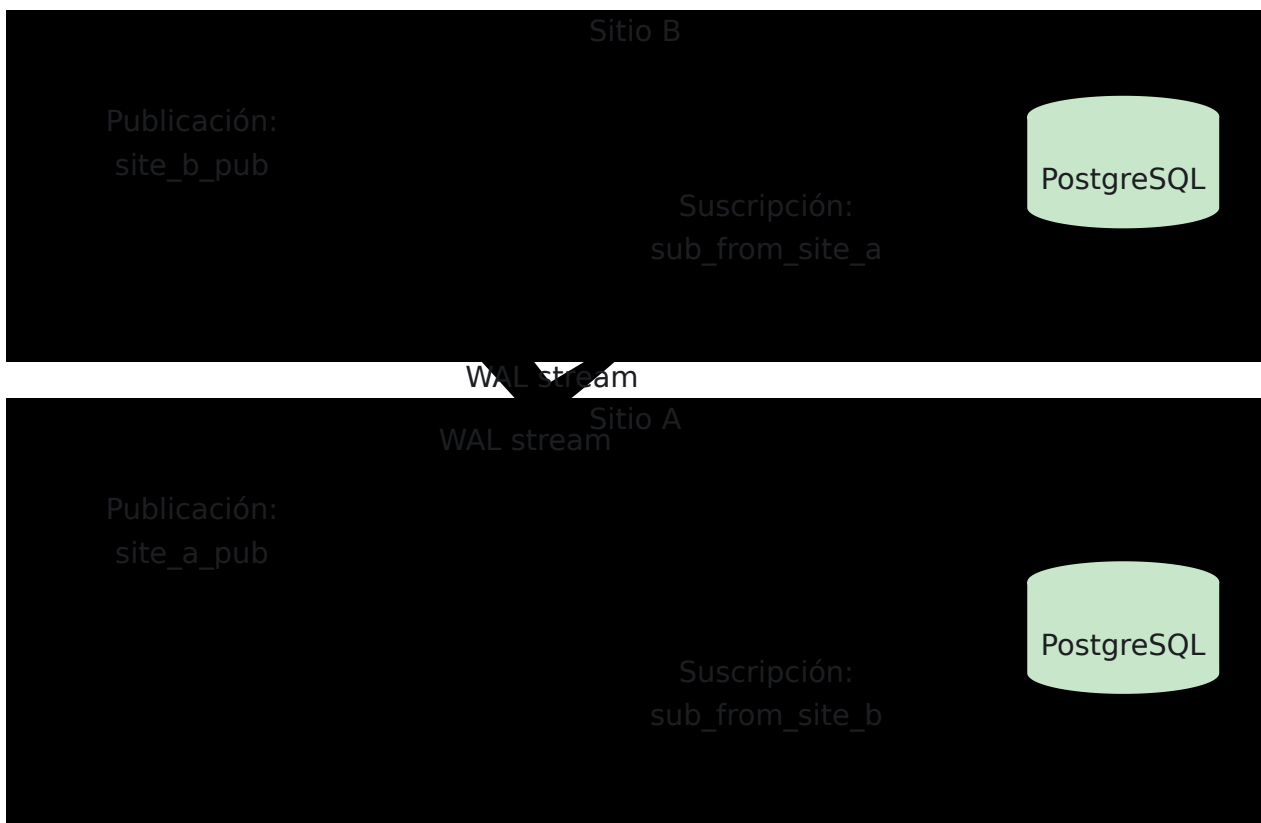
Flujo de Replicación Lógica



Modelo de Publicación / Suscripción

Cada sitio tiene:

- Una **publicación** que transmite todos los cambios de tabla (excepto `schema_migrations`)
- Una **suscripción** a la publicación de cada sitio par



Cola de WAL Durante la Caída del Enlace

Cuando el enlace intersitios no está disponible:

1. Las escrituras locales continúan sin interrupción.
2. Los segmentos de WAL se acumulan en el lado de publicación.
3. El slot de replicación rastrea dónde se quedó cada suscriptor.
4. Cuando el enlace se recupera, el WAL en cola se reproduce desde la última posición reconocida.
5. Ambos sitios convergen a un estado idéntico.

La retención de WAL está limitada por `max_slot_wal_keep_size` para prevenir el crecimiento descontrolado del disco durante caídas prolongadas.

Prevención de Conflictos

Las claves primarias UUID eliminan la fuente principal de conflictos en la replicación bidireccional. Dado que cada sitio genera identificadores únicos globalmente de forma independiente, las operaciones INSERT nunca colisionan.

La opción de suscripción `origin = none` previene bucles de replicación. Los cambios que llegaron a través de la replicación no se vuelven a publicar a otros suscriptores.

La tabla `schema_migrations` se excluye de las publicaciones porque ambos sitios ejecutan migraciones idénticas de forma independiente.

Última Escritura Gana para Estado Dinámico

Las tablas de estado dinámico (`subscriber_state`, `pdn_session`, `lte_call`) se actualizan con frecuencia mediante señalización Diameter. Cada ULR actualiza el MME que sirve, cada CCR actualiza la sesión PGW, y cada AAR actualiza la llamada activa.

En un despliegue de múltiples sitios, un suscriptor es atendido por un sitio a la vez. Cuando el suscriptor se mueve entre sitios, ambos sitios pueden tener actualizaciones a la misma fila de `subscriber_state` de diferentes momentos. Sin resolución de conflictos, el orden de replicación determinaría qué valor sobrevive. Esto podría sobrescribir el MME que sirve actualmente con un valor obsoleto.

OmniHSS utiliza **triggers de Última Escritura Gana (LWW)** en tablas de estado dinámico:

```
CREATE TRIGGER lww_subscriber_state_trigger
  BEFORE UPDATE ON subscriber_state
  FOR EACH ROW
  EXECUTE FUNCTION lww_subscriber_state();
```

El trigger compara la marca de tiempo `updated_at` de la actualización replicada entrante con la fila existente. Si la fila existente es más nueva, la actualización se suprime silenciosamente. Esto asegura:

- Cuando un suscriptor se mueve de Sitio A a Sitio B, la actualización más nueva de Sitio B siempre gana.
- Las actualizaciones obsoletas de Sitio A (de antes de que el suscriptor se moviera) se descartan.
- Ambos sitios convergen al mismo valor: la escritura más reciente.

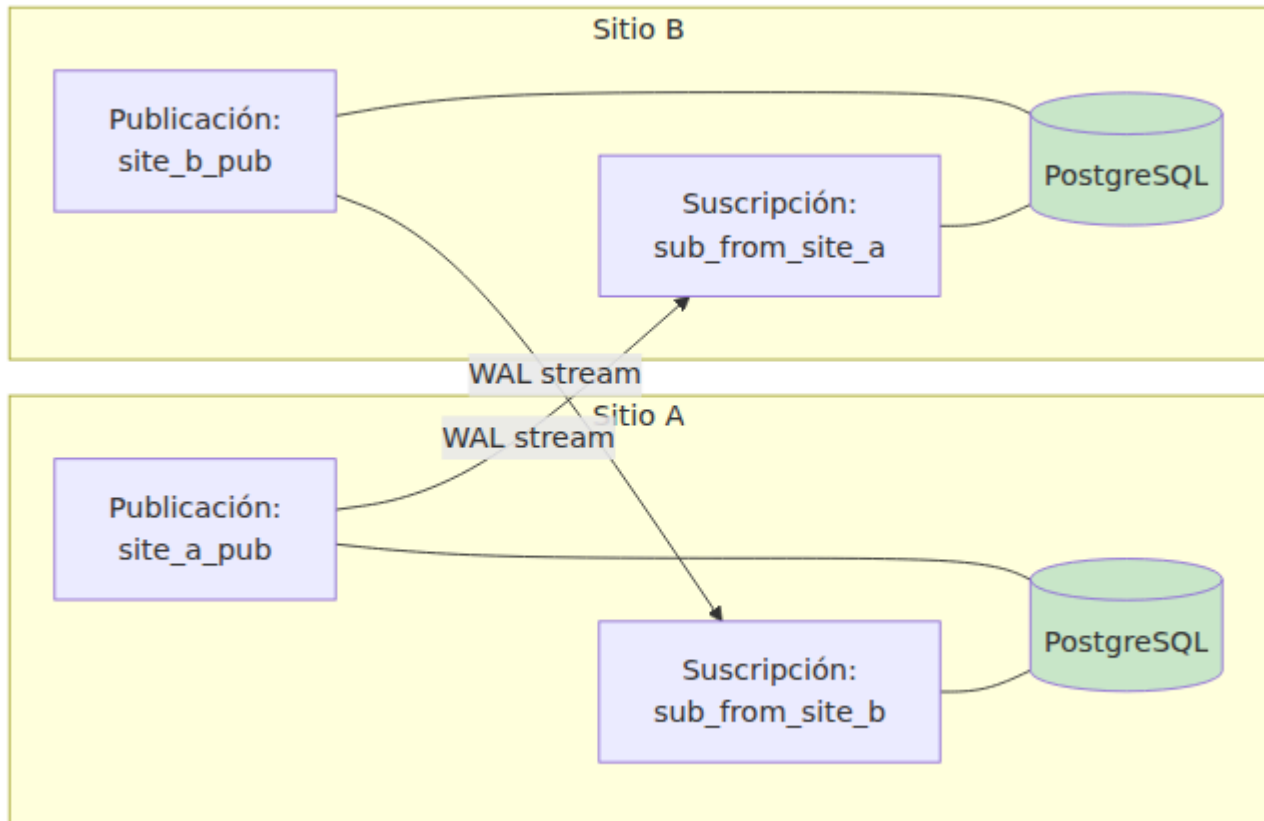
Tablas con triggers LWW:

Tabla	Actualizado Por	Frecuencia
subscriber_state	ULR, SAR, AIR, PUR	Cada actualización de adjunto/ubicación
pdn_session	CCR-I, CCR-T	Cada creación/eliminación de sesión PDN
lte_call	AAR, STR	Cada configuración/desmontaje de llamada VoLTE

Los datos de aprovisionamiento estático (suscriptores, perfiles, claves, APNs) no necesitan LWW. La API de aprovisionamiento solo actualiza estos registros, típicamente desde un solo plano de gestión.

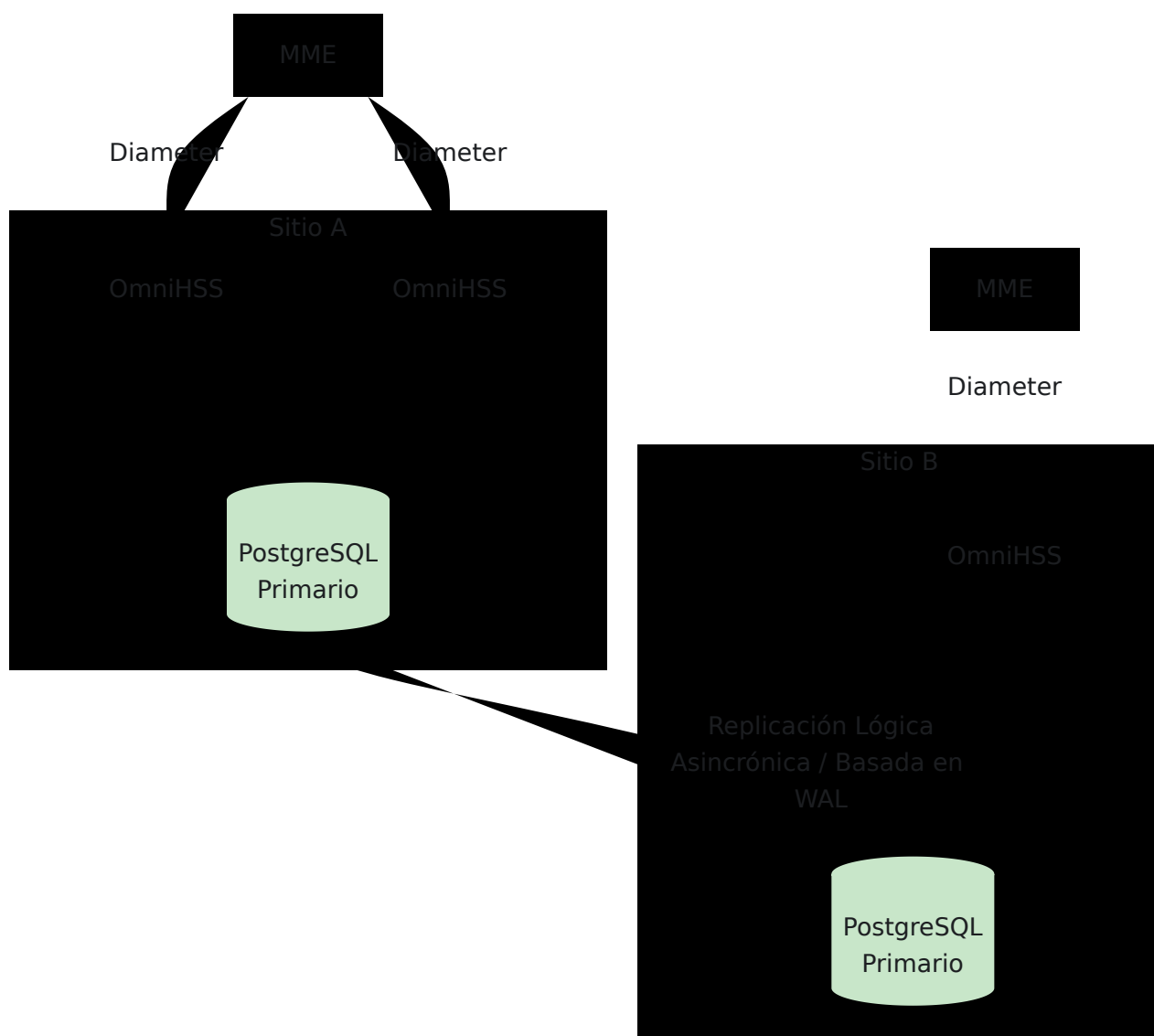
Arquitecturas de Despliegue

Sitio Único (Sin Replicación)



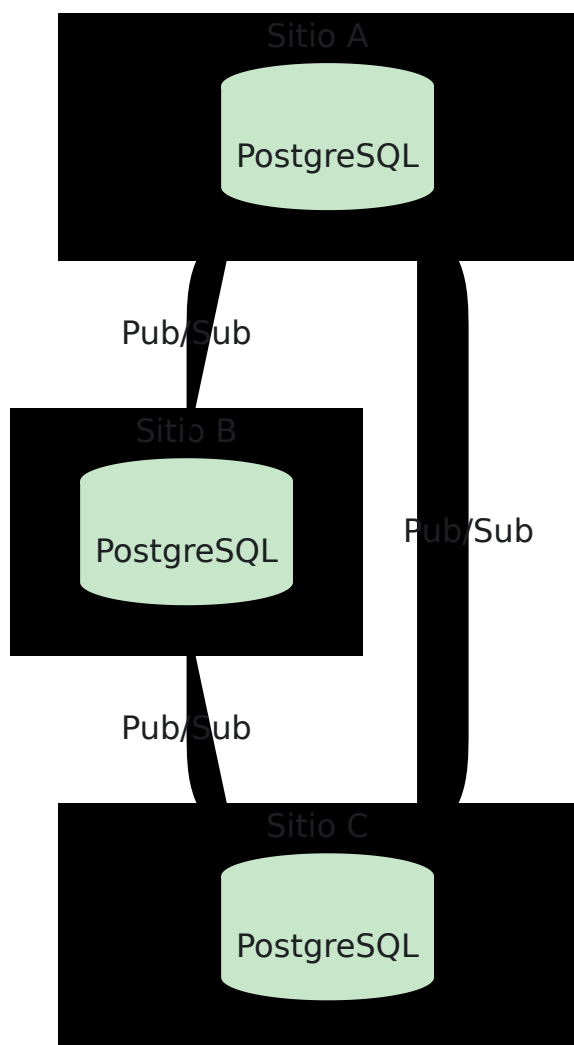
Múltiples instancias de aplicación HSS comparten una única base de datos PostgreSQL. Se puede utilizar replicación de streaming estándar de PostgreSQL para failover de base de datos local si es necesario.

Despliegue de Dos Sitios



Ambos sitios son primarios completos. El aprovisionamiento de suscriptores en cualquiera de los sitios se replica al otro. Cada MME se conecta a su HSS local. No hay dependencia de Diameter entre sitios.

Despliegue de Múltiples Sitios



Cada sitio se suscribe a la publicación de cada otro sitio. Los pares se descubren automáticamente desde el inventario de Ansible. Para agregar un sitio, agrégalo al grupo de inventario `hss` y ejecuta el playbook.

Requisitos de Red

Puerto	Protocolo	Propósito
5432	TCP	Conexiones de cliente y replicación de PostgreSQL

Referencia de Configuración

Variables de Ansible

La replicación se configura por grupo HSS en tu inventario:

```
hss:
  hosts:
    site-a-hss01:
      ansible_host: 10.80.12.140
    site-a-hss02:
      ansible_host: 10.80.12.141
  vars:
    omnihss:
      database_type: postgres
      database_host: localhost
      database_port: 5432
      database_name: omnihss
      database_username: omnihss
      database_password: "secure_password"
    replication:
      enabled: true
```

Parámetros de Ansible

Parámetro	Tipo	Requerido	Predeterminado	Descripción
database_type	Cadena	No	postgres	Backend de datos a ser utilizado para la base de datos.
database_host	Cadena	No	localhost	Host de la base de datos PostgreSQL. Puede ser localhost o una IP, cuando se ejecute en un servidor distinto al que se ejecuta el playbook.
database_port	Entero	No	5432	Puerto de la base de datos PostgreSQL.
database_name	Cadena	No	omnihss	Nombre de la base de datos.
database_username	Cadena	Sí	-	Usuario de la base de datos PostgreSQL. Debe tener privilegios de CREATE y REPLICATION.
database_password	Cadena	Sí	-	Contraseña de la base de datos PostgreSQL.
replication.enabled	Booleano	No	false	Habilita o deshabilita la replicación bidireccional. Cuando se habilita, crea el rol de replicación.

Parámetro	Tipo	Requerido	Predeterminado	De
				confi publi susci entra pg_h auton

Descubrimiento de Pares

Los pares se descubren automáticamente desde dos fuentes:

1. **Grupo de inventario local:** Todos los demás hosts en el grupo Ansible `hss`
2. **Sitios remotos:** Entradas en `connected_sites.hss` de `prod_master_peers.yml`

No se requiere configuración de pares por host. Agregar un host al grupo `hss` o a `connected_sites.hss` y ejecutar el playbook es suficiente.

Pares de Sitios Remotos (prod_master_peers.yml)

Para replicación intersitios a través de ubicaciones geográficas:

```
# group_vars/prod_master_peers.yml
connected_sites:
  hss:
    - remote-site-hss01: 10.80.20.140
    - remote-site-hss02: 10.80.20.141
```

Configuración de PostgreSQL

El rol de Ansible configura automáticamente los siguientes parámetros de PostgreSQL cuando se habilita la replicación:

Parámetro	Valor	Propósito
<code>wal_level</code>	<code>logical</code>	Requerido para replicación lógica. Incluye datos de fila completos en WAL.
<code>max_wal_senders</code>	<code>10</code>	Máximo de procesos de envío WAL concurrentes (uno por suscriptor).
<code>max_replication_slots</code>	<code>10</code>	Máximo de slots de replicación. Cada par utiliza un slot.
<code>listen_addresses</code>	<code>*</code>	Aceptar conexiones de sitios pares.

El rol también agrega entradas `pg_hba.conf` para permitir conexiones de replicación desde cada IP de par descubierta.

Gestión de Pares

Agregar un Nuevo Sitio

1. Agrega el/los nuevo(s) host(s) al grupo de inventario `hss`, o agrégalo a `connected_sites.hss` en `prod_master_peers.yml`
2. Ejecuta el playbook de OmniHSS

El rol hará:

- Instalar PostgreSQL y OmniHSS en el nuevo host
- Ejecutar migraciones de base de datos
- Crear una publicación para el nuevo sitio
- Crear suscripciones a todos los pares existentes
- Actualizar `pg_hba.conf` en todos los pares existentes para permitir el nuevo sitio
- Crear suscripciones desde pares existentes al nuevo sitio

Eliminar un Sitio

```
ansible-playbook -i hosts site.yml --tags hss-remove-peer \
-e "peer_name=site_b confirm_remove=yes"
```

El parámetro `confirm_remove=yes` es requerido como medida de seguridad. Sin él, el playbook se niega a continuar y muestra lo que sucedería.

Eliminar un par:

- Elimina la suscripción (detiene la replicación entrante desde ese par)
- Elimina la IP del par de `pg_hba.conf`
- Los datos ya replicados desde el par permanecen en la base de datos local
- La suscripción del sitio par a este sitio debe eliminarse por separado en el par

Agregar un Par Ad-Hoc

Para casos donde necesitas agregar un par fuera del flujo estándar del playbook:

```
ansible-playbook -i hosts site.yml --tags hss-add-peer \
-e "peer_name=site_b peer_host=10.80.20.140"
```

Monitoreo

Métricas de Prometheus

El servicio **postgres_exporter** se ejecuta en cada host HSS en el puerto `9187`, exponiendo métricas de PostgreSQL a Prometheus.

Métricas de Replicación

Métrica	Tipo	Descripción
<code>pg_replication_slots_active</code>	Gauge	1 si el slot de replicación está activo (par conectado), 0 si inactivo
<code>pg_replication_slots_pg_wal_lsn_diff</code>	Gauge	Retraso de replicación en bytes. Distancia entre la posición actual de WAL y la última posición confirmada del par
<code>pg_stat_replication_pg_current_wal_lsn_bytes</code>	Gauge	Posición actual de WAL en este nodo

Ejemplos de Consultas de Prometheus


```
# Slot de replicación activo (1 = conectado, 0 = desconectado)
pg_replication_slots_active{slot_name=~"sub_from_.*"}

# Retraso de replicación en megabytes
pg_replication_slots_pg_wal_lsn_diff / 1048576

# Alerta: slot de replicación inactivo por más de 60 segundos
pg_replication_slots_active == 0
```

Alertas Recomendadas

Alerta	Condición	Severidad	Descripción
Slot de Replicación Inactivo	<code>pg_replication_slots_active == 0</code> por 60s	Crítica	El parámetro de WAL acumulado es 0.
Retraso de WAL Excesivo	<code>pg_replication_slots_pg_wal_lsn_diff > 104857600</code> por 5m	Advertencia	El retraso de replicación es excesivo (más de 100MB) lo que puede ralentizar la replicación y degradar el rendimiento.
Slot de WAL Perdido	El estado de WAL es <code>lost</code>	Crítica	El slot de WAL es inválido para replicación, lo que puede causar un fallo en la replicación o un inicio de recuperación.

Validación de Ansible

El playbook de OmniHSS valida la salud de la replicación al final de cada ejecución. Asegura:

1. Todos los trabajadores de suscripción están vivos
2. Todos los slots de replicación están activos
3. El retraso de WAL está dentro del umbral (100MB por defecto)
4. El estado del slot de WAL es `reserved` o `extended` (no `lost`)

Si alguna afirmación falla, el playbook falla con un mensaje de error claro identificando el problema.

Validación Manual

```
# Verificar que los trabajadores de suscripción están vivos
sudo -u postgres psql -d omnihss -c \
    "SELECT subname, pid IS NOT NULL as worker_alive FROM
pg_stat_subscription;"

# Verificar slots de replicación y retraso
sudo -u postgres psql -d omnihss -c \
    "SELECT slot_name, active,
        pg_wal_lsn_diff(pg_current_wal_lsn(), confirmed_flush_lsn) as
lag_bytes,
        wal_status
    FROM pg_replication_slots WHERE slot_type = 'logical';"

# Comparar conteos de suscriptores entre sitios
sudo -u postgres psql -d omnihss -c "SELECT count(*) FROM
subscriber;"
```

Solución de Problemas

Trabajador de Suscripción Muerto

Síntomas: `pg_stat_subscription` muestra `pid IS NULL` para una suscripción. La validación de Ansible falla con "Trabajadores muertos."

Causas Comunes:

- La tabla existe en el publicador pero no en el suscriptor (desajuste DDL)
- Conflicto de clave duplicada de un registro insertado manualmente
- Par inalcanzable durante un período prolongado causando invalidación del slot de WAL

Resolución:

1. Verifica los registros de PostgreSQL para el error específico:

```
journalctl -u postgresql | grep "logical replication" | tail -20
```

2. Si hay un desajuste DDL: aplica la migración faltante en este sitio, luego el trabajador se reiniciará automáticamente.
3. Si hay una clave duplicada: resuelve el conflicto manualmente, luego vuelve a habilitar la suscripción:

```
ALTER SUBSCRIPTION sub_from_<peer> ENABLE;
```

Slot de Replicación Inactivo

Síntomas: `pg_replication_slots` muestra `active = false`. Se activa la alerta de Prometheus.

Causas Comunes:

- Problema de conectividad de red entre sitios
- PostgreSQL en el sitio par está detenido

- Firewall bloqueando el puerto 5432 desde la IP del par

Resolución:

1. Verifica la conectividad de red al par:

```
pg_isready -h <peer_ip> -U <db_user> -d omnihss
```

2. Verifica que PostgreSQL en el sitio par esté en ejecución.
3. Verifica que las reglas del firewall permitan el puerto 5432 desde la IP de este sitio.

El trabajador de suscripción se reconectará automáticamente cuando el par se vuelva accesible.

Slot de WAL Perdido

Síntomas: `pg_replication_slots` muestra `wal_status = 'lost'`. La validación de Ansible falla con "WAL SLOT CRÍTICO."

Causa: El par estuvo desconectado durante tanto tiempo que el WAL retenido excedió `max_slot_wal_keep_size` y fue limpiado.

Resolución: El par requiere un nuevo inicio completo:

1. Elimina la suscripción rota en este sitio:

```
DROP SUBSCRIPTION sub_from_<peer>;
```

2. Elimina el slot roto en el sitio par:

```
SELECT pg_drop_replication_slot('sub_from_<this_site>');
```

3. Vuelve a ejecutar el playbook de OmniHSS. Este recrea la suscripción con `copy_data = true` para realizar una sincronización inicial.

Retraso de WAL Excesivo

Síntomas: `pg_replication_slots_pg_wal_lsn_diff` es grande y creciente. Se activa la alerta de Prometheus.

Causas Comunes:

- Enlace intersitios de alta latencia o congestionado
- Sitio par bajo carga pesada (el trabajador de aplicación no puede seguir el ritmo)
- Operación masiva grande (por ejemplo, aprovisionamiento masivo) generando un volumen significativo de WAL

Resolución:

1. Verifica si el retraso está creciendo o estable:

```
SELECT slot_name,  
       pg_wal_lsn_diff(pg_current_wal_lsn(), confirmed_flush_lsn) as  
lag_bytes  
FROM pg_replication_slots WHERE slot_type = 'logical';
```

2. Si es estable: el par está aplicando cambios pero está atrasado. Se pondrá al día.
3. Si está creciendo: investiga el enlace de red o la carga del sitio par.
4. Para operaciones masivas: el retraso durante la operación es esperado y se resolverá después de que la operación se complete.

Coordinación de Migraciones de Esquema

Importante: Los cambios en el esquema de la base de datos (migraciones) no se replican a través de la replicación lógica. Al desplegar una nueva versión de OmniHSS que incluye cambios en el esquema:

1. Aplica la migración en **todos los sitios** antes de desplegar el código de la aplicación que depende de nuevas columnas/tablas.
2. El playbook de Ansible maneja esto automáticamente. Ejecuta migraciones en cada host.

3. Si despliegas manualmente, ejecuta migraciones en todos los sitios primero:

```
/opt/omnihss/bin/hss rpc "Hss.Command.Database.migrate()"
```

Relaciones de Entidad de OmniHSS

[← Volver a la Guía de Operaciones](#)

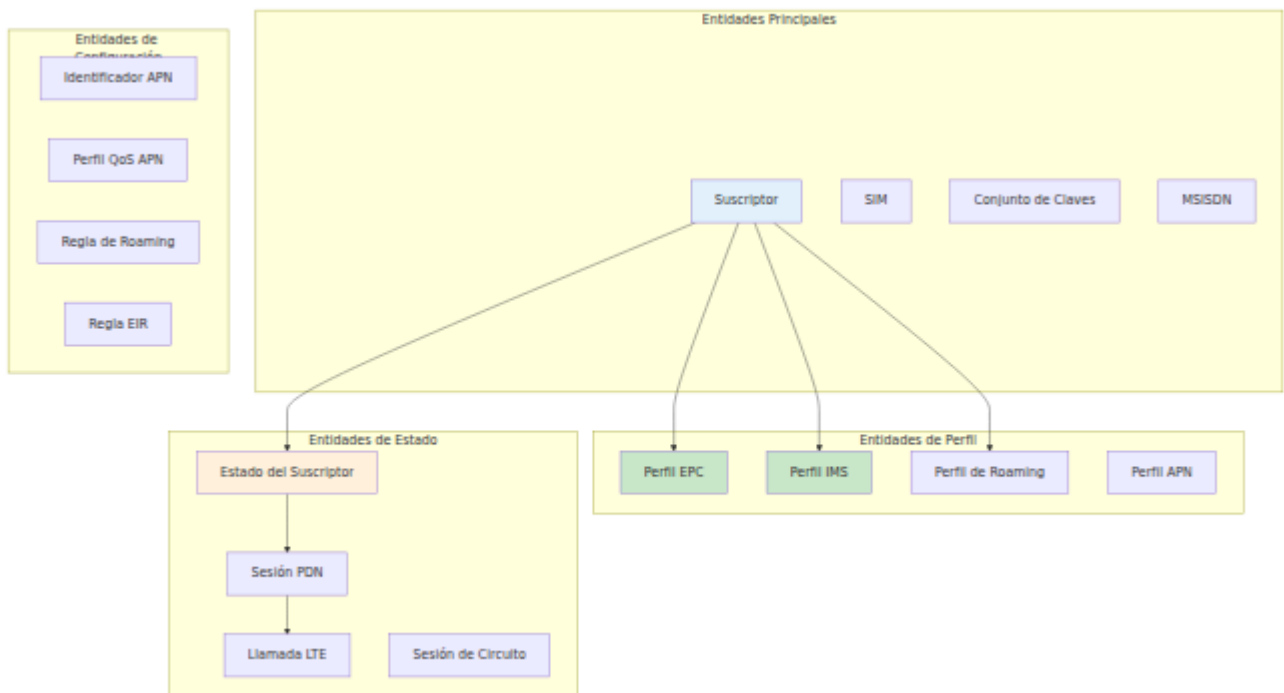
Tabla de Contenidos

- [Descripción de la Entidad](#)
 - [Entidades Principales](#)
 - [Entidades de Perfil](#)
 - [Entidades de Estado](#)
 - [Diagramas de Relaciones de Entidad](#)
 - [Ciclo de Vida de la Entidad](#)
 - [Patrones de Flujo de Datos](#)
-

Descripción de la Entidad

OmniHSS organiza los datos de los suscriptores en entidades lógicas con relaciones claras. Comprender estas entidades es crucial para tareas operativas como aprovisionamiento, solución de problemas y planificación de capacidad.

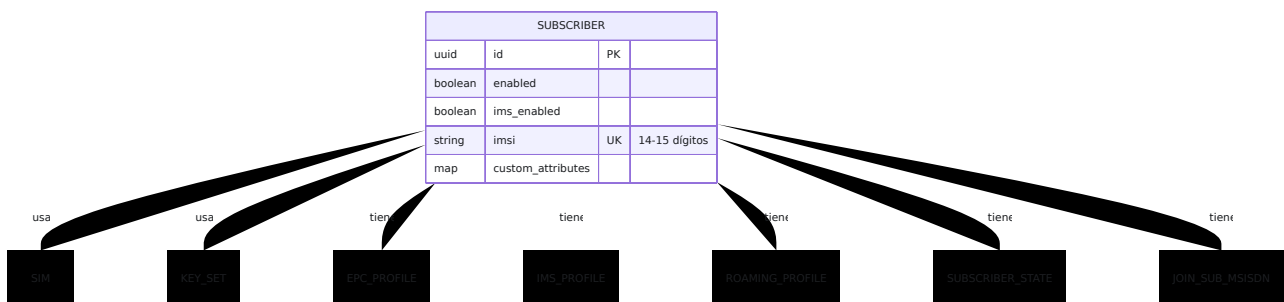
Categorías de Entidades



Entidades Principales

Suscriptor

El **Suscriptor** es la entidad central que representa a un usuario móvil.



Campos:

Campo	Tipo	Descripción	Restricciones
<code>id</code>	uuid	Clave primaria	UUID, generado (<code>gen_random_uuid()</code>)
<code>enabled</code>	boolean	Indicador de servicio habilitado	Predeterminado: true
<code>ims_enabled</code>	boolean	Servicios IMS habilitados	Predeterminado: true
<code>imsi</code>	string	Identidad Internacional de Suscriptor Móvil	14-15 dígitos, único
<code>custom_attributes</code>	map	Datos personalizados clave-valor	Opcional
<code>sim_id</code>	uuid	Clave foránea a SIM	Requerido para autenticación (puede ser nulo mientras esté inactivo)
<code>key_set_id</code>	uuid	Clave foránea a Conjunto de Claves	Requerido
<code>epc_profile_id</code>	uuid	Clave foránea a Perfil EPC	Requerido para servicio de datos (puede ser nulo mientras esté inactivo)

Campo	Tipo	Descripción	Restricciones
<code>ims_profile_id</code>	uuid	Clave foránea a Perfil IMS	Requerido para IMS/voz (puede ser nulo mientras esté inactivo)
<code>roaming_profile_id</code>	uuid	Clave foránea a Perfil de Roaming	Opcional; si es nulo, el suscriptor no puede hacer roaming (solo red local)
<code>subscriber_state_id</code>	uuid	Clave foránea a Estado del Suscriptor	Creado automáticamente

La columna "Restricciones" anterior indica para qué se requiere cada objeto **para un servicio**, no lo que la base de datos necesita para insertar una fila. La base de datos acepta un suscriptor que tiene solo un IMSI y un Conjunto de Claves. Tal suscriptor está *inactivo*: existe, pero ningún servicio funciona hasta que asigne el objeto correspondiente. Use esto para aprovisionar previamente a los suscriptores y luego activarlos más tarde. Consulte [Aprovisionamiento Previo de Suscriptores Inactivos](#).

Lo que habilita cada objeto:

Para que esto funcione	El suscriptor necesita
Autenticación (adjuntar, autenticación IMS)	<code>key_set</code> y <code>sim</code>
Servicio de datos LTE (adjunto S6a)	<code>epc_profile</code>
IMS / voz (registro Cx)	<code>ims_profile</code> , y al menos un MSISDN
Roaming en una red visitada	un <code>roaming_profile</code> con una regla coincidente

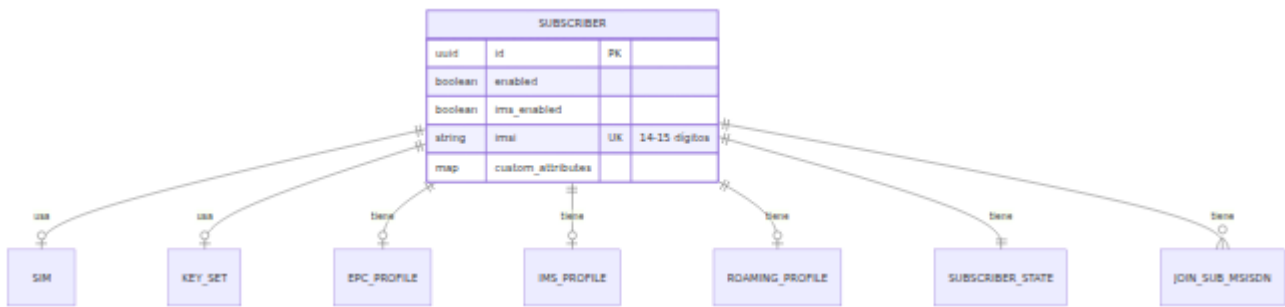
Si falta un objeto requerido cuando el suscriptor aparece en la red, el HSS rechaza la solicitud y registra la razón exacta. Consulte [Comportamiento de Suscriptor Inactivo en la Red](#).

Puntos Clave:

- Cada suscriptor debe tener exactamente un IMSI.
- El IMSI debe tener 14-15 dígitos (sin letras ni caracteres especiales).
- Un suscriptor puede tener múltiples MSISDNs (números de teléfono).
- El estado del suscriptor se crea automáticamente cuando se crea el suscriptor.
- La bandera `enabled` controla todos los servicios (datos e IMS).
- La bandera `ims_enabled` controla solo los servicios IMS.
- La base de datos solo necesita el IMSI y el Conjunto de Claves para insertar un suscriptor. Cada otro objeto es necesario para su propio servicio, como se indica arriba. Un suscriptor sin perfil IMS no puede usar IMS, aunque el registro se guarda sin uno.

SIM

La entidad **SIM** representa una tarjeta SIM física o embebida.



Campos:

Campo	Tipo	Descripción	Nivel de Seguridad
<code>iccid</code>	string	Identificación de Circuito Integrado	Público
<code>sim_vendor</code>	string	Fabricante de la SIM	Público
<code>batch_name</code>	string	Lote de fabricación	Público
<code>is_esim</code>	boolean	Indicador de SIM embebida	Público
<code>pin1</code> , <code>pin2</code>	string	Códigos PIN	Sensible
<code>puk1</code> , <code>puk2</code>	string	Códigos PUK	Sensible
<code>adm1</code> - <code>adm10</code>	string	Códigos administrativos	Muy Sensible
<code>kic</code> , <code>kid</code>	binary	Claves de seguridad OTA	Muy Sensible

Puntos Clave:

- El ICCID identifica de manera única la tarjeta SIM.
- Una SIM puede ser asignada a un suscriptor a la vez.
- Los códigos PIN/PUK son para el bloqueo de SIM por parte del usuario final.
- Los códigos ADM son para operaciones administrativas de la SIM.
- KIC/KID son para actualizaciones OTA (Over-The-Air) de la SIM.

Conjunto de Claves

El **Conjunto de Claves** contiene claves criptográficas para autenticación.

KEY_SET			
uuid	id	PK	
binary	ki		128-bit
binary	opc		128-bit
binary	op		128-bit
binary	amf		16-bit
bigint	sqn		48-bit sequence
string	authentication_algorithm		

usado pc



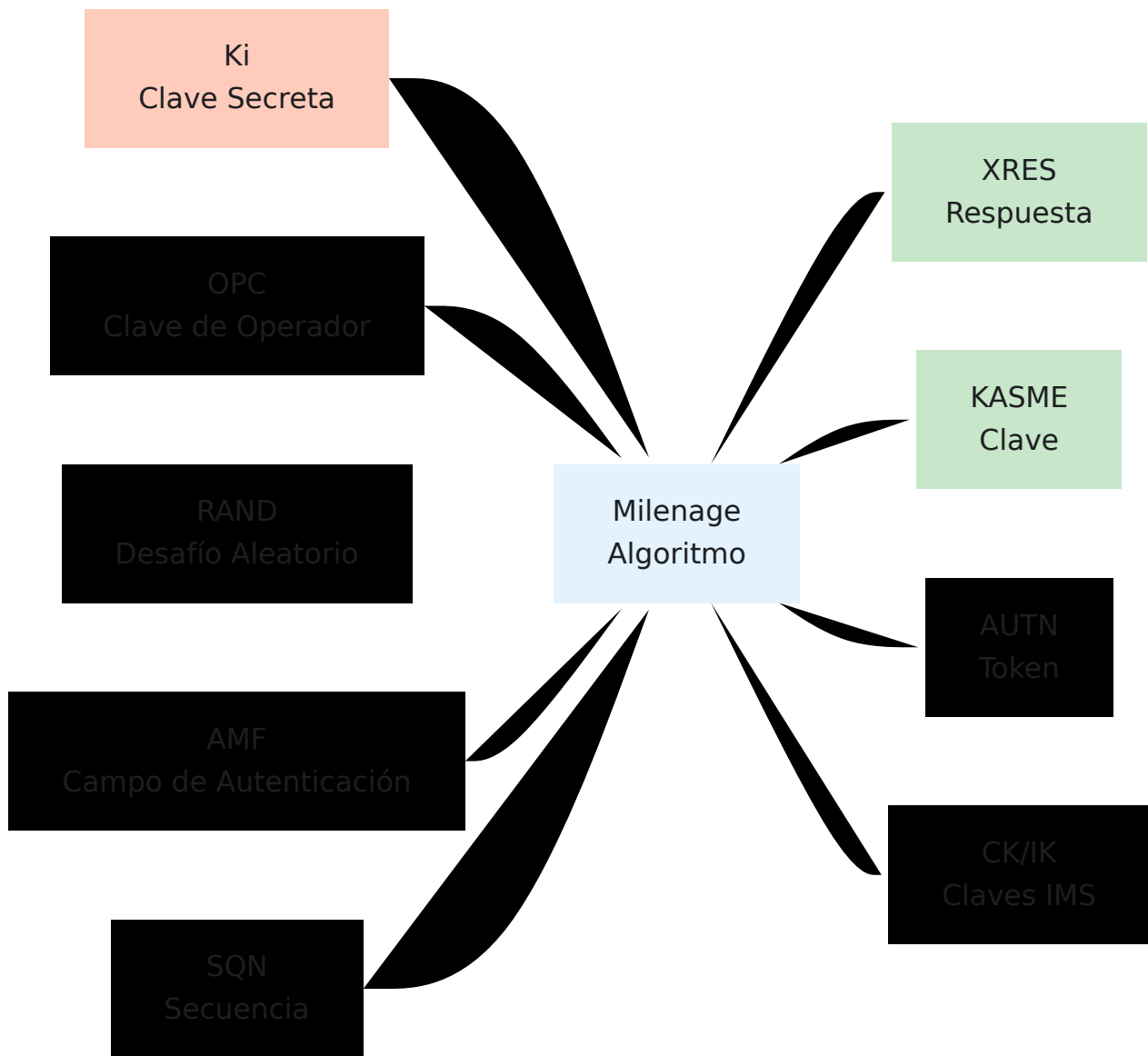
Campos:

Campo	Tipo	Descripción	Tamaño
ki	binary	Clave secreta	128 bits (16 bytes)
opc	binary	Clave variante de operador (derivada)	128 bits
op	binary	Clave de operador (para derivar OPC)	128 bits
amf	binary	Campo de Gestión de Autenticación	16 bits (2 bytes)
sqn	bigint	Número de secuencia (anti-repetición)	48 bits
authentication_algorithm	string	Nombre del algoritmo	Actualmente "milenage"
ota_counter	bigint	Contador de operaciones OTA	Entero

Puntos Clave:

- Múltiples suscriptores pueden compartir el mismo conjunto de claves.
- Ki es el secreto maestro compartido con la SIM.
- Se debe proporcionar OPC o OP (OPC puede derivarse de OP).
- SQN se incrementa con cada autenticación.
- Milenage es actualmente el único algoritmo soportado.

Algoritmo de Autenticación:

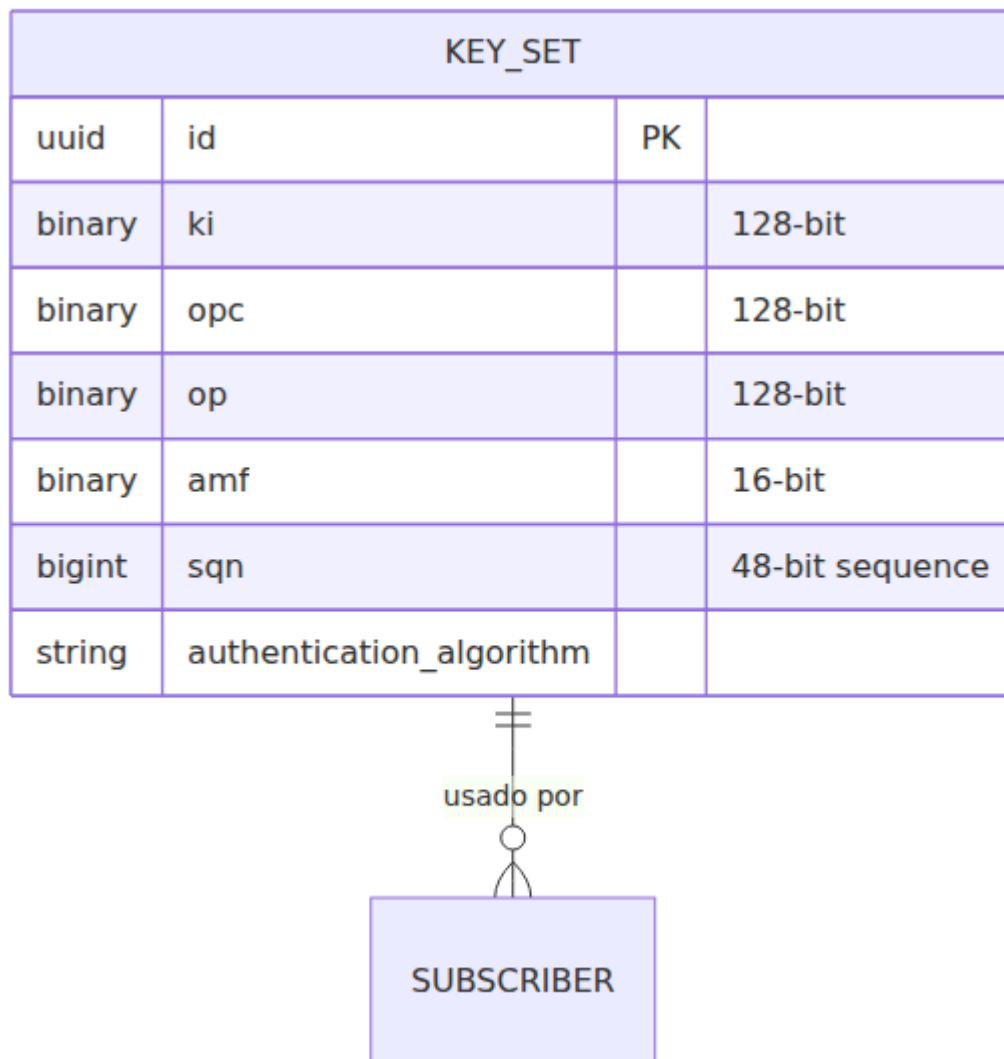


Conjunto de Claves, SIM y Suscriptor

La SIM, el Conjunto de Claves y el Suscriptor son objetos separados. Cada objeto tiene su propio ciclo de vida. El Suscriptor es el registro que los vincula.

- **SIM** - la tarjeta física o el eSIM. Contiene el ICCID y los códigos PIN, PUK y ADM. Es inventario.
- **Conjunto de Claves** - las claves de autenticación (Ki, OPc, AMF, SQN). La red se autentica contra estas claves.
- **Suscriptor** - la identidad de la red y el servicio (IMSI, MSISDN, perfiles, estado habilitado).

Un Suscriptor referencia una SIM (`sim_id`) y un Conjunto de Claves (`key_set_id`). Un Conjunto de Claves no referencia una SIM. Para encontrar a qué SIM pertenece un Conjunto de Claves, lea el Suscriptor que referencia ambos.



Por qué los objetos son separados

Los objetos son separados porque no se mapean uno a uno en todos los casos:

- **Cambio de SIM.** Un suscriptor deja caer un teléfono y necesita una nueva SIM. Mantiene el Suscriptor, con su MSISDN, perfiles y datos IMS. Lo apunta a una nueva SIM y a un nuevo Conjunto de Claves. El servicio continúa.
- **SIM Multi-IMSI.** Un ICCID lleva varios IMSIs. Cada IMSI es un Suscriptor separado. Algunos IMSIs comparten un Conjunto de Claves. Algunos IMSIs tienen su propio Conjunto de Claves. Las claves pertenecen a un IMSI, no a una tarjeta. Consulte [Soporte para SIM Multi-IMSI](#).

- **Roaming hospedado o patrocinado.** El applet de la SIM se autentica con un IMSI visitado. La red anfitriona traduce el IMSI visitado a su IMSI local antes de que la solicitud llegue al HSS. Los dos IMSIs comparten un Conjunto de Claves.

Por lo tanto, un Conjunto de Claves puede servir a más de un Suscriptor. Esta es la razón por la que el Conjunto de Claves es un objeto separado, y no un campo en la SIM.

Correlación en la importación

El archivo del proveedor de SIM le da el ICCID y las claves en una fila. Al importar, crea el Conjunto de Claves, crea la SIM y crea el Suscriptor que referencia ambos. El Suscriptor es el registro conectivo. Para el flujo de trabajo de importación, consulte [Aprovisionamiento Previo de Suscriptores Inactivos](#).

MSISDN

El **MSISDN** representa un número de teléfono.

MSISDN			
uuid	id	PK	
string	msisdn	UK	1-15 dígitos

asignado

JOIN_SUB_MSISDN		
uuid	subscriber_id	FK
uuid	msisdn_id	FK

pertenece



Campos:

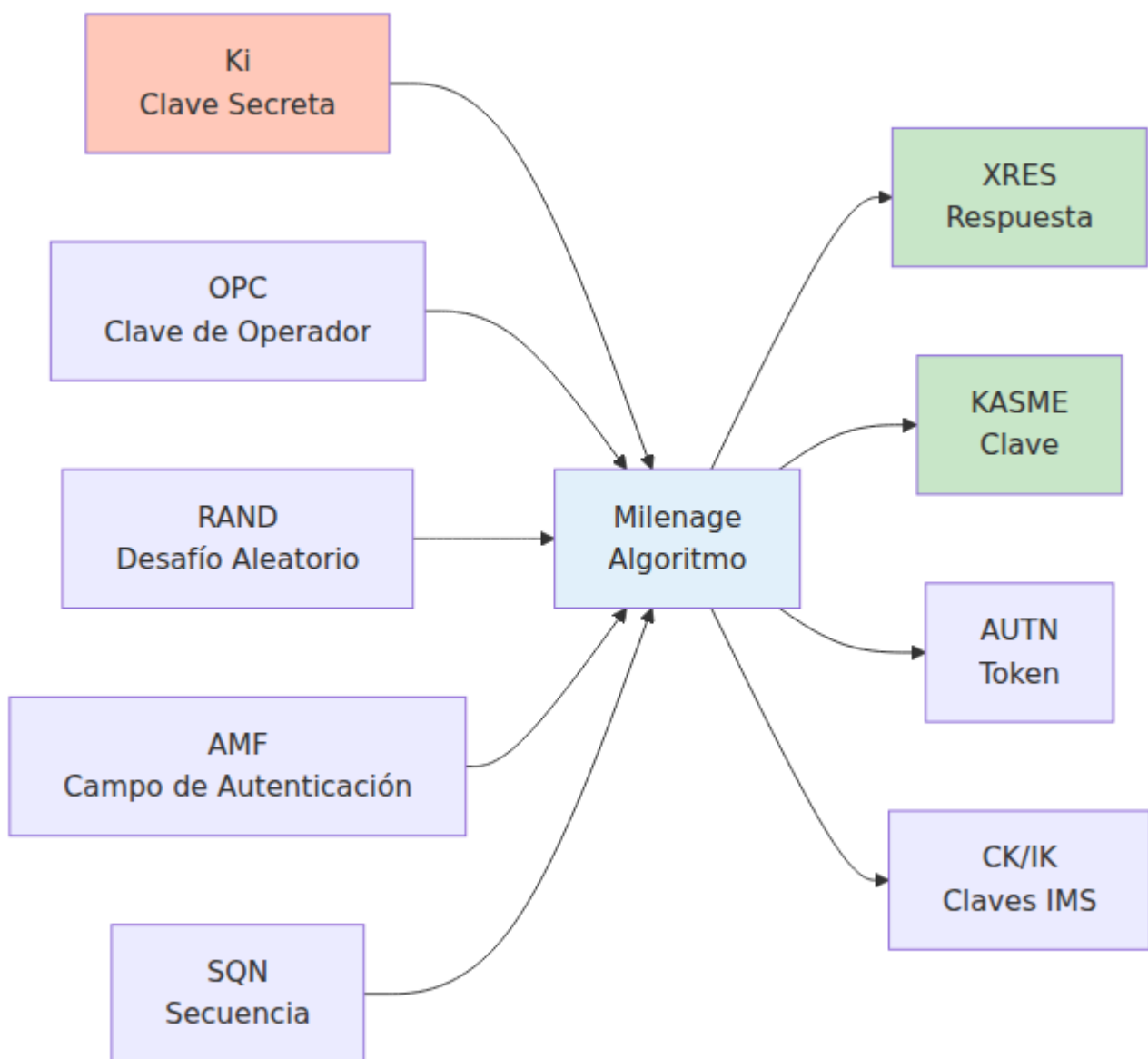
Campo	Tipo	Descripción	Formato
msisdn	string	Número ISDN de Estación Móvil	1-15 dígitos, formato E.164

Puntos Clave:

- MSISDN es el número de teléfono en formato internacional.
- Un suscriptor puede tener muchos MSISDNs (un IMSI, muchos números).
- Un MSISDN puede ser asignado a muchos suscriptores (muchos IMSIs, un número). Use esto para un número compartido, por ejemplo, un teléfono y un reloj inteligente. El número se almacena como un registro MSISDN, y cada suscriptor mantiene una fila de unión a él.

- Una búsqueda inversa por MSISDN (por ejemplo, la API `GET /subscriber/msisdn/:msisdn`, o una búsqueda Diameter clave en el número) devuelve un suscriptor. Cuando un número es compartido, use el IMSI o el ICCID para seleccionar un suscriptor específico.
- Formato: Código de país + Número nacional, solo dígitos - sin prefijo `+` (por ejemplo, `14155551234` no `+14155551234`)
- El prefijo `+` se elimina automáticamente durante las búsquedas Diameter Cx/Rx cuando el S-CSCF o P-CSCF envía un URI SIP con o sin el `+`

Patrón Multi-MSISDN:

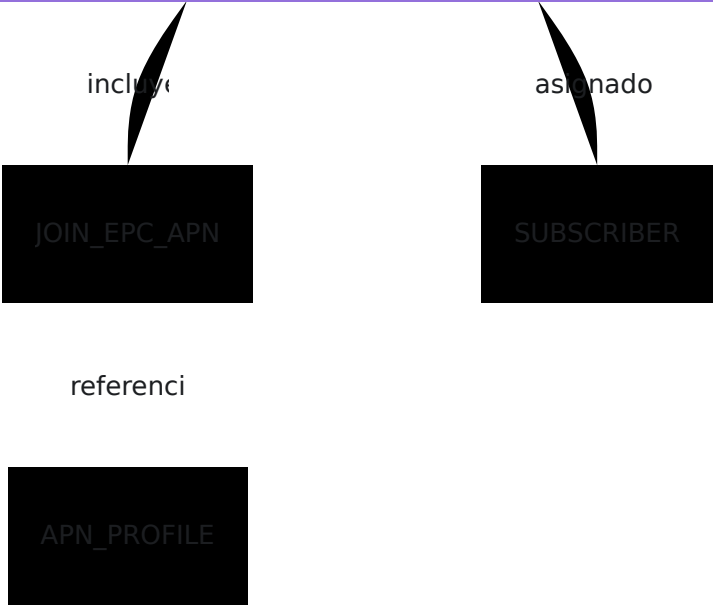


Entidades de Perfil

Perfil EPC

El **Perfil EPC** define las características del servicio de datos para LTE.

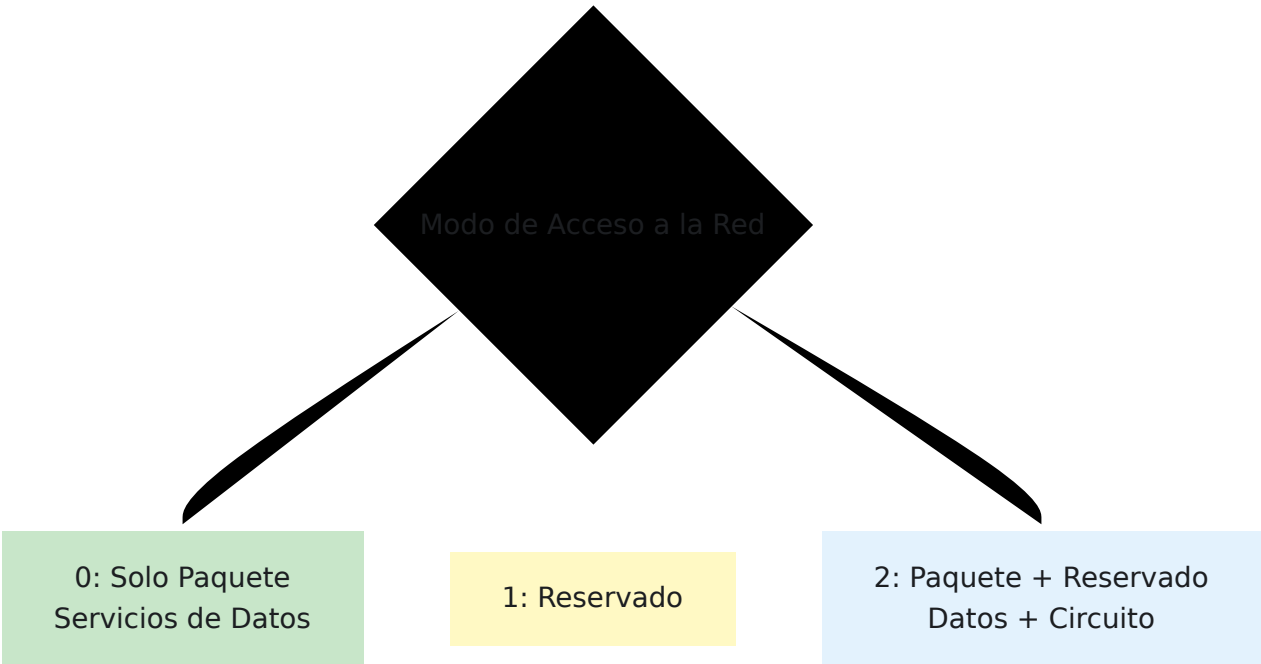
EPC_PROFILE			
uuid	id	PK	
string	name	UK	
integer	ue_ambr_dl_kbps		
integer	ue_ambr_ul_kbps		
string	network_access_mode		solo_paquete o paquete_y_circuito
integer	tracking_area_update_interval_seconds		



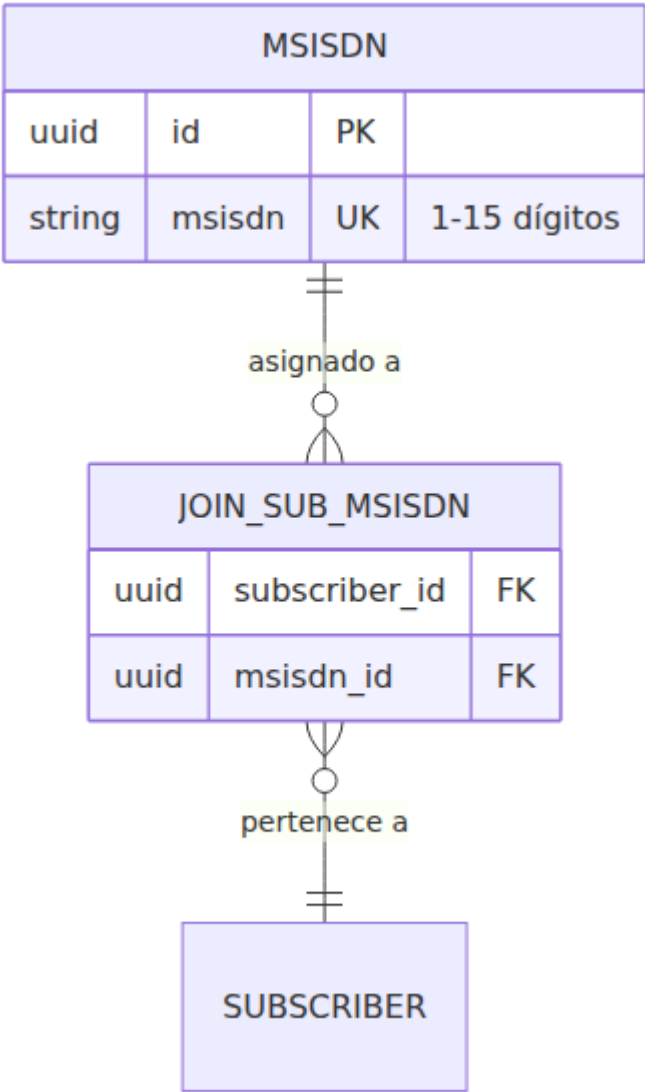
Campos:

Campo	Tipo	Descripción	Unidad
name	string	Nombre del perfil	Texto
ue_ambr_dl_kbps	integer	Límite de ancho de banda de descarga	Kbps
ue_ambr_ul_kbps	integer	Límite de ancho de banda de carga	Kbps
network_access_mode	string	Restricciones de acceso	"solo_paquete"
tracking_area_update_interval_seconds	integer	Intervalo de TAU	Segundos

Modos de Acceso a la Red:



AMBR (Tasa de Bits Máxima Agregada):



Perfil IMS

El **Perfil IMS** define las características del servicio de voz/video.

