

Guía de Operaciones de OmniHSS

Introducción

OmniHSS es una implementación de un Servidor de Suscriptor en el Hogar (HSS) diseñada para redes 4G LTE (EPC) e IMS (Sistema de Multimedia por IP). Como la base de datos central y el centro de autenticación para redes móviles, OmniHSS gestiona las credenciales de los suscriptores, los datos del perfil y proporciona servicios de autenticación y autorización tanto para servicios de datos como de voz.

Construido sobre Elixir y la máquina virtual Erlang, OmniHSS ofrece alta disponibilidad, tolerancia a fallos y escalabilidad requeridas para la infraestructura moderna de telecomunicaciones.

¿Qué es un Servidor de Suscriptor en el Hogar?

El HSS es un componente crítico en las redes LTE e IMS que:

- **Almacena datos de suscriptores** - Credenciales, información del perfil y suscripciones a servicios
- **Realiza autenticación** - Valida a los suscriptores que intentan acceder a la red
- **Gestiona autorización** - Controla qué servicios pueden acceder los suscriptores
- **Rastrea ubicación** - Mantiene información de ubicación actual para el enrutamiento
- **Controla roaming** - Aplica políticas de roaming basadas en redes visitadas

- **Gestiona equipos** - Funciona como Registro de Identidad de Equipos (EIR) para el control de dispositivos

Características Clave

Características Operativas

- **Interfaz S6a** - Autenticación y gestión de ubicación para redes LTE/EPC
- **Interfaz Cx** - Registro y autenticación IMS
- **Interfaz Sh** - Acceso a datos de perfil IMS y notificaciones de suscripción
- **Interfaz S13** - Verificación de Identidad de Equipos (OmniHSS funciona como EIR)
- **Interfaz Gx** - Control de Políticas y Cargos (OmniHSS funciona como PCRF)
- **Interfaz Rx** - Control de políticas de medios IMS (OmniHSS funciona como PCRF)
- **Control de Roaming** - Control granular sobre datos y roaming IMS por PLMN
- **Múltiples MSISDNs** - Soporte para múltiples números de teléfono por suscriptor
- **API RESTful** - API de aprovisionamiento completa para integración (también utilizada por OmniHLR)
- **Panel de Control Web** - Monitoreo en tiempo real y estado del sistema

Integración de Elementos de Red

OmniHSS se integra con los siguientes elementos de red:

- **MME** (Entidad de Gestión de Movilidad) - Gestión de movilidad y sesiones LTE
- **P-GW** (Puerta de Enlace PDN) - Recibe políticas de OmniHSS (función PCRF)
- **P-CSCF** (Función de Control de Sesiones de Llamadas Proxy) - Autorización de medios IMS
- **I-CSCF** (CSCF Interrogante) - Consultas de enrutamiento IMS
- **S-CSCF** (CSCF de Servicio) - Registro y autenticación IMS

- **AS** (Servidor de Aplicaciones) - Acceso a datos de suscriptores IMS
- **OmniHLR** - HLR heredado que se comunica con OmniHSS a través de API

Estructura de la Documentación

Esta guía de operaciones está organizada en los siguientes documentos:

Documentación Central

- **Descripción de la Arquitectura** - Arquitectura del sistema, componentes y pila Diameter
- **Guía de Configuración** - Referencia de configuración completa con ejemplos
- **Relaciones de Entidades** - Modelo de datos y relaciones de entidades

Guías Operativas

- **Panel de Control** - Uso de la interfaz de monitoreo basada en web
- **Métricas y Monitoreo** - Monitoreo del sistema y chequeos de salud
- **Guía de Solución de Problemas** - Diagnóstico y resolución de problemas comunes
- **Referencia de API** - Documentación completa de los puntos finales de la API
- **Webhooks** - Notificaciones de eventos en tiempo real e integración

Documentación de Características

- **Gestión de Perfiles** - Perfiles EPC, IMS, APN y de roaming
- **Control de Roaming** - Configuración de políticas de roaming
- **Flujos de Protocolo** - Procedimientos del protocolo Diameter y flujos de mensajes
- **PCRF** - Función de Reglas de Políticas y Cargos (interfaces Gx/Rx, QoS, VoLTE)
- **EIR** - Registro de Identidad de Equipos (interfaz S13, validación IMEI)

- **Características Multi-MSISDN y Multi-IMSI** - Soporte para múltiples números de teléfono y múltiples IMSI

Alta Disponibilidad

- **Replicación de Base de Datos Galera** - Clúster de múltiples nodos para implementaciones HA

Inicio Rápido para Operaciones

Accediendo al Sistema

Panel de Control (Interfaz Web)

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

El Panel de Control proporciona monitoreo en tiempo real de suscriptores y pares Diameter.

Punto Final de API

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

La API RESTful permite el aprovisionamiento y la gestión de suscriptores.

Archivos de Configuración Clave

- `config/runtime.exs` - Configuración en tiempo de ejecución (base de datos, Diameter, configuraciones de red)
- `priv/cert/` - Certificados TLS para HTTPS y Diameter

Operaciones Esenciales

1. **Verificar Estado del Sistema** - Acceder a la página de Resumen del Panel de Control

2. **Monitorear Pares Diameter** - Acceder a la página Diameter del Panel de Control
3. **Consultar Suscriptor** - Usar el punto final de API `/api/subscriber/imsi/:imsi`
4. **Ver Base de Datos** - Conectarse a la Base de Datos SQL en el hostname configurado

Soporte y Solución de Problemas

Archivos de Registro

Los registros del sistema se envían a stdout/stderr y pueden ser capturados por su gestor de procesos (systemd, supervisord, etc.).

Comprobaciones Comunes

- **Conectividad Diameter** - Verificar la página Diameter para el estado de los pares
- **Conectividad de Base de Datos** - Verificar la configuración de la base de datos en runtime.exs
- **Fallos de autenticación de suscriptores** - Verificar el estado del suscriptor para contar fallos

Monitoreo de Salud

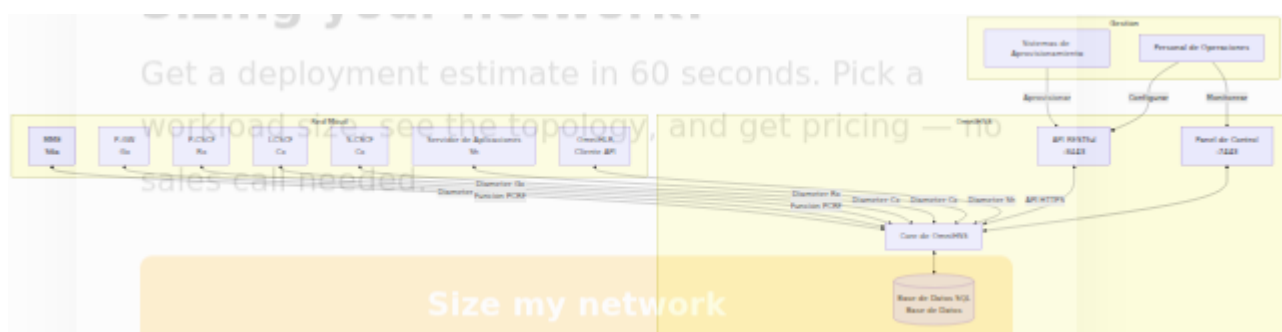
- **Chequeo de Salud de API** - `GET /api/status`
- **Panel de Control** - Acceder a cualquier página del Panel de Control
- **Base de Datos** - Conectarse a la Base de Datos SQL y verificar el acceso a las tablas

Consideraciones de Seguridad

- **TLS Requerido** - Tanto la API como el Panel de Control utilizan HTTPS

- **Gestión de Certificados** - Los certificados en `priv/cert/` deben ser válidos
- **Seguridad de la Base de Datos** - Asegurar las credenciales de la base de datos en `runtime.exs`
- **Aislamiento de Red** - La interfaz Diameter debe estar en la red de gestión
- **Autenticación de API** - Considerar implementar autenticación para uso en producción

Arquitectura a Gran Escala



Próximos Pasos

Para procedimientos operativos detallados, consulte las secciones de documentación específicas:

- Comience con **Descripción de la Arquitectura** para entender los componentes del sistema
- Revise **Guía de Configuración** para personalizar su implementación
- Explore **Panel de Control** para el monitoreo diario
- Consulte **Referencia de API** para la automatización del aprovisionamiento

Versión del Documento: 1.0

Mantenido Por: Equipo de Operaciones de Omnitouch

EIR (Registro de Identidad de Equipos)

Descripción General

El HSS incluye un EIR (Registro de Identidad de Equipos) integrado 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	Negar acceso a la red
Greylist	2	Equipo bajo observación	Permitir con monitoreo

Interfaz S13

Operaciones Soportadas

Solicitud de Verificación de Identidad de Equipos (ECR) / Respuesta de Verificación de Identidad de Equipos (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 de 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 búsqueda de 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 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 (fallback)

- 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 (fallback 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 (fallback final)

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

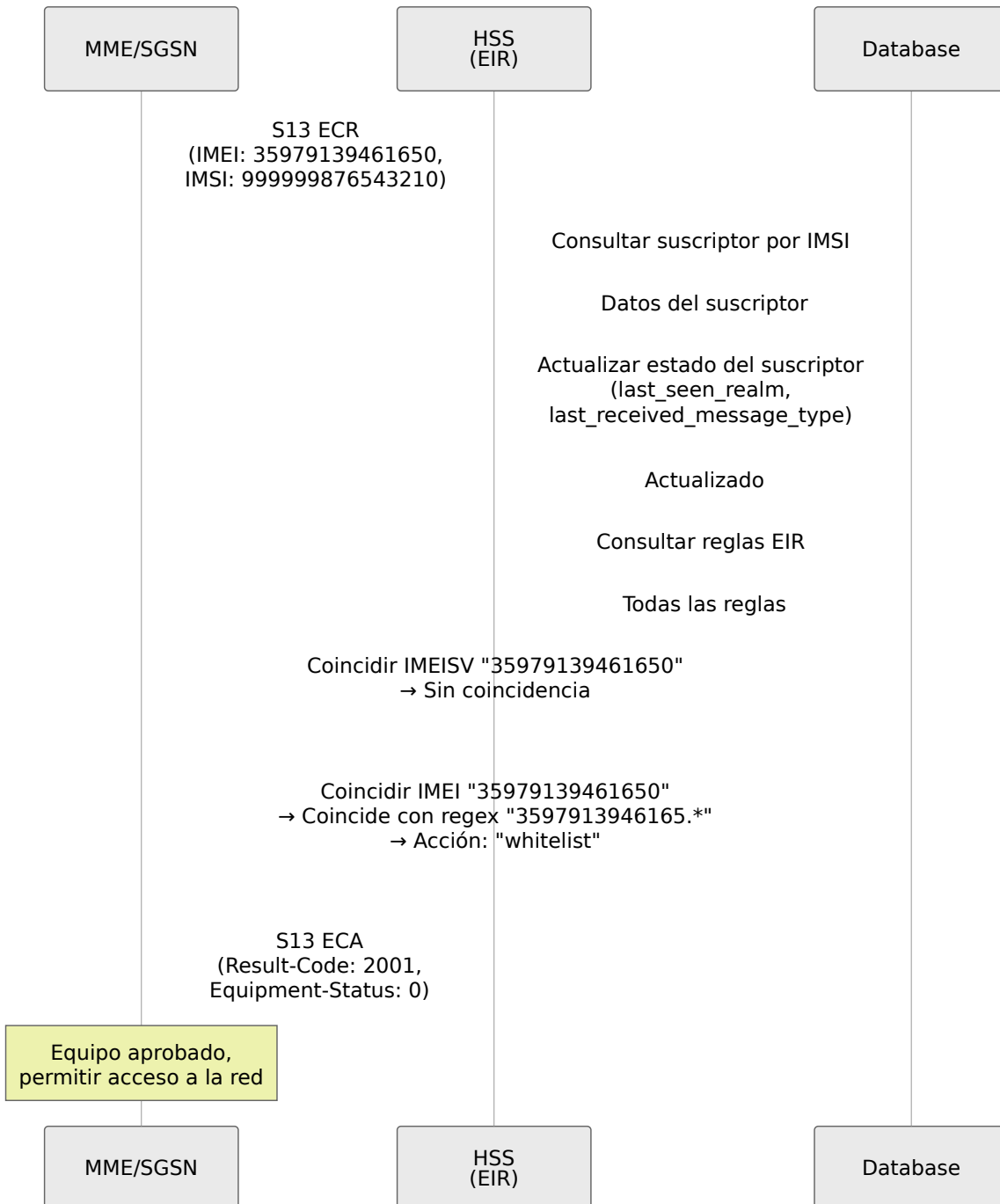
- `:greylist` - Observar equipo desconocido (moderado)
- `:reject_unknown_equipment` - Devolver error 5422 (estricto)

Ejemplos de Patrones Regex

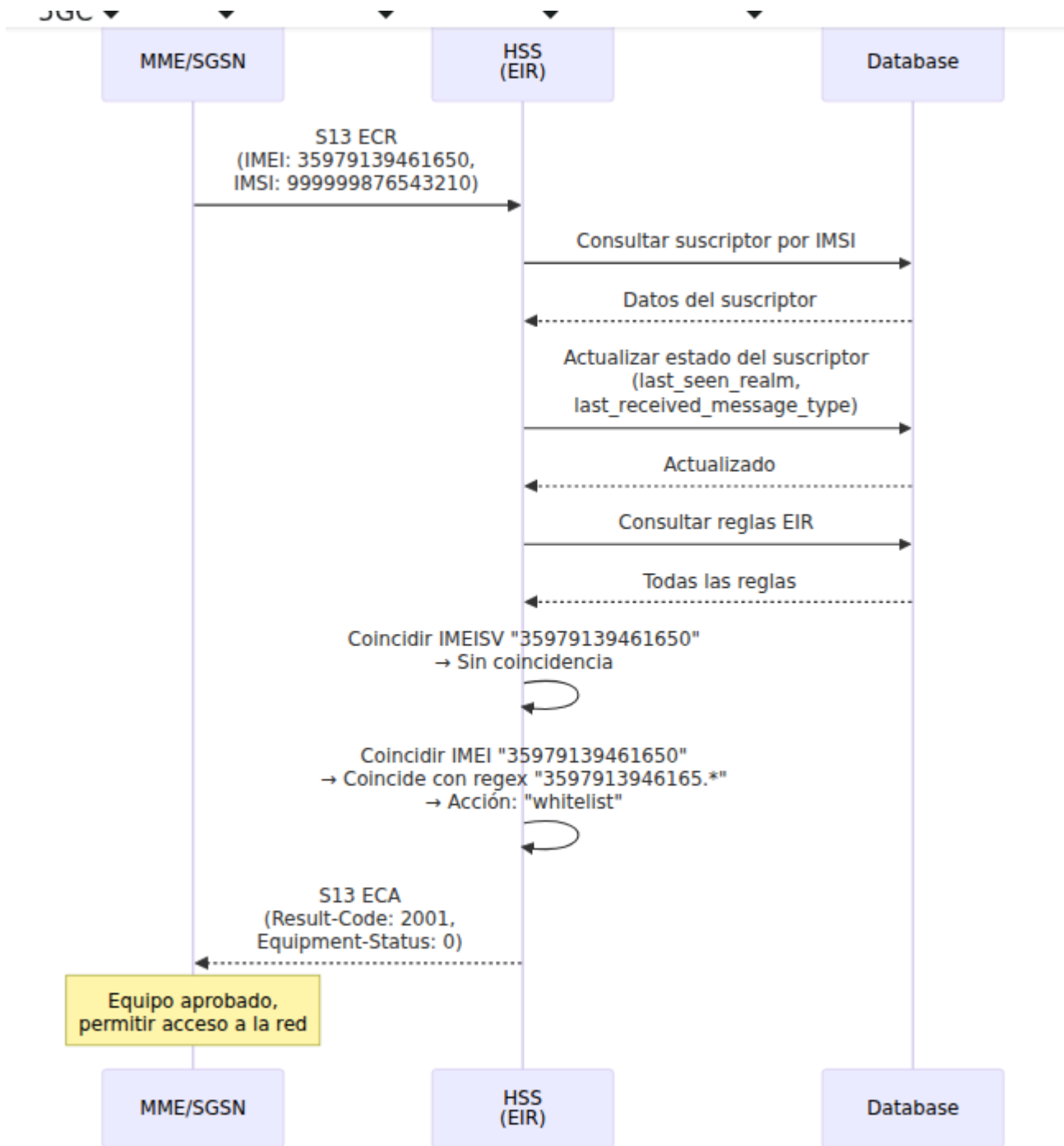
Patrón	Coincide	Caso de Uso
<code>"35979139461650"</code>	IMEI exacto	Lista blanca/lista negra de un solo dispositivo
<code>"3597913946165.*"</code>	Wildcard de prefijo IMEI	Rango de fabricante/modelo
<code>"3597913946161108"</code>	IMEISV exacto	Dispositivo específico con versión de software
<code>"999999876543210"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

Flujos de Mensajes Comunes

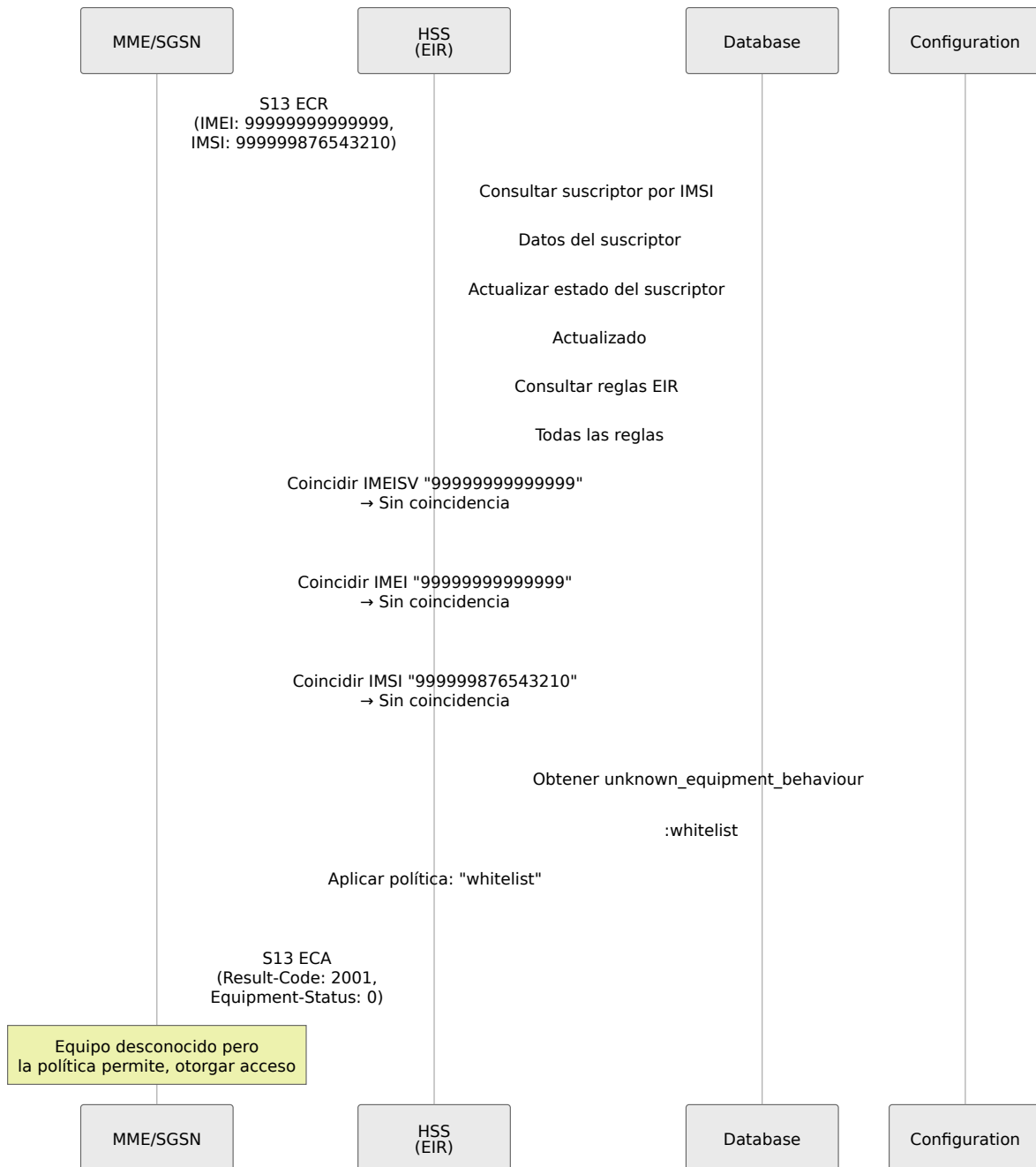
Flujo 1: Verificación de Equipo - IMEI Conocido en Lista Blanca



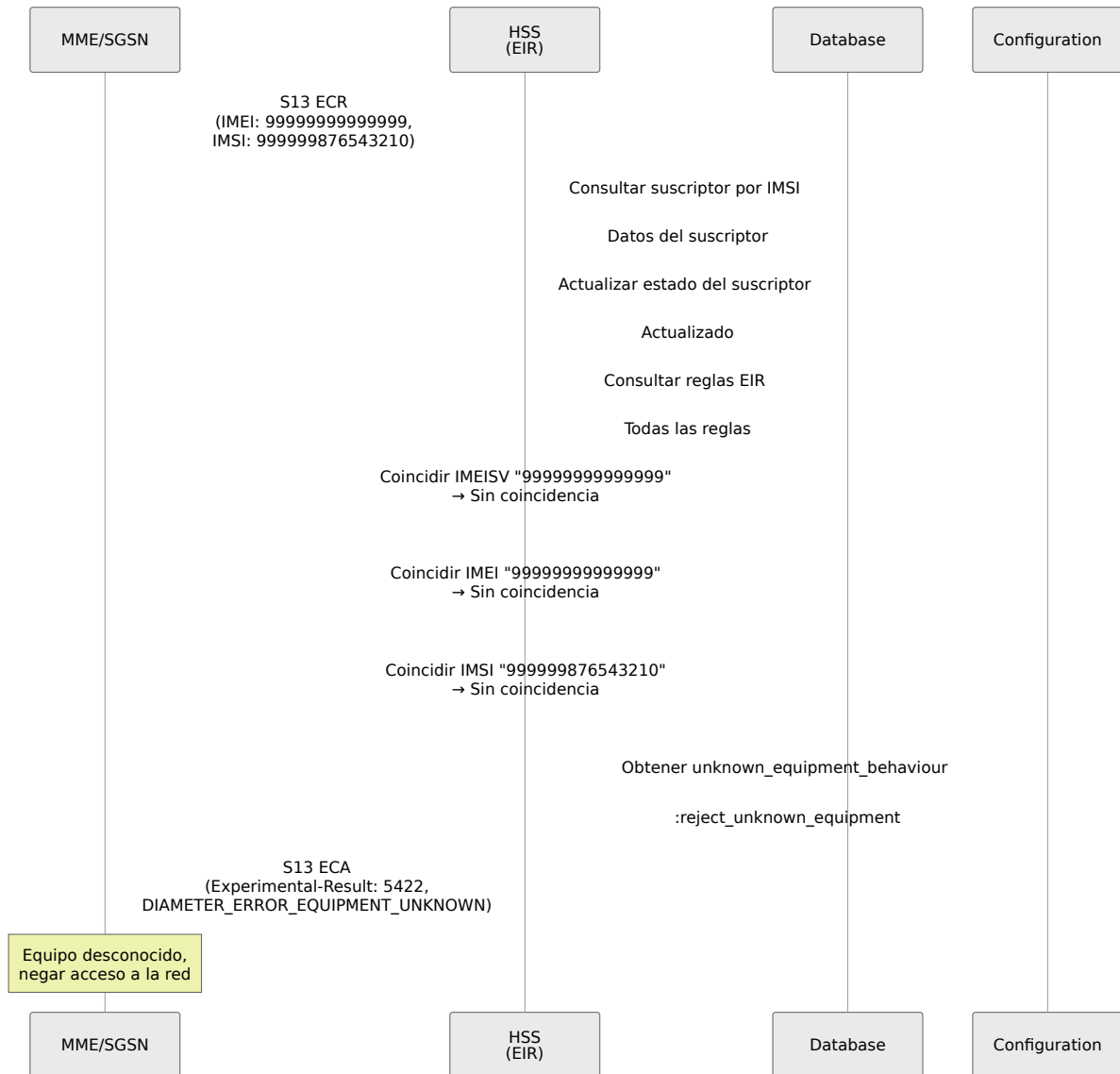
Flujo 2: Verificación de Equipo - IMEI en Lista Negra (Dispositivo Robado)



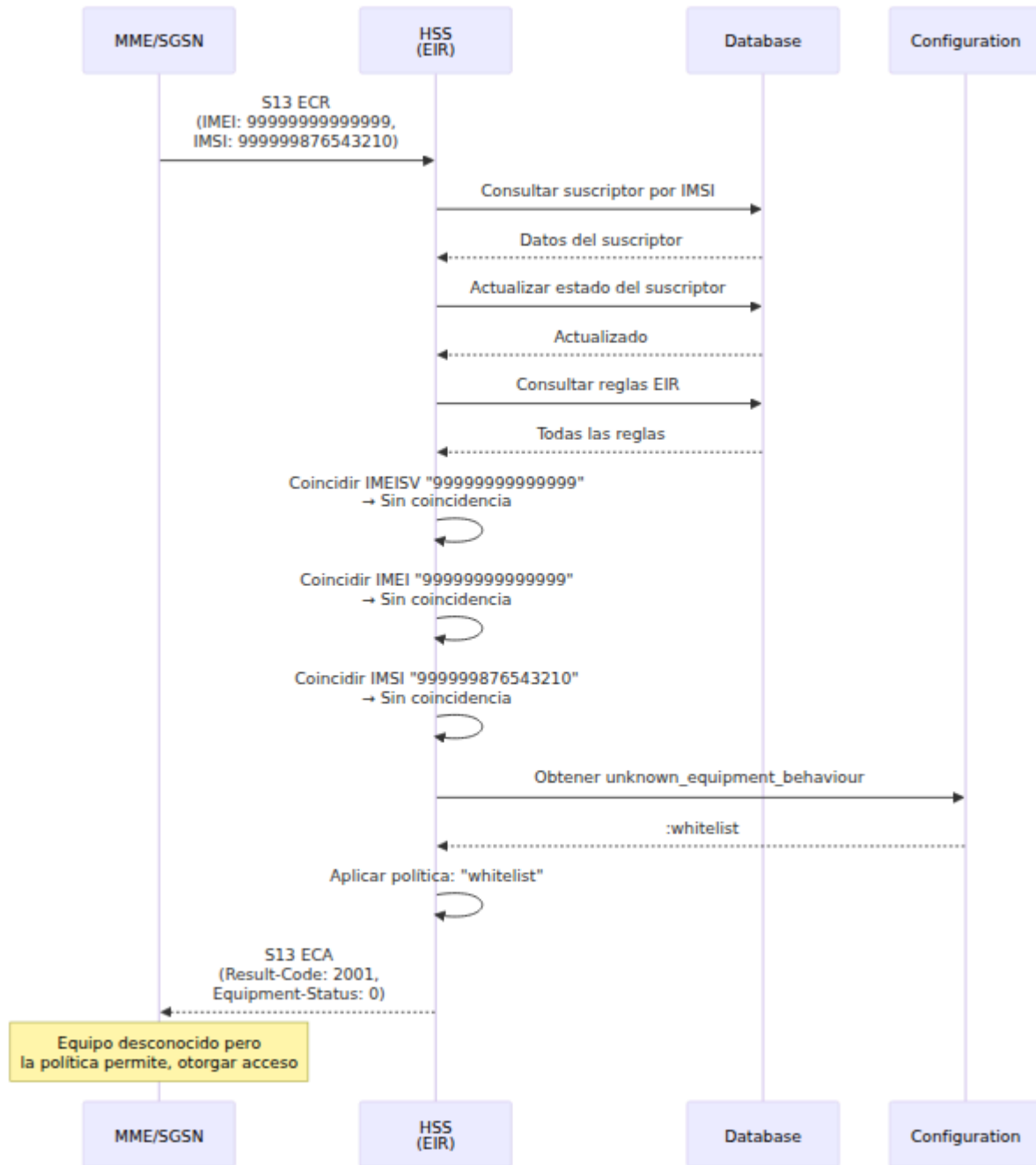
Flujo 3: Verificación de Equipo - Equipo Desconocido (Política de Lista Blanca)



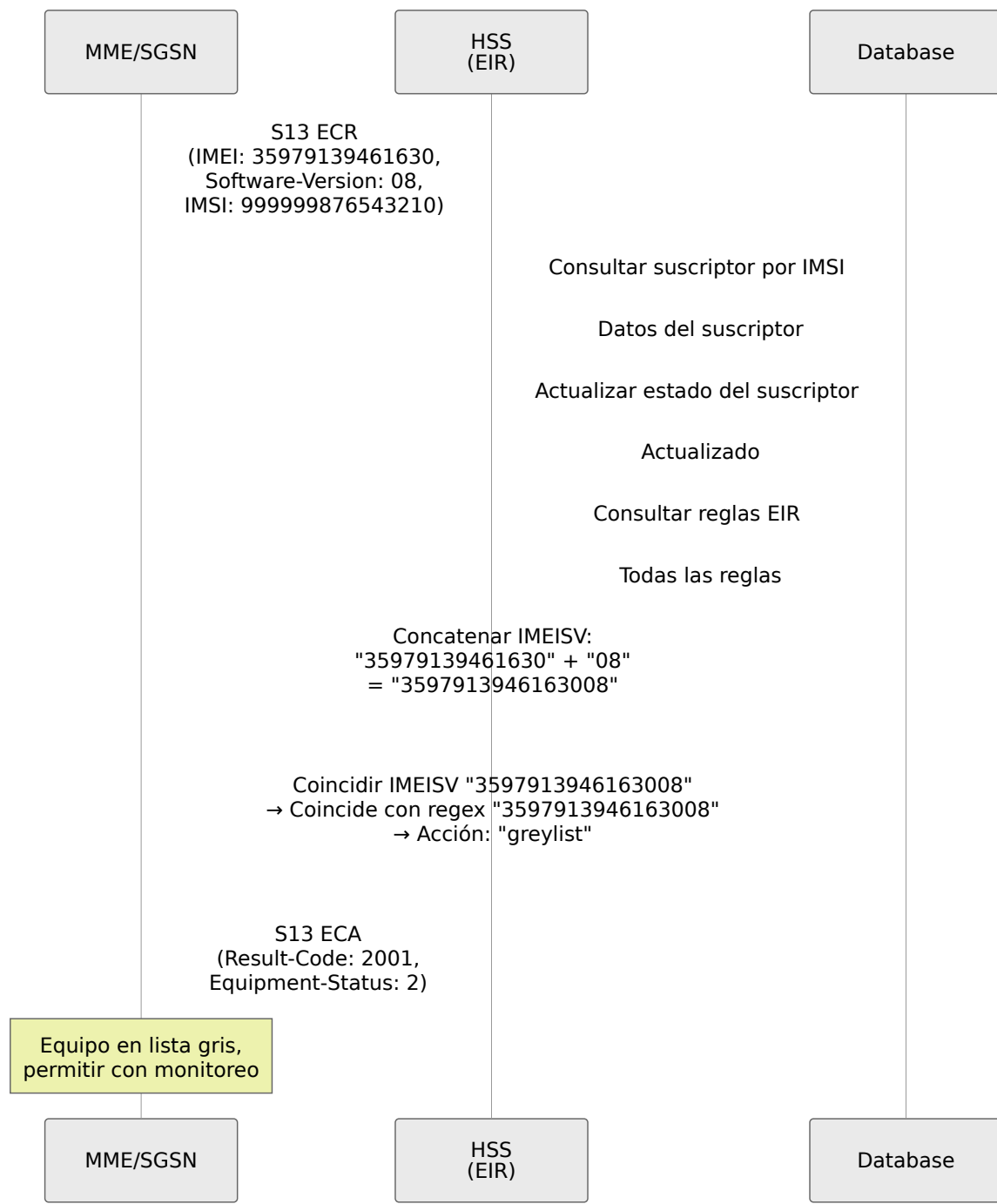
Flujo 4: Verificación de Equipo - Equipo Desconocido (Política de Rechazo)



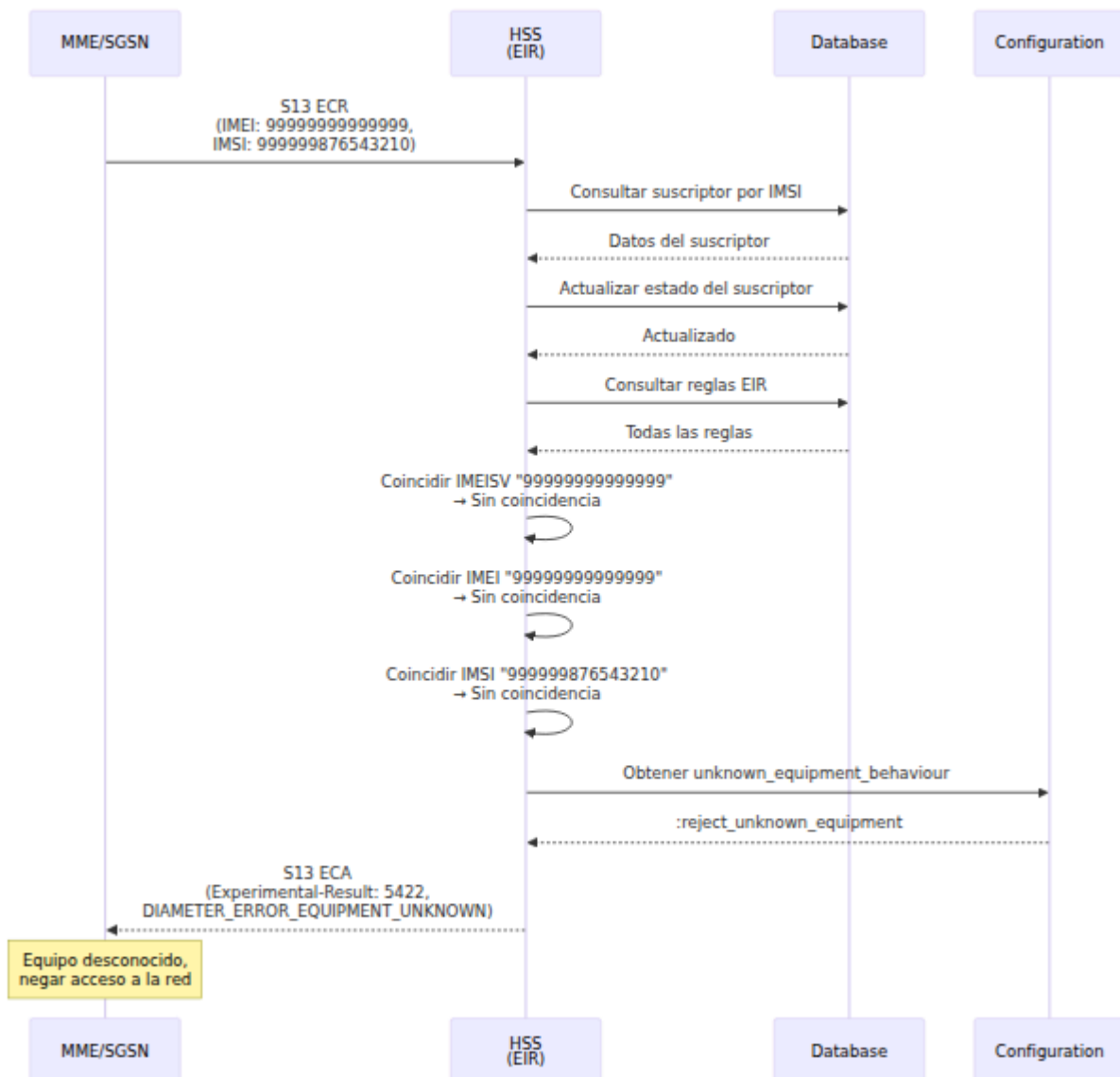
Flujo 5: Verificación de Equipo - Suscriptor Desconocido