IMS_PROFILE		
uuid	id	PK
string	name	UK
text	ifc_template	

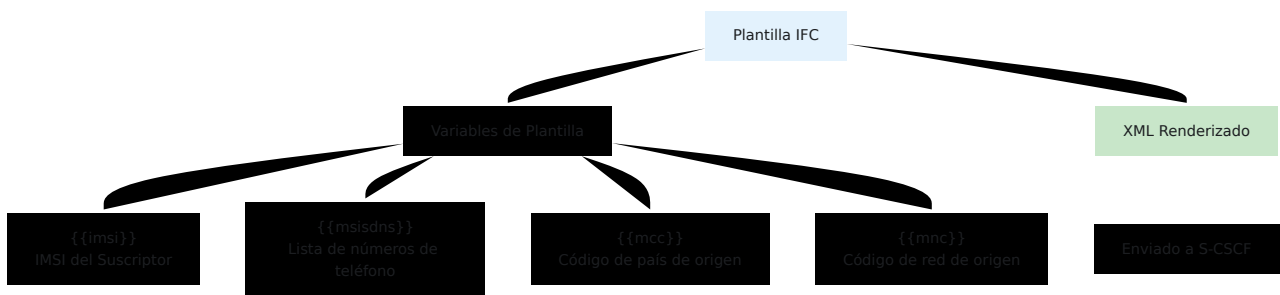
asignado



Campos:

Campo	Tipo	Descripción	Formato
name	string	Nombre del perfil	Texto
ifc_template	text	Plantilla XML de Criterios de Filtro Inicial	XML con variables

Variables de Plantilla IFC:



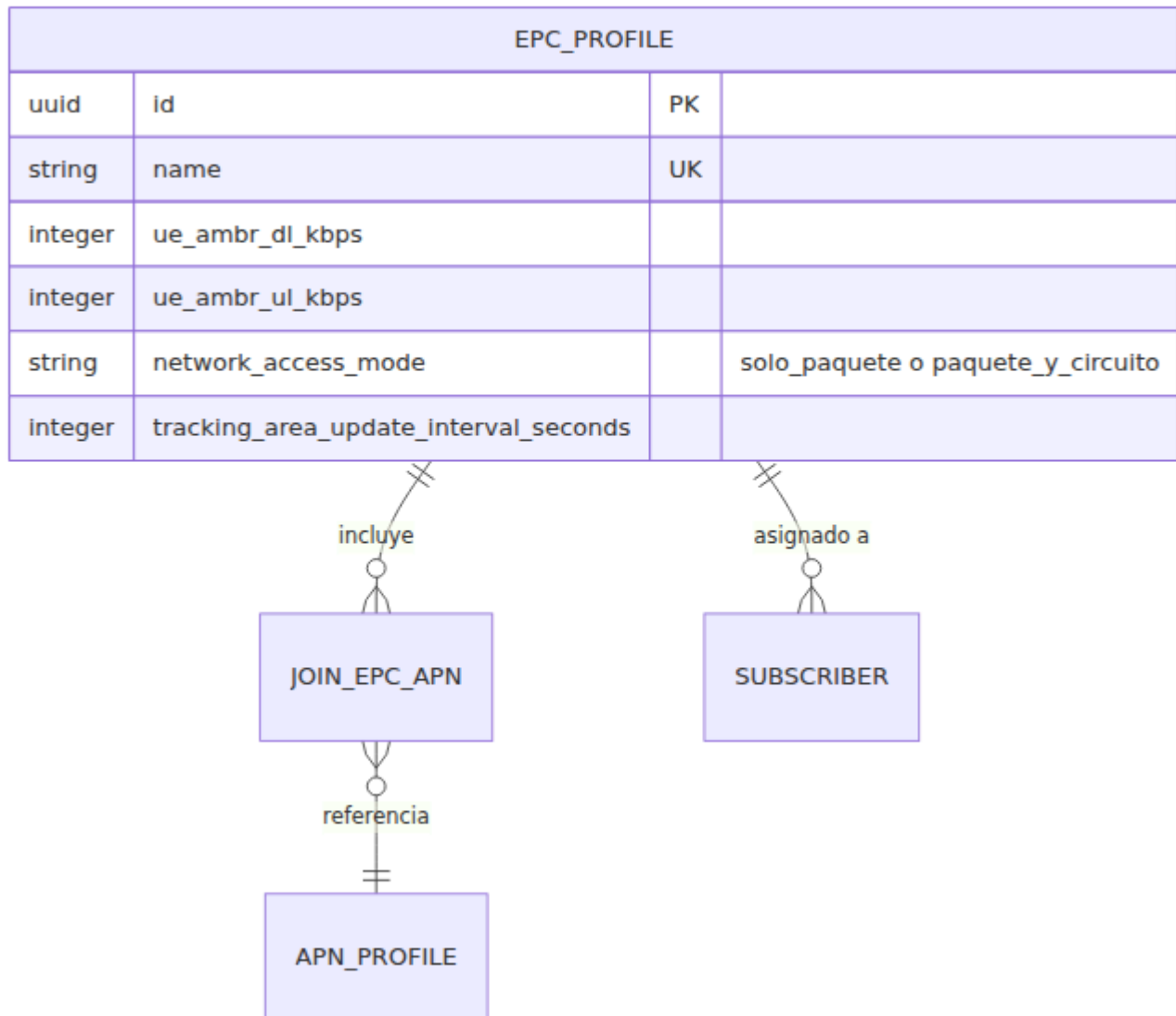
Puntos Clave:

- IFC (Criterios de Filtro Inicial) controla el enrutamiento de llamadas en IMS.
- La plantilla se renderiza cuando el suscriptor se registra.
- Las variables se sustituyen con los datos reales del suscriptor.

- Se envía al S-CSCF durante el registro IMS.

Perfil APN

El **Perfil APN** define características para un punto de acceso de datos específico.



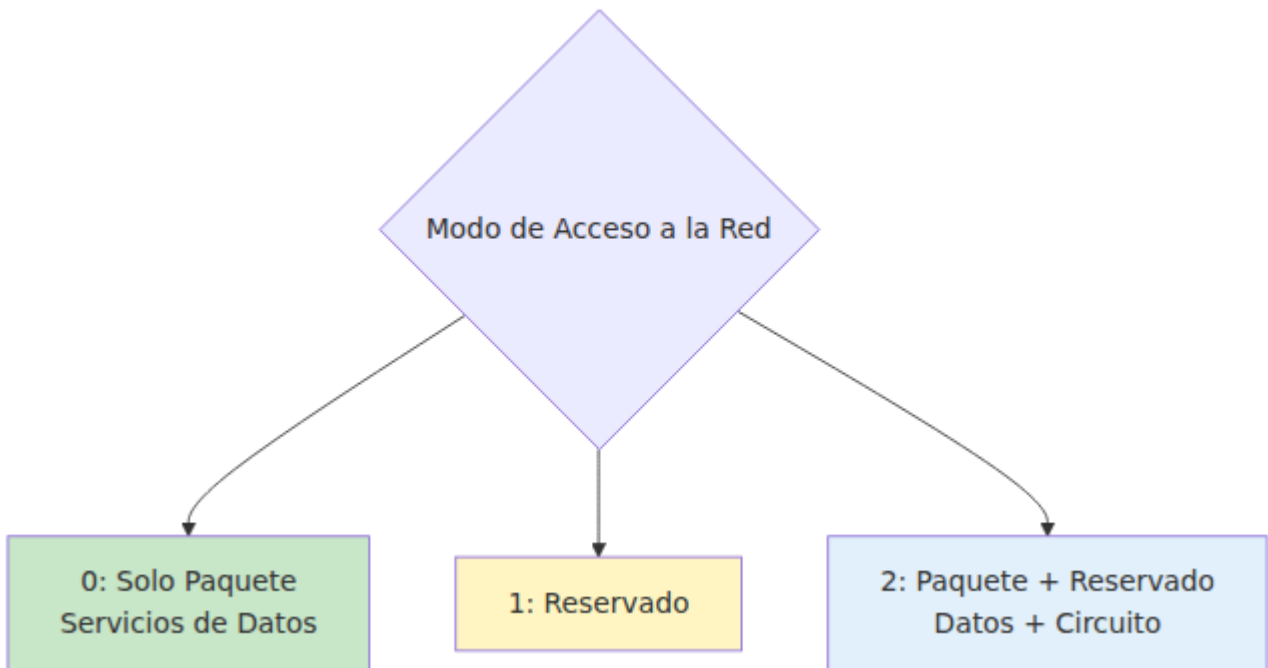
Entidades Relacionadas:

Identificador APN

APN_IDENTIFIER			
uuid	id	PK	
string	apn	UK	
string	ip_version		ipv4, ipv6, ipv4v6, o ipv4_o_ipv6

Campo	Tipo	Descripción	Ejemplo
apn	string	Nombre APN	"internet", "ims", "mms"
ip_version	string	Soporte de protocolo IP	Ver abajo

Opciones de Versión IP:



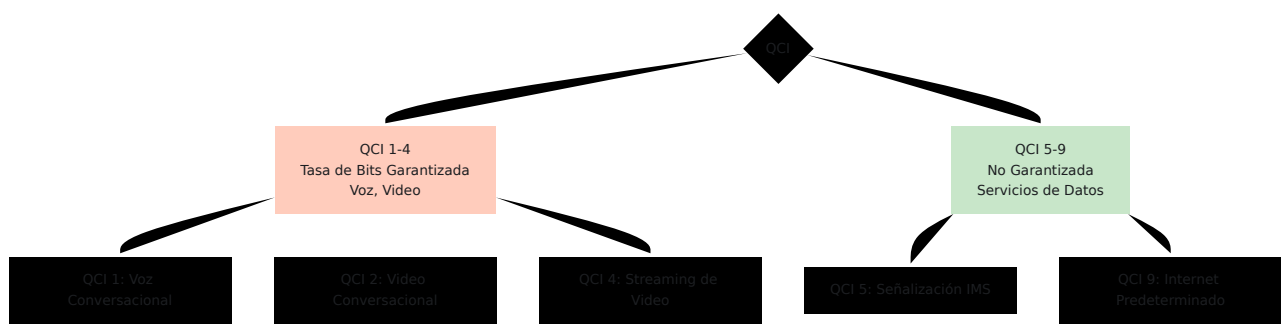
Perfil QoS APN

APN_QOS_PROFILE		
uuid	id	PK
string	name	UK
integer	qci	
integer	allocation_retention_priority	
integer	apn_ambr_dl_kbps	
integer	apn_ambr_ul_kbps	
boolean	pre_emption_capability	
boolean	pre_emption_vulnerability	

Parámetros QoS:

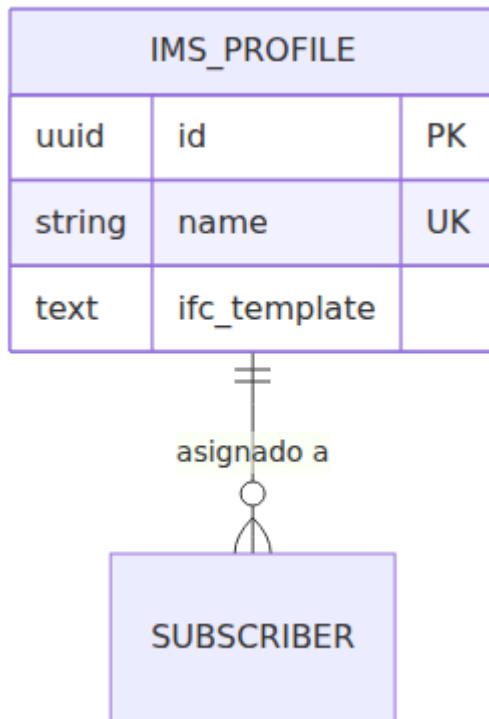
Parámetro	Descripción	Rango	Portado Predeterminado
qci	Identificador de Clase QoS	1-9	QCI 9 (Internet)
allocation_retention_priority	Prioridad ARP	1-15	8 (prioridad alta)
apn_ambr_dl_kbps	Límite de descarga APN	0+	Varía
apn_ambr_ul_kbps	Límite de carga APN	0+	Varía
pre_emption_capability	Puede preemptar a otros	true/false	false
pre_emption_vulnerability	Puede ser preemptado	true/false	true

Valores QCI:



Perfil de Roaming

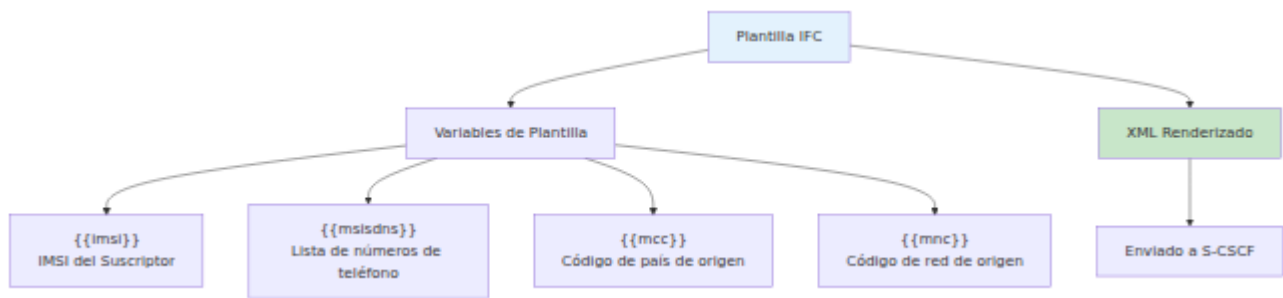
El **Perfil de Roaming** controla el acceso cuando el suscriptor visita otras redes.



Regla de Roaming:

ROAMING_RULE			
uuid	id	PK	
string	name	UK	
string	mcc		3 dígitos
string	mnc		2-3 dígitos
string	data_action		permitir o denegar
string	ims_action		permitir o denegar

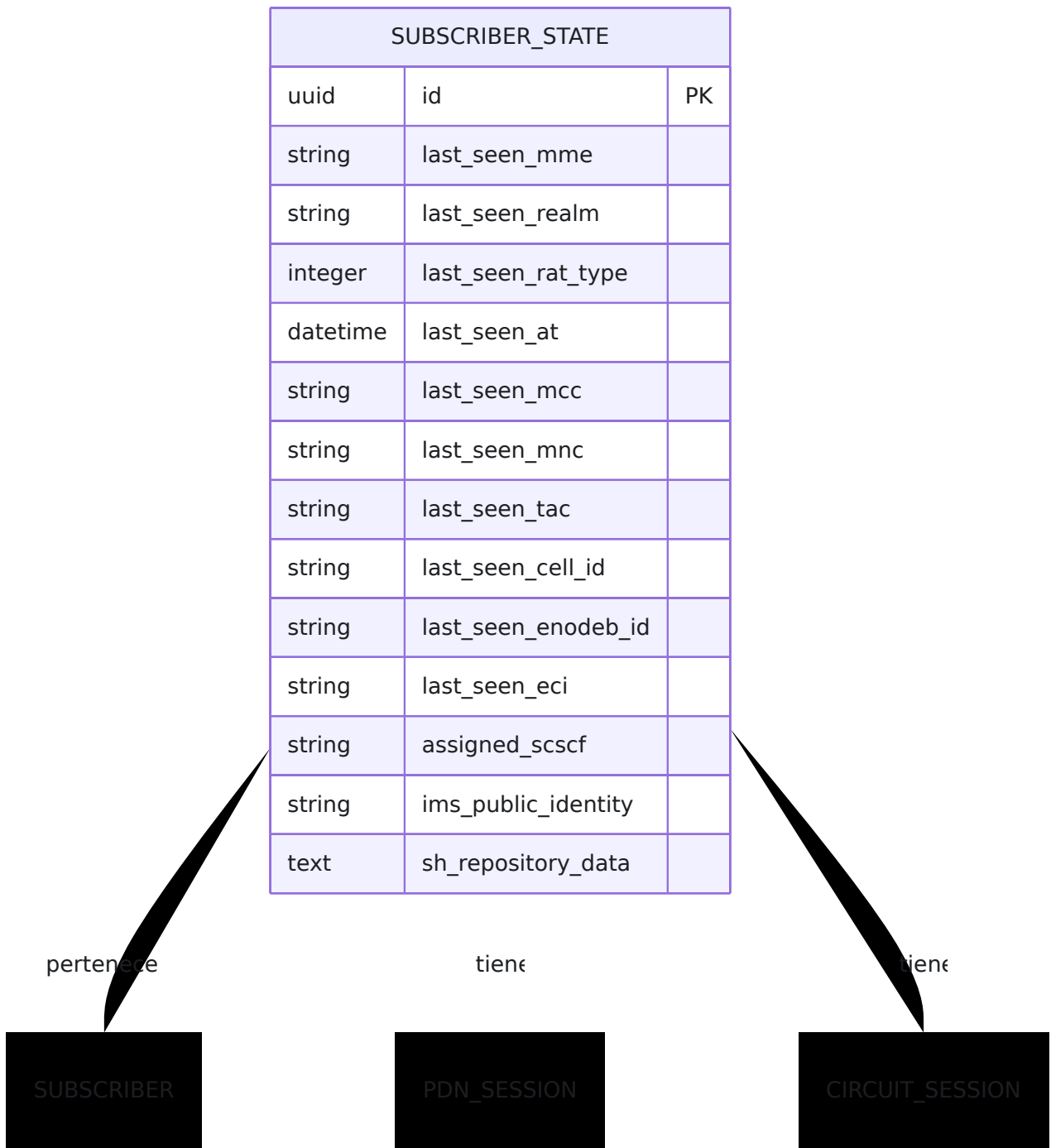
Evaluación de Reglas:



Entidades de Estado

Estado del Suscriptor

El **Estado del Suscriptor** rastrea el estado del suscriptor en tiempo real.



Campos Clave:

Información de Ubicación:

- `last_seen_mcc`, `last_seen_mnc` - Red visitada
- `last_seen_tac` - Código de Área de Seguimiento
- `last_seen_cell_id` - ID de Celda
- `last_seen_enodeb_id` - ID de eNodeB
- `last_seen_eci` - Identificador de Celda E-UTRAN

Elementos de Red:

- `last_seen_mme` - MME actual que atiende al suscriptor
- `last_seen_realms` - Dominio Diameter del MME
- `last_seen_rat_type` - Tecnología de Acceso Radio (LTE, 5G, etc.)

Información IMS:

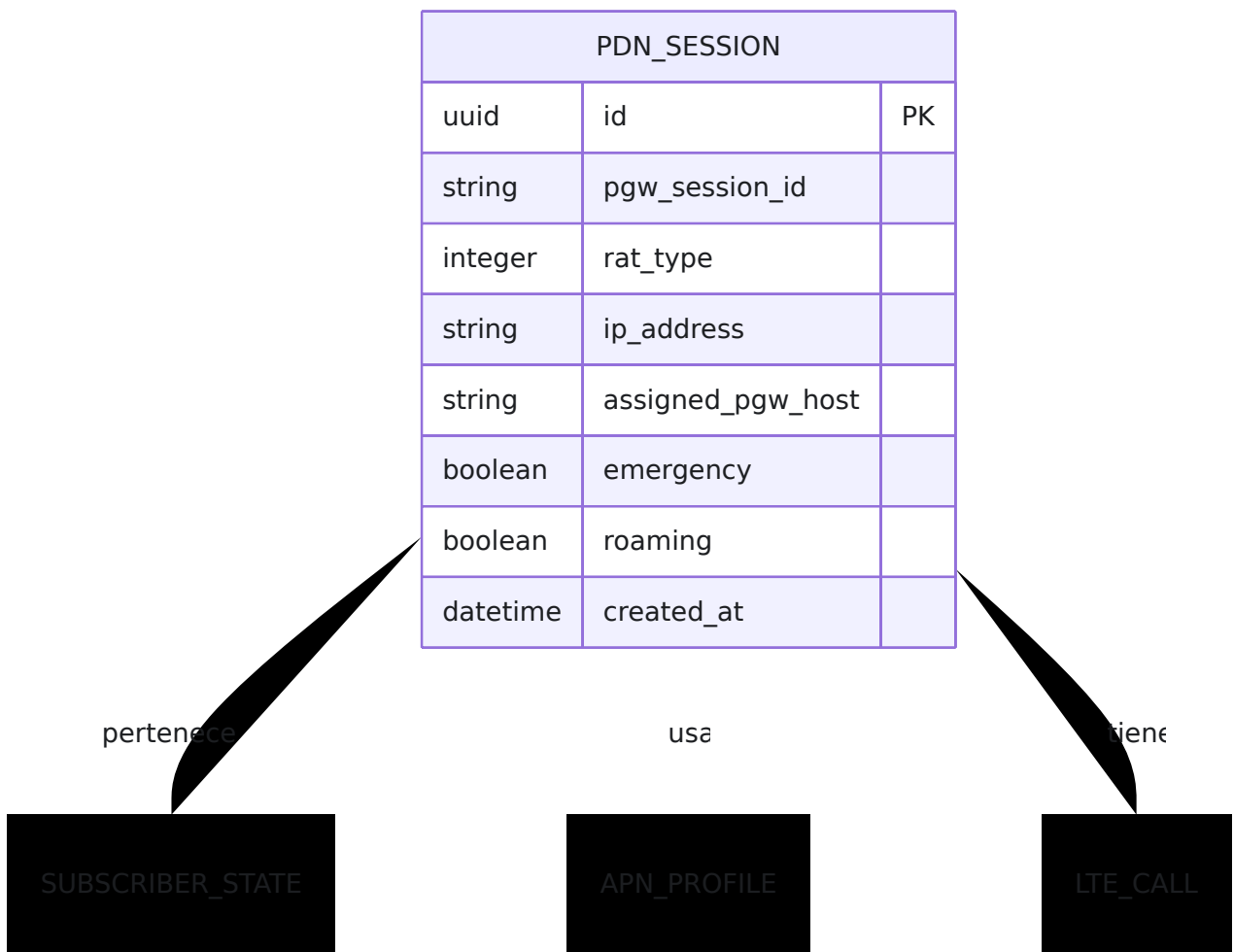
- `assigned_scscf` - S-CSCF actual que atiende al suscriptor
- `ims_public_identity` - URI SIP (por ejemplo, sip:+14155551234@ims.example.com)
- `sh_repository_data` - Datos de perfil IMS personalizados

Tiempos:

- `last_seen_at` - Último mensaje Diameter recibido
- Varios timestamps `last*_at` para diferentes procedimientos

Sesión PDN

La **Sesión PDN** representa una conexión de datos activa.



Ciclo de Vida de la Sesión PDN:

APN_IDENTIFIER			
uuid	id	PK	
string	apn	UK	
string	ip_version		ipv4, ipv6, ipv4v6, o ipv4_o_ipv6

Llamada LTE

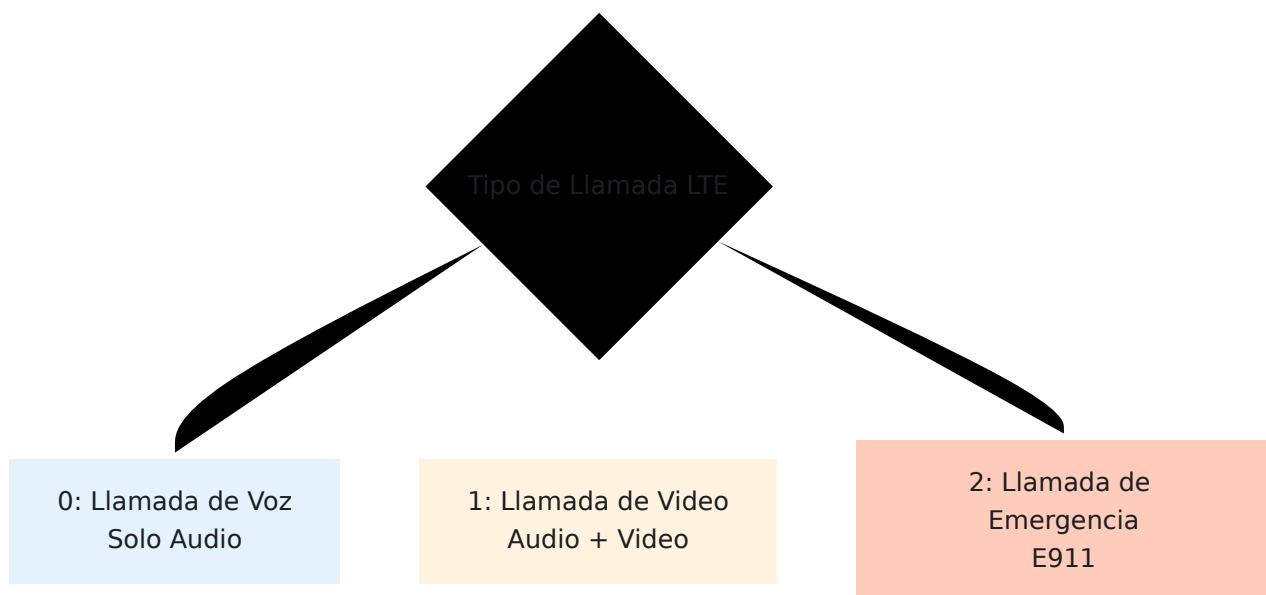
La **Llamada LTE** representa una llamada de voz/video VoLTE activa.

LTE_CALL		
uuid	id	PK
string	pcscf_session_id	
string	assigned_pcscf_host	
string	codec	
integer	type	
boolean	dedicated_bearer_active	
integer	dedicated_bandwidth_ul	
integer	dedicated_bandwidth_dl	
text	flow_rules	
datetime	created_at	

pertenece

PDN_SESSION

Tipos de Llamadas:

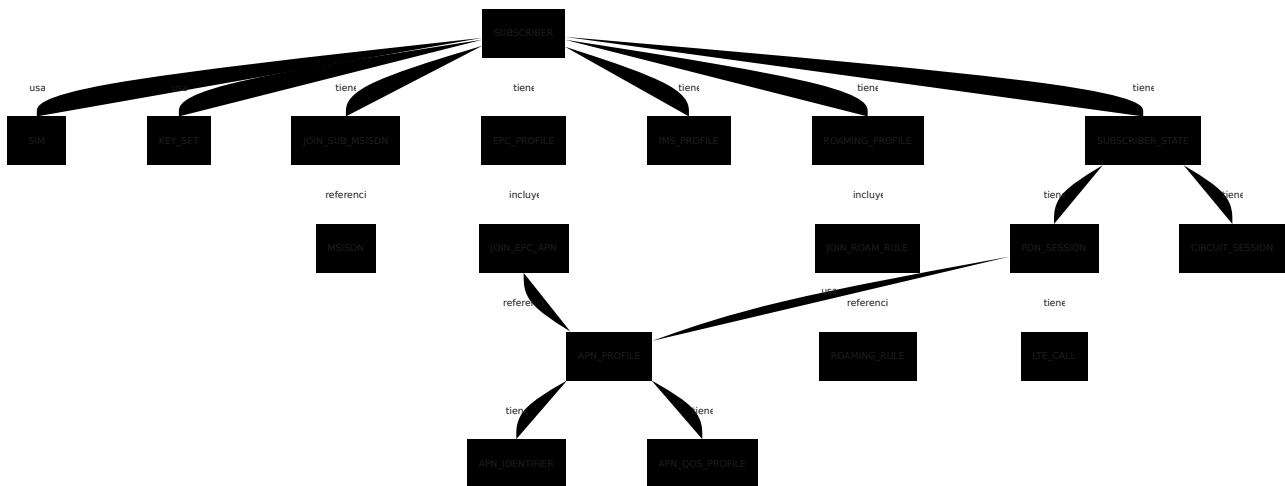


Flujo de Llamada VoLTE:

APN_QOS_PROFILE		
uuid	id	PK
string	name	UK
integer	qci	
integer	allocation_retention_priority	
integer	apn_ambr_dl_kbps	
integer	apn_ambr_ul_kbps	
boolean	pre_emption_capability	
boolean	pre_emption_vulnerability	

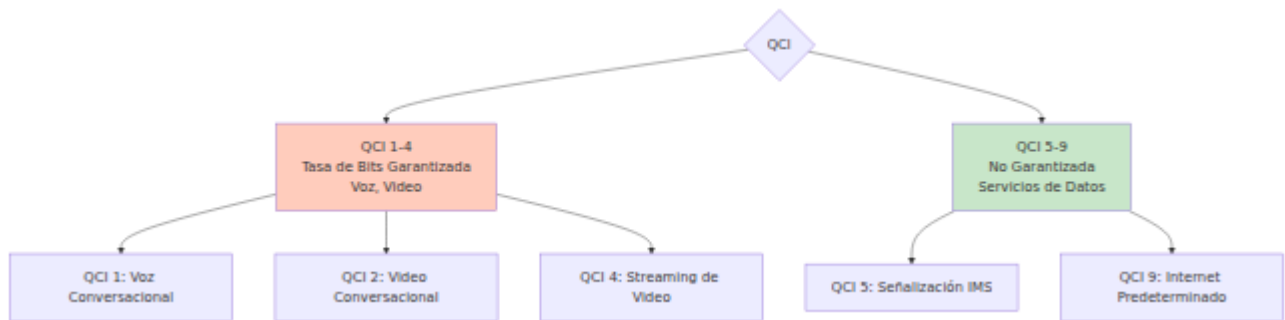
Diagramas de Relaciones de Entidad

Relaciones de Entidad Completas

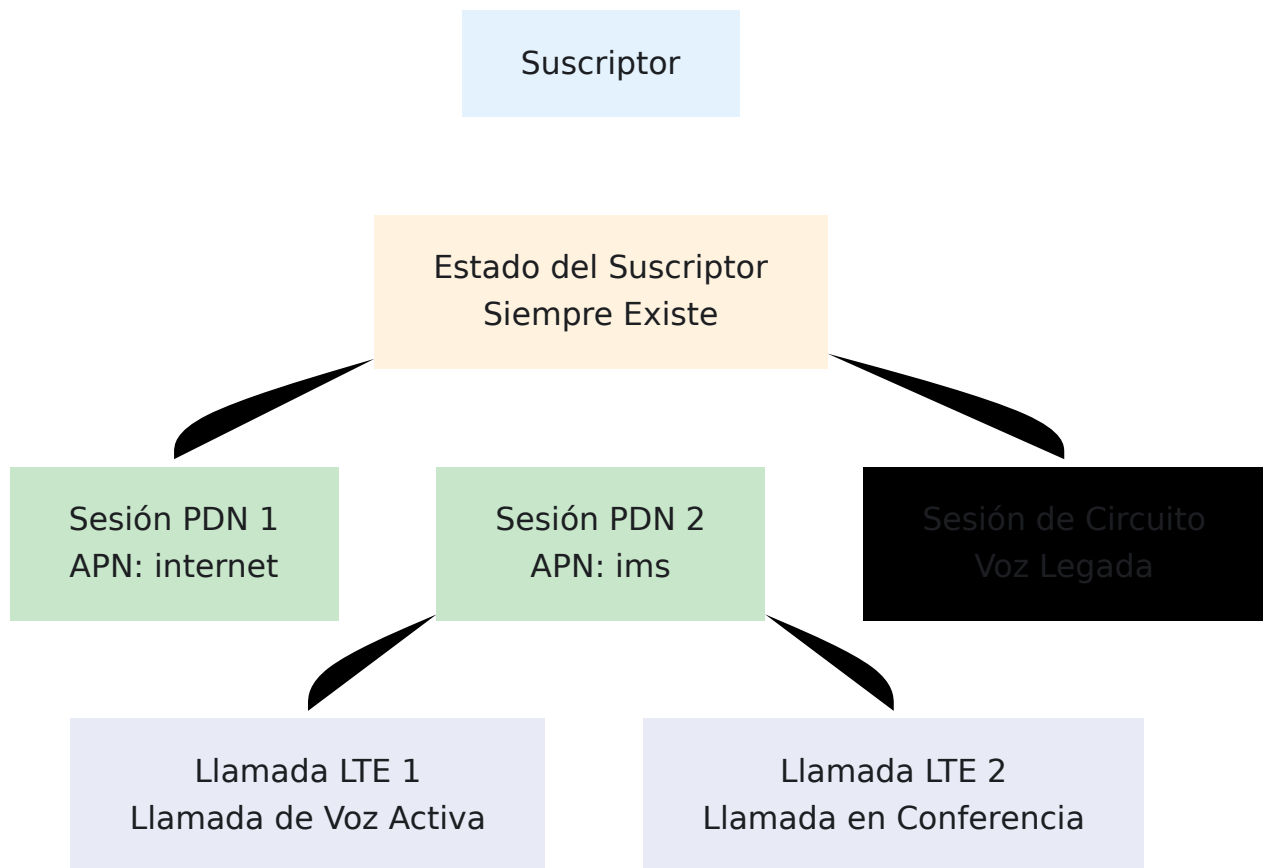


Relaciones de Aprovisionamiento

Este diagrama muestra lo que debe existir antes de crear un suscriptor:



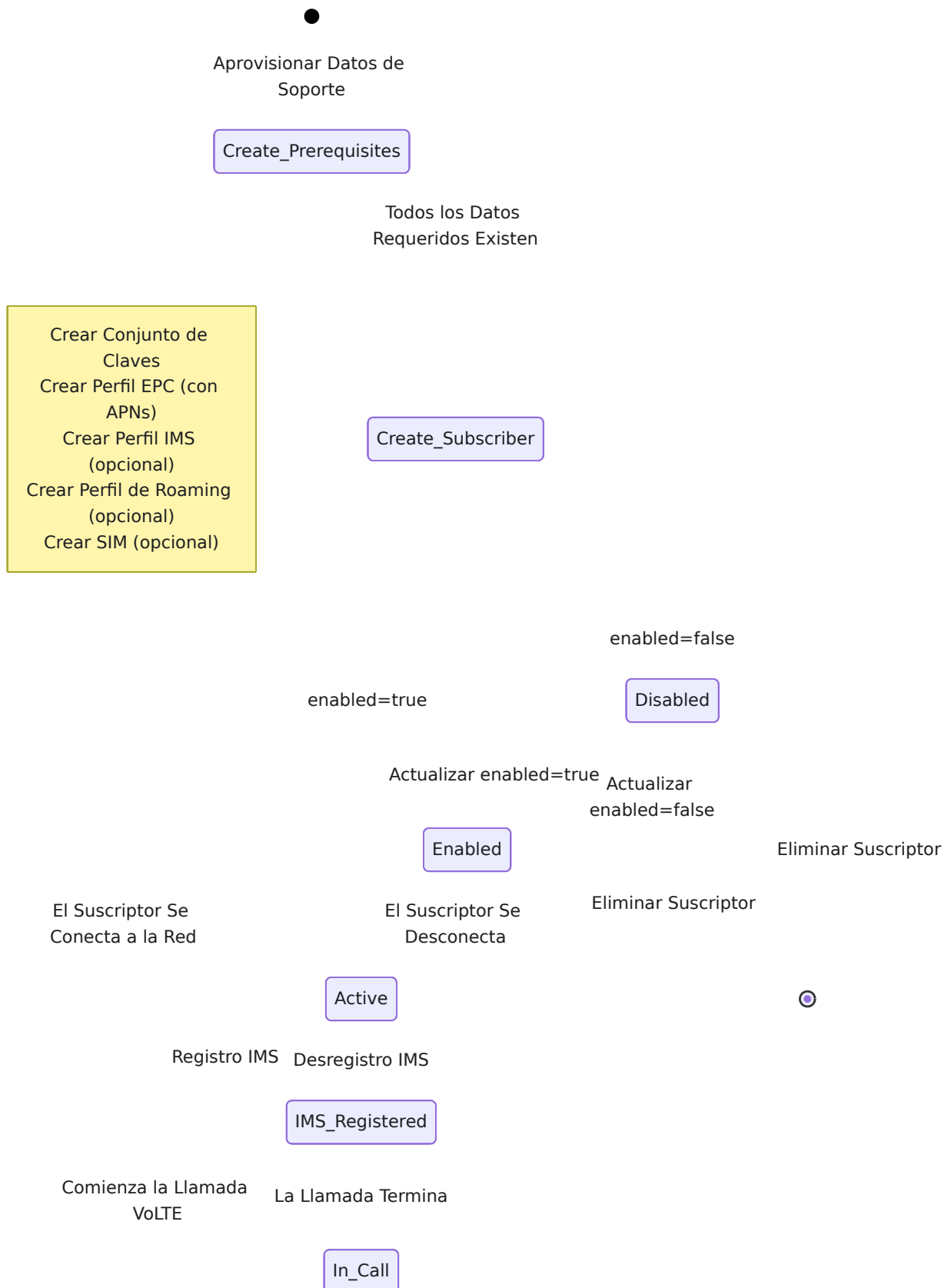
Relaciones de Estado de Sesión



Ciclo de Vida de la Entidad

Ciclo de Vida de Aprovisionamiento del

Suscriptor



Ciclo de Vida de la Sesión

ROAMING_RULE			
uuid	id	PK	
string	name	UK	
string	mcc		3 dígitos
string	mnc		2-3 dígitos
string	data_action		permitir o denegar
string	ims_action		permitir o denegar

Patrones de Flujo de Datos

Flujo de Autenticación

S6a Solicitud AIR

Buscar Suscriptor
por IMSI

Cargar Conjunto de
Claves

Verificar Perfil de
Roaming

Generar Vectores de
Autenticación
usando Milenage

S6a Respuesta AIA

Flujo de Actualización de Ubicación

S6a Solicitud ULR

Buscar Suscriptor
por IMSI

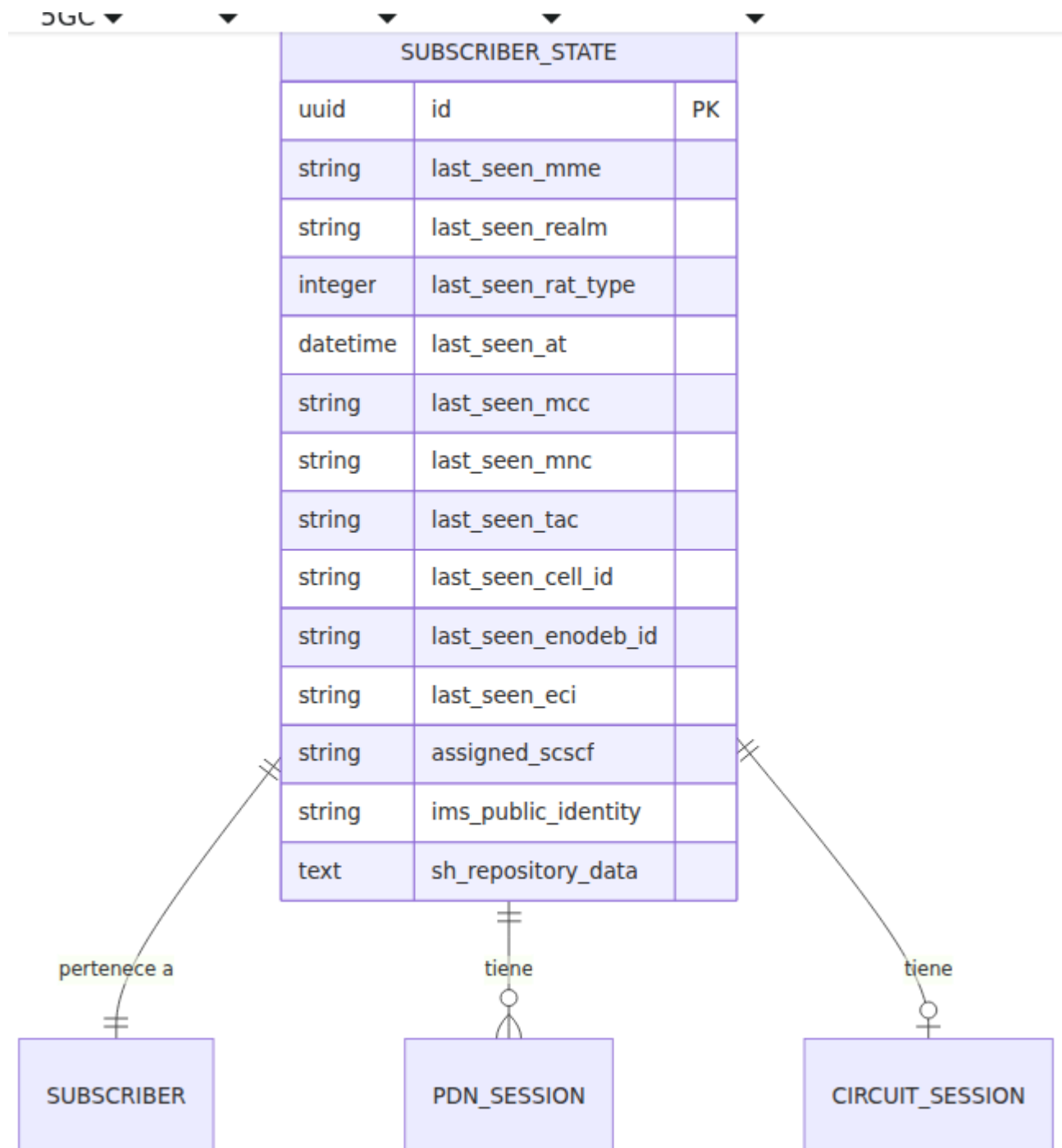
Cargar Perfil EPC
+ Perfiles APN

Actualizar Estado del
Suscriptor
Ubicación, MME, etc.

Construir Datos de
Suscripción
AMBR, APNs, QoS

S6a Respuesta ULA

Flujo de Registro IMS



Flujo de Establecimiento de Sesión

Gx Solicitud CCR-I

Buscar Suscriptor
por IMSI

Cargar Perfil APN
+ Perfil QoS

Verificar Estado de
Roaming

Crear Registro de
Sesión PDN
en Estado

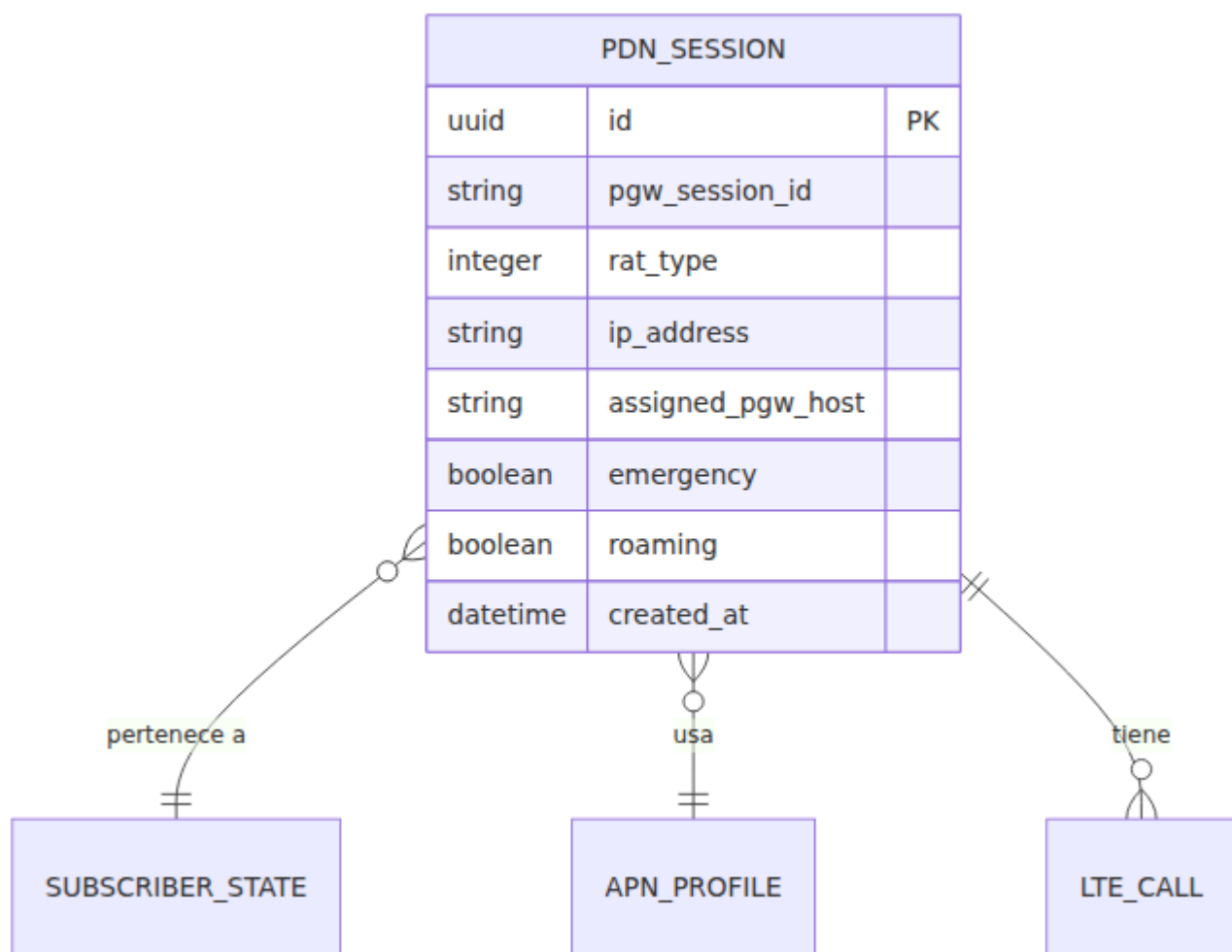
Construir Reglas QoS
AMBR, QCI, ARP

Gx Respuesta CCA-I

Patrones de Optimización de Consultas

OmniHSS optimiza las consultas a la base de datos pre-cargando selectivamente solo las asociaciones necesarias para cada operación:

Consulta Mínima (Autenticación)



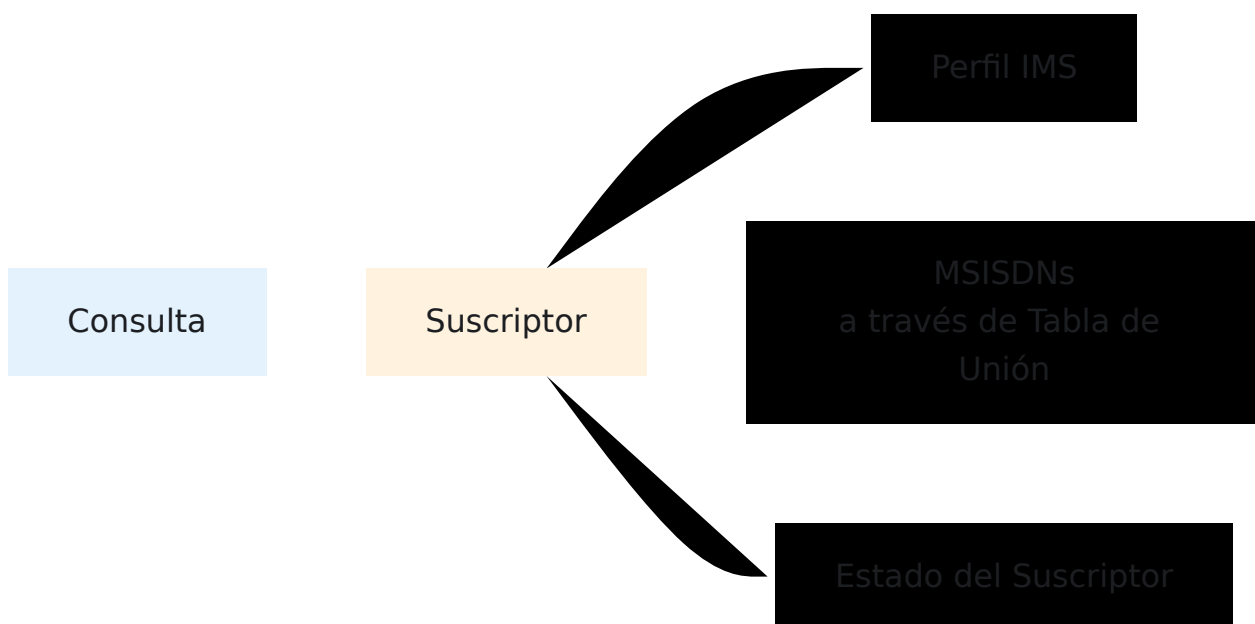
Caso de Uso: S6a AIR - Solo necesita claves criptográficas y reglas de roaming

Consulta Moderada (Actualización de Ubicación)



Caso de Uso: S6a ULR - Necesita datos completos del perfil EPC

Consulta Completa (Registro IMS)



Caso de Uso: Cx SAR - Necesita perfil IMS y todos los números de teléfono

[← Volver a la Guía de Operaciones](#) | [Siguiente: Referencia de API](#) →

Mapeo de Datos de Respuesta de Diámetro

[← Volver a la Guía de Operaciones](#)

Este documento proporciona diagramas mermaid detallados que muestran de dónde proviene cada campo en las respuestas del protocolo Diámetro en el sistema OmniHSS.

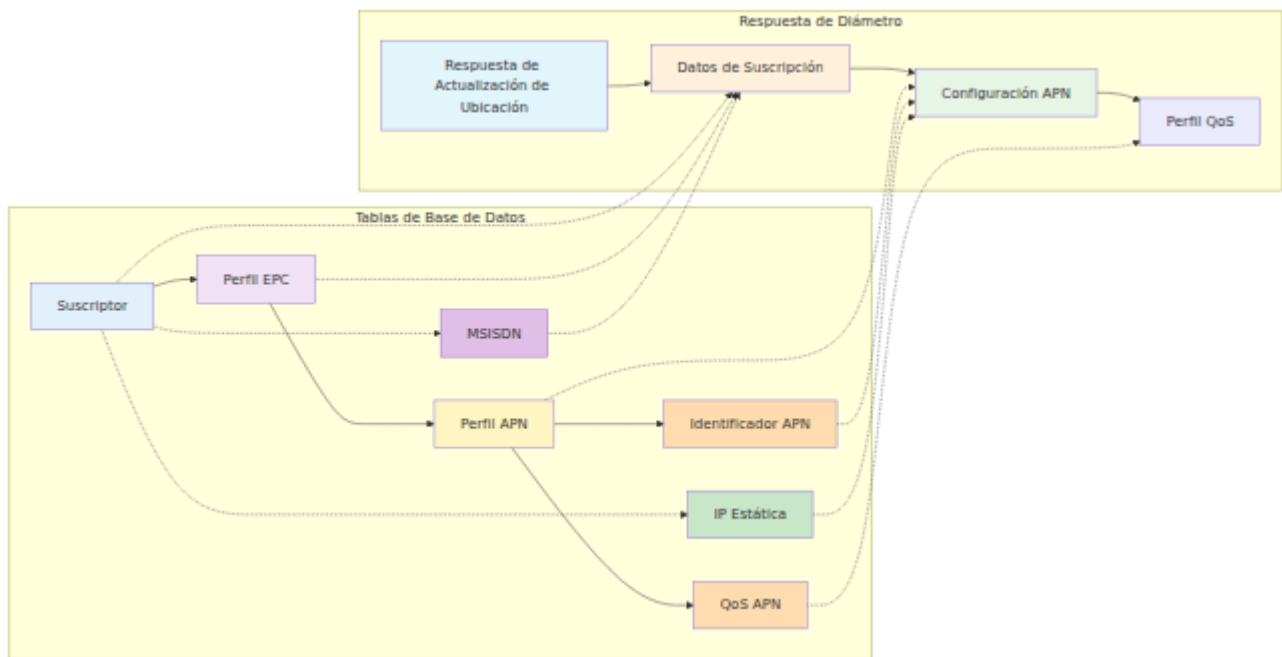
Tabla de Contenidos

- [Respuesta de Actualización de Ubicación \(S6a ULA\)](#)
 - [Respuesta de Información de Autenticación \(S6a AIA\)](#)
 - [Respuesta de Asignación de Servidor \(Cx SAA\)](#)
 - [Respuesta de Control de Crédito \(Gx CCA\)](#)
 - [Respuesta de Datos de Usuario \(Sh UDA\)](#)
 - [Respuesta de Verificación de Identidad de ME \(S13 ECA\)](#)
-

Respuesta de Actualización de Ubicación (S6a ULA)

La Respuesta de Actualización de Ubicación es enviada por el HSS al MME durante los procedimientos de conexión LTE. Este diagrama muestra el flujo completo de datos desde las tablas de la base de datos hasta los AVPs de Diámetro.

Mapeo de Fuentes de Datos



Mapecto Detallado de Campos

Fuente de Base de Datos	Campo	Descripción
subscriber.enabled	true/false	Estado de activación del suscriptor
msisdn.msisdn	'14155551234'	Número de suscriptor
epc_profile.ue_ambr_ul_kbps	50000	Velocidad máxima de transmisión de datos en el enlace de acceso (UL)
epc_profile.ue_ambr_dl_kbps	100000	Velocidad máxima de recepción de datos en el enlace de acceso (DL)
epc_profile.network_access_mode	'packet_only'	Modo de acceso a la red (solo paquetes)
apn_identifier.apn	'internet'	Nombre de punto de acceso (APN)
apn_identifier.ip_version	'ipv4v6'	Versión de protocolo de Internet (IPv4 o IPv6)
apn_qos_profile.qci	9	Clase de servicio (QoS)

Fuente de Base de Datos	Campo	D
apn_qos_profile.allocation_retention_priority	8	Pr Le
apn_qos_profile.pre_emption_capability	false	Pr en Ca
apn_qos_profile.pre_emption_vulnerability	true	Pr en Vu
apn_qos_profile.apn_ambr_ul_kbps	25000	AF UL
apn_qos_profile.apn_ambr_dl_kbps	50000	AF DL
static_ip.ipv4_static_ip	'100.64.1.1'	Se Pa Ac (IF
static_ip.ipv6_static_ip	'2606:4700::1111'	Se Pa Ac (IF

Transformaciones Clave:

- Ancho de banda AMBR:** La base de datos almacena en kbps, Diámetro espera bps (multiplicar por 1000)
- Codificación de Versión IP:** 0=IPv4, 1=IPv6, 2=IPv4v6, 3=IPv4_or_IPv6

3. **Estado del Suscriptor:** `enabled: true → 0 (SERVICIO_CONCEDIDO)`,
`enabled: false → 1 (BLOQUEO_DETERMINADO_POR_OPERADOR)`
4. **Identificador de Contexto:** Numeración secuencial (0, 1, 2...) para cada APN en el perfil
5. **IP Estática:** Solo incluida si se asigna a través de `static_ips` relación muchos a muchos

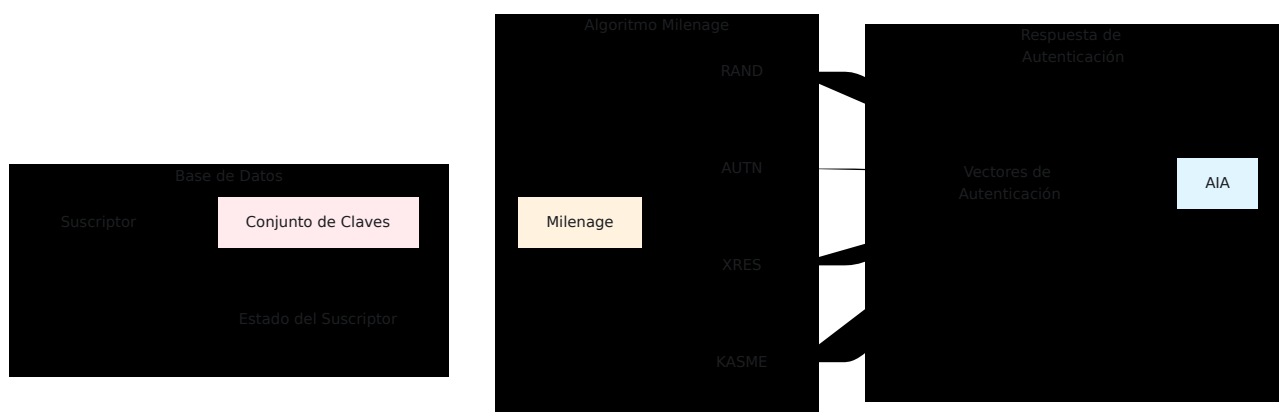
Validación de Lógica Empresarial:

- Verificación de itinerancia: Coincidir PLMN visitado contra `roaming_profile.roaming_rules`
- Verificación de suscriptor habilitado: `subscriber.enabled == true`
- Filtrar APNs: Puede excluir APNs de IMS si la política de itinerancia niega IMS

Respuesta de Información de Autenticación (S6a AIA)

La Respuesta de Información de Autenticación proporciona vectores de autenticación para suscriptores LTE/EPC.

Mapecto de Fuentes de Datos



Componentes Clave:

1. **Claves Criptográficas:** Todas las claves se almacenan como cadenas hexadecimales en la tabla `key_set`

2. **Gestión de SQN:** Número de secuencia incrementado después de cada generación de vector de autenticación (previene ataques de repetición)
3. **Algoritmo Milenage:** 3GPP TS 35.206 - genera vectores de autenticación
4. **Derivación de KASME:** Clave derivada de CK||IK usando KDF según TS 33.401

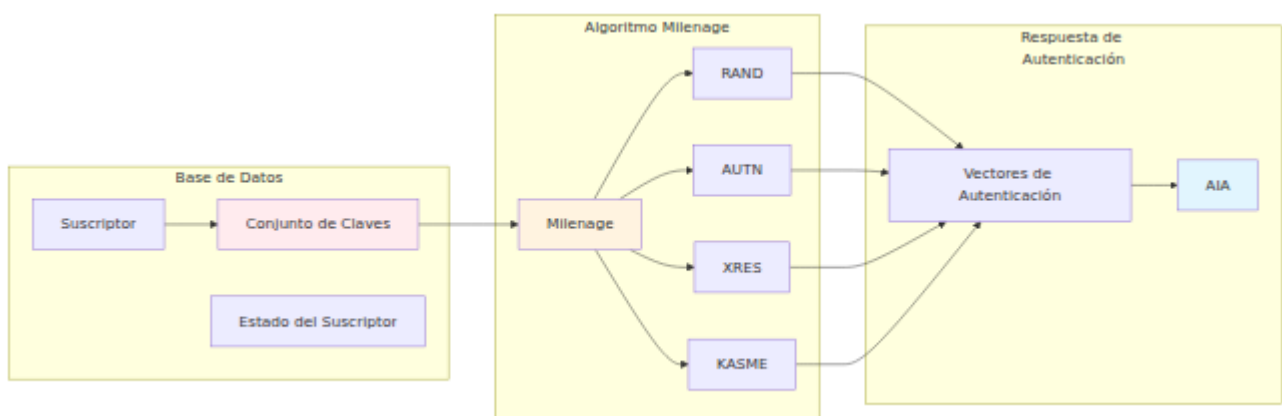
Características de Seguridad:

- SQN almacenado por suscriptor (no global)
- Ki/OPc nunca salen del HSS (solo se transmiten valores derivados)
- AUTN incluye número de secuencia (SQN) y AMF para autenticación de red
- El algoritmo Milenage proporciona autenticación mutua entre UE y red

Respuesta de Asignación de Servidor (Cx SAA)

La Respuesta de Asignación de Servidor es enviada por el HSS al S-CSCF durante el registro IMS.

Mapecto de Fuentes de Datos



Características Clave:

1. **Plantilla IFC:** Plantilla XML almacenada en `ims_profile.ifc_template`
2. **Sustitución Dinámica:** Reemplaza `{{msisdn}}`, `{{imsi}}`, `{{impu}}` en tiempo de ejecución

3. **Asignación de S-CSCF:** Almacena S-CSCF asignado en

`subscriber_state.assigned_scscf`

4. **Identidad Pública IMS:** Formato: `sip:+{msisdn}@{ims_domain}` o `tel:++{msisdn}`

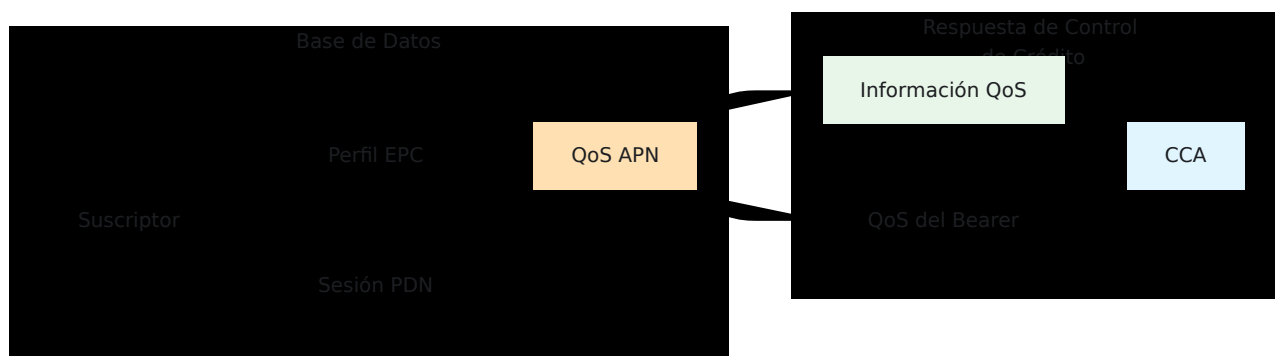
Parámetros de Plantilla IFC:

- `{{msisdn}}` - Primer MSISDN del suscriptor
- `{{imsi}}` - IMSI del suscriptor
- `{{impu}}` - Identidad Pública de Usuario IMS (del estado del suscriptor)
- `{{impi}}` - Identidad Privada de Usuario IMS (típicamente IMSI@realm)

Respuesta de Control de Crédito (Gx CCA)

La Respuesta de Control de Crédito es enviada por la función PCRF al PGW durante el establecimiento del bearer.

Mapeo de Fuentes de Datos



Características Clave:

1. **Seguimiento de Sesiones:** Crea/actualiza el registro `pdn_session` para cada bearer
2. **Aplicación de QoS:** Proporciona QCI y límites de ancho de banda del perfil QoS de APN

3. **Reglas de Cobro:** Devuelve reglas de cobro predeterminadas para la integración de facturación
4. **CC-Request-Type:** Maneja INITIAL (1), UPDATE (2), TERMINATION (3)

Gestión del Estado de Sesión:

- **INITIAL_REQUEST:** Crea un nuevo registro de sesión PDN
 - **UPDATE_REQUEST:** Actualiza la sesión PDN existente
 - **TERMINATION_REQUEST:** Elimina el registro de sesión PDN
-

Respuesta de Datos de Usuario (Sh UDA)

La Respuesta de Datos de Usuario es enviada por el HSS al AS (Servidor de Aplicaciones) a través de la interfaz Sh.

Mapecto de Fuentes de Datos



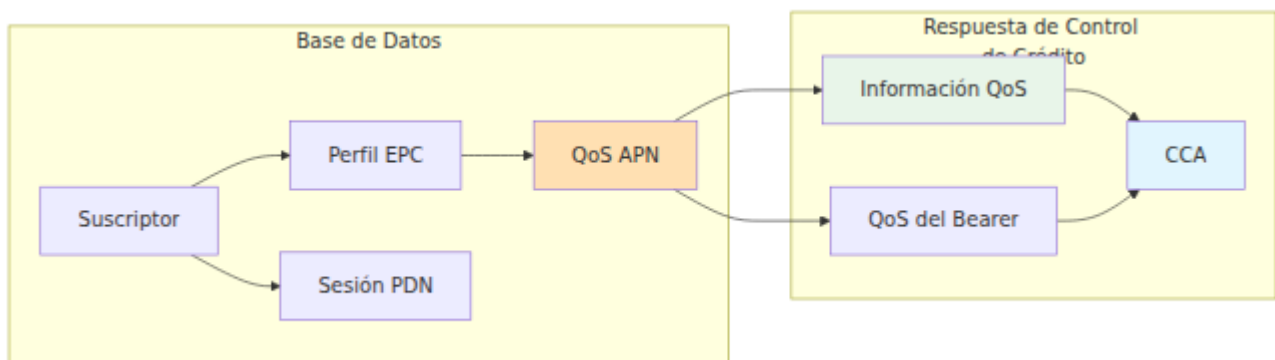
Características Clave:

1. **Datos del Repositorio:** Puede almacenar XML personalizado en `subscriber_state.sh_repository_data`
 2. **Indicación de Servicio:** Filtra datos por servicio solicitado (por ejemplo, presencia, mensajería)
 3. **Identidades Públicas:** Devuelve todas las identidades públicas IMS para el suscriptor
 4. **Referencia vs Transparente:** Soporta ambos modos de datos de referencia y transparentes
-

Respuesta de Verificación de Identidad de ME (S13 ECA)

La Respuesta de Verificación de Identidad de ME es enviada por la función EIR al MME para la validación de IMEI.