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": 1,
      "action": "whitelist",
      "regex": "3597913946165.*",
      "inserted_at": "2025-01-15T10:30:00Z",
      "updated_at": "2025-01-15T10:30:00Z"
    },
    {
      "id": 2,
      "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": 1,
    "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": 3,
    "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": 3,
    "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": 3,
    "action": "whitelist",
    "regex": "359791394616.*"
  }
}
```

Eliminar Regla EIR

Solicitud:

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

Respuesta (HTTP 204 Sin Contenido)

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 Equipos Desconocidos

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)

- `:greylis` - 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):** `:greylis` - 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 ec cc
5422	Experimental	DIAMETER_ERROR_EQUIPMENT_UNKNOWN	Su er ec de re
5012	Experimental	DIAMETER_ERROR_UNKNOWN	Er 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 Equipos de Suscriptores

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 Versiones de Software

Escenario: Bloquear una 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 la 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 de Equipos

La búsqueda de estado de equipos 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 de IMEI en texto plano por defecto

- Utiliza búsquedas en bases de datos hash (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 los comodines amplios para asegurar que la lista negra tenga prioridad.

Limitación de Tasa

Considere implementar limitación de tasa en:

- Solicitudes S13 ECR de pares no confiables
- Modificaciones de reglas de API REST EIR
- 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

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 tanto para portadoras predeterminadas como dedicadas en redes LTE.

Capacidades Clave

- **Interfaz Gx:** Control de políticas para PGW/PCEF (Puerta de Enlace de Datos de Paquete / Función de Aplicación y Ejecución de Políticas)
- **Interfaz Rx:** Autorización y QoS para flujos de medios IMS (Subsistema Multimedia IP)
- **Gestión de Políticas Dinámicas:** 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)
- **API REST:** Control programático de la aplicación de políticas y gestión de reglas

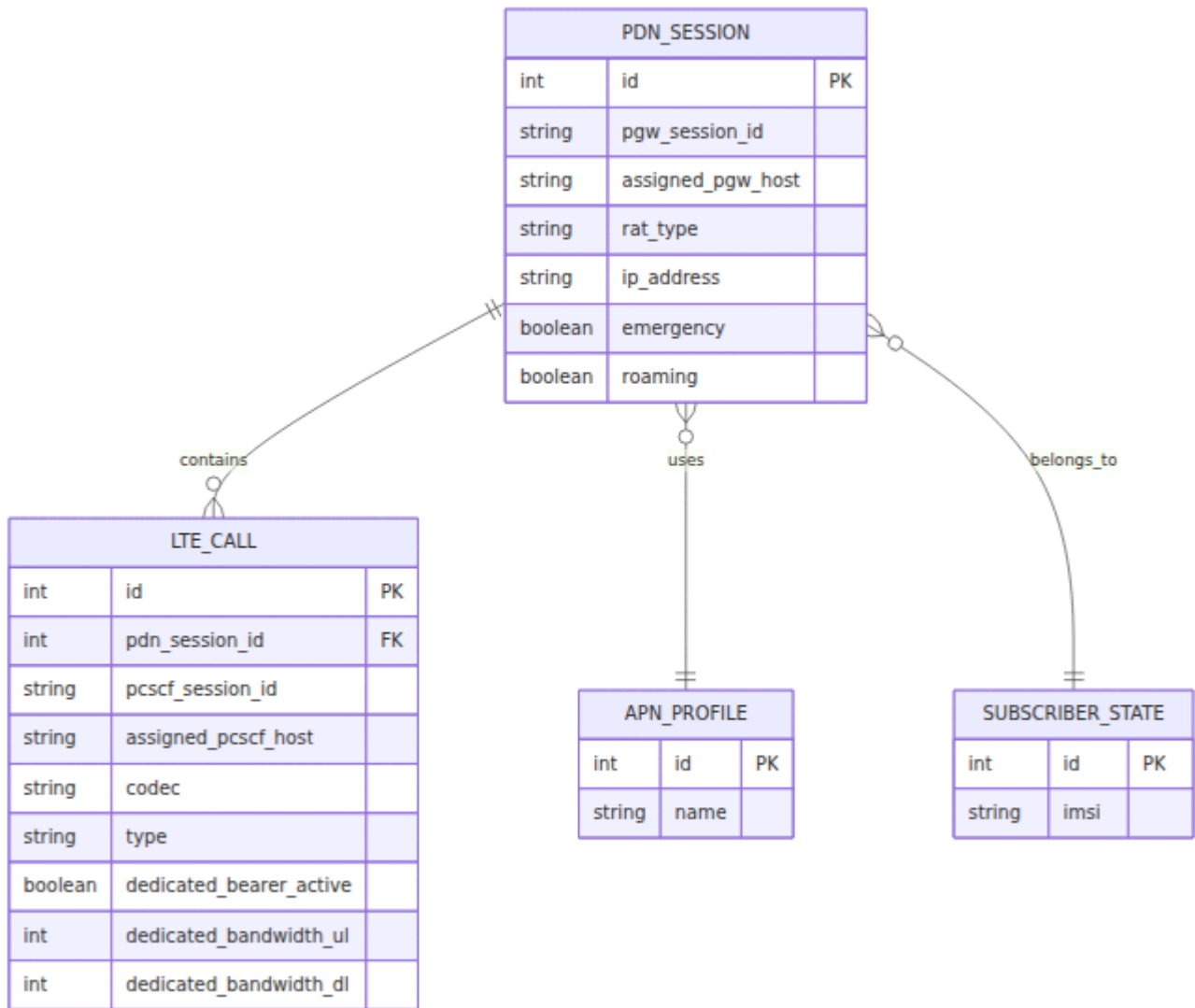
Arquitectura

Interfaces Diameter

Interfaz	ID de Aplicación	Par	Propósito
Gx	16,777,238	PGW (PCEF)	Gestión de sesiones PDN, aplicación de QoS, reglas de cargos
Rx	16,777,236	P-CSCF (AF)	Autorización de medios IMS, reserva de ancho de banda

Gestión del Estado de Sesión

El PCRF mantiene el estado de la 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

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 terminación

Respuesta: Result-Code 2001

4. Solicitud de Reautenticación (RAR)

Dirección: PCRF → PGW (HSS inicia)

Disparador:

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

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 cargos

Reglas de Cargos y Plantillas de Flujo de Tráfico

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

- **Cargos específicos 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 cargos pueden ser:

- Instaladas dinámicamente a través de Gx RAR basadas 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-tuple: 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 posterior a la 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, limitada para contenido estándar
- **Políticas basadas en tiempo** - Streaming ilimitado fuera de picos, priorización en horas pico
- **Políticas de roaming** - Cargos diferentes para uso de datos internacional frente a nacional
- **SLAs empresariales** - QoS garantizada para aplicaciones críticas para el negocio

Estructura de la Política de QoS

QoS de Portadora Predeterminada (del perfil de APN):

```

{
  "QoS-Class-Identifler": 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 ser preemptado
    "Pre-emption-Vulnerability": 1    // Puede ser preemptor
  }
}

```

QoS de Portadora Dedicada (para VoLTE):

```

{
  "QoS-Class-Identifler": 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 la 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 5-tuple)
- 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)

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

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

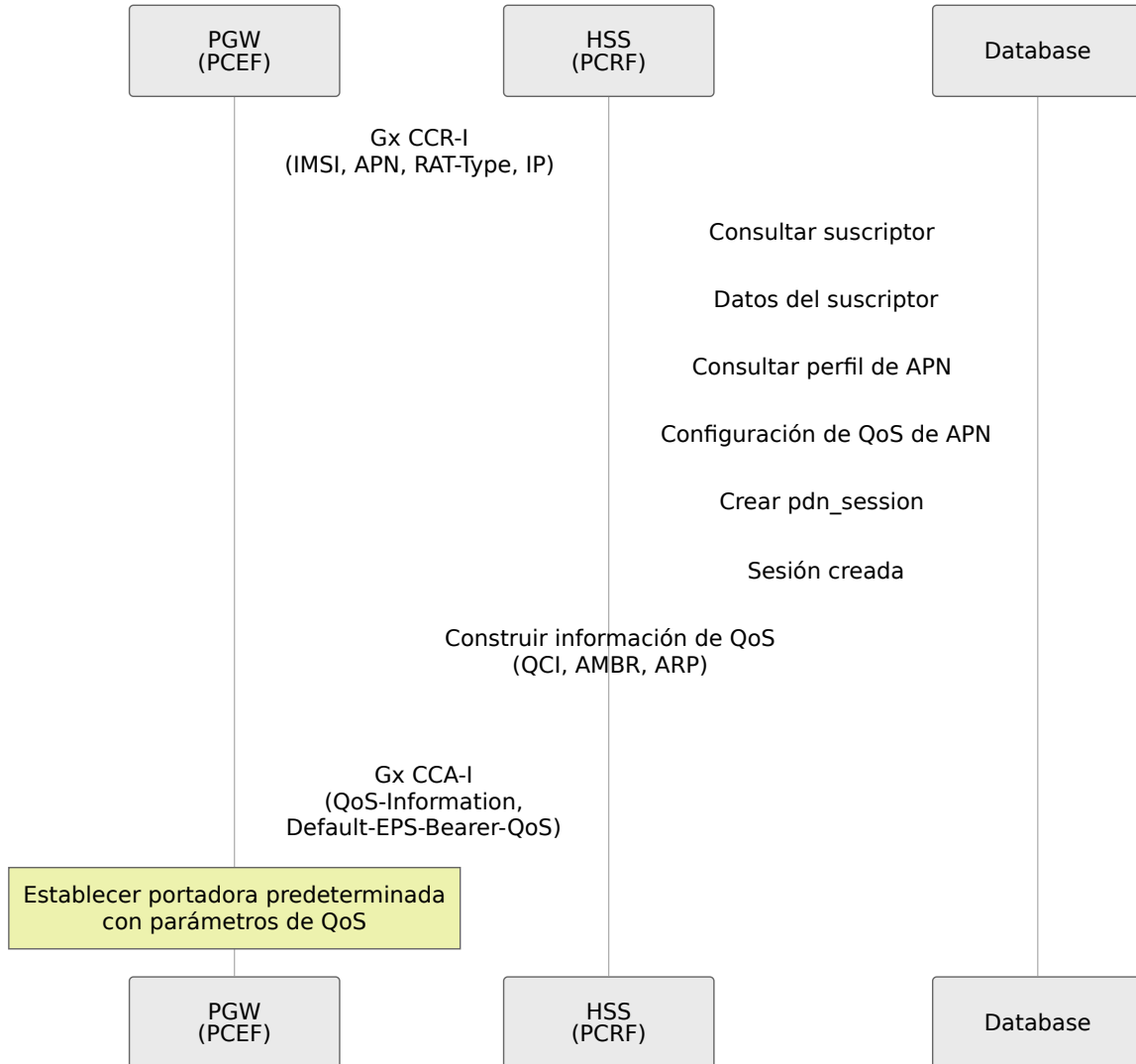
Acciones del PCRF:

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 STA

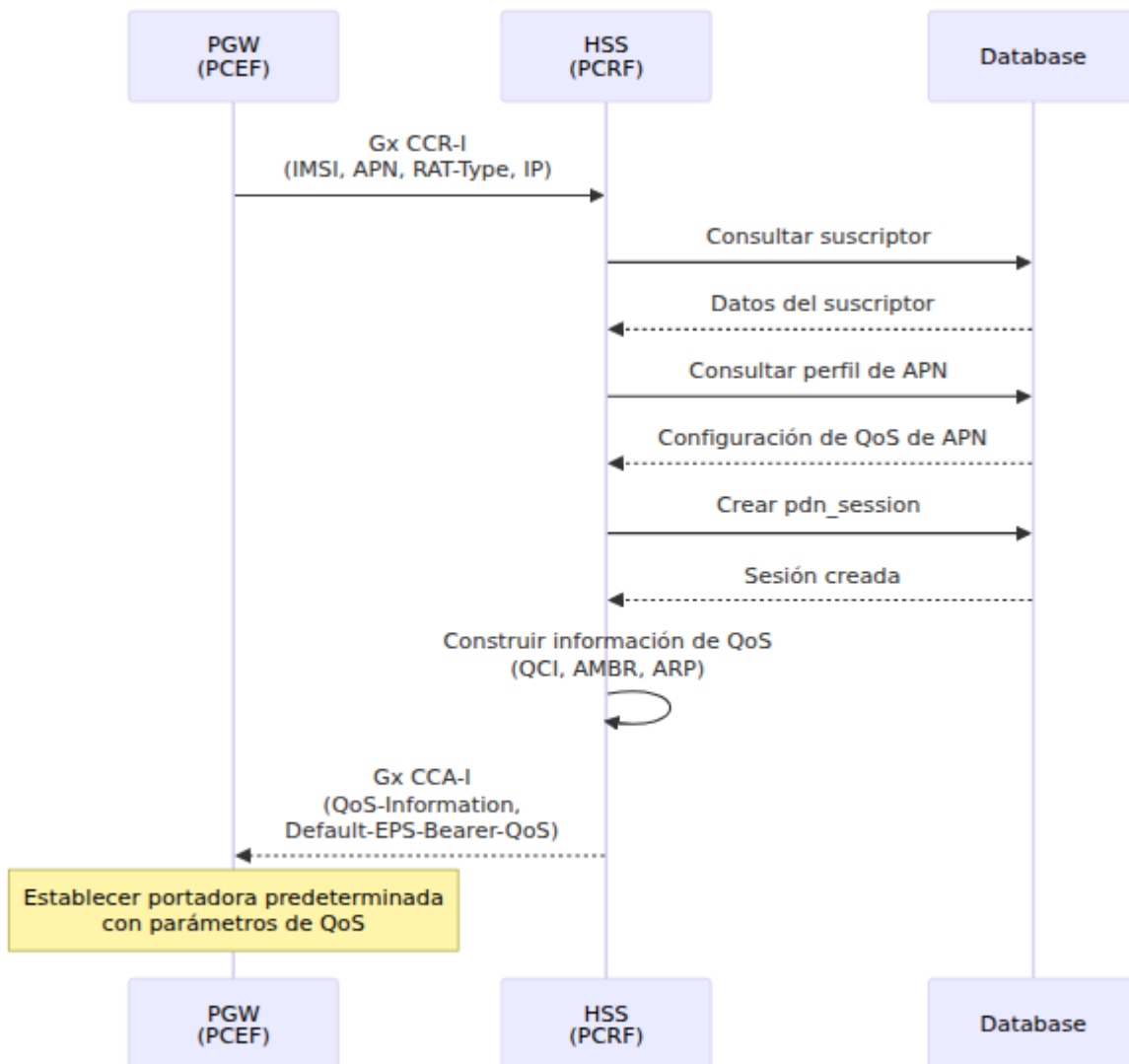
Respuesta: Result-Code 2001

Flujos de Mensajes Comunes

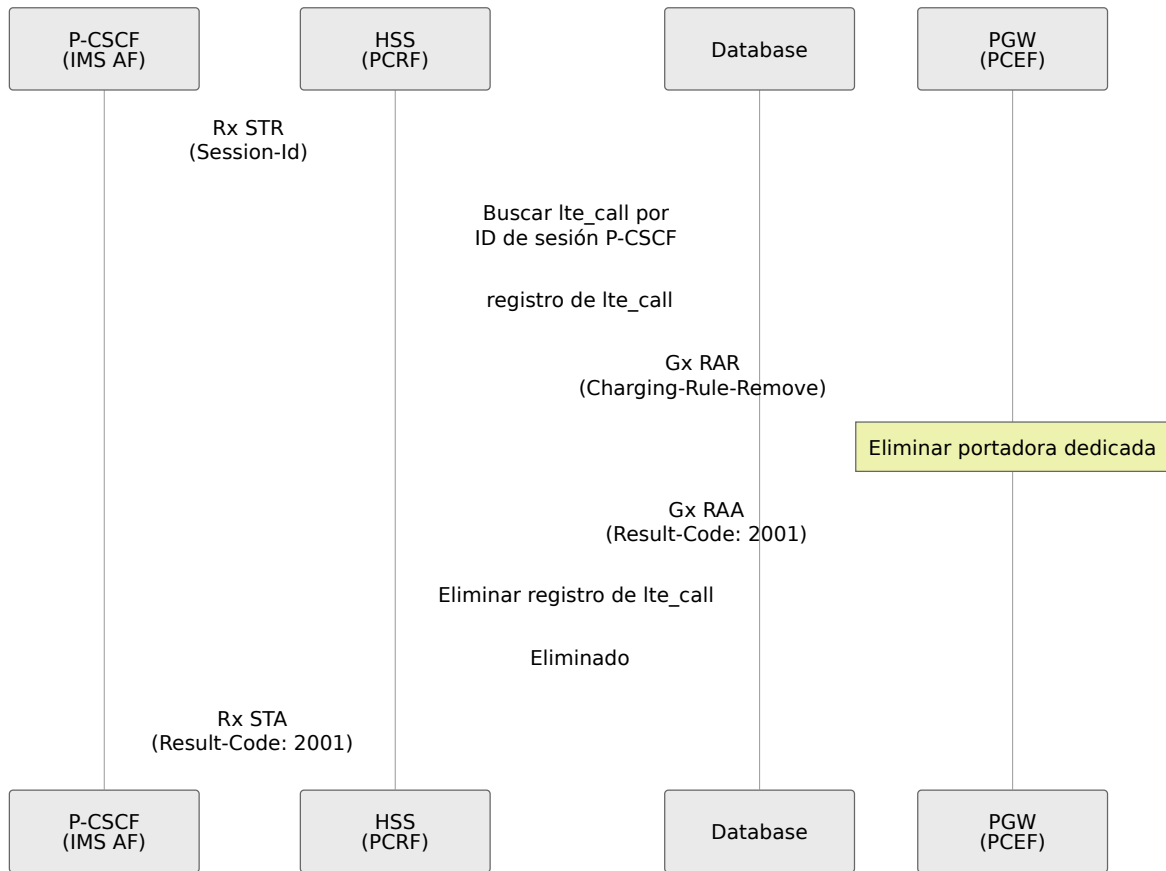
Flujo 1: Establecimiento de Sesión PDN



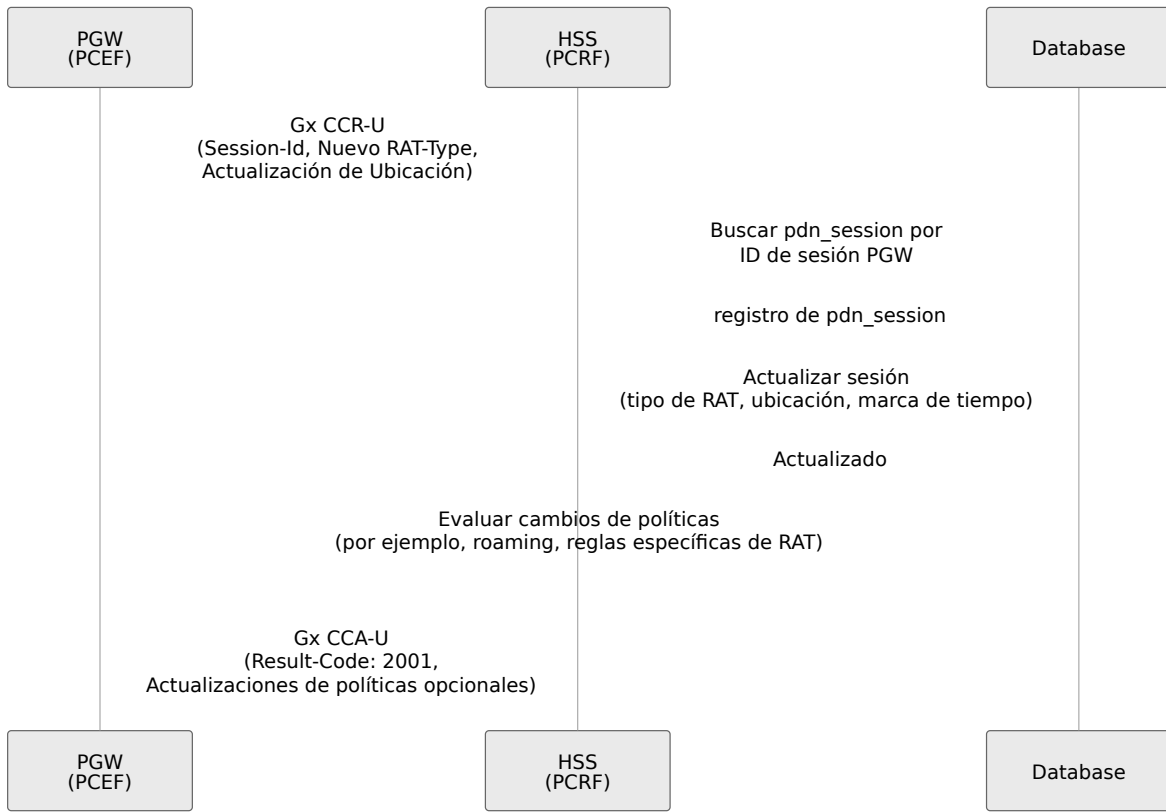
Flujo 2: Configuración de Llamada VoLTE (Rx AAR → Gx RAR)



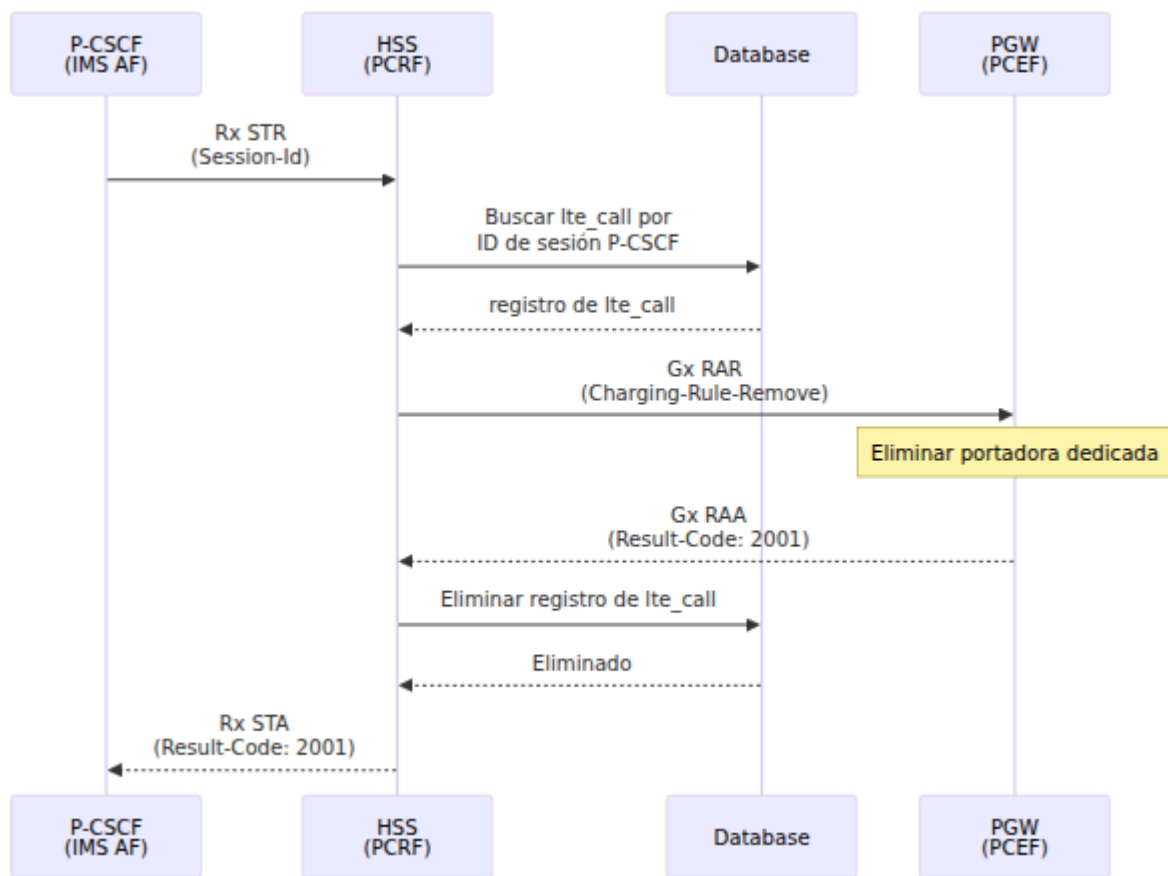
Flujo 3: Desconexión de Llamada VoLTE (Rx STR → Gx RAR)



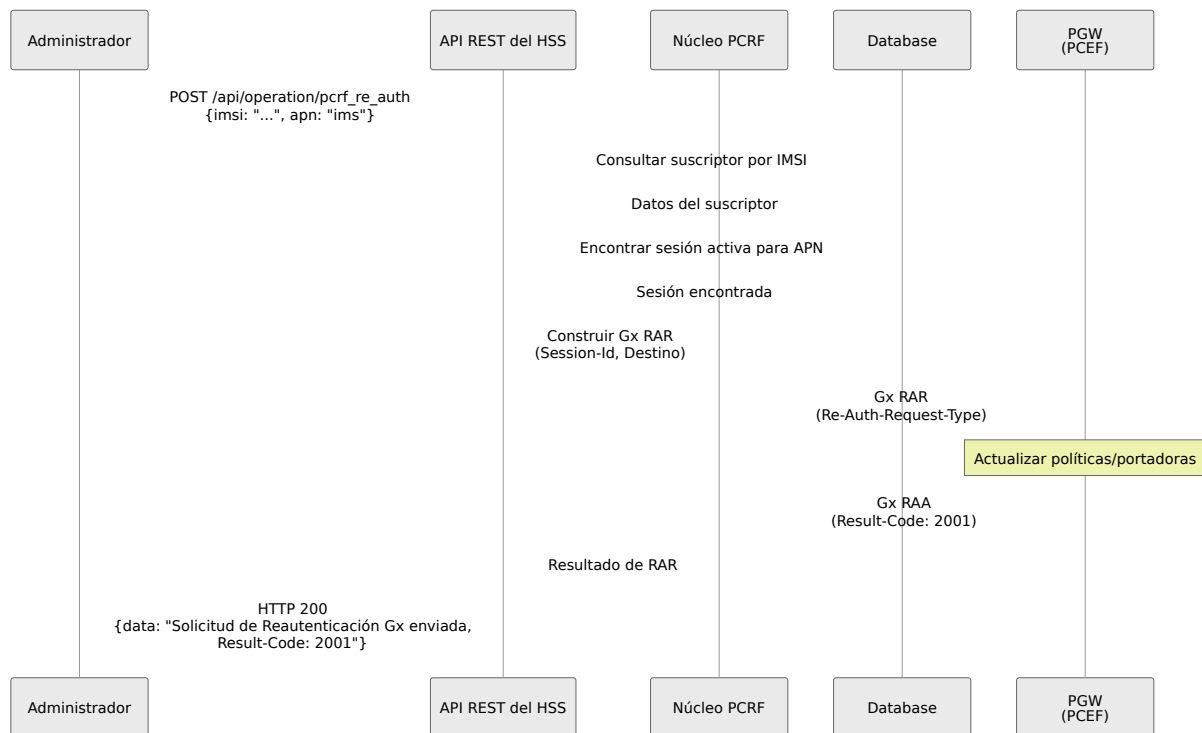
Flujo 4: Actualización de Sesión PDN



Flujo 5: Terminación de Sesión PDN



Flujo 6: Reautenticación Manual a través de API REST



API REST

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 rutinarias (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 puede 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 las configuraciones de APN almacenadas en la base de datos. Estas políticas pueden ser creadas y gestionadas a través de la API REST.

Aplicación Automática de Políticas: Cuando actualiza un perfil de QoS de APN (por ejemplo, cambia los 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 políticas 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

Definir el nombre de 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" - Doble pila (tanto IPv4 como IPv6)
- "ipv4_or_ipv6" - La red decide (ya sea IPv4 o IPv6)

Respuesta (HTTP 201):

```
{
  "data": {
    "id": 1,
    "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

Definir 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
  }
}
```

Parámetros de QoS:

Campo	Tipo	Rango	Descripción
<code>name</code>	string	1-254 chars	Nombre del perfil (único)
<code>qci</code>	integer	1-254	Identificador de Clase de QoS (1-4 = GBR, 5-9 = No-GBR)
<code>allocation_retention_priority</code>	integer	1-15	Nivel de ARP (1 = mayor prioridad)
<code>apn_ambr_dl_kbps</code>	integer	1-4,294,967,293	Tasa Máxima Agregada de Bit Rate Descendente de APN (kbps)
<code>apn_ambr_ul_kbps</code>	integer	1-4,294,967,293	Tasa Máxima Agregada de Bit Rate Ascendente de APN (kbps)
<code>pre_emption_capability</code>	boolean	true/false	Puede preemptar portadoras de menor prioridad
<code>pre_emption_vulnerability</code>	boolean	true/false	Puede ser preemptado

Campo	Tipo	Rango	Descripción
			por portadoras de mayor prioridad

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": 1,
    "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
  }
}
```

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

3. Crear Perfil de APN

Vincular 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": 1,
    "apn_qos_profile_id": 1
  }
}
```

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": 1,
    "name": "Perfil de APN de Internet",
    "apn_identifier_id": 1,
    "apn_qos_profile_id": 1
  }
}
```

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": 2, ...}}

# 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": 2, ...}}

# 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": 2,
    "apn_qos_profile_id": 2
  }
}'
# Respuesta: {"data": {"id": 2, ...}}
```

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 perfil de QoS ID 1 para aumentar ancho de banda
curl -X PATCH https://hss.example.com:8443/api/apn/qos_profile/1 \
-H "Content-Type: application/json" \
-d '{
  "apn_qos_profile": {
    "apn_ambr_dl_kbps": 150000,
    "apn_ambr_ul_kbps": 75000
  }
}'
```

Qué Ocurre 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 el perfil de QoS ID 1, todos los 100 tendrán sus límites de ancho de banda actualizados a 150 Mbps de bajada / 75 Mbps de subida en cuestión de segundos después de completar la llamada a la API.

Nota: Cuando actualiza un perfil de QoS de APN, el sistema **dispara automáticamente reautenticaciones** para todas las sesiones PDN activas que utilizan ese APN, aplicando las nuevas políticas inmediatamente 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 bajada / 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 bajada / 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 Máxima Agregada de Bit Rate Ascendente)
 - `apn_qos_profile.apn_ambr_dl_kbps` (Tasa Máxima Agregada de Bit Rate Descendente)

- `apn_qos_profile.priority_level` (Prioridad de Retención de Asignación)
- **Portadora Dedicada:** Extraído de la Descripción del Componente de Medios de Rx AAR
 - 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 está 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 Cargos** - 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 cargos** 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 la configuración de reglas de cargos avanzadas y políticas basadas en TFT.

Documentación Relacionada

- [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 de 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
- Faltan campos requeridos
- 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 externa no existen

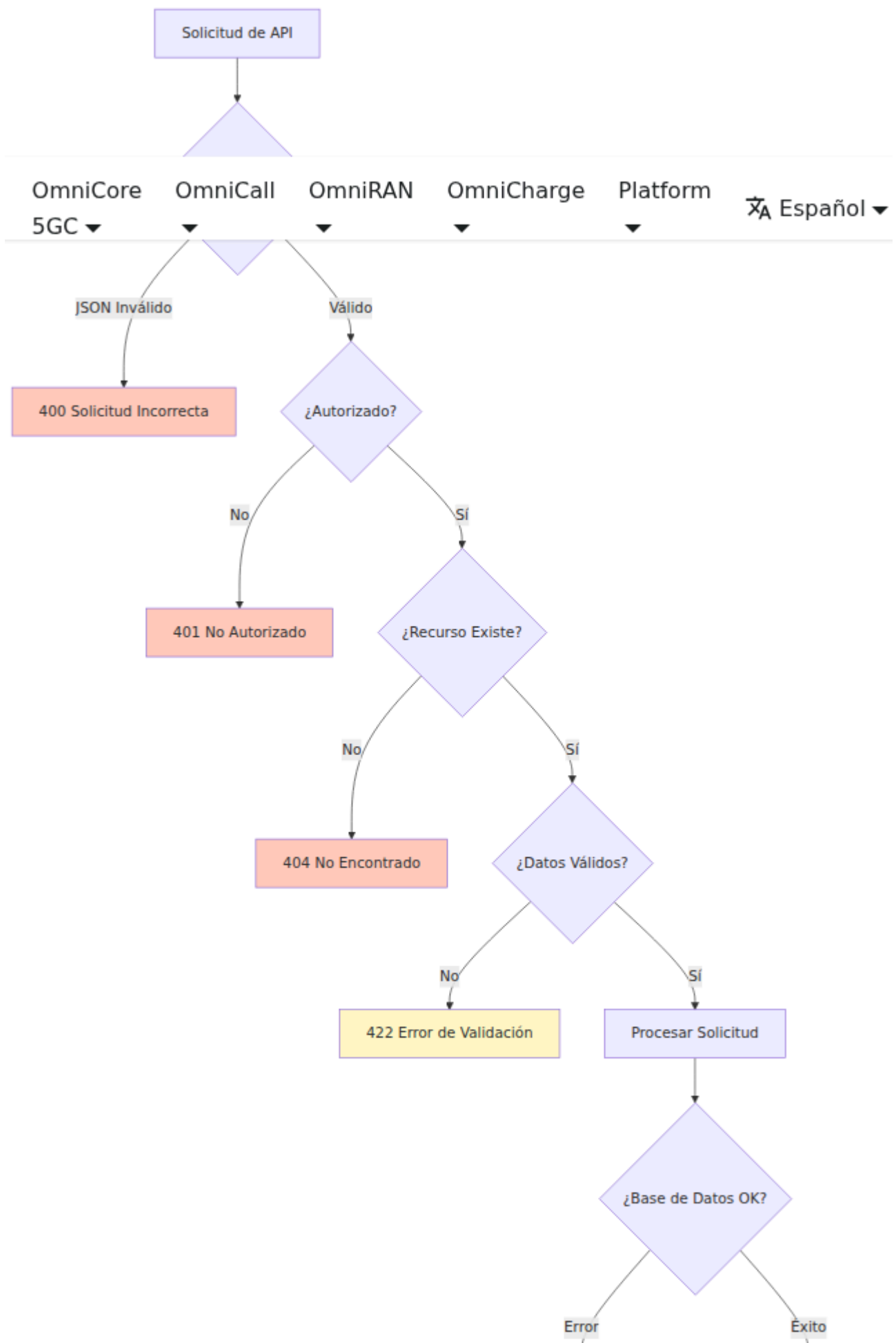
500 Error Interno del Servidor

```
{
  "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](#)
 - [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 al 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 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 exitosamente 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 suscriptora 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
-

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": "milena",  
  "amf": "8000",  
  "sqn": 0  
}' | jq -r '.response.id')
```

```
# 2. Crear Perfil 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\ ": \ "001001999999999\  
  \ "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 exitosamente!"  
echo "  ID de 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 suscriptora completa

Resultado:

Cuando este suscriptor se conecta 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 de 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](#)
 - [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": "..."}'

# ✗ 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": { ... }
}
```

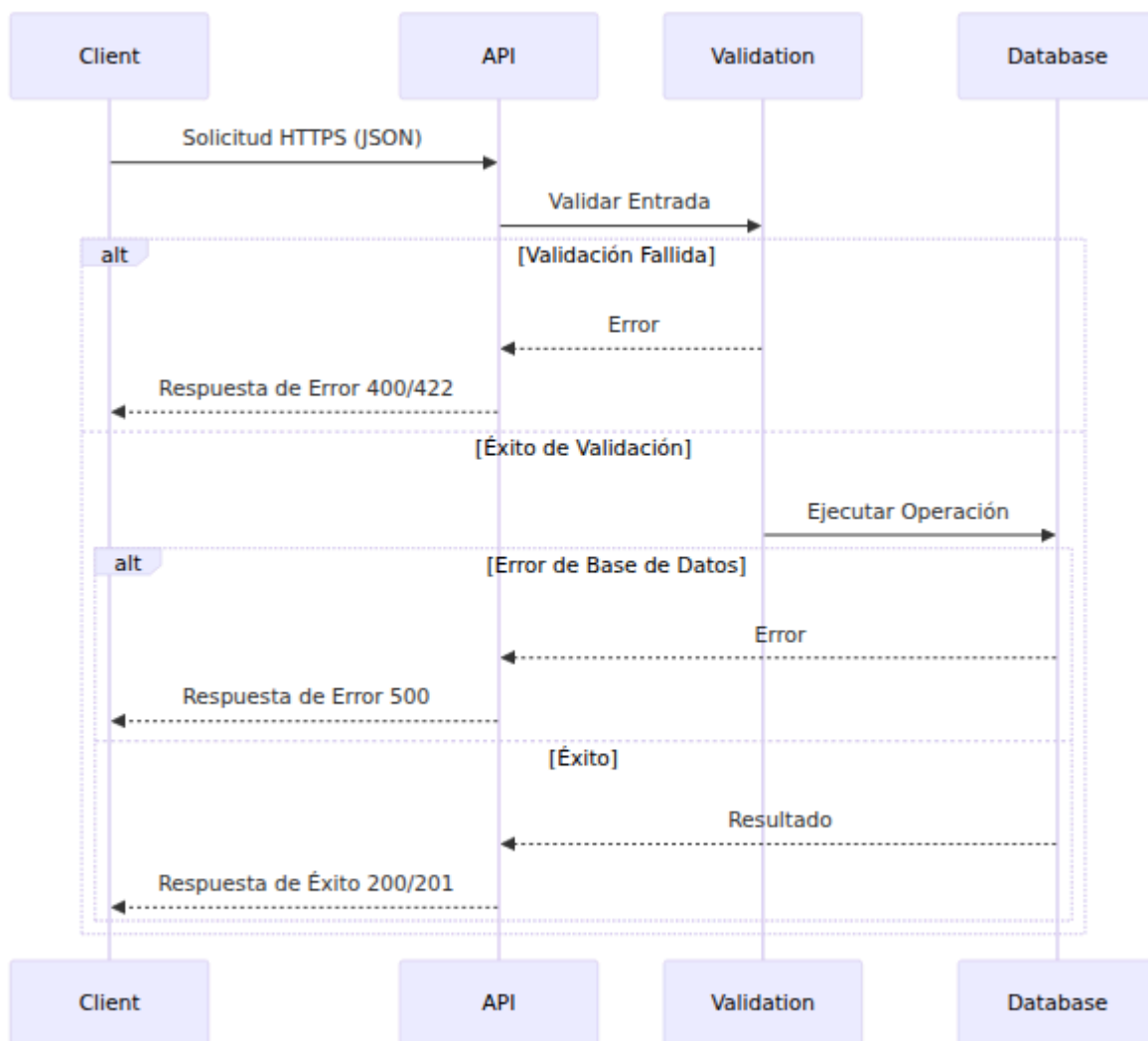
Respuesta de Error:

```
{
  "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>	boolean	Filtrar por estado habilitado
<code>ims_enabled</code>	boolean	Filtrar por estado habilitado de IMS

Ejemplo de Solicitud:

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

Ejemplo de Respuesta:

```
{
  "data": [
    {
      "id": 1,
      "imsi": "001001123456789",
      "enabled": true,
      "ims_enabled": true,
      "sim_id": 1,
      "key_set_id": 1,
      "epc_profile_id": 1,
      "ims_profile_id": 1,
      "roaming_profile_id": 1,
      "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	integer	ID de base de datos del suscriptor

Ejemplo de Solicitud:

```
curl -k https://hss.example.com:8443/api/subscriber/1
```

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 del 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 tienes 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": 1,  
    "key_set_id": 1,  
    "epc_profile_id": 1,  
    "ims_profile_id": 1,  
    "roaming_profile_id": 1,  
    "custom_attributes": {  
      "note": "Suscriptor de prueba"  
    }  
  }  
}
```

Campos Requeridos:

- `imsi` - Debe ser de 14-15 dígitos, único
- `key_set_id` - Debe hacer referencia a un [Conjunto de Claves](#) existente
- `epc_profile_id` - Debe hacer referencia a 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 principio a fin
- [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": 1,
    "epc_profile_id": 1
  }
}'
```

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	integer	ID de base de datos del suscriptor

Cuerpo de Solicitud:

```
{
  "subscriber": {
    "enabled": false,
    "ims_enabled": false,
    "epc_profile_id": 2,
    "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/1 \
-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": 2}` (ver [Perfiles EPC](#))
- Actualizar la política de roaming: `{"roaming_profile_id": 3}` (ver [Gestión de Roaming](#))

Eliminar Suscriptor

Eliminar un suscriptor del sistema.

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

Parámetros de Ruta:

Parámetro	Tipo	Descripción
id	integer	ID de base de datos del suscriptor

Ejemplo de Solicitud:

```
curl -k -X DELETE https://hss.example.com:8443/api/subscriber/1
```

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 actualmente registrado.

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 actualmente registrado (`subscriber_state.last_seen_mme`)
- Usa `Cancellation-Type: subscription_withdrawal` (forzar 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/SIM físico)

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, Suscriptor B
sin afectar
```

Notas Importantes:

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

Documentación Relacionada:

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

Gestión de MSISDN

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

Listar MSISDNs

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/1
```

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 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, necesita crear un registro de unión. Esto se realiza típicamente a través del endpoint de actualización del 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



Consulte [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/1
```

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/1
```

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/1 \  
-H "Content-Type: application/json" \  
-d '{  
  "sim": {  
    "batch_name": "Nombre del Lote Actualizado"  
  }  
'
```

Eliminar SIM

Eliminar un registro de tarjeta SIM.

Endpoint: DELETE /api/sim/:id

Advertencia: Asegúrese de que no haya suscriptores que hagan referencia a esta SIM antes de eliminar.

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 hacer referencia a 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/1
```

Ejemplo de Respuesta:

```
{
  "data": {
    "id": 1,
    "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)
- O `opc` O `op` (OPC puede derivarse de 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

Modificar un conjunto de claves existente.

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

Advertencia: Cambiar las claves para un **suscriptor** activo causará fallos de autenticación. Solo actualice las 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 no haya **suscriptores** que hagan referencia a este conjunto de claves antes de eliminar. Consulte primero a los suscriptores para verificar referencias.

Gestión de Perfiles

Perfiles EPC

Los perfiles EPC (Evolved Packet Core) definen parámetros de servicio de datos para 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 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
ue_ambr_dl_kbps	Límite de ancho de banda de descarga	Kbps	10
ue_ambr_ul_kbps	Límite de ancho de banda de subida	Kbps	50
network_access_mode	Tipo de acceso	Cadena	"p" "p"
tracking_area_update_interval_seconds	Temporizador TAU	Segundos	60
apn_profiles	Lista de IDs de perfil APN	Array	[]

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
}'
```

Ver También:

- [Documentación de Perfiles](#) - Guía de configuración de perfil detallada
- [Provisionamiento Completo de Suscriptores](#) - Usando perfiles EPC en el provisionamiento

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 no haya [suscriptores](#) que hagan referencia a este perfil antes de eliminar.

Perfiles IMS

Los perfiles IMS (IP Multimedia Subsystem) definen parámetros de servicio de voz y Criterios de Filtro Inicial (IFC) para 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 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 creas 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 un 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 simple de variables -->
{{ 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": 1,
    "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

Ver También:

- [Documentación de Perfiles](#) - Detalles y ejemplos de la plantilla IFC
- [Flujos de Protocolo](#) - Flujos de registro IMS y 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 del APN** - Define los parámetros de Calidad de Servicio
3. **Perfil APN** - Combina el identificador y QoS, vinculado a [Perfiles EPC](#)

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

Endpoint: GET /api/apn/qos_profile

Crear Perfil QoS del APN

Endpoint: POST /api/apn/qos_profile

Cuerpo de 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 Solicitud:

```
{
  "apn_identifier_id": 1,
  "apn_qos_profile_id": 1,
  "name": "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 del APN](#) existente

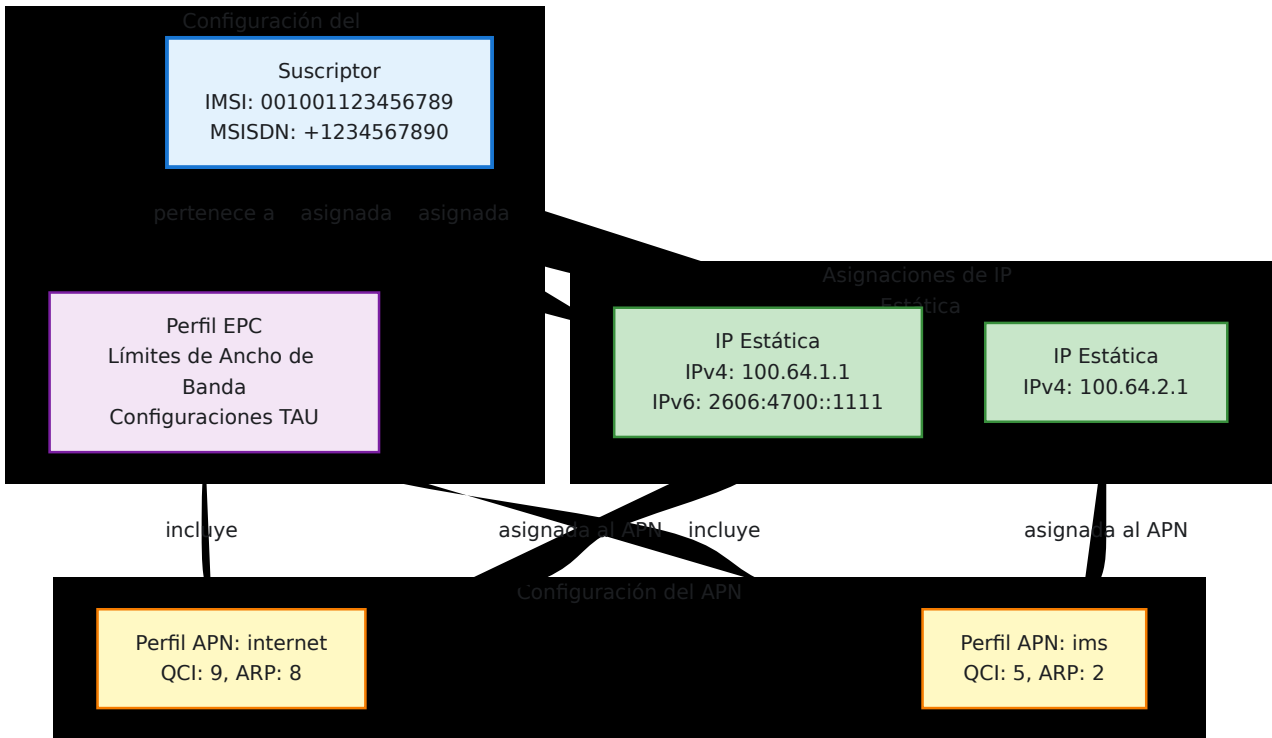
Ver También:

- [Provisionamiento Completo de Suscriptores](#) - Ejemplo completo que incluye configuración de APN
 - [Perfiles EPC](#) - Los perfiles APN están vinculados a perfiles EPC
-

Gestión de IPs Estáticas

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

Arquitectura:



Flujo de Datos Cuando el Suscriptor Se Conecta:

Parse error on line 7: ...N Nota sobre UE,PGW: El Suscriptor -----^
 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

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

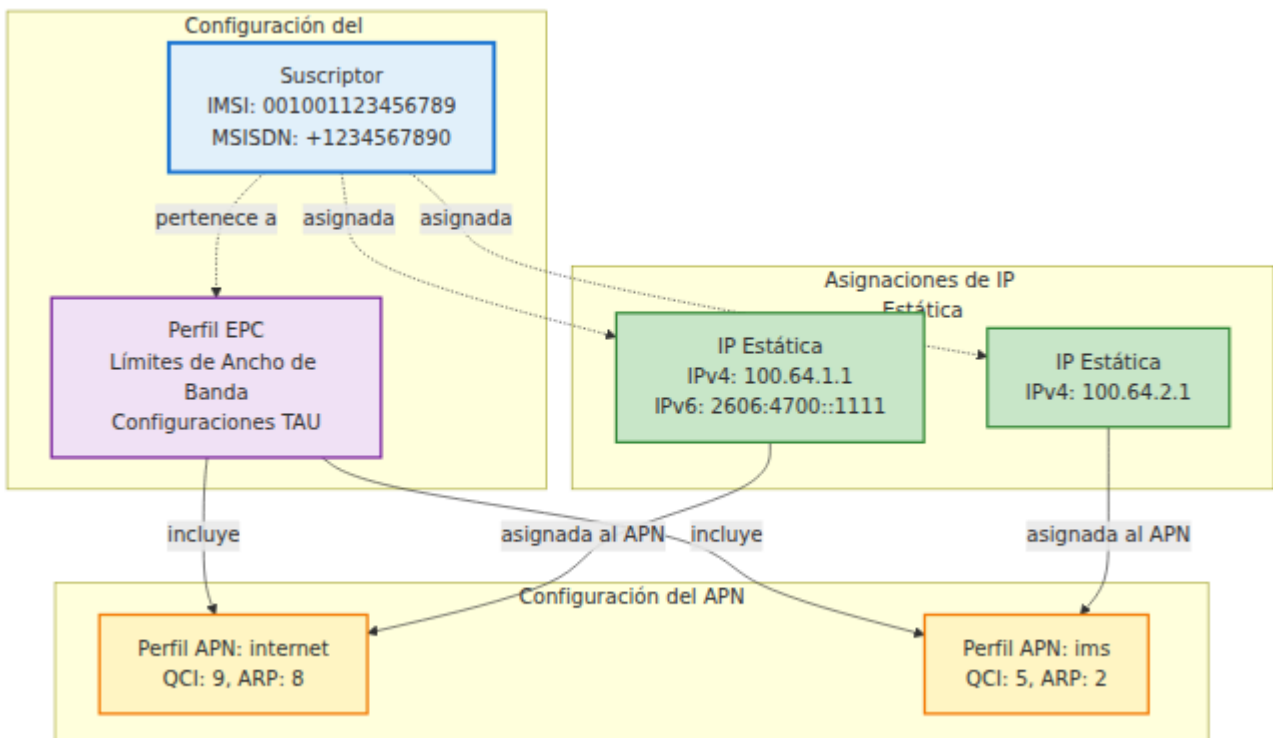
Este diagrama muestra exactamente de dónde proviene cada campo en el AVP de Configuración de APN de la Respuesta de Actualización de Ubicación S6a en la base de datos:



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 de la tabla `apn_qos_profile`
5. **Ancho de Banda AMBR:** Los valores se multiplican por 1000 (kbps → bps)
6. **Dirección IP del Parte 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
 - Se verifica la compatibilidad de la versión IP con `apn_identifier.ip_version`
7. **VPLMN-Dynamic-Address-Allowed:** Codificado en 0 (no permitido) - fuerza el 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 IPs 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 estática del sistema
 - La misma dirección IPv4 o IPv6 no puede ser asignada a múltiples suscriptores (incluso en diferentes APNs)
 - Esto previene conflictos de enrutamiento y ambigüedad de dirección 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 IPs 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 regulatorio 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": 1,
      "apn_profile_id": 5,
      "ipv4_static_ip": "100.64.1.1",
      "ipv6_static_ip": "2606:4700:4700::1111",
      "apn_profile": {
        "id": 5,
        "name": "APN de Internet",
        "apn_identfier": {
          "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	integer	ID de base de datos de la IP estática

Ejemplo de Solicitud:

```
curl -k https://hss.example.com:8443/api/epc/static_ip/1
```

Crear IP Estática

Crear una nueva asignación de IP estática para un APN.

Endpoint: POST /api/epc/static_ip

Cuerpo de Solicitud:

```
{
  "static_ip": {
    "apn_profile_id": 5,
    "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 de Formato de 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 estática**
 - 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>
Doble Pila	✓	✓	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": 5,
    "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": 6,
    "ipv6_static_ip": "2606:4700:4700::1111"
  }
}'
```

IP Estática de Doble Pila:

```
curl -k -X POST https://hss.example.com:8443/api/epc/static_ip \
-H "Content-Type: application/json" \
-d '{
  "static_ip": {
    "apn_profile_id": 5,
    "ipv4_static_ip": "100.64.1.1",
    "ipv6_static_ip": "2606:4700:4700::1111"
  }
}'
```

Respuesta de Éxito (201 Creado):

```
{
  "data": {
    "id": 1,
    "apn_profile_id": 5,
    "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 de 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	integer	ID de base de datos de la 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 de 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 seguirán 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/1 \
-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	integer	ID de base de datos de la IP estática

Ejemplo de Solicitud:

```
curl -k -X DELETE https://hss.example.com:8443/api/epc/static_ip/1
```

Comportamiento:

- Elimina la asignación de IP estática
- NO afecta al [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 fuera de línea o envíe una [Solicitud de Cancelación de Ubicación](#) antes de eliminar.

Asignar IP Estática a Suscriptor

Para asignar una IP estática a un suscriptor, necesita 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 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": 5,
    "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\": 1,
    \"epc_profile_id\": 1,
    \"static_ips\": [\$STATIC_IP_ID]
  }
}"
```

Actualizar Suscriptor Existente con IP Estática:

```
curl -k -X PUT https://hss.example.com:8443/api/subscriber/1 \
-H "Content-Type: application/json" \
-d '{
  "subscriber": {
    "static_ips": [1, 2]
  }
}'
```

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 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": 5,
    "ipv4_static_ip": "100.64.1.1"
  }
}' | jq -r '.data.id')

# Crear IP estática para 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": 6,
    "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\": 1,
    \"epc_profile_id\": 1,
    \"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": [1, 2]
    }
  }'
```

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

Ver También:

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

Gestión de Roaming

Los perfiles de roaming controlan si los suscriptores pueden acceder a servicios de datos e IMS en redes visitadas. Los perfiles se asignan a [suscriptores](#) y consisten en reglas que se emparejan 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 y ejemplos detallados
- [Flujos de Protocolo](#) - Cómo funciona el control de roaming en flujos 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.

Consulte [Documentación de EIR](#) para una 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 con 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 provisionamiento 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

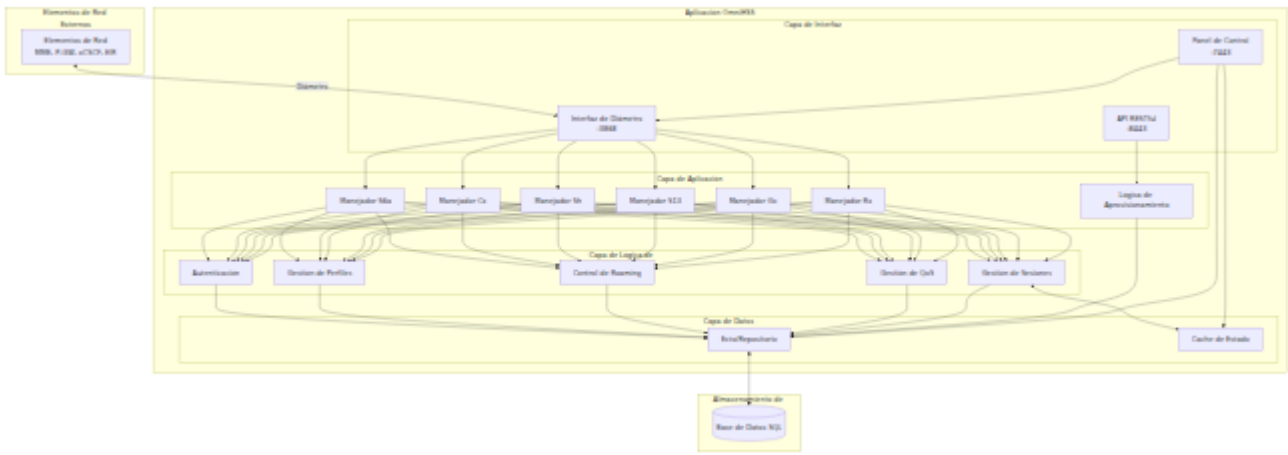
[← Volver a la Guía de Operaciones](#)

Tabla de Contenidos

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

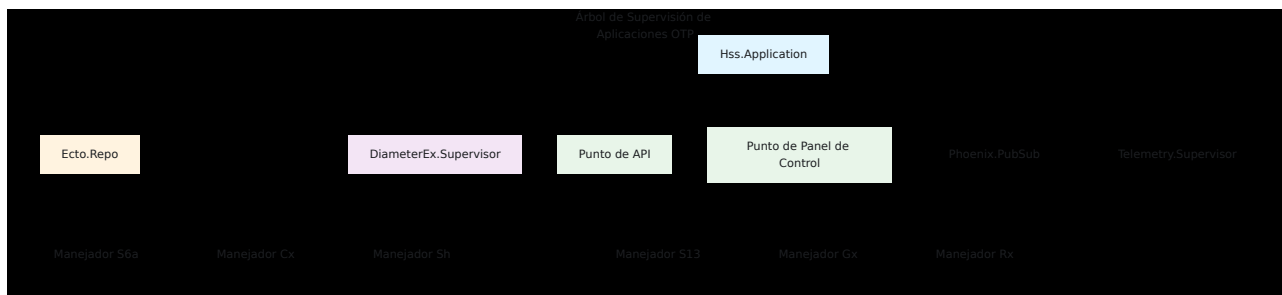
Visión General del Sistema

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.



Arquitectura de Componentes

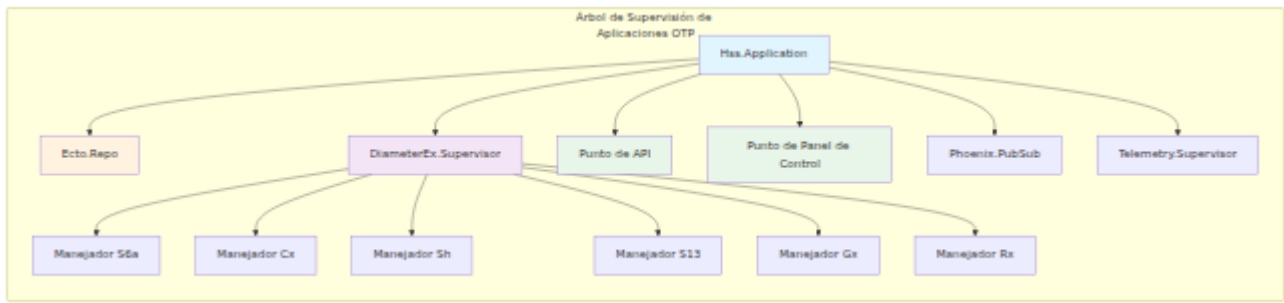
Componentes Principales



Manejadores de Aplicaciones de Diámetro

Cada aplicación de Diámetro (S6a, Cx, Sh, S13, Gx, Rx) se implementa como un módulo de manejador de DiameterEx que:

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

Capa de Transporte
TCP/SCTP :3868

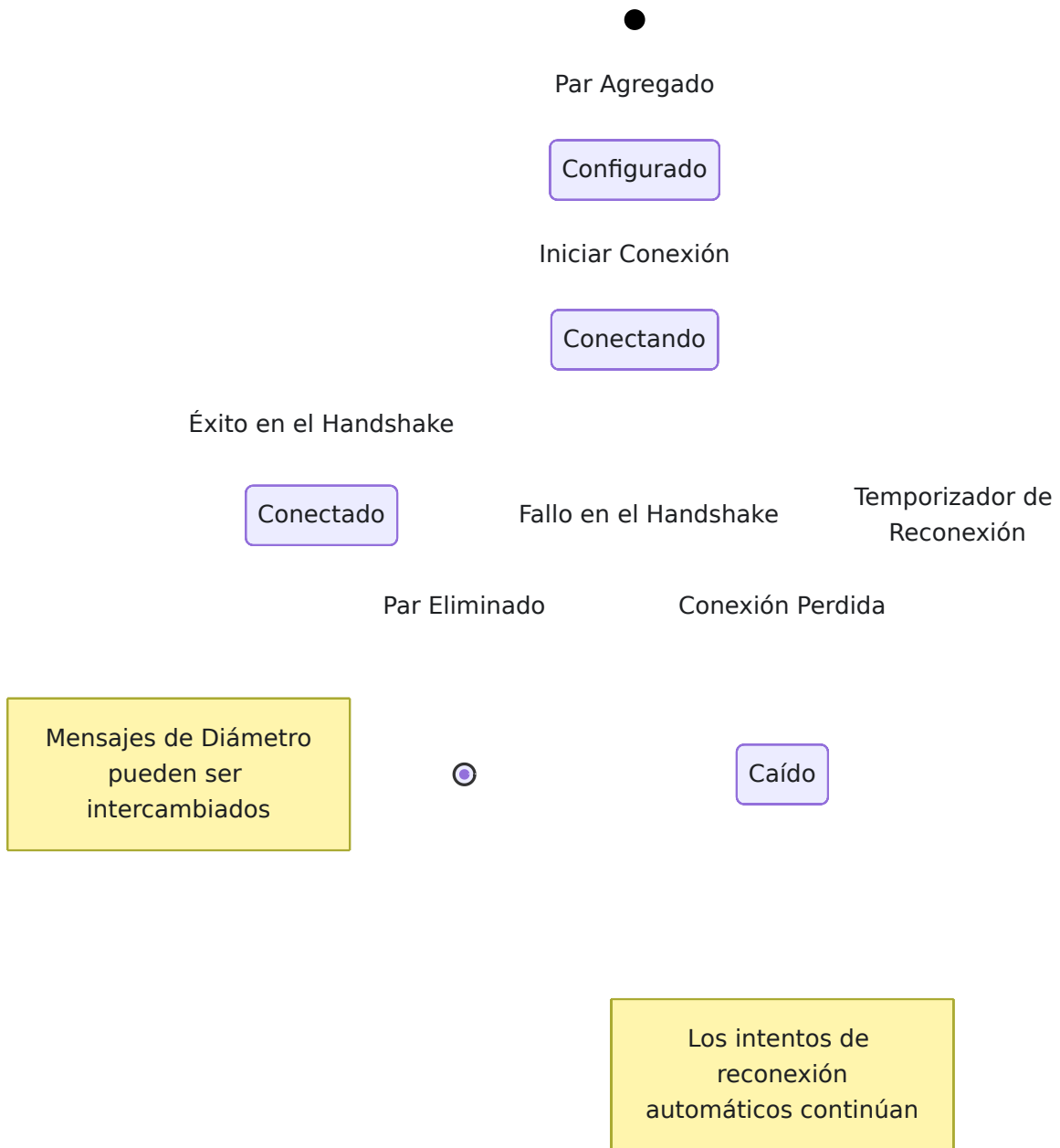
Capa de Aplicación

Sh
ID de App: 16777217

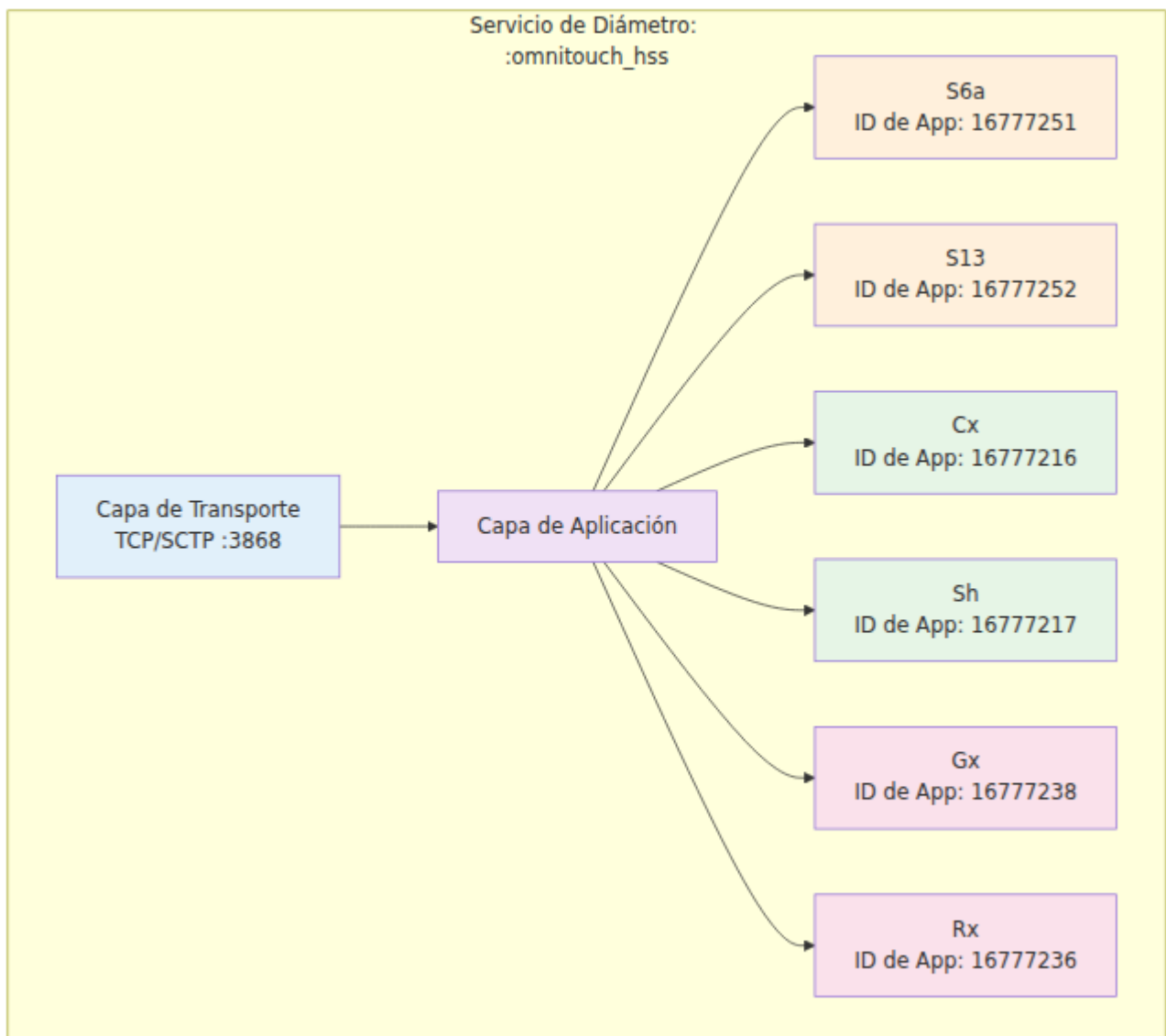
Gx
ID de App: 16777238

Rx
ID de App: 16777236

Gestión de Conexiones de Pares



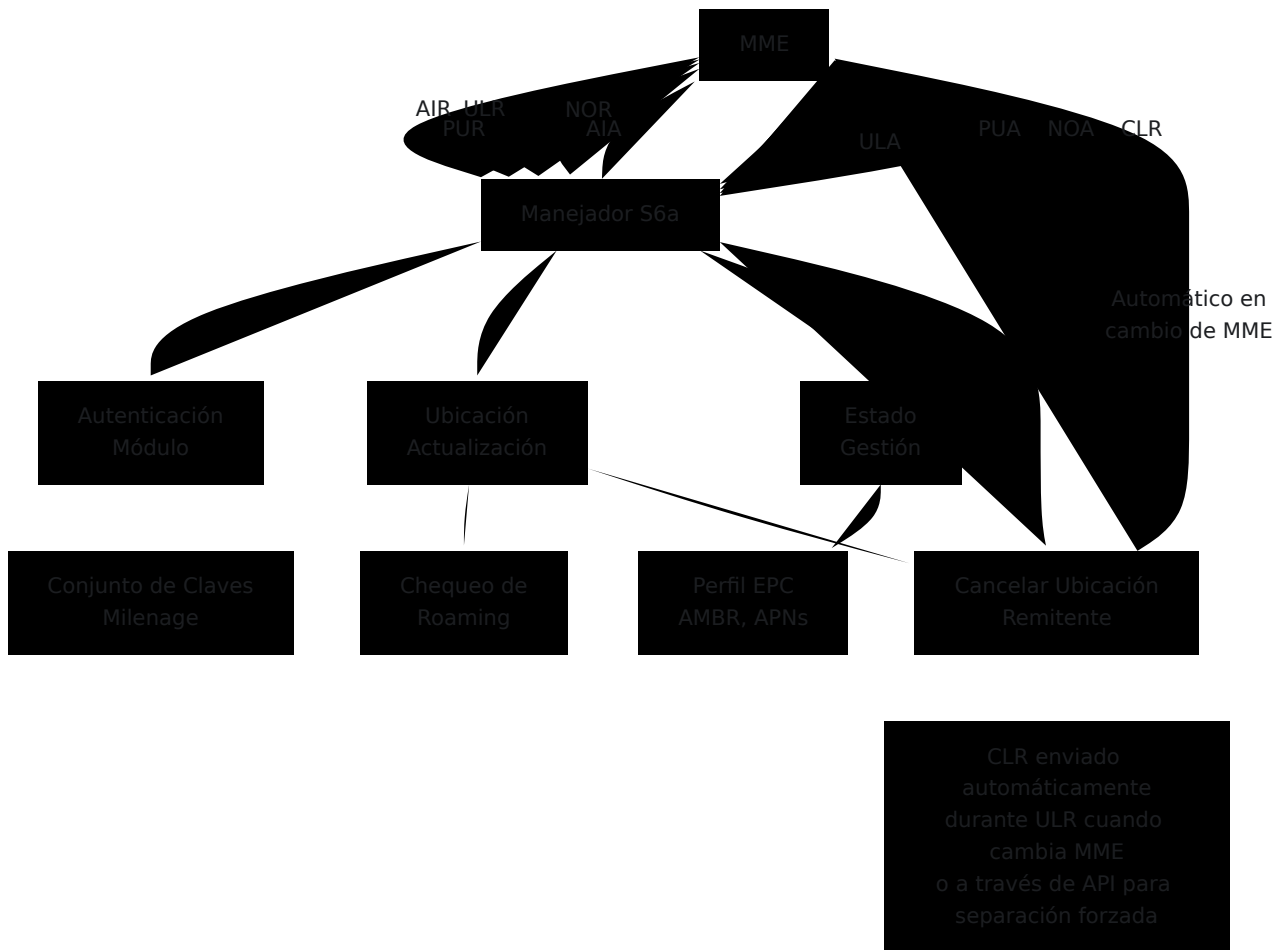
Flujo de Mensajes de Diámetro



Capa de Aplicación

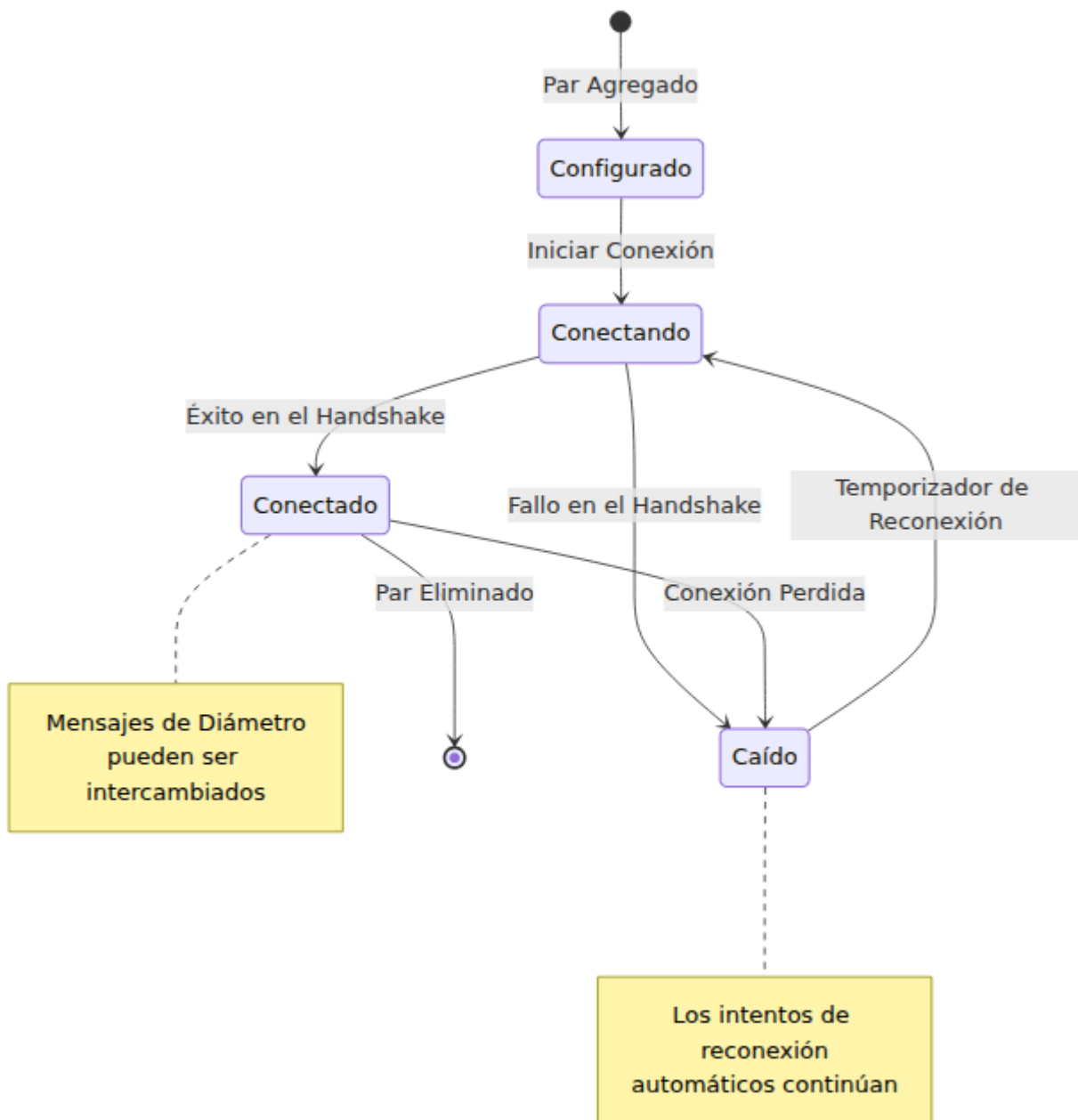
Interfaz S6a (LTE/EPC)