Mapecto de Fuentes de Datos



Características Clave:

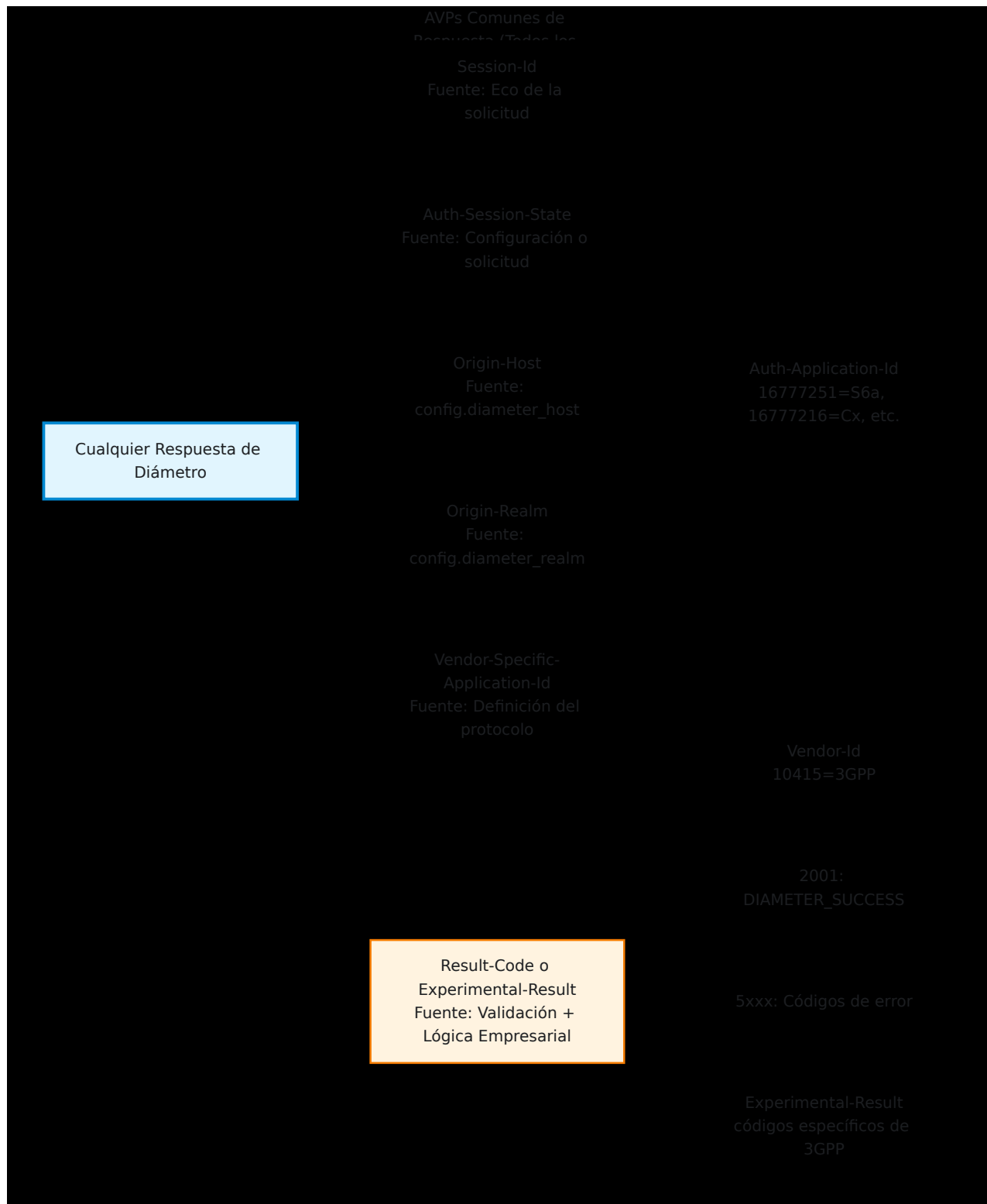
1. **Coincidencia de Regex de IMEI:** Las reglas utilizan expresiones regulares para coincidencias flexibles
2. **Reglas basadas en TAC:** Puede coincidir el Código de Asignación de Tipo (primeros 8 dígitos)
3. **Comportamiento Predeterminado:** Configurable para IMEIs desconocidos (aceptar o rechazar)
4. **Valores de Estado del Equipo:**
 - 0 = LISTA BLANCA (permitido explícitamente)
 - 1 = LISTA NEGRA (robado/bloqueado)
 - 2 = LISTA GRIS (permitido pero monitoreado)
 - 5 = DESCONOCIDO (sin regla coincidente)

Casos de Uso:

- Bloquear dispositivos robados por IMEI exacto
- Bloquear modelos de dispositivos por patrón TAC
- Solo permitir dispositivos aprobados
- Rastrear dispositivos del mercado gris

Elementos Comunes de Respuesta

Todas las respuestas de Diámetro comparten estos AVPs comunes:

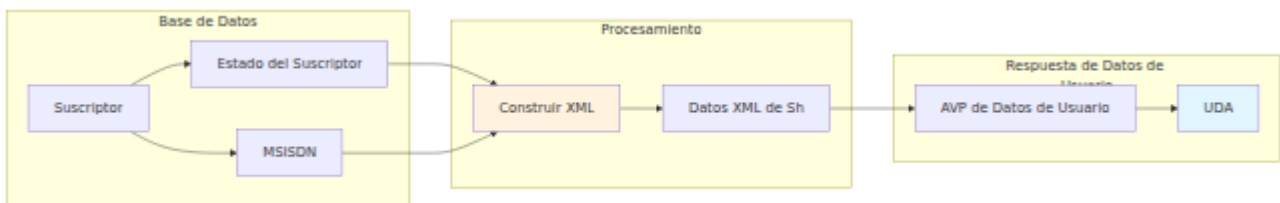


Ejemplo de Configuración:

```
config :diameter_ex,  
  diameter_host: "hss",  
  diameter_realm: "example.com",  
  diameter_service_name: "OmniHSS"
```

Resumen del Flujo de Datos

Pipeline de Procesamiento de Solicitudes



Notas de Implementación

Controladores de Protocolo

El sistema implementa controladores para los siguientes protocolos de Diámetro:

- **S6a** - Interfaz LTE/MME para autenticación y actualizaciones de ubicación
- **Cx** - Interfaz IMS/CSCF para registro IMS y asignación de servidor
- **Sh** - Interfaz IMS/AS para recuperación de datos de suscriptor
- **Gx** - Interfaz PCRF para control de políticas y cobro
- **Rx** - Interfaz IMS/AF para autorización de medios
- **S13** - Interfaz EIR para validación de IMEI
- **SWx** - Interfaz WiFi/IMS para autenticación de acceso no 3GPP

Modelos de Datos

El esquema de la base de datos incluye las siguientes entidades centrales:

- **Suscriptor** - Registro central del suscriptor con IMSI
- **Conjunto de Claves** - Claves criptográficas para autenticación
- **Perfil EPC** - Configuración del servicio LTE
- **Perfil APN** - Configuración del punto de acceso
- **Perfil IMS** - Configuración del servicio IMS con plantillas IFC
- **Perfil de Itinerancia** - Reglas y restricciones de itinerancia
- **Estado del Suscriptor** - Seguimiento dinámico de sesiones y estados
- **Sesión PDN** - Seguimiento de sesiones de bearer activas
- **IP Estática** - Asignaciones de direcciones IP estáticas
- **Regla EIR** - Reglas de validación de IMEI

[← Volver a la Guía de Operaciones](#) | [Referencia de API](#) → | [Flujos de Protocolo](#) →

Guía de Métricas y Monitoreo de OmniHSS

[← Volver a la Guía de Operaciones](#)

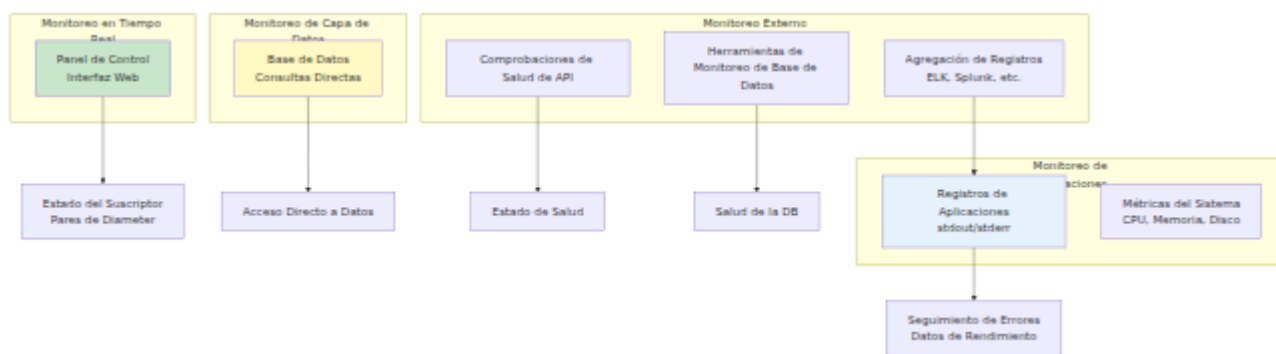
Tabla de Contenidos

- [Descripción General del Monitoreo](#)
 - [Monitoreo del Panel de Control](#)
 - [Monitoreo de la Base de Datos](#)
 - [Monitoreo de Registros](#)
 - [Integración de Monitoreo Externo](#)
 - [Indicadores Clave de Rendimiento](#)
 - [Estrategias de Alertas](#)
-

Descripción General del Monitoreo

OmniHSS proporciona varios mecanismos para monitorear la salud del sistema, el rendimiento y la actividad de los suscriptores. El personal de operaciones debe utilizar una combinación de estas herramientas para una visibilidad completa.

Capas de Monitoreo



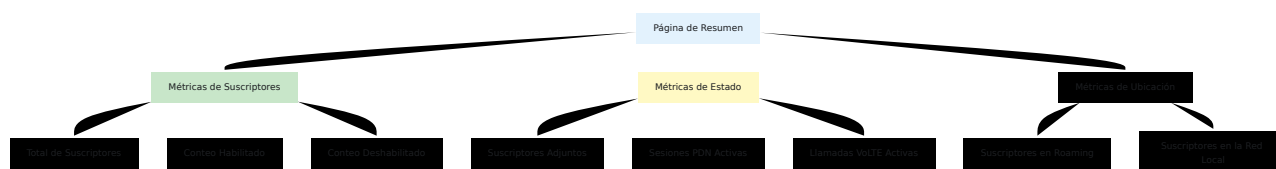
Monitoreo del Panel de Control

El Panel de Control proporciona la interfaz principal de monitoreo en tiempo real.

Monitoreo de la Página de Resumen

URL: `https://[hostname]:7443/overview`

Métricas Clave Disponibles



Estados de Suscriptores Monitoreados

Estado	Indicador	Lo Que Significa
Inactivo	Sin información de ubicación	Suscriptor apagado o fuera de cobertura
Adjunto	MME presente	Suscriptor registrado en la red
PDN Activo	Conteo de sesiones PDN > 0	Conexión de datos activa
IMS Registrado	S-CSCF asignado	Servicios de voz listos
En Llamada	Conteo de llamadas activas > 0	Llamada VoLTE en progreso

Extracción de Métricas del Resumen

El Panel de Control no exporta métricas directamente. Puedes:

1. **Contar filas visibles** para el total de suscriptores
2. **Buscar marcas de verificación verdes** para contar suscriptores habilitados
3. **Revisar detalles ampliados** para información de estado
4. **Anotar marcas de tiempo de última vista** para la capacidad de respuesta

Monitoreo de la Página de Diameter

URL: `https://[hostname]:7443/diameter`

Métricas Clave



Monitoreo de Pares Críticos

Identifica pares críticos y monitorea su estado:

Tipo de Par	Criticidad	Impacto si Está Caído
MME	Alto	No hay nuevos adjuntos LTE
P-GW	Alto	No hay sesiones de datos
S-CSCF	Alto	No hay registros IMS
P-CSCF	Alto	No hay llamadas VoLTE
I-CSCF	Medio	Problemas de enrutamiento IMS
AS	Bajo-Medio	Servicio específico no disponible

Monitoreo de la Página de Aplicaciones

URL: `https://[hostname]:7443/application`

Métricas Clave

Métrica	Descripción	Rango Normal	Umbral de Acción
Conteo de Procesos	Procesos Erlang activos	Varía según la carga	> 90% del límite
Uso de Memoria	Memoria total consumida	< 80%	> 90%
Tiempo de Actividad	Tiempo desde el último reinicio	N/A	Seguimiento para estabilidad

Monitoreo de la Base de Datos

Consultas Directas a la Base de Datos

Conéctate a la Base de Datos SQL para extraer métricas detalladas:

Conteos de Suscriptores

Consulta la base de datos para recuperar:

- Conteo total de todos los suscriptores
- Conteo de suscriptores habilitados
- Conteo de suscriptores habilitados para IMS

Estadísticas de Sesiones

Consulta la base de datos para recuperar:

- Conteo de sesiones PDN activas
- Conteo de llamadas VoLTE activas
- Desglose de sesiones PDN por perfil APN

Estadísticas de Ubicación

Consulta la base de datos para recuperar:

- Conteo de suscriptores agrupados por red visitada (combinación MCC-MNC)
- Conteo de suscriptores actualmente en roaming (no en PLMN local 001-001)
- Distribución de suscriptores a través de diferentes redes visitadas

Actividad Reciente

Consulta la base de datos para recuperar:

- Conteo de suscriptores vistos en la última hora
- Distribución de suscriptores por MME que sirve
- Análisis de marcas de tiempo de la última actividad del suscriptor

Monitoreo de Salud de la Base de Datos

Monitorea la salud de la base de datos consultando:

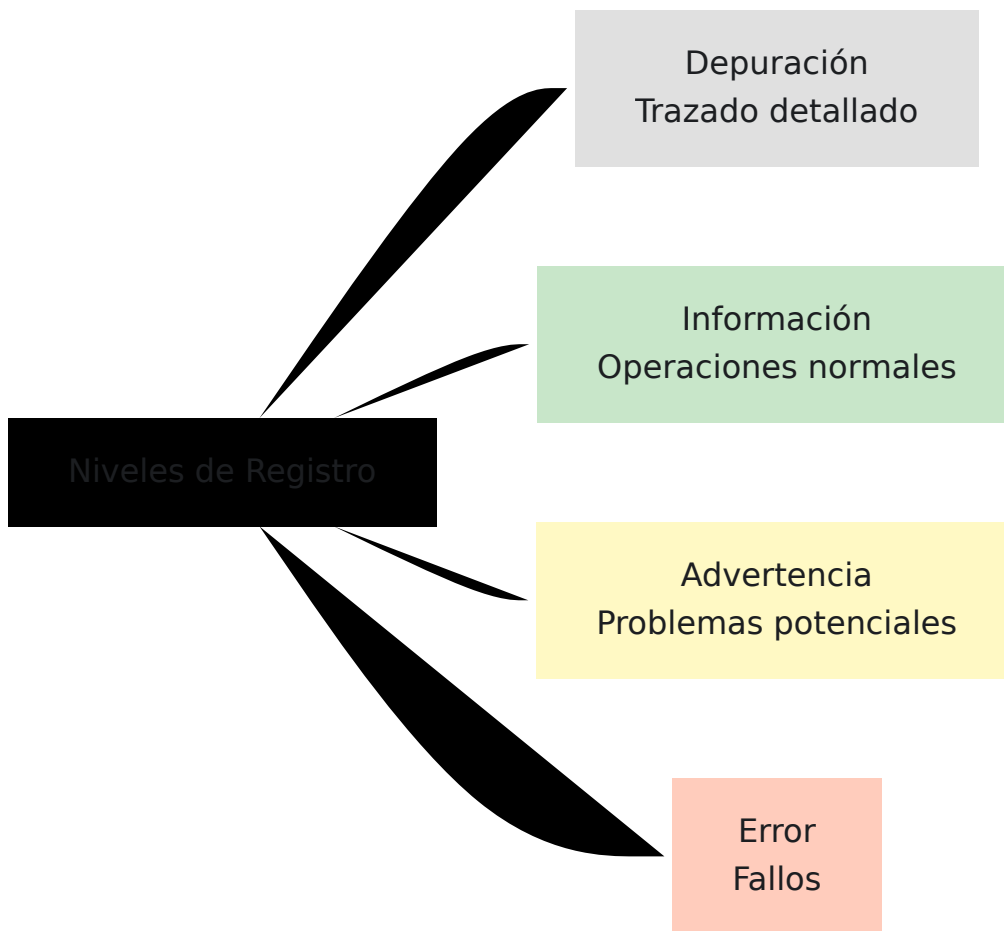
- Tamaño total de la base de datos y tendencias de crecimiento
 - Tamaños de tablas individuales y conteos de filas
 - Conteo actual de conexiones a la base de datos
 - Rendimiento de consultas y uso de recursos
-

Monitoreo de Registros

Salida de Registros

OmniHSS genera registros en **stdout/stderr**, que deben ser capturados por tu administrador de procesos.

Niveles de Registro



Patrones Clave de Registro a Monitorear

Eventos de Pares de Diameter:

```
[info] Par de Diameter conectado: mme01.epc.example.com  
[warn] Par de Diameter desconectado: pgw01.epc.example.com  
[error] Fallo en la conexión del par de Diameter: tiempo de espera
```

Eventos de Base de Datos:

```
[info] Conexión a la base de datos establecida  
[error] Conexión a la base de datos perdida: tiempo de espera  
[error] Consulta de base de datos fallida: bloqueo detectado
```

Eventos de Autenticación:


```
[info] Autenticación exitosa: IMSI 001001123456789  
[warn] Fallo en la autenticación: IMSI 001001123456789, vector  
inválido  
[error] Roaming denegado: IMSI 001001123456789, MCC 310 MNC 410
```

Agregación de Registros

Para implementaciones en producción, implementa la agregación de registros:

OmniHSS

stdout/stderr

Administrador de
Procesos
systemd, supervisord

Archivos de Registros

Agregador de Registros

Pila ELK

Splunk

Registro en la Nube
CloudWatch, Stackdriver

Tableros

Integración de Monitoreo Externo

Endpoint de Comprobación de Salud

Comprobación de Salud de API: GET /api/status

```
curl -k https://hss.example.com:8443/api/status
```

Respuesta Esperada:

```
{"status": "ok"}
```

Estado HTTP: 200 OK

Integración de Herramientas de Monitoreo

Ejemplo de Nagios/Icinga

```
#!/bin/bash
# check_omnihss.sh

API_URL="https://hss.example.com:8443/api/status"

response=$(curl -k -s -o /dev/null -w "%{http_code}" "$API_URL" --max-time 5)

if [ "$response" = "200" ]; then
    echo "OK - API de OmniHSS respondiendo"
    exit 0
else
    echo "CRÍTICO - API de OmniHSS no responde (HTTP $response)"
    exit 2
fi
```

Integración con Prometheus

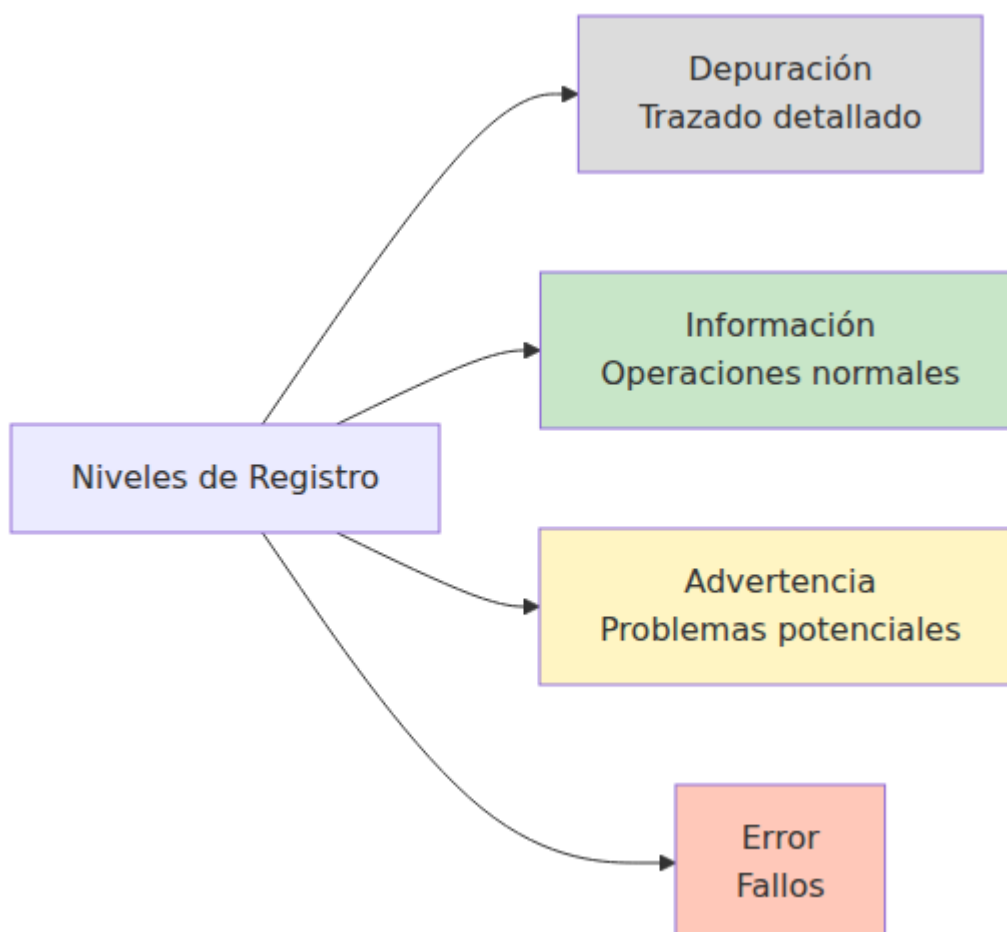
Se pueden crear exportadores personalizados para exportar métricas de OmniHSS a Prometheus consultando la API y la base de datos.

Integración SNMP

Para el monitoreo basado en SNMP, se pueden crear scripts de extensión SNMP personalizados que consulten la base de datos o la API para métricas y devuelvan valores a través de OIDs SNMP.

Indicadores Clave de Rendimiento

KPIs Operativos



Umbrales de KPI Recomendados

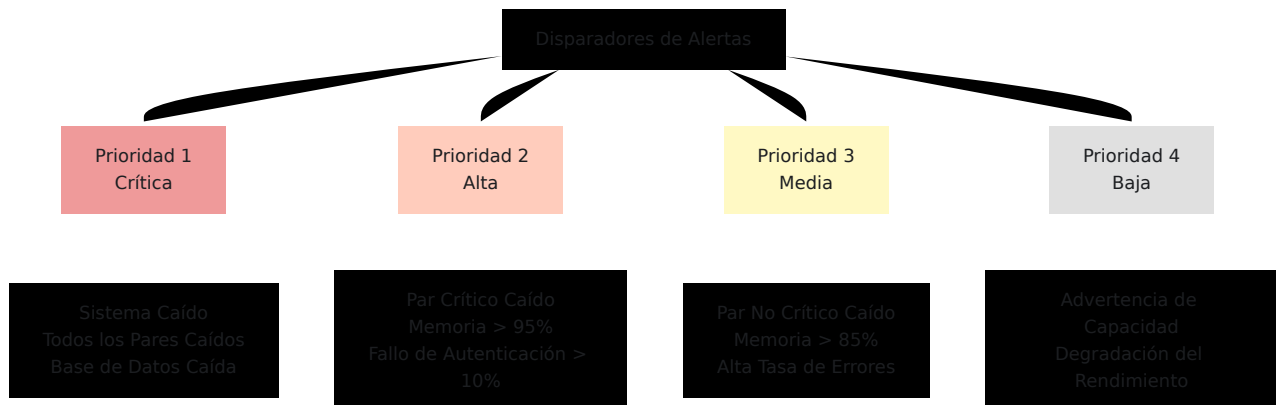
KPI	Objetivo	Advertencia	Crítico
Tiempo de Actividad del Sistema	99.99%	< 99.95%	< 99.9%
Tiempo de Actividad de Pares de Diameter	99.9%	< 99.5%	< 99%
Tasa de Éxito de Autenticación	> 99%	< 99%	< 95%
Tiempo de Respuesta de Diameter	< 100ms	> 200ms	> 500ms
Tiempo de Consulta de Base de Datos	< 50ms	> 100ms	> 500ms
Tasa de Errores	< 0.1%	> 0.5%	> 1%

KPIs de Capacidad

Métrica	Monitoreo	Plan de Acción en
Total de Suscriptores	Conteo actual	80% de la capacidad esperada
Sesiones PDN Concurrentes	Sesiones activas	70% del máximo esperado
Tamaño de la Base de Datos	MB utilizados	80% del almacenamiento asignado
Conexiones a la Base de Datos	Conexiones activas	80% del tamaño del grupo

Estrategias de Alertas

Prioridades de Alertas



Definiciones de Alertas

Alertas Críticas (P1)

Sistema No Disponible:

- La comprobación de salud de la API falla
- Panel de Control inaccesible
- Falla de conexión a la base de datos
- Acción: Investigación y escalamiento inmediato

Todos los Pares de Diameter Desconectados:

- Cero pares conectados
- Acción: Verificar red, reiniciar si es necesario

Base de Datos Caída:

- No se puede conectar a la Base de Datos SQL
- Acción: Investigar el servidor de base de datos, reiniciar si es necesario

Alertas de Alta Prioridad (P2)

Par Crítico de Diameter Caído:

- MME primario desconectado
- P-GW primario desconectado
- S-CSCF primario desconectado
- Acción: Investigar la conectividad del par dentro de los 15 minutos

Uso Elevado de Memoria:

- Memoria > 95%
- Acción: Investigar fuga de memoria, planificar reinicio

Alta Tasa de Fallos de Autenticación:

- 10% de las solicitudes de autenticación fallan
- Acción: Verificar la provisión de suscriptores, investigar la causa

Alertas de Prioridad Media (P3)

Par No Crítico Caído:

- Par secundario desconectado
- Servidor de Aplicaciones desconectado
- Acción: Investigar dentro de 1 hora

Uso Elevado de Memoria:

- Memoria > 85%
- Acción: Monitorear tendencia, planificar actualización de capacidad

Tasa Elevada de Errores:

- Tasa de errores > 1%
- Acción: Revisar registros, identificar causa raíz

Alertas de Baja Prioridad (P4)

Advertencia de Capacidad:

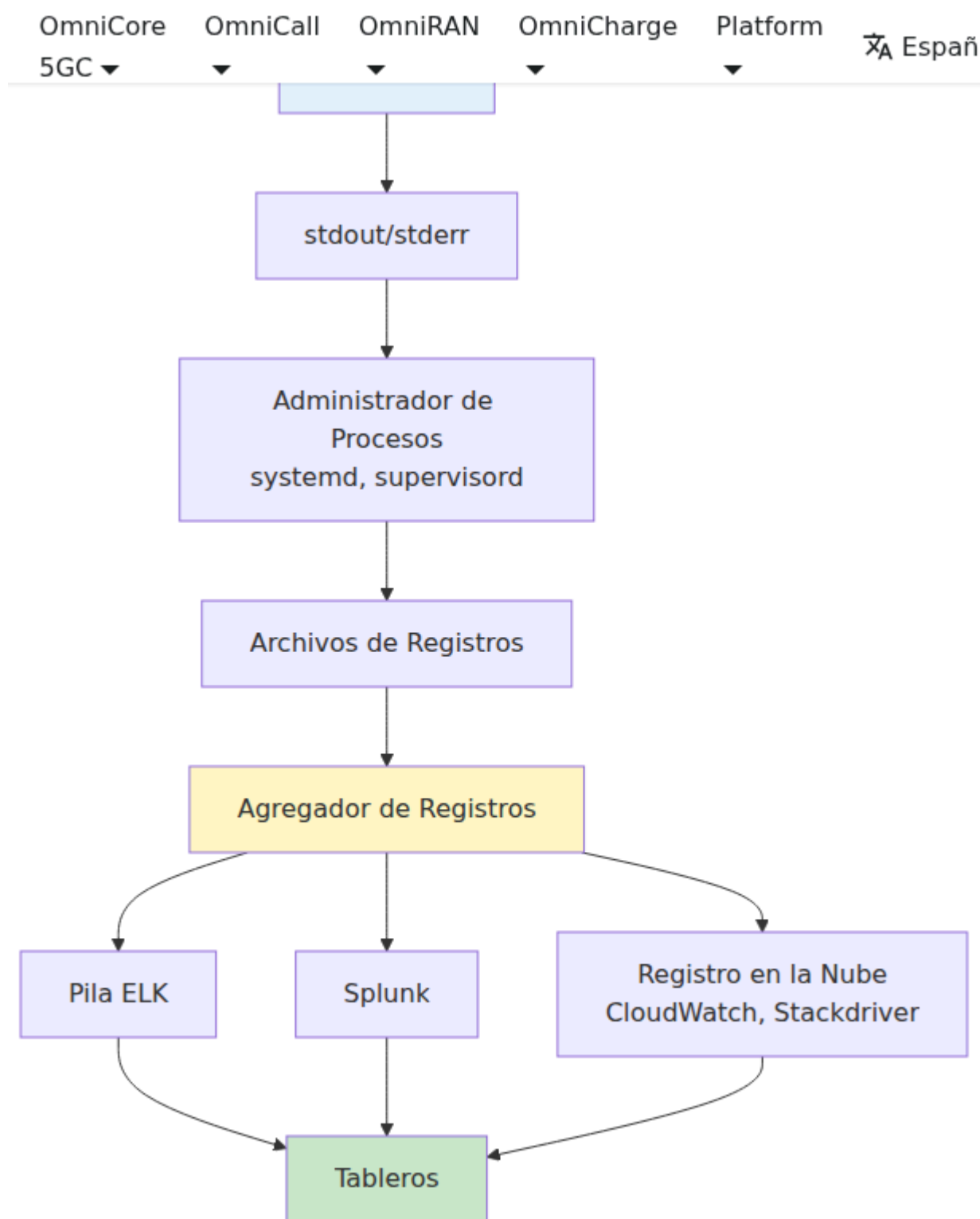
- Suscriptores > 80% de la capacidad
- Base de Datos > 80% del almacenamiento asignado

- Acción: Planificar expansión de capacidad

Degradación del Rendimiento:

- Tiempos de respuesta elevados pero aceptables
- Acción: Monitorear y optimizar consultas

Canales de Notificación de Alertas



Lista de Verificación de Monitoreo

Comprobaciones Diarias

- ☐ Revisar Resumen del Panel de Control - conteos de suscriptores normales
- ☐ Revisar página de Diameter - todos los pares críticos conectados
- ☐ Revisar página de Aplicaciones - memoria y procesos dentro de los límites
- ☐ Comprobar registros de errores - sin errores críticos en las últimas 24 horas
- ☐ Verificar que la copia de seguridad se completó con éxito

Comprobaciones Semanales

- ☐ Revisar tendencias de capacidad - crecimiento de suscriptores
- ☐ Revisar tendencias de rendimiento - tiempos de respuesta
- ☐ Revisar tamaño de la base de datos - tasa de crecimiento aceptable
- ☐ Revisar tasas de errores - identificar patrones
- ☐ Probar notificaciones de alertas - asegurar funcionamiento

Comprobaciones Mensuales

- ☐ Revisión de planificación de capacidad - proyectar 6 meses hacia adelante
- ☐ Revisión de optimización de rendimiento - identificar consultas lentas
- ☐ Revisión de seguridad - expiración de certificados, vulnerabilidades
- ☐ Revisión de documentación - actualizar manuales de operación
- ☐ Prueba de recuperación ante desastres - verificar que las copias de seguridad se restauren correctamente

[← Volver a la Guía de Operaciones](#) | [Siguiendo: Múltiples Características](#) →

Funciones Multi-MSISDN y Multi-IMSI de OmniHSS

[← Volver a la Guía de Operaciones](#)

Tabla de Contenidos

- [Descripción General](#)
 - [Multi-MSISDN: Múltiples Números de Teléfono](#)
 - [SIM Multi-IMSI: Múltiples Identidades de Red](#)
 - [Escenarios Combinados](#)
 - [Ejemplos de Configuración](#)
 - [Procedimientos Operativos](#)
-

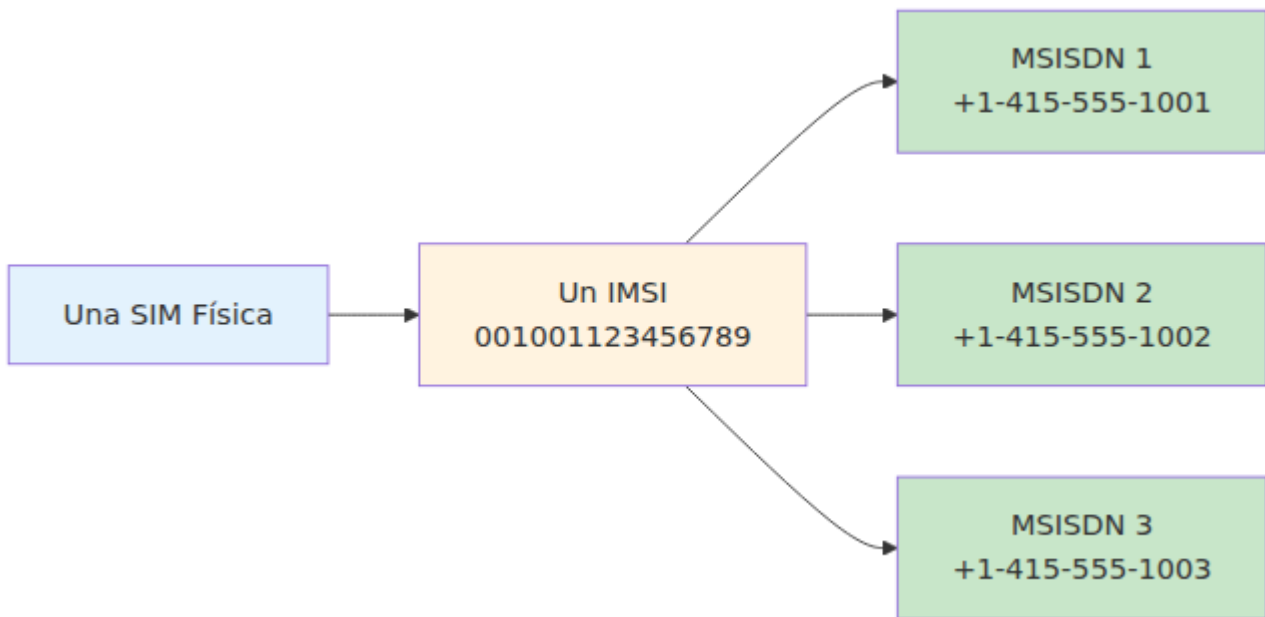
Descripción General

OmniHSS admite capacidades avanzadas de aprovisionamiento que permiten configuraciones de servicio flexibles:

Soporte Multi-MSISDN

Un IMSI → Múltiples Números de Teléfono

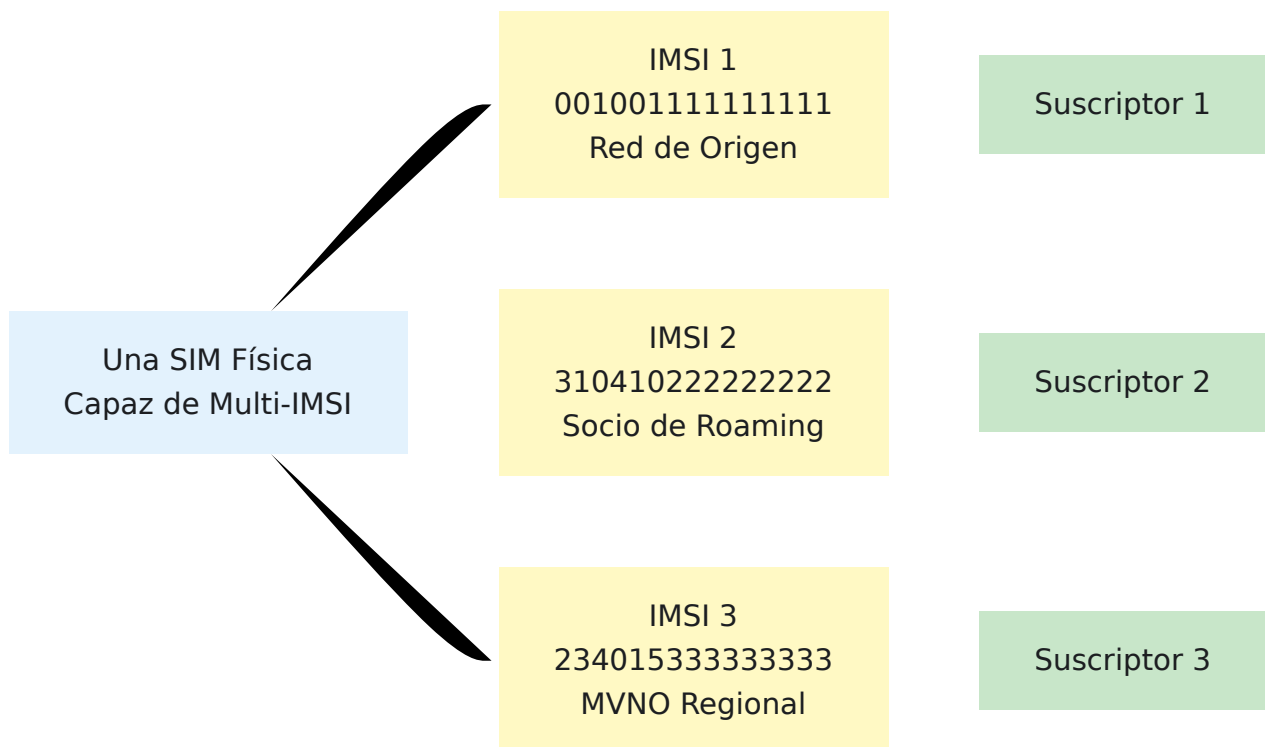
Un único suscriptor (identificado por un IMSI) puede tener múltiples MSISDN (números de teléfono) asignados. Todos los números suenan en el mismo dispositivo y comparten los mismos perfiles de servicio.



Soporte de SIM Multi-IMSI

Una SIM → Múltiples IMSIs

Una única tarjeta SIM física puede contener múltiples IMSIs, lo que permite que el dispositivo se conecte a diferentes redes utilizando diferentes identidades de red. Esto es útil para escenarios de roaming internacional y MVNO.



Multi-MSISDN: Múltiples Números de Teléfono

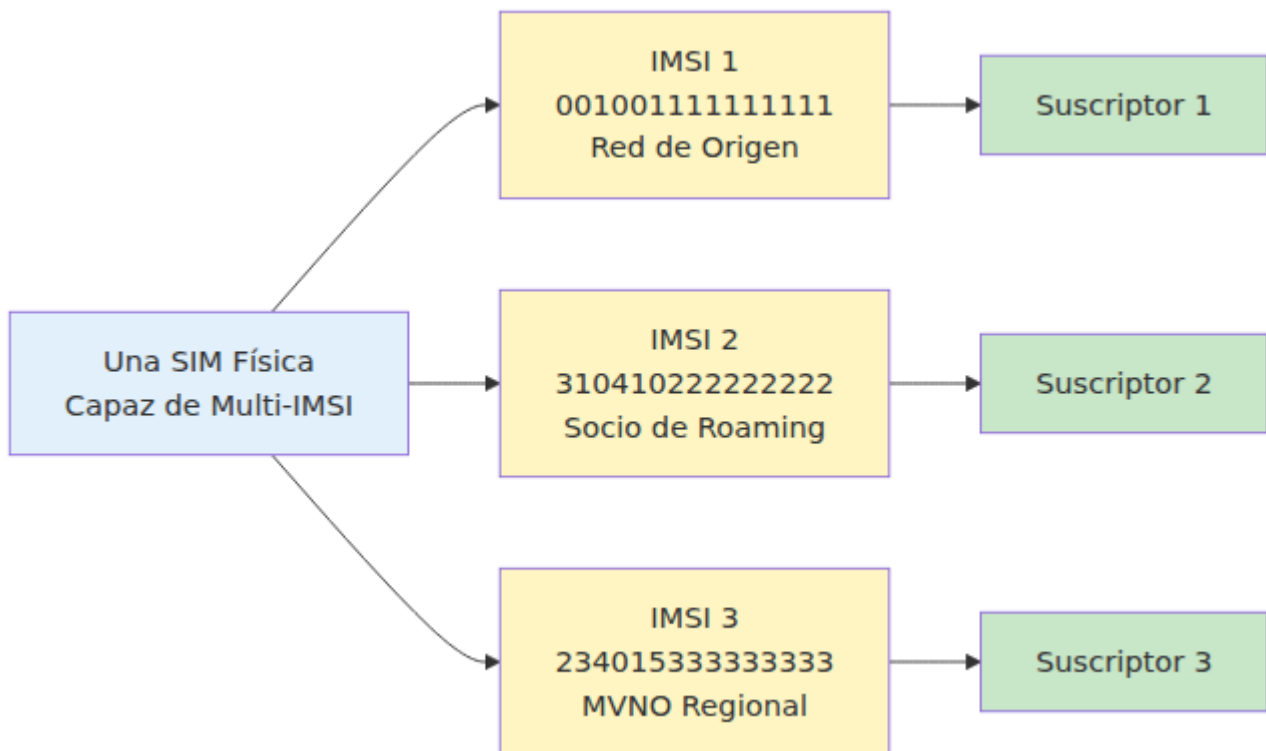
Cómo Funciona

Un registro de suscriptor en el HSS tiene múltiples MSISDN vinculados a través de una tabla de unión. Cuando el suscriptor se registra en IMS, todos los MSISDN se incluyen en el perfil de IMS, permitiendo que las llamadas entrantes a cualquier número lleguen al dispositivo.

Características Clave

- **Un IMSI** - El suscriptor tiene un único IMSI vinculado a su tarjeta SIM
- **Múltiples MSISDNs** - El suscriptor puede tener múltiples números de teléfono
- **Integración IMS** - Todos los MSISDN están registrados en IMS
- **Servicio Compartido** - Todos los números comparten los mismos perfiles de servicio (EPC, IMS, Roaming)

Modelo de Datos

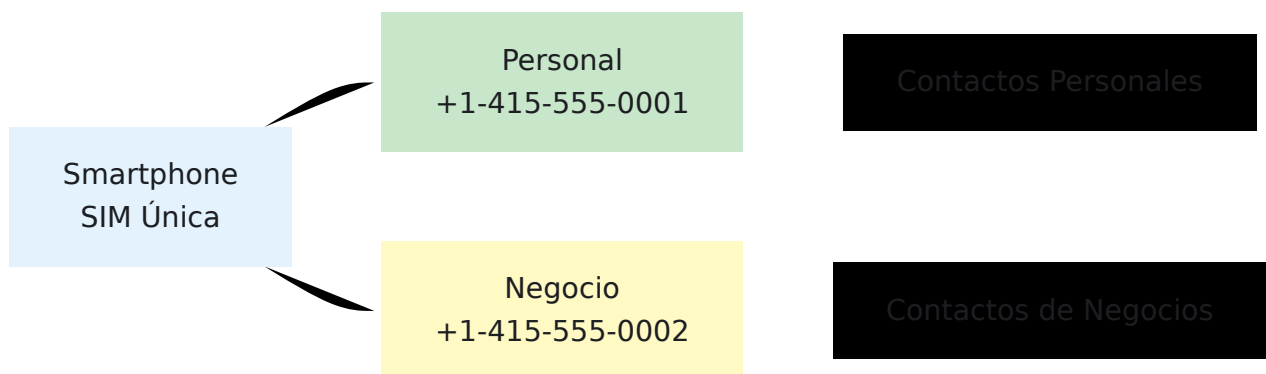


Importante: Un MSISDN solo puede ser asignado a UN suscriptor a la vez. Sin embargo, un suscriptor puede tener MUCHOS MSISDNs.

Casos de Uso

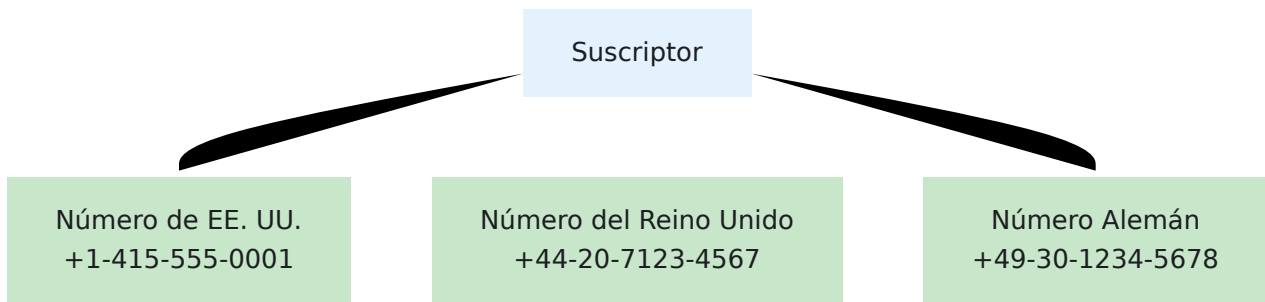
1. Líneas de Negocios y Personales

Un suscriptor tiene tanto números de teléfono de negocios como personales en el mismo dispositivo:



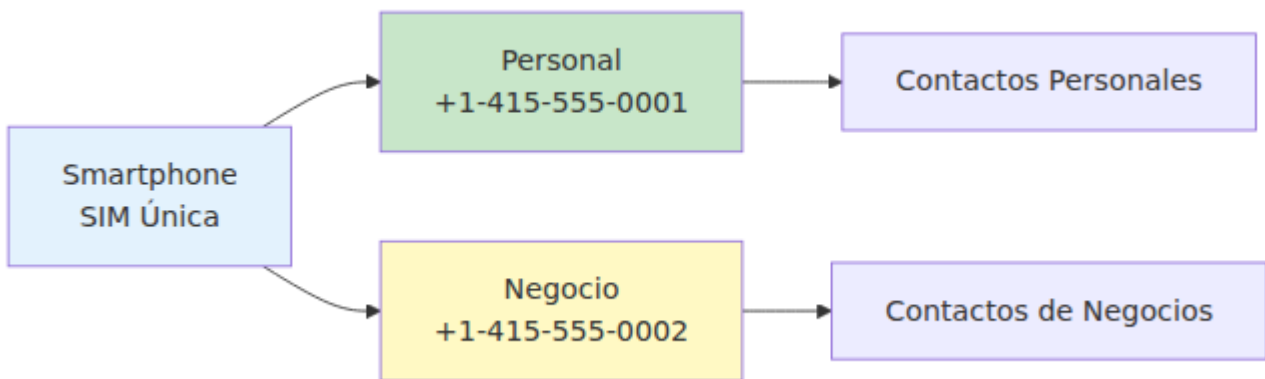
2. Números Internacionales

Un suscriptor que viaja con frecuencia tiene números en múltiples países:



3. Planes Familiares

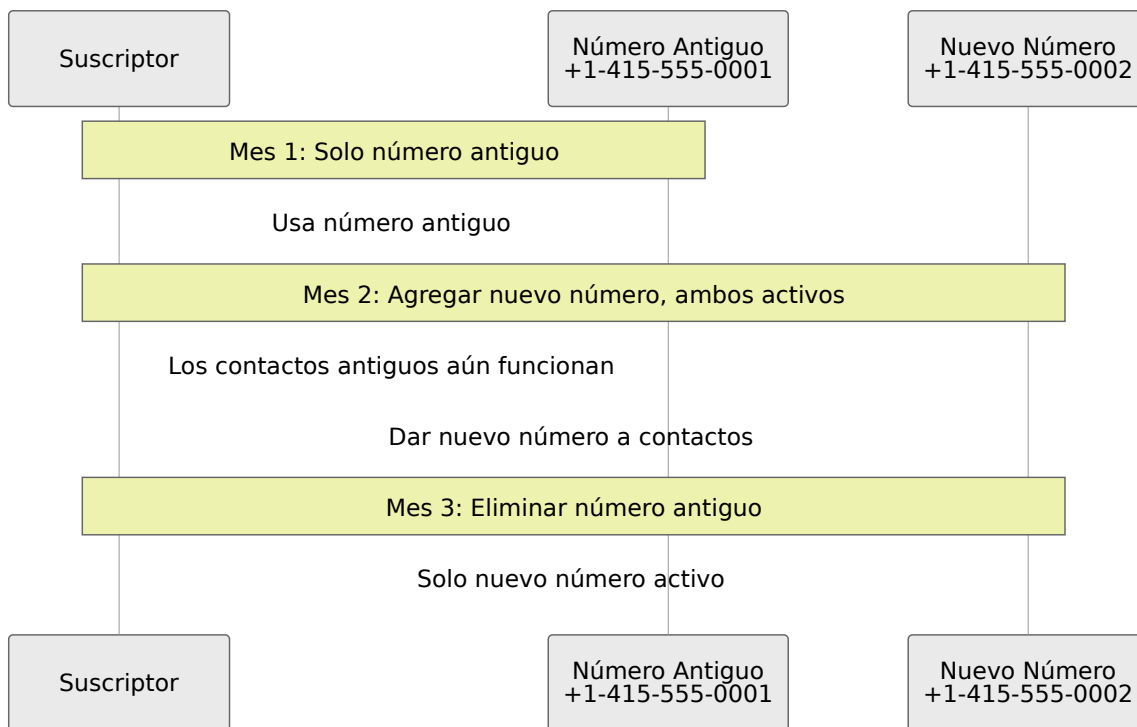
Un padre gestiona múltiples números de miembros de la familia:



Nota: En OmniHSS, esto requerir  a múltiples suscriptores (uno por SIM/IMSI), cada uno con potencialmente múltiples MSISDNs.

4. Portabilidad de Línea Legada

Cuando un suscriptor cambia de número pero quiere mantener el antiguo número activo durante la transición:



Configuración

Creando MSISDNs

Los MSISDNs deben ser creados antes de asignarlos a los suscriptores.

```
# Crear primer MSISDN
curl -k -X POST https://hss.example.com:8443/api/msisdn \
-H "Content-Type: application/json" \
-d '{"msisdn": {"msisdn": "14155551001"}}'

# Crear segundo MSISDN
curl -k -X POST https://hss.example.com:8443/api/msisdn \
-H "Content-Type: application/json" \
-d '{"msisdn": {"msisdn": "14155551002"}}'
```

Asignando MSISDNs a Suscriptores

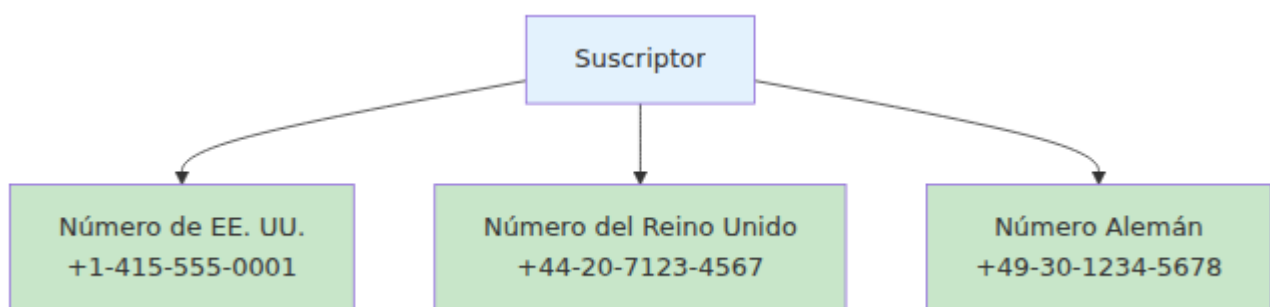
La asignación se realiza a través de la tabla de unión en la base de datos.

Método de Base de Datos:

1. Consultar la base de datos para obtener el ID del suscriptor para el IMSI objetivo
2. Consultar la base de datos para obtener los IDs de MSISDN para los números de teléfono
3. Insertar registros en la tabla de unión vinculando subscriber_id a cada msisdn_id

Esto crea la relación de muchos a muchos entre el suscriptor y sus números de teléfono.

Flujo de Aprovisionamiento



Verificando la Asignación

Consultar la base de datos para recuperar el suscriptor junto con todos los MSISDN vinculados mediante:

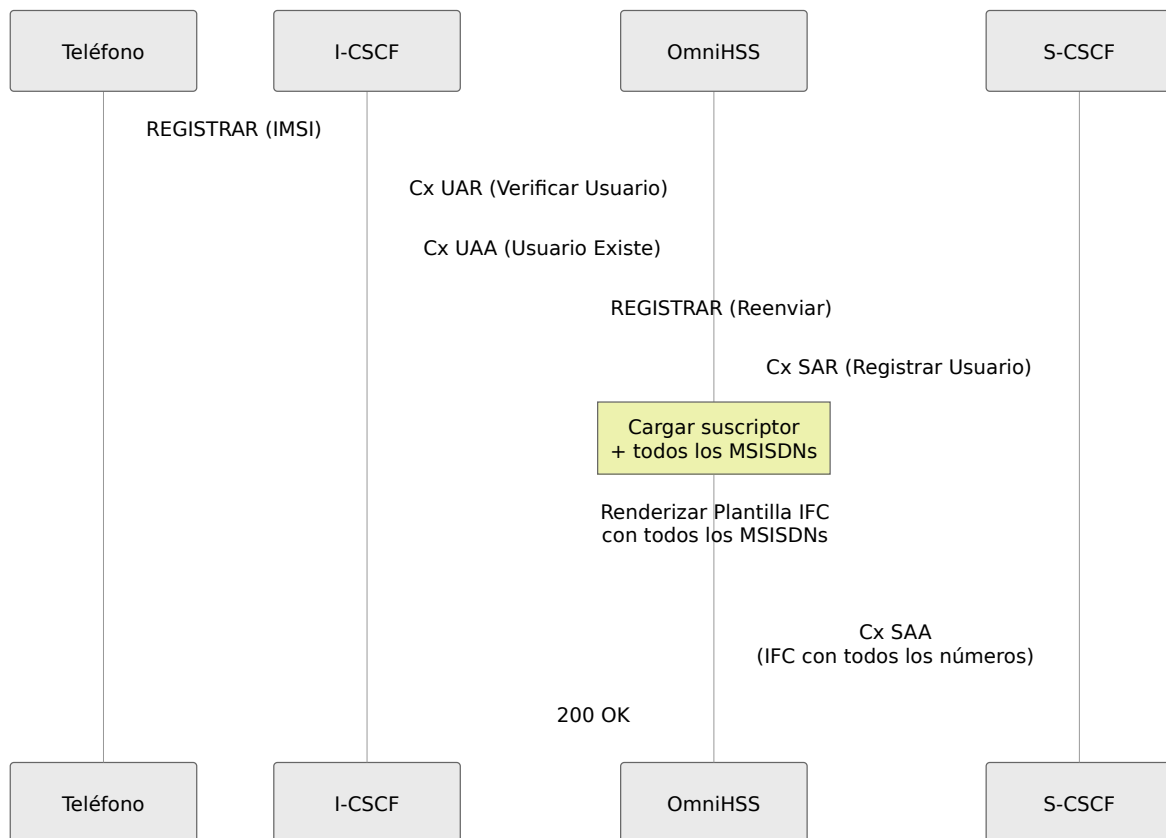
- Uniendo la tabla de suscriptores con la tabla de unión
- Uniendo la tabla de unión con la tabla de msisdn
- Agrupando resultados por suscriptor para ver todos los números de teléfono juntos

Esto mostrará el ID del suscriptor, IMSI y una lista de todos los MSISDNs asignados.

Integración IMS

Registro IMS

Cuando un suscriptor se registra en IMS, **todos los MSISDNs asignados se incluyen** en el perfil de IMS enviado al S-CSCF.



Renderización de Plantilla IFC

La plantilla IFC de IMS puede hacer referencia a todos los MSISDNs utilizando la variable `{{msisdns}}`.

Ejemplo de Plantilla IFC:

```

<ServiceProfile>
  <PublicIdentity>
    <Identity>sip:
{{imsi}}@ims.mnc{{mnc}}.mcc{{mcc}}.3gppnetwork.org</Identity>
  </PublicIdentity>
  <!-- Repetir para cada MSISDN -->
  <PublicIdentity>
    <Identity>sip:+14155551001@ims.example.com</Identity>
  </PublicIdentity>
  <PublicIdentity>
    <Identity>tel:+14155551001</Identity>
  </PublicIdentity>
  <PublicIdentity>
    <Identity>sip:+14155551002@ims.example.com</Identity>
  </PublicIdentity>
  <PublicIdentity>
    <Identity>tel:+14155551002</Identity>
  </PublicIdentity>
  <!-- ... -->
</ServiceProfile>

```

Variable de Plantilla:

- `{{msisdns}}` - Lista de todos los MSISDNs asignados al suscriptor

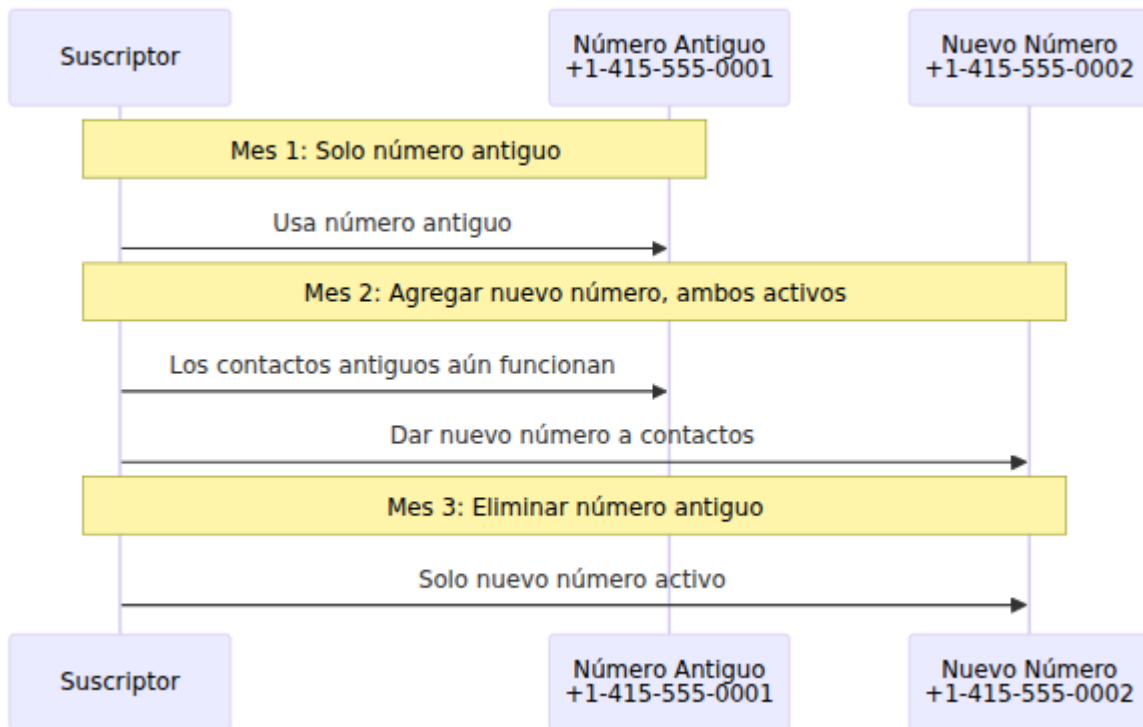
Identidades Públicas

Cada MSISDN típicamente resulta en dos identidades públicas IMS:



Enrutamiento de Llamadas Entrantes

Cuando alguien llama a uno de los números del suscriptor, la red IMS enruta al URI SIP correcto:



Presentación de Llamadas Salientes

El teléfono puede elegir qué número presentar como ID de llamada para las llamadas salientes.

Ejemplo de SIP INVITE:

```
INVITE sip:+15105551234@ims.example.com SIP/2.0
From: "+14155551002" <sip:+14155551002@ims.example.com>;tag=123
To: <sip:+15105551234@ims.example.com>
P-Asserted-Identity: <sip:+14155551002@ims.example.com>
```

Los encabezados `From` y `P-Asserted-Identity` indican cuál de los números del suscriptor se está utilizando.