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



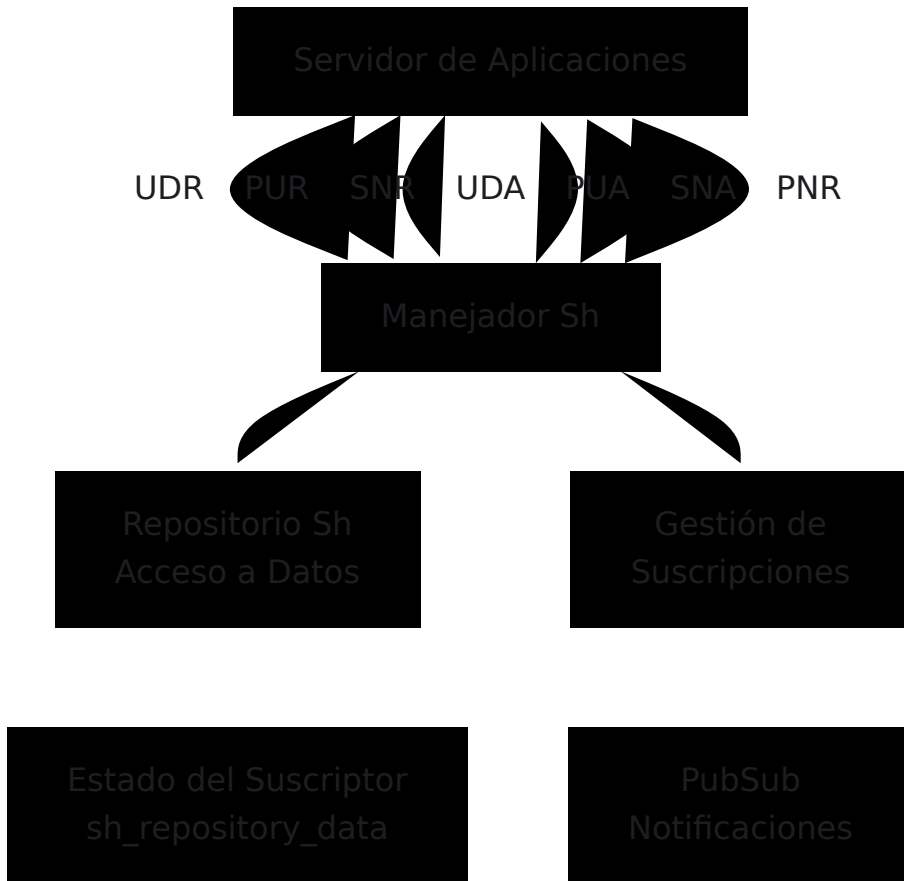
Interfaz Cx (IMS)

Maneja el registro y la autenticación de IMS.



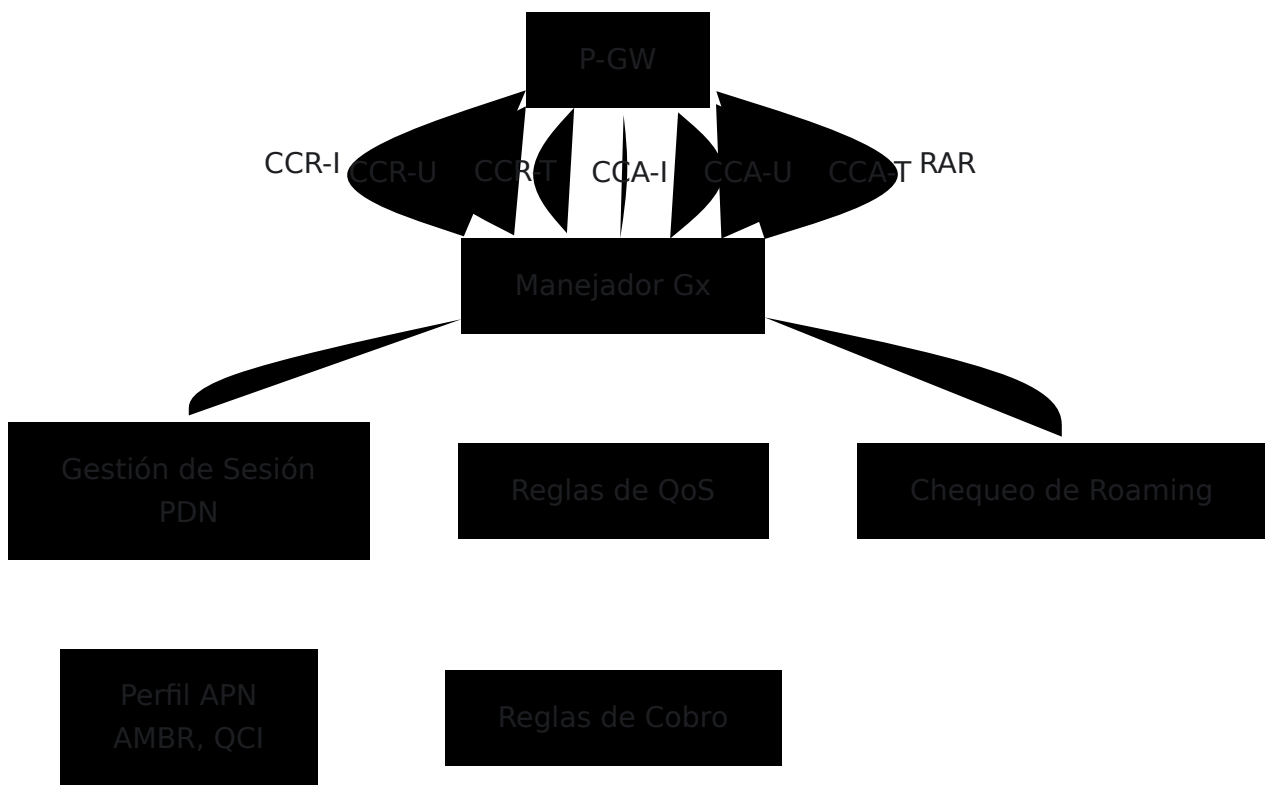
Interfaz Sh (Datos de Perfil IMS)

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



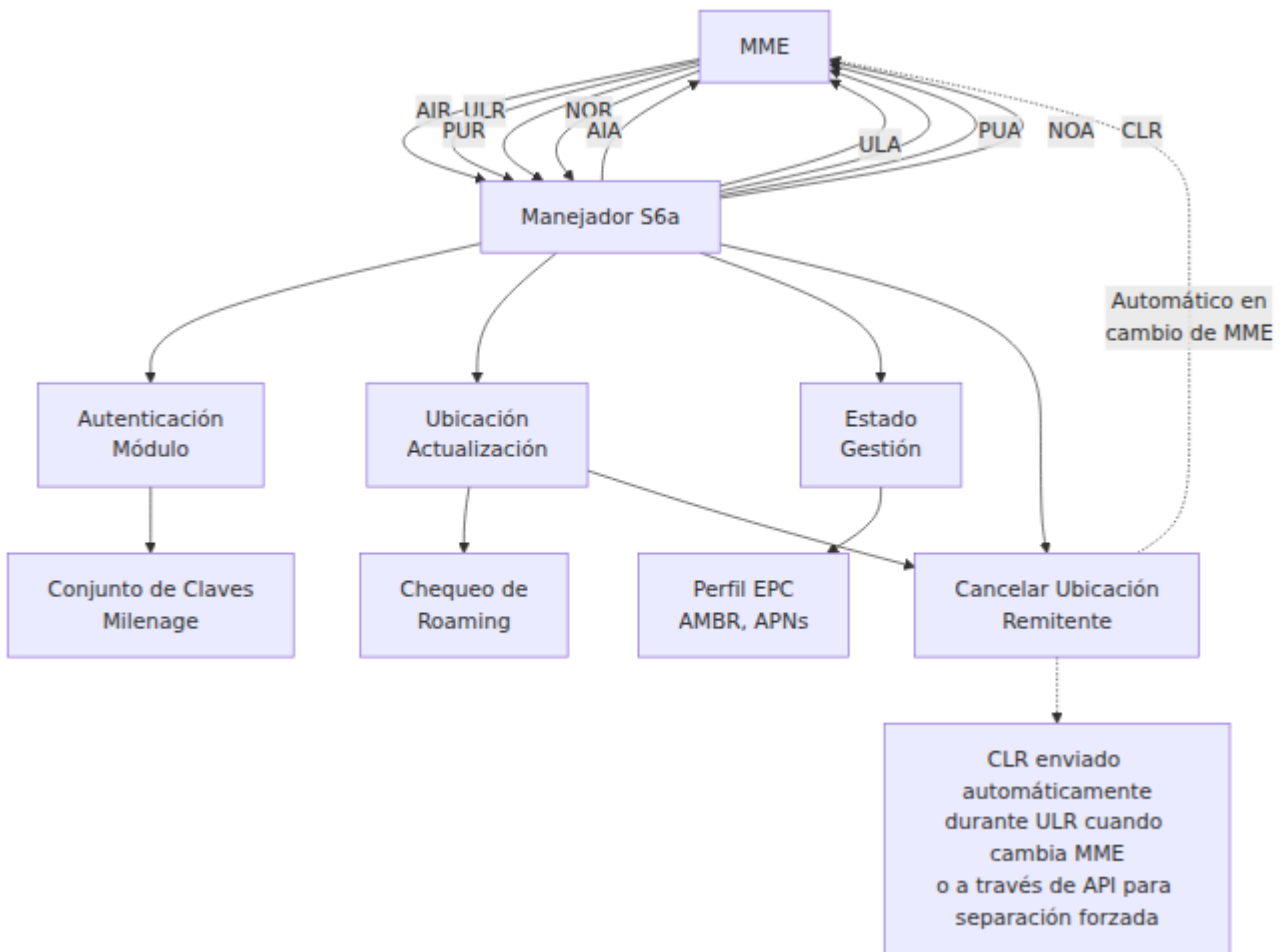
Interfaz Gx (Control de Políticas)

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



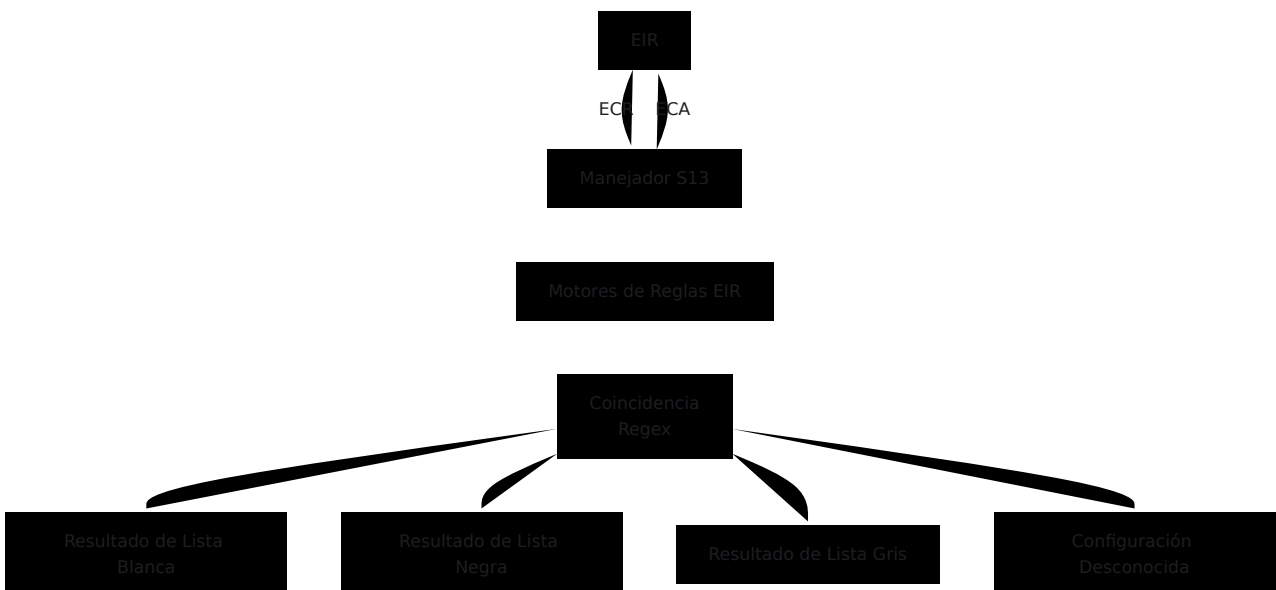
Interfaz Rx (Medios IMS)

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



Interfaz S13 (EIR)

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



Capa de Datos

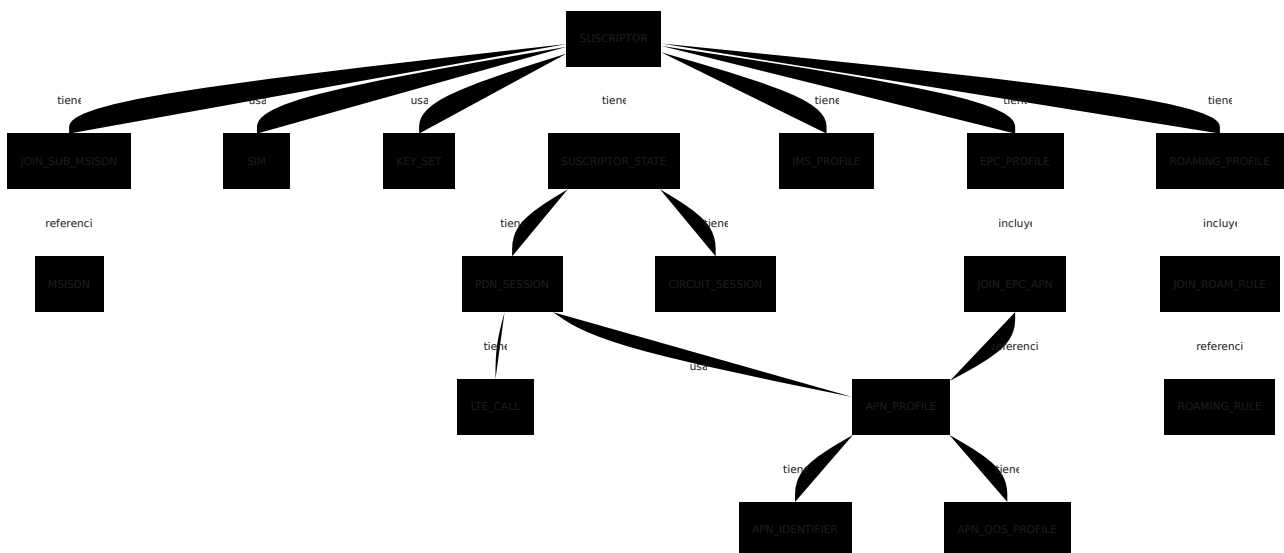
Backend de Base de Datos

OmniHSS utiliza **Ecto** como su capa de abstracción de base de datos. Ecto soporta múltiples backends de bases de datos relacionales, permitiendo flexibilidad en la selección de bases de datos. **MariaDB** con Galera Cluster es una configuración soportada.

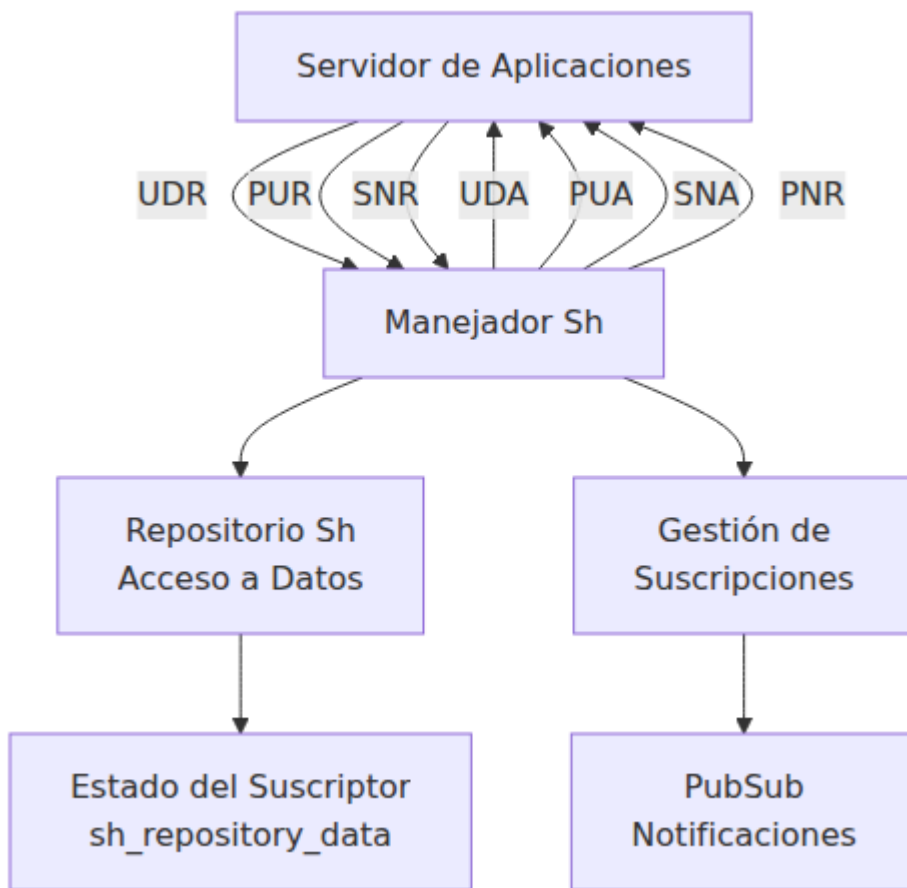
Se pueden utilizar otros backends de bases de datos dependiendo de los requisitos de su infraestructura. **Trabaje con su equipo de integración en ONS** para determinar el backend de base de datos y la estrategia de replicación más apropiados para su entorno.

Consulte [Replicación de Base de Datos Galera](#) para la configuración de Galera Cluster.

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

S6a UIR

Cx SAR

Cx CCR-I

Consulta: suscriptor
+ conjunto_de_claves
+ perfil_de_roaming

Consulta: suscriptor
+ perfil_epc + apns
+ estado_del_suscriptor

Consulta: suscriptor
+ perfil_ims
+ msisdns

Consulta: suscriptor
+ perfil_apn + qos
+ estado_del_suscriptor

Datos Mínimos
Respuesta Rápida

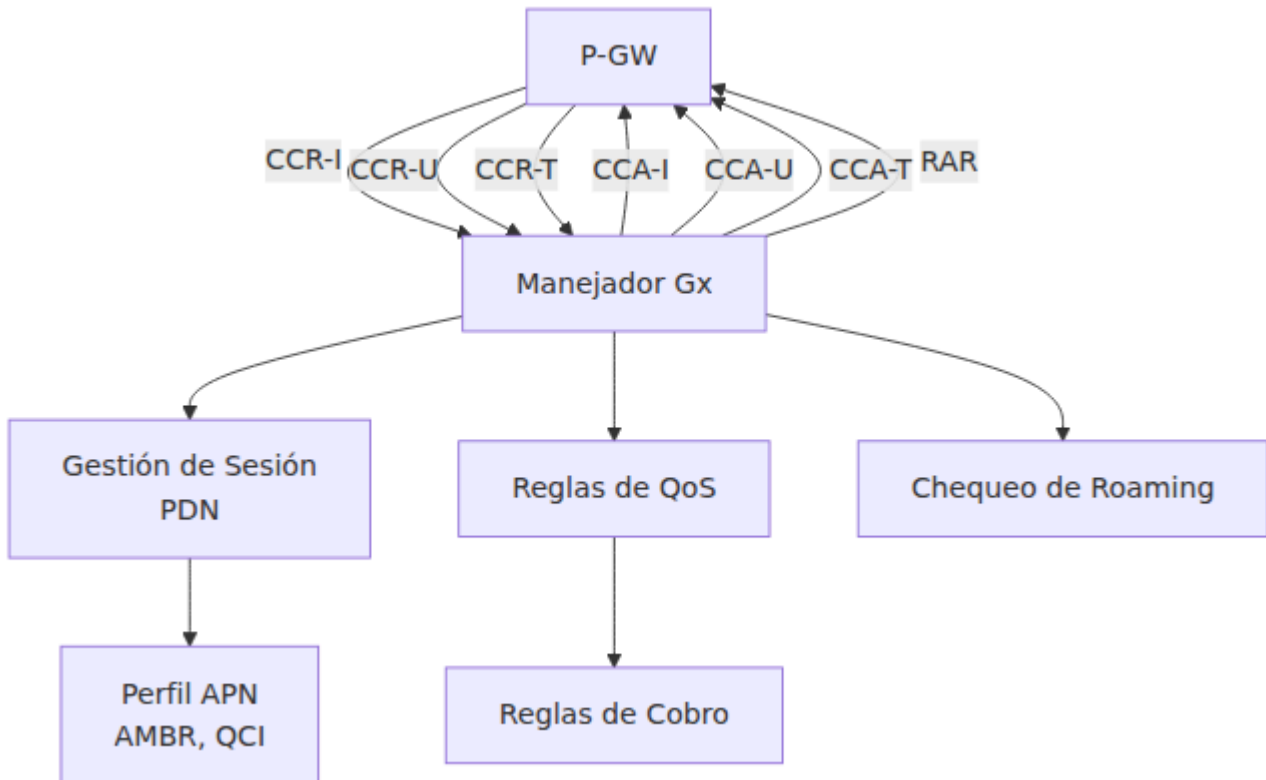
Datos Moderados
Información del Perfil

Datos IMS Completos
Perfil Completo

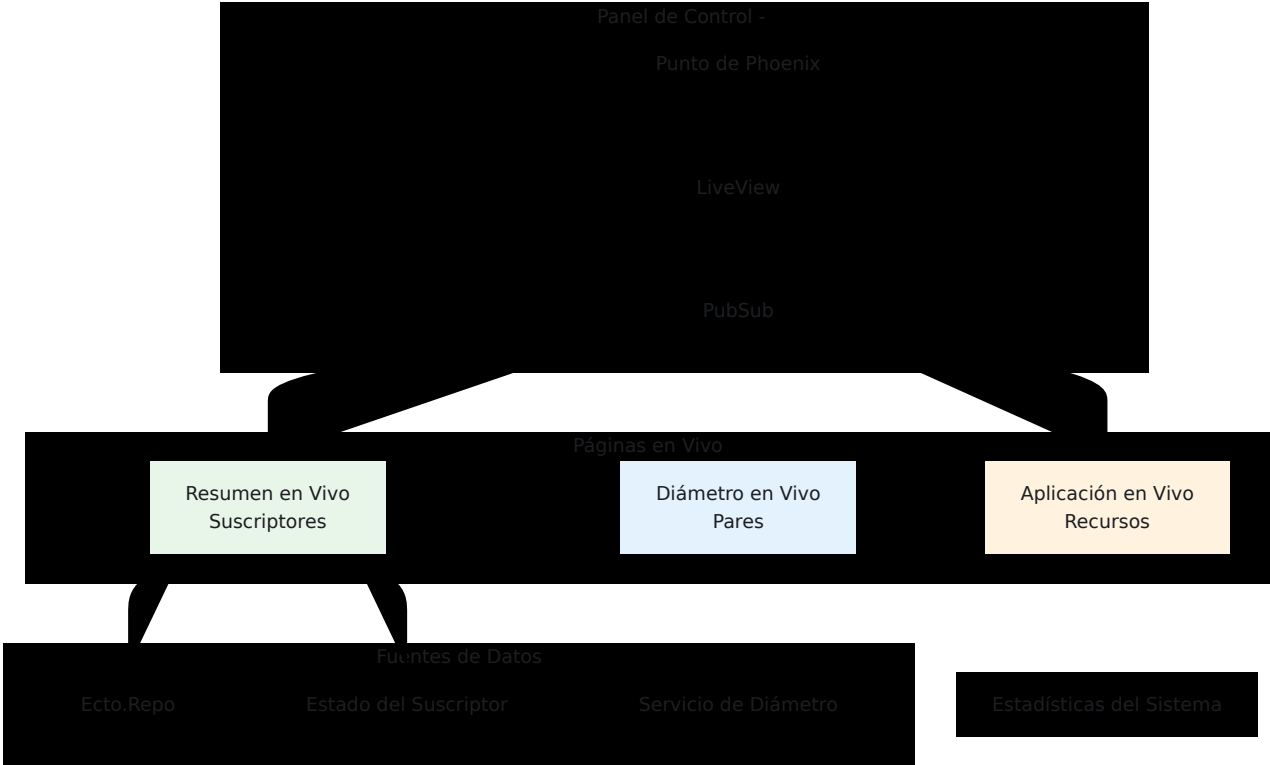
Datos de Sesión
Reglas de QoS

Interfaces Externas

Arquitectura de API

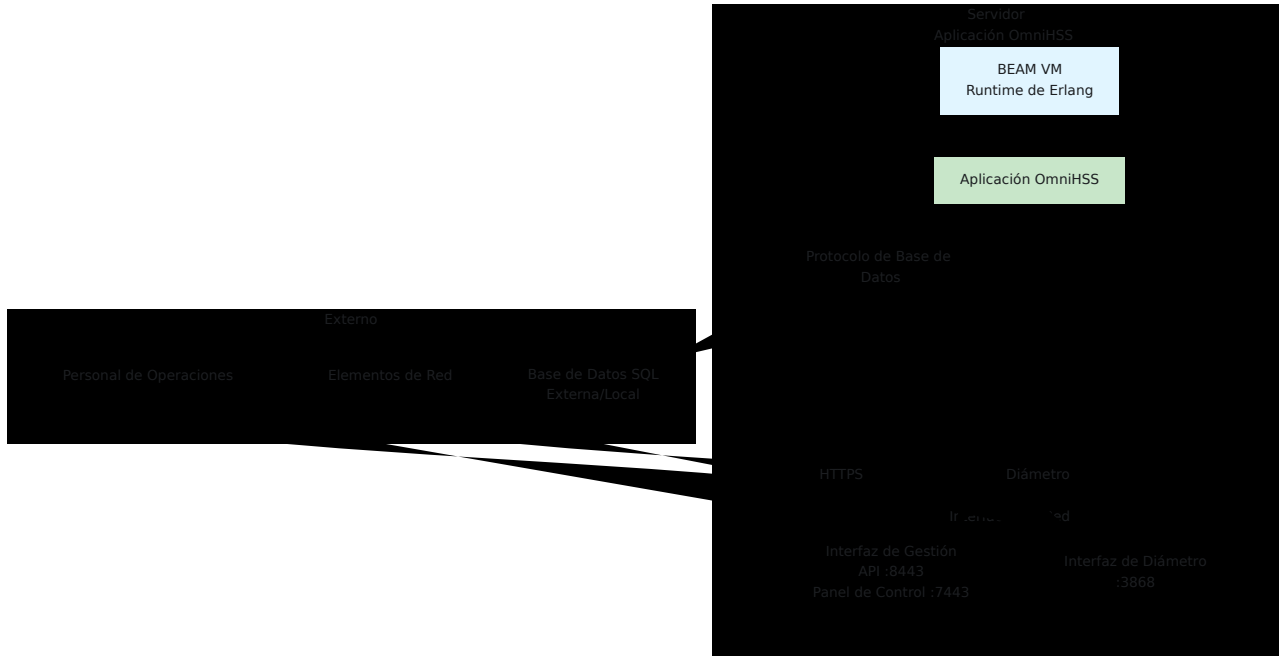


Arquitectura del Panel de Control



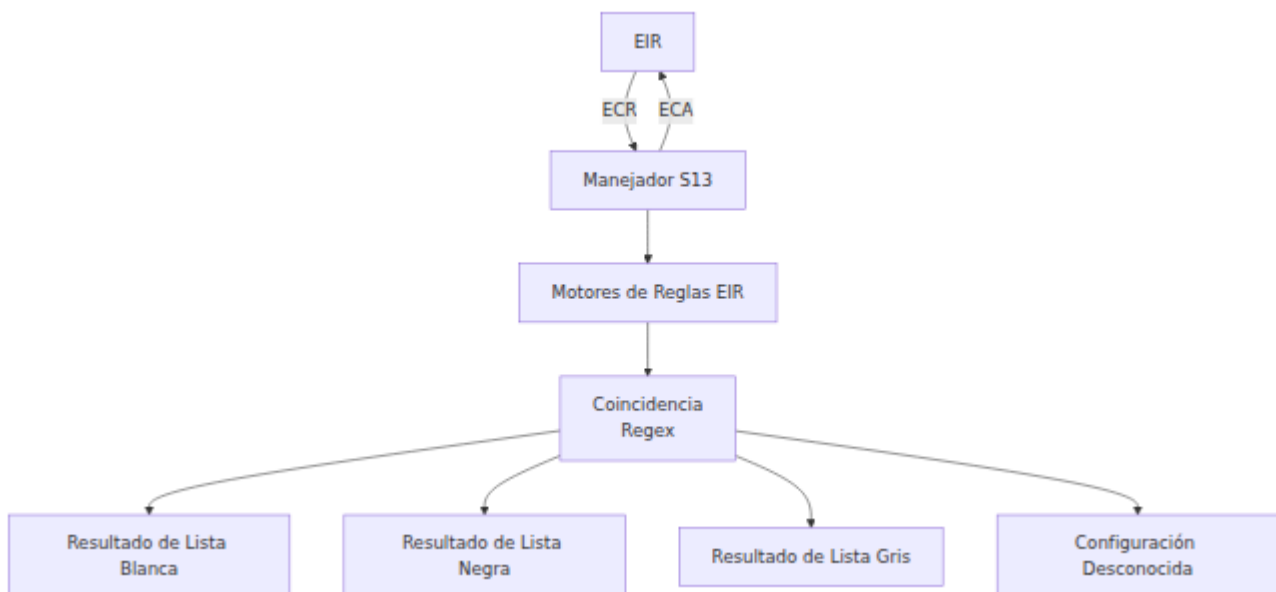
Arquitectura de Despliegue

Despliegue en Nodo Único



Despliegue HA en Múltiples Nodos (Galera Cluster)

Para despliegues de alta disponibilidad, OmniHSS soporta MariaDB Galera Cluster para replicación de base de datos multi-maestro síncrona.