Solución de Problemas Multi-MSISDN

Problema: MSISDN No Aparece en el Registro IMS

Síntomas:

- S-CSCF muestra solo una identidad pública
- Las llamadas al segundo número fallan

Pasos de Solución de Problemas:

1. Verificar Asignación de MSISDN en la Base de Datos:

- Consultar la base de datos para recuperar todos los MSISDNs vinculados al IMSI del suscriptor
- Verificar la tabla de unión para asegurar que las relaciones existan

2. Verificar Plantilla de Perfil IMS:

- Verificar que la plantilla incluya la variable `{{msisdns}}`
- Confirmar que la sintaxis de la plantilla sea XML válido

3. Revisar Registros de HSS:

- Buscar mensajes de registro IMS (Cx SAR)
- Verificar que todos los MSISDNs estén incluidos en la respuesta

4. Probar Registro IMS:

- Activar re-registro en el teléfono
- Verificar los registros de S-CSCF para identidades públicas registradas

Problema: No se Puede Asignar MSISDN a Suscriptor

Síntomas:

- La inserción en la base de datos falla
- Error: "Entrada duplicada" o "Restricción de clave foránea"

Causas Posibles:

1. MSISDN Ya Asignado:

- Consultar la base de datos para verificar si el MSISDN ya está vinculado a otro suscriptor

- **Solución:** Eliminar la asignación existente primero, luego crear la nueva asignación

2. MSISDN No Existe:

- Consultar la base de datos para verificar que el registro de MSISDN exista
- **Solución:** Crear primero el registro de MSISDN a través de la API o inserción en la base de datos

Problema: Las Llamadas a Un Número Funcionan, Otro No

Síntomas:

- Las llamadas al número principal funcionan
- Las llamadas al número secundario fallan o se enrutan incorrectamente

Pasos de Solución de Problemas:

1. Verificar Ambos Números en el Registro IMS:

- Verificar identidades públicas registradas en S-CSCF
- Confirmar que ambos URIs SIP estén presentes

2. Verificar Reglas de Enrutamiento IMS:

- Verificar que las reglas de enrutamiento de la plantilla IFC se apliquen a todas las identidades
- Comprobar si un número específico necesita un enrutamiento especial

3. Probar Ambos Números:

```
# Probar desde el cliente SIP
sip:+14155551001@ims.example.com # Debería funcionar
sip:+14155551002@ims.example.com # También debería funcionar
```

Problema: La Consulta de API por MSISDN Devuelve el Suscriptor Incorrecto

Síntomas:

- La consulta de API `/api/subscriber/msisdn/:msisdn` devuelve un suscriptor inesperado

Verificación:

Consultar la base de datos para encontrar a qué suscriptor está asignado el MSISDN. Esto debería devolver exactamente un suscriptor. Si devuelve múltiples o el suscriptor incorrecto, la tabla de unión tiene datos incorrectos que deben corregirse.

Mejores Prácticas

Orden de Aprovisionamiento

1. Crear todos los MSISDNs primero
2. Crear suscriptor
3. Asignar MSISDNs al suscriptor
4. Verificar la asignación antes de la activación

Gestión de MSISDN

- **Documentar números primarios vs secundarios** en custom_attributes del suscriptor
- **Portar números secuencialmente** al portar para evitar interrupciones en el servicio
- **Probar todos los números** después del aprovisionamiento antes de entregarlos al cliente

Configuración IMS

- Asegurarse de que la plantilla IFC maneje correctamente múltiples identidades públicas
- Probar el enrutamiento entrante a todos los números
- Verificar la presentación de ID de llamada para las llamadas salientes

Migración

Al migrar de un único a multi-MSISDN:

El suscriptor tiene 1
MSISDN

Agregar segundo
MSISDN

Probar ambos números

¿Ambos funcionan?

Sí

Activar para el cliente

No

Depurar problema

Completo

SIM Multi-IMSI: Múltiples Identidades de Red

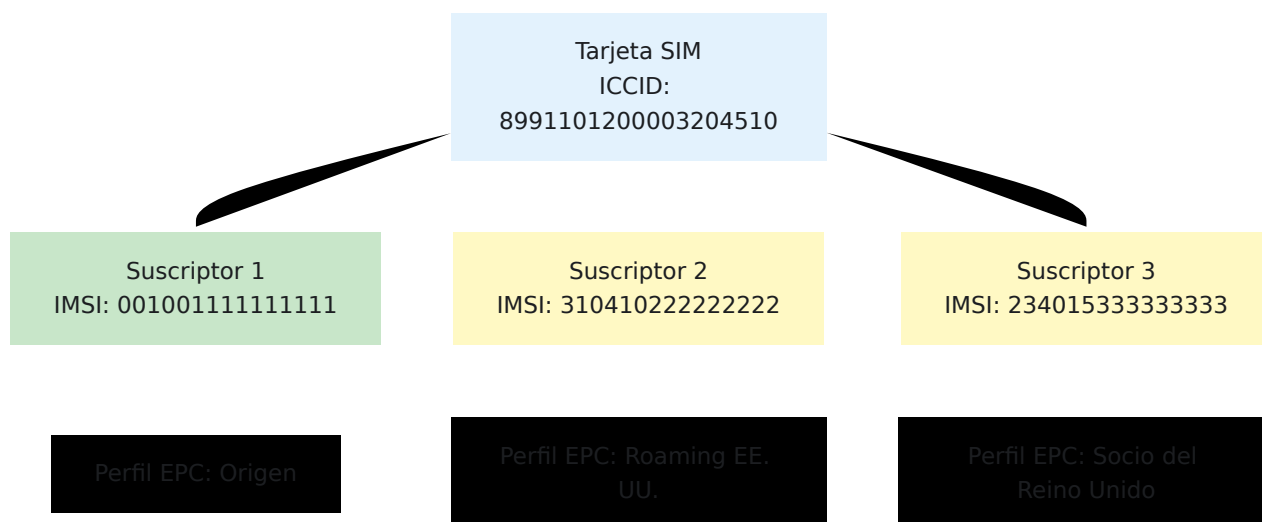
Cómo Funciona

Una SIM multi-IMSI contiene múltiples perfiles de suscriptor completos, cada uno con su propio IMSI, claves y credenciales. El dispositivo puede cambiar entre IMSIs para conectarse a diferentes redes, a menudo automáticamente según la ubicación o disponibilidad de la red.

Importante: Solo **un IMSI puede estar activo en un momento dado**. Cuando un dispositivo cambia a un IMSI diferente en la misma tarjeta SIM, el HSS automáticamente desregistrará el IMSI previamente activo.

Implementación de OmniHSS

En OmniHSS, cada IMSI en una SIM multi-IMSI se aprovisiona como un **registro de suscriptor separado**, pero todos hacen referencia a la **misma tarjeta SIM**:



Casos de Uso

1. Optimización de Roaming Internacional

- IMSI de origen: 001-001 (tarifas de red de origen)

- IMSI de roaming en EE. UU.: 310-410 (tarifas locales de EE. UU.)
- IMSI de roaming en la UE: 234-015 (tarifas locales de la UE)
- El dispositivo cambia IMSI según la ubicación

2. Servicio MVNO

- IMSI primario: red MVNO (revendedor)
- IMSI de respaldo: red anfitriona (operador principal)
- Failover automático si la cobertura de MVNO no está disponible

3. IoT/M2M Multi-Rede

- IMSI 1: operador primario
- IMSI 2: operador de respaldo para redundancia
- IMSI 3: respaldo de emergencia/bajo costo
- Dispositivos críticos mantienen conectividad

4. Cumplimiento Regulatorio

- Diferentes IMSIs para diferentes zonas regulatorias
- Cumplir con los requisitos locales de residencia de datos
- Usar identidad de red local por jurisdicción

Características Multi-IMSI

Autenticación Independiente

- Cada IMSI tiene su propio Ki, OPC y conjunto de claves
- Vectores de autenticación separados por IMSI
- Diferentes credenciales de seguridad por red

Perfiles de Servicio Separados

- Diferentes perfiles EPC (ancho de banda, APNs)
- Diferentes perfiles IMS (servicios de voz)
- Diferentes reglas de roaming por IMSI

Identidad Física Compartida

- Todos los IMSIs hacen referencia a la misma SIM (a través de sim_id)
- El mismo ICCID en todos los registros de suscriptor
- Agrupación lógica a través de la tarjeta SIM

Selección de Red

- El dispositivo o la tarjeta SIM decide qué IMSI usar
- Basado en redes disponibles, ubicación, política
- HSS autentica cualquier IMSI que el dispositivo presente

Configuración

```
# 1. Crear tarjeta SIM (capaz de multi-IMSI)
SIM_ID=$(curl -k -X POST https://hss.example.com:8443/api/sim \
  -d '{"sim": {"iccid": "8991101200003204510", "is_esim": false}}' \
  \
  | jq -r '.data.id')

# 2. Crear conjunto de claves para IMSI 1 (red de origen)
KEYSET1=$(curl -k -X POST https://hss.example.com:8443/api/key_set \
  \
  -d '{"key_set": {"ki": "0123456789ABCDEF...", "opc":
"FEDCBA9876..."}}' \
  | jq -r '.data.id')

# 3. Crear suscriptor 1 (IMSI de origen)
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -d '{"subscriber": {
    "imsi": "\"001001111111111\"",
    "sim_id": "\"$SIM_ID\"",
    "key_set_id": "\"$KEYSET1\"",
    "epc_profile_id": "\"e58ed763-928c-4155-bee9-fdbaaadc15f3\""
  }}'

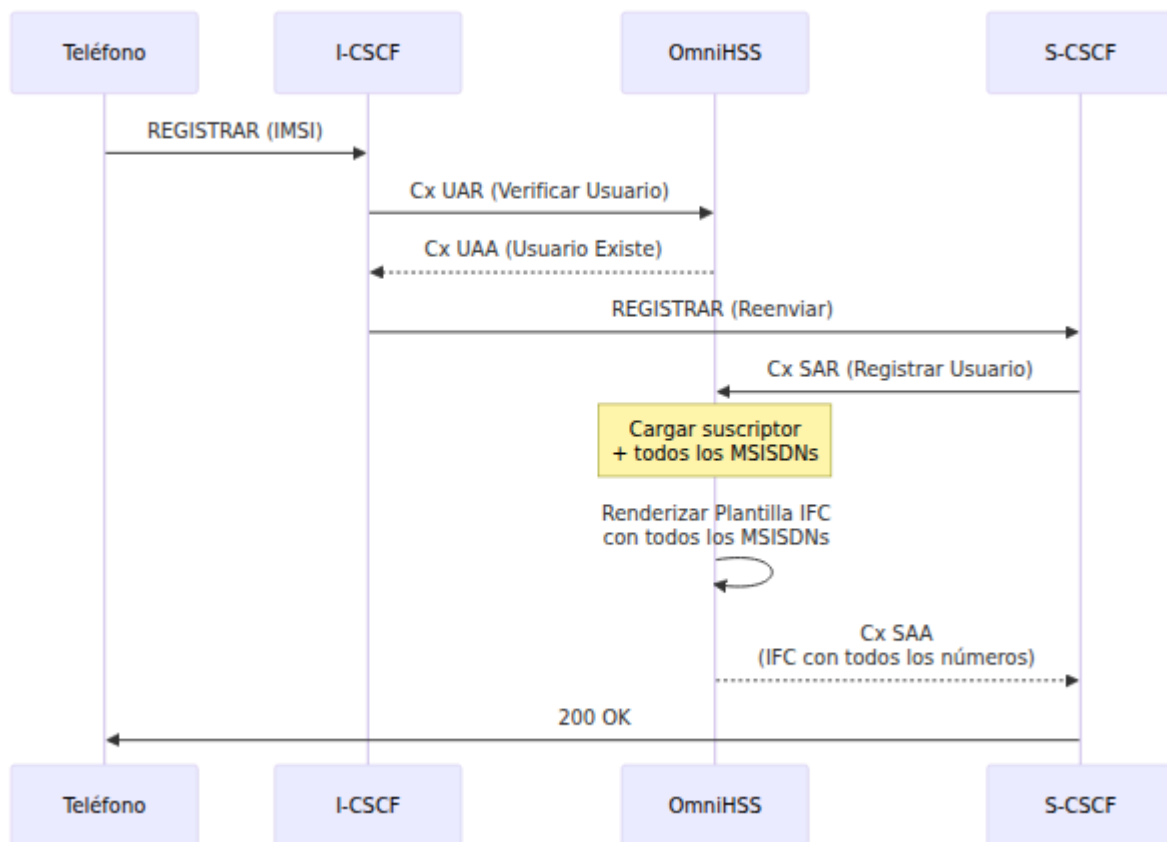
# 4. Crear conjunto de claves para IMSI 2 (socio de roaming)
KEYSET2=$(curl -k -X POST https://hss.example.com:8443/api/key_set \
  \
  -d '{"key_set": {"ki": "111111111111111...", "opc":
"2222222222..."}}' \
  | jq -r '.data.id')

# 5. Crear suscriptor 2 (IMSI de roaming)
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -d '{"subscriber": {
    "imsi": "\"310410222222222\"",
    "sim_id": "\"$SIM_ID\"",
    "key_set_id": "\"$KEYSET2\"",
    "epc_profile_id": "\"f47ac10b-58cc-4372-a567-0e02b2c3d479\""
  }}'

# 6. Repetir para IMSIs adicionales en la SIM...
```

Flujo de Autenticación

Cuando un dispositivo multi-IMSI se conecta:



El HSS no necesita saber que es una SIM multi-IMSI. Autentica cualquier IMSI que el dispositivo presente.

Cambio de IMSI y Desregistro Automático

Cuando una SIM multi-IMSI cambia de un IMSI a otro, solo un IMSI puede estar registrado a la vez en la red. OmniHSS maneja esto automáticamente enviando una **Solicitud de Cancelación de Ubicación (CLR)** para desregistrar el IMSI previamente activo cuando un nuevo IMSI de la misma tarjeta SIM se registra.

Regla de IMSI Activo Único

Concepto Clave: Solo un suscriptor (IMSI) por tarjeta SIM puede estar activo en un momento dado.

- Si un suscriptor está registrado en un MME usando **IMSI X**

- Esto asegura una transferencia limpia entre IMSIs y previene conflictos en la red.

```

sequenceDiagram
    participant Dispositivo
    participant MME
    participant OmniHSS

    Dispositivo->>MME: Actualmente registrado con IMSI X  
001001111111111
    Note over Dispositivo: El usuario viaja a un país diferente  
SIM cambia a IMSI Y
    Dispositivo->>MME: Solicitud de Conexión (IMSI Y: 310410222222222)
    Note over Dispositivo: Desafío de Autenticación
    Note over Dispositivo: Respuesta de Autenticación
    MME->>OmniHSS: S6a AIR (IMSI Y)
    MME->>OmniHSS: S6a AIA (vectores de autenticación para IMSI Y)
    OmniHSS->>MME: S6a ULR (Actualizar Ubicación para IMSI Y)
    Note over OmniHSS: Consultar: Encontrar otros suscriptores  
con el mismo sim_id
    Note over OmniHSS: SELECT * FROM subscriber  
WHERE sim_id = (SELECT sim_id FROM subscriber WHERE imsi='310410...')  
AND imsi != '310410...'  
AND subscriber_state is REGISTERED
    Note over OmniHSS: Encontrado: IMSI X todavía está registrado  
en MME-001
    MME->>OmniHSS: S6a CLR (Cancelar Ubicación para IMSI X)  
Destino: MME-001
    Note over MME: Desregistrar IMSI X  
Liberar recursos
    OmniHSS->>MME: S6a CLA (Respuesta de Cancelación de Ubicación)
    Note over OmniHSS: Marcar IMSI X como desregistrado  
Registrar IMSI Y
    MME->>OmniHSS: S6a ULA (Respuesta de Actualización de Ubicación para IMSI Y)
    Note over Dispositivo: Aceptar Conexión (IMSI Y ahora activo)
    Note over Dispositivo: IMSI Y ahora está registrado
    Dispositivo->>MME: 
    Note over Dispositivo: IMSI X está desregistrado  
IMSI Y está activo
    MME->>OmniHSS: 
    Note over Dispositivo: Dispositivo
    Note over MME: MME
    Note over OmniHSS: OmniHSS
  
```

Integridad de la Red:

- Previene registros duplicados desde la misma SIM física

- Asegura que los recursos de la red se liberen correctamente
- Mantiene datos de ubicación de suscriptores precisos

Precisión de Facturación:

- Solo un IMSI es cobrado por acceso a la red a la vez
- Límites de sesión claros entre cambios de IMSI
- Generación precisa de CDR (Registro de Detalle de Llamadas)

Gestión de Recursos:

- Los recursos de MME para el IMSI antiguo son liberados
- Los contextos y portadores PDP son limpiados
- El seguimiento de ubicación permanece preciso

Disparadores de Cambio de IMSI

El dispositivo/SIM decide cuándo cambiar IMSIs basado en:

1. Disponibilidad de la Red

- Red IMSI de origen no disponible
- Cambiar a IMSI de socio de roaming

2. Selección Manual

- El usuario selecciona manualmente la red
- La SIM cambia al IMSI correspondiente

3. Basado en Políticas

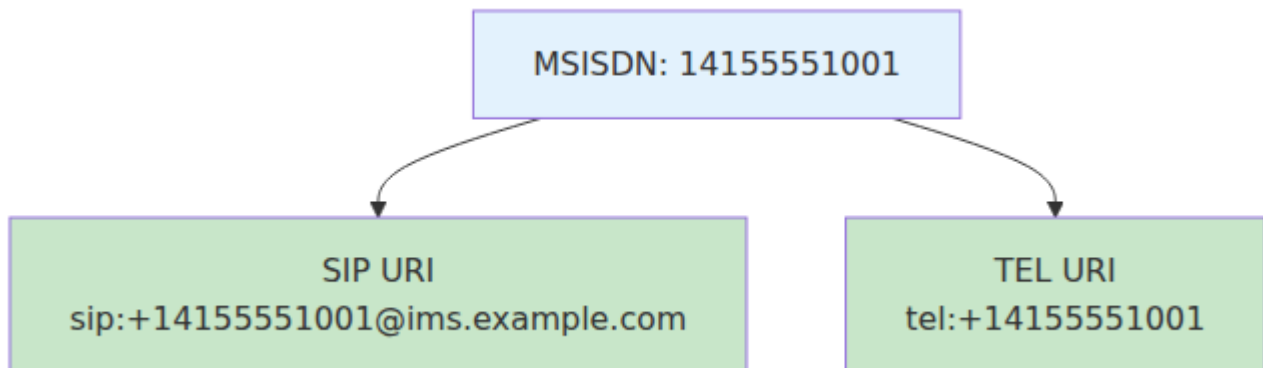
- La tarjeta SIM tiene reglas internas (por ejemplo, preferir IMSI local en ciertos países)
- Cambio automático basado en MCC/MNC

4. Optimización de Costos

- Cambiar a IMSI con tarifas de roaming más bajas
- Usar IMSI local para evitar cargos de roaming

Consideraciones de IMS

El mismo comportamiento de Cancelar Solicitud de Ubicación se aplica al registro de IMS:



Impacto Operacional

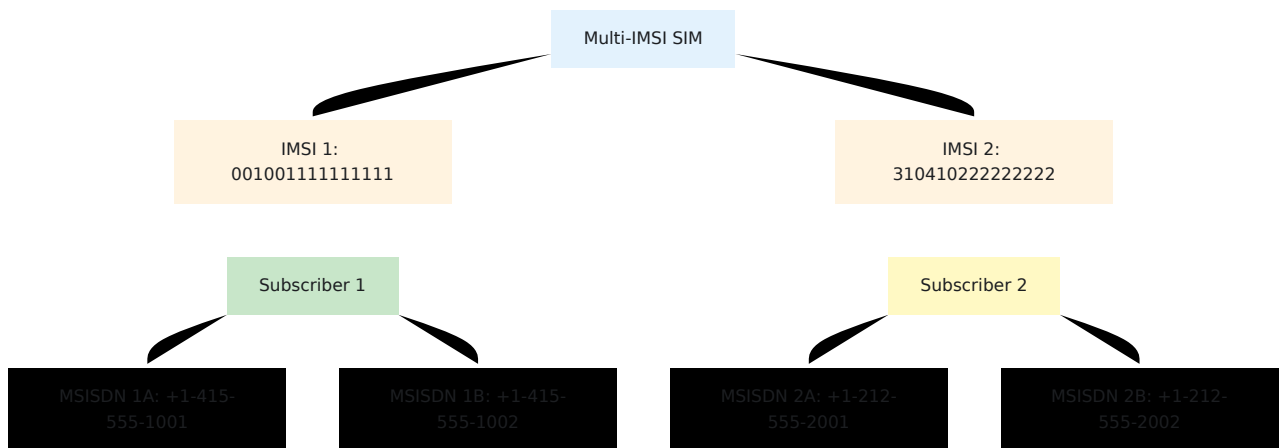
Para el Personal de Operaciones:

1. **El suscriptor aparece fuera de línea:** Cuando el IMSI cambia, el IMSI antiguo se mostrará como "dado de baja" en el HSS. Este es un comportamiento normal.
 2. **Dos registros de suscriptor para una SIM:** Las SIMs multi-IMSI tendrán múltiples registros de suscriptor compartiendo el mismo `sim_id`. Solo uno estará en estado "registrado" a la vez.
 3. **Seguimiento de ubicación:** La tabla `subscriber_state` rastrea con qué MME/SGSN está registrado cada IMSI. Cuando el IMSI cambia, la ubicación antigua se borra.
 4. **Resolución de problemas:** Si no se puede alcanzar un dispositivo:
 - Verifique qué IMSI está actualmente registrado
 - Verifique que el IMSI correcto se esté utilizando para la red actual
 - Confirme que solo un IMSI por SIM esté en estado registrado
-

Escenarios Combinados

Multi-IMSI + Multi-MSISDN

Puede combinar ambas características: múltiples IMSIs en una SIM, cada una con múltiples MSISDNs.



Caso de Uso Ejemplo:

- **Red de Origen (IMSI 1):**
 - Número personal: +1-415-555-1001
 - Número de negocio: +1-415-555-1002
- **Red de Roaming en EE. UU. (IMSI 2):**
 - Número personal: +1-212-555-2001
 - Número de negocio: +1-212-555-2002

Cuando el dispositivo está en territorio de origen, utiliza IMSI 1 con sus MSISDNs. Cuando está en roaming en EE. UU., cambia a IMSI 2 con diferentes MSISDNs optimizados para la red de EE. UU.

Procedimientos Operacionales

Gestión de Suscriptores Multi-MSISDN

Ver todos los MSISDNs para un suscriptor:

```
Query via API: GET /api/subscriber/imsi/:imsi
```

La respuesta incluye todos los MSISDNs vinculados.

Resolución de Problemas Multi-IMSI

El dispositivo no se conecta con el segundo IMSI:

1. Verifique que exista un segundo registro de suscriptor para ese IMSI
2. Verifique que `key_set` esté configurado correctamente para ese IMSI
3. Verifique que el perfil EPC esté asignado
4. Confirme que las reglas de roaming permitan la conexión

El dispositivo cambia de IMSIs inesperadamente:

- Esto es controlado por la lógica del dispositivo/SIM, no por el HSS
- El HSS autentica cualquier IMSI que se presente
- Verifique la configuración de selección de IMSI del dispositivo

Resolución de Problemas Multi-MSISDN

El segundo número no suena:

1. Verifique que el MSISDN esté vinculado en la tabla de unión
2. Verifique que la plantilla de perfil IMS incluya la variable `{{msisdns}}`
3. Confirme que el registro IMS incluya todas las identidades públicas
4. Revise los registros de S-CSCF para identidades registradas

Las llamadas salientes solo muestran un número:

- El dispositivo selecciona qué número presentar como ID de llamada
 - Esta es la configuración del dispositivo, no del HSS
 - El HSS proporciona todas las identidades; el dispositivo elige
-

Resumen de Beneficios

Beneficios de Multi-MSISDN

- ✓ Una SIM, múltiples números de teléfono
- ✓ Líneas de negocio y personales separadas
- ✓ Presencia local internacional
- ✓ Gestión de dispositivos simplificada
- ✓ Todos los números comparten el mismo servicio de datos
- ✓ Facturación centralizada por IMSI

Beneficios de SIM Multi-IMSI

- ✓ Costos de roaming optimizados
- ✓ Selección automática de red
- ✓ Redundancia y conmutación por error
- ✓ Identidad de red local
- ✓ Cumplimiento regulatorio
- ✓ Continuidad del servicio a través de redes

Beneficios Combinados

- ✓ Máxima flexibilidad
 - ✓ Diferentes conjuntos de números por red
 - ✓ Optimizado para cada caso de uso
 - ✓ Escenarios empresariales complejos
 - ✓ Optimización internacional y local
-

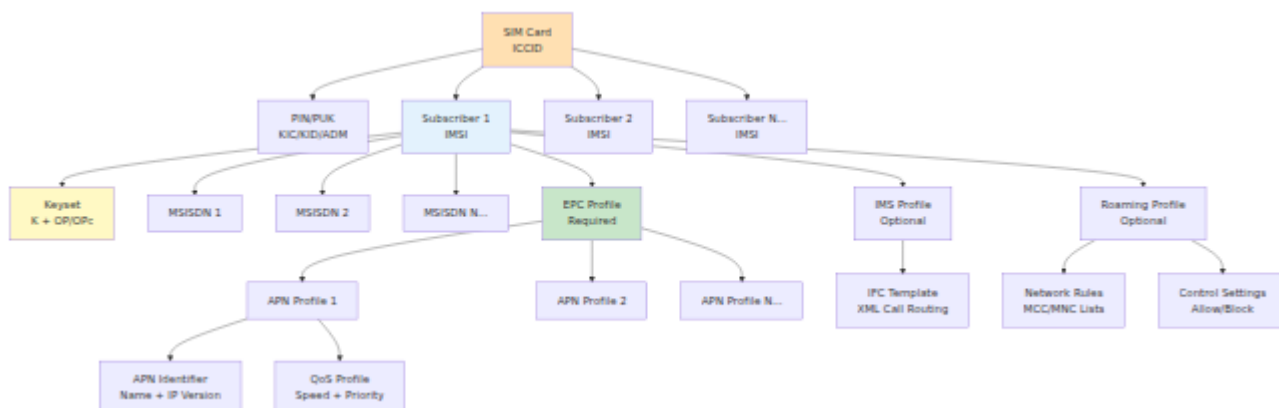
[← Volver a la Guía de Operaciones](#)

Gestión de Perfiles de OmniHSS

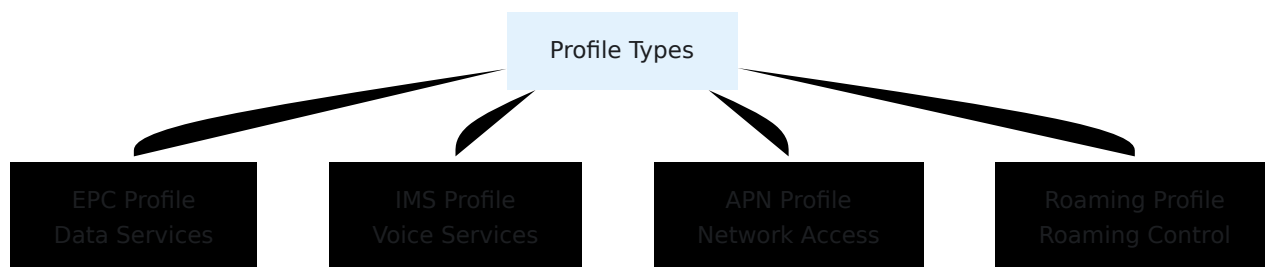
[← Volver a la Guía de Operaciones](#)

Descripción General

OmniHSS utiliza **perfiles** para definir las características del servicio para los suscriptores. Los perfiles permiten crear plantillas de servicio reutilizables que pueden asignarse a múltiples suscriptores, simplificando el aprovisionamiento y garantizando la consistencia.



Tipos de Perfiles



Perfiles EPC

Los Perfiles EPC (Evolved Packet Core) definen las características del servicio de datos para suscriptores LTE.

Parámetros Clave

Parámetro	Descripción	Valores Típicos
ue_ambr_dl_kbps	Límite de velocidad de descarga	10,000 - 1,000,000 Kbps
ue_ambr_ul_kbps	Límite de velocidad de carga	5,000 - 500,000 Kbps
network_access_mode	Tipo de servicio	"packet_only" o "packet_and_circuit"
tracking_area_update_interval_seconds	Temporizador TAU	54 segundos (típico)

Creación de Perfiles EPC

```
curl -k -X POST https://hss.example.com:8443/api/epc/profile \
-H "Content-Type: application/json" \
-d '{
  "apn_profiles": [],
  "name": "Premium 100Mbps",
  "network_access_mode": "packet_only",
  "tracking_area_update_interval_seconds": 600,
  "ue_ambr_dl_kbps": 100000,
  "ue_ambr_ul_kbps": 50000
}'
```

Plantillas Comunes de Perfiles EPC

Internet Básico:

- Descarga: 10 Mbps (10,000 Kbps)
- Carga: 5 Mbps (5,000 Kbps)

Estándar:

- Descarga: 50 Mbps (50,000 Kbps)
- Carga: 25 Mbps (25,000 Kbps)

Premium:

- Descarga: 100 Mbps (100,000 Kbps)
- Carga: 50 Mbps (50,000 Kbps)

Ilimitado:

- Descarga: 1 Gbps (1,000,000 Kbps)
 - Carga: 500 Mbps (500,000 Kbps)
-

Perfiles IMS

Los Perfiles IMS definen las características del servicio de voz, principalmente a través de plantillas IFC (Initial Filter Criteria).

Plantillas IFC

Las plantillas IFC son documentos XML que definen las reglas de enrutamiento de llamadas para el S-CSCF.

Variables de Plantilla:

- `{{imsi}}` - IMSI del suscriptor
- `{{msisdns}}` - Lista de números de teléfono
- `{{mcc}}` - Código del país de origen

- `{{mnc}}` - Código de la red de origen

Creación de Perfiles IMS

```
curl -k -X POST https://hss.example.com:8443/api/ims/profile \
-H "Content-Type: application/json" \
-d '{
  "ims_profile": {
    "name": "Standard VoLTE",
    "ifc_template": "<InitialFilterCriteria>...
</InitialFilterCriteria>"
  }
}'
```

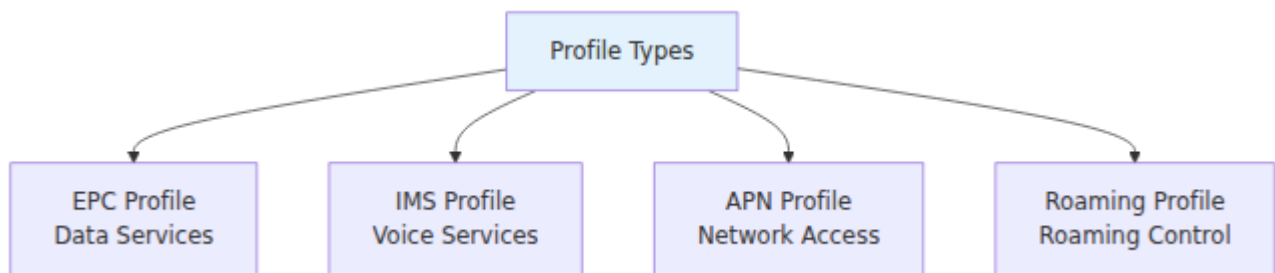
Ejemplo de Plantilla IFC

```
<ServiceProfile>
  <PublicIdentity>
    <Identity>sip:
{{imsi}}@ims.mnc{{mnc}}.mcc{{mcc}}.3gppnetwork.org</Identity>
  </PublicIdentity>
  <InitialFilterCriteria>
    <Priority>0</Priority>
    <TriggerPoint>
      <ConditionTypeCNF>0</ConditionTypeCNF>
      <SPT>
        <ConditionNegated>0</ConditionNegated>
        <Group>0</Group>
        <Method>INVITE</Method>
      </SPT>
    </TriggerPoint>
    <ApplicationServer>
      <ServerName>sip:as.ims.example.com</ServerName>
      <DefaultHandling>0</DefaultHandling>
    </ApplicationServer>
  </InitialFilterCriteria>
</ServiceProfile>
```

Perfiles APN

Los Perfiles APN (Access Point Name) definen los puntos de acceso a la red para conexiones de datos.

Componentes APN



Identificador APN

Define el nombre del APN y el soporte para el protocolo IP.

APNs Comunes:

- `internet` - Acceso general a internet
- `ims` - Señalización IMS/VoLTE
- `mms` - Mensajería multimedia
- `vzwadmin` - Específico del operador

Opciones de Versión IP:

- `"ipv4"`: Solo IPv4
- `"ipv6"`: Solo IPv6
- `"ipv4v6"`: IPv4v6 (doble pila)
- `"ipv4_or_ipv6"`: IPv4 o IPv6 (elección de la red)

Perfil QoS APN

Define los parámetros de calidad de servicio.

Valores de QCI (QoS Class Identifier):

QCI	Tipo	Caso de Uso	Prioridad
1	GBR	Voz conversacional	Más alto
2	GBR	Video conversacional	Alto
4	GBR	Streaming de video	Alto
5	Non-GBR	Señalización IMS	Medio
9	Non-GBR	Internet (por defecto)	Más bajo

Método de Carga a Nivel de Sesión (opcional):

El perfil QoS APN también puede fijar el método de carga por defecto para la sesión IP-CAN, enviado como los AVPs `Online/Offline` de nivel superior en el Gx CCA-I.

Campo	Tipo	Por Defecto	Descripción
online_charging_enabled	booleano	null	Cuando se establece, fuerza el AVP <code>Online</code> a nivel de sesión (<code>true</code> = habilitar, <code>false</code> = deshabilitar). Cuando es <code>null</code>, el PCRF refleja el valor que el PGW envió en el CCR-I.
offline_charging_enabled	booleano	null	Cuando se establece, fuerza el AVP <code>Offline</code> a nivel de sesión (<code>true</code> = habilitar, <code>false</code> = deshabilitar). Cuando es <code>null</code>, el PCRF refleja el valor que el PGW envió en el CCR-I.

Consulte [PCRF: Carga en Línea/Fuera de Línea a Nivel de Sesión](#) para el comportamiento completo y la referencia de valores AVP.

Creación de Configuración Completa de APN

```
# 1. Crear Identificador APN
APN_ID=$(curl -k -X POST
https://hss.example.com:8443/api/apn/identifier \
-H "Content-Type: application/json" \
-d '{"apn": "internet", "ip_version": "ipv4v6"}' \
| jq -r '.response.id')

# 2. Crear Perfil QoS APN
QOS_ID=$(curl -k -X POST
https://hss.example.com:8443/api/apn/qos_profile \
-H "Content-Type: application/json" \
-d '{
  "name": "Best Effort",
  "allocation_retention_priority": 8,
  "apn_ambr_dl_kbps": 50000,
  "apn_ambr_ul_kbps": 25000,
  "pre_emption_capability": false,
  "pre_emption_vulnerability": true,
  "qci": 9
}' | jq -r '.response.id')

# 3. Crear Perfil APN
curl -k -X POST https://hss.example.com:8443/api/apn/profile \
-H "Content-Type: application/json" \
-d "{
  \"apn_identifier_id\": \"$APN_ID\",
  \"apn_qos_profile_id\": \"$QOS_ID\",
  \"name\": \"Internet APN\"
}"
```

Asignación de APNs a Perfiles EPC

Los APNs están vinculados a Perfiles EPC a través de la tabla

`join_epc_profile_to_apn_profile`.

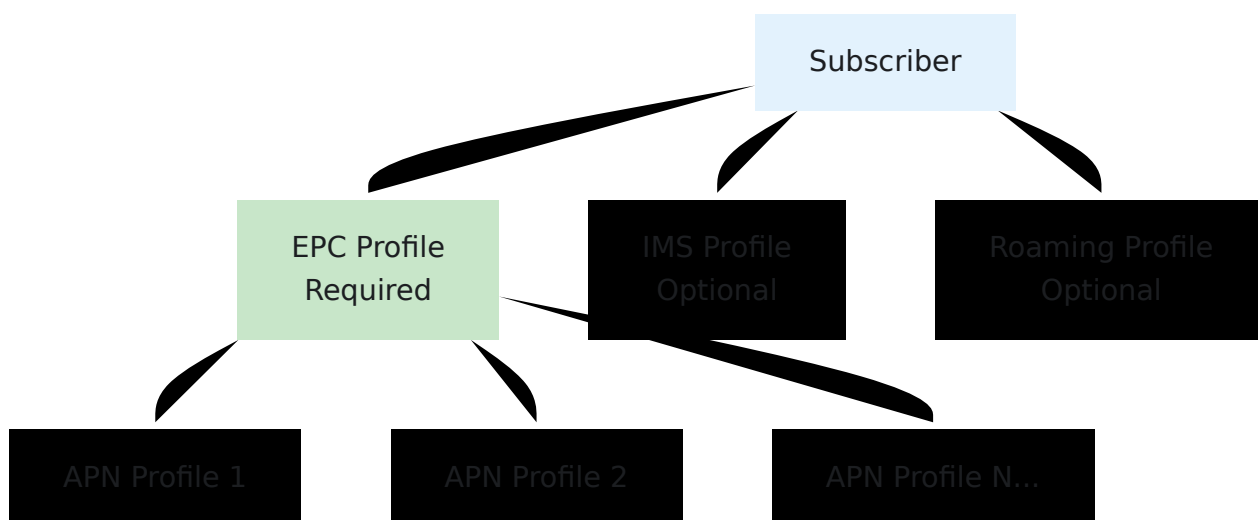
Inserte registros en la tabla de unión para vincular los IDs de perfil APN al ID de perfil EPC. Se pueden asignar múltiples perfiles APN a un perfil EPC.

Perfiles de Roaming

Consulte la documentación detallada en [Guía de Control de Roaming](#).

Asignación de Perfiles

Relaciones de Perfiles de Suscriptores



Asignación de Perfiles a Suscriptores

```
# Asignar perfiles EPC e IMS durante la creación del suscriptor
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "imsi": "001001123456789",
      "key_set_id": "6ba7b810-9dad-41d1-80b4-00c04fd430c8",
      "epc_profile_id": "e58ed763-928c-4155-bee9-fdbaaadc15f3",
      "ims_profile_id": "7c9e6679-7425-40de-944b-e07fc1f90ae7",
      "roaming_profile_id": "9c858901-8a57-4791-81fe-4c455b099bc9"
    }
  }'
```

```
# Actualizar perfil del suscriptor
curl -k -X PUT
https://hss.example.com:8443/api/subscriber/d290f1ee-6c54-4b01-
90e6-d701748f0851 \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "epc_profile_id": "f47ac10b-58cc-4372-a567-0e02b2c3d479"
    }
  }'
```

Mejores Prácticas para la Gestión de Perfiles

Principios de Diseño

1. **Crear Perfiles Estándar** - Definir niveles de servicio comunes (Básico, Estándar, Premium)
2. **Reutilizar Perfiles** - Asignar el mismo perfil a múltiples suscriptores
3. **Documentar Cambios** - Rastrear modificaciones de perfil

4. **Probar Antes de Producción** - Verificar que el perfil funcione primero con un suscriptor de prueba

Convención de Nombres de Perfiles

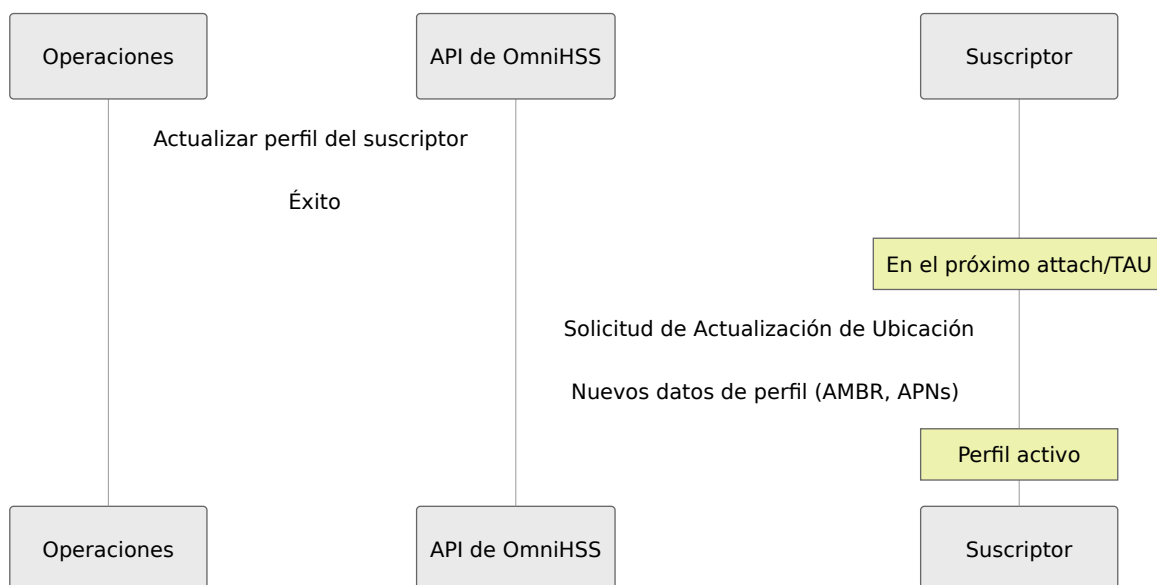
[Nivel de Servicio]-[Velocidad]-[Características]

Ejemplos:

- "Básico-10Mbps-Internet"
- "Premium-100Mbps-VoLTE"
- "Empresarial-1Gbps-MultiAPN"

Migración de Perfiles

Al cambiar el perfil de un suscriptor:



Importante: Los cambios de perfil entran en efecto en el siguiente:

- Actualización del Área de Seguimiento (TAU)
- Attach
- Registro IMS (para cambios en el perfil IMS)

Solución de Problemas de Perfiles

El suscriptor no obtiene la velocidad esperada:

1. Verifique los valores AMBR del perfil EPC asignado
2. Verifique los valores AMBR del perfil QoS APN
3. Verifique que el MME/P-GW esté aplicando QoS correctamente
4. Verifique si hay congestión en la red

El registro IMS falla:

1. Verifique el perfil IMS asignado
2. Verifique la validez del XML de la plantilla IFC
3. Revise los registros del S-CSCF para errores en el procesamiento de IFC
4. Confirme la configuración de selección del S-CSCF

APN no disponible:

1. Verifique que el perfil APN esté vinculado al perfil EPC
2. Verifique que el identificador APN coincida con la solicitud de la red
3. Revise la solicitud de conectividad PDN del UE

[← Volver a la Guía de Operaciones](#) | [Siguiente: Control de Roaming →](#)

Flujos de Protocolo OmniHSS

[← Volver a la Guía de Operaciones](#)

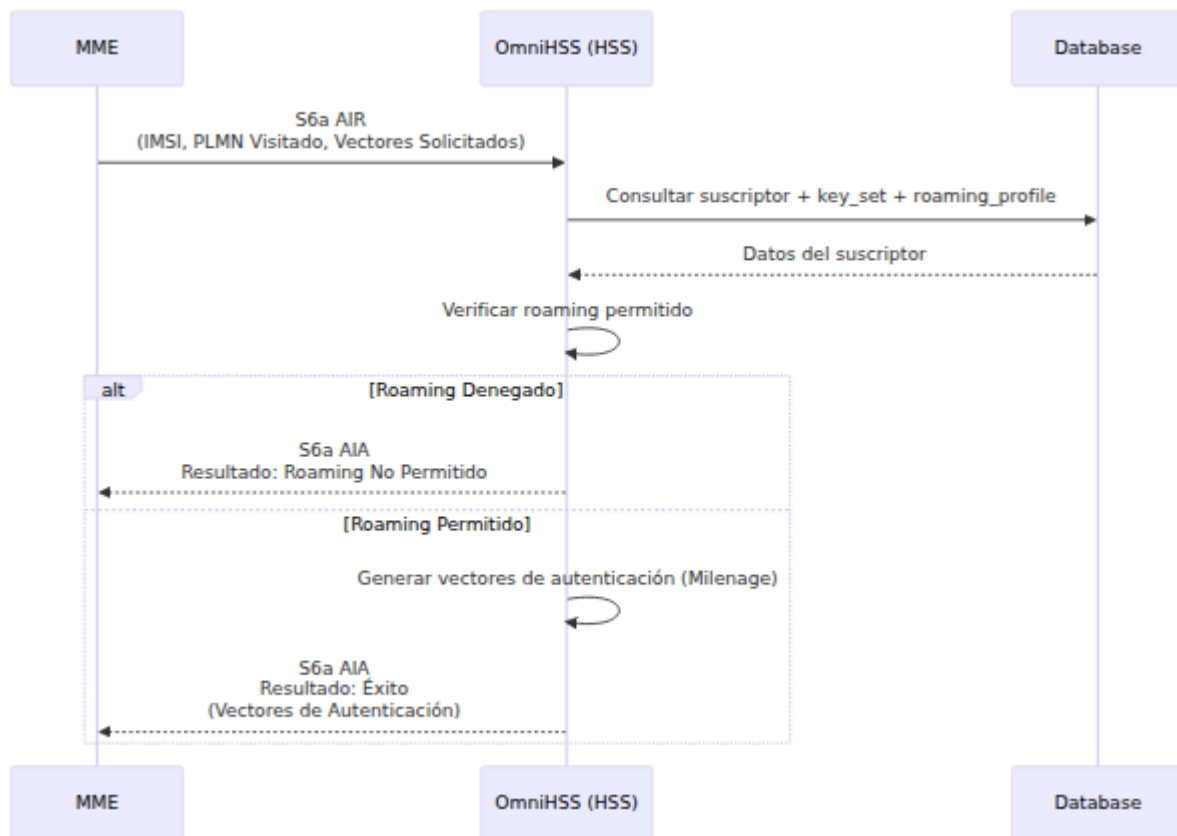
Descripción General

Este documento detalla los flujos de mensajes del protocolo Diameter soportados por OmniHSS. Entender estos flujos es esencial para la solución de problemas y las operaciones.

Interfaz S6a (LTE/EPC)

Solicitud de Información de Autenticación (AIR/AIA)

MME solicita vectores de autenticación para el suscriptor.

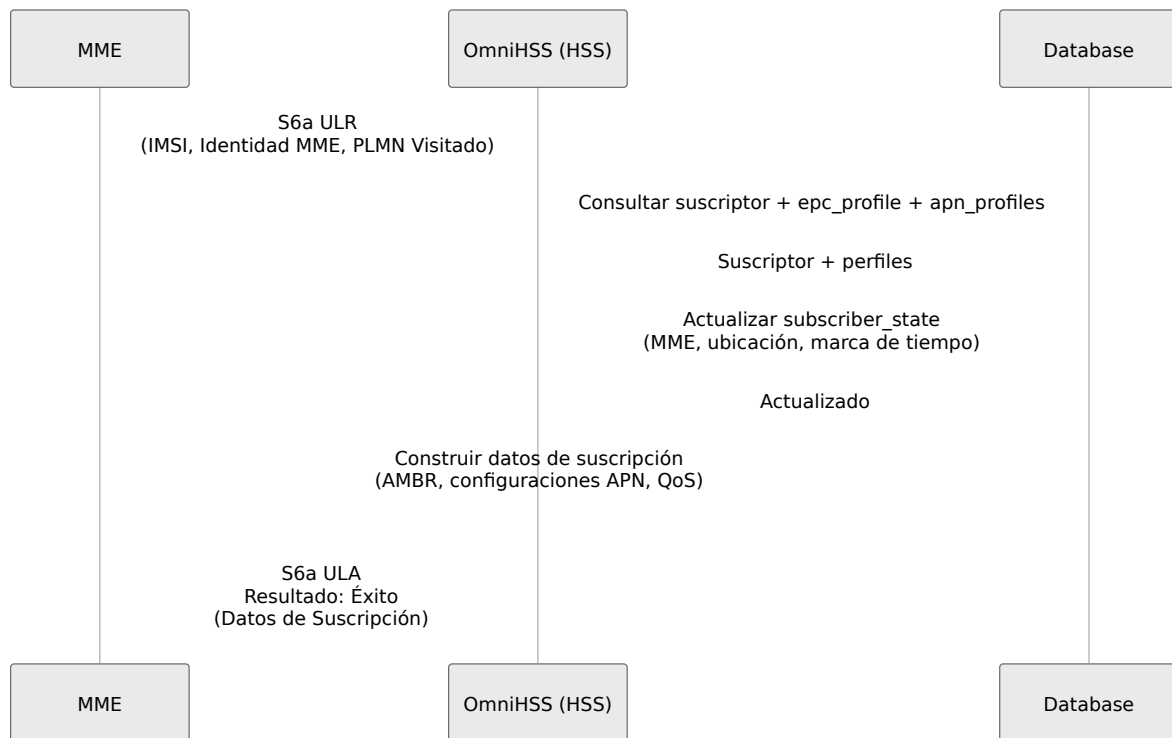


AVPs Clave:

- Solicitud: User-Name (IMSI), Visited-PLMN-Id, Número de Vectores Solicitados
- Respuesta: Authentication-Info (RAND, AUTN, XRES, KASME)

Solicitud de Actualización de Ubicación (ULR/ULA)

MME notifica a HSS sobre la ubicación del suscriptor y recupera datos de suscripción.

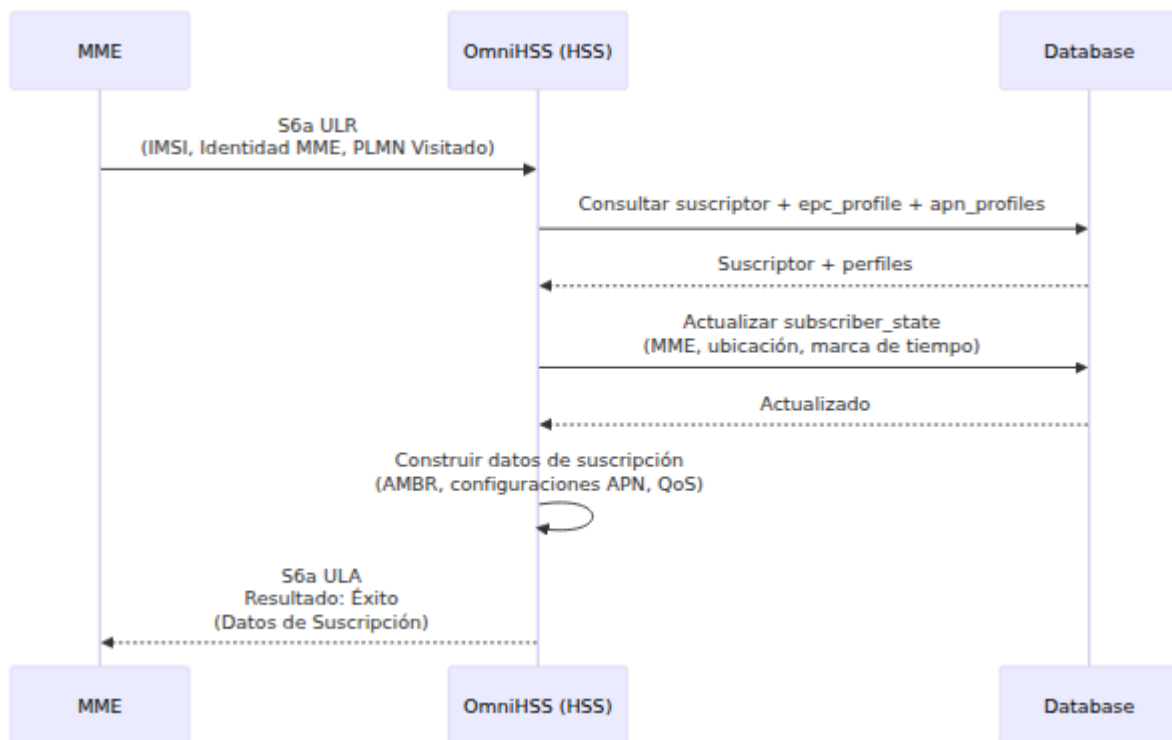


AVPs Clave:

- Solicitud: User-Name (IMSI), RAT-Type, ULR-Flags, Visited-PLMN-Id, UE-SRVCC-Capability
- Respuesta: Subscription-Data (AMBR, APN-Configuration, Network-Access-Mode)

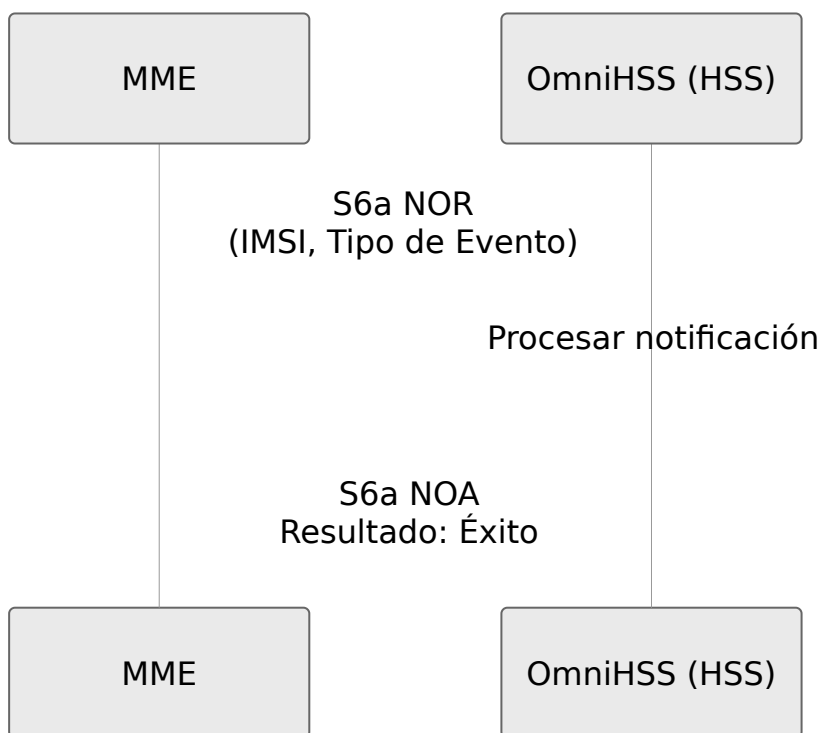
Solicitud de Purga de UE (PUR/PUA)

MME notifica a HSS cuando el contexto del suscriptor es eliminado.



Solicitud de Notificación (NOR/NOA)

MME informa a HSS sobre varios eventos.

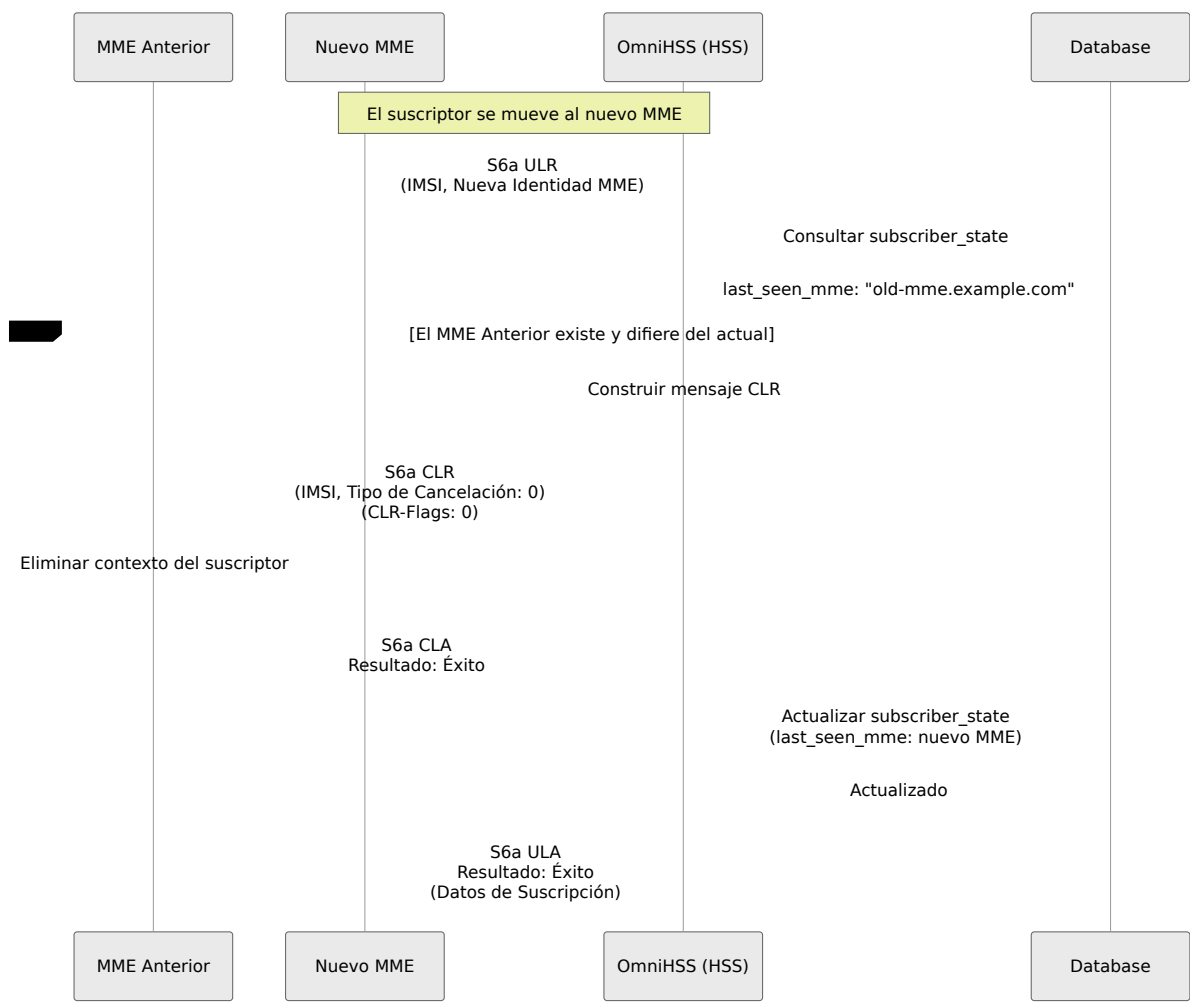


Solicitud de Cancelación de Ubicación (CLR/CLA)

HSS inicia la cancelación de ubicación para informar a MME que el suscriptor debe ser desasociado. OmniHSS soporta tanto el envío automático como programático de CLR.

CLR Automático (Transferencia de MME)

Cuando un suscriptor realiza una Solicitud de Actualización de Ubicación desde un nuevo MME, OmniHSS envía automáticamente un CLR al MME anterior para limpiar registros obsoletos.



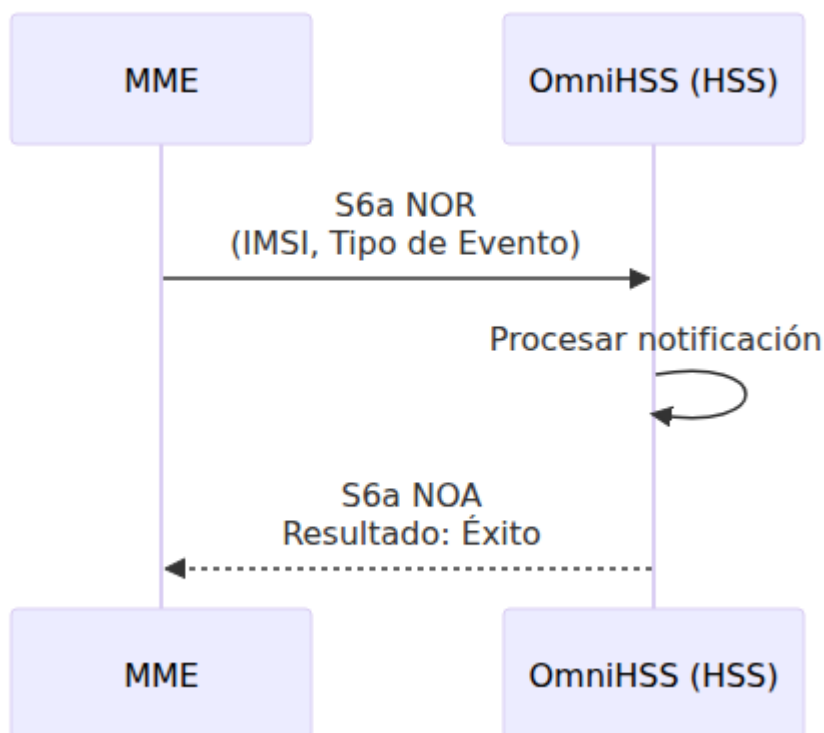
AVPs Clave (CLR Automático):

- User-Name: IMSI del suscriptor
- Destination-Host: Nombre de host del MME anterior
- Destination-Realm: Reino del MME anterior

- Cancellation-Type: 0 (Procedimiento de Actualización de MME)
- CLR-Flags: 0
- Subscription-Data: Perfil de suscripción completo

CLR Programático (Activado por API)

Los administradores pueden activar CLR a través de la API programática para forzar la desasociación de suscriptores (por ejemplo, por retiro de suscripción, prevención de fraude o acciones administrativas).



AVPs Clave (CLR Programático):

- User-Name: IMSI del suscriptor
- Destination-Host: Nombre de host del último MME visto
- Destination-Realm: Reino del último MME visto
- Cancellation-Type: `:subscription_withdrawal` (codificado como entero según 3GPP TS 29.272)
- CLR-Flags:
 - s6a_indicator: 1 (indica que se utiliza la interfaz S6a)
 - reattach_required: 1 (la UE debe re-autenticarse para volver a asociarse)

Tipos de Cancelación

OmniHSS soporta múltiples tipos de cancelación según 3GPP TS 29.272:

Tipo	Valor	Descripción	Caso de Uso
Procedimiento de Actualización de MME	0	Cambio normal de MME	Automático durante ULR desde nuevo MME
Procedimiento de Actualización de SGSN	1	Transferencia de SGSN	Escenarios de transferencia 3G/2G
Retiro de Suscripción	2	Terminación administrativa	Desasociación manual a través de API
Procedimiento de Actualización IWF	3	Actualización de función de intertrabajo	Interoperabilidad de red heredada
Procedimiento de Adjunción Inicial	4	Registro nuevo	Forzar re-autenticación

CLR-Flags

El AVP CLR-Flags es una máscara de bits con los siguientes campos:

Bandera	Bit	Descripción
Indicador S6a/S6d	0	1 = interfaz S6a utilizada
Reasociación Requerida	1	1 = la UE debe realizar un nuevo adjunto

Ejemplo de Configuración de CLR-Flags:

```
clr_flags: %{  
  s6a_indicator: 1,          # Usando la interfaz S6a  
  reattach_required: 1      # Forzar re-autenticación  
}
```

Escenarios Multi-IMSI

OmniHSS rastrea el registro de MME **por suscriptor (IMSI)**, no por MSISDN. Esto es crítico para entender el comportamiento de CLR en escenarios multi-IMSI:

Escenario 1: Múltiples MSISDNs, Un Solo IMSI

```
Suscriptor A:  
- IMSI: 999000123456789  
- MSISDNs: ["+1234567890", "+9876543210"]  
- last_seen_mme: "mme01.operator.com"
```

Cuando este suscriptor se mueve a un nuevo MME:

- **Un CLR enviado** a "mme01.operator.com" con IMSI 999000123456789
- Ambos MSISDNs se ven afectados (mismo suscriptor, misma SIM)
- El AVP User-Name contiene el IMSI, no MSISDNs

Escenario 2: Múltiples Suscriptores (IMSI Diferentes), Mismo MSISDN

OmniHSS aplica la **restricción de MSISDN único** (un MSISDN no puede pertenecer a múltiples suscriptores simultáneamente). Sin embargo, durante la portación/migración:

Suscriptor A:

- IMSI: 999000111111111
- MSISDN: "+1234567890"
- last_seen_mme: "mme01.operator.com"

Suscriptor B (después de la portación):

- IMSI: 999000222222222
- MSISDN: "+1234567890" # Mismo MSISDN, SIM/IMSI diferente
- last_seen_mme: "mme02.operator.com"

Cuando el Suscriptor B se registra:

- **No se envía CLR** (IMSI diferente = suscriptor diferente)
- El Suscriptor A permanece registrado en mme01
- El Suscriptor B se registra en mme02
- Ambos pueden estar activos simultáneamente (dispositivos físicos diferentes)

Escenario 3: CLR Programático para Suscriptor Multi-MSISDN

Resultado:

- **Un CLR enviado** al last_seen_mme del suscriptor
- **Todos los MSISDNs** asociados con ese IMSI están efectivamente desasociados
- El IMSI es la clave principal para rastrear el registro de MME

Notas Importantes

1. **IMSI es la Clave:** Las operaciones CLR son siempre **por IMSI**, nunca por MSISDN. La tabla `subscriber_state` rastrea `last_seen_mme` por suscriptor (IMSI).
2. **Operación Atómica:** Cada suscriptor solo puede estar registrado en un MME a la vez. El CLR automático asegura esto limpiando el registro antiguo.
3. **No CLR si No Hay MME Anterior:** Si `last_seen_mme` es `nil` (el suscriptor nunca se registró), no se envía CLR durante ULR.

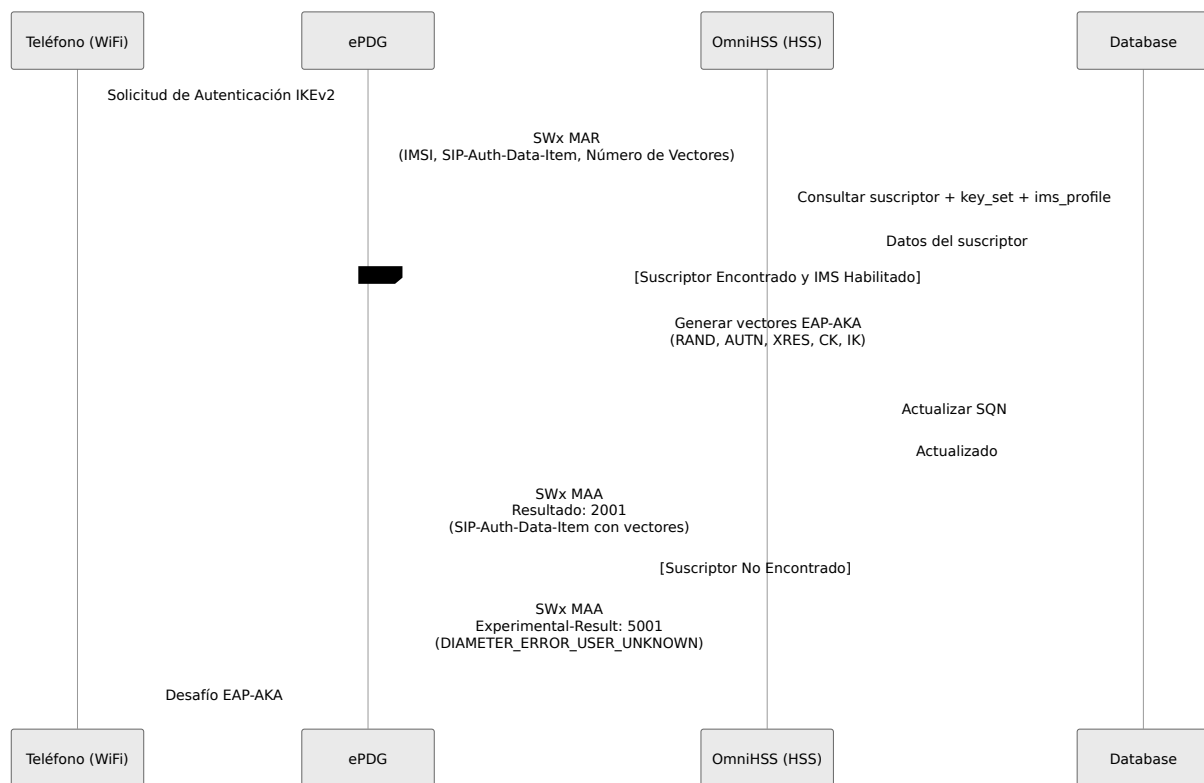
4. **Datos de Suscripción Incluidos:** El CLR automático (durante ULR) incluye el AVP completo `Subscription-Data` para ayudar al antiguo MME a limpiar correctamente el contexto.
 5. **Asincrónico:** El CLR se envía de manera asincrónica (fire-and-forget). La respuesta ULA al nuevo MME no espera la CLA del antiguo MME.
 6. **Manejo de CLA:** OmniHSS recibe respuestas CLA pero actualmente las descarta. Esto previene bucles de mensajes y es un comportamiento estándar del HSS.
-

Interfaz SWx (Acceso No 3GPP / Llamadas WiFi)

La interfaz SWx permite llamadas WiFi conectando el ePDG (Evolved Packet Data Gateway) al HSS para la autenticación y autorización del suscriptor a través de redes de acceso no 3GPP.

Solicitud de Autenticación Multimedia (MAR/MAA)

ePDG solicita vectores de autenticación EAP-AKA para el registro de llamadas WiFi.



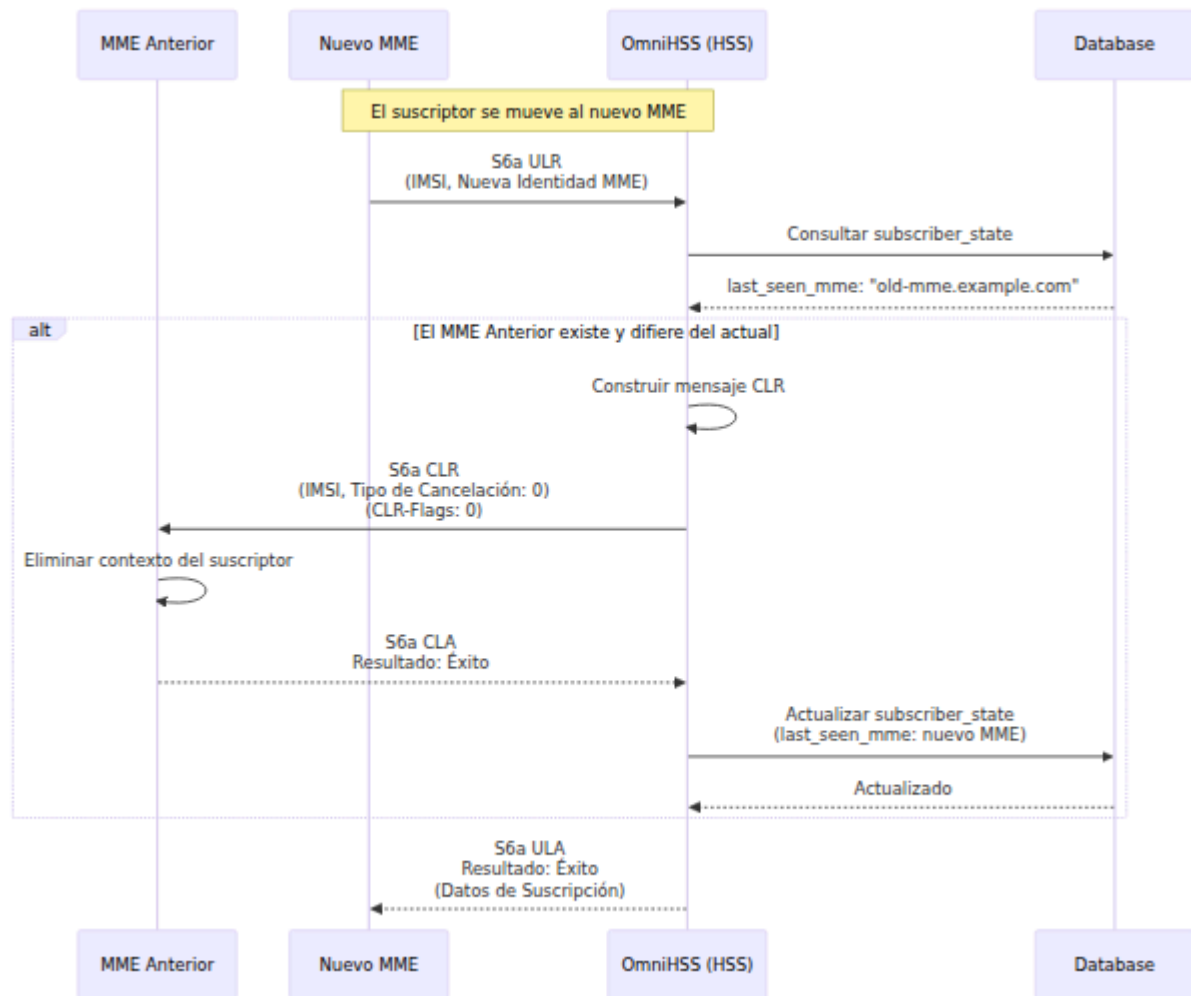
AVPs Clave:

- Solicitud: User-Name (IMSI o IMSI@realm), SIP-Auth-Data-Item (esquema de autenticación), SIP-Number-Auth-Items
- Respuesta: SIP-Auth-Data-Item (SIP-Authenticate, SIP-Authorization, Confidentiality-Key, Integrity-Key)

Resincronización de SQN: Cuando la UE detecta un fallo de autenticación debido a un desajuste de SQN, el ePDG incluye datos de resincronización en el AVP SIP-Authorization. OmniHSS extrae AUTS de este campo y recalcula SQN utilizando un cálculo consciente de la longitud de IND según 3GPP TS 33.102.

Solicitud de Asignación de Servidor (SAR/SAA)

ePDG registra o desregistra al suscriptor para servicios de llamadas WiFi.



Tipos de Asignación de Servidor:

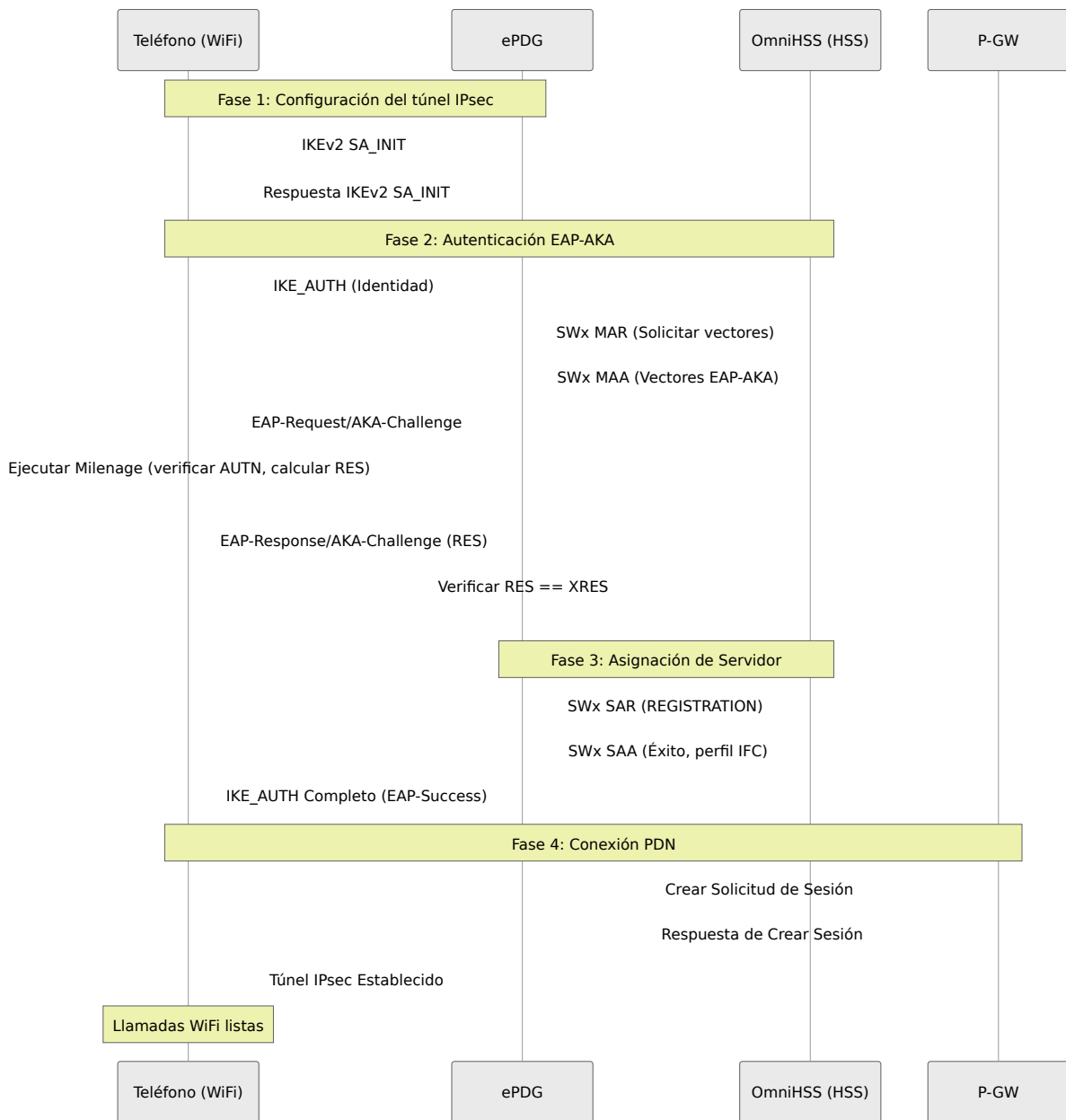
Tipo	Valor	Descripción
NO_ASSIGNMENT	0	Solo consulta, sin cambio de estado
REGISTRATION	1	Registro inicial de llamadas WiFi
RE_REGISTRATION	2	Actualización de registro
UNREGISTERED_USER	3	Servicios para usuario no registrado
TIMEOUT_DEREGISTRATION	4	Tiempo de espera de registro
USER_DEREGISTRATION	5	Desregistro iniciado por el usuario
AUTHENTICATION_FAILURE	7	Fallo de autenticación, limpiar estado
ADMINISTRATIVE_DEREGISTRATION	8	Desregistro iniciado por el administrador

AVPs Clave:

- Solicitud: User-Name (IMSI), Server-Assignment-Type, Server-Name (identidad ePDG), Service-Selection (APN)
- Respuesta: User-Data (perfil IFC XML), Non-3GPP-User-Data

Flujo de Registro de Llamadas WiFi

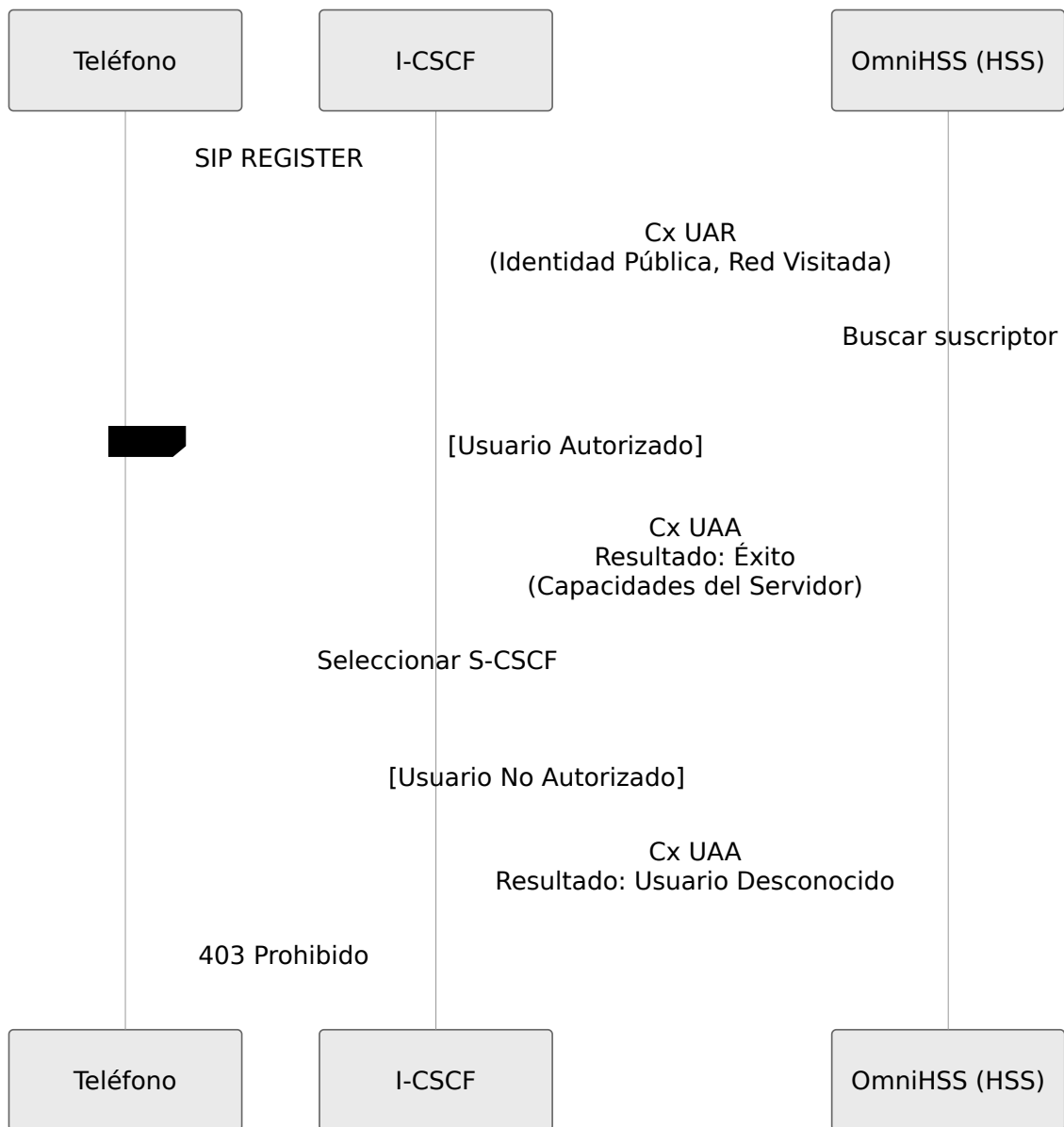
Registro completo de llamadas WiFi de extremo a extremo.



Interfaz Cx (IMS)

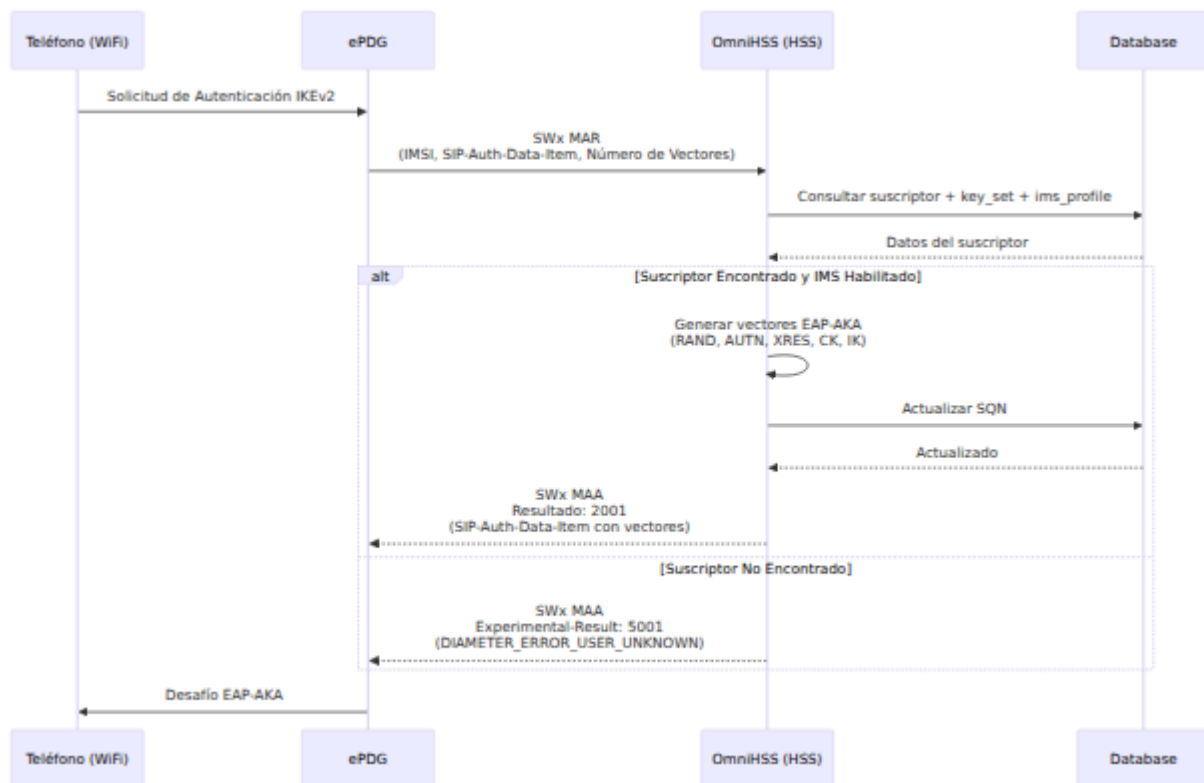
Solicitud de Autorización de Usuario (UAR/UAA)

I-CSCF consulta si el usuario está autorizado para registrarse.



Solicitud de Asignación de Servidor (SAR/SAA)

S-CSCF registra/desregistra al usuario y recupera el perfil IMS.

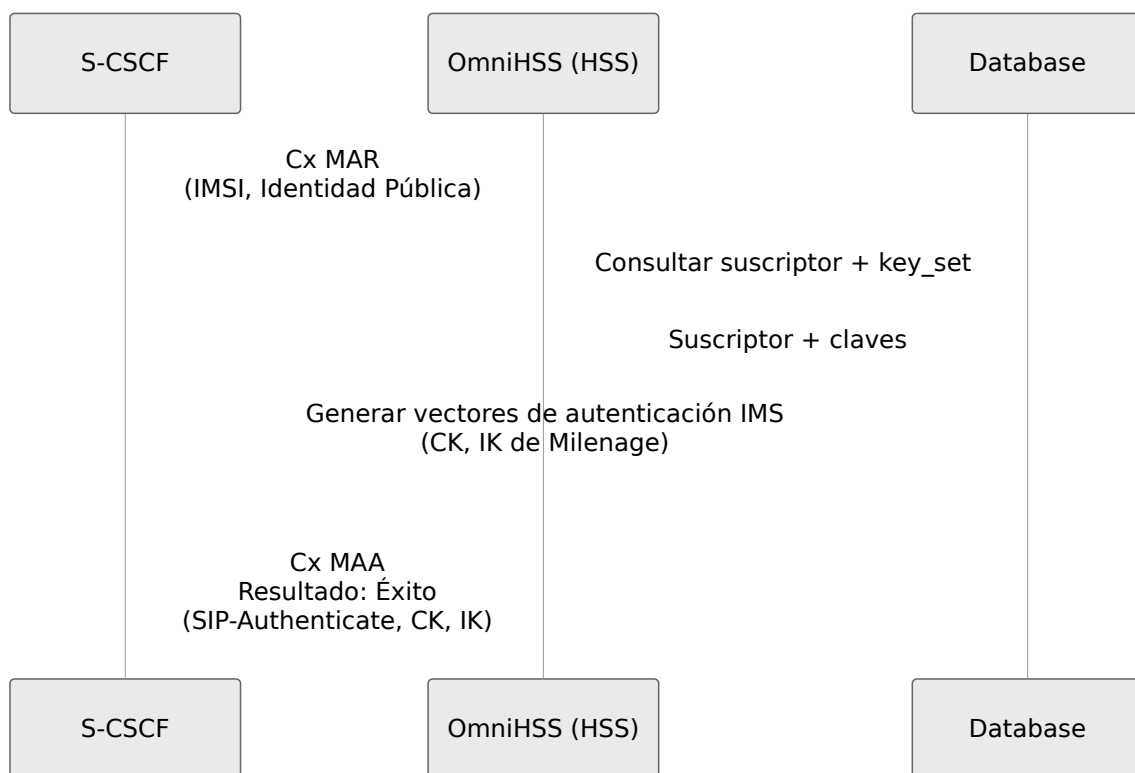


Renderización de Plantilla IFC:

- `{{imsi}}` → IMSI real
- `{{msisdns}}` → Lista de números de teléfono
- `{{mcc}}`, `{{mnc}}` → Códigos PLMN de origen

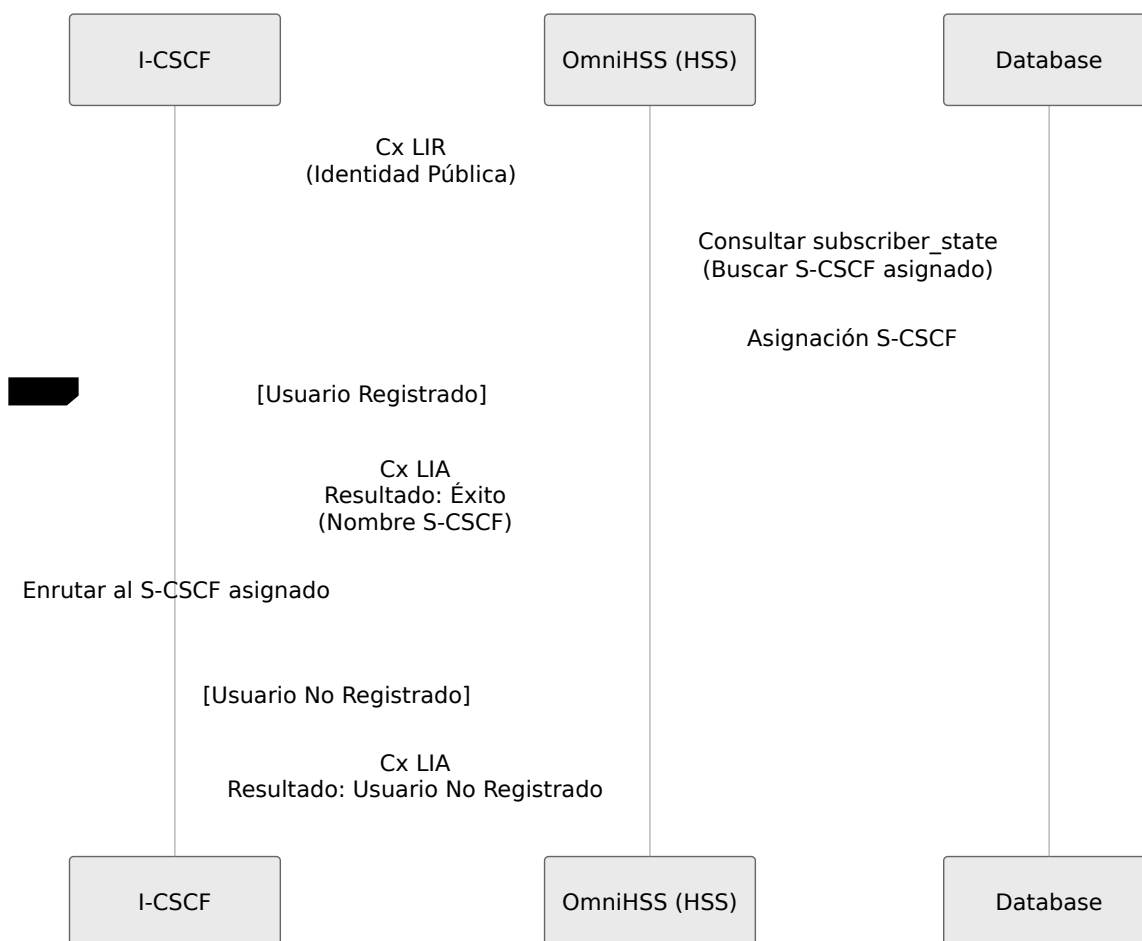
Solicitud de Autenticación Multimedia (MAR/MAA)

S-CSCF solicita vectores de autenticación para el registro IMS.



Solicitud de Información de Ubicación (LIR/LIA)

I-CSCF consulta qué S-CSCF está sirviendo al usuario.

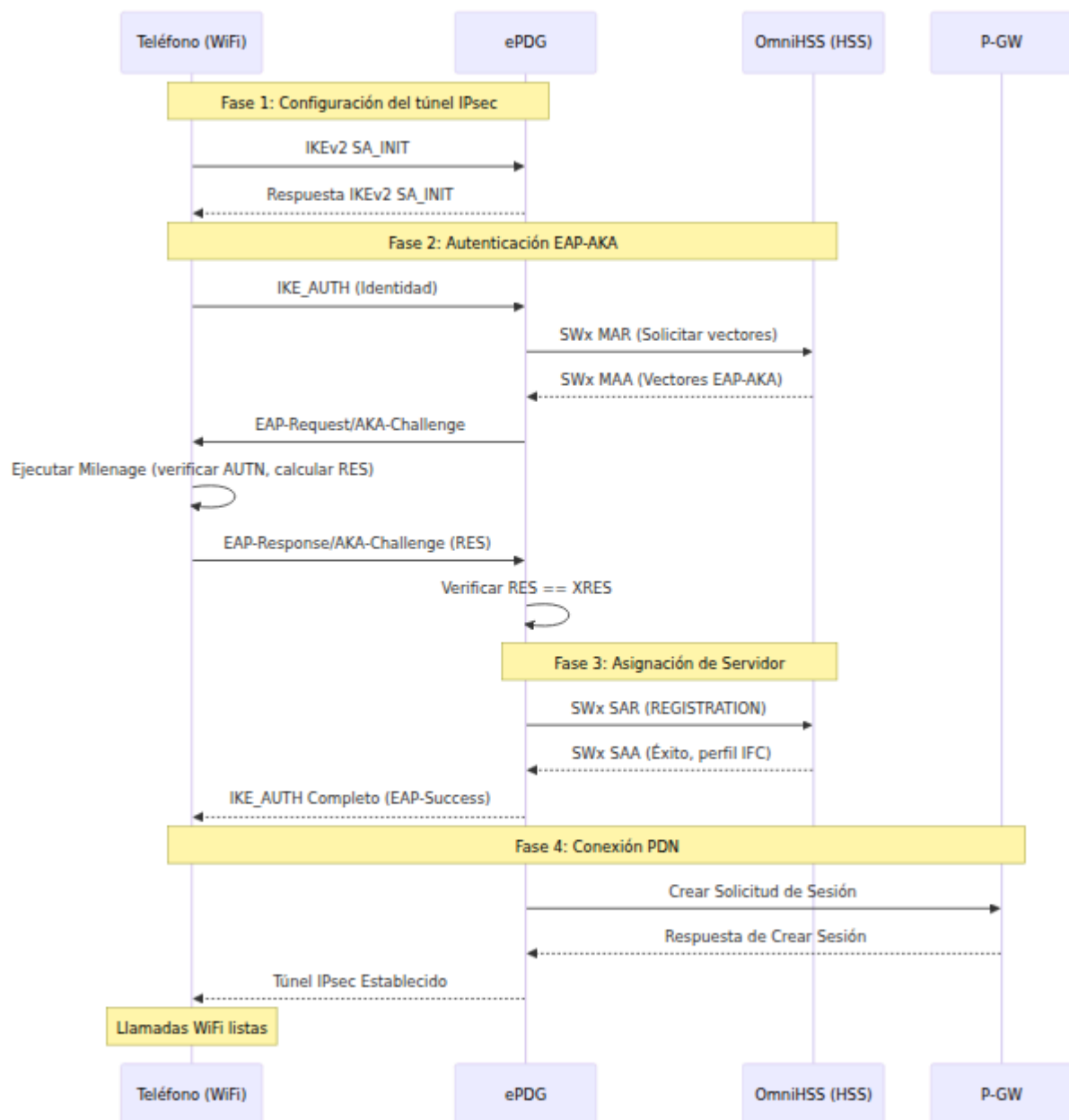


Interfaz Sh (Datos de Perfil IMS)

Ver **Sh RepositoryData (Datos Transparentes)** para el modelo de datos, reglas de secuencia/n concurrencia, y la API de aprovisionamiento REST para documentos de MMTEL-Services / IMS-ODB-Information.

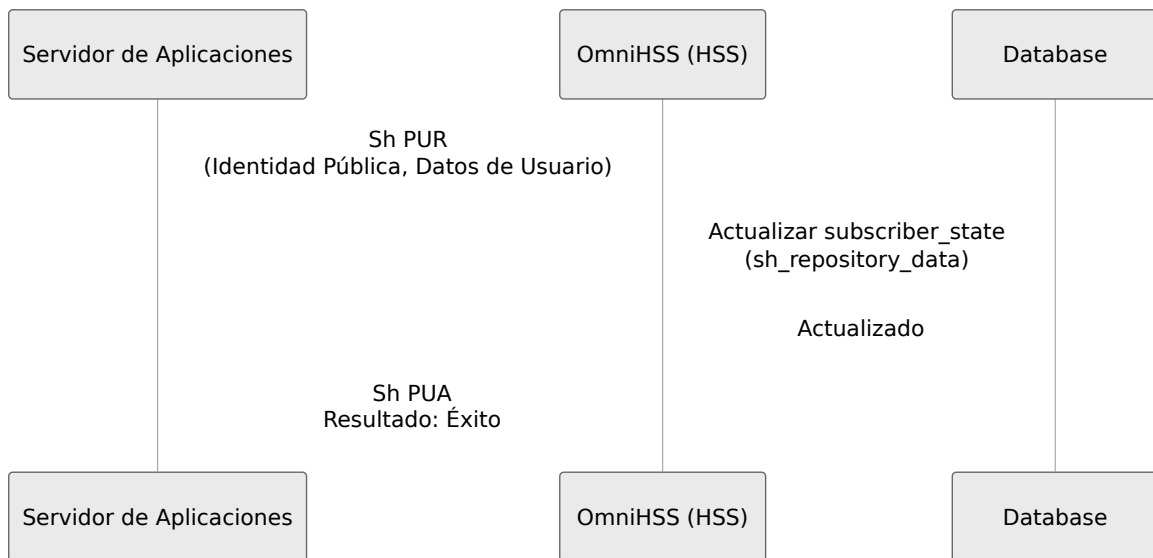
Solicitud de Datos de Usuario (UDR/UDA)

El Servidor de Aplicaciones solicita datos del perfil del suscriptor.



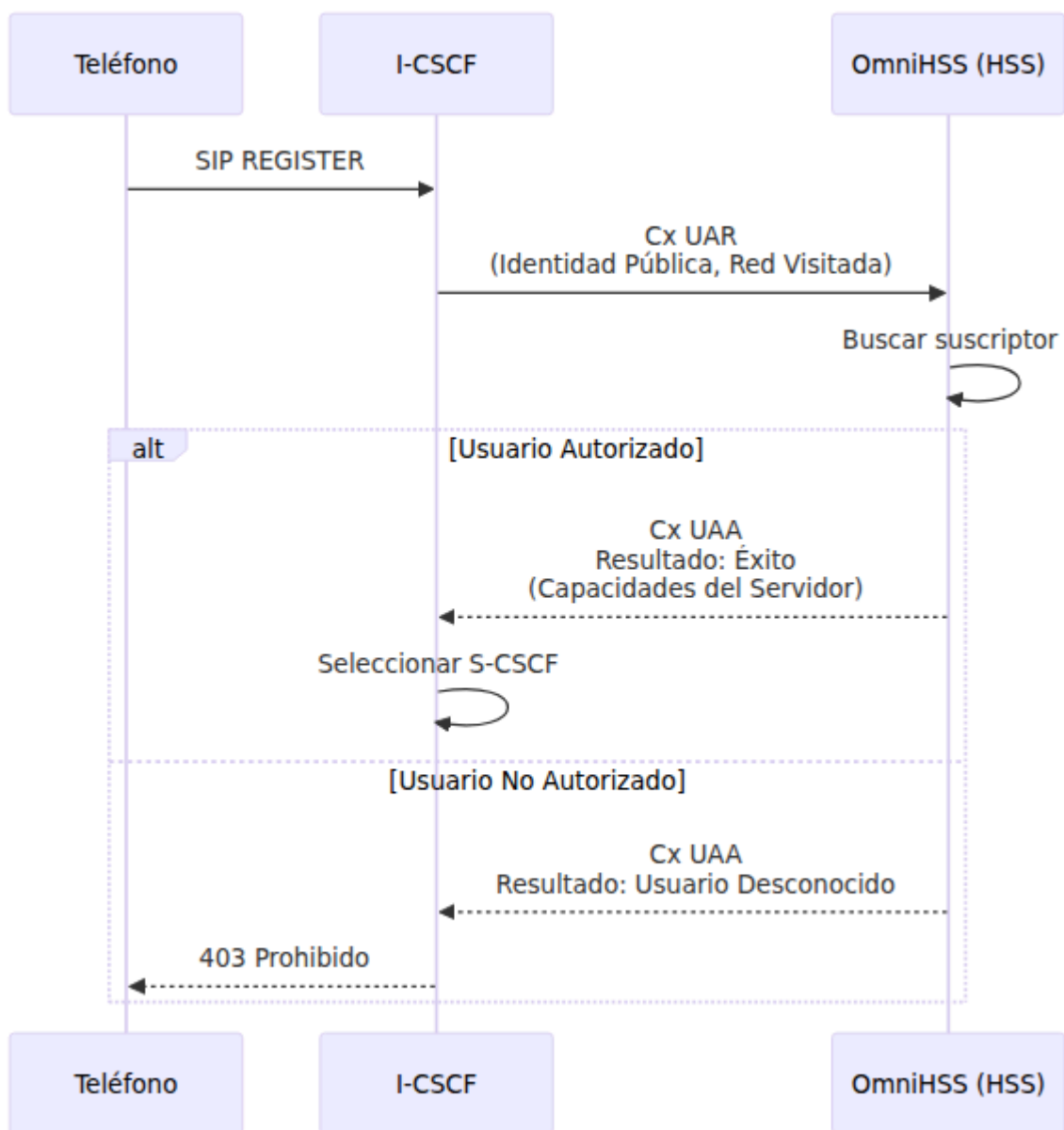
Solicitud de Actualización de Perfil (PUR/PUA)

El Servidor de Aplicaciones actualiza los datos del perfil del suscriptor.



Solicitud de Notificaciones de Suscripción (SNR/SNA)

El Servidor de Aplicaciones se suscribe a cambios en el perfil.



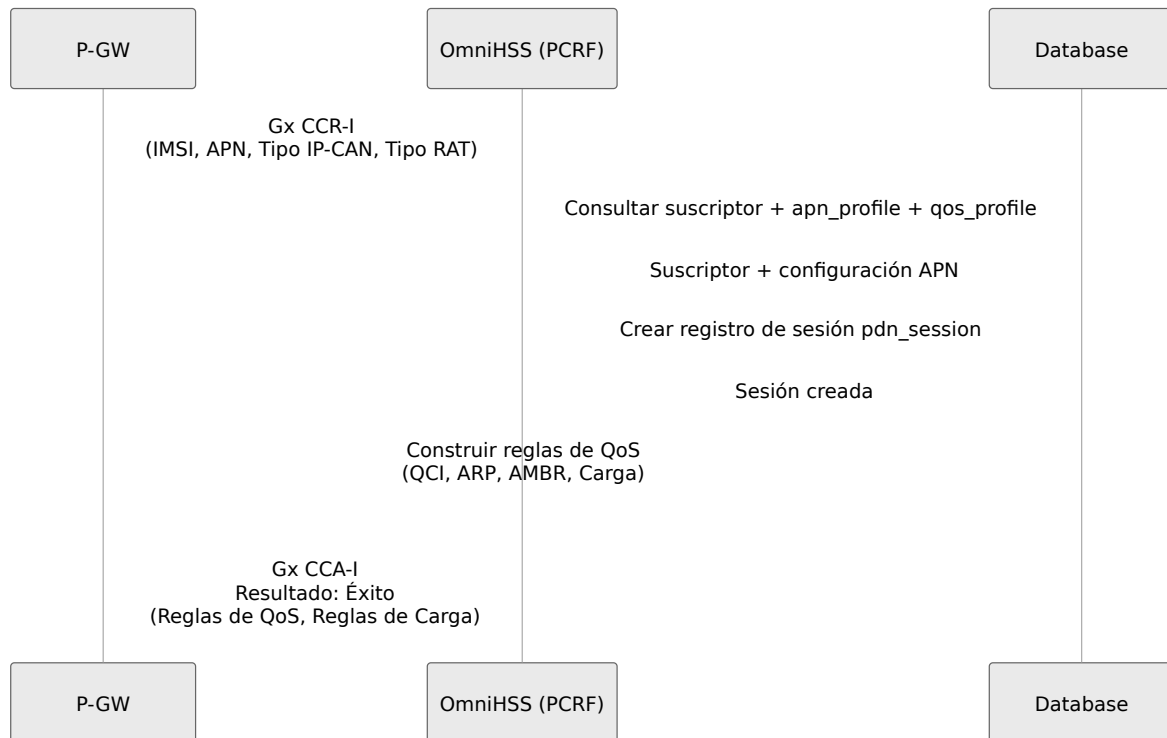
Interfaz Gx (Control de Políticas)

OmniHSS funciona como el PCRF (Función de Reglas de Políticas y Carga) a través de la interfaz Gx.

Ver **Documentación PCRF** para arquitectura detallada, configuración de políticas y gestión de QoS.

Solicitud de Control de Crédito - Inicial (CCR-I/CCA-I)

P-GW solicita reglas de políticas cuando se establece la sesión PDN.

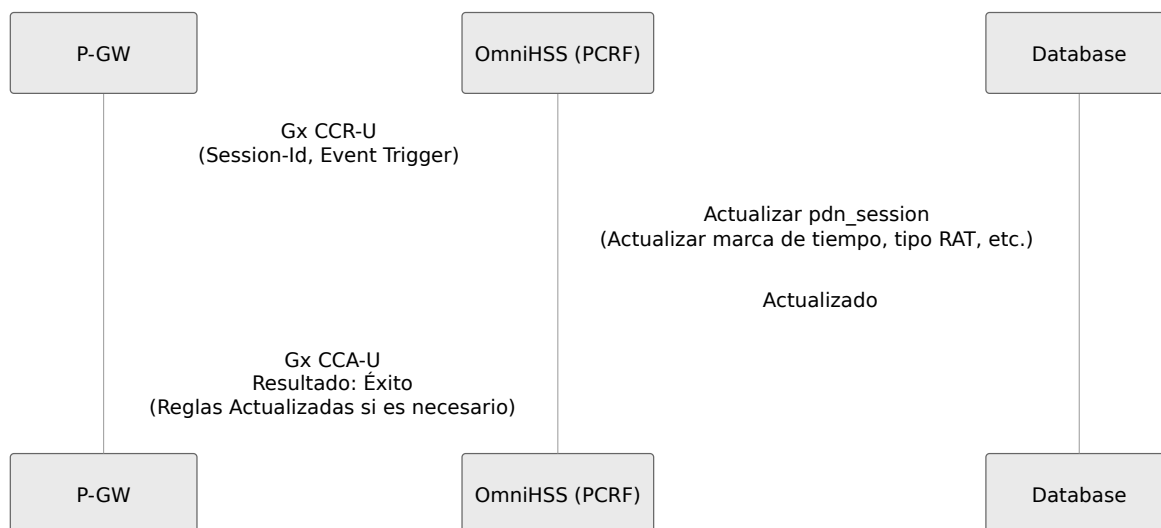


AVPs Clave:

- Solicitud: Subscription-Id (IMSI), Called-Station-Id (APN), RAT-Type, IP-CAN-Type
- Respuesta: QoS-Information (QCI, ARP, AMBR), Charging-Rule-Install

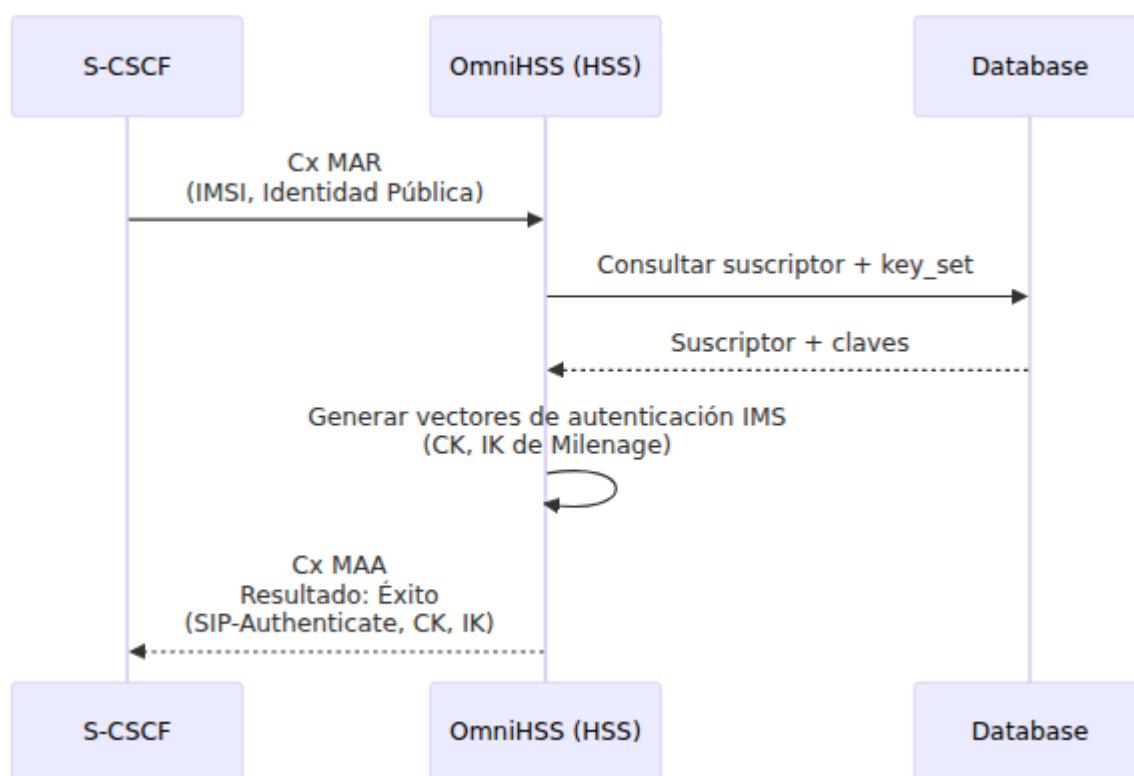
Solicitud de Control de Crédito - Actualización (CCR-U/CCA-U)

P-GW notifica cambios en la sesión.



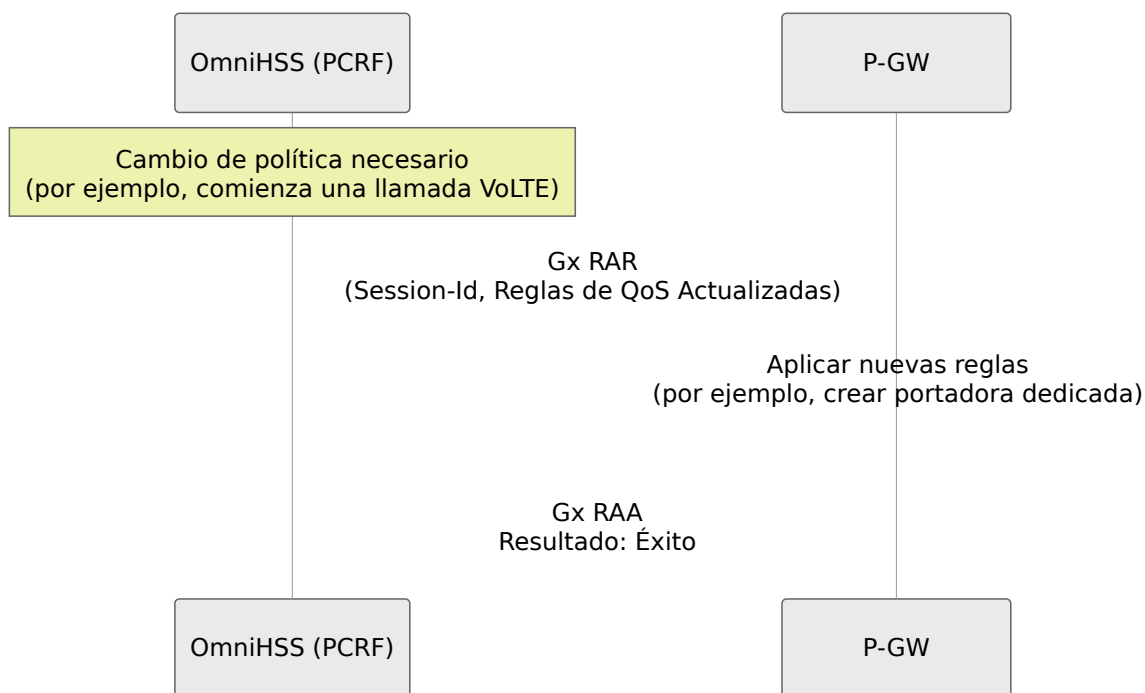
Solicitud de Control de Crédito - Terminar (CCR-T/CCA-T)

P-GW notifica cuando termina la sesión PDN.



Solicitud de Reautenticación (RAR/RAA)

OmniHSS (PCRF) inicia la actualización de políticas al P-GW.



Interfaz Rx (Política de Medios IMS)

OmniHSS funciona como el PCRF a través de la interfaz Rx para la autorización de medios IMS.

Consulte la **Documentación de PCRF** para flujos de llamadas VoLTE y autorización de medios detallados.

Solicitud AA (AAR/AAA)

P-CSCF solicita autorización de medios para la sesión IMS.

Parse error on line 19: ... Nota sobre HSS: Activar configurac... -----
^ Expecting 'SOLID_OPEN_ARROW', 'DOTTED_OPEN_ARROW',
'SOLID_ARROW', 'BIDIRECTIONAL_SOLID_ARROW', 'DOTTED_ARROW',
'BIDIRECTIONAL_DOTTED_ARROW', 'SOLID_CROSS', 'DOTTED_CROSS',
'SOLID_POINT', 'DOTTED_POINT', got 'TXT'

Intente de nuevo

Información Clave:

- Analizar SDP para determinar códec y ancho de banda
- Calcular ancho de banda requerido (UL/DL)
- Crear filtros SDF para flujos de medios
- Activar portadora dedicada a través de Gx RAR

Solicitud de Terminación de Sesión (STR/STA)

P-CSCF notifica cuando la sesión IMS finaliza.

Parse error on line 14: ... Nota sobre HSS: Liberar portadora ... -----
^ Expecting 'SOLID_OPEN_ARROW', 'DOTTED_OPEN_ARROW',
'SOLID_ARROW', 'BIDIRECTIONAL_SOLID_ARROW', 'DOTTED_ARROW',
'BIDIRECTIONAL_DOTTED_ARROW', 'SOLID_CROSS', 'DOTTED_CROSS',
'SOLID_POINT', 'DOTTED_POINT', got 'TXT'

Intente de nuevo

Interfaz Sy (Control de Límite de Gastos)

OmniHSS, actuando como el PCRF, utiliza la interfaz Sy para obtener el estado del límite de gastos del suscriptor de un OCS externo (Sistema de Carga en Línea) y aplicar políticas impulsadas por el gasto a través de Gx. Sy utiliza el ID de aplicación Diameter `16777302` (3GPP TS 29.219). El HSS es el cliente Sy; el OCS es el servidor. Consulte la [Interfaz Sy](#) para la referencia completa (mapeo de contadores de política, AVPs, configuración).

Solicitud de Límite de Gastos (SLR/SLA)

El PCRF abre una sesión Sy por suscriptor para obtener el estado actual de los contadores de política del OCS, luego incorpora las reglas resultantes en el Gx CCA que ya devuelve.

Parse error on line 9: ...) Nota sobre HSS: Resolver regla de ... -----
-^ Expecting 'SOLID_OPEN_ARROW', 'DOTTED_OPEN_ARROW',
'SOLID_ARROW', 'BIDIRECTIONAL_SOLID_ARROW', 'DOTTED_ARROW',
'BIDIRECTIONAL_DOTTED_ARROW', 'SOLID_CROSS', 'DOTTED_CROSS',
'SOLID_POINT', 'DOTTED_POINT', got 'TXT'

Intente de nuevo

Notificación de Estado de Gastos (SNR/SNA)

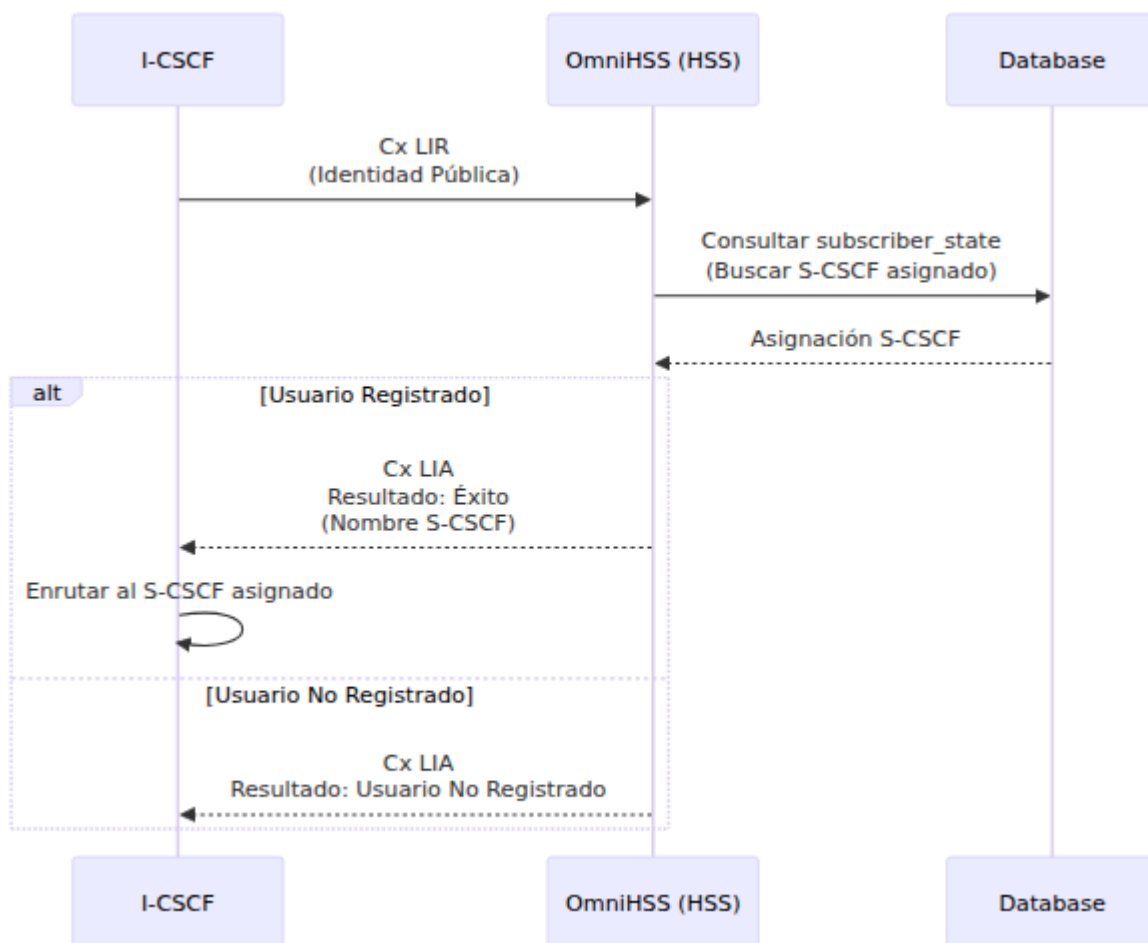
Cuando cambia el estado de un contador (por ejemplo, se agota un límite de datos), el OCS notifica al PCRF, que envía el cambio de política al PGW con un Gx RAR.

Parse error on line 8: ...o Nota sobre HSS: Nuevo estado -> in... -----
---^ Expecting 'SOLID_OPEN_ARROW', 'DOTTED_OPEN_ARROW',
'SOLID_ARROW', 'BIDIRECTIONAL_SOLID_ARROW', 'DOTTED_ARROW',
'BIDIRECTIONAL_DOTTED_ARROW', 'SOLID_CROSS', 'DOTTED_CROSS',
'SOLID_POINT', 'DOTTED_POINT', got 'TXT'

Intente de nuevo

Terminación de Sesión (STR/STA)

Cuando finaliza la última sesión de datos del suscriptor, el PCRF cierra la sesión Sy.



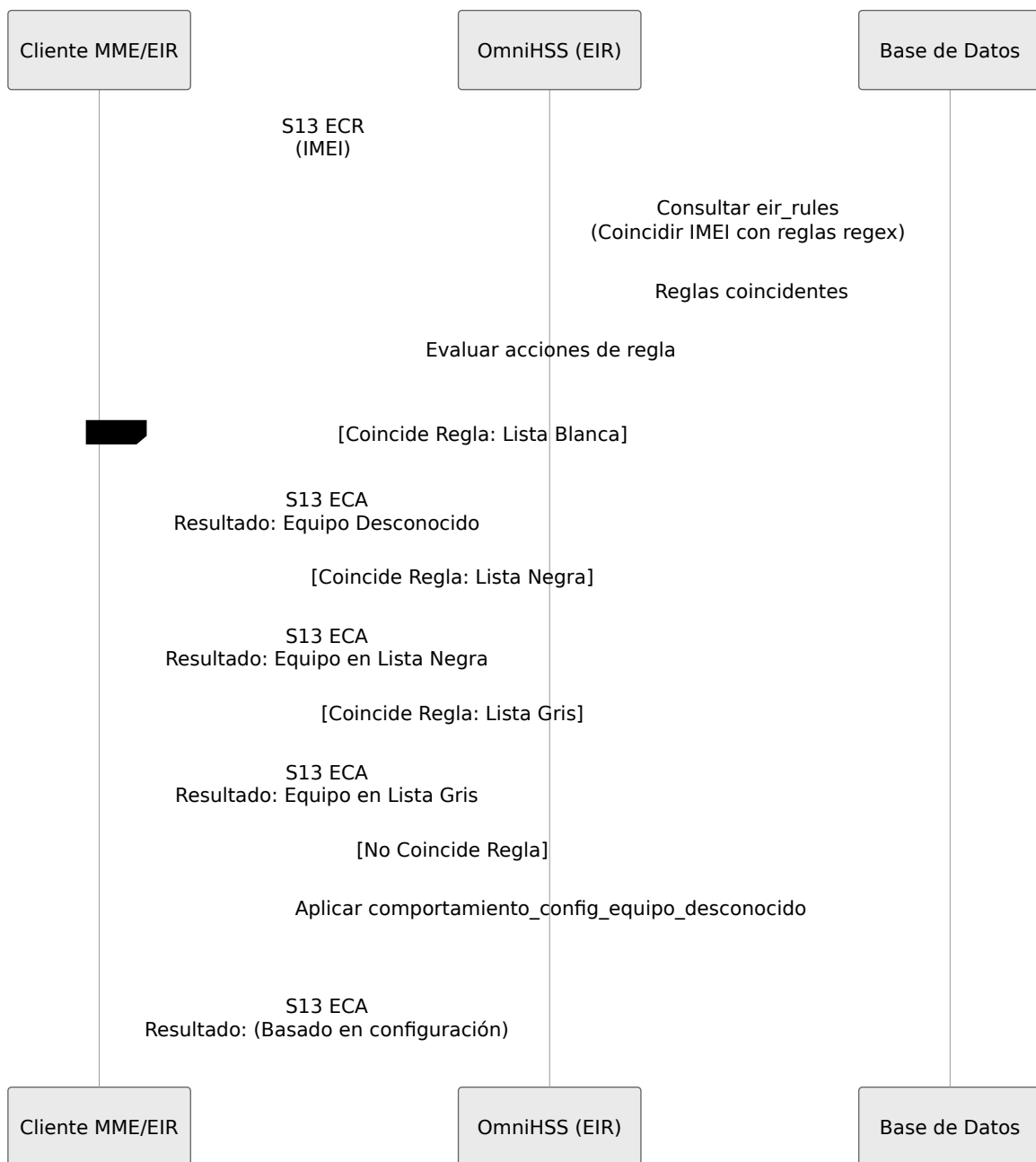
Interfaz S13 (EIR)

OmniHSS funciona como el EIR (Registro de Identidad de Equipos) a través de la interfaz S13.

Consulte la **Documentación de EIR** para la verificación detallada de la identidad del equipo, validación de IMEI y gestión de listas negras.

Solicitud de Verificación de Identidad del ME (ECR/ECA)

El cliente EIR externo (o MME) solicita la validación del equipo.