Características Clave:

- **Replicación Síncrona:** Todas las escrituras se confirman en todos los nodos antes de devolver éxito
- **Multi-Maestro:** Cualquier nodo puede aceptar operaciones de lectura y escritura
- **Failover Automático:** Si un nodo falla, los otros continúan operando sin pérdida de datos
- **Basado en Certificación:** Las transacciones se validan en todos los nodos para prevenir conflictos

Ver **Replicación de Base de Datos Galera** 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 a la 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 a la base de datos para consultas paralelas

3. Modularidad

- Cada aplicación de Diámetro en un módulo separado
- Separación clara entre la interfaz, la lógica de negocios y las capas de datos
- Algoritmos de autenticación enchufables

4. Rendimiento

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

5. Observabilidad

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

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

Guía de Configuración de OmniHSS

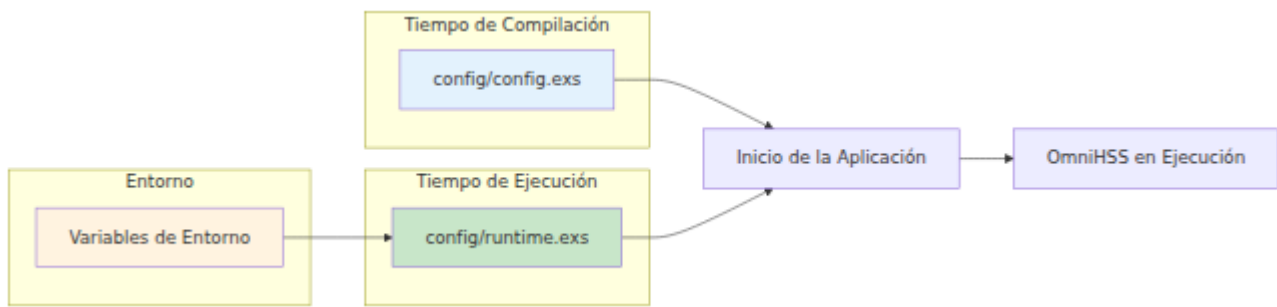
[← Volver a la Guía de Operaciones](#)

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 Casa](#)
 - [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 despliegue:

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

Configuración del Cliente de Licencias

El Cliente de Licencias valida la licencia de 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	Ejemplo
<code>license_server_api_urls</code>	Lista de URLs del servidor de licencias	Sí	<code>["https://10.0.0.1:8443/api"]</code>
<code>licensee</code>	Nombre de la organización en la licencia	Sí	<code>"ACME Telecom"</code>
<code>product_name</code>	Identificador del producto para la licencia	Sí	<code>"omnihss"</code>

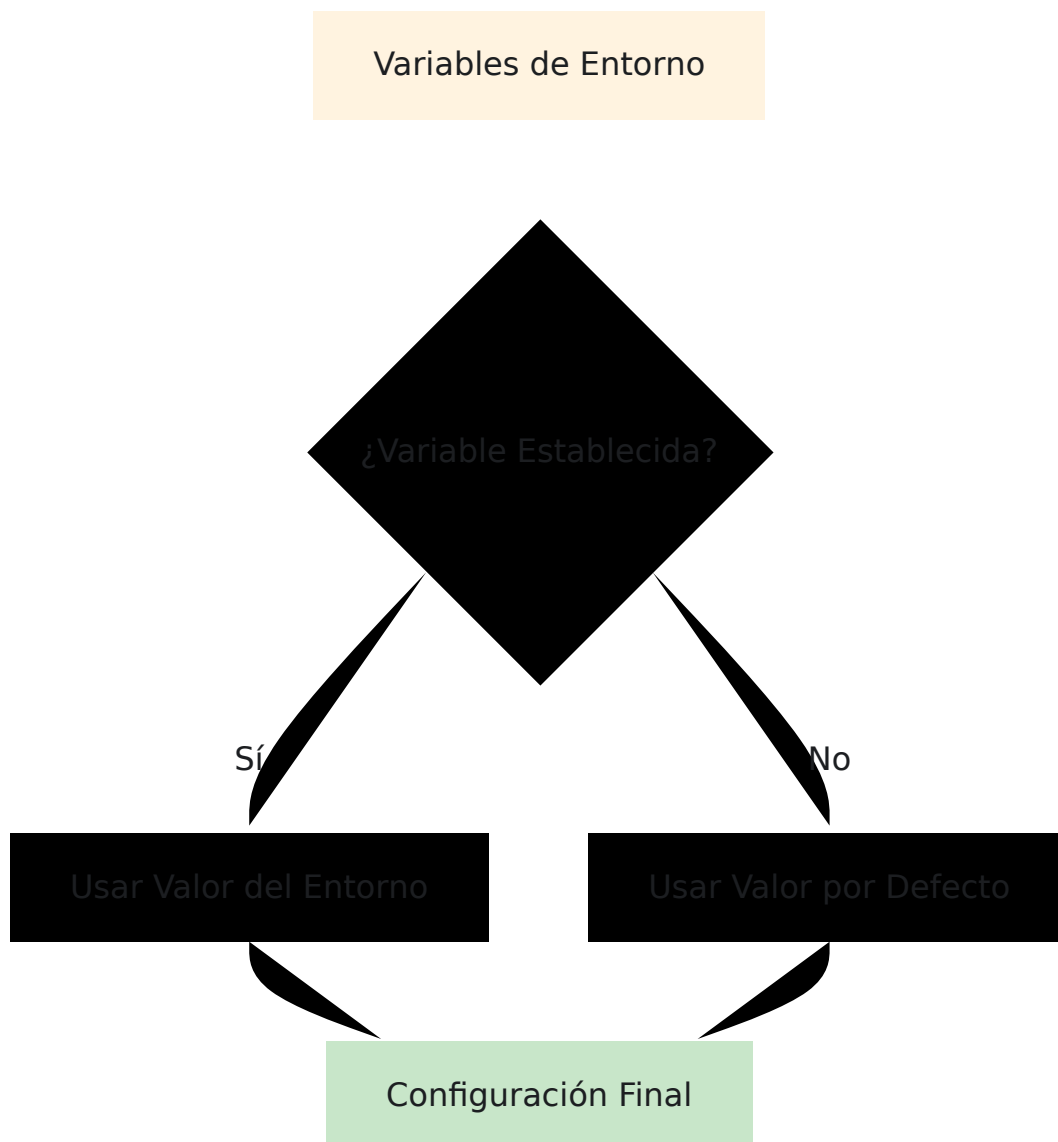
Notas Importantes:

- El servidor de licencias debe ser accesible desde HSS
- Utilice HTTPS para la validación segura de la licencia
- 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 por defecto 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")),

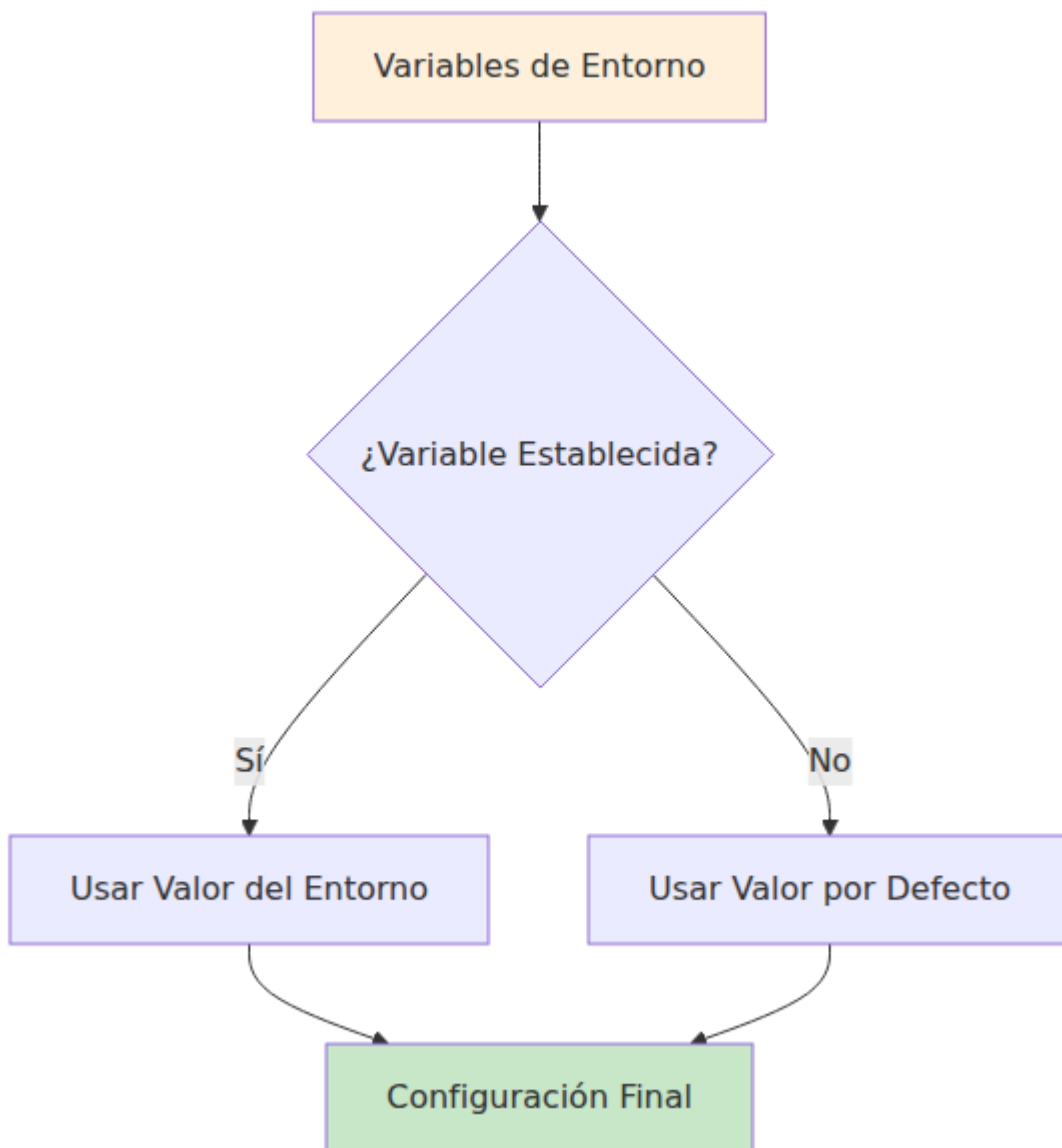
  # Tiempos de espera (en milisegundos)
  timeout: 15_000,
  connect_timeout: 15_000,

  # Opciones adicionales
  show_sensitive_data_on_connection_error: false
```

Parámetros de Configuración de la Base de Datos

Parámetro	Descripción	Por Defecto	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 var 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 por defecto 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:

- Comenzar con 20 conexiones
- Monitorear errores de "tiempo de espera del grupo de conexiones"
- Aumentar en 10 si ocurren tiempos de espera 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",
    "3306")),
  pool_size:
    String.to_integer(System.get_env("DATABASE_POOL_SIZE", "30")),
  ssl: true,
  ssl_opts: [
    cacertfile: "/etc/ssl/certs/mysql-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"),

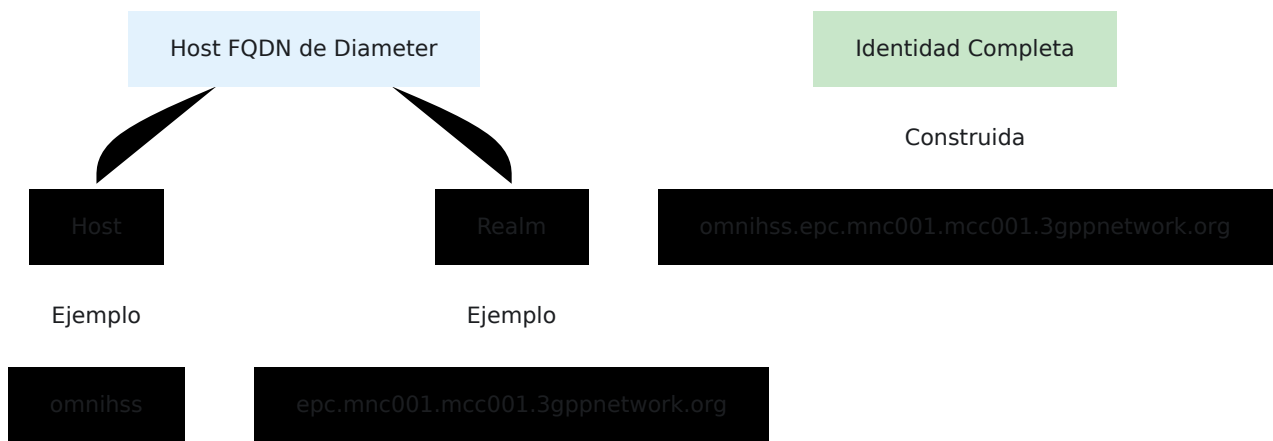
  # Identificación del producto
  product_name: "OmniHSS",
  vendor_id: 10415, # 3GPP
  supported_vendor_ids: [5535, 10415],

  # Configuración del protocolo
  request_timeout: 5000,

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

config :hss, :diameter, diameter_config
```

Configuración de Identidad de Diameter



Directrices:

- **Host:** Nombre corto del host 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]
  }
]
```

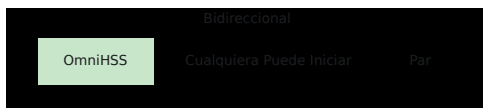
Modo Solo Escucha

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 Casa

El PLMN de casa identifica a su operador de red:

```
# config/runtime.exs

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

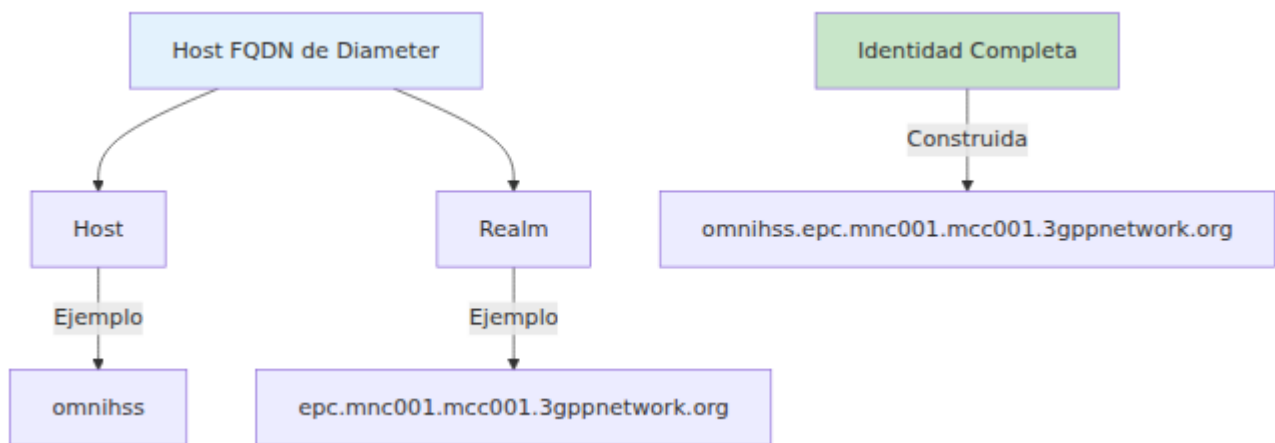
  # Detener el servicio Diameter durante fallos de base de datos
  stop_diameter_on_database_failure: true,

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

Parámetros del Núcleo HSS:

Parámetro	Descripción	Por Defecto	Re
<code>ecto_repos</code>	Lista de repositorios Ecto utilizados por la aplicación	<code>[Hss.Repo]</code>	Re op ba
<code>send_clr_on_mme_change</code>	Enviar Cancel Location Request cuando el suscriptor cambia de MME	<code>true</code>	M ha m ac
<code>stop_diameter_on_database_failure</code>	Deshabilitar el servicio Diameter si la base de datos se vuelve no disponible	<code>true</code>	Hi cc da
<code>license_enforced</code>	Habilitar la aplicación de la licencia	<code>true</code>	Re pr
<code>license_module</code>	Módulo que maneja las verificaciones de licencia	<code>LicenseClient</code>	No

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 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:

Elección de Vínculo

0.0.0.0
(Todas las Interfaces)

IP de Gestión
(por ejemplo,
192.168.1.10)

127.0.0.1
(Solo Localhost)

Accesible desde
cualquier red

Accesible solo desde
la red de gestión

Accesible solo
desde el servidor mismo

Configuración de IMS

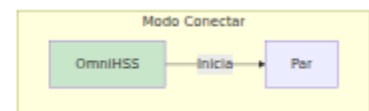
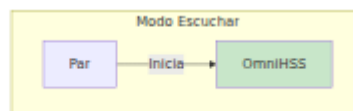
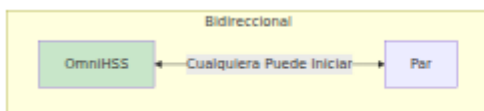
Configuración de Selección de S-CSCF

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

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

Configuración de EIR

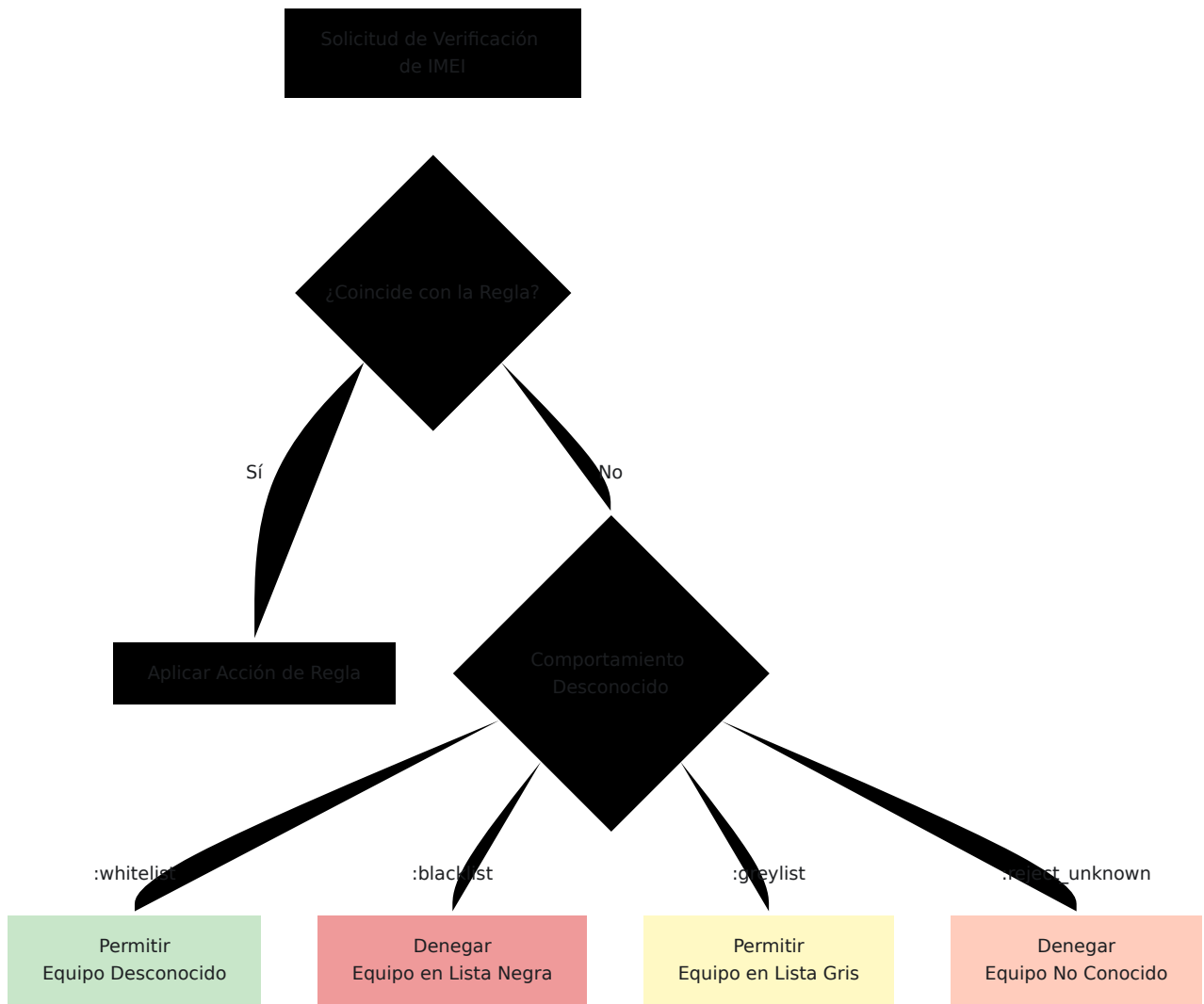
Consulte la [Documentación de EIR](#) para obtener detalles completos sobre la verificación de identidad del equipo.

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
<code>:whitelist</code>	Permitir todos los IMEI desconocidos	Red abierta, pruebas
<code>:blacklist</code>	Bloquear todos los IMEI desconocidos	Seguridad moderada
<code>:greylist</code>	Permitir pero rastrear IMEI desconocidos	Modo de monitoreo
<code>:reject_unknown_equipment</code>	Rechazar con código específico	Alta seguridad

Recomendación: Comenzar con `:whitelist` durante las pruebas, pasar a `:greylist` para monitoreo en producción, luego `:blacklist` para 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"
]
```

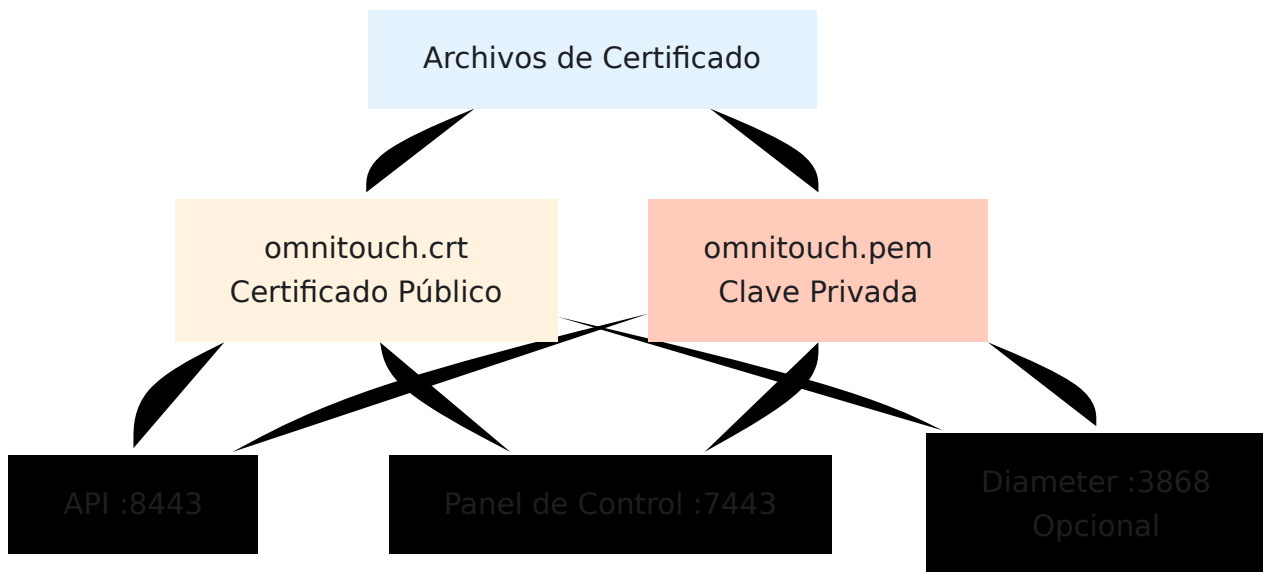
Configuración del Panel de Control

```
# 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:

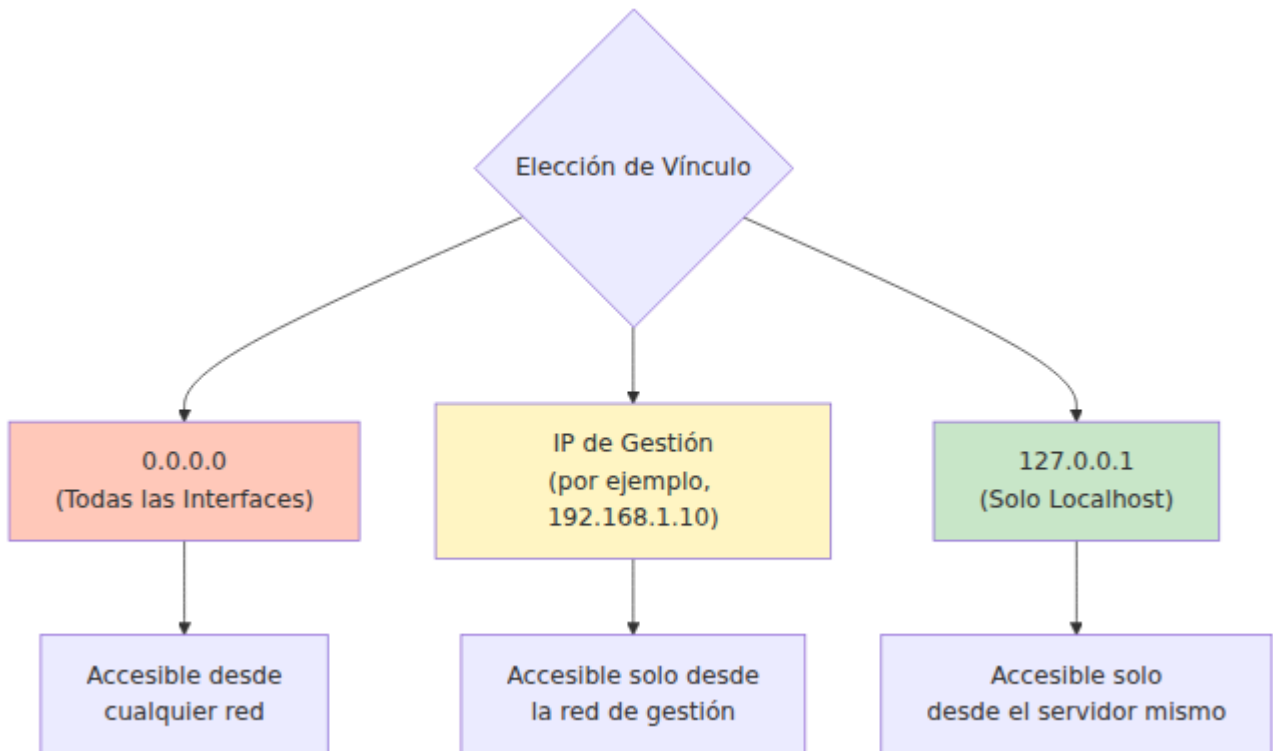
- Certificado X.509 válido
- Clave privada correspondiente
- Incluir certificados intermedios si es necesario
- CN o SAN debe coincidir con el nombre de host

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 del Despliegue



Lista de Verificación de Configuración

Configuración Esencial

- Conexión a la base de datos (nombre de host, credenciales)
- PLMN de casa (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 licencia (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 usa 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 características 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 la base de datos ajustado
- Vínculo de interfaz de red restringido

Verificación de la Configuración

Después de modificar la configuración:

1. Verificación de Sintaxis:

```
Verificar registros en busca de errores de carga de configuración
```

2. Acceso al Panel de Control:

```
Acceder a https://[hostname]:7443  
Verificar que se carga la página de Resumen
```

3. Acceso a la API:

```
curl -k https://[hostname]:8443/api/status
```

4. Estado de Diameter:

Verificar la página de Diameter en el Panel de Control
Verificar conexiones de pares

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

Verificar el Panel de Control para datos de suscriptores
O conectarse 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", "3306")),
  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/mysql-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 CASA 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](#) | [Siguiete: 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 sobre el estado del sistema, la actividad de los suscriptores y la conectividad de Diámetro. Construido con Phoenix LiveView, se actualiza automáticamente sin necesidad de recargar la página.

Características Clave

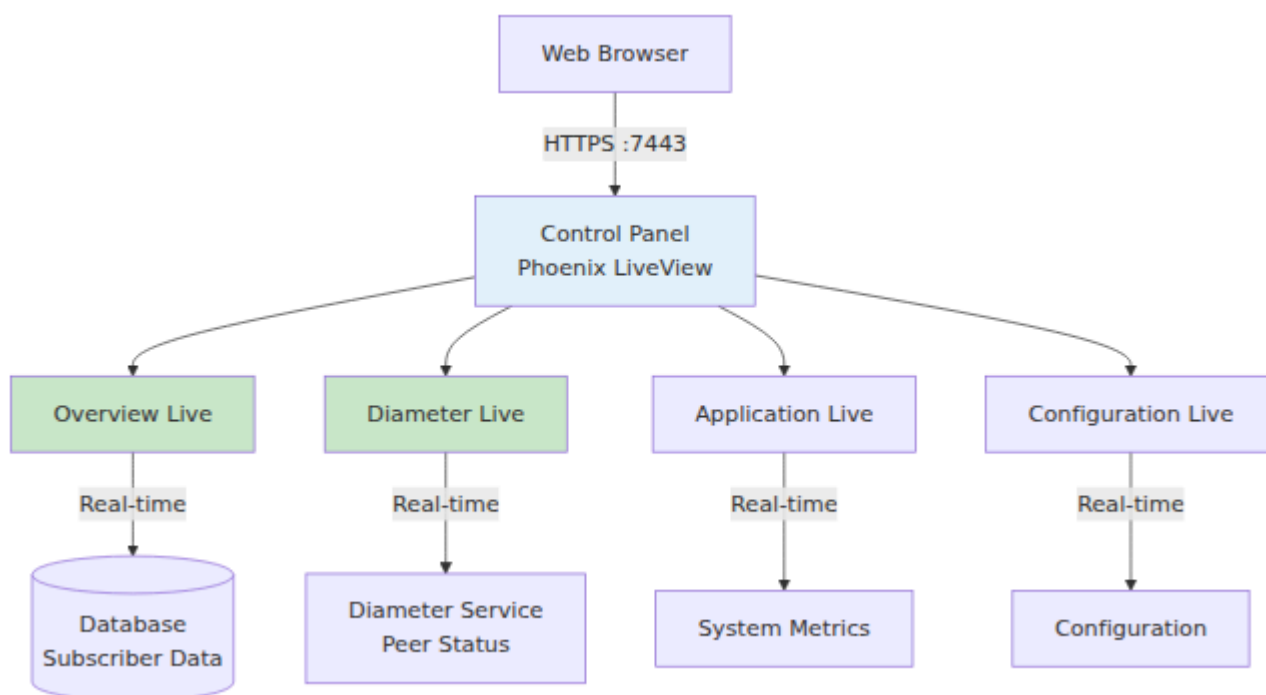
- **Actualizaciones en Tiempo Real** - Se actualiza automáticamente cada segundo
- **Monitoreo de Suscriptores** - Ver suscriptores activos y su estado actual

- **Estado de Diámetro** - Monitorear conexiones entre 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: Usa 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 de 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

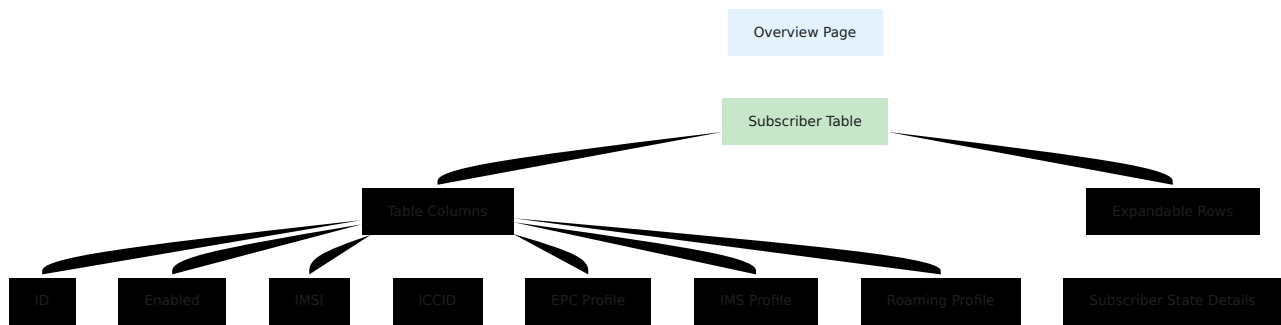
Nota: Internet Explorer no es compatible.

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



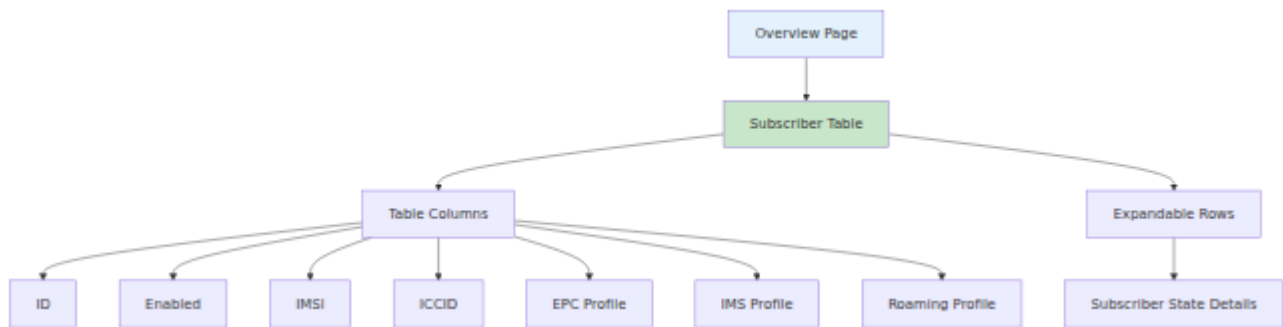
Columnas de la Tabla

Columna	Descripción	Valores
ID	ID de base de datos del suscriptor	Entero
Enabled	Estado del servicio	✓ (habilitado) / ✗ (deshabilitado)
IMSI	Identidad Internacional de Suscriptor Móvil	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 del perfil o ID
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 Realm Visto** - Realm 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:

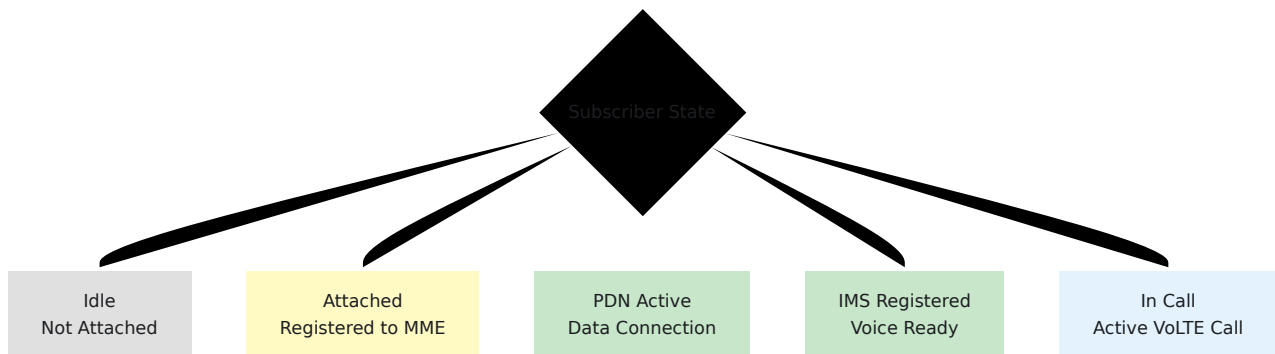
- **S-CSCF Asignado** - URI SIP S-CSCF actualmente asignado
- **Identidad Pública IMS** - URI SIP (por ejemplo, sip:+14155551234@ims.example.com)
- **Último P-CSCF Visto** - Último P-CSCF que contactó al HSS
- **Último I-CSCF Visto** - Último I-CSCF que contactó al HSS

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 recargar la 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 conectados
- Verificar la red de servicio actual (para roaming)
- Confirmar el estado de registro de IMS

2. Resolución de Problemas

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

3. Monitoreo de Capacidad

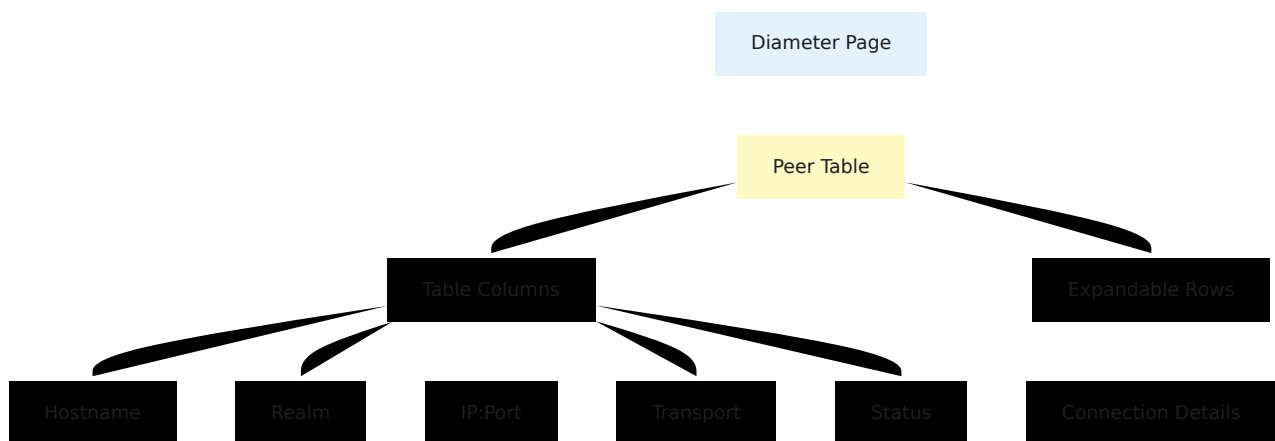
- Contar el total de suscriptores conectados
- Monitorear conteos de sesiones PDN
- Rastrear llamadas VoLTE activas

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.

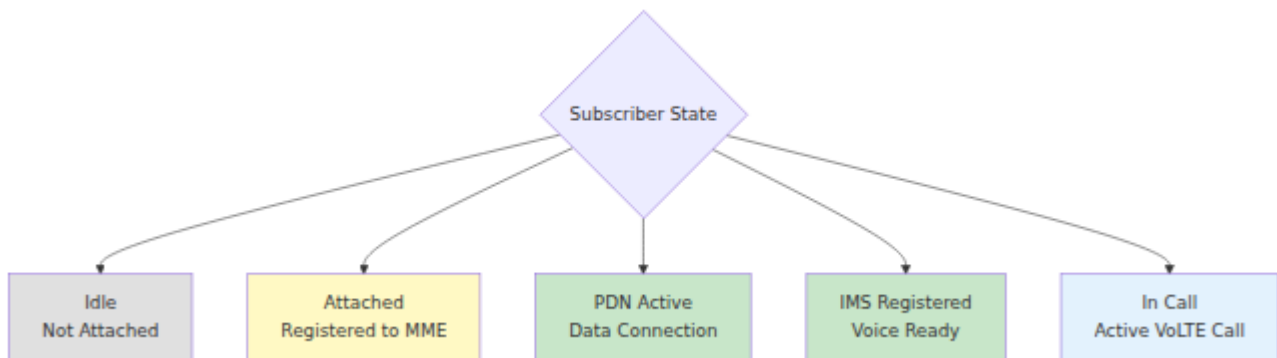
Diseño de la Página



Columnas de la Tabla

Columna	Descripción	Valores
Hostname	Nombre de host del par de Diámetro	FQDN
Realm	Realm 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 Conexión



Detalles de Filas Expandibles

Haz clic en cualquier par para ver información adicional:

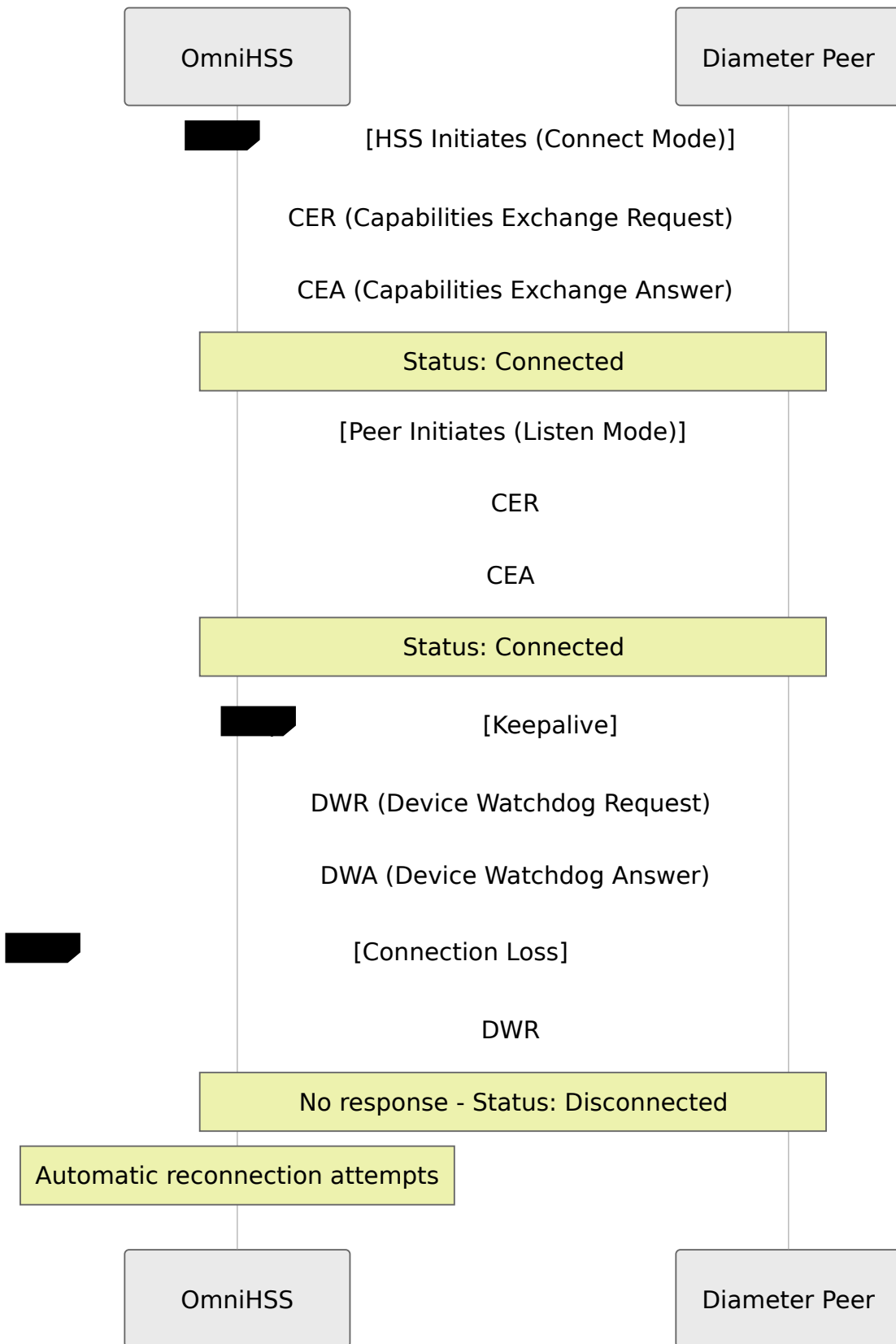
Información de Conexión:

- **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 (Servidor de Aplicaciones)
- 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

Causas Posibles:

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

Pasos de Resolución de Problemas:

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

El Par Se Conecta y Desconecta Repetidamente

Causas Posibles:

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. Verificar 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`

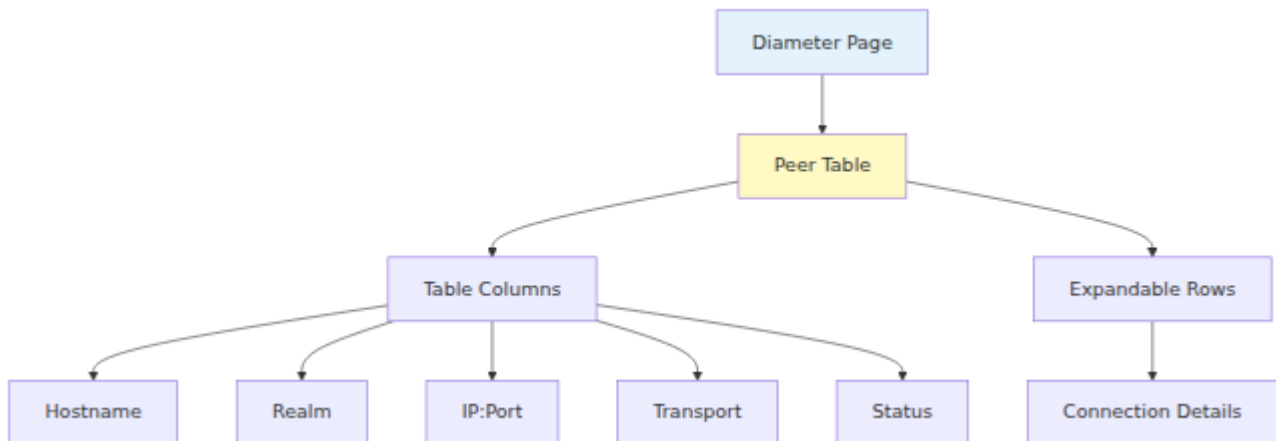
La página de Aplicación proporciona información de monitoreo a nivel de sistema y uso de recursos.

Características

- **Información del Proceso** - 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 ejecución

Métricas Clave



Casos de Uso

1. Monitoreo de Salud

- Verificar que la aplicación esté en funcionamiento
- Comprobar si hay 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 escalabilidad basada en el conteo de procesos
- Verificar recursos del sistema adecuados

3. Resolución de Problemas

- Identificar agotamiento de recursos
 - Comprobar si se necesita reiniciar
 - Verificar la versión de la VM de Erlang
-

Página de Configuración

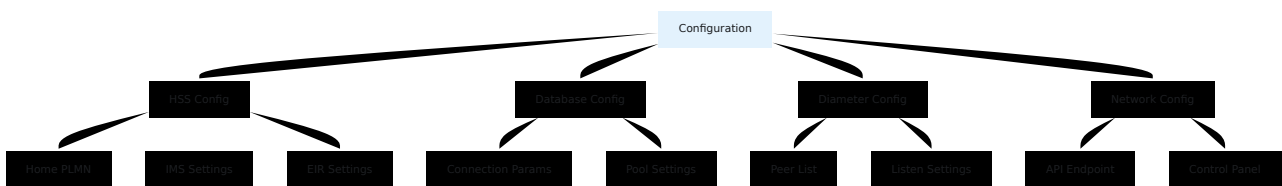
URL: `https://[hostname]:7443/configuration`

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 los ajustes de runtime.exs estén aplicados
- Confirmar parámetros de conexión a la base de datos
- Comprobar la configuración de pares de Diámetro

2. Resolución de Problemas

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

3. Documentación

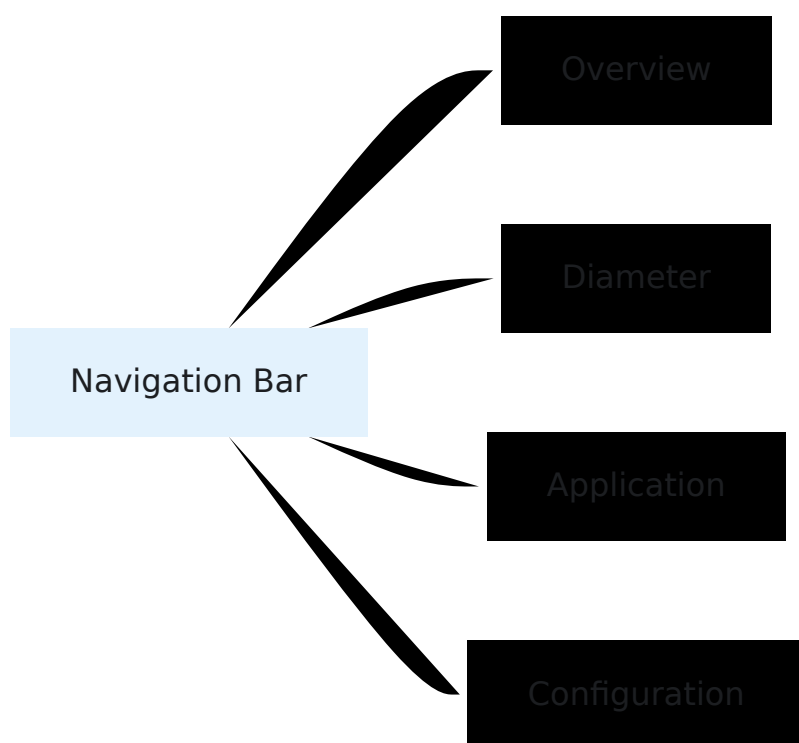
- Exportar la configuración actual para documentación

- 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

Aunque 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 manera independiente.

Diseño Responsivo

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

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

Mejores Prácticas de Monitoreo

Operaciones Diarias

1. Inicio del Turno

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

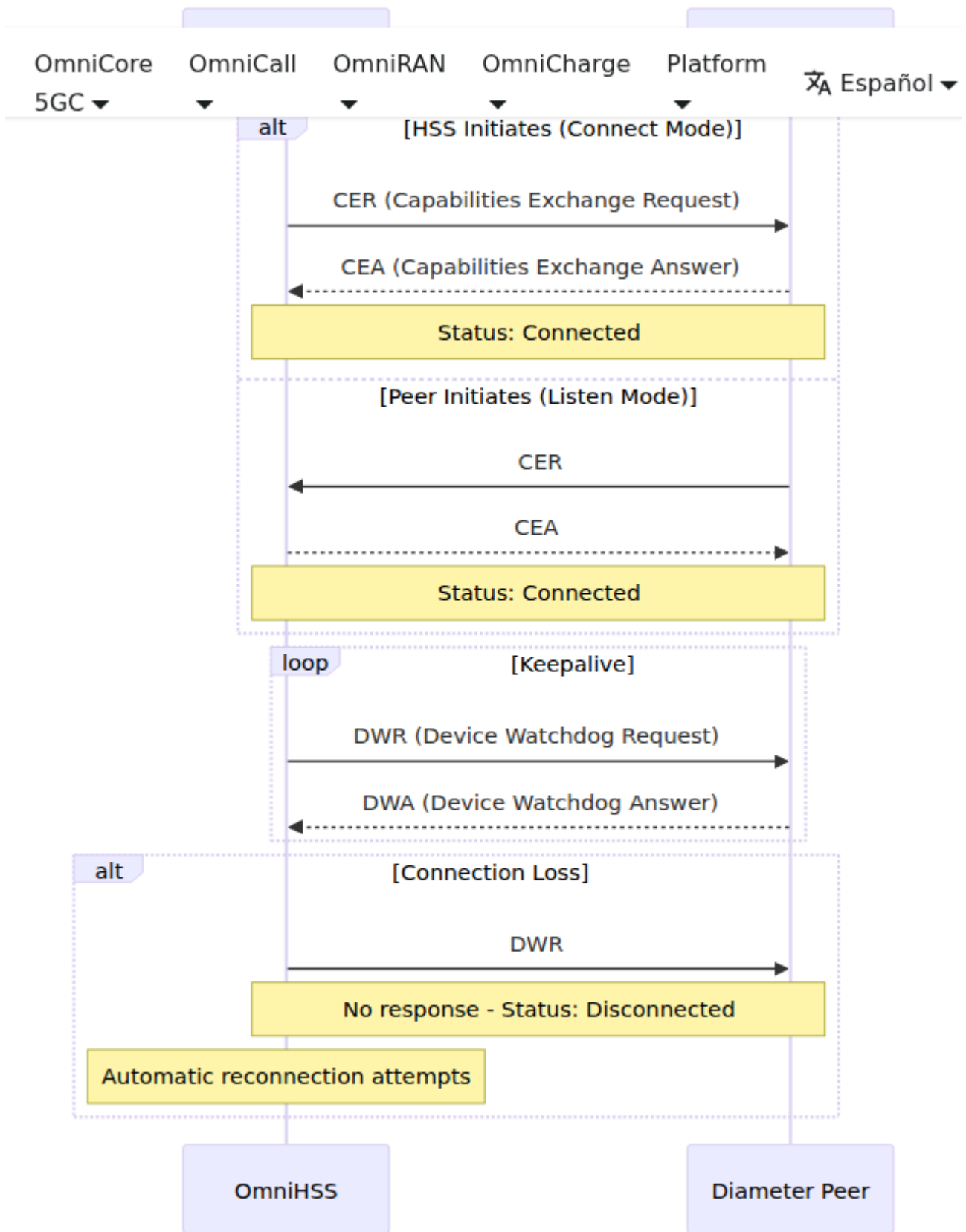
2. Durante el Turno

- 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 del Turno

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

Flujo de Trabajo de 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](#) | [Siguiete: Métricas y Monitoreo](#) →

Relaciones de Entidades de OmniHSS

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

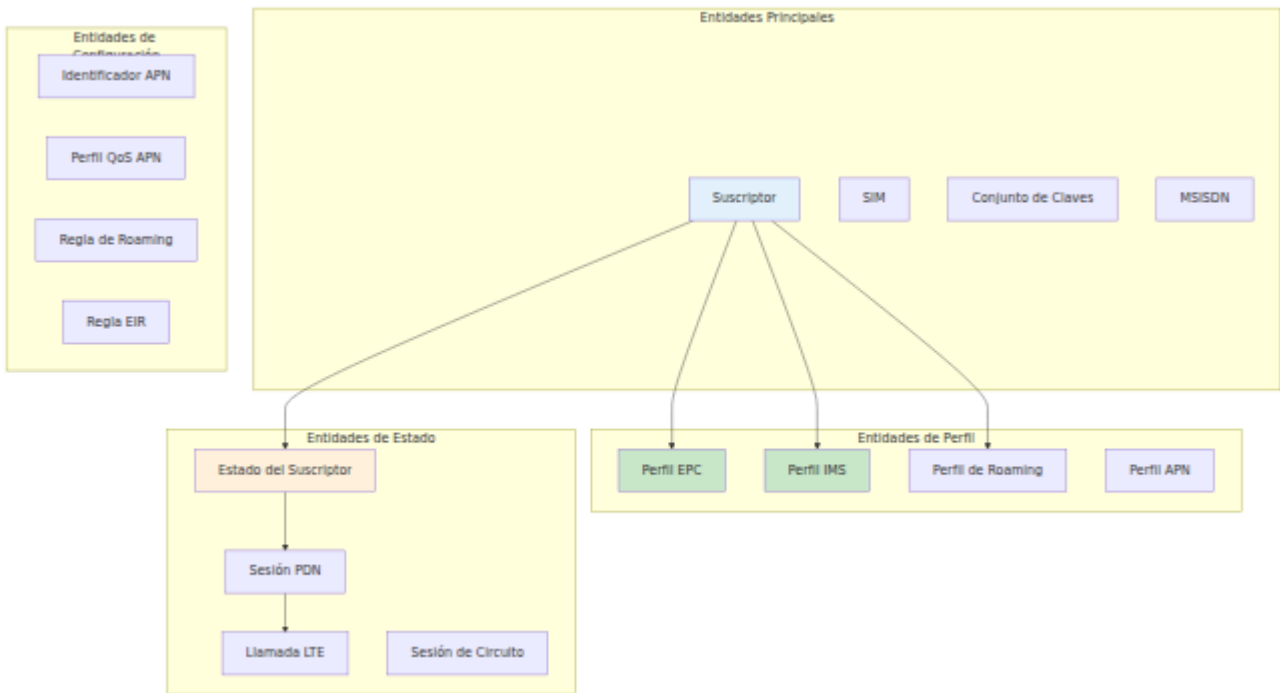
Tabla de Contenidos

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

Descripción de Entidades

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

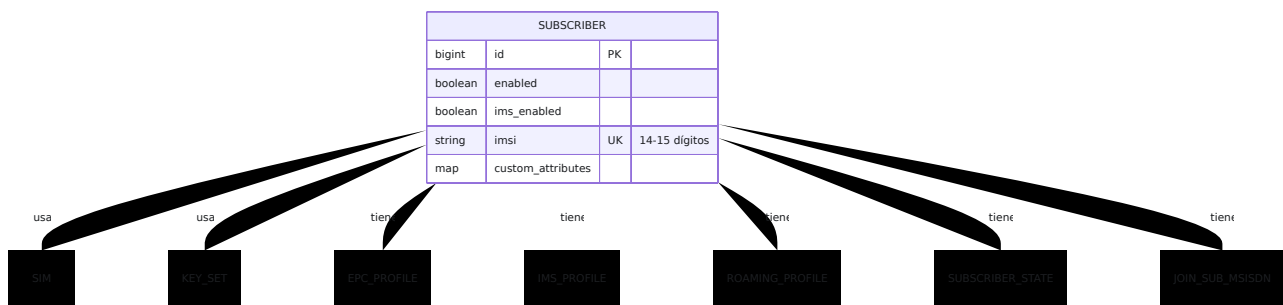
Categorías de Entidades



Entidades Principales

Suscriptor

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



Campos:

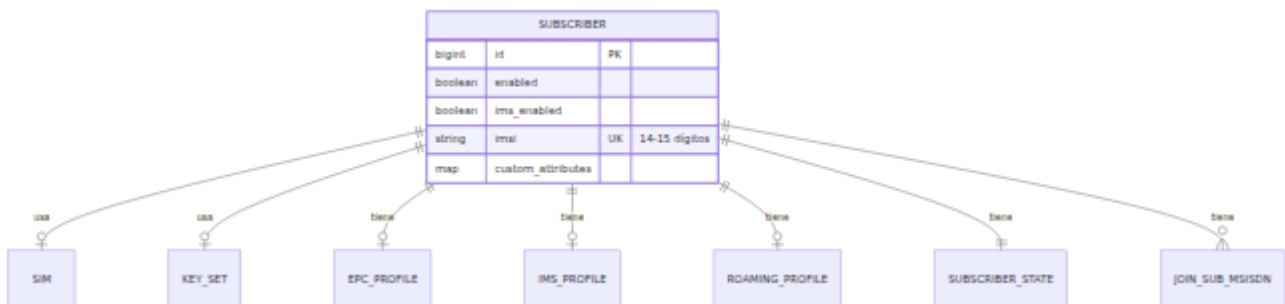
Campo	Tipo	Descripción	Restricciones
<code>id</code>	bigint	Clave primaria	Auto-incremento
<code>enabled</code>	boolean	Indicador de servicio habilitado	Predeterminado: true
<code>ims_enabled</code>	boolean	Servicios IMS habilitados	Predeterminado: true
<code>imsi</code>	string	Identidad Internacional de Suscriptor Móvil	14-15 dígitos, único
<code>custom_attributes</code>	map	Datos personalizados clave-valor	Opcional
<code>sim_id</code>	bigint	Clave foránea a SIM	Opcional
<code>key_set_id</code>	bigint	Clave foránea a Conjunto de Claves	Requerido
<code>epc_profile_id</code>	bigint	Clave foránea a Perfil EPC	Requerido
<code>ims_profile_id</code>	bigint	Clave foránea a Perfil IMS	Opcional
<code>roaming_profile_id</code>	bigint	Clave foránea a Perfil de Roaming	Opcional
<code>subscriber_state_id</code>	bigint	Clave foránea a Estado del Suscriptor	Auto-creado

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
- El indicador `enabled` controla todos los servicios (datos e IMS)
- El indicador `ims_enabled` controla solo los servicios IMS

SIM

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



Campos:

Campo	Tipo	Descripción	Nivel de Seguridad
<code>iccid</code>	string	Identificador de Circuito Integrado	Público
<code>sim_vendor</code>	string	Fabricante de 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 del usuario final
- Los códigos ADM son para operaciones administrativas de SIM
- KIC/KID son para actualizaciones OTA (Over-The-Air) de SIM

Conjunto de Claves

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

KEY_SET			
bigint	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



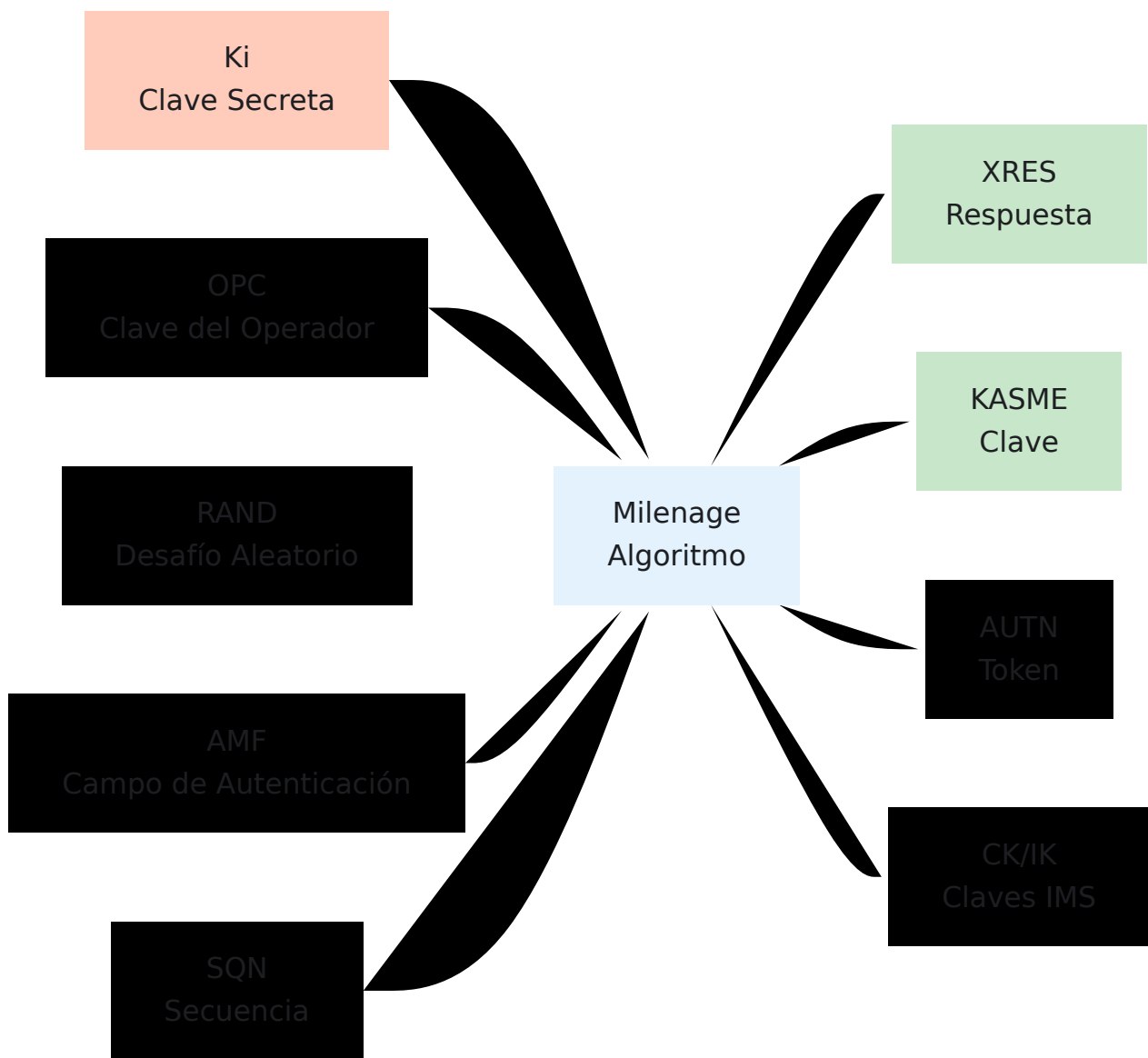
Campos:

Campo	Tipo	Descripción	Tamaño
<code>ki</code>	binary	Clave secreta	128 bits (16 bytes)
<code>opc</code>	binary	Clave variante del operador (derivada)	128 bits
<code>op</code>	binary	Clave del operador (para derivar OPC)	128 bits
<code>amf</code>	binary	Campo de Gestión de Autenticación	16 bits (2 bytes)
<code>sqn</code>	bigint	Número de secuencia (anti-repetición)	48 bits
<code>authentication_algorithm</code>	string	Nombre del algoritmo	Actualmente "milenage"
<code>ota_counter</code>	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 u OP (OPC puede ser derivado de OP)
- SQN se incrementa con cada autenticación
- Milenage es actualmente el único algoritmo soportado

Algoritmo de Autenticación:



MSISDN

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

KEY_SET			
bigint	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		



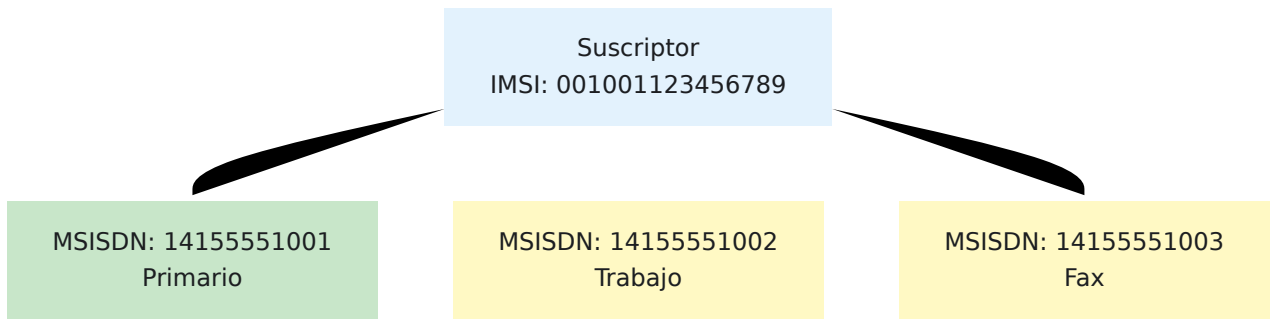
Campos:

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
- Múltiples MSISDNs pueden ser asignados a un suscriptor
- Un MSISDN no puede ser compartido entre múltiples suscriptores
- Formato: Código de país + Número nacional (por ejemplo, "14155551234" para +1 415-555-1234)

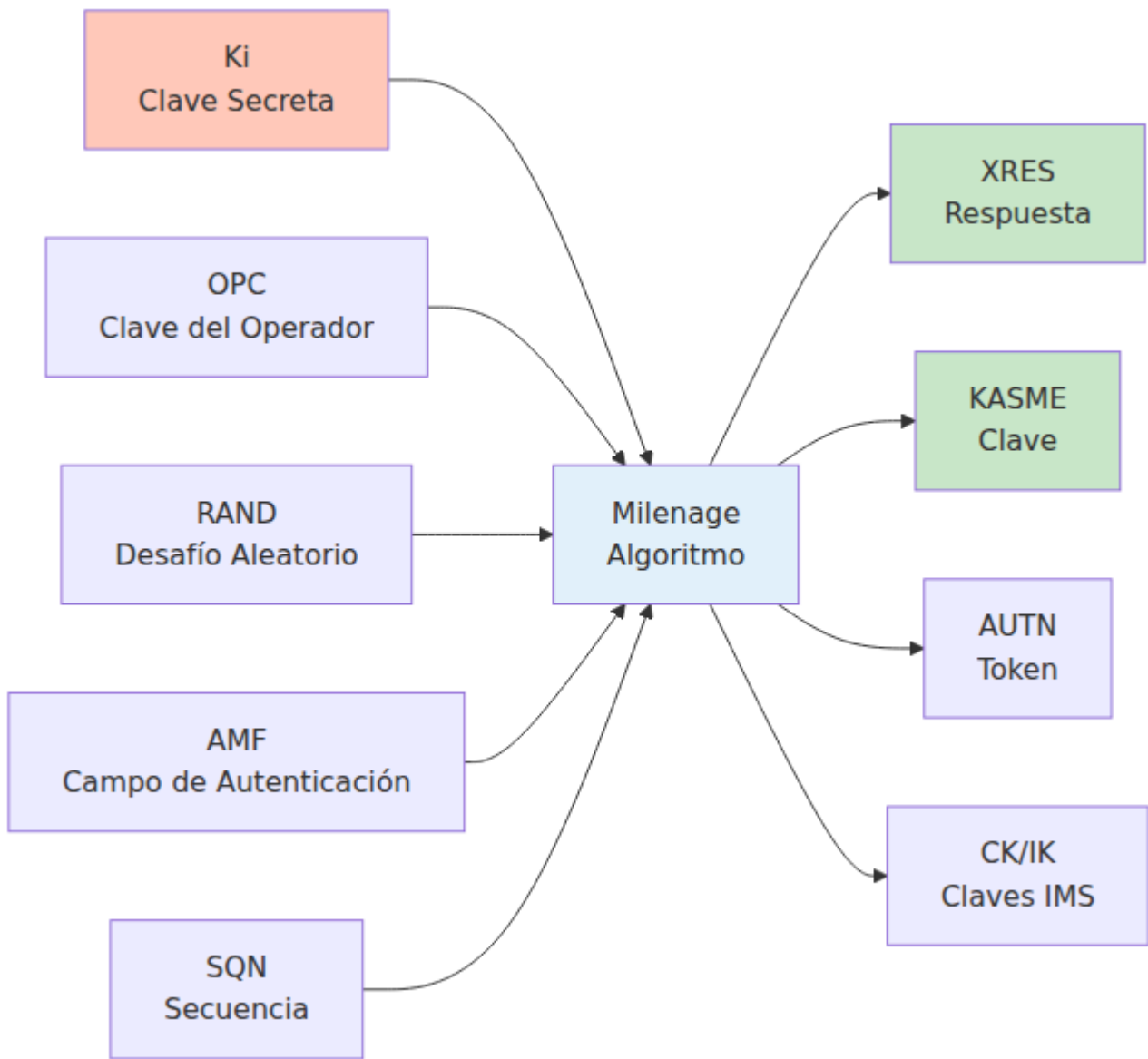
Patrón Multi-MSISDN:



Entidades de Perfil

Perfil EPC

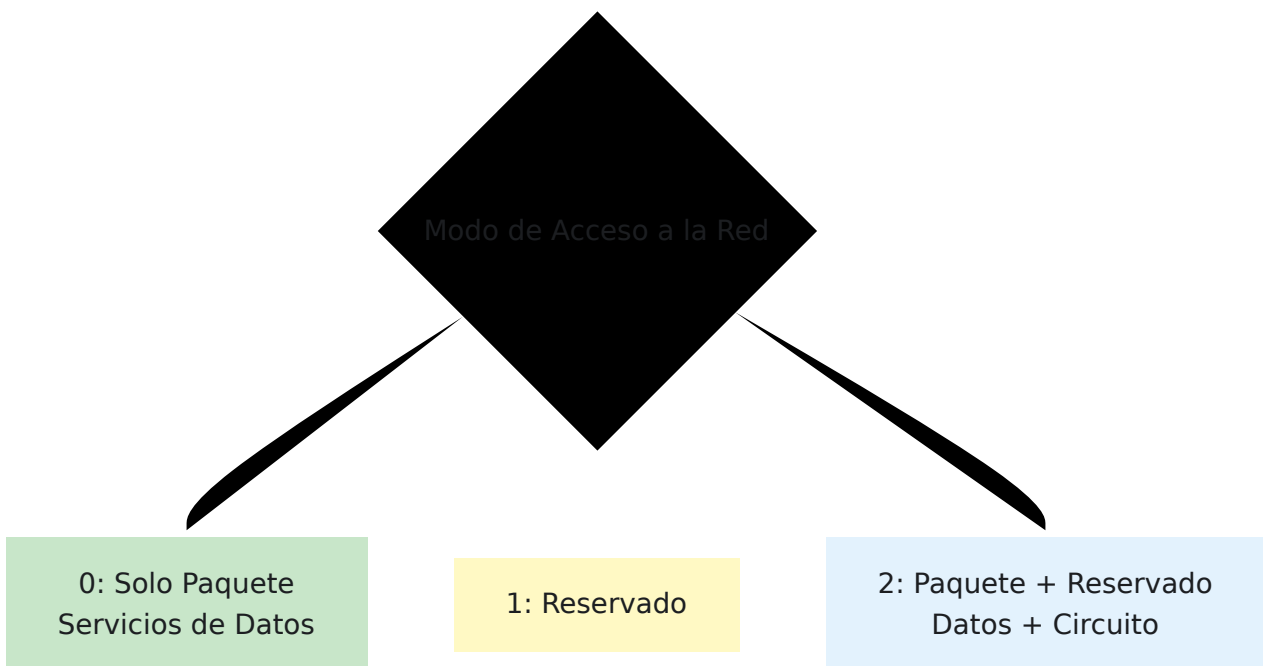
El **Perfil EPC** define las características del servicio de datos para LTE.