Valores de Estado del Equipo:

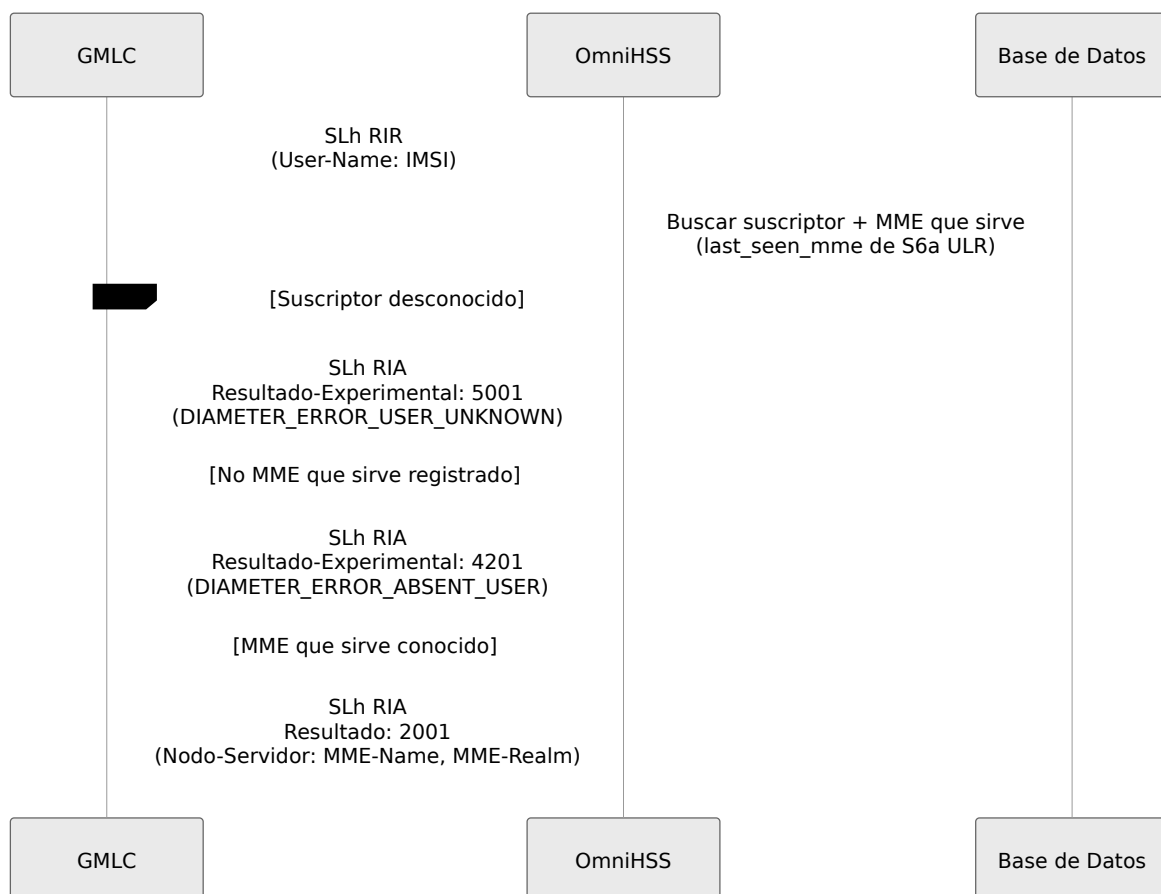
- **Equipo Desconocido (0)** - Dispositivo permitido (lista blanca)
 - **Equipo en Lista Negra (1)** - Dispositivo bloqueado
 - **Equipo en Lista Gris (2)** - Dispositivo permitido pero rastreado
-

Interfaz SLh (LCS / Servicios de Localización)

OmniHSS responde a SLh `LCS-Routing-Info-Request` (RIR) para que un GMLC pueda descubrir qué MME está sirviendo actualmente a un suscriptor antes de solicitar su ubicación a través de SLg. El MME que sirve es el que se registró en la S6a (Update-Location). SLh utiliza el ID de aplicación Diameter `16777291` (3GPP TS 29.173).

Solicitud de Información de Enrutamiento LCS (RIR/RIA)

GMLC solicita el nodo que sirve a un suscriptor.



Notas:

- El IMSI se toma de `User-Name`; se utiliza una búsqueda de MSISDN como respaldo.

- El `Nodo-Servidor` devuelto lleva el `MME-Name/MME-Realm` registrado por última vez por los controladores S6a AIR/ULR (`subscriber_state.last_seen_mme` / `last_seen_realm`) - no se requiere aprovisionamiento adicional.
- Un GMLC típicamente sigue una RIA exitosa con una SLg Provide-Location-Request al MME devuelto.

Códigos de Resultado:

- **2001** - Éxito; `Nodo-Servidor` devuelto.
- **5001** - `DIAMETER_ERROR_USER_UNKNOWN`; IMSI/MSISDN no aprovisionado.
- **4201** - `DIAMETER_ERROR_ABSENT_USER`; suscriptor conocido pero sin MME que sirva registrado (nunca adjunto, o ubicación cancelada).

Flujo Completo de Llamadas: Llamada VoLTE

Configuración de llamada VoLTE de extremo a extremo que muestra múltiples interfaces.

Parse error on line 8: ...S Nota sobre UE,MME: Fase 1: Adjunt -----^
Expecting 'SOLID_OPEN_ARROW', 'DOTTED_OPEN_ARROW', 'SOLID_ARROW',
'BIDIRECTIONAL_SOLID_ARROW', 'DOTTED_ARROW',
'BIDIRECTIONAL_DOTTED_ARROW', 'SOLID_CROSS', 'DOTTED_CROSS',
'SOLID_POINT', 'DOTTED_POINT', got ','

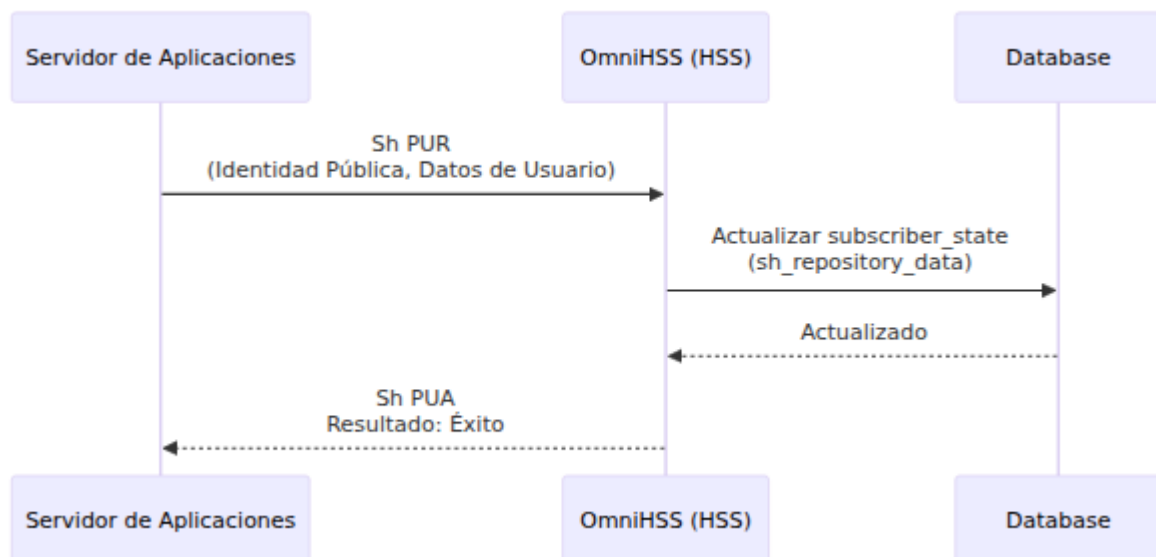
Intente de nuevo

Interfaz Zh (Arquitectura de Arranque Genérico)

La interfaz Zh habilita la Arquitectura de Arranque Genérico (GBA) conectando la Función del Servidor de Arranque (BSF) al HSS para la autenticación del suscriptor y la derivación de claves.

Solicitud de Autenticación Multimedia (MAR/MAA)

BSF solicita vectores de autenticación GBA para el arranque.



AVPs Clave:

- Solicitud: User-Name (IMPI), Identidad Pública, Elemento de Datos de Autenticación SIP (esquema de autenticación), Dominio de Destino
- Respuesta: Elemento de Datos de Autenticación SIP (SIP-Authenticate, SIP-Authorization, Confidentiality-Key, Integrity-Key), GBA-UserSecSettings

Casos de Uso de GBA:

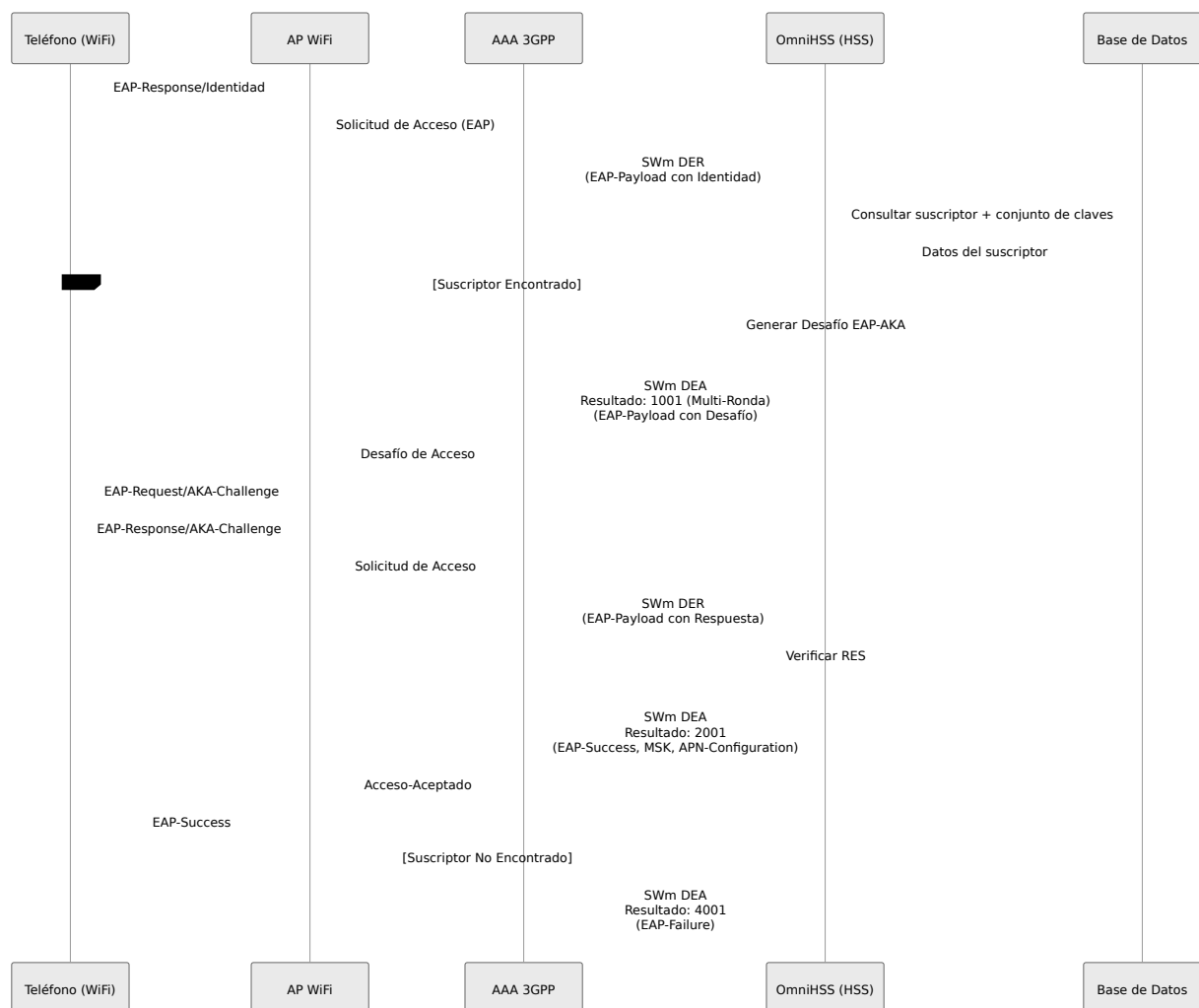
Aplicación	Descripción
MBMS	Gestión de claves del Servicio de Multicast Móvil
HTTPS	Aprovisionamiento de certificados basado en GBA
NAF	Autenticación de Función de Aplicación de Red Genérica
Presencia	Autenticación de servicio de presencia segura

Interfaz SWm (Acceso No Confiable No 3GPP)

La interfaz SWm habilita la autenticación EAP-AKA para redes de acceso no confiables no 3GPP (por ejemplo, WiFi a través de ePDG) al conectar el Servidor AAA 3GPP al HSS.

Solicitud Diameter-EAP (DER/DEA)

Intercambio de autenticación EAP para acceso WiFi.

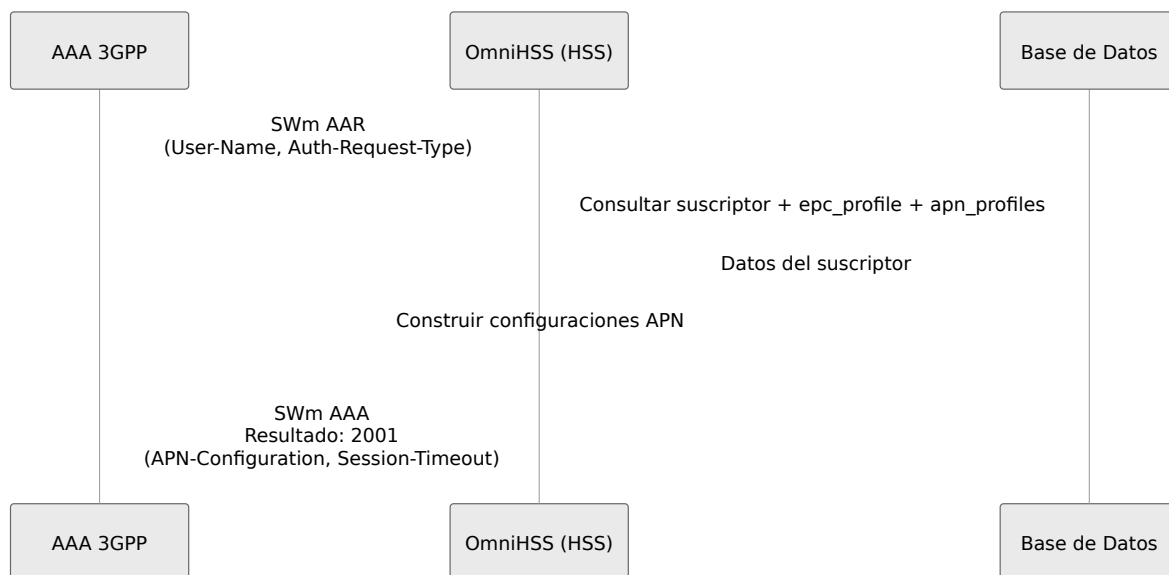


AVPs Clave:

- Solicitud: Session-Id, Auth-Application-Id, EAP-Payload, Auth-Request-Type, User-Name (opcional)
- Respuesta: EAP-Payload, EAP-Master-Session-Key (MSK), APN-Configuration, Session-Timeout

Solicitud AA (AAR/AAA)

Autorización después de una autenticación EAP exitosa.

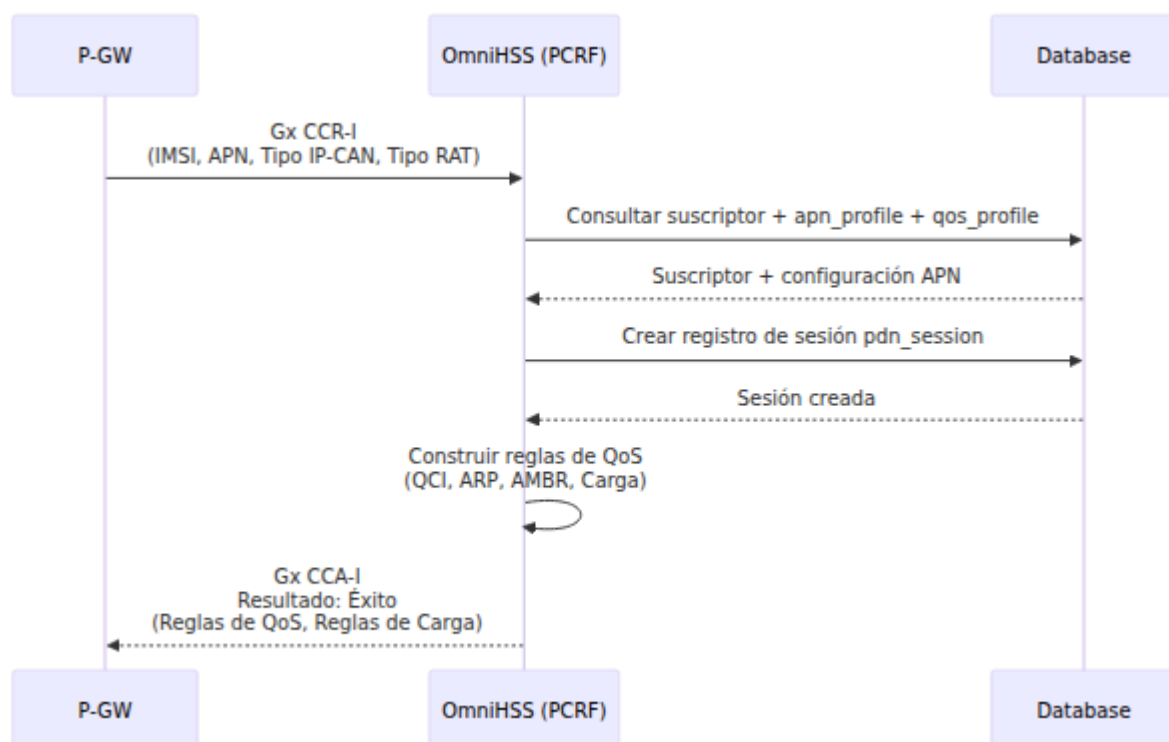


AVPs Clave:

- Solicitud: Session-Id, Auth-Application-Id, User-Name, Auth-Request-Type, AAR-Flags
- Respuesta: APN-Configuration, 3GPP-Charging-Characteristics, Session-Timeout

Solicitud de Terminación de Sesión (STR/STA)

Notificación de terminación de sesión WiFi.



Causas de Terminación:

Causa	Valor	Descripción
DIAMETER_LOGOUT	1	Cierre de sesión del usuario
DIAMETER_SERVICE_NOT_PROVIDED	2	Servicio no disponible
DIAMETER_BAD_ANSWER	3	Error de protocolo
DIAMETER_ADMINISTRATIVE	4	Terminación administrativa
DIAMETER_LINK_BROKEN	5	Conexión perdida
DIAMETER_AUTH_EXPIRED	6	Tiempo de autenticación agotado
DIAMETER_USER_MOVED	7	Usuario movido a otro acceso
DIAMETER_SESSION_TIMEOUT	8	Tiempo de sesión agotado

Solución de Problemas de Problemas de Protocolo

Fallos de Autenticación (S6a AIR)

Verifique:

1. Conjunto de claves configurado correctamente (Ki, OPC, AMF)
2. Sincronización de SQN (si hay fallos repetidos)
3. Las reglas de roaming permiten la red visitada

Fallos de Actualización de Ubicación (S6a ULR)

Verifique:

1. El perfil EPC existe y tiene APNs configurados
2. Se permite roaming para servicios de datos
3. El formato de identidad de MME es correcto

Fallos de Registro IMS (Cx SAR)

Verifique:

1. El perfil IMS asignado al suscriptor
2. Plantilla IFC válida XML
3. Selección de S-CSCF configurada
4. MSISDN asignados si se utilizan en la plantilla

Fallos de Conexión PDN (Gx CCR-I)

Verifique:

1. El APN existe en la lista de APN del perfil EPC
2. El perfil QoS del APN está configurado
3. La tabla de sesiones PDN no está llena (si existen límites)

[← Volver a la Guía de Operaciones](#)

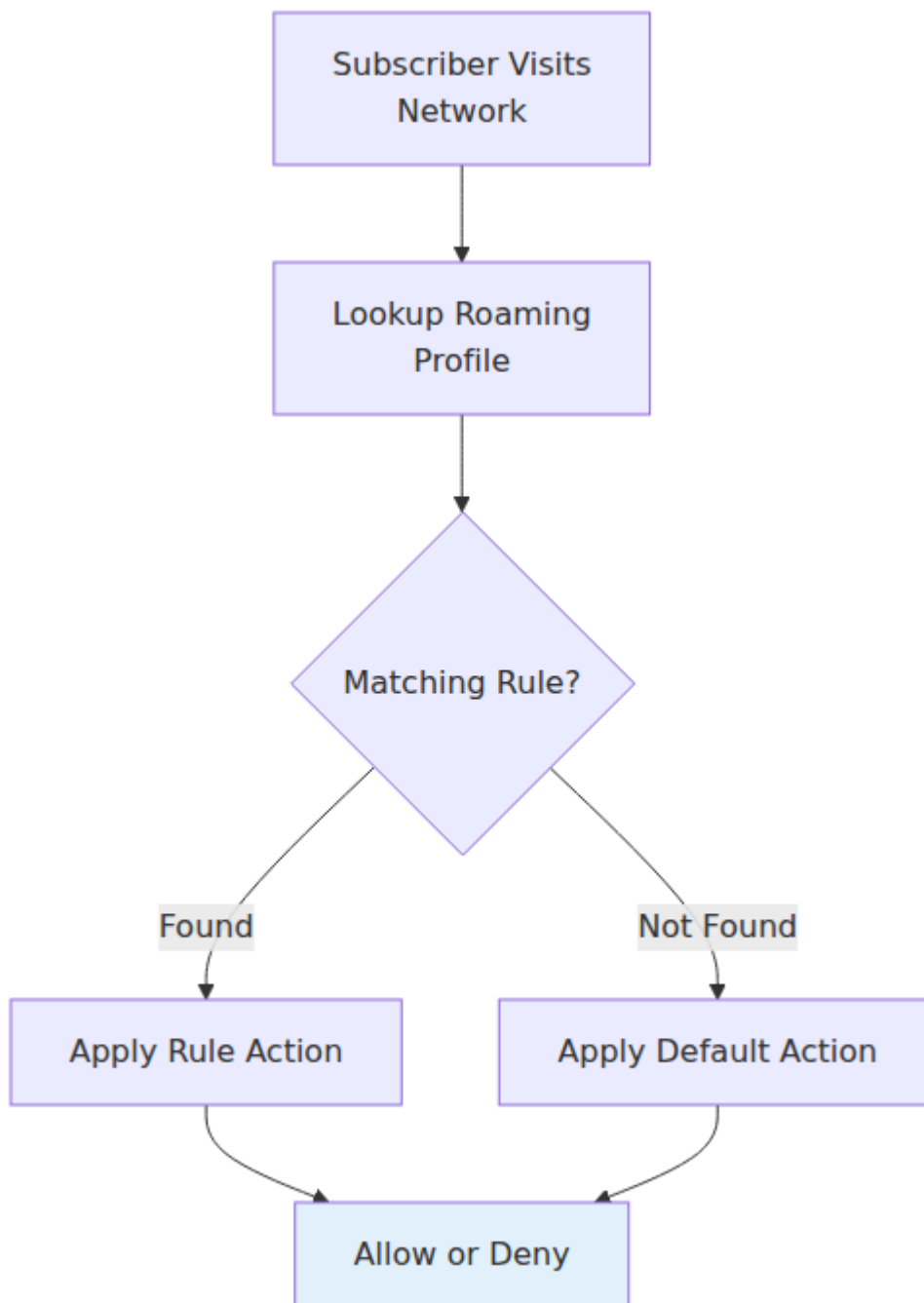
Control de Roaming de OmniHSS

[← Volver a la Guía de Operaciones](#)

Descripción General

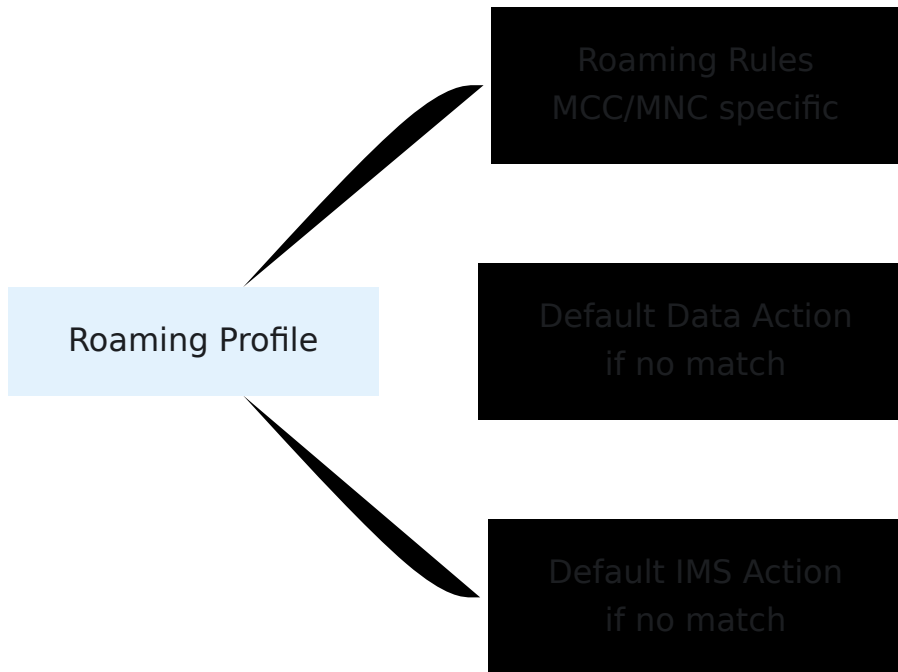
OmniHSS proporciona un control de roaming granular, permitiéndote definir qué redes pueden acceder los suscriptores tanto para servicios de datos como de IMS al hacer roaming.

Flujo de Control de Roaming



Estructura del Perfil de Roaming

Componentes



Regla de Roaming

Cada regla especifica una acción para una red específica (combinación de MCC/MNC).

Campos:

- `name` - Nombre descriptivo
- `mcc` - Código de País Móvil (3 dígitos)
- `mnc` - Código de Red Móvil (2-3 dígitos)
- `data_action` - "allow" o "deny"
- `ims_action` - "allow" o "deny"

Perfil de Roaming

Define el comportamiento predeterminado y vincula a las reglas.

Campos:

- `name` - Nombre del perfil
 - `data_action_if_no_rules_match` - "allow" o "deny"
 - `ims_action_if_no_rules_match` - "allow" o "deny"
-

Ejemplos de Configuración

Permitir Todo el Roaming

```
# Crear perfil que permite todo
curl -k -X POST https://hss.example.com:8443/api/roaming/profile \
-H "Content-Type: application/json" \
-d '{
  "roaming_profile": {
    "name": "Allow All",
    "data_action_if_no_rules_match": "allow",
    "ims_action_if_no_rules_match": "allow",
    "roaming_rules": []
  }
}'
```

Denegar Todo el Roaming

```
# Crear perfil que bloquea todo
curl -k -X POST https://hss.example.com:8443/api/roaming/profile \
-H "Content-Type: application/json" \
-d '{
  "roaming_profile": {
    "name": "No Roaming",
    "data_action_if_no_rules_match": "deny",
    "ims_action_if_no_rules_match": "deny",
    "roaming_rules": []
  }
}'
```

Permitir Redes Específicas (Lista Blanca)

```
# Crear regla de AT&T
RULE1=$(curl -k -X POST
https://hss.example.com:8443/api/roaming/rule \
-H "Content-Type: application/json" \
-d '{
  "roaming_rule": {
    "name": "Allow AT&T",
    "mcc": "310",
    "mnc": "410",
    "data_action": "allow",
    "ims_action": "allow"
  }
}' | jq -r '.response.id')

# Crear regla de Verizon
RULE2=$(curl -k -X POST
https://hss.example.com:8443/api/roaming/rule \
-H "Content-Type: application/json" \
-d '{
  "roaming_rule": {
    "name": "Allow Verizon",
    "mcc": "311",
    "mnc": "480",
    "data_action": "allow",
    "ims_action": "allow"
  }
}' | jq -r '.response.id')

# Crear perfil con denegar por defecto y vincular reglas
curl -k -X POST https://hss.example.com:8443/api/roaming/profile \
-H "Content-Type: application/json" \
-d "{
  \"roaming_profile\": {
    \"name\": \"US Carriers Only\",
    \"data_action_if_no_rules_match\": \"deny\",
    \"ims_action_if_no_rules_match\": \"deny\",
    \"roaming_rules\": [$RULE1, $RULE2]
  }
}"
```


Permitir Datos, Bloquear Voz

```
# Crear regla que permite datos pero bloquea IMS
curl -k -X POST https://hss.example.com:8443/api/roaming/rule \
-H "Content-Type: application/json" \
-d '{
  "roaming_rule": {
    "name": "Data Only - T-Mobile",
    "mcc": "310",
    "mnc": "260",
    "data_action": "allow",
    "ims_action": "deny"
  }
}'
```

Bloquear Redes Específicas (Lista Negra)

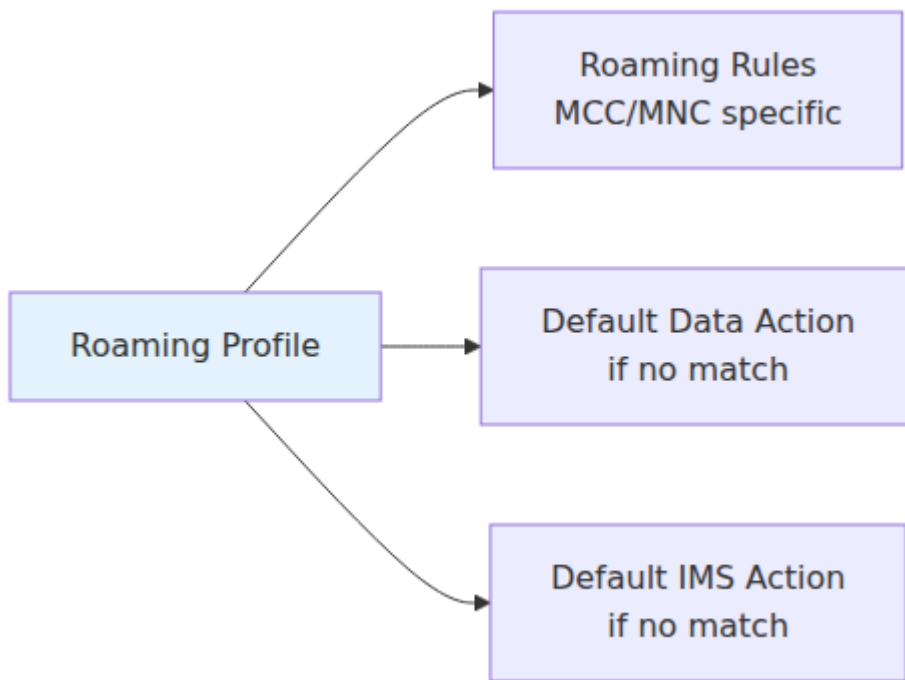
```
# Crear regla de bloqueo de red cara
RULE=$(curl -k -X POST
https://hss.example.com:8443/api/roaming/rule \
-H "Content-Type: application/json" \
-d '{
  "roaming_rule": {
    "name": "Block Expensive Network",
    "mcc": "206",
    "mnc": "01",
    "data_action": "deny",
    "ims_action": "deny"
  }
}' | jq -r '.response.id')

# Crear perfil con permitir por defecto
curl -k -X POST https://hss.example.com:8443/api/roaming/profile \
-H "Content-Type: application/json" \
-d "{
  \"roaming_profile\": {
    \"name\": \"Block Expensive Networks\",
    \"data_action_if_no_rules_match\": \"allow\",
    \"ims_action_if_no_rules_match\": \"allow\",
    \"roaming_rules\": [$RULE]
  }
}"
```

Escenarios Comunes de Roaming

Escenario 1: Solo Roaming Nacional

El suscriptor puede hacer roaming dentro del país de origen, pero no internacionalmente.

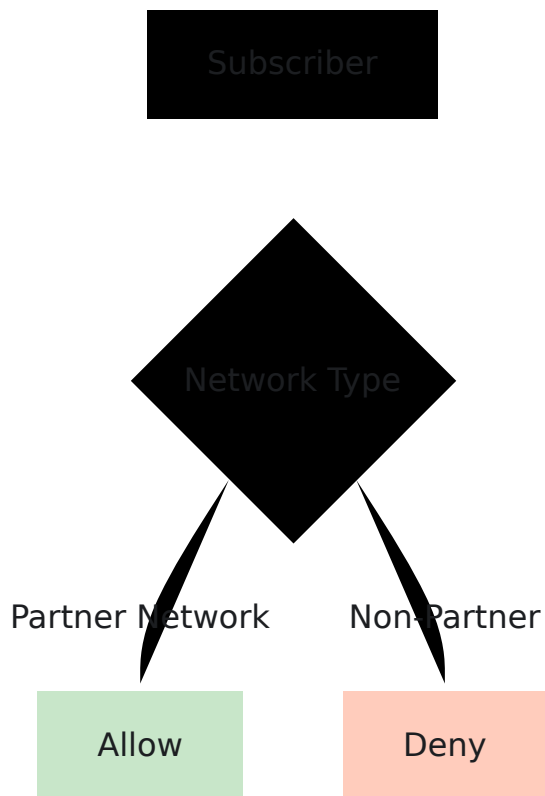


Configuración:

- Predeterminado: Denegar todo
- Reglas: Permitir todos los códigos MCC de EE. UU. (310, 311, 312, 313, 314, 315, 316)

Escenario 2: Solo Socios de Roaming

El suscriptor solo puede hacer roaming en redes con acuerdos comerciales.

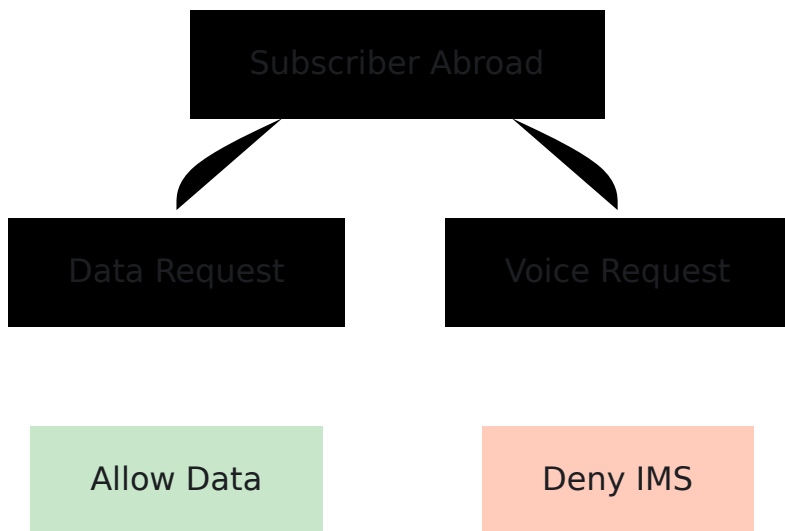


Configuración:

- Predeterminado: Denegar todo
- Reglas: Permitir cada red asociada explícitamente (por MCC/MNC)

Escenario 3: Roaming de Datos, Sin Roaming de Voz

El suscriptor puede usar datos en el extranjero, pero debe usar WiFi para llamadas de voz.



Configuración:

- Reglas: `data_action: "allow", ims_action: "deny"`

Escenario 4: Acceso a Servicios de Emergencia

Siempre permitir servicios de emergencia, incluso si el roaming está bloqueado.

Nota: El manejo de servicios de emergencia generalmente se realiza a nivel de MME/red. Las reglas de roaming de OmniHSS se aplican a servicios normales.

Referencia de MCC/MNC

Códigos de País Comunes (MCC)

MCC	País	Redes
310-316	EE. UU.	AT&T, Verizon, T-Mobile, etc.
302	Canadá	Rogers, Bell, Telus
234-235	Reino Unido	Vodafone, O2, EE
262	Alemania	Deutsche Telekom, Vodafone
208	Francia	Orange, SFR, Bouygues
222	Italia	TIM, Vodafone, Wind
214	España	Movistar, Vodafone

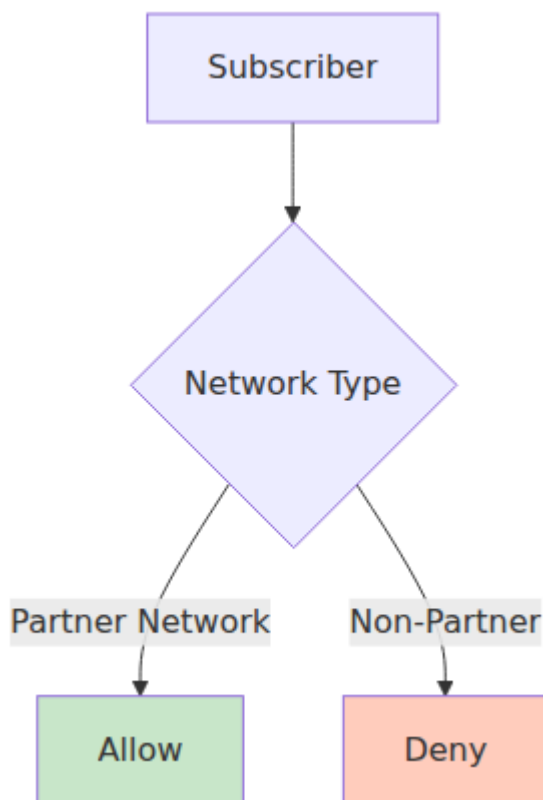
Operadores Comunes de EE. UU. (MCC 310-316)

MCC	MNC	Operador
310	410	AT&T
311	480	Verizon
310	260	T-Mobile
310	120	Sprint
313	380	(Ejemplo de red de prueba)

Puntos de Aplicación del Roaming

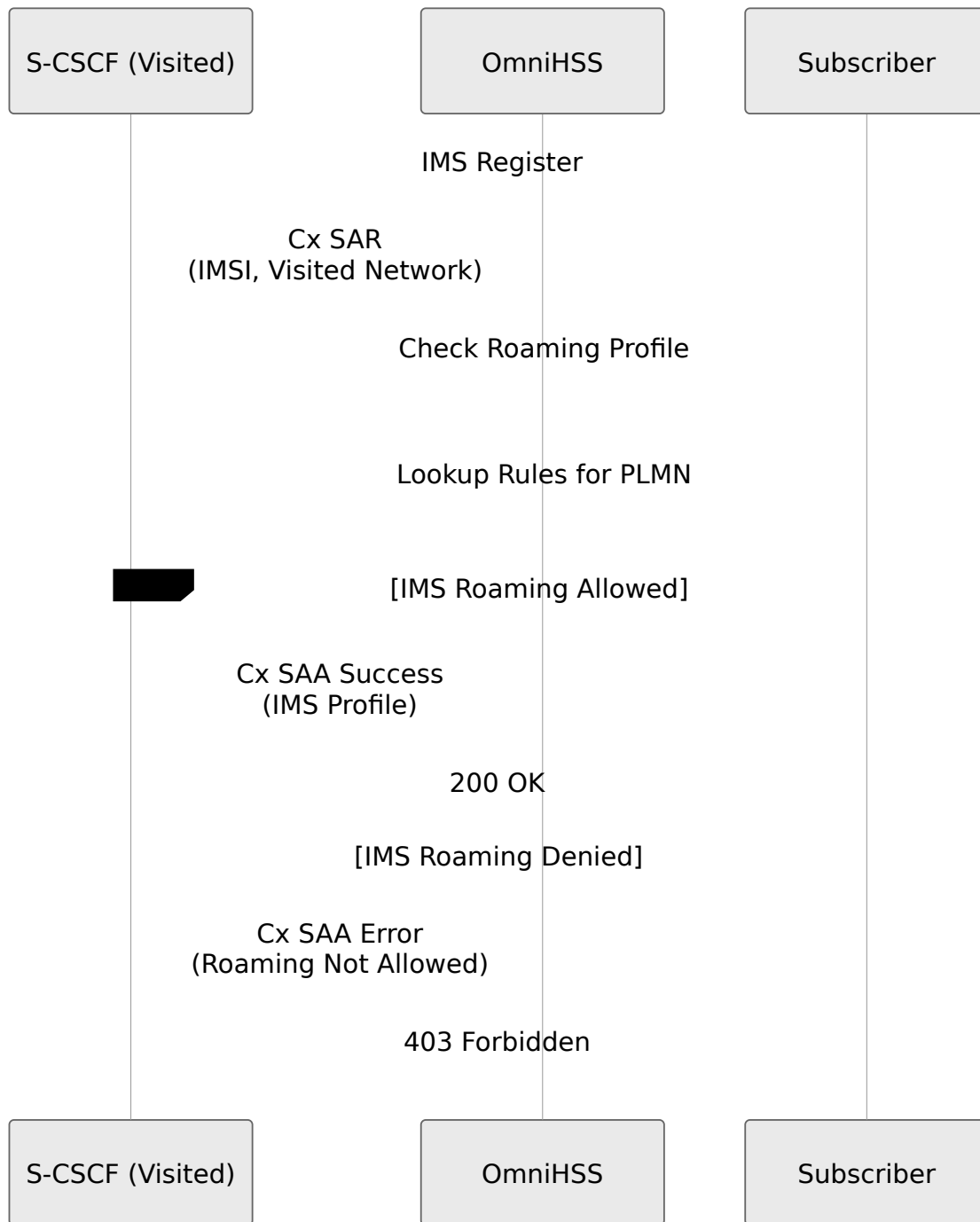
Interfaz S6a (Datos)

Cuando el suscriptor se conecta a la red visitada:



Interfaz Cx (IMS)

Cuando el suscriptor se registra en IMS en la red visitada:



Solución de Problemas de Roaming

El Suscriptor No Puede Conectarse en la Red Visitada

Verificar la asignación del perfil de roaming:

- Consultar la base de datos para ver el perfil de roaming asignado al suscriptor
- Verificar el nombre del perfil y la configuración de la acción predeterminada

Verificar si existe una regla para la red visitada:

- Consultar la base de datos para reglas de roaming que coincidan con el MCC/MNC de la red visitada
- Verificar si existe una regla para el perfil de roaming del suscriptor
- Comprobar el valor de `data_action` para esa red específica

El Suscriptor Puede Conectarse Pero No Registrarse en IMS

Verificar la acción de IMS por separado:

- Consultar las reglas de roaming para la red visitada
- Verificar los valores de `data_action` y `ims_action`
- Buscar casos donde se permiten datos pero se niega IMS

Comportamiento de Roaming Inesperado

Revisar los registros para verificaciones de roaming:

```
[info] Roaming check: IMSI 001001123456789, Visited PLMN 310-410  
[info] Roaming rule matched: "Allow AT&T"  
[info] Data action: allow, IMS action: allow
```

Mejores Prácticas

Diseño del Perfil

1. **Comenzar restrictivo** - Denegar por defecto, permitir explícitamente a los socios

2. **Probar a fondo** - Verificar reglas en laboratorio antes de producción
3. **Documentar reglas** - Mantener lista de redes permitidas y por qué
4. **Revisar regularmente** - Actualizar a medida que cambian los acuerdos de roaming

Gestión de Reglas

1. **Usar nombres descriptivos** - "Allow-ATT-Data-Only" no "Rule1"
2. **Verificar MCC/MNC** - Comprobar códigos contra bases de datos oficiales
3. **Considerar ambos servicios** - Pensar en datos e IMS por separado
4. **Monitorear uso** - Rastrear qué redes visitan realmente los suscriptores

Procedimientos Operativos

1. **Cambios de Emergencia** - Tener un procedimiento para habilitar/deshabilitar rápidamente el roaming
2. **Actualizaciones Masivas** - Planificar la actualización de los perfiles de roaming de múltiples suscriptores
3. **Informes** - Rastrear el uso de roaming y los intentos denegados
4. **Comunicación con el Cliente** - Notificar a los clientes sobre cambios en la política de roaming

[← Volver a la Guía de Operaciones](#) | [Siguiente: Flujos de Protocolo →](#)

Sh RepositoryData (Datos Transparentes)

OmniHSS actúa como un **repositorio transparente** para los datos de servicio que los Servidores de Aplicaciones (AS) almacenan contra un suscriptor a través de la **interfaz Sh**. Documentos como **MMTEL-Services** (servicios suplementarios / desvío de llamadas, espera de llamadas, OIP/OIR, restricción) y **IMS-ODB-Information** (restricción determinada por el operador) son escritos por el AS, mantenidos por el HSS y leídos a demanda.

"Transparente" tiene un significado preciso en **3GPP TS 29.328**: el HSS entiende estos datos **sintácticamente pero no semánticamente**. Es XML opaco propiedad del AS. OmniHSS almacena y devuelve la carga útil `ServiceData` **byte por byte**. Nunca vuelve a analizar ni a serializar la carga útil. Un documento que un AS etiqueta o suma de verificación (por ejemplo XCAP/MMTel) se devuelve exactamente como fue escrito.

Los mismos documentos también pueden ser gestionados fuera de banda por sistemas de aprovisionamiento/CRM a través de la **API de Aprovisionamiento REST**.

Tabla de Contenidos

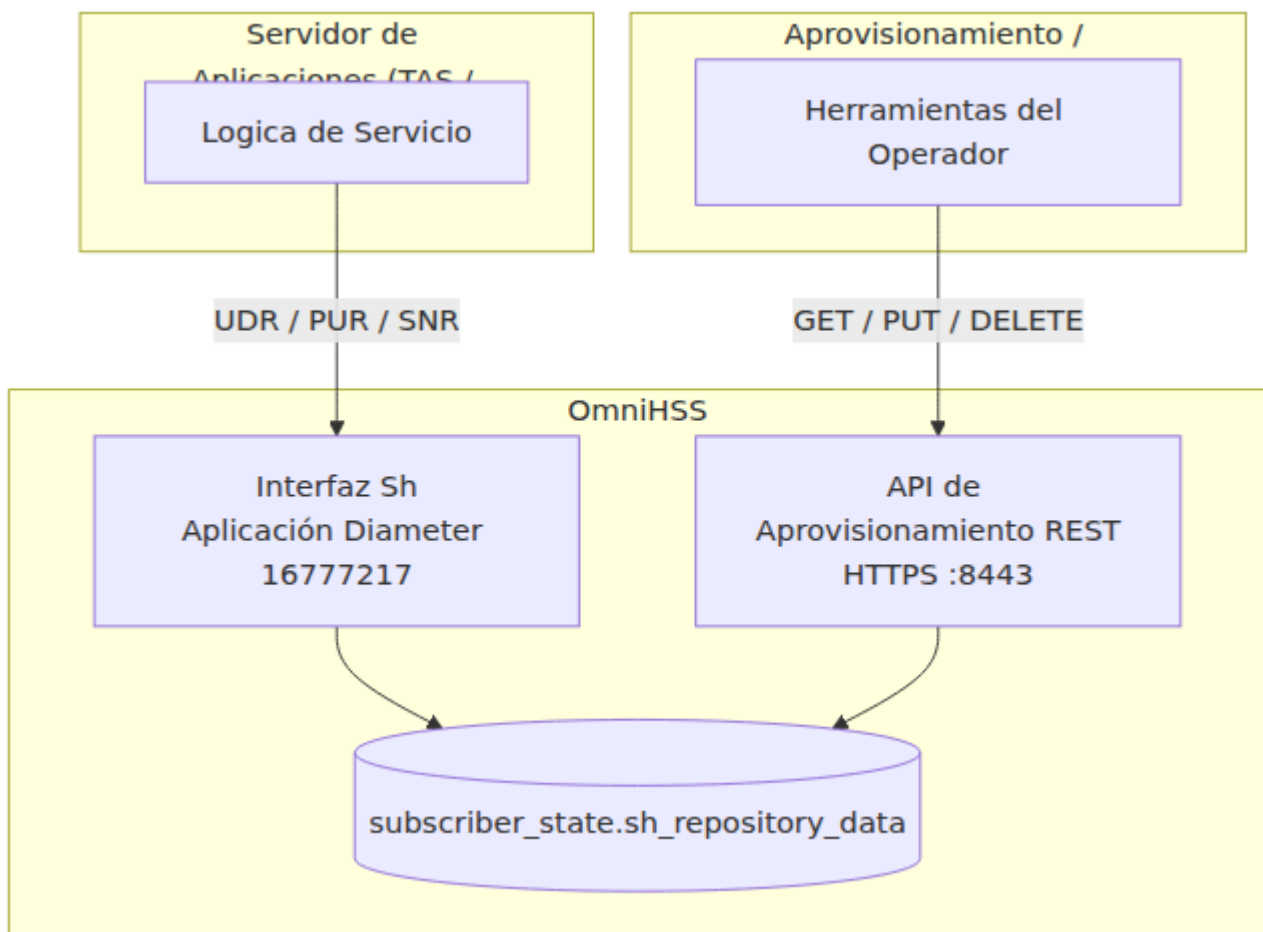
- **Conceptos**
- **Modelo de Datos**
- **Flujos de Mensajes Sh**
- **SequenceNumber y Concurrency**
- **API de Aprovisionamiento REST**
- **Tablas de Referencia**
- **Resolución de Problemas**

Conceptos

Un suscriptor puede tener cualquier número de **documentos transparentes** independientes, cada uno identificado por una **Service-Indication** (el "nombre del archivo"). Un documento tiene tres partes:

Elemento	Propietario	Significado
Service-Indication	Gestionado por HSS	Nombra el documento (por ejemplo, <code>MMTEL-Services</code> , <code>IMS-ODB-Information</code>).
SequenceNumber	Gestionado por HSS	Contador de versión utilizado para concurrencia optimista. Ver SequenceNumber y Concurrencia .
ServiceData	Propiedad del AS (opaco)	La carga útil XML en sí. Almacenada y devuelta textualmente.

El HSS solo interpreta Service-Indication y SequenceNumber. El cuerpo `ServiceData` se trata como bytes opacos.



Modelo de Datos

Todos los documentos transparentes de un suscriptor se mantienen en un solo campo, `subscriber_state.sh_repository_data`, como un objeto JSON indexado por Service-Indication. Cada entrada almacena la versión y la carga útil textual:

```
{
  "MMTEL-Services": { "sequence_number": "0", "service_data":
    "<MMTelServices ...>...</MMTelServices>" },
  "IMS-ODB-Information": { "sequence_number": "1", "service_data":
    "<OdbForImsOrientedServices xmlns=\"odb.mmtel.omnitou.ch\"/>" }
}
```

Campo	Descripción
sequence_number	La versión actual de este documento, según lo aceptado por última vez por el HSS. Devuelto en cada UDA y utilizado para validar actualizaciones.
service_data	El cuerpo XML opaco, almacenado exactamente como lo envió el AS (sin normalización de espacio de nombres, orden de atributos o espacios en blanco). Un documento sin elemento ServiceData (los <i>datos de repositorio vacíos</i> de la especificación) omite este campo.

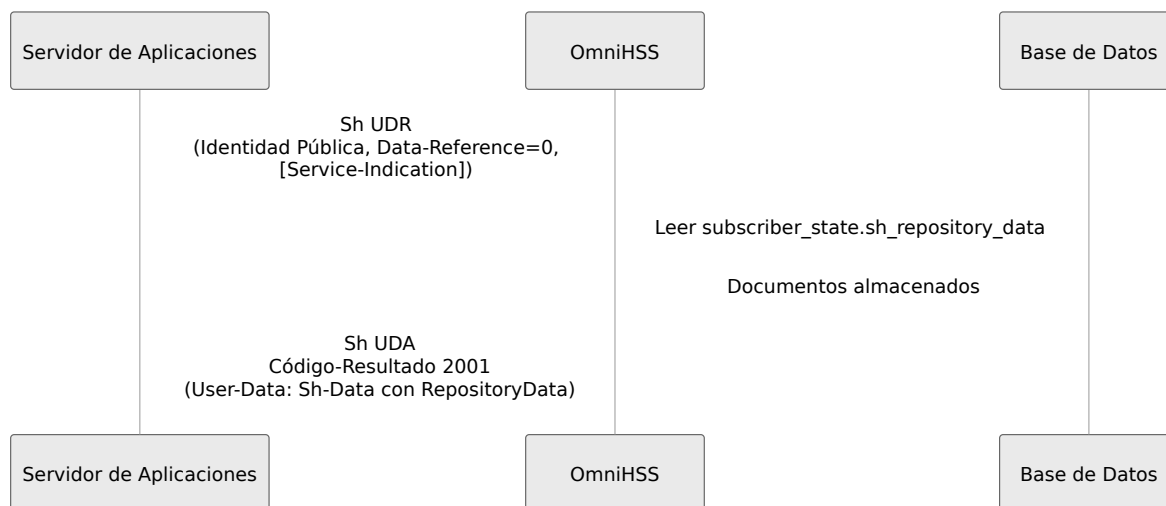
Este modelo significa que un solo suscriptor puede tener muchos documentos distintos, cada uno versionado de forma independiente, sin un esquema fijo impuesto por el HSS.

Flujos de Mensajes Sh

RepositoryData se transporta en el AVP User-Data como un documento XML Sh-Data. RepositoryData se selecciona con **valor Data-Reference 0**. Un AVP **Service-Indication** opcional restringe una solicitud a un solo documento.

Solicitud de Datos de Usuario (UDR/UDA): Leer

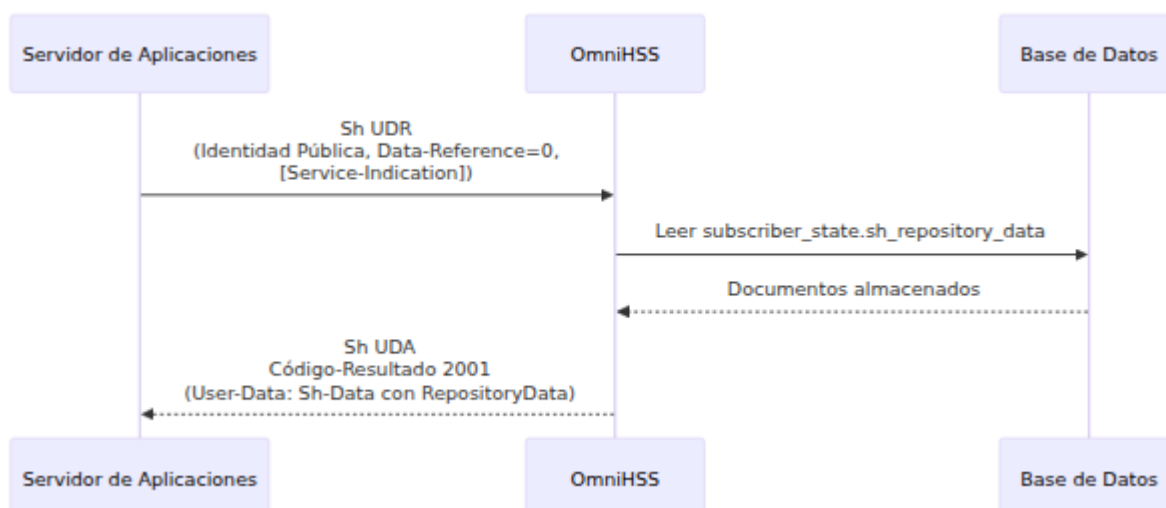
El AS lee uno o todos los documentos transparentes. Con un Service-Indication, solo se devuelve el documento correspondiente; sin uno, se devuelven todos los documentos almacenados, cada uno como su propio elemento <RepositoryData>.



Un suscriptor desconocido o no IMS recibe **Experimental-Result 5001 (DIAMETER_ERROR_USER_UNKNOWN)**.

Solicitud de Actualización de Perfil (PUR/PUA): Escribir

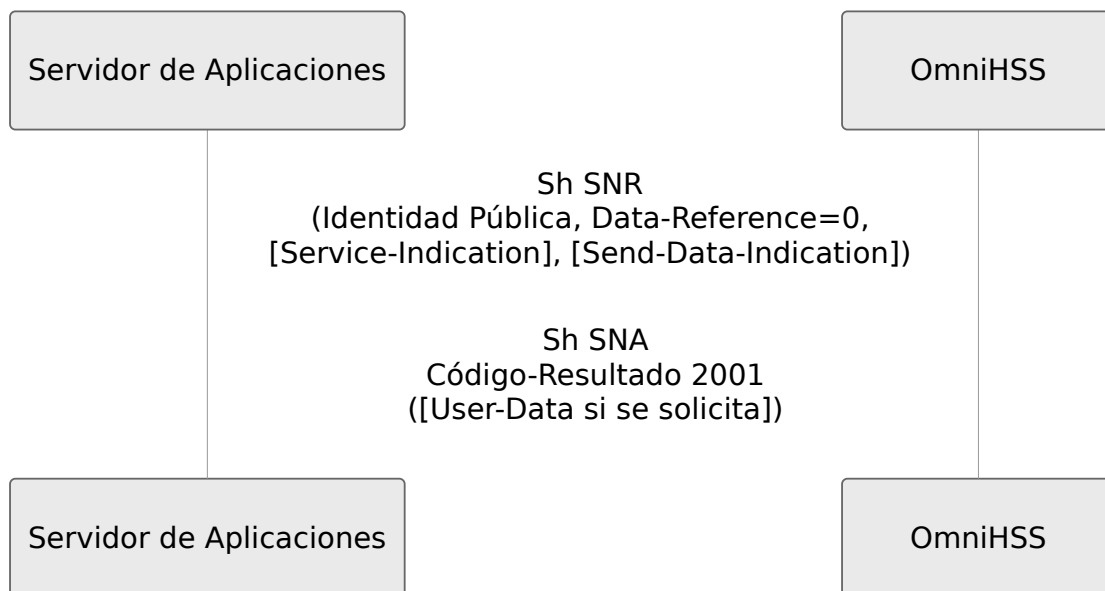
El AS crea o actualiza un solo documento. La carga útil `ServiceData` se almacena textualmente. La actualización se acepta solo si su SequenceNumber es válido (ver más abajo).



Cuando un PUR se resuelve a múltiples suscriptores (una Identidad Pública con comodín), la actualización se aplica de forma atómica: si algún documento está fuera de sincronización, ninguno se persiste.

Solicitud de Notificaciones de Suscripción (SNR/SNA): Suscribirse

El AS se suscribe a los datos de un suscriptor y puede solicitar que se devuelva el valor actual de inmediato (`Send-Data-Indication`). OmniHSS responde al SNR y, cuando se solicita, incluye el RepositoryData actual.



SequenceNumber y Concurrencia

El SequenceNumber proporciona control de concurrencia optimista para que dos Servidores de Aplicaciones no puedan sobrescribirse silenciosamente entre sí, según [3GPP TS 29.328](#).

- **Crear** un nuevo documento utiliza **SequenceNumber 0** (el valor `0` está reservado exclusivamente para datos recién añadidos).
- **Actualizar** un documento existente debe llevar el **sucesor inmediato** del SequenceNumber almacenado (almacenado + 1).
- El contador **envuelve de 65535 de vuelta a 1** (no a 0, ya que 0 está reservado).
- Una actualización cuyo SequenceNumber no es el sucesor esperado se rechaza con **Experimental-Result 5105 (DIAMETER_ERROR_TRANSPARENT_DATA_OUT_OF_SYNC)** y el documento almacenado queda sin cambios.



Ausente

PUR SequenceNumber
0 (crear)

Almacenado0

PUR SequenceNumber
1 (almacenado+1) ELIMINAR (REST)

Almacenado1

PUR SequenceNumber
n+1

AlmacenadoN

PUR con
SequenceNumber
incorrecto
→ 5105, sin cambio

Ejemplo: un documento se almacena en SequenceNumber 0. Un PUR con SequenceNumber 5 es rechazado con 5105 y nada cambia. Un PUR con SequenceNumber 1 es aceptado y el documento avanza a la versión 1.

API de Aprovisionamiento REST

Los mismos documentos pueden ser leídos y escritos directamente por sistemas de aprovisionamiento/CRM. El suscriptor se dirige por IMSI en la ruta;

el documento se identifica por `service_indication` (en el cuerpo de la solicitud para actualizaciones, o la cadena de consulta para lecturas/eliminaciones). El opaco `service_data` se envía byte por byte, exactamente como a través de Sh.

Todas las respuestas utilizan el sobre estándar de la API:

```
{ "status": "success", "response": { } }
```

A diferencia de la ruta Sh, la API REST es un acceso de aprovisionamiento autoritativo y **no** aplica la verificación de desincronización del `SequenceNumber`. Una escritura establece el documento directamente.

Listar Todos los Documentos

Devuelve todos los documentos almacenados para el suscriptor.

Endpoint: `GET /api/subscriber/repository_data/:imsi`

```
curl -k  
https://hss.example.com:8443/api/subscriber/repository_data/001001123
```

```
{  
  "status": "success",  
  "response": {  
    "MMTEL-Services": { "sequence_number": "0",  
    "service_data": "<MMTelServices .../>" },  
    "IMS-ODB-Information": { "sequence_number": "1",  
    "service_data": "<OdbForImsOrientedServices  
xmlns=\"odb.mmtel.omnitou.ch\"/>" }  
  }  
}
```

Obtener un Solo Documento

Devuelve un documento por Service-Indication.

Endpoint: GET /api/subscriber/repository_data/:imsi?
service_indication=:service_indication

```
curl -k  
"https://hss.example.com:8443/api/subscriber/repository_data/001001123  
service_indication=MMTEL-Services"
```

```
{  
  "status": "success",  
  "response": { "sequence_number": "0", "service_data": "  
<MMTelServices .../>" }  
}
```

Crear o Actualizar un Documento

Crea el documento si está ausente, o lo sobrescribe.

Endpoint: PUT /api/subscriber/repository_data/:imsi

```
curl -k -X PUT  
https://hss.example.com:8443/api/subscriber/repository_data/001001123  
\  
-H "Content-Type: application/json" \  
-d '{  
  "service_indication": "MMTEL-Services",  
  "service_data": "<MMTelServices version=\"1\"/>",  
  "sequence_number": "0"  
}'
```

Campo	Tipo	Requerido	Por Defecto	Descripción
<code>service_indication</code>	Cadena	Sí	-	El nombre del documento a crear/actualizar (por ejemplo, <code>MMTEL-Services</code>)
<code>service_data</code>	Cadena	No	-	La carga útil XML opaca, almacenada textualmente. Omitir para almacenar un documento vacío (solo Service-Indication y SequenceNumbe
<code>sequence_number</code>	Cadena	No	0	La versión a registrar para el documento.

La respuesta refleja el documento almacenado:

```
{
  "status": "success",
  "response": { "sequence_number": "0", "service_data": "
<MMTelServices version=\"1\"/>" }
}
```

Eliminar un Documento

Elimina un solo documento por Service-Indication.

Endpoint: `DELETE /api/subscriber/repository_data/:imsi`

```
curl -k -X DELETE
https://hss.example.com:8443/api/subscriber/repository_data/001001123
\
-H "Content-Type: application/json" \
-d '{ "service_indication": "MMTEL-Services" }'
```

Campo	Tipo	Requerido	Por Defecto	Descripción
<code>service_indication</code>	Cadena	Sí	-	El documento a eliminar.

La respuesta devuelve los documentos restantes para el suscriptor.