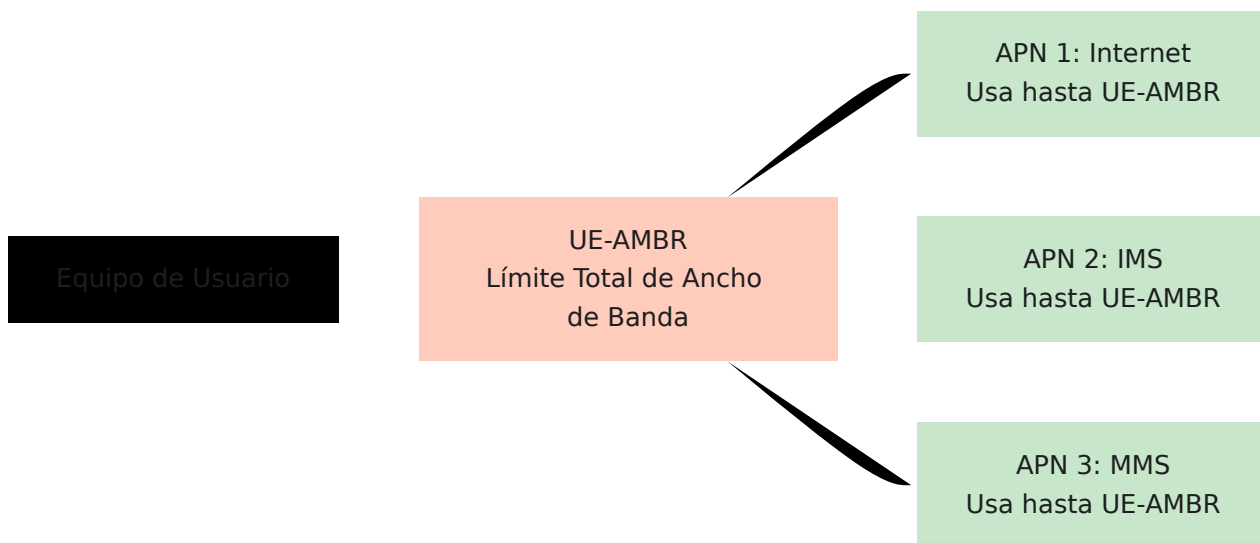
Campos:

Campo	Tipo	Descripción	U
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_" "paqu
tracking_area_update_interval_seconds	integer	Intervalo de TAU	Segun

Modos de Acceso a la Red:

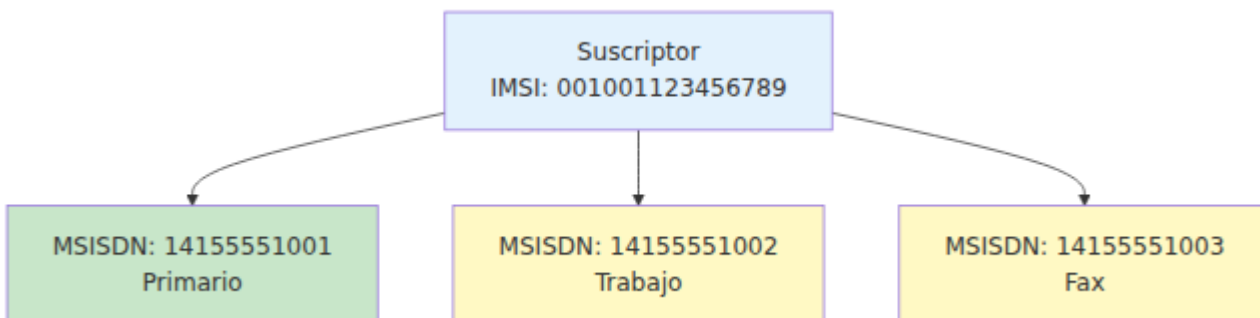


AMBR (Tasa de Bits Máxima Agregada):



Perfil IMS

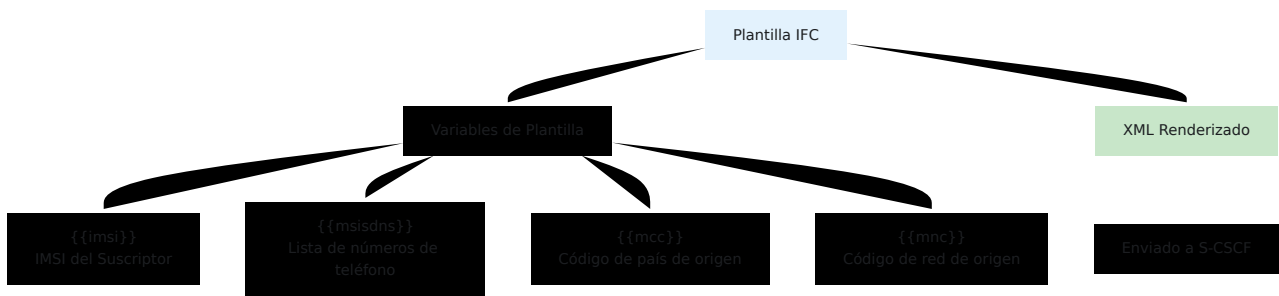
El **Perfil IMS** define las características del servicio de voz/video.



Campos:

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

Variables de Plantilla IFC:

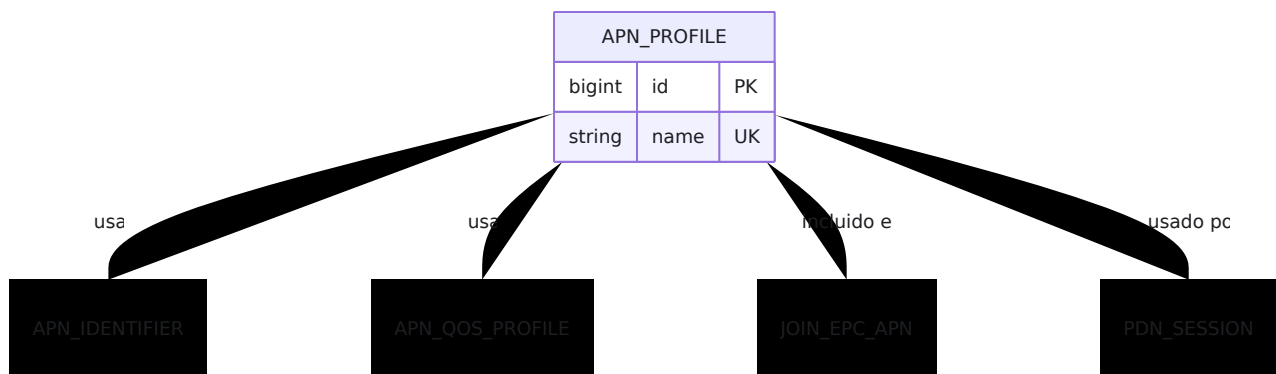


Puntos Clave:

- 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 datos reales del suscriptor
- Se envía a S-CSCF durante el registro IMS

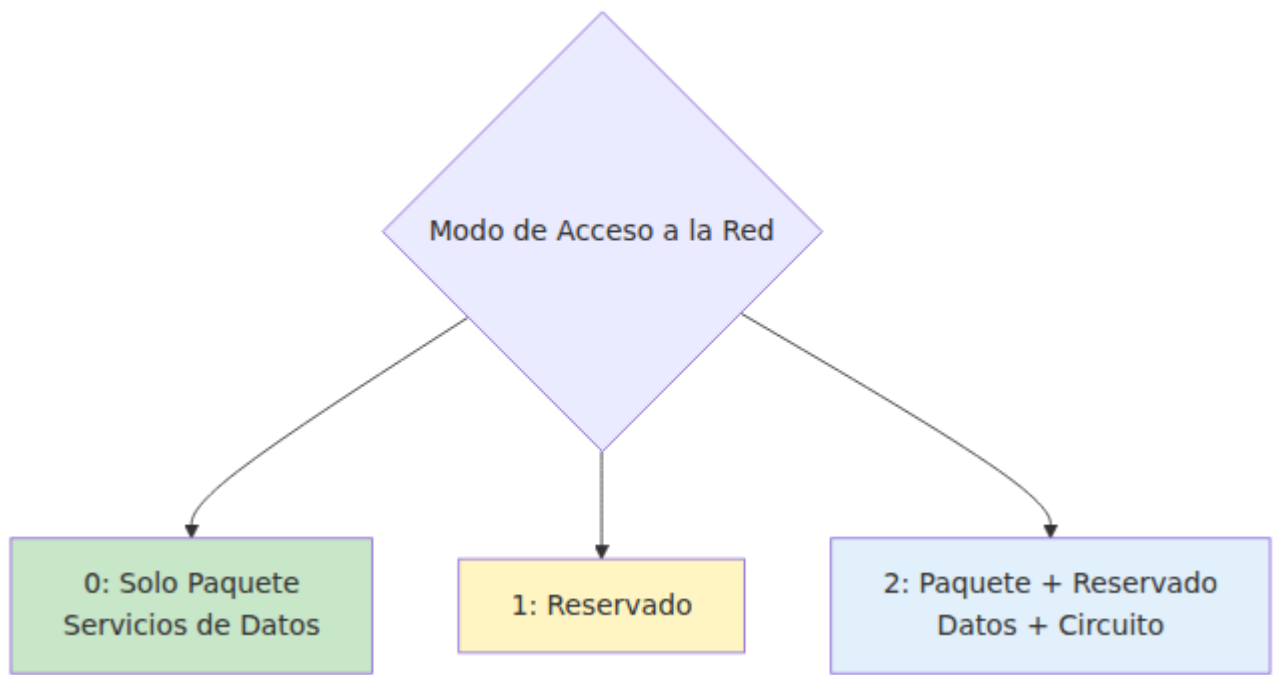
Perfil APN

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



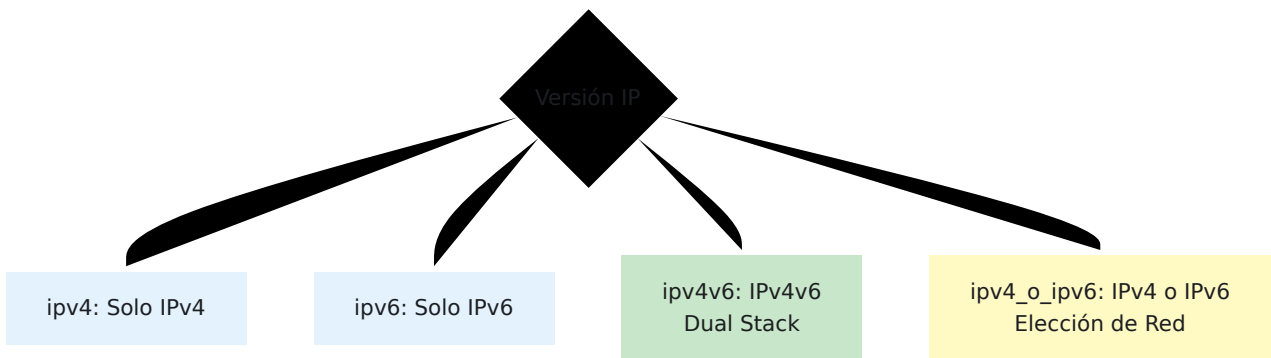
Entidades Relacionadas:

Identificador APN

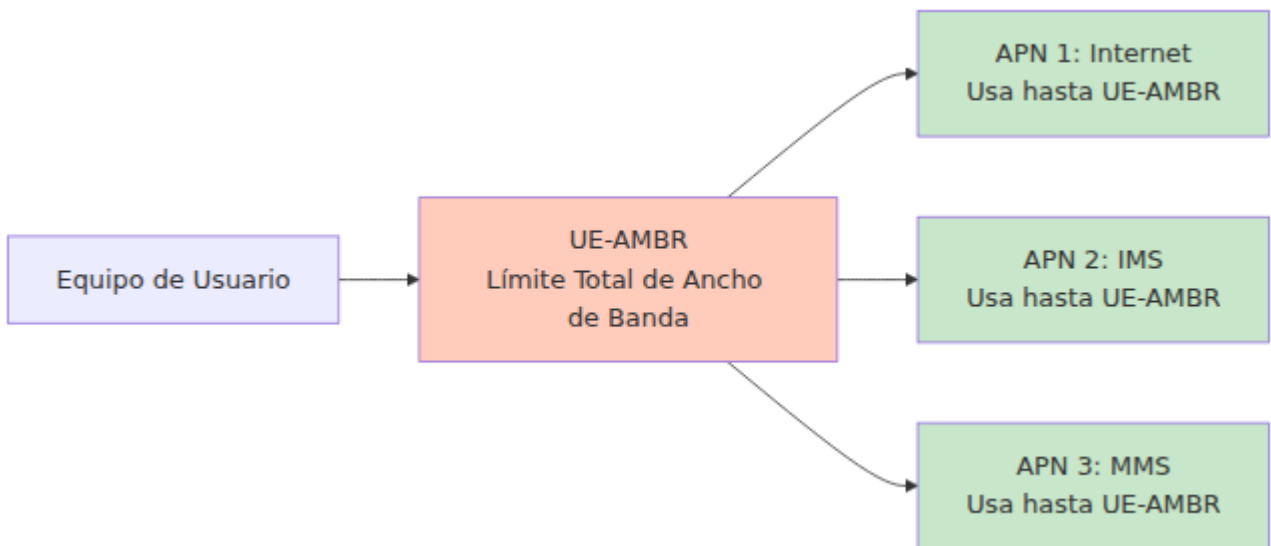


Campo	Tipo	Descripción	Ejemplo
apn	string	Nombre APN	"internet", "ims", "mms"
ip_version	string	Soporte de protocolo IP	Ver abajo

Opciones de Versión IP:



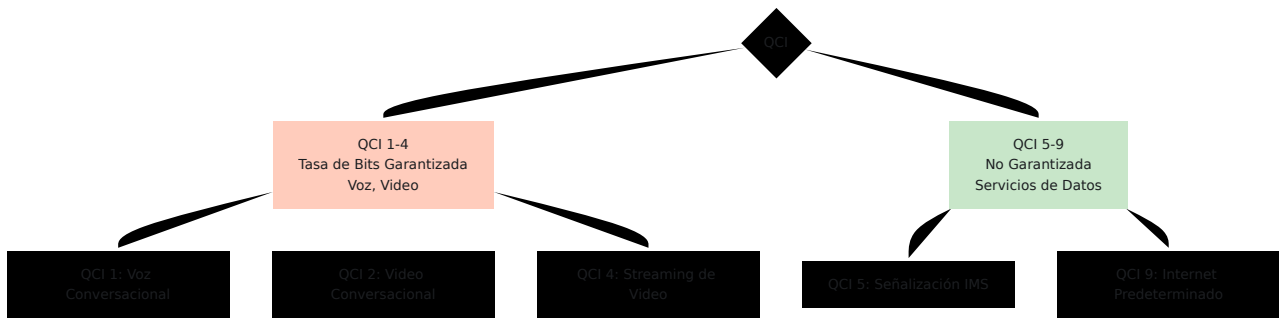
Perfil QoS APN



Parámetros QoS:

Parámetro	Descripción	Rango	Portado Predeterminado
qci	Identificador de Clase QoS	1-9	QCI 9 (Intern
allocation_retention_priority	Prioridad ARP	1-15	8 (prioridad k
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

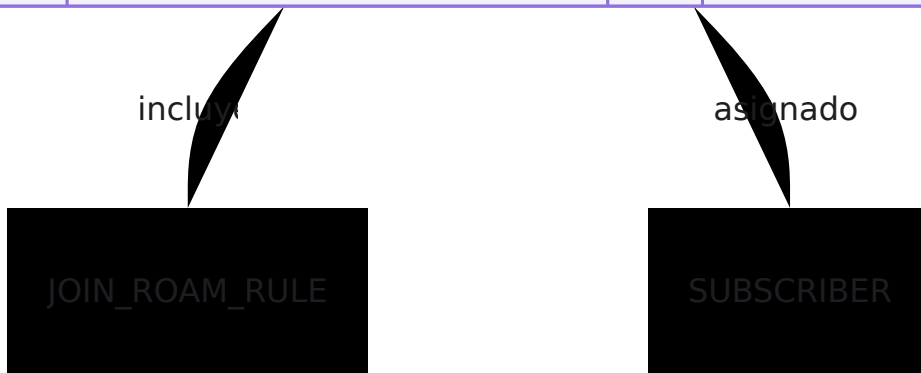
Valores QCI:



Perfil de Roaming

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

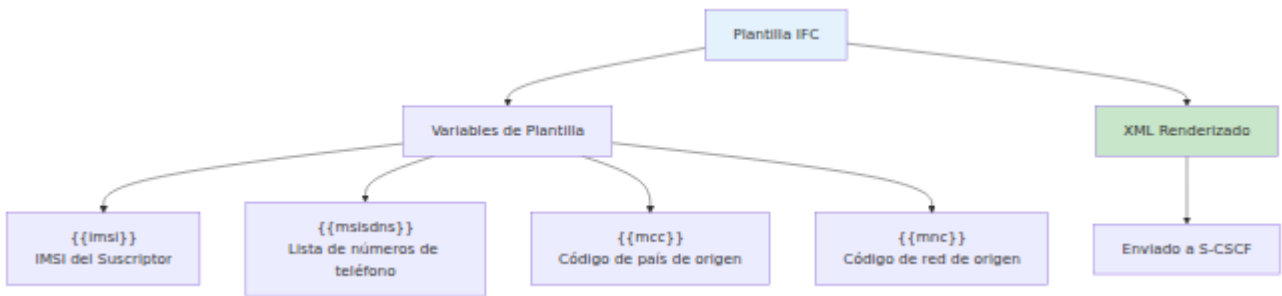
ROAMING_PROFILE			
bigint	id	PK	
string	name	UK	
string	data_action_if_no_rules_match		permitir o denegar
string	ims_action_if_no_rules_match		permitir o denegar



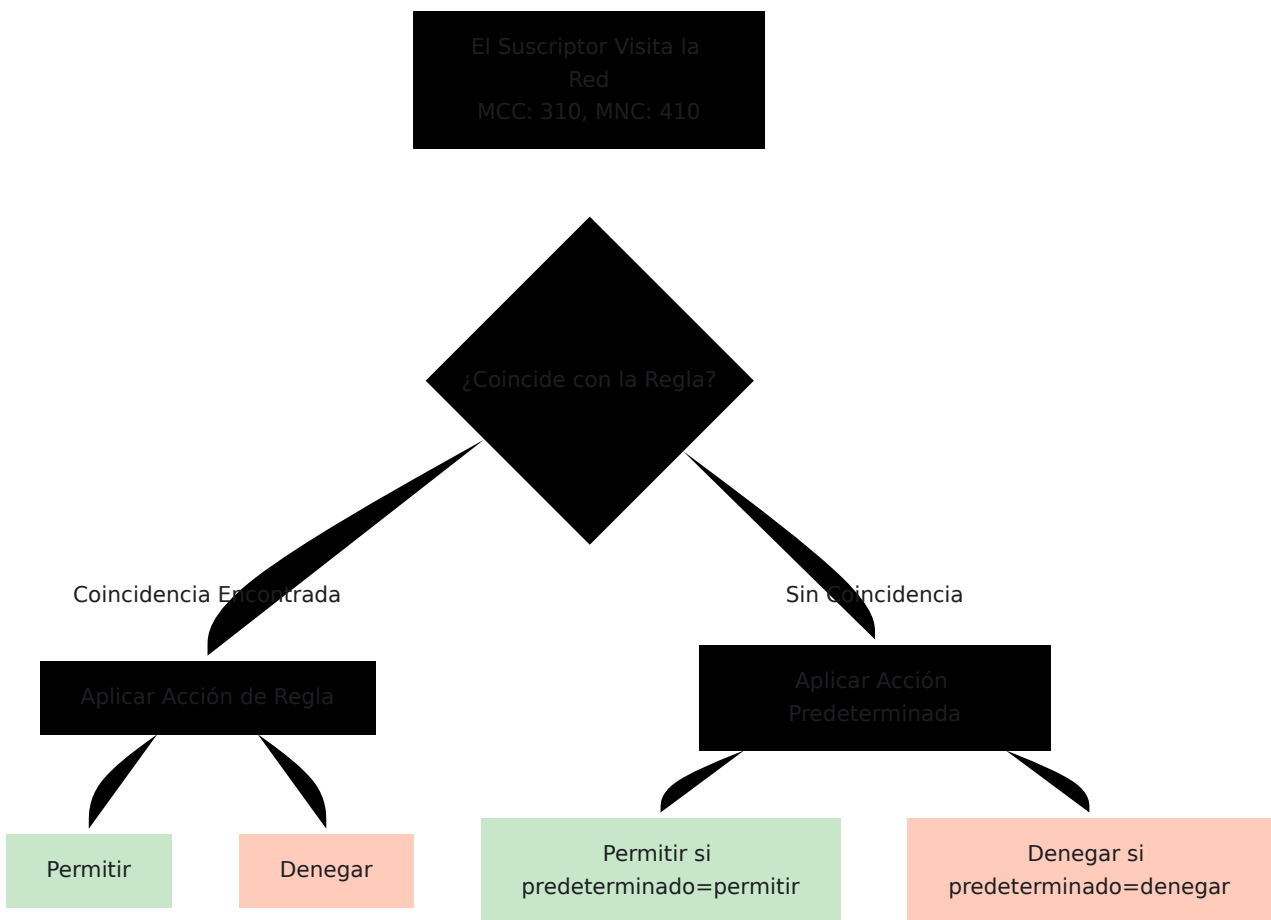
referenci



Regla de Roaming:



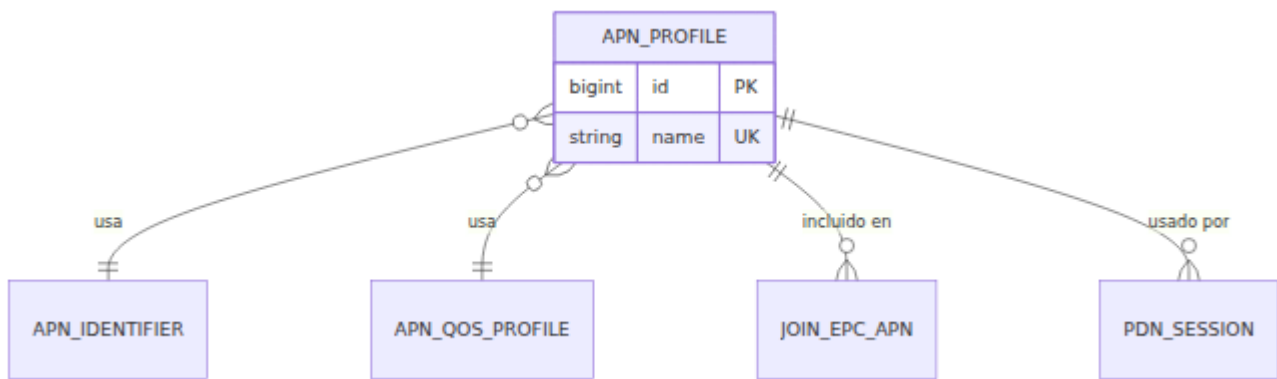
Evaluación de Reglas:



Entidades de Estado

Estado del Suscriptor

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



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_realm` - Dominio Diameter del MME
- `last_seen_rat_type` - Tecnología de Acceso Radio (LTE, 5G, etc.)

Información IMS:

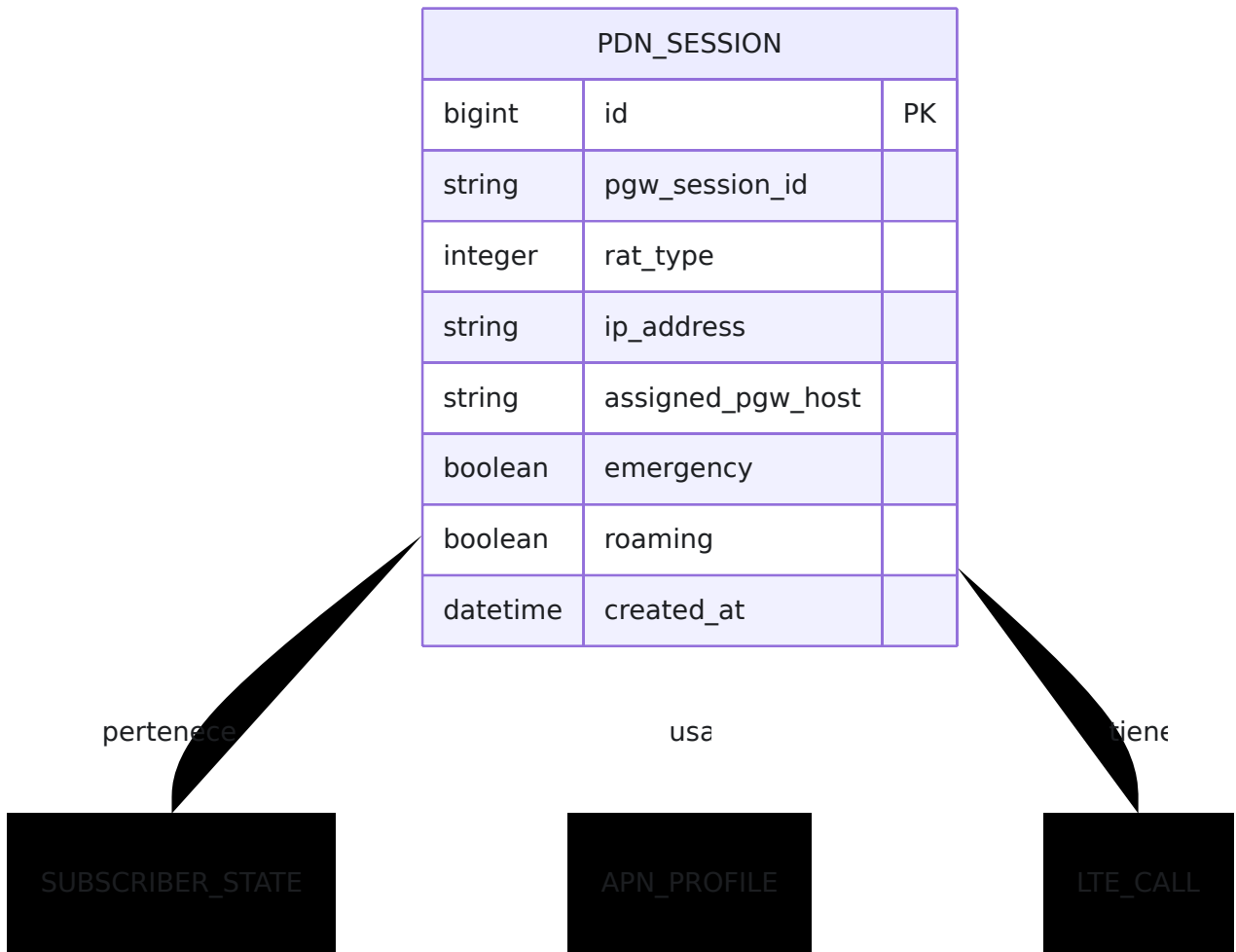
- `assigned_scscf` - S-CSCF actual que atiende al suscriptor
- `ims_public_identity` - URI SIP (por ejemplo, sip:+14155551234@ims.example.com)
- `sh_repository_data` - Datos de perfil IMS personalizados

Tiempos:

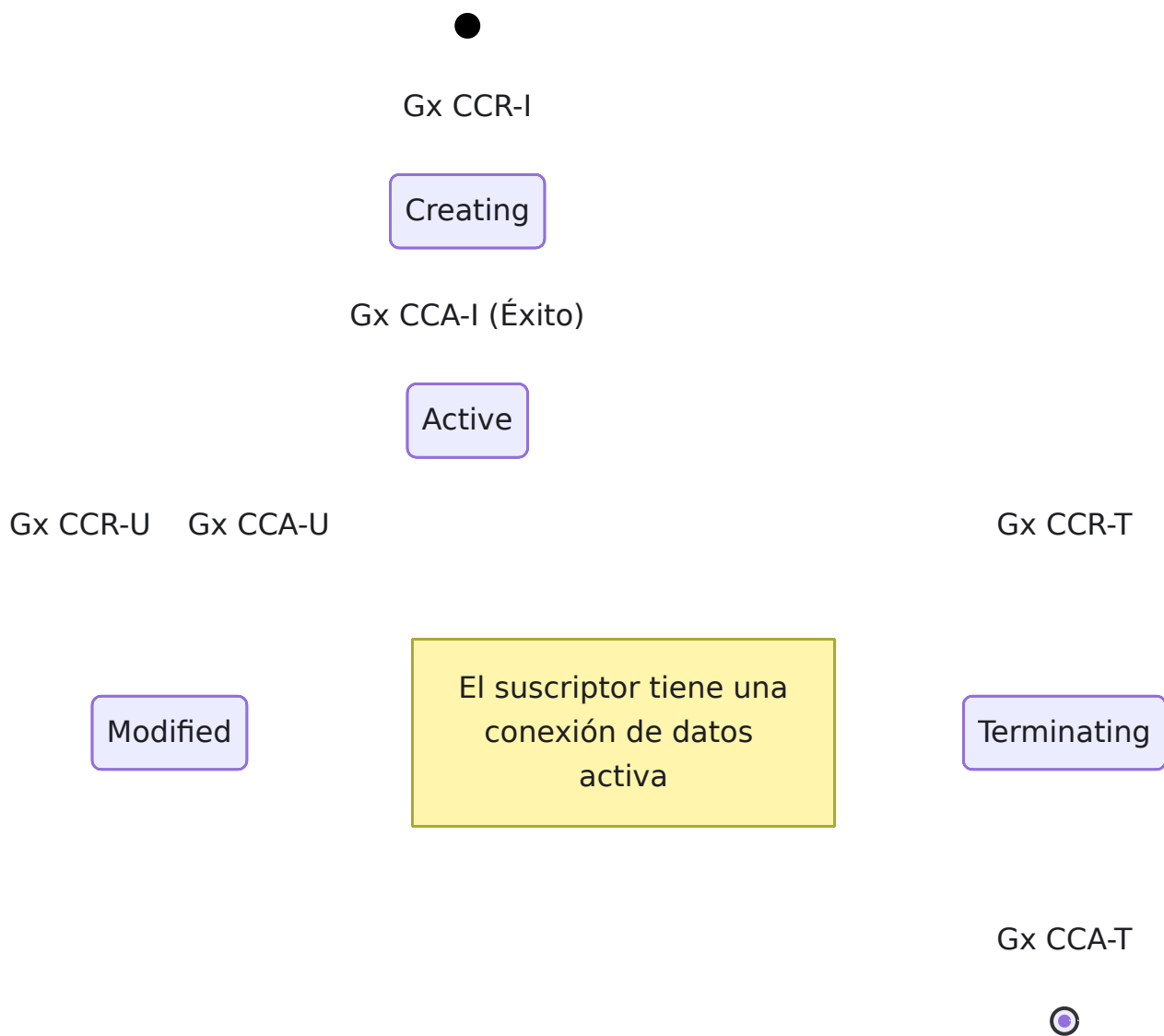
- `last_seen_at` - Último mensaje Diameter recibido
- Varios timestamps `last*_at` para diferentes procedimientos

Sesión PDN

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

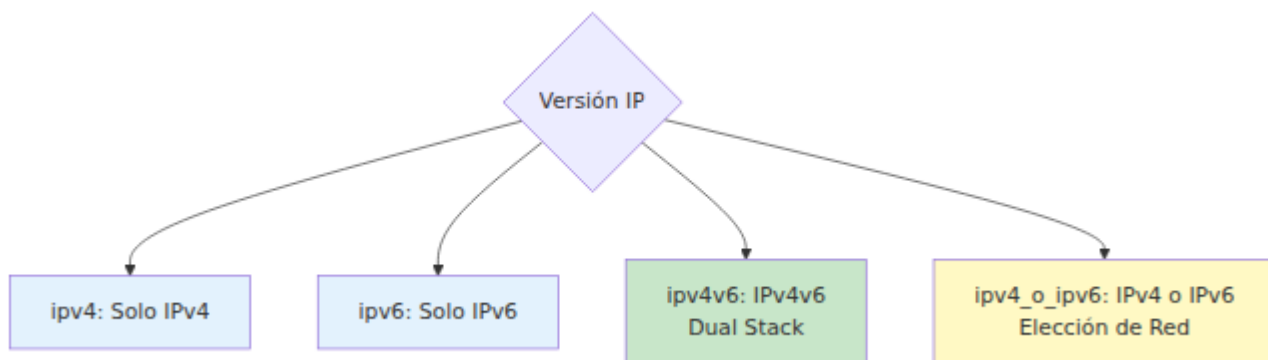


Ciclo de Vida de la Sesión PDN:

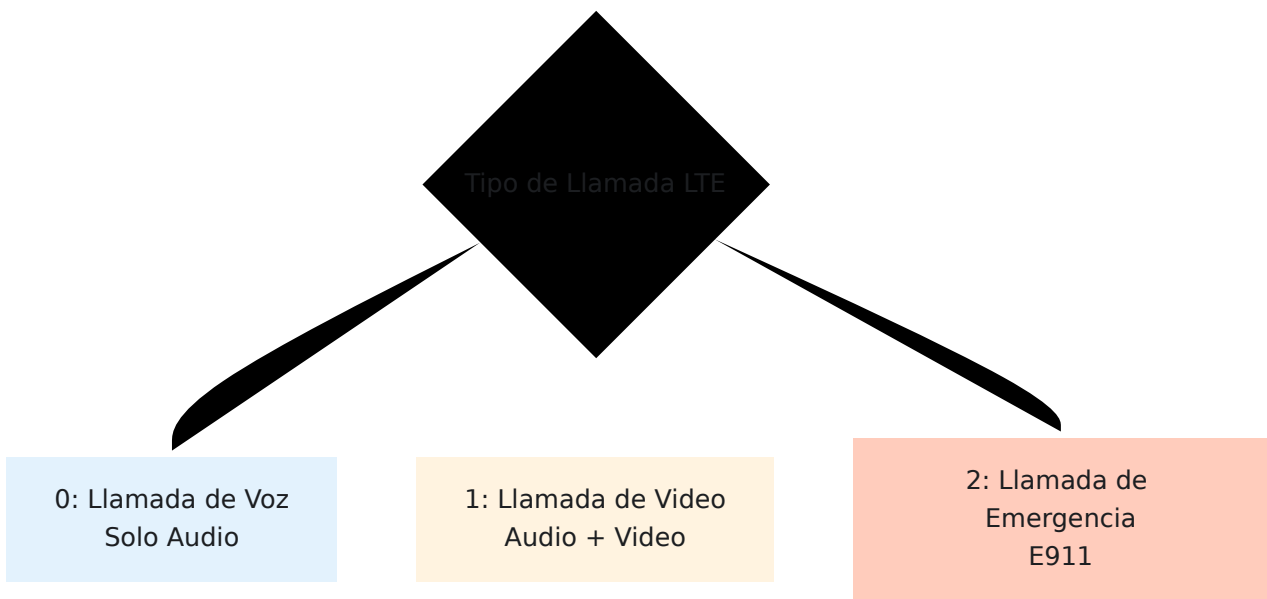


Llamada LTE

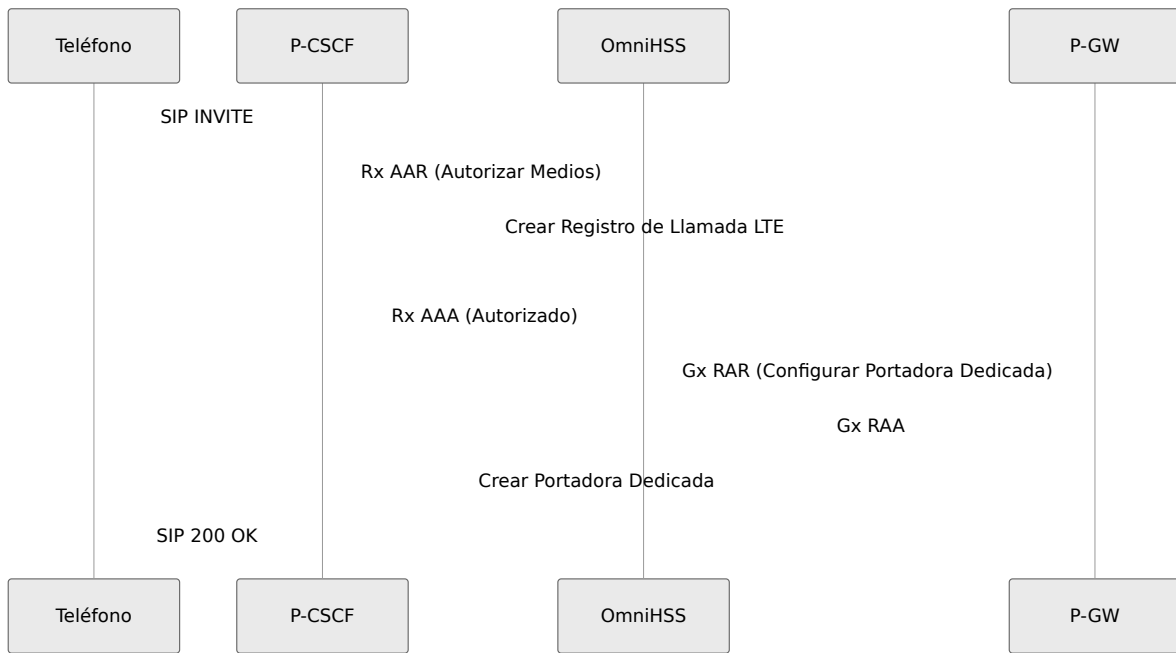
La **Llamada LTE** representa una llamada de voz/video VoLTE activa.