Tablas de Referencia

Valores de Data-Reference (RepositoryData)

Valor	Nombre	Descripción	Referencia
0	RepositoryData	Datos de servicio transparentes identificados por Service-Indication	3GPP TS 29.328 §7.6

Códigos de Resultado y Experimental-Result

Código	Nombre	Signif
2001	DIAMETER_SUCCESS	UDR/PUR, procesado éxito
5001	DIAMETER_ERROR_USER_UNKNOWN	Suscripto encontrado habilitado IMS
5105	DIAMETER_ERROR_TRANSPARENT_DATA_OUT_OF_SYNC	El Sequence de actual no es el s del valor almacena

ID de Aplicación

ID	Interfaz	Descripción	Referencia
16777217	Sh	AS ↔ HSS datos de usuario	3GPP TS 29.329

Indicaciones de Servicio Comunes

Service-Indication	Contenido Típico
MMTEL - Services	Servicios suplementarios MMTel (desvío de llamadas, espera/suspensión de comunicación, OIP/OIR, conferencias): XML simservs
IMS-ODB-Information	Información de restricción determinada por el operador para servicios orientados a IMS

Los valores de Service-Indication son definidos por el Servidor de Aplicaciones y su correspondiente esquema XML; el HSS no impone ninguna lista fija.

Resolución de Problemas

El Servidor de Aplicaciones recibe 5105 en la actualización

Síntomas: Un PUR es respondido con Experimental-Result 5105 y el documento no cambia.

Causas posibles:

- El AS envió un SequenceNumber que no es el sucesor inmediato del valor almacenado en el HSS (su copia en caché está obsoleta).
- Una actualización concurrente de otro AS avanzó el SequenceNumber.

Resolución:

1. Lee el documento actual con un UDR para obtener el SequenceNumber actualizado.
2. Re-emite el PUR con SequenceNumber = almacenado + 1.

3. Para forzar un valor administrativamente, configúralo a través de la **API REST**, que no aplica la verificación de concurrencia.

ServiceData devuelto difiere de lo que fue escrito

Síntomas: El AS cree que la carga útil fue alterada por el HSS.

Causas posibles:

- Esto no debería ocurrir. OmniHSS almacena y devuelve `ServiceData` byte por byte. Las diferencias aparentes generalmente provienen de la propia biblioteca XML del AS que re-serializa el documento (cambiando los prefijos de espacio de nombres, el orden de los atributos o los espacios en blanco) antes de la comparación.

Resolución:

1. Compara los bytes en bruto devueltos en la respuesta `UDA/REST` contra los bytes en bruto enviados, no una representación reanalizada.
2. Confirma que el AS no está normalizando el XML en su lado antes de la comparación.

Documento no encontrado a través de REST

Síntomas: `GET .../repository_data/:imsi?service_indication=...` devuelve un error.

Causas posibles:

- No hay documento con esa Service-Indication almacenado para el suscriptor.
- El IMSI no corresponde a un suscriptor existente.

Resolución:

1. Lista todos los documentos con `GET /api/subscriber/repository_data/:imsi` para ver qué está almacenado.

2. Verifica el IMSI con [Obtener Suscriptor por IMSI](#).

SRVCC - Continuidad de Llamadas de Voz de Radio Único

[← Volver a la Guía de Operaciones](#)

Descripción General

SRVCC (Continuidad de Llamadas de Voz de Radio Único) permite que un UE transfiera una llamada activa de VoLTE a un portador CS (Conmutado por Circuito) 2G/3G cuando falla la cobertura LTE. El MME orquesta la transferencia a través de la **interfaz Sv** ([TS 29.280](#)). Para construir la Solicitud Sv PS-a-CS, el MME necesita dos valores provenientes del HSS:

AVP	Código	Propósito
STN-SR	1433	Número de Transferencia de Sesión para SRVCC. El servidor MSC marca este número E.164 para alcanzar el TAS/S-CSCF, que ejecuta un SIP REFER para mover la sesión activa de VoLTE al portador CS.
C-MSISDN	1452	MSISDN de correlación. El TAS utiliza esto para emparejar la llamada entrante STN-SR con la sesión activa correcta cuando el suscriptor tiene múltiples llamadas en curso.

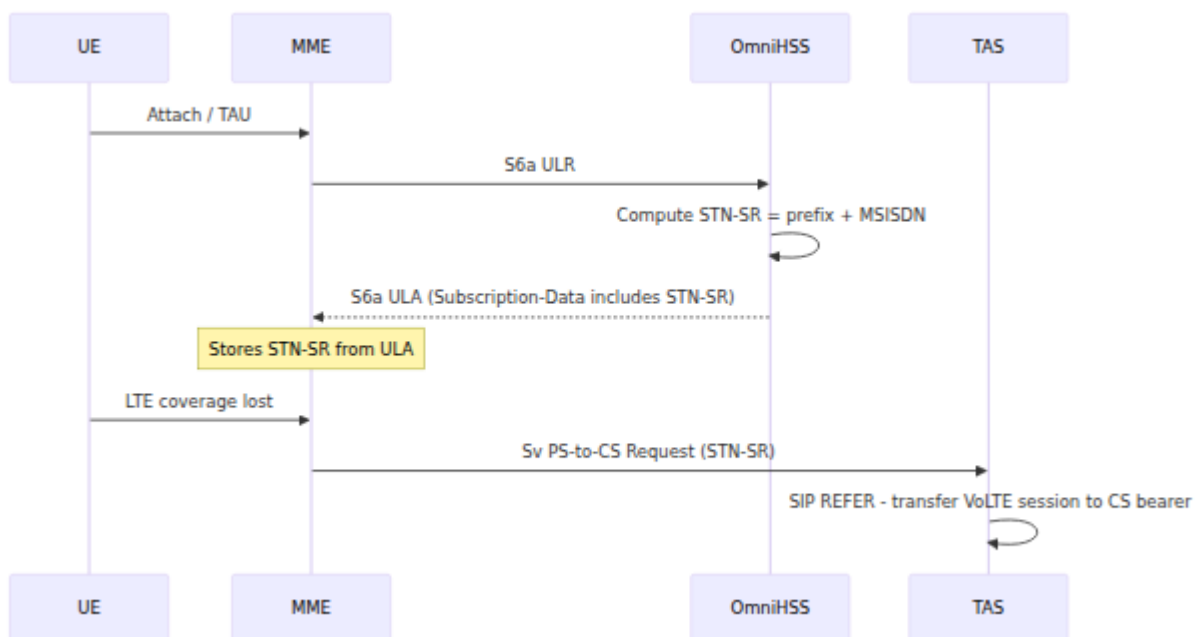
OmniHSS entrega **STN-SR** en la **Respuesta de Actualización de Ubicación** (ULA) S6a **Subscription-Data** AVP. El MME lo lee de la ULA y lo reenvía en la Solicitud Sv PS-a-CS.

Especificaciones de referencia:

Especificación	Título
TS 23.216	Procedimiento SRVCC PS-a-CS
TS 29.272	Interfaz S6a (STN-SR §7.3.89, Subscription-Data §7.3.2)
TS 23.003	Formato de número STN-SR (§13.4)

Cómo Funciona

OmniHSS utiliza un enfoque basado en prefijos. Se configura un único prefijo STN-SR a nivel de operador. El HSS calcula el número completo STN-SR en el momento de la ULA concatenando el prefijo con el MSISDN del suscriptor. El resultado se codifica en TBCD y se coloca en el AVP **STN-SR** dentro de **Subscription-Data**.



Este enfoque no requiere aprovisionamiento por suscriptor. Todos los suscriptores en el HSS reciben el mismo prefijo, por lo que un único cambio de configuración habilita SRVCC para toda la base de suscriptores.

Si el prefijo no está configurado, OmniHSS omite completamente el AVP **STN-SR**. La ULA no se ve afectada de otra manera. Las implementaciones no SRVCC

no ven cambios en el comportamiento.

Configuración

Agregue la clave `srvcc` a la configuración de la aplicación `:hss` en `config/runtime.exs`.

```
config :hss, :srvcc,  
  stn_sr_prefix: "9"
```

Parámetros

Parámetro	Tipo	Requerido	Predeterminado	Descripción
stn_sr_prefix	String	No	(ninguno)	Prefijo STN-SR asignado por el operador que se antepone al MSISDN de cada suscriptor para formar el número STN-SR E.164 completo. Cuando no se establece, OmniHSS omite el AVP STN-SR de todas las respuestas ULA.

Formato del Número STN-SR

El número completo STN-SR es:

STN-SR = stn_sr_prefix + subscriber MSISDN

El número se codifica como **TBCD** (Decimal Codificado en Binario de Telefonía, según TS 24.008 §10.5.4.7) y se coloca en el AVP STN-SR (código 1433, proveedor 10415).

Ejemplo:

Entrada	Valor
Prefijo configurado	9
MSISDN del suscriptor	61412345678
STN-SR calculado	961412345678

El servidor MSC marca 961412345678. La llamada llega al TAS, que utiliza la porción MSISDN para localizar la sesión IMS activa y emite el SIP REFER para transferirla al portador CS.

Ejemplo de Configuración

SRVCC Habilitado

```
# config/runtime.exs

config :hss, :srvcc,
  # Prefijo marcado por el servidor MSC para alcanzar el TAS a
  # través de PSTN/CS.
  # STN-SR = stn_sr_prefix + subscriber MSISDN.
  stn_sr_prefix: "9"
```

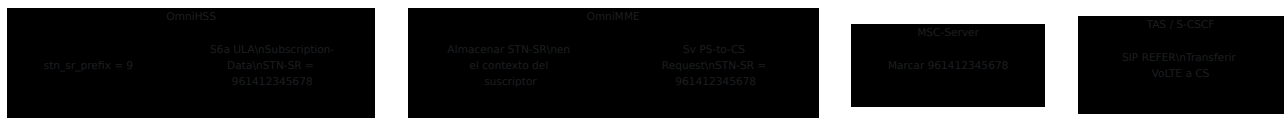
Cómo funciona: Cada respuesta ULA incluye STN-SR en Subscription-Data. El valor es la codificación TBCD del prefijo concatenado con el MSISDN del suscriptor. El MME almacena el valor y lo reenvía en las Solicitudes Sv PS-a-CS cuando se activa SRVCC.

SRVCC Deshabilitado (predeterminado)

Cuando la clave `srvcc` está ausente o `stn_sr_prefix` no está configurado, OmniHSS omite el AVP STN-SR. La ULA es idéntica de otro modo. Utilice esto para implementaciones que no requieren SRVCC.

Interacción con el MME

El MME (OmniMME) lee `STN-SR` de la ULA `Subscription-Data` y lo almacena en el contexto del suscriptor. Cuando se activa SRVCC, incluye `STN-SR` en la **Solicitud Sv PS-a-CS** enviada al servidor MSC. Consulte [Omnitouch/omnimme#426](#) para la implementación del MME.



Solución de Problemas

STN-SR No Presente en ULA

Síntomas: El MME no puede completar la Solicitud Sv PS-a-CS. Las transferencias SRVCC fallan.

Causas posibles:

- `stn_sr_prefix` no está configurado en `config/runtime.exs`.
- El servicio HSS se inició antes de que el cambio de configuración tuviera efecto.

Resolución:

1. Verifique que el bloque `srvcc` esté presente en `config/runtime.exs` con un `stn_sr_prefix` no vacío.
2. Reinicie el servicio OmniHSS para aplicar el cambio de configuración.
3. Active un nuevo ULR desde el MME (por ejemplo, forzando un TAU).
Confirme que los `Subscription-Data` de la ULA ahora contienen `STN-SR`.

Valor STN-SR Incorrecto

Síntomas: El servidor MSC recibe un número mal formado o no enrutable.

Causas posibles:

- El prefijo es incorrecto o falta dígitos iniciales.
- El MSISDN del suscriptor almacenado en el HSS no está en formato internacional E.164 (solo dígitos, sin +).

Resolución:

1. Verifique el MSISDN del suscriptor a través de la API (GET `/api/subscriber/imsi/:imsi`).
2. Verifique el STN-SR esperado: concatene `stn_sr_prefix` con el MSISDN almacenado.
3. Confirme que la tabla de enrutamiento del servidor MSC maneje ese rango de números.

[← Volver a la Guía de Operaciones](#)

Interfaz Sy (Control de Límite de Gastos)

Descripción General

La interfaz Sy conecta el HSS (actuando como el **PCRF**, Función de Reglas de Políticas y Cobranzas) a un **OCS** externo (Sistema de Cobranzas en Línea) para el **control de límite de gastos de suscriptores**. Permite que el PCRF base sus decisiones de política - por ejemplo, qué regla de cobro aplicar, o si debe limitar a un suscriptor - en el estado de los **contadores de políticas** que el OCS mantiene para cada suscriptor (cantidad de datos consumidos, gastos contra un límite mensual, y así sucesivamente).

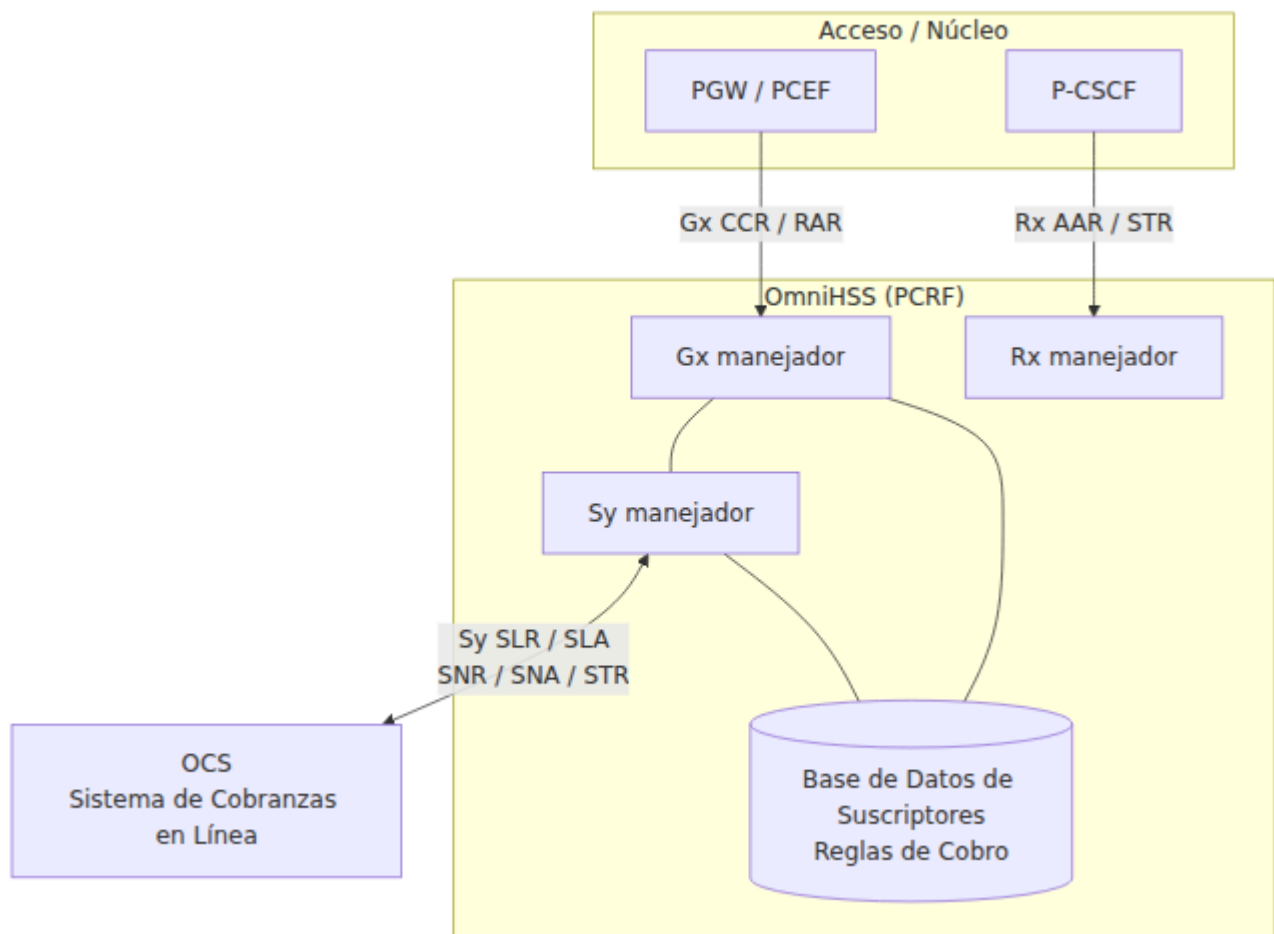
El PCRF de OmniHSS instala reglas de cobro y QoS a través de **Gx** y autoriza medios IMS a través de **Rx**. A través de Sy, se suscribe al estado de los contadores de políticas de un suscriptor en el OCS y es notificado cuando cambian, para que esas decisiones de Gx puedan tener en cuenta el gasto y la cuota actuales del suscriptor.

Sy está definido por **3GPP TS 29.219** y utiliza el ID de aplicación Diameter **16777302**.

Propiedad	Valor
ID de Aplicación	16777302
Especificación	3GPP TS 29.219
Rol del HSS	PCRF (cliente Diameter para SLR/STR, servidor para SNR)
Par	OCS (Sistema de Cobranzas en Línea)
Transporte	TCP o SCTP, puerto 3868

Sy vs Gy. Sy no es cobro en línea. Gy (TS 32.299) es donde el PGW pide al OCS que otorgue crédito para tráfico en vivo. Sy es una interfaz separada y ligera donde el **PCRF** se suscribe al **estado** de los contadores de políticas del OCS y es notificado cuando cambian, para que pueda ajustar la política. El OCS es el servidor en ambos.

Arquitectura



El HSS es el **cliente Sy**: abre una sesión Sy con el OCS cuando necesita por primera vez el estado de gastos de un suscriptor, y la cierra cuando finaliza la última sesión de datos del suscriptor. El OCS es el **servidor Sy**: responde a las solicitudes de estado y, cada vez que cambia el estado de un contador, notifica al PCRF para que pueda volver a aplicar la política a través de Gx.

Contadores de Políticas y Reglas de Cobro

El OCS mantiene uno o más **contadores de políticas** por suscriptor. Cada contador tiene:

- un **Identificador de Contador de Políticas** (AVP 2901) - un nombre estable para el contador, y
- un **Estado del Contador de Políticas** (AVP 2902) - una etiqueta que describe dónde se encuentra actualmente el contador (por ejemplo, `activo`, `sobre_cuota`, `limitado`). El conjunto de valores de estado no está definido por 3GPP; se configura conjuntamente por el operador tanto en el OCS como en el PCRF ([TS 29.219 §3.1](#)).

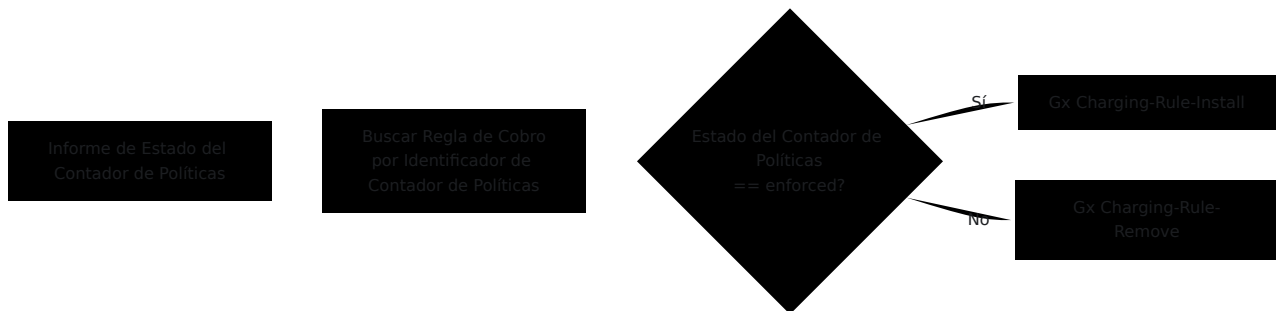
OmniHSS vincula estos a las **reglas de cobro** que ya están en su base de datos:

AVP Sy	Naturaleza	Mapea a	Rol
<code>Policy-Counter-Identifier</code> (2901)	Estático - nombra el contador	Un nombre de Regla de Cobro en la base de datos del HSS	Selecciona <i>qué</i> regla de cobro rige el contador
<code>Policy-Counter-Status</code> (2902)	Dinámico - cambia en umbrales	Una acción de aplicación	Decide <i>qué hacer</i> con esa regla ahora: instalar, eliminar o seleccionar un nivel

El identificador es estable durante la vida del contador, por lo que por sí solo no puede expresar "bajo cuota" frente a "sobre cuota". El **estado** es el valor que cambia cuando el suscriptor cruza un umbral, por lo que impulsa la acción:

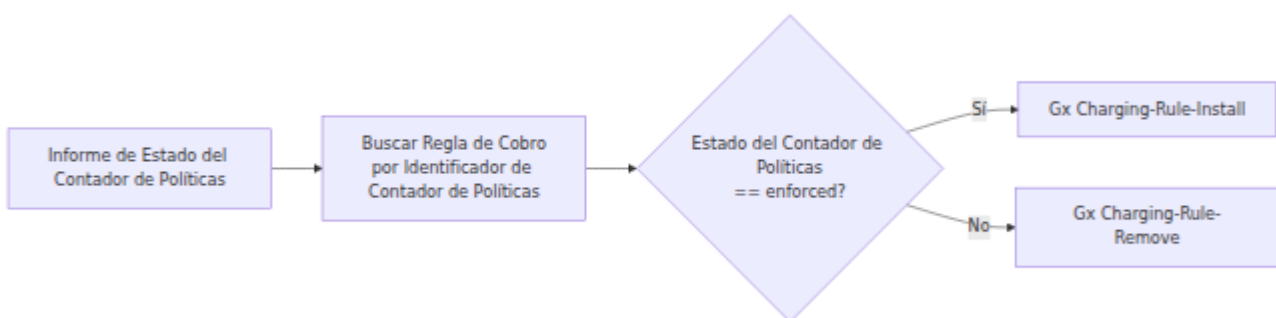
- el estado fijo **enforced** instala la regla de cobro nombrada (`Charging-Rule-Install` a través de Gx);
- cualquier otro estado la elimina (`Charging-Rule-Remove`).

Sy no lleva sus propias reglas de cobro. Sy no tiene AVPs de Regla de Cobro, QoS o Flujo; esos existen solo en Gx. Por lo tanto, el OCS no puede entregar al PCRF una definición de regla; solo puede *nombrar* la regla (a través del identificador del contador) y señalar *cuándo* aplicarla (a través del estado). La definición de la regla en sí se aprovisiona en el HSS. Esta es la razón por la que `Policy-Counter-Identifier` debe coincidir con un nombre de regla de cobro, y el OCS debe emitir esos nombres exactos con el estado `enforced` cuando la regla debe ser aplicada.



Ciclo de Vida de la Sesión Sy

Una sesión Sy es **por suscriptor**, no por portadora de datos. El PCRF mantiene una sesión Sy (identificada por un único `Session-Id` de Diameter) para un suscriptor mientras cualquiera de las sesiones de datos de ese suscriptor dependa del estado de gastos ([TS 29.219 §4.4.1](#)).



- **Establecer (SLR, SOLICITUD_INICIAL).** En el primer Gx CCR-I donde la política del suscriptor depende del estado de gastos, el PCRF abre la sesión Sy y solicita los contadores de políticas relevantes. El OCS responde con el estado actual de cada uno en el SLA.
- **Actualizar (SLR, SOLICITUD_INTERMEDIA).** Si el PCRF necesita más contadores más adelante, reutiliza la misma sesión Sy con una solicitud intermedia.

- **Notificar (SNR / SNA).** Cuando cambia el estado de un contador, el OCS envía una Solicitud de Notificación de Estado de Gastos. El PCRF reconoce con un SNA y aplica el cambio a través de Gx.
- **Terminar (STR / STA).** Cuando termina la última sesión de datos del suscriptor, el PCRF cierra la sesión Sy con una Solicitud de Terminación de Sesión.

Flujos de Mensajes

Flujo 1: Informe Inicial de Límite de Gastos en la Configuración del PDN

Parse error on line 14: .../eliminar por estado PCRF-->>PGW: Gx -----
 -----^ Expecting 'SOLID_OPEN_ARROW', 'DOTTED_OPEN_ARROW',
 'SOLID_ARROW', 'BIDIRECTIONAL_SOLID_ARROW', 'DOTTED_ARROW',
 'BIDIRECTIONAL_DOTTED_ARROW', 'SOLID_CROSS', 'DOTTED_CROSS',
 'SOLID_POINT', 'DOTTED_POINT', got 'NEWLINE'

Intente de nuevo

El PCRF incorpora las reglas derivadas del gasto en la **misma CCA-I** que ya construye para la sesión Gx. Si el OCS no responde a tiempo, el PCRF recurre a la política predeterminada del APN, de modo que una interrupción de Sy nunca bloquee el adjunto.

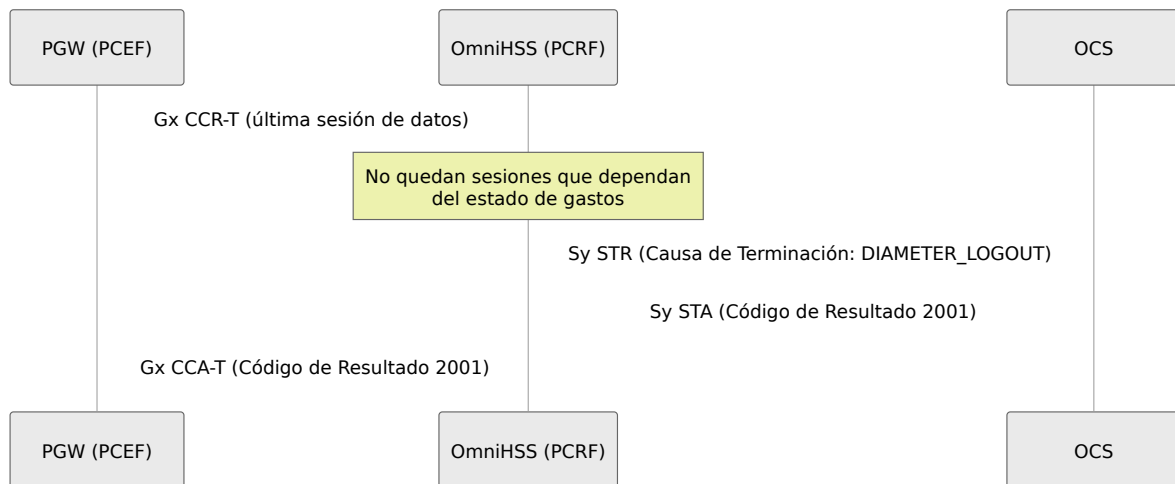
Flujo 2: Cambio de Estado de Gastos (OCS -> PCRF -> Gx RAR)

Parse error on line 11: ...o por identificador;
nuevo estado -> -----
 -----^ Expecting 'SPACE', 'NEWLINE', 'create', 'box', 'end', 'autonumber',
 'activate', 'deactivate', 'title', 'legacy_title', 'acc_title', 'acc_descr',
 'acc_descr_multiline_value', 'loop', 'rect', 'opt', 'alt', 'par', 'par_over', 'critical',
 'break', 'option', 'and', 'else', 'participant', 'participant_actor', 'destroy', 'note',
 'links', 'link', 'properties', 'details', 'ACTOR', got 'INVALID'

Intente de nuevo

Esto reutiliza la maquinaria existente de **Reautenticación Gx** del PCRF - el mismo camino que instala portadoras dedicadas de VoLTE - para impulsar el cambio de política impulsado por el gasto al PGW sin esperar el próximo CCR.

Flujo 3: Terminación de la Sesión Sy



Configuración

Aplicación Sy

La aplicación Sy está registrada en el servicio Diameter del HSS junto con Gx y Rx (`config/runtime.exs`):

```
%{
  application_name: :sy,
  application_dictionary: :diameter_gen_3gpp_sy,
  vendor_specific_application_ids: [
    %{vendor_id: 10415, auth_application_id: 16_777_302,
    acct_application_id: nil}
  ]
}
```

Parámetro	Tipo	Requerido	Predetermina
<code>application_name</code>	Átomo	Sí	-
<code>application_dictionary</code>	Átomo	Sí	-
<code>vendor_specific_application_ids</code>	Lista	Sí	-
<code>vendor_id</code>	Entero	Sí	-
<code>auth_application_id</code>	Entero	Sí	-
<code>acct_application_id</code>	Entero nil	No	<code>nil</code>

Configuración de Sy

El comportamiento de Sy se configura bajo la clave `:hss, :sy` (`config/runtime.exs`):

```
config :hss,
  sy: %{
    enabled: false
  }
```

Parámetro	Tipo	Requerido	Predeterminado	Descripción
<code>enabled</code>	Booleano	No	<code>false</code>	Interruptor maestro. Cuando es <code>true</code> , el PCRF abre una sesión por suscriptor en G CCR-I. Cuando es <code>false</code> , Sy se omite completamente.

El valor de `Policy-Counter-Status` que instala la regla de cobro nombrada es la convención fija `enforced`; cualquier otro valor elimina la regla. Esto se acuerda con el OCS y no es configurable.

Enrutamiento OCS

El HSS **no** fija un host o dominio OCS. Las SLR y STR originadas llevan el **propio** `Destination-Realm` del HSS y ningún `Destination-Host`, y se enrutan por dominio más el ID de Aplicación Sy (16777302). Cualquier par que publique la aplicación Sy en ese dominio recibe la solicitud - típicamente el **DRA**, que reenvía a un OCS disponible. Esto funciona de manera idéntica ya sea que el OCS se alcance a través del DRA o se conecte directamente, y permite que la capa de enrutamiento elija entre múltiples OCS.

El único requisito es que exista un par que publique la aplicación Sy en el dominio. En un despliegue de DRA, ese es el par DRA ya configurado para el HSS; no se necesita una entrada de par específica de Sy.

Mapeo de Contadores de Políticas

Para que la vinculación de identificador a regla funcione, el operador configura **ambos** extremos de manera consistente:

- En el **OCS**: el `Policy-Counter-Identifier` de cada contador de políticas se establece en el **nombre** exacto de una **Regla de Cobro** definida en el HSS, y el contador informa el estado `enforced` cuando esa regla debe ser aplicada.
- En el **HSS**: las reglas de cobro referenciadas existen en la base de datos.

Ver **Contadores de Políticas y Reglas de Cobro** para el modelo de mapeo.

Métricas

Sy expone métricas de Prometheus junto con las otras métricas de interfaz del HSS (ver **Métricas y Monitoreo**).

Métrica: `hss_sy_messages_total` **Tipo:** Contador **Descripción:** Mensajes Sy procesados, por comando, dirección y resultado. **Etiquetas:**

- `command` - `slr`, `sla`, `snr`, `sna`, `str`, o `sta`
- `direction` - `incoming` (recibido del OCS) o `outgoing` (enviado al OCS)
- `result` - `sent`, `received`, `success`, o `error`

Métrica: `hss_sy_policy_updates_total` **Tipo:** Contador **Descripción:** Cambios en las reglas de cobro Gx impulsados por el estado de un contador de políticas Sy, por acción y resultado. **Etiquetas:**

- `action` - `install` o `remove`
- `result` - `success` o `error` (el resultado del Gx RAR al PGW)

Consultas de ejemplo:

```
# Tasa de notificación Sy del OCS
rate(hss_sy_messages_total{command="snr", direction="incoming"}
[5m])

# Tasa de instalaciones de reglas de limitación/aplicación
impulsadas por límites de gastos
rate(hss_sy_policy_updates_total{action="install",
result="success"}[5m])

# Tasa de fallos de Sy Gx RAR
sum(rate(hss_sy_policy_updates_total{result="error"}[5m]))
/ sum(rate(hss_sy_policy_updates_total[5m]))
```

Documentación de Referencia

Comandos

Comando	Abreviatura	Código	Dirección	Propósito
Solicitud de Límite de Gastos	SLR	8388635	PCRF -> OCS	Solicitar estado del contador de políticas; suscribirse a cambios
Respuesta de Límite de Gastos	SLA	8388635	OCS -> PCRF	Devolver estado actual del contador
Solicitud de Notificación de Estado de Gastos	SNR	8388636	OCS -> PCRF	Notificar un cambio de estado de contador
Respuesta de Notificación de Estado de Gastos	SNA	8388636	PCRF -> OCS	Reconocer una notificación
Solicitud de Terminación de Sesión	STR	275	PCRF -> OCS	Cerrar la sesión Sy (informe final)
Respuesta de Terminación de Sesión	STA	275	OCS -> PCRF	Confirmar el cierre de la sesión

Todos los comandos llevan el ID de Aplicación **16777302**, incluyendo el STR/STA reutilizado (**RFC 6733** terminación de sesión).

AVPs Clave

AVP	Código	Tipo	Descripción
Policy-Counter-Identifier	2901	UTF8String	Nombra un contador de políticas. Vinculado a un nombre de Regla de Cobro en OmniHSS.
Policy-Counter-Status	2902	UTF8String	Etiqueta de estado definida por el operador para el contador. Impulsa la acción de aplicación.
Policy-Counter-Status-Report	2903	Agrupado	Identificador de un contador + estado (+ cualquier estado pendiente).
SL-Request-Type	2904	Enumerado	INITIAL_REQUEST (0) para la primera solicitud, INTERMEDIATE_REQUEST (1) en adelante.
Pending-Policy-Counter-Information	2905	Agrupado	Un estado futuro y el momento en que se vuelve actual.
Pending-Policy-Counter-Change-Time	2906	Tiempo	Cuándo entra en efecto un estado pendiente.
SN-Request-Type	2907	Unsigned32	Bitmask en un SNR. Bit 0 = informe normal, bit 1 = abortar (el OCS pide finalizar la sesión Sy).

AVP	Código	Tipo	Descripción
Subscription-Id	443	Agrupado	Identidad del suscriptor (IMSI y/o MSISDN) en el SLR.

Códigos de Resultado

Código	Nombre	Significado
2001	DIAMETER_SUCCESS	Solicitud procesada con éxito
5030	DIAMETER_USER_UNKNOWN	El OCS no conoce al suscriptor; sesión Sy n se crea
5570	DIAMETER_ERROR_UNKNOWN_POLICY_COUNTERS	Uno o más contadores de política solicitados son desconocidos para el OC
4241	DIAMETER_ERROR_NO_AVAILABLE_POLICY_COUNTERS	El OCS no tiene contadores de política para el suscriptor

Los códigos 5570 y 4241 son valores de Código de Resultado Experimental específicos de Sy ([TS 29.219 §5.5](#)); 5030 está definido por [RFC 4006](#).

Documentación Relacionada

- **PCRF** - Control de políticas Gx y Rx que Sy alimenta
- **Protocolos Diameter** - Flujos de mensajes a través de todas las interfaces del HSS
- **Arquitectura** - Arquitectura general del HSS

Guía de Solución de Problemas de OmniHSS

[← Volver a la Guía de Operaciones](#)

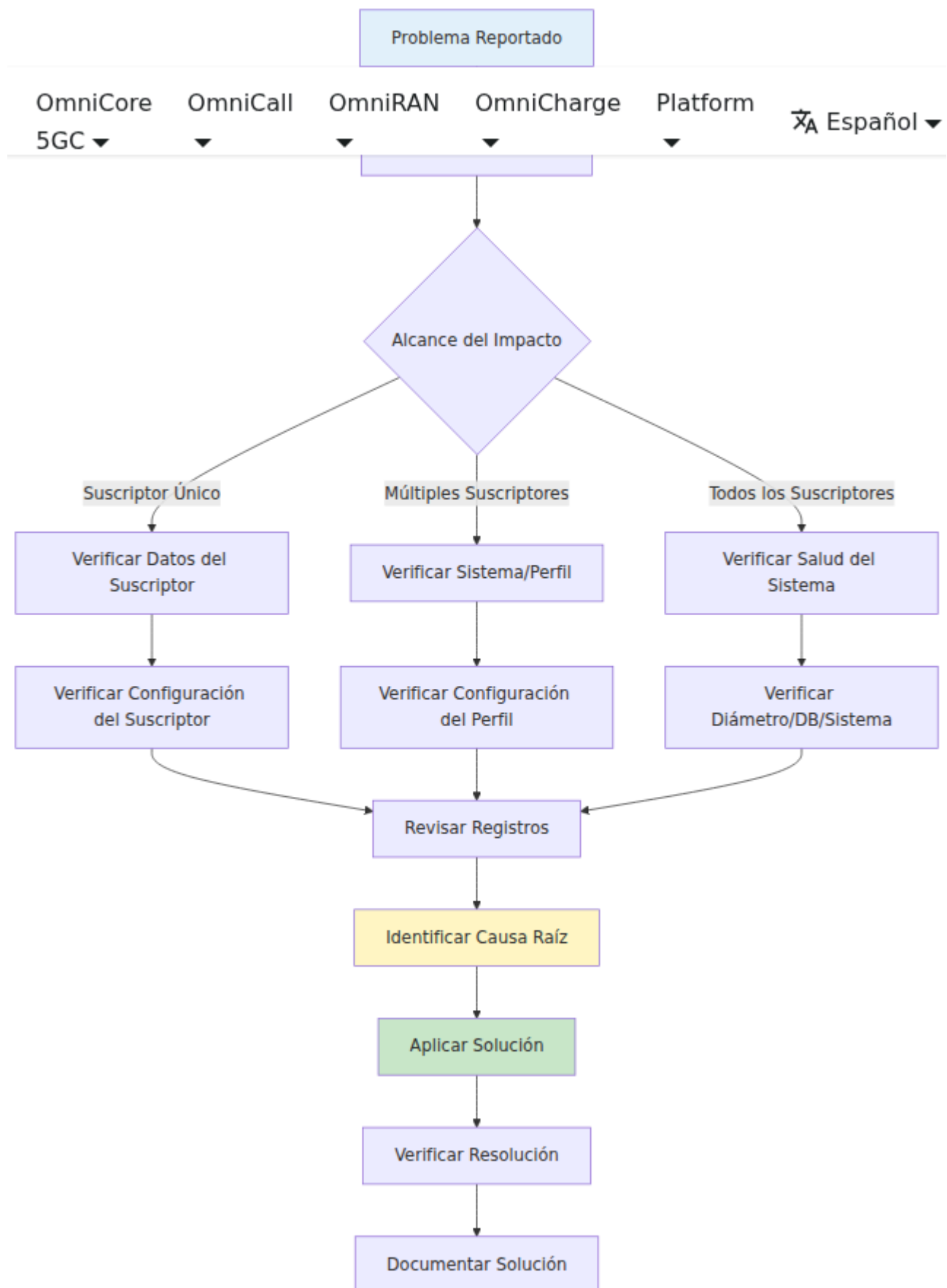
Tabla de Contenidos

- [Descripción General de la Solución de Problemas](#)
 - [Fallos de Autenticación](#)
 - [Problemas de Conectividad de Diámetro](#)
 - [Problemas de Base de Datos](#)
 - [Fallos de Registro EPC](#)
 - [Fallos de Registro IMS](#)
 - [Fallos de Llamadas VoLTE](#)
 - [Problemas de Roaming](#)
 - [Problemas de EIR](#)
 - [Problemas de Rendimiento](#)
 - [Problemas de Estado del Suscriptor](#)
 - [Problemas de API](#)
 - [Herramientas y Comandos de Diagnóstico](#)
-

Descripción General de la Solución de Problemas

Enfoque General para la Solución de

Problemas



Información a Recopilar

Antes de solucionar cualquier problema, recopile:

1. Información del Suscriptor (si es específico del suscriptor)

- IMSI
- MSISDN (número de teléfono)
- Último estado conocido
- Mensajes de error del dispositivo

2. Información de Tiempo

- ¿Cuándo comenzó el problema?
- ¿Es intermitente o constante?
- Hora de la última operación exitosa

3. Alcance del Impacto

- ¿Suscriptor único o múltiple?
- ¿Red específica o todas las redes?
- ¿Servicio específico (datos/voz) o ambos?

4. Estado del Sistema

- Verificar **Panel de Control** para el estado del sistema
 - Revisar el estado del par de Diámetro
 - Verificar conectividad de la base de datos
-

Fallos de Autenticación

Síntomas

- El suscriptor no puede adjuntarse a la red
- Errores de "autenticación rechazada"
- Intentos de autenticación repetidos

Causas Comunes y Soluciones

Causa 1: Conjunto de Claves Incorrecto

Síntomas:

- Fallo de autenticación constante para un suscriptor específico
- Funciona para otros suscriptores con el mismo perfil

Pasos de Diagnóstico:

1. Consultar al suscriptor para verificar key_set_id:

```
curl -k https://hss.example.com:8443/api/subscriber/imsi/[IMSI]
```

2. Verificar que el conjunto de claves exista y tenga los valores correctos:

```
curl -k https://hss.example.com:8443/api/key_set/[KEY_SET_ID]
```

3. Comparar los valores de Ki y OPC con la documentación de la tarjeta SIM

Solución:

- Actualizar el suscriptor con el **conjunto de claves** correcto
- Si las claves son correctas, la tarjeta SIM puede estar defectuosa

Causa 2: SQN Fuera de Sincronización

Síntomas:

- La autenticación falla después de funcionar previamente
- Error: "Fallo de sincronización de SQN"
- Funciona de manera intermitente

Pasos de Diagnóstico:

1. Verificar el estado del suscriptor para el valor de SQN en la base de datos
2. Buscar errores relacionados con SQN en los registros

3. Verificar el valor de SQN del conjunto de claves del suscriptor

Solución:

- SQN se volverá a sincronizar automáticamente después de que el suscriptor envíe AUTS
- Si persiste, restablecer SQN a 0 en el conjunto de claves (requiere que el suscriptor se vuelva a adjuntar)

Advertencia: Restablecer SQN puede causar problemas de seguridad. Hacerlo solo durante el mantenimiento.

Causa 3: Suscriptor Deshabilitado

Síntomas:

- Autenticación rechazada de inmediato
- No se generan vectores de autenticación

Pasos de Diagnóstico:

1. Verificar el estado habilitado del suscriptor:

```
curl -k https://hss.example.com:8443/api/subscriber/imsi/[IMSI]
```

2. Verificar que el campo `enabled` sea `true`

Solución:

- **Habilitar suscriptor:**

```
curl -k -X PUT https://hss.example.com:8443/api/subscriber/[ID] \
-H "Content-Type: application/json" \
-d '{"subscriber": {"enabled": true}}'
```

Causa 4: Perfil EPC Falta

Síntomas:

- La búsqueda del suscriptor tiene éxito pero la autenticación falla
- Error: "No se asignó perfil EPC"

Pasos de Diagnóstico:

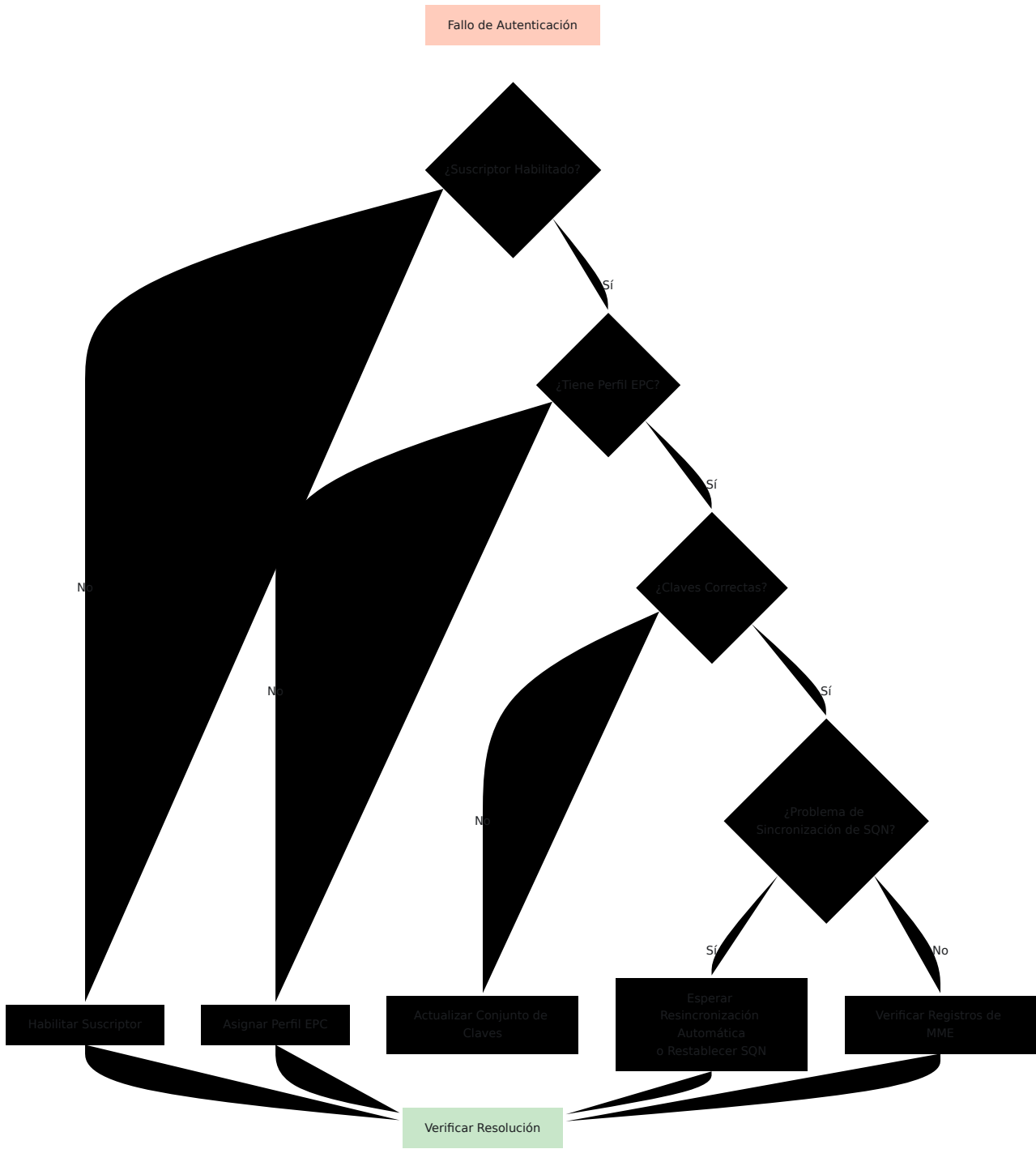
1. Verificar el campo `epc_profile_id` del suscriptor
2. Verificar que el perfil EPC exista:

```
curl -k  
https://hss.example.com:8443/api/epc/profile/[PROFILE_ID]
```

Solución:

- Asignar un **perfil EPC** válido al suscriptor

Diagrama de Flujo de Solución de Problemas de Autenticación



Problemas de Conectividad de Diámetro

Síntomas

- Los pares de Diámetro aparecen como desconectados en el [Panel de Control](#)
- Errores de "Sin ruta al host"
- Servicios fallando para todos los suscriptores

Causas Comunes y Soluciones

Causa 1: Conectividad de Red

Síntomas:

- El par nunca se conecta
- Errores de tiempo de espera de conexión
- Ping falla al par

Pasos de Diagnóstico:

1. Verificar conectividad de red desde OmniHSS al par:

```
ping [PEER_IP]
```

2. Verificar si el puerto de Diámetro es accesible:

```
telnet [PEER_IP] 3868
```

3. Verificar que las reglas del firewall permitan tráfico de Diámetro (puerto 3868)

Solución:

- Corregir el enrutamiento de red

- Actualizar reglas del firewall
- Verificar que el par esté en ejecución y escuchando

Causa 2: Configuración Incorrecta de Diámetro

Síntomas:

- Los intentos de conexión fallan
- El intercambio CER/CEA falla
- El par rechaza la conexión

Pasos de Diagnóstico:

1. Revisar la configuración de Diámetro en runtime.exs:
 - Verificar que el origin_host del par coincida con el valor esperado del par
 - Verificar la configuración del origin_realm
 - Verificar que la dirección IP del par sea correcta
2. Revisar los registros en busca de errores CER/CEA
3. Verificar que la configuración del par espere el origin_host de OmniHSS

Solución:

- Actualizar runtime.exs con la **configuración de Diámetro correcta**
- Reiniciar OmniHSS después del cambio de configuración
- Coordinar con el administrador del par para verificar la configuración

Causa 3: Problemas de Certificado (TLS Diámetro)

Síntomas:

- La conexión falla durante el apretón de manos TLS
- Errores de validación de certificado
- Errores de "Certificado expirado" o "Certificado inválido"

Pasos de Diagnóstico:

1. Verificar que los archivos de certificado existan en `priv/cert/`
2. Verificar la expiración del certificado:

```
openssl x509 -in priv/cert/diameter.crt -noout -dates
```

3. Verificar que la cadena de certificados esté completa
4. Verificar el certificado del par si se utiliza TLS mutuo

Solución:

- Renovar certificados expirados
- Instalar la cadena de certificados correcta
- Actualizar los archivos de certificados y reiniciar OmniHSS

Causa 4: Desajuste de Soporte de Aplicaciones del Par

Síntomas:

- El par se conecta pero no soporta las aplicaciones requeridas
- El intercambio de capacidades tiene éxito pero las operaciones fallan
- Errores de "Aplicación no soportada"

Pasos de Diagnóstico:

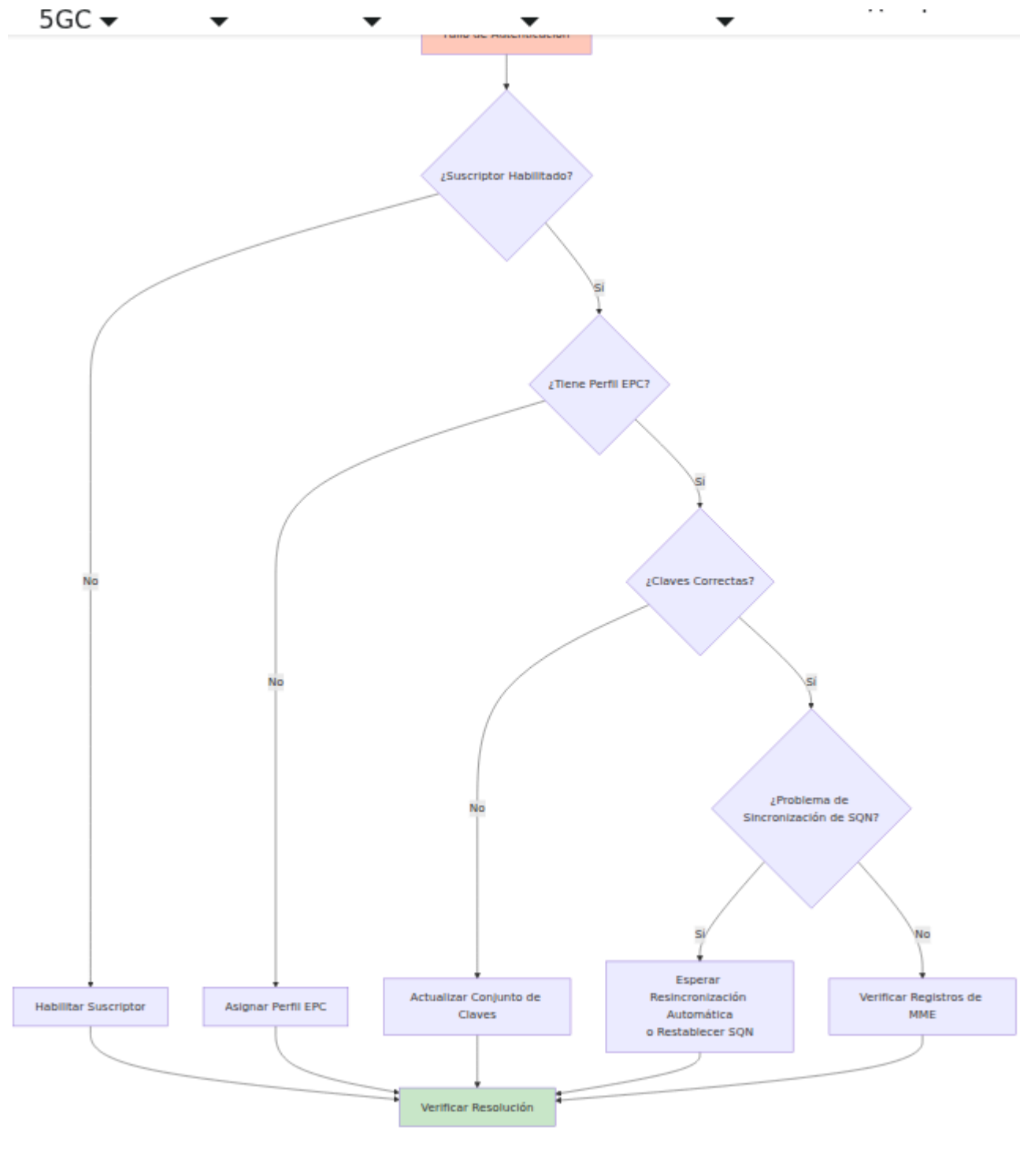
1. Verificar la [página de Diámetro del Panel de Control](#) para las aplicaciones del par
2. Verificar que el par soporte la aplicación requerida (S6a, Cx, Sh, etc.)
3. Revisar el intercambio CER/CEA en los registros

Solución:

- Verificar que la configuración del par incluya las aplicaciones de Diámetro requeridas
- Verificar que el tipo de par coincida con la funcionalidad esperada:
 - MME debe soportar S6a (16777251)
 - S-CSCF debe soportar Cx (16777216)

- P-GW debe soportar Gx (16777238)

Diagrama de Flujo de Solución de Problemas de Diámetro



Problemas de Base de Datos

Síntomas

- La API devuelve errores 500
- El Panel de Control no se carga
- Errores de "Conexión a la base de datos fallida"
- Rendimiento de consultas lento

Causas Comunes y Soluciones

Causa 1: Servidor de Base de Datos Caído

Síntomas:

- Todas las llamadas a la API fallan
- El Panel de Control muestra un error
- Errores de "Conexión rechazada"

Pasos de Diagnóstico:

1. Probar la conectividad de la base de datos:

```
# Conectar a la base de datos  
psql -h [DB_HOST] -U [DB_USER] -d [DB_NAME]
```

2. Verificar el estado del servicio de base de datos en el servidor de base de datos
3. Verificar la conectividad de red al servidor de base de datos

Solución:

- Iniciar el servicio de base de datos
- Corregir problemas del servidor de base de datos
- Verificar el enrutamiento de red al servidor de base de datos

Causa 2: Credenciales de Base de Datos Incorrectas

Síntomas:

- Errores de "Autenticación fallida"
- OmniHSS no puede conectarse al iniciar

Pasos de Diagnóstico:

1. Revisar la configuración de la base de datos en runtime.exs
2. Probar las credenciales manualmente con el cliente de base de datos
3. Verificar los permisos del usuario de la base de datos

Solución:

- Actualizar la **configuración de la base de datos** en runtime.exs
- Otorgar los permisos correctos al usuario de la base de datos
- Reiniciar OmniHSS después del cambio de configuración

Causa 3: Pool de Conexiones Agotado

Síntomas:

- Errores 500 intermitentes
- Errores de "Sin conexiones disponibles"
- Períodos de alta carga provocan fallos

Pasos de Diagnóstico:

1. Verificar el conteo actual de conexiones en la base de datos
2. Revisar el tamaño del pool de la base de datos en runtime.exs
3. Monitorear el uso de conexiones durante la carga máxima

Solución:

- Aumentar el tamaño del pool en la configuración de runtime.exs
- Investigar fugas de conexiones si el pool se agota repetidamente
- Considerar la escalabilidad de la base de datos si la carga es consistentemente alta

Causa 4: Consultas Lentas

Síntomas:

- Respuestas de API muy lentas
- Tiempos de espera en búsquedas de suscriptores
- Alta CPU en la base de datos

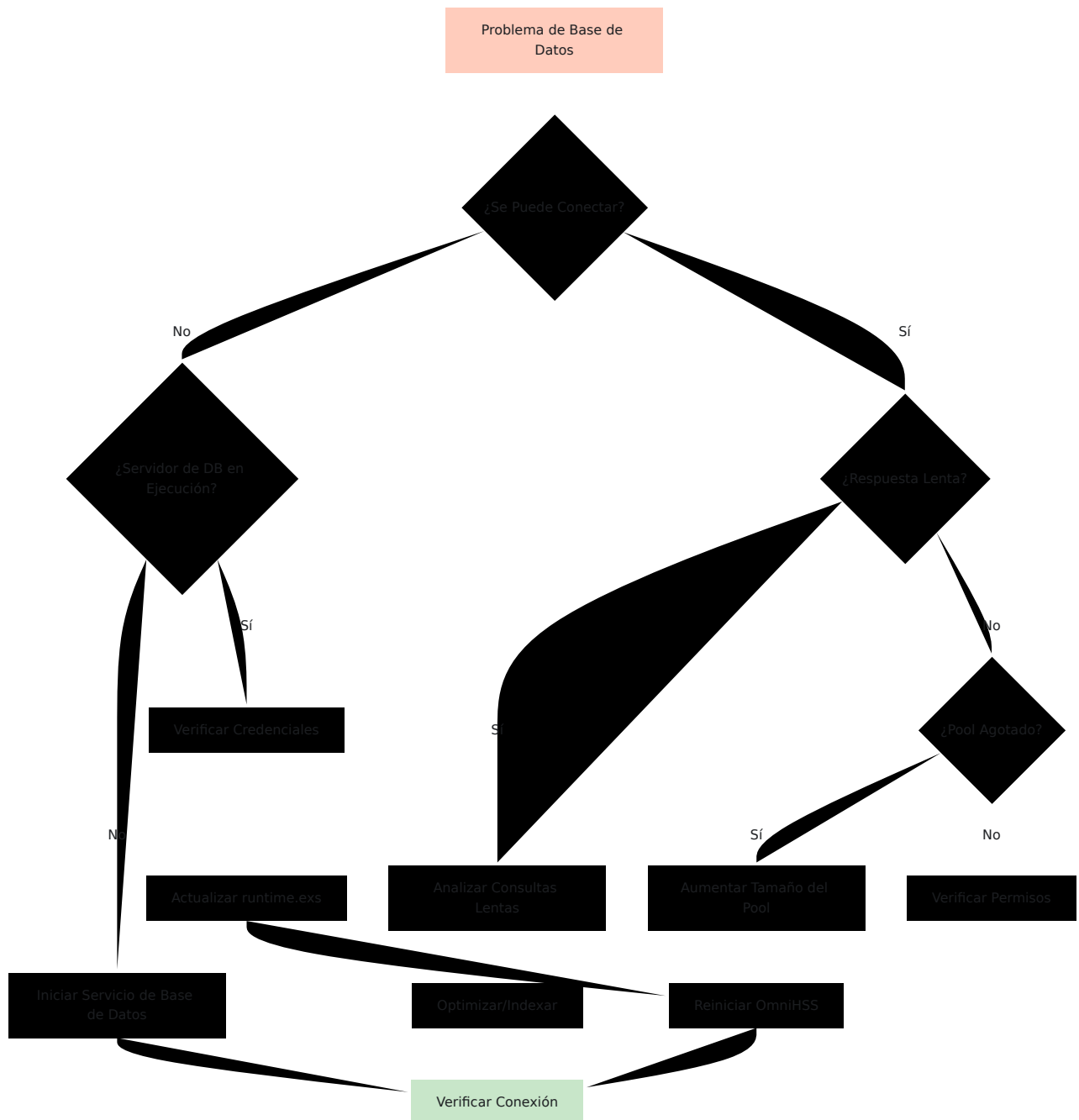
Pasos de Diagnóstico:

1. Consultar la base de datos para el registro de consultas lentas
2. Identificar consultas específicas lentas
3. Verificar si faltan índices
4. Verificar el conteo de suscriptores y tamaños de tablas

Solución:

- Optimizar consultas lentas
- Agregar índices faltantes
- Considerar la optimización del rendimiento de la base de datos
- Planificar la escalabilidad de la base de datos si es necesario

Diagrama de Flujo de Solución de Problemas de Base de Datos



Fallos de Registro EPC

Síntomas

- El suscriptor no puede adjuntarse a la red LTE

- MME rechaza la adjunción
- No se establece sesión PDN

Causas Comunes y Soluciones

Causa 1: Roaming Denegado

Síntomas:

- El suscriptor funciona en la red local pero falla al hacer roaming
- Errores de "roaming no permitido"
- Funciona para algunas redes pero no para otras

Pasos de Diagnóstico:

1. Verificar el campo roaming_profile_id del suscriptor
2. Consultar el perfil de roaming y las reglas
3. Verificar MCC/MNC de la red visitada
4. Verificar si existe una regla de roaming para esa red

Solución:

- Agregar una **regla de roaming** para el MCC/MNC de la red visitada
- O actualizar la acción predeterminada del perfil de roaming para permitir
- Ver **Documentación de Roaming** para la configuración

Causa 2: Configuración APN Faltante

Síntomas:

- La adjunción tiene éxito pero la sesión PDN falla
- Errores de "APN desconocido" del MME
- El suscriptor no puede obtener conexión de datos

Pasos de Diagnóstico:

1. Verificar que el perfil EPC tenga perfiles APN vinculados
2. Verificar que el identificador APN coincida con lo que solicita el dispositivo

3. Consultar la configuración del perfil APN

Solución:

- Vincular **perfiles APN** al perfil EPC del suscriptor
- Asegurarse de que el nombre APN coincida con la configuración del dispositivo
- Verificar que exista el perfil de QoS del APN

Causa 3: MME No Conectado

Síntomas:

- Todos los suscriptores fallan al adjuntarse
- No hay comunicación con el MME
- Par de Diámetro caído

Pasos de Diagnóstico:

1. Verificar la **página de Diámetro del Panel de Control**
2. Verificar que el estado del par MME sea "Conectado"
3. Verificar que el MME soporte la aplicación S6a

Solución:

- Solucionar **conectividad de Diámetro**
- Verificar la configuración del MME
- Contactar al administrador del MME

Causa 4: Corrupción del Estado del Suscriptor

Síntomas:

- El suscriptor aparece como adjunto pero no puede volver a adjuntarse
- El estado no coincide con la realidad
- La desvinculación y el re-adjunción fallan

Pasos de Diagnóstico:

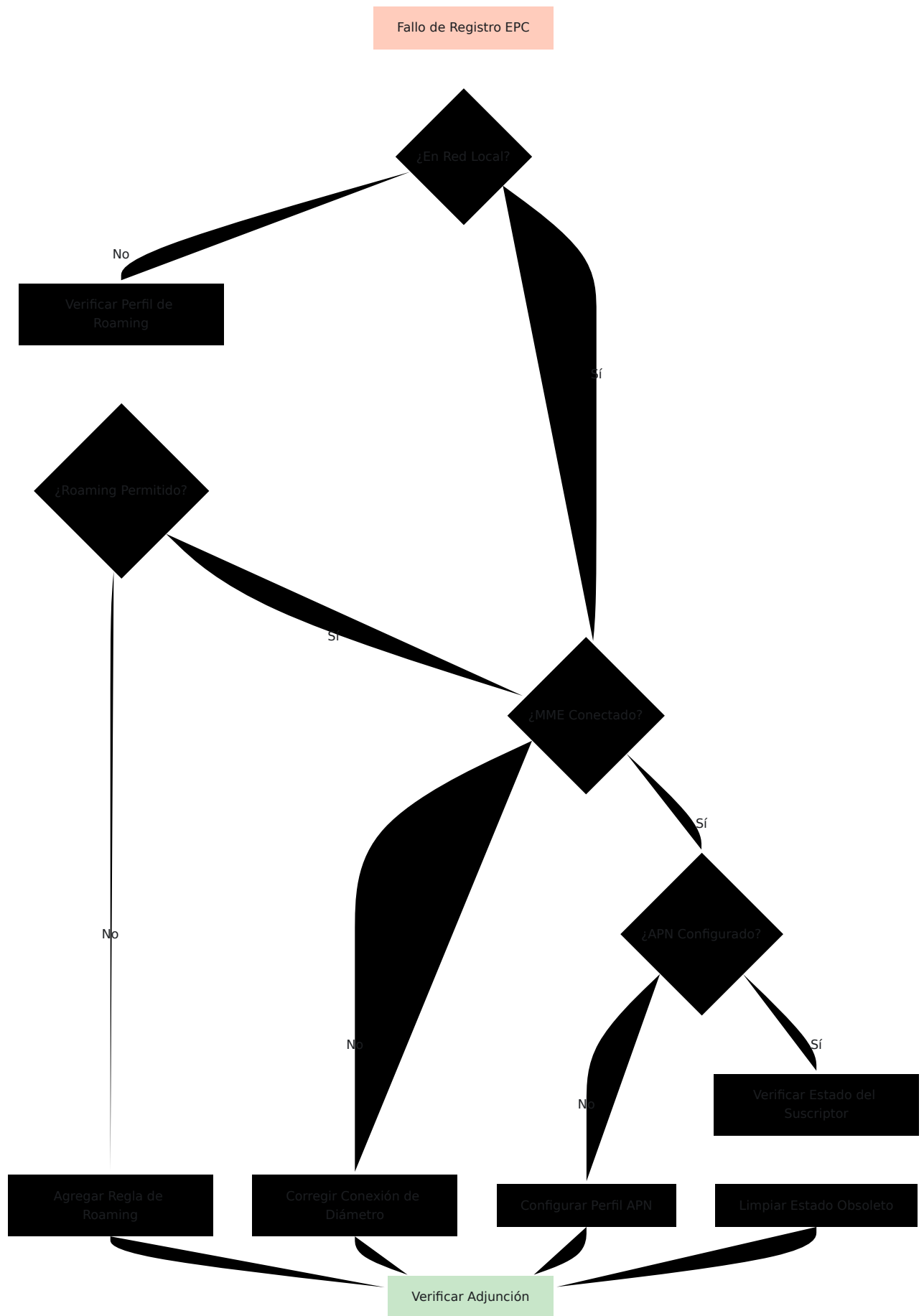
1. Consultar el estado del suscriptor desde la base de datos
2. Verificar si hay asignaciones de MME obsoletas
3. Verificar la marca de tiempo de la última actualización

Solución:

- Limpiar el estado del suscriptor (procedimiento de desvinculación)
- Restablecer el MME que sirve en el estado del suscriptor
- Puede requerir un ciclo de energía del suscriptor

Diagrama de Flujo de Solución de Problemas

de Registro EPC



Fallos de Registro IMS

Síntomas

- El suscriptor no puede registrarse para VoLTE
- "Fallo de registro IMS" en el dispositivo
- Los datos funcionan pero la voz no

Causas Comunes y Soluciones

Causa 1: IMS Deshabilitado para el Suscriptor

Síntomas:

- El suscriptor tiene datos pero no IMS
- Registro rechazado de inmediato

Pasos de Diagnóstico:

1. Consultar al suscriptor y verificar el campo `ims_enabled`
2. Verificar que el suscriptor tenga asignado `ims_profile_id`

Solución:

- **Habilitar IMS** para el suscriptor
- Asignar **perfil IMS**

Causa 2: S-CSCF No Conectado

Síntomas:

- Todos los registros IMS fallan
- No hay tráfico de Diámetro relacionado con IMS

Pasos de Diagnóstico:

1. Verificar la **página de Diámetro del Panel de Control**
2. Verificar que el par S-CSCF esté conectado

3. Verificar que el S-CSCF soporte la aplicación Cx

Solución:

- Corregir la [conectividad de Diámetro](#) al S-CSCF
- Verificar la configuración del S-CSCF

Causa 3: Plantilla IFC Faltante o Inválida

Síntomas:

- El registro falla durante la Respuesta de Autorización de Usuario
- Errores relacionados con IFC en los registros

Pasos de Diagnóstico:

1. Consultar el perfil IMS del suscriptor
2. Verificar que la plantilla IFC esté presente
3. Verificar la sintaxis XML de IFC

Solución:

- Actualizar el [perfil IMS](#) con una plantilla IFC válida
- Ver [Documentación de Perfiles](#) para ejemplos de IFC

Causa 4: Roaming Denegado para IMS

Síntomas:

- IMS funciona en la red local
- Falla al hacer roaming
- El roaming de datos funciona pero no IMS

Pasos de Diagnóstico:

1. Verificar la acción IMS del perfil de roaming
2. Verificar que las reglas de roaming tengan el `ims_action` correcto

Solución:

- Actualizar las **reglas de roaming** para permitir IMS
- O actualizar la acción IMS predeterminada del perfil de roaming

Diagrama de Flujo de Solución de Problemas de Registro IMS



Fallos de Llamadas VoLTE

Síntomas

- El registro IMS tiene éxito pero las llamadas fallan
- Audio unidireccional
- La llamada se corta inmediatamente
- Error de "llamada fallida" en el dispositivo

Causas Comunes y Soluciones

Causa 1: P-CSCF No Conectado

Síntomas:

- El registro funciona pero las llamadas fallan
- La autorización de medios falla

Pasos de Diagnóstico:

1. Verificar la [página de Diámetro del Panel de Control](#)
2. Verificar que el par P-CSCF esté conectado
3. Verificar que el P-CSCF soporte la aplicación Rx (función PCRF de OmniHSS)

Solución:

- Corregir la [conectividad de Diámetro](#) al P-CSCF
- Verificar que la configuración del P-CSCF apunte a OmniHSS para Rx

Causa 2: Autorización de Medios Faltante

Síntomas:

- La configuración de la llamada comienza pero falla
- El intercambio AAR/AAA falla
- Errores en la interfaz Rx

Pasos de Diagnóstico:

1. Verificar los registros en busca de mensajes de Diámetro Rx
2. Verificar que se haya recibido AAR (AA-Request)
3. Verificar la respuesta AAA (AA-Answer)

Solución:

- Verificar que el P-CSCF esté enviando AAR para la autorización de medios
- Verificar la configuración de la aplicación Rx de OmniHSS
- Verificar que el suscriptor tenga un registro IMS activo

Causa 3: Problemas de QoS/Bearer

Síntomas:

- La llamada se conecta pero no hay audio
- Audio unidireccional
- Problemas de calidad

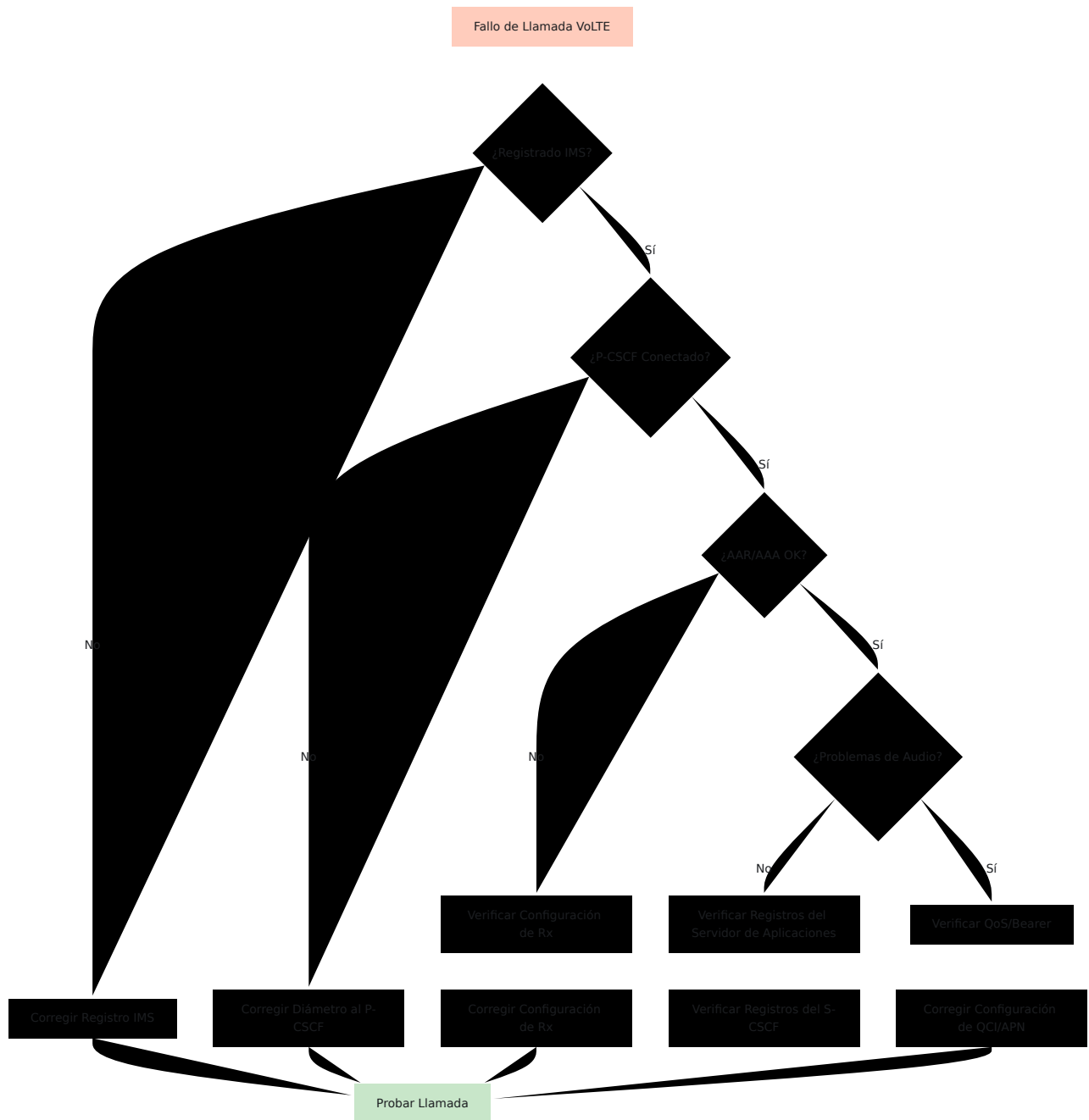
Pasos de Diagnóstico:

1. Verificar el perfil de QoS del APN para el APN de voz
2. Verificar que QCI esté configurado correctamente (típicamente QCI 1 para voz)
3. Verificar que el P-GW esté conectado para Gx (función PCRF)

Solución:

- Verificar el **perfil de QoS del APN** para el APN IMS
- Asegurarse de que QCI 1 esté configurado para el bearer de voz
- Corregir la **conectividad de Diámetro** al P-GW si es necesario

Diagrama de Flujo de Solución de Problemas de Llamadas VoLTE



Problemas de Roaming

Síntomas

- El suscriptor funciona en casa pero no al hacer roaming

- Algunas redes de roaming funcionan, otras no
- El roaming de datos funciona pero no la voz (o viceversa)

Causas Comunes y Soluciones

Causa 1: No se Asignó un Perfil de Roaming

Síntomas:

- El roaming falla para el suscriptor
- Otros suscriptores realizan roaming con éxito

Pasos de Diagnóstico:

1. Consultar `roaming_profile_id` del suscriptor
2. Verificar si el campo es nulo

Solución:

- Asignar **perfil de roaming** al suscriptor

Causa 2: Roaming Denegado por Política

Síntomas:

- El roaming falla consistentemente en una red específica
- El error indica rechazo de la política

Pasos de Diagnóstico:

1. Identificar la MCC/MNC de la red visitada desde el dispositivo del suscriptor o MME
2. Consultar el perfil de roaming del suscriptor
3. Verificar las reglas de roaming para la MCC/MNC coincidente
4. Verificar la acción predeterminada del perfil

Solución:

- Agregar **regla de roaming** para permitir la red visitada:

```
curl -k -X POST https://hss.example.com:8443/api/roaming/rule \
-H "Content-Type: application/json" \
-d '{
  "roaming_rule": {
    "name": "Allow Visited Network",
    "mcc": "310",
    "mnc": "410",
    "data_action": "allow",
    "ims_action": "allow"
  }
}'
```

Causa 3: Datos Permitidos pero IMS Denegado

Síntomas:

- El roaming de datos funciona
- El roaming de voz/IMS falla
- Disponibilidad del servicio dividida

Pasos de Diagnóstico:

1. Consultar las reglas de roaming para la red visitada
2. Verificar los valores de `data_action` vs `ims_action`
3. Verificar las acciones predeterminadas del perfil de roaming

Solución:

- Actualizar la regla de roaming para permitir IMS:
 - Establecer `ims_action: "allow"`
- O actualizar `ims_action_if_no_rules_match` del perfil a `"allow"`

Consulte la [Documentación de Roaming](#) para una configuración detallada.

Problemas de EIR

Síntomas

- Dispositivos bloqueados inesperadamente
- Dispositivos robados no bloqueados
- Verificación de EIR fallida

Causas Comunes y Soluciones

Causa 1: Regex de IMEI Incorrecto

Síntomas:

- Dispositivos incorrectos bloqueados/permitidos
- La regla coincide incorrectamente

Pasos de Diagnóstico:

1. Consultar reglas de EIR
2. Identificar qué regla está coincidiendo
3. Probar el patrón regex contra el IMEI real
4. Verificar la prioridad/orden de la regla

Solución:

- Actualizar **regla de EIR** con regex correcto
- Probar el regex a fondo antes de aplicar
- Considerar el orden de la regla (la primera coincidencia gana)

Causa 2: MME No Envía Solicitudes S13

Síntomas:

- La verificación de EIR nunca ocurre
- Todos los dispositivos permitidos independientemente de las reglas

Pasos de Diagnóstico:

1. Verificar si el MME está configurado para usar la interfaz S13
2. Verificar que el par Diameter del MME esté conectado
3. Verificar el soporte de la aplicación S13
4. Revisar la configuración del MME

Solución:

- Configurar el MME para realizar verificaciones de EIR a través de S13
- Verificar que el par Diameter soporte la aplicación S13 (16777252)
- Contactar al administrador del MME si es necesario

Causa 3: Sin Regla Predeterminada

Síntomas:

- Dispositivos que no coinciden con ninguna regla tienen un comportamiento inesperado

Pasos de Diagnóstico:

1. Consultar todas las reglas de EIR
2. Verificar si existe una regla de captura
3. Verificar el orden de las reglas

Solución:

- Agregar una regla predeterminada con regex `.*` para coincidir con todos los IMEIs
 - Establecer la acción apropiada (lista blanca o lista negra)
 - Asegurarse de que las reglas específicas se verifiquen antes de la regla de captura
-

Problemas de Rendimiento

Síntomas

- Respuestas lentas de la API
- Tiempo de espera en solicitudes Diameter
- Alto uso de CPU o memoria
- El Panel de Control se carga lentamente

Causas Comunes y Soluciones

Causa 1: Alta Carga en la Base de Datos

Síntomas:

- Todas las operaciones lentas
- Alta CPU en la base de datos
- Tiempos de espera en consultas

Pasos de Diagnóstico:

1. Verificar el uso de recursos del servidor de base de datos
2. Identificar consultas lentas
3. Verificar si faltan índices
4. Monitorear patrones de consulta

Solución:

- Optimizar consultas lentas
- Agregar índices a la base de datos
- Aumentar los recursos de la base de datos
- Considerar la escalabilidad de la base de datos
- Ver [Problemas de Base de Datos](#)

Causa 2: Alto Número de Suscriptores

Síntomas:

- Rendimiento degradado con el tiempo
- La lentitud se correlaciona con el crecimiento de suscriptores
- Operaciones de lista especialmente lentas

Pasos de Diagnóstico:

1. Consultar el número total de suscriptores
2. Verificar tamaños de tablas
3. Revisar planes de ejecución de consultas
4. Monitorear tendencias de uso de recursos

Solución:

- Planificar una actualización de capacidad
- Optimizar consultas para grandes conjuntos de datos
- Considerar la paginación para grandes resultados
- Implementar caché si es necesario

Causa 3: Problemas con el Par Diameter

Síntomas:

- Operaciones Diameter lentas
- Tiempos de espera en un par específico
- Algunos pares rápidos, otros lentos

Pasos de Diagnóstico:

1. Verificar la [página Diameter del Panel de Control](#)
2. Identificar el par lento
3. Probar la latencia de red hacia el par
4. Verificar el uso de recursos del par

Solución:

- Investigar problemas de rendimiento del par
- Verificar la ruta de red en busca de congestión
- Considerar agregar pares redundantes

- Aumentar el tiempo de espera de Diameter si es necesario

Causa 4: Problemas de Memoria

Síntomas:

- Uso de memoria de OmniHSS alto
- Errores de falta de memoria
- El rendimiento se degrada con el tiempo

Pasos de Diagnóstico:

1. Verificar el uso de memoria de OmniHSS en la página de Aplicaciones
2. Monitorear la tendencia de memoria
3. Verificar si hay fugas de memoria
4. Revisar la configuración de la VM de Erlang

Solución:

- Reiniciar OmniHSS para limpiar la condición temporal
 - Investigar la fuga de memoria si el uso crece continuamente
 - Ajustar la configuración de memoria de la VM de Erlang en runtime.exs
 - Planificar una actualización de hardware si es consistentemente alto
-

Problemas de Estado del Suscriptor

Síntomas

- El suscriptor aparece como conectado pero no lo está
- Información de estado obsoleta
- Información de ubicación incorrecta
- No se puede desasociar al suscriptor

Causas Comunes y Soluciones

Causa 1: Caída/Reinicio del MME

Síntomas:

- El suscriptor muestra un MME que ya no está en servicio
- El suscriptor no puede conectarse después del reinicio del MME
- El estado está obsoleto

Pasos de Diagnóstico:

1. Verificar el estado del suscriptor para el MME en servicio
2. Verificar si el MME se ha reiniciado
3. Verificar la última hora de conexión del MME

Solución:

- Esperar a que el suscriptor se conecte nuevamente (el estado se actualizará)
- O limpiar manualmente el estado del suscriptor
- El MME debe enviar Cancel-Location al reiniciarse

Causa 2: Desasociación de Red No Recibida

Síntomas:

- Suscriptor apagado pero aparece como conectado
- Las sesiones PDN permanecen en la base de datos
- La ubicación no se ha limpiado

Pasos de Diagnóstico:

1. Verificar la marca de tiempo last_seen del suscriptor
2. Verificar si el estado es antiguo (horas o días)
3. Verificar si el dispositivo del suscriptor es accesible

Solución:

- El estado se limpiará cuando el suscriptor se conecte nuevamente
- O esperar el tiempo de espera del estado (si se implementa)
- Puede ser necesaria una limpieza manual para un estado muy obsoleto

Causa 3: Corrupción de Base de Datos

Síntomas:

- Estado inconsistente entre tablas
- Violaciones de clave foránea
- El estado no tiene sentido

Pasos de Diagnóstico:

1. Consultar el estado del suscriptor directamente desde la base de datos
2. Verificar si hay registros huérfanos
3. Verificar la integridad referencial

Solución:

- Identificar y corregir datos inconsistentes
 - Puede requerir limpieza manual de la base de datos
 - Contactar soporte si la corrupción es generalizada
-

Problemas de API

Síntomas

- La API devuelve errores
- Respuestas lentas de la API
- No se pueden crear/actualizar entidades
- Errores 500

Causas Comunes y Soluciones

Causa 1: Datos de Solicitud Inválidos

Síntomas:

- Errores 400 o 422
- Mensajes de error de validación
- Campo rechazado

Pasos de Diagnóstico:

1. Revisar la respuesta de error para errores específicos de campo
2. Verificar el formato de la solicitud de API
3. Verificar que los campos requeridos estén presentes
4. Verificar tipos de datos

Solución:

- Corregir los datos de la solicitud para que coincidan con la [referencia de API](#)
- Asegurarse de que se incluyan todos los campos requeridos
- Verificar que existan referencias de clave foránea (IDs de perfil, etc.)

Causa 2: Restricción de Clave Foránea

Síntomas:

- No se puede crear un suscriptor
- Error: "key_set_id does not exist"
- Entidad referenciada no encontrada

Pasos de Diagnóstico:

1. Identificar qué clave foránea está fallando
2. Verificar que la entidad referenciada exista:
 - key_set_id → conjuntos de claves
 - epc_profile_id → perfiles EPC
 - ims_profile_id → perfiles IMS

Solución:

- Crear primero la entidad referenciada
- O usar el ID de entidad existente
- Seguir el [flujo de aprovisionamiento completo](#)

Causa 3: Conectividad de Base de Datos

Síntomas:

- Errores 500
- Todas las llamadas a la API fallan
- Errores de conexión a la base de datos

Solución:

- Ver [Problemas de Base de Datos](#)
-

Herramientas y Comandos de Diagnóstico

Comprobaciones Rápidas del Panel de Control

1. Descripción General del Sistema

- URL: `https://[hostname]:7443/overview`
- Verificar: Cantidades de suscriptores, sesiones activas, estado del sistema

2. Estado de Diameter

- URL: `https://[hostname]:7443/diameter`
- Verificar: Todos los pares críticos conectados

3. Salud de la Aplicación

- URL: `https://[hostname]:7443/application`

- Verificar: Uso de memoria, conteo de procesos, tiempo de actividad

Comandos de Diagnóstico de API

Verificar la Salud del Sistema:

```
curl -k https://hss.example.com:8443/api/status
```

Consultar Suscriptor:

```
# Por IMSI
curl -k
https://hss.example.com:8443/api/subscriber/imsi/001001123456789

# Por MSISDN
curl -k
https://hss.example.com:8443/api/subscriber/msisdn/14155551234

# Por ID
curl -k https://hss.example.com:8443/api/subscriber/d290f1ee-6c54-
4b01-90e6-d701748f0851
```

Listar Todos los Suscriptores:

```
curl -k https://hss.example.com:8443/api/subscriber
```

Verificar Configuración del Perfil:

```
# Perfil EPC
curl -k https://hss.example.com:8443/api/epc/profile/e58ed763-928c-4155-bee9-fdbaaadc15f3

# Perfil IMS
curl -k https://hss.example.com:8443/api/ims/profile/7c9e6679-7425-40de-944b-e07fc1f90ae7

# Perfil de Roaming
curl -k https://hss.example.com:8443/api/roaming/profile/9c858901-8a57-4791-81fe-4c455b099bc9
```

Comandos de Diagnóstico de Red

Probar Conectividad del Puerto Diameter:

```
telnet [PEER_IP] 3868
```

Verificar Certificado TLS:

```
openssl s_client -connect [hostname]:8443 -showcerts
```

Probar Conectividad de Base de Datos:

```
psql -h [DB_HOST] -U [DB_USER] -d [DB_NAME] -c "SELECT COUNT(*)
FROM subscriber;"
```

Análisis de Registros

Buscar Registros para un IMSI Específico:

```
grep "001001123456789" /var/log/omnihss/omnihss.log
```

Encontrar Fallos de Autenticación:

```
grep "authentication.*fail" /var/log/omnihss/omnihss.log
```

Verificar Eventos de Pares Diameter:

```
grep "Diameter peer" /var/log/omnihss/omnihss.log
```

Encontrar Errores de Base de Datos:

```
grep -i "database.*error" /var/log/omnihss/omnihss.log
```

Directrices de Escalación

Cuándo Escalar

Escalar a soporte de ingeniería/proveedor cuando:

1. **Fallos en todo el sistema** que no se pueden resolver con procedimientos documentados
2. **Corrupción de datos** o estado inconsistente de la base de datos
3. **Errores de software sospechosos** o comportamiento inesperado
4. **Problemas de rendimiento** que no se pueden resolver con ajustes
5. **Incidentes de seguridad** o acceso no autorizado
6. **Preguntas sobre comportamiento no documentado**

Información a Proporcionar

Al escalar, incluir:

1. **Síntomas detallados** - Qué está fallando, cuándo, para quién
2. **Pasos tomados** - Qué solución de problemas ya ha realizado
3. **Registros** - Extractos de registros relevantes que muestran el problema

4. **Configuración** - Porciones relevantes de runtime.exs (redactar datos sensibles)
5. **Entorno** - Versión de OmniHSS, versión de base de datos, versión de SO
6. **Impacto** - Cuántos suscriptores se ven afectados, impacto en el negocio
7. **Ejemplos de suscriptores** - IMSIs específicos que muestran el problema

Crítico vs No Crítico

Problemas Críticos (Escalar Inmediatamente):

- Sistema completamente caído
- Todos los suscriptores incapaces de conectarse
- Corrupción de base de datos
- Brecha de seguridad

Problemas No Críticos (Documentar y Escalar Durante Horas Laborales):

- Problemas de un solo suscriptor que se pueden sortear
 - Degradación del rendimiento que es manejable
 - Solicitudes de mejora
 - Preguntas sobre documentación
-

Referencia de Mensajes de Error Comunes

Errores de Autenticación

Mensaje de Error	Causa	Solución
"La generación de vectores de autenticación falló"	Conjunto de claves faltante o inválido	Verificar configuración del conjunto de claves
"Fallo de sincronización de SQN"	SQN fuera de sincronización	Esperar la resincronización
"Suscriptor no encontrado"	IMSI inválido	Verificar IMSI, aprovisionar suscriptor
"Suscriptor deshabilitado"	enabled=false	Habilitar suscriptor

Errores de Diameter

Mensaje de Error	Causa	Solución
"Tiempo de espera de conexión de par Diameter"	Problema de red	Verificar conectividad de red
"Intercambio CER/CEA fallido"	Desajuste de configuración	Verificar configuración de Diameter
"Aplicación no soportada"	El par no soporta la aplicación requerida	Verificar aplicaciones de par
"Fallo en el apretón de manos TLS"	Problema con el certificado	Verificar certificados

Errores de Base de Datos

Mensaje de Error	Causa	Solución
"Conexión rechazada"	Base de datos caída	Iniciar base de datos
"Autenticación fallida"	Credenciales incorrectas	Corregir credenciales
"No hay conexiones disponibles"	Pool agotado	Aumentar tamaño del pool
"Tiempo de espera de consulta"	Consulta lenta	Optimizar consultas

Errores de API

Mensaje de Error	Causa	Solución
"key_set_id does not exist"	Clave foránea inválida	Crear conjunto de claves primero
"IMSI ya ha sido tomado"	IMSI duplicado	Usar IMSI diferente o eliminar el existente
"Error de validación"	Entrada inválida	Verificar formato y requisitos del campo

[← Volver a la Guía de Operaciones](#) | [Siguiente: Referencia de API →](#)

Integración de Webhook de OmniHSS

[← Volver a la Guía de Operaciones](#)

Tabla de Contenidos

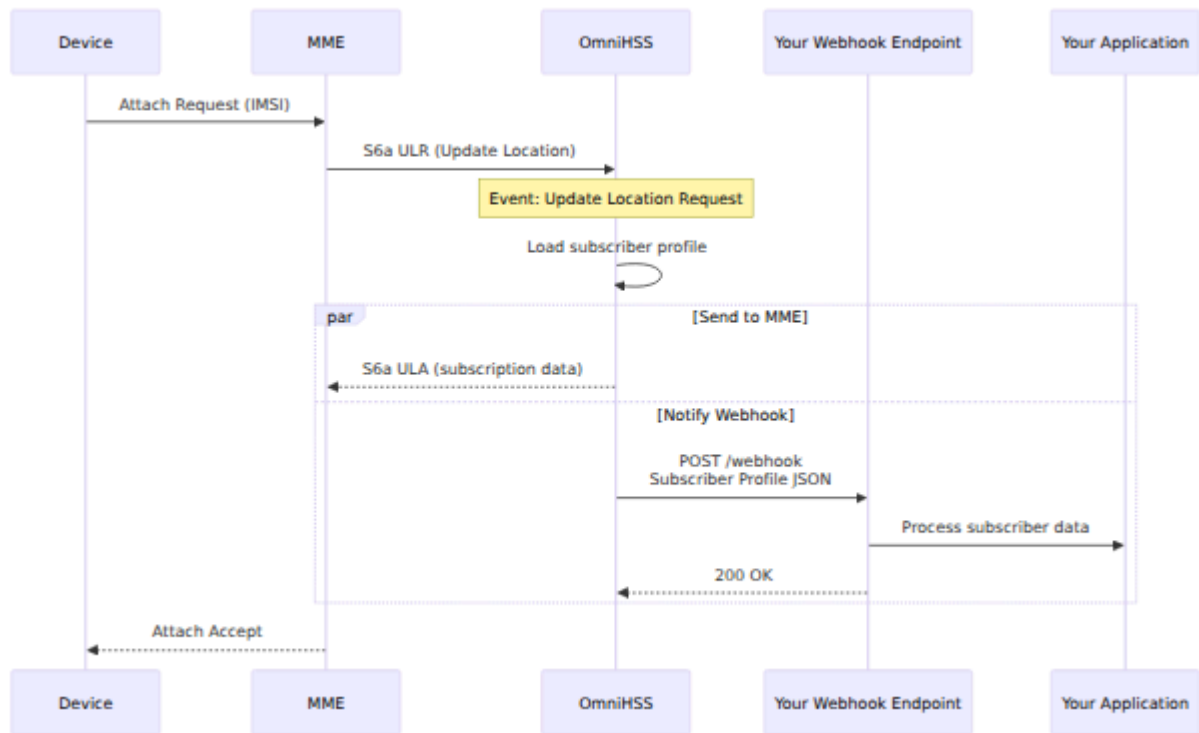
- [Descripción General](#)
 - [Cómo Funcionan los Webhooks](#)
 - [Eventos de Webhook](#)
 - [Carga Útil del Webhook](#)
 - [Configuración](#)
 - [Casos de Uso](#)
 - [Consideraciones de Seguridad](#)
 - [Solución de Problemas](#)
-

Descripción General

OmniHSS soporta **webhooks** para notificar a sistemas externos sobre eventos de suscriptores en tiempo real. Cuando ocurren eventos específicos (como actualizaciones de ubicación, solicitudes de autenticación o registros IMS), OmniHSS puede enviar una solicitud HTTP POST a tu endpoint de webhook configurado con los datos completos del perfil del suscriptor.

¿Qué Son los Webhooks?

Los webhooks son callbacks HTTP que permiten a OmniHSS enviar notificaciones de eventos a tu aplicación a medida que ocurren, en lugar de requerir que tu aplicación consulte la API de HSS en busca de cambios.



Beneficios Clave

- **Notificaciones en tiempo real** - Recibe actualizaciones instantáneas cuando ocurren eventos de suscriptores
- **Datos completos del suscriptor** - Cada webhook incluye el perfil completo del suscriptor (igual que `GET /api/subscriber`)
- **Automatización impulsada por eventos** - Activa flujos de trabajo, análisis o aprovisionamiento basados en eventos de red
- **Reducción de consultas** - No es necesario consultar continuamente la API por cambios en el estado del suscriptor
- **Flexibilidad de integración** - Conecta OmniHSS a sistemas de facturación, plataformas de análisis o aplicaciones personalizadas

Cómo Funcionan los Webhooks

Flujo de Eventos

1. **Ocurre un evento** - Un suscriptor realiza una acción (adjuntar, actualización de ubicación, registro IMS, etc.)

2. **HSS procesa el evento** - OmniHSS maneja la solicitud/respuesta de Diameter normalmente
3. **Webhook activado** - Si hay un webhook registrado para este tipo de evento, HSS envía un POST HTTP a tu endpoint
4. **Datos del suscriptor incluidos** - La carga útil del webhook contiene el perfil completo del suscriptor como JSON
5. **Tu aplicación responde** - Tu endpoint debe devolver HTTP 200-299 para reconocer la recepción

Garantías de Entrega

- **Entrega de mejor esfuerzo** - Los webhooks se envían de forma asíncrona y no bloquean las operaciones de red
- **Tiempo de espera** - Las solicitudes de webhook tienen un tiempo de espera de 5 segundos
- **Sin reintentos** - Si tu endpoint no está disponible o devuelve un error, el webhook no se reintenta
- **Orden no garantizado** - Los eventos pueden llegar fuera de orden bajo alta carga

Importante: Las operaciones de red (autenticación, actualizaciones de ubicación, etc.) **no** dependen de la entrega del webhook. Si tu endpoint de webhook está caído, el servicio del suscriptor continúa normalmente.

Eventos de Webhook

OmniHSS puede activar webhooks para los siguientes eventos:

Eventos EPC/LTE

Evento	Activador	Descripción
update_location_request	S6a ULR	El suscriptor se adjunta o realiza una actualización de área de seguimiento
authentication_information_request	S6a AIR	La red solicita vectores de autenticación para el suscriptor
purge_request	S6a PUR	MME elimina el contexto del suscriptor (dispositivo apagado, desasociado)
cancel_location_answer	S6a CLA	MME reconoce la desregistración del suscriptor

Eventos IMS

Evento	Activador	Descripción
ims_registration	Cx SAR	El suscriptor se registra para el servicio IMS/VoLTE
ims_deregistration	Cx SAR (de-reg)	El suscriptor se desregistra de IMS
ims_profile_request	Sh UDR	El Servidor de Aplicaciones solicita el perfil IMS del suscriptor

Eventos de Políticas (PCRF)

Evento	Activador	Descripción
policy_request	Gx CCR	P-GW solicita política para la sesión de datos del suscriptor
media_authorization	Rx AAR	P-CSCF solicita autorización de medios para la llamada IMS

Eventos Multi-IMSI

Evento	Activador	Descripción
imsi_switch	ULR para diferente IMSI en la misma SIM	El dispositivo cambia a un IMSI diferente en una SIM multi-IMSI

Carga Útil del Webhook

Formato de Solicitud

Cuando ocurre un evento, OmniHSS envía una solicitud HTTP POST a tu URL de webhook configurada:

POST /your-webhook-endpoint HTTP/1.1
Host: your-server.com
Content-Type: application/json
X-OmniHSS-Event: update_location_request
X-OmniHSS-Event-ID: 550e8400-e29b-41d4-a716-446655440000
X-OmniHSS-Timestamp: 2025-01-15T14:30:00Z

```
{
  "event": "update_location_request",
  "event_id": "550e8400-e29b-41d4-a716-446655440000",
  "timestamp": "2025-01-15T14:30:00Z",
  "subscriber": {
    "id": "d290f1ee-6c54-4b01-90e6-d701748f0851",
    "imsi": "001001123456789",
    "enabled": true,
    "ims_enabled": true,
    "msisdns": [
      {"id": "16fd2706-8baf-433b-82eb-8c7fada847da", "msisdn":
"14155551001"},
      {"id": "27ae3807-9cbf-4a4c-93fc-9d8afdb958eb", "msisdn":
"14155551002"}
    ],
    "sim": {
      "id": "3f2504e0-4f89-41d3-9a0c-0305e82c3301",
      "iccid": "8991101200003204510",
      "is_esim": false
    },
    "key_set": {
      "id": "6ba7b810-9dad-41d1-80b4-00c04fd430c8",
      "amf": "8000"
    },
    "epc_profile": {
      "id": "e58ed763-928c-4155-bee9-fdbaaadc15f3",
      "name": "Premium 100Mbps",
      "ue_ambr_dl_kbps": 100000,
      "ue_ambr_ul_kbps": 50000
    },
    "ims_profile": {
      "id": "7c9e6679-7425-40de-944b-e07fc1f90ae7",
      "name": "Standard VoLTE"
    },
    "roaming_profile": {
      "id": "9c858901-8a57-4791-81fe-4c455b099bc9",
```

```

    "name": "International Roaming Allowed"
  },
  "subscriber_state": {
    "mme_host": "mme-01.example.com",
    "mme_realm": "epc.mnc001.mcc001.3gppnetwork.org",
    "visited_plmn": "001001",
    "last_update": "2025-01-15T14:30:00Z"
  },
  "custom_attributes": {
    "account_type": "premium",
    "billing_plan": "unlimited"
  }
},
"event_context": {
  "visited_plmn": "310410",
  "mme_host": "mme-roaming.example.com",
  "location_update_type": "initial_attach"
}
}

```

Estructura de la Carga Útil

Campo	Tipo	Descripción
<code>event</code>	string	Tipo de evento (por ejemplo, <code>update_location_request</code>)
<code>event_id</code>	string	UUID único para esta entrega de webhook
<code>timestamp</code>	string	Marca de tiempo ISO 8601 cuando ocurrió el evento
<code>subscriber</code>	object	Perfil completo del suscriptor (igual que <code>GET /api/subscriber/:id</code>)
<code>event_context</code>	object	Datos adicionales específicos del evento

Campos del Contexto del Evento

El objeto `event_context` contiene información específica del evento:

Para `update_location_request`:

```
{
  "visited_plmn": "310410",
  "mme_host": "mme-roaming.example.com",
  "mme_realm": "epc.mnc410.mcc310.3gppnetwork.org",
  "location_update_type": "initial_attach"
}
```

Para `imsi_switch`:

```
{
  "previous_imsi": "001001111111111",
  "new_imsi": "310410222222222",
  "sim_id": "3f2504e0-4f89-41d3-9a0c-0305e82c3301",
  "previous_mme_host": "mme-home.example.com",
  "new_mme_host": "mme-roaming.example.com"
}
```

Para `ims_registration`:

```
{
  "scscf_host": "scscf-01.ims.example.com",
  "public_identities": [
    "sip:001001123456789@ims.mnc001.mcc001.3gppnetwork.org",
    "sip:+14155551001@ims.example.com",
    "tel:+14155551001"
  ]
}
```

Encabezados HTTP

Encabezado	Descripción	Ejemplo
Content-Type	Siempre application/json	application/json
X-OmniHSS-Event	Tipo de evento	update_location_request
X-OmniHSS-Event-ID	Identificador único del evento	UUID
X-OmniHSS-Timestamp	Marca de tiempo del evento	Formato ISO 8601
User-Agent	Versión de OmniHSS	OmniHSS/1.0

Configuración

Registro de Webhooks

Los webhooks se configuran a través de la API de OmniHSS.

Registrar un Webhook

```
curl -k -X POST https://hss.example.com:8443/api/webhook \
-H "Content-Type: application/json" \
-d '{
  "webhook": {
    "url": "https://your-server.com/omnihss-webhook",
    "events": [
      "update_location_request",
      "ims_registration",
      "imsi_switch"
    ],
    "enabled": true,
    "description": "Webhook del sistema de facturación de
producción"
  }
}'
```

Respuesta:

```
{
  "data": {
    "id": "4e5d6c7b-8a9f-4b0c-8d1e-2f3a4b5c6d7e",
    "url": "https://your-server.com/omnihss-webhook",
    "events": [
      "update_location_request",
      "ims_registration",
      "imsi_switch"
    ],
    "enabled": true,
    "description": "Webhook del sistema de facturación de
producción",
    "created_at": "2025-01-15T14:00:00Z"
  }
}
```

Listar Webhooks

```
curl -k https://hss.example.com:8443/api/webhook
```

Actualizar Webhook

```
curl -k -X PUT https://hss.example.com:8443/api/webhook/4e5d6c7b-8a9f-4b0c-8d1e-2f3a4b5c6d7e \
-H "Content-Type: application/json" \
-d '{
  "webhook": {
    "enabled": false
  }
}'
```

Eliminar Webhook

```
curl -k -X DELETE
https://hss.example.com:8443/api/webhook/4e5d6c7b-8a9f-4b0c-8d1e-2f3a4b5c6d7e
```

Requisitos del Endpoint de Webhook

Tu endpoint de webhook debe:

1. **Aceptar solicitudes POST** con `Content-Type: application/json`
2. **Responder rápidamente** - Devolver HTTP 200-299 dentro de 5 segundos
3. **Ser idempotente** - Manejar entregas duplicadas de manera adecuada
4. **Usar HTTPS** - Por seguridad, utilizar endpoints TLS/SSL (recomendado)
5. **Validar cargas útiles** - Verificar que la solicitud provenga de OmniHSS (ver sección de Seguridad)

Ejemplo de Manejador de Webhook (Node.js/Express):


```
const express = require('express');
const app = express();

app.post('/omnihss-webhook', express.json(), (req, res) => {
  const { event, subscriber, event_context } = req.body;

  console.log(`Evento recibido: ${event}`);
  console.log(`IMSI del suscriptor: ${subscriber.imsi}`);

  // Procesar los datos del suscriptor
  // ... tu lógica de negocio aquí ...

  // Responder inmediatamente para reconocer la recepción
  res.status(200).json({ received: true });

  // Manejar procesamiento asíncrono después de la respuesta
  processWebhook(req.body).catch(console.error);
});

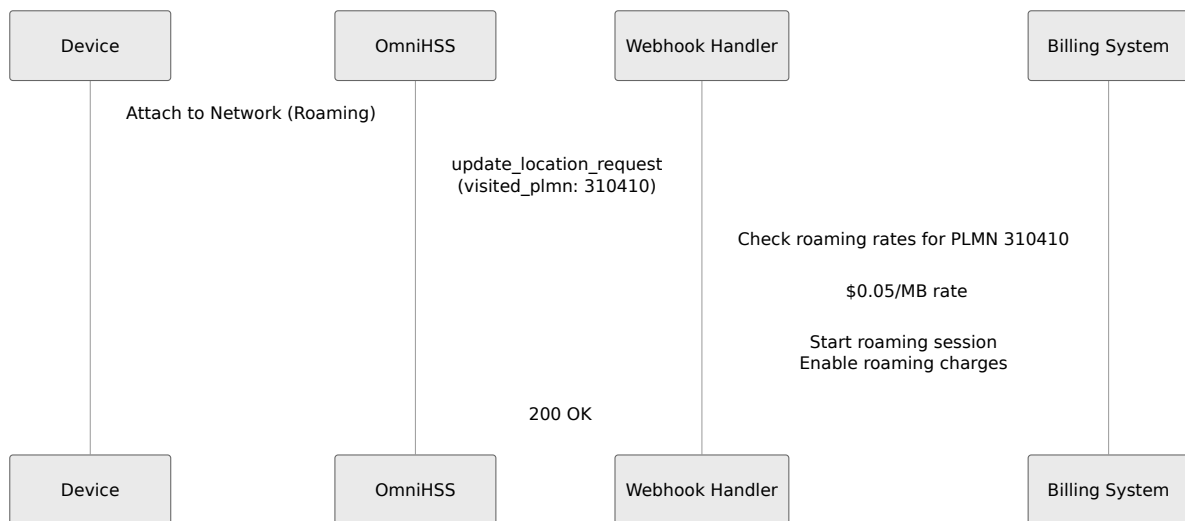
async function processWebhook(payload) {
  // Tu lógica de procesamiento asíncrono
  // por ejemplo, actualizar el sistema de facturación, activar
  análisis, etc.
}

app.listen(3000);
```

Casos de Uso

1. Facturación en Tiempo Real y Seguimiento de Uso

Rastrear el uso de la red por parte del suscriptor y activar eventos de facturación en tiempo real.



Beneficios:

- Detectar instantáneamente cuando los suscriptores viajan internacionalmente
- Aplicar cargos de roaming apropiados en tiempo real
- Rastrear con precisión los tiempos de inicio/finalización de sesiones
- Generar alertas de uso cuando se alcanzan los umbrales

2. Análisis y Monitoreo

Alimentar datos de actividad del suscriptor en plataformas de análisis para paneles de control y reportes en tiempo real.

Caso de Uso: Rastrear suscriptores activos por región

```
// Manejador de webhook alimentando datos a la plataforma de análisis
app.post('/omnihss-webhook', async (req, res) => {
  const { event, subscriber, event_context } = req.body;

  if (event === 'update_location_request') {
    await analytics.track({
      event: 'subscriber_location_update',
      imsi: subscriber.imsi,
      visited_plmn: event_context.visited_plmn,
      timestamp: req.body.timestamp,
      profile: subscriber.epc_profile.name
    });
  }

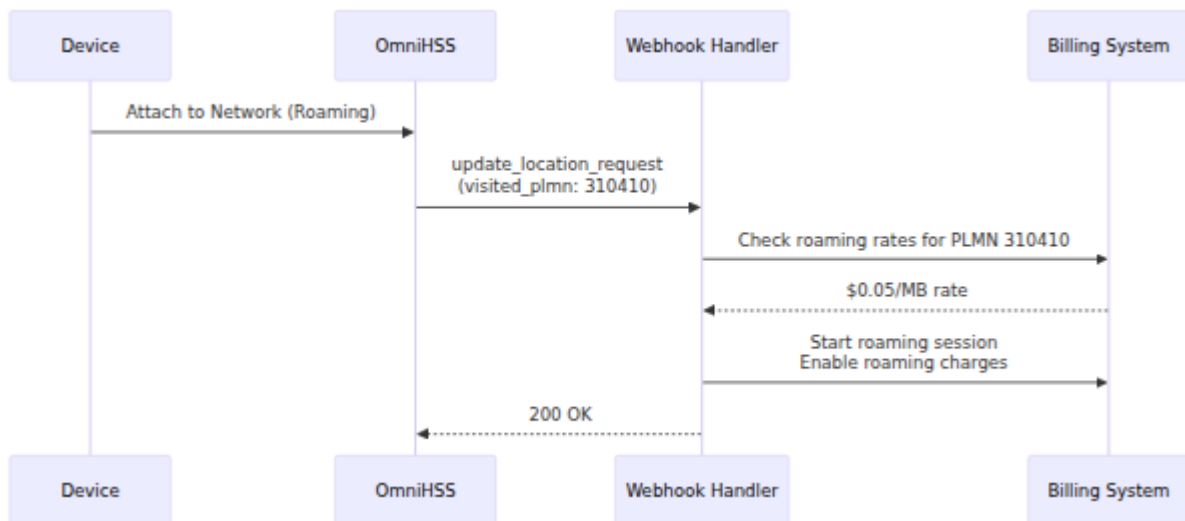
  res.status(200).send();
});
```

Panel de Análisis:

- Suscriptores activos por MME
- Suscriptores en roaming por país
- Distribución de niveles de servicio
- Tasa de éxito de registro IMS

3. Detección de Fraude y Seguridad

Detectar patrones de actividad sospechosos en tiempo real y activar respuestas automatizadas.



Escenarios de Detección de Fraude:

1. Cambios Rápidos de Ubicación

- El suscriptor se adjunta en el País A
- 30 minutos después, se adjunta en el País B (físicamente imposible)
- Acción: Marcar cuenta, enviar alerta al equipo de seguridad

2. Abuso de Cambio de IMSI

- Múltiples cambios rápidos de IMSI en la misma SIM
- Posible clonación de SIM o uso no autorizado de multi-IMSI
- Acción: Desactivar todos los IMSIs en la SIM, notificar al equipo de fraude

3. Roaming No Autorizado

- El suscriptor viaja a un país bloqueado (sanciones, riesgo de fraude)
- Acción: Desactivar automáticamente al suscriptor, bloquear acceso a la red

Implementación de Ejemplo:

```

@app.route('/omnihss-webhook', methods=['POST'])
def webhook_handler():
    data = request.json
    subscriber = data['subscriber']
    event_context = data.get('event_context', {})

    if data['event'] == 'update_location_request':
        visited_plmn = event_context.get('visited_plmn')

        # Verificar países bloqueados
        if visited_plmn in BLOCKED_PLMNS:
            disable_subscriber(subscriber['imsi'])
            alert_security_team(subscriber, 'Roaming a PLMN
bloqueado')

        # Verificar viajes imposibles
        if is_impossible_travel(subscriber['imsi'], visited_plmn):
            flag_for_review(subscriber['imsi'])
            alert_fraud_team(subscriber, 'Viaje imposible
detectado')

    return jsonify({'status': 'ok'}), 200

```

4. Automatización de Aprovisionamiento

Aprovisionar o actualizar automáticamente los servicios del suscriptor basándose en eventos de red.

Caso de Uso: Activar IMS automáticamente cuando el suscriptor utiliza VoLTE por primera vez

```

app.post('/omnihss-webhook', async (req, res) => {
  const { event, subscriber } = req.body;

  if (event === 'ims_registration' && !subscriber.ims_enabled) {
    // Primer usuario de IMS - habilitar IMS permanentemente
    await omnihss.updateSubscriber(subscriber.id, {
      ims_enabled: true,
      custom_attributes: {
        ...subscriber.custom_attributes,
        volte_activated_at: new Date().toISOString()
      }
    });

    // Actualizar CRM
    await crm.updateCustomer(subscriber.imsi, {
      features: ['volte']
    });
  }

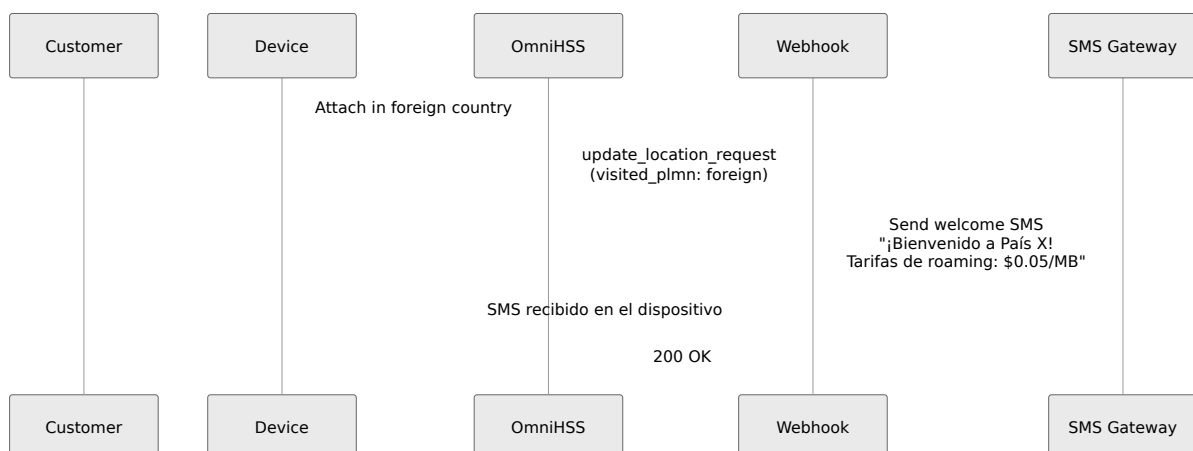
  res.status(200).send();
});

```

5. Notificaciones a Clientes

Enviar notificaciones en tiempo real a los clientes sobre su servicio.

Caso de Uso: Mensaje de bienvenida cuando viaja internacionalmente



Ejemplo de Notificaciones:

- "¡Bienvenido a [País]! Se aplican tarifas de roaming."
- "Has utilizado el 80% de tu asignación de datos"
- "El servicio VoLTE ahora está activo en tu dispositivo"
- "Tu cuenta ha sido actualizada a Premium"

6. Gestión de SIM Multi-IMSI

Rastrear y gestionar suscriptores con SIMs multi-IMSI, recibiendo notificaciones cuando cambian IMSIs.

```
app.post('/omnihss-webhook', async (req, res) => {
  const { event, subscriber, event_context } = req.body;

  if (event === 'imsi_switch') {
    const { previous_imsi, new_imsi, sim_id } = event_context;

    // Registrar cambio de IMSI para análisis
    await db.logImsiSwitch({
      sim_id,
      from_imsi: previous_imsi,
      to_imsi: new_imsi,
      timestamp: req.body.timestamp
    });

    // Actualizar sistema de facturación
    await billing.endSession(previous_imsi);
    await billing.startSession(new_imsi);

    // Alertar si hay cambios excesivos (posible fraude)
    const switchCount = await db.getSwitchCount(sim_id, '24h');
    if (switchCount > 10) {
      await alertFraudTeam(`Cambio excesivo de IMSI: SIM
${sim_id}`);
    }
  }

  res.status(200).send();
});
```

7. Integración con Sistemas Externos

Conectar OmniHSS a sistemas de terceros sin necesidad de consultas.

Ejemplos de Integraciones:

- **Sistemas CRM** - Actualizar registros de clientes con el uso del servicio
 - **Monitoreo de Red** - Alimentar datos de suscriptores a plataformas de análisis de red
 - **Sistemas de Facturación** - Activar cargos basados en eventos de red
 - **Sistemas de Tickets** - Crear automáticamente tickets para autenticaciones fallidas
 - **Almacenes de Datos** - Transmitir eventos de suscriptores para análisis de big data
-

Consideraciones de Seguridad

Secreto/Firma del Webhook

Para verificar que los webhooks provienen de OmniHSS, implementa la verificación de firma:

```
# Configurar webhook con secreto
curl -k -X POST https://hss.example.com:8443/api/webhook \
  -H "Content-Type: application/json" \
  -d '{
    "webhook": {
      "url": "https://your-server.com/omnihss-webhook",
      "events": ["update_location_request"],
      "secret": "your-secret-key-here"
    }
  }'
```

OmniHSS incluirá un encabezado `X-OmniHSS-Signature`:

X-OmniHSS-Signature:

sha256=5d7a8f9b2c1e3a4d6f7e8b9c0a1b2c3d4e5f6a7b8c9d0e1f2a3b4c5d6e7f8a

Verifica la firma:

```
const crypto = require('crypto');

function verifyWebhook(req) {
  const signature = req.headers['x-omnihss-signature'];
  const secret = process.env.WEBHOOK_SECRET;
  const payload = JSON.stringify(req.body);

  const expectedSignature = 'sha256=' +
    crypto.createHmac('sha256', secret)
      .update(payload)
      .digest('hex');

  return crypto.timingSafeEqual(
    Buffer.from(signature),
    Buffer.from(expectedSignature)
  );
}

app.post('/omnihss-webhook', (req, res) => {
  if (!verifyWebhook(req)) {
    return res.status(401).json({ error: 'Firma inválida' });
  }

  // Procesar webhook...
  res.status(200).send();
});
```

Mejores Prácticas

1. **Usar HTTPS** - Siempre utiliza TLS para los endpoints de webhook
2. **Validar firmas** - Verifica las firmas de los webhooks para prevenir suplantaciones
3. **Limitación de tasa** - Implementa limitación de tasa en los endpoints de webhook

4. **Lista blanca de IP** - Restringe el acceso al webhook a direcciones IP de OmniHSS
5. **Monitorear fallos** - Rastrear fallos de entrega de webhooks y errores
6. **Sanitizar datos** - Validar y sanitizar las cargas útiles de los webhooks antes de procesarlas
7. **Proteger credenciales** - Almacenar secretos de webhook en una configuración segura (variables de entorno, gestor de secretos)

Privacidad de Datos

Las cargas útiles de los webhooks contienen **información sensible del suscriptor**:

- IMSI (identidad del suscriptor)
- MSISDNs (números de teléfono)
- Datos de ubicación (PLMN visitado, MME)
- Información del perfil de servicio

Requisitos de Cumplimiento:

- **GDPR** - Asegurarse de que los datos del webhook se procesen en cumplimiento con el GDPR
 - **Retención de datos** - Implementar políticas adecuadas de retención de datos
 - **Control de acceso** - Restringir el acceso al endpoint del webhook
 - **Cifrado** - Usar TLS para el transporte de webhooks
 - **Registro de auditoría** - Registrar todas las entregas de webhooks para cumplimiento
-

Solución de Problemas

Webhook No Recibido

Síntomas:

- Ocurren eventos pero el webhook no se activa
- El endpoint de webhook nunca recibe solicitudes

Pasos de Solución de Problemas:

1. Verificar que el webhook esté habilitado:

```
curl -k https://hss.example.com:8443/api/webhook  
# Verificar "enabled": true
```

2. Comprobar la configuración de eventos del webhook:

- Asegúrate de que el tipo de evento esté incluido en la lista de `events` del webhook
- Ejemplo: Si deseas eventos `ims_registration`, verifica que esté en el array de eventos

3. Revisar los registros de HSS:

- Verificar errores de entrega de webhook
- Buscar problemas de conectividad de red
- Verificar que no haya fallos en la resolución de DNS

4. Probar la accesibilidad del endpoint:

```
curl -X POST https://your-server.com/omnihss-webhook \  
-H "Content-Type: application/json" \  
-d '{"test": true}'
```

Tiempo de espera del Webhook

Síntomas:

- Los registros de HSS muestran errores de tiempo de espera del webhook
- El endpoint del webhook recibe la solicitud pero HSS la marca como fallida

Solución:

1. Responder inmediatamente:

- Devolver HTTP 200 dentro de los 5 segundos
- Procesar datos de forma asíncrona después de responder

2. Optimizar el rendimiento del endpoint:

```
// MALO - Procesamiento sincrónico lento
app.post('/webhook', (req, res) => {
  processData(req.body); // Bloquea durante 10 segundos
  res.status(200).send();
});

// BUENO - Procesamiento asíncrono después de la respuesta
app.post('/webhook', (req, res) => {
  res.status(200).send(); // Responder inmediatamente
  processData(req.body); // Procesar de forma asíncrona
});
```

Webhooks Duplicados

Síntomas:

- El mismo evento se entrega múltiples veces
- `event_id` es idéntico para entregas duplicadas

Causa:

- Reintentos de red (aunque OmniHSS no reintenta, la infraestructura de red podría)
- Múltiples webhooks registrados para el mismo evento

Solución:

Implementar idempotencia utilizando `event_id`:

```

const processedEvents = new Set();

app.post('/omnihss-webhook', (req, res) => {
  const eventId = req.body.event_id;

  if (processedEvents.has(eventId)) {
    // Ya procesado, omitir
    return res.status(200).json({ status: 'duplicate' });
  }

  processedEvents.add(eventId);

  // Procesar webhook...
  processWebhook(req.body);

  res.status(200).json({ status: 'processed' });
});

```

El Webhook Devuelve un Error

Síntomas:

- El endpoint devuelve HTTP 4xx o 5xx
- Los registros de HSS indican fallo en la entrega del webhook

Errores Comunes:

- 1. 401 No Autorizado** - La verificación de la firma falló
 - Verificar que el secreto del webhook coincida con la configuración
 - Verificar el algoritmo de cálculo de la firma
- 2. 400 Solicitud Incorrecta** - Carga útil inválida
 - Verificar el análisis de la carga útil del webhook
 - Asegurarse de que se maneje el encabezado Content-Type
- 3. 500 Error Interno del Servidor** - El endpoint falló
 - Revisar los registros de errores del endpoint

- Agregar manejo de errores y registro

Solución:

Agregar manejo de errores integral:

```
app.post('/omnihss-webhook', async (req, res) => {
  try {
    // Verificar firma
    if (!verifyWebhook(req)) {
      return res.status(401).json({ error: 'Firma inválida' });
    }

    // Validar carga útil
    if (!req.body.event || !req.body.subscriber) {
      return res.status(400).json({ error: 'Carga útil inválida'
    });
    }

    // Procesar webhook
    await processWebhook(req.body);

    res.status(200).json({ status: 'ok' });

  } catch (error) {
    console.error('Error en el procesamiento del webhook:',
error);
    // Devolver 200 para prevenir reintentos, registrar error para
investigación
    res.status(200).json({ status: 'error', message: error.message
  });
  }
});
```

Falta de Datos del Suscriptor

Síntomas:

- Webhook recibido pero el objeto del suscriptor está incompleto
- Los campos esperados son nulos o faltan

Causas Posibles:

1. **Suscriptor no completamente provisionado** - Algunos perfiles pueden ser opcionales (IMS, itinerancia)
2. **Condición de carrera de datos** - Suscriptor actualizado entre el disparador del evento y el envío del webhook

Solución:

Manejar campos opcionales de manera adecuada:

```
const { subscriber } = req.body;

// Verificar campos opcionales
const imsProfile = subscriber.ims_profile || { name: 'Sin IMS' };
const roamingProfile = subscriber.roaming_profile || { name: 'Sin Itinerancia' };

// Manejar MSISDNs faltantes
const msisdns = subscriber.msisdns || [];
```

Monitoreo y Observabilidad

Métricas del Webhook

Rastrear el rendimiento y la confiabilidad del webhook:

Métricas a Monitorear:

- Tasa de entrega del webhook (exitosa vs. fallida)
- Latencia del webhook (tiempo desde el evento hasta la respuesta del endpoint)
- Tiempos de respuesta del endpoint
- Tasas de error por endpoint
- Eventos por segundo

Ejemplo de Consulta de Dashboard (Prometheus/Grafana):

```
# Tasa de éxito del webhook
rate(omnihss_webhook_success_total[5m]) /
rate(omnihss_webhook_attempts_total[5m])

# Latencia del webhook
histogram_quantile(0.95, omnihss_webhook_duration_seconds)
```

Registros del Webhook

Habilitar el registro detallado del webhook para solucionar problemas:

Formato de Registro:

```
{
  "timestamp": "2025-01-15T14:30:00Z",
  "level": "info",
  "component": "webhook",
  "event_id": "550e8400-e29b-41d4-a716-446655440000",
  "webhook_id": "4e5d6c7b-8a9f-4b0c-8d1e-2f3a4b5c6d7e",
  "event_type": "update_location_request",
  "subscriber_imsi": "001001123456789",
  "endpoint": "https://your-server.com/omnihss-webhook",
  "http_status": 200,
  "duration_ms": 145,
  "error": null
}
```

[← Volver a la Guía de Operaciones](#) | [Siguiente: Referencia de API](#) →