Tipos de Llamadas:

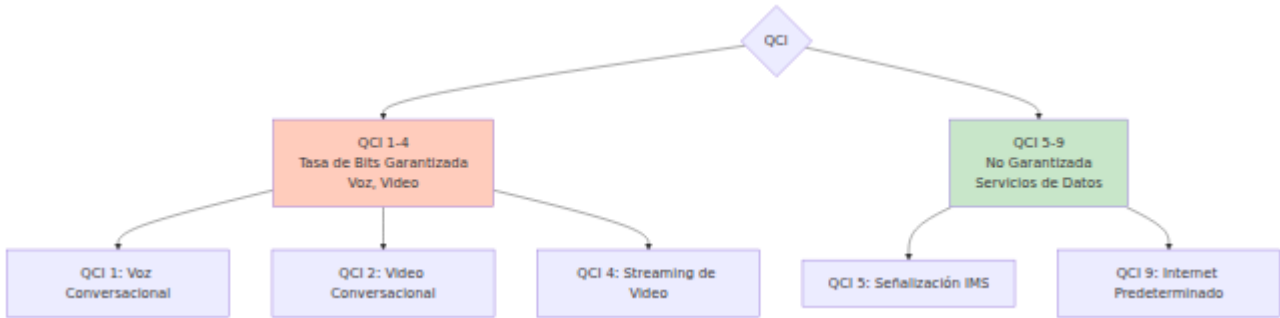


Flujo de Llamada VoLTE:



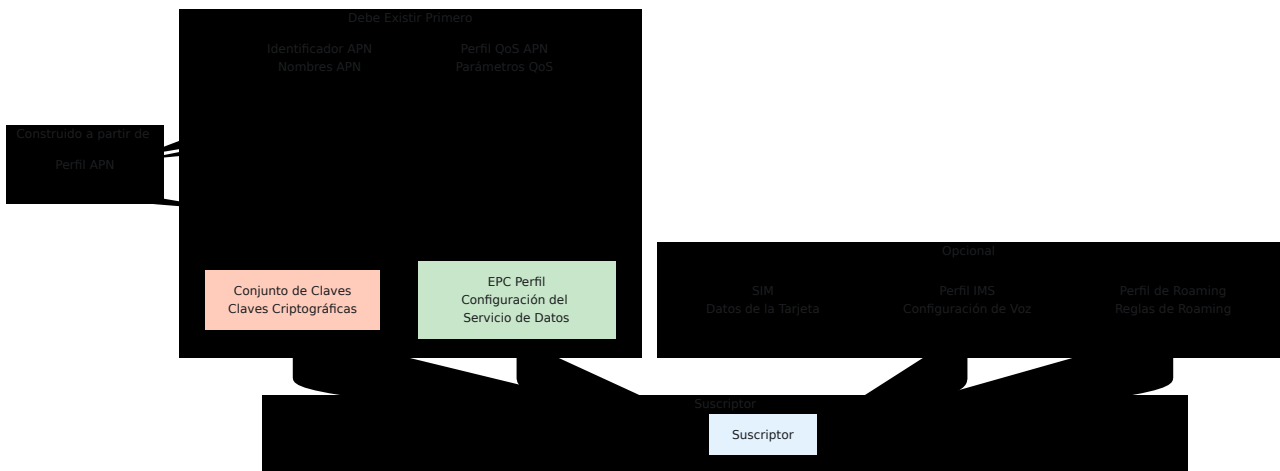
Diagramas de Relaciones de Entidades

Relaciones Completas de Entidades

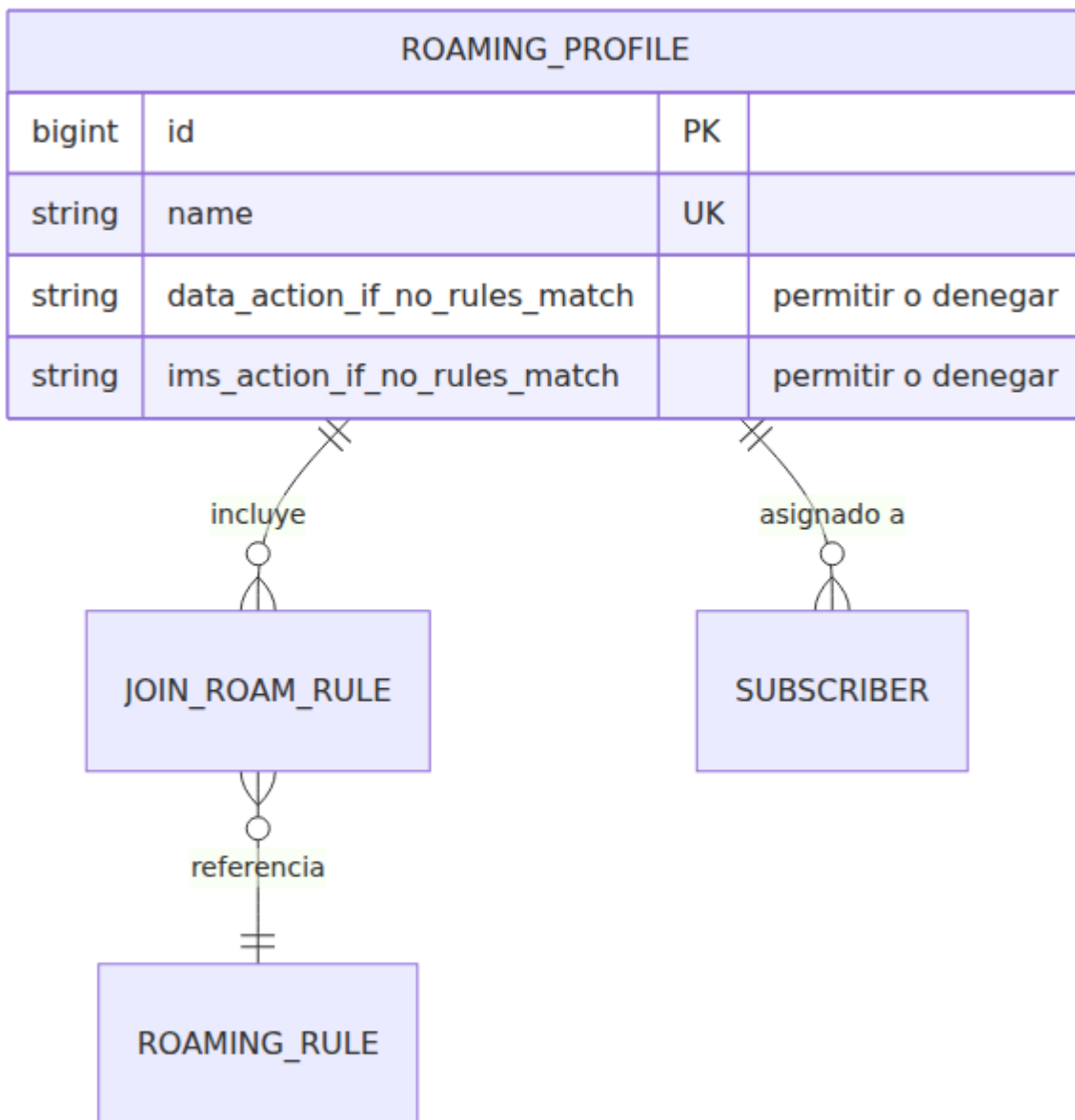


Relaciones de Aprovisionamiento

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



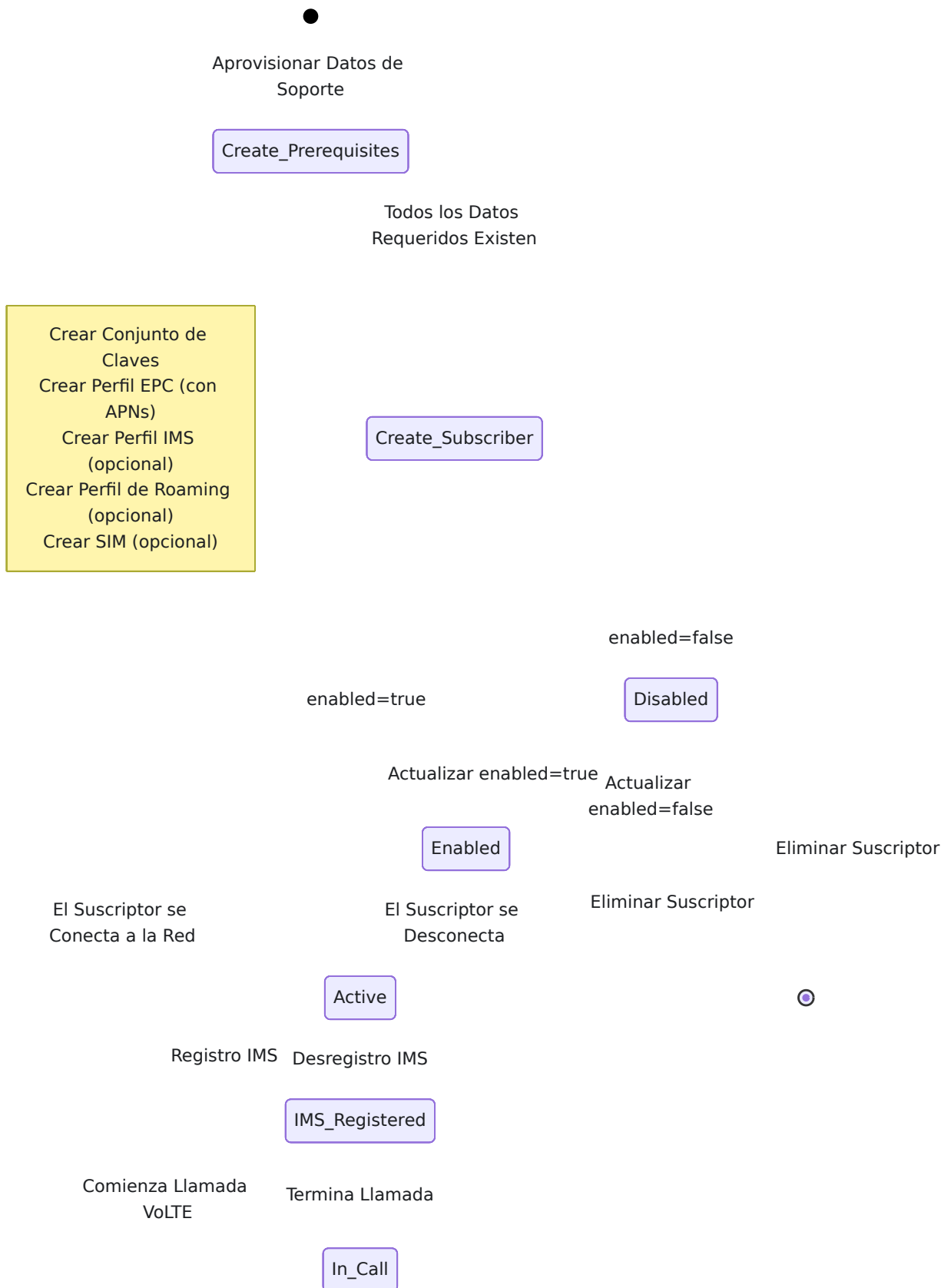
Relaciones de Estado de Sesión



Ciclo de Vida de la Entidad

Ciclo de Vida de Aprovisionamiento del

Suscriptor



Ciclo de Vida de la Sesión



Suscriptor Inactivo

No_Sessions

Comienza Conexión de
Datos

Termina Conexión de
Datos

PDN_Active

Comienza Llamada
VoLTE

Termina Llamada VoLTE

El registro de la Sesión
PDN existe
en la base de datos

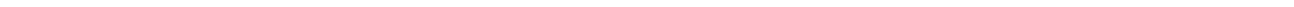
PDN_And_Call

Comienza Segunda
Llamada

Termina Segunda
Llamada

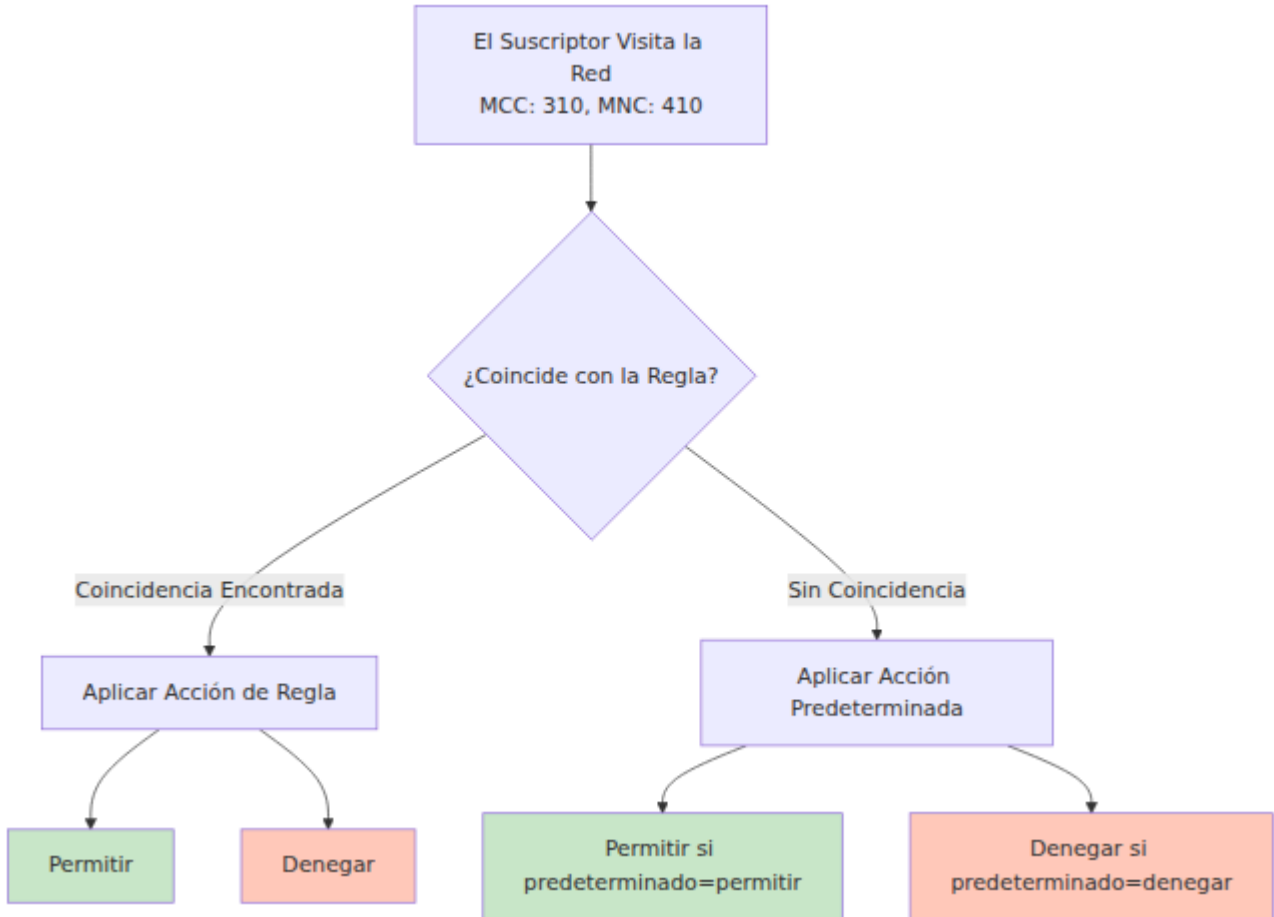
Multiple_Calls

Registros de Sesión
PDN + Llamada LTE
existen



Patrones de Flujo de Datos

Flujo de Autenticación



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

Cx Solicitud SAR

Buscar Suscriptor
por IMSI/MSISDN

Cargar Perfil IMS
+ MSISDNs

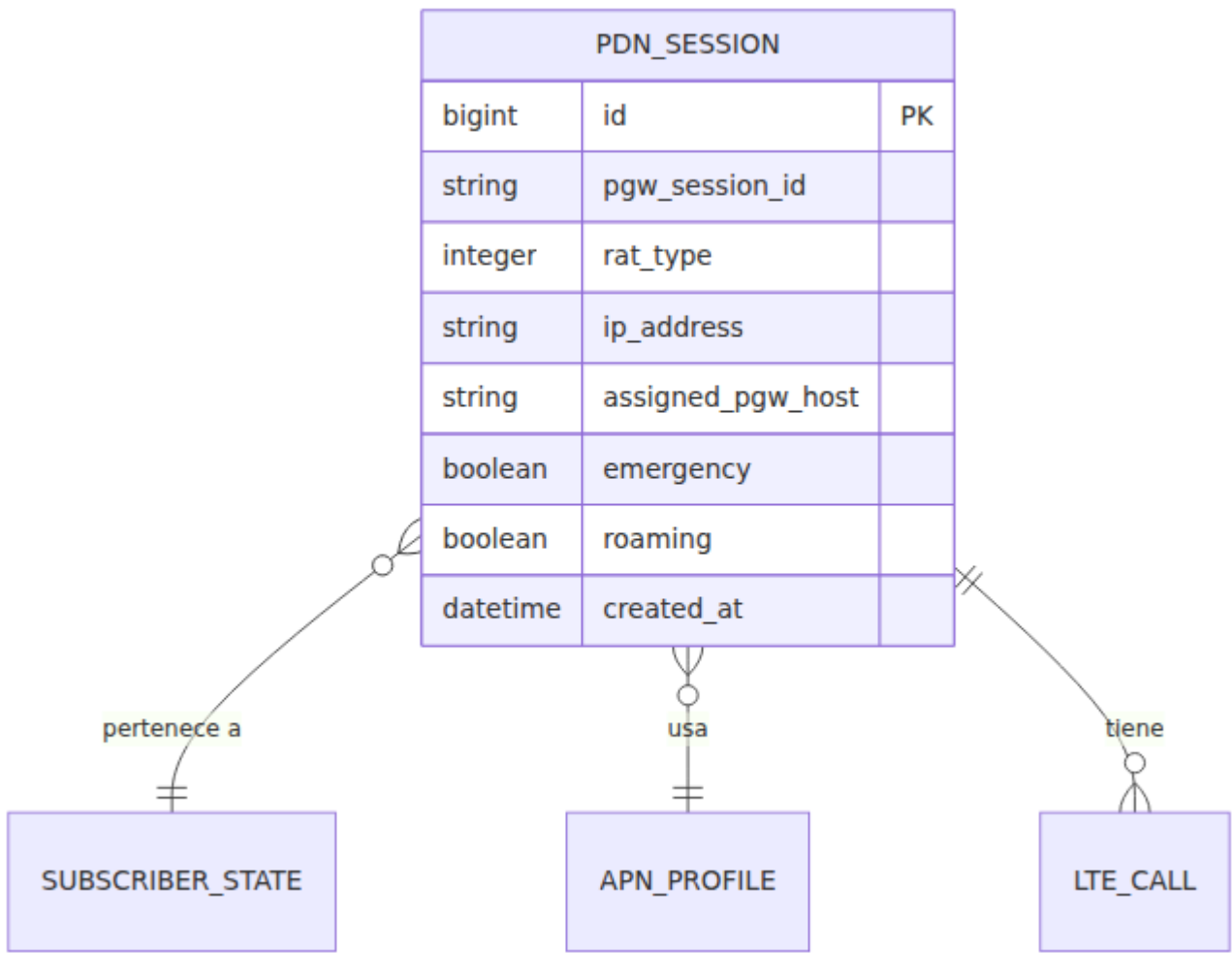
Seleccionar S-CSCF
Aleatorio/Round-Robin

Renderizar Plantilla IFC
con Variables

Actualizar Estado del
Suscriptor
Asignación S-CSCF

Cx Respuesta SAA

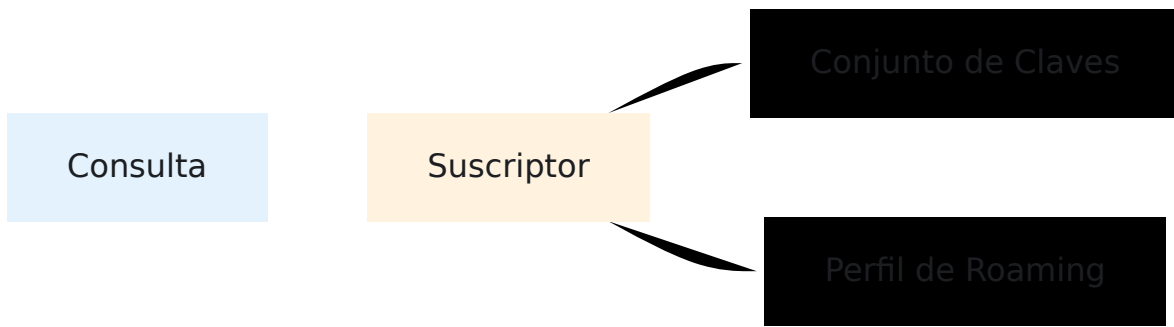
Flujo de Establecimiento de Sesión



Patrones de Optimización de Consultas

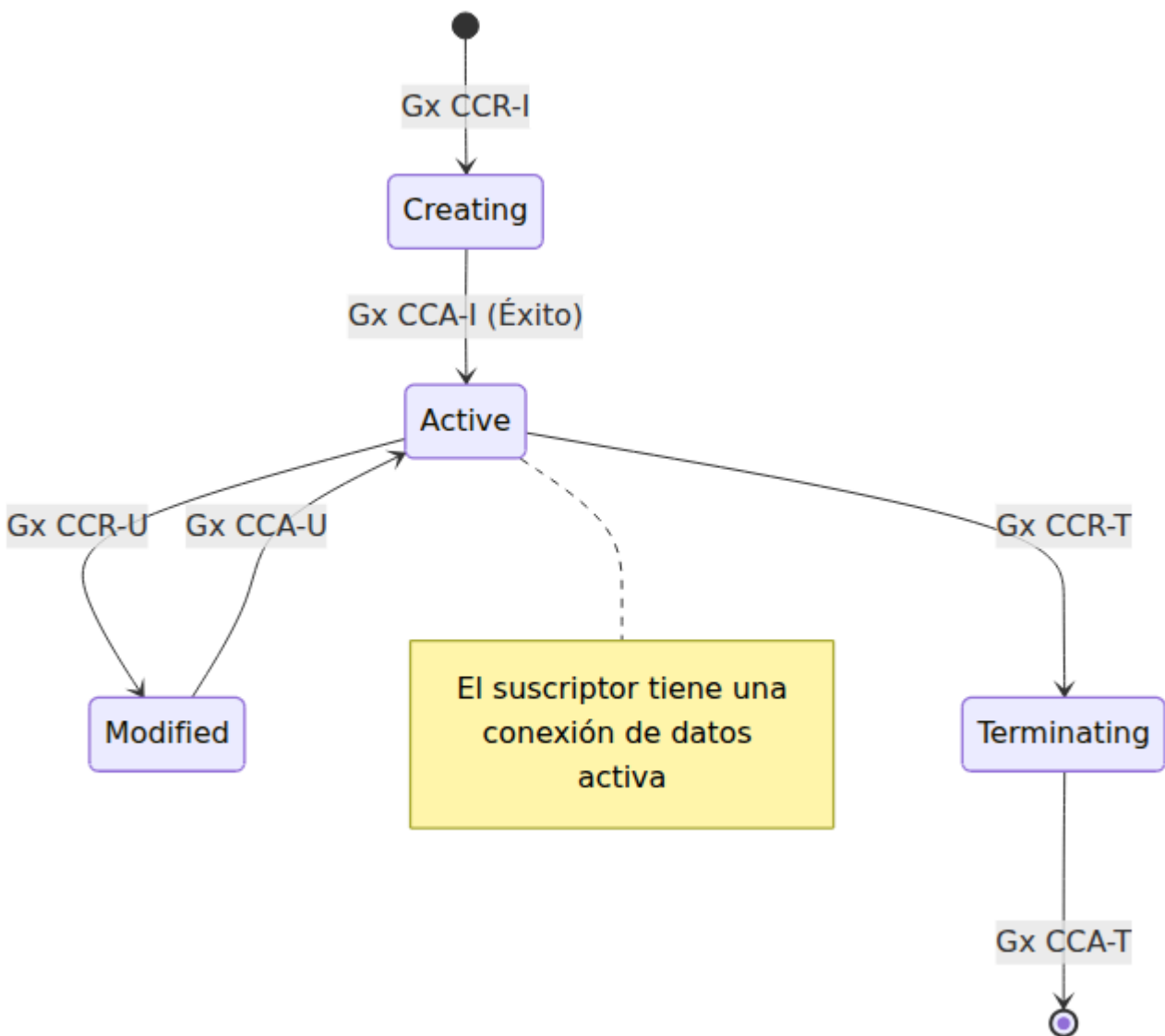
OmniHSS optimiza las consultas a la base de datos pre-cargando selectivamente solo las asociaciones necesarias para cada operación:

Consulta Mínima (Autenticación)



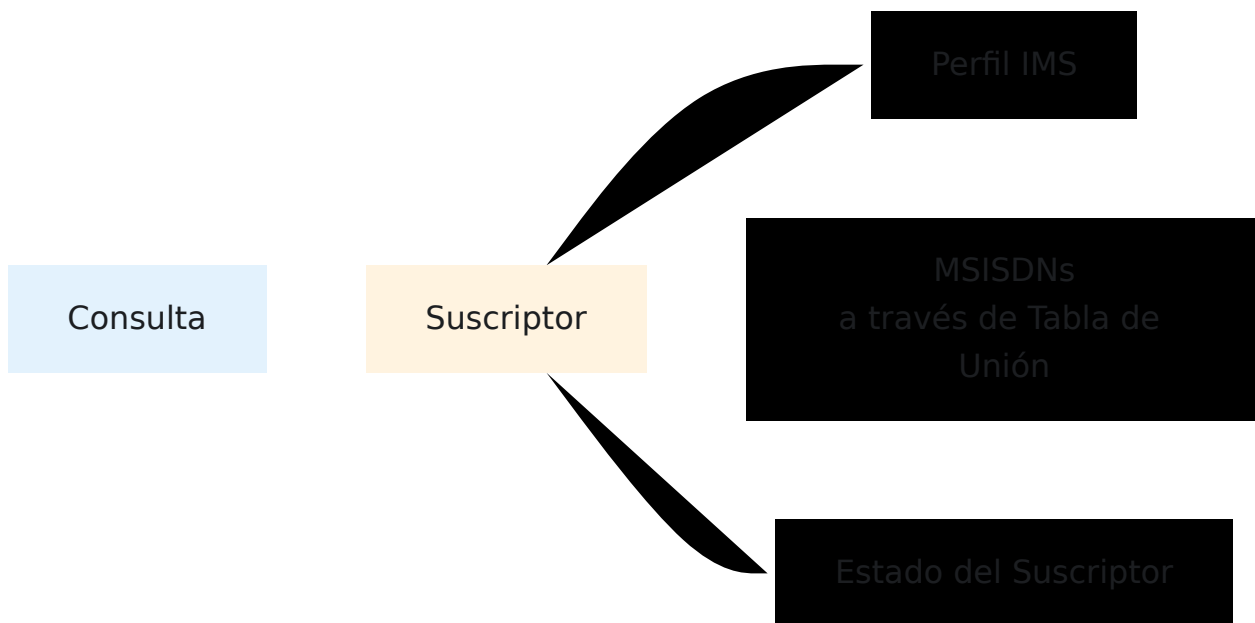
Caso de Uso: S6a AIR - Solo necesita claves criptográficas y reglas de roaming

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](#) | [Siguiete: Referencia de API](#) →

Replicación de Base de Datos Galera

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

Tabla de Contenidos

- [Opciones de Backend de Base de Datos](#)
 - [Descripción General](#)
 - [Cómo Funciona Galera](#)
 - [Arquitectura de Implementación](#)
 - [Referencia de Configuración](#)
 - [Proceso de Bootstrap](#)
 - [Operaciones](#)
 - [Monitoreo](#)
 - [Solución de Problemas](#)
-

Backend de Base de Datos

OmniHSS está construido en Elixir utilizando **Ecto** como su capa de abstracción de base de datos. Ecto soporta múltiples backends de bases de datos relacionales, permitiendo flexibilidad en la selección de la base de datos.

MariaDB con Galera Cluster es una configuración soportada, documentada [aquí](#).

Se pueden utilizar otros backends de bases de datos relacionales dependiendo de los requisitos de infraestructura y preferencias operativas. **Trabaje con su equipo de integración en Omnitouch Network Services (ONS)** para determinar el backend de base de datos y la estrategia de replicación más apropiados para su entorno.

MariaDB con Galera

Base de Datos	Opciones de Replicación
MariaDB 10.6+	Galera Cluster (este documento)

Elegir el Enfoque Correcto

La mejor estrategia de base de datos y replicación depende de su entorno:

- Infraestructura de base de datos existente y experiencia operativa
- Número de nodos HSS y distribución geográfica
- Requisitos de disponibilidad y conmutación por error
- Latencia de red entre nodos

Su equipo de integración de ONS puede asesorar sobre:

- Qué backend de base de datos se adapta a su infraestructura
- Topología de replicación apropiada para sus requisitos de disponibilidad
- Ajuste de rendimiento para su volumen de suscriptores
- Integración con sus sistemas de monitoreo y respaldo existentes

Descripción General

Este documento cubre **MariaDB Galera Cluster**, la opción principal de replicación para implementaciones de alta disponibilidad de OmniHSS. Galera proporciona replicación multi-maestro síncrona, asegurando que todos los nodos HSS compartan datos idénticos de suscriptores con conmutación por error automática.

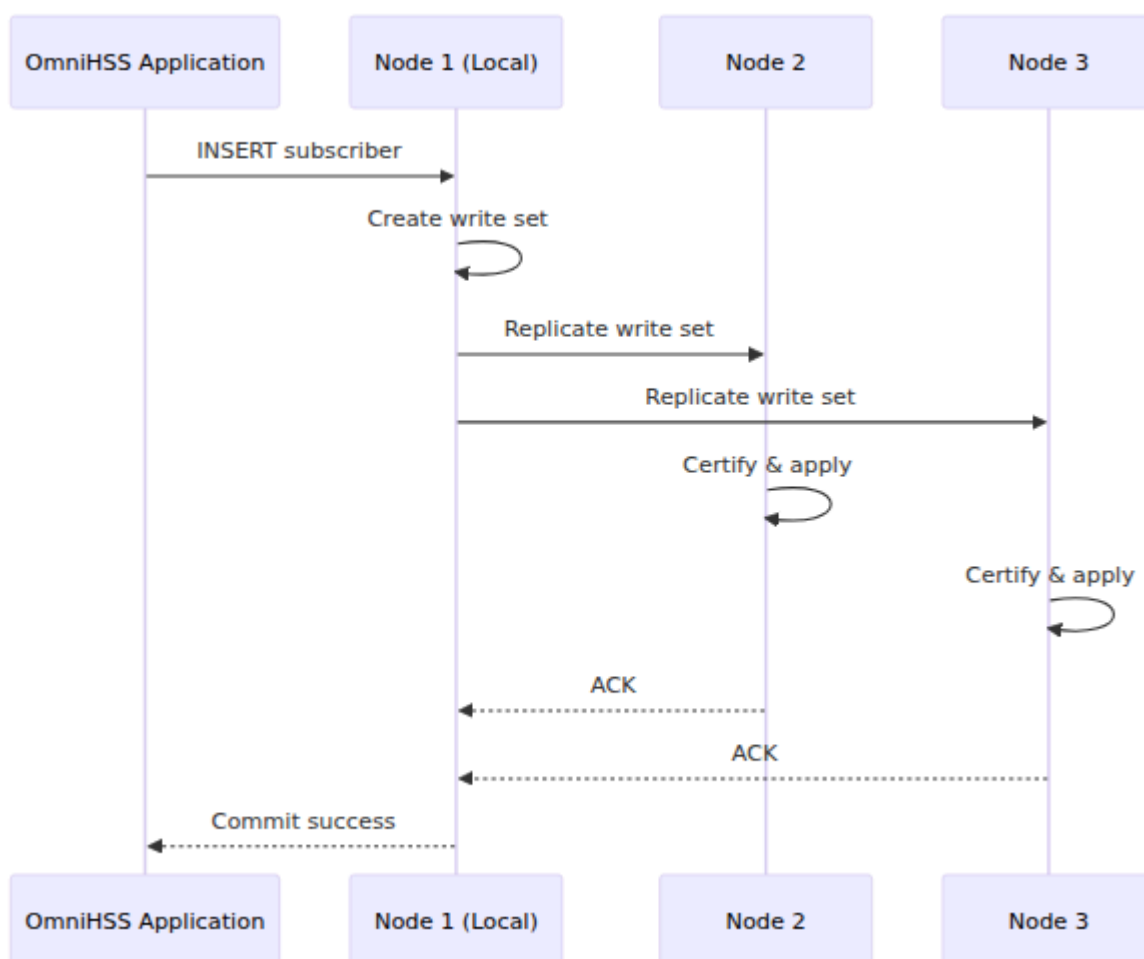
Beneficios Clave

- **Replicación Síncrona:** Todos los nodos tienen datos consistentes en todo momento

- **Multi-Maestro:** Cualquier nodo puede aceptar operaciones de lectura y escritura
- **Conmutación por Error Automática:** Si un nodo falla, los otros continúan operando
- **Recuperación Automática de Nodos:** Los nodos que regresan se resincronizan automáticamente
- **Sin Split-Brain:** La replicación basada en certificación previene conflictos

Cómo Funciona Galera

Flujo de Replicación Síncrona



Replicación de Conjunto de Escritura (WSREP)

Cada transacción de base de datos sigue este proceso:

1. **Ejecución de Transacción:** El cliente ejecuta SQL en el nodo local
2. **Creación de Conjunto de Escritura:** El nodo empaqueta los cambios en un "conjunto de escritura"
3. **Certificación:** Todos los nodos validan el conjunto de escritura para conflictos
4. **Compromiso:** Si la certificación pasa, todos los nodos se comprometen atómicamente
5. **Reconocimiento:** El éxito se devuelve al cliente solo después de que todos los nodos se comprometen

Métodos de Transferencia de Estado

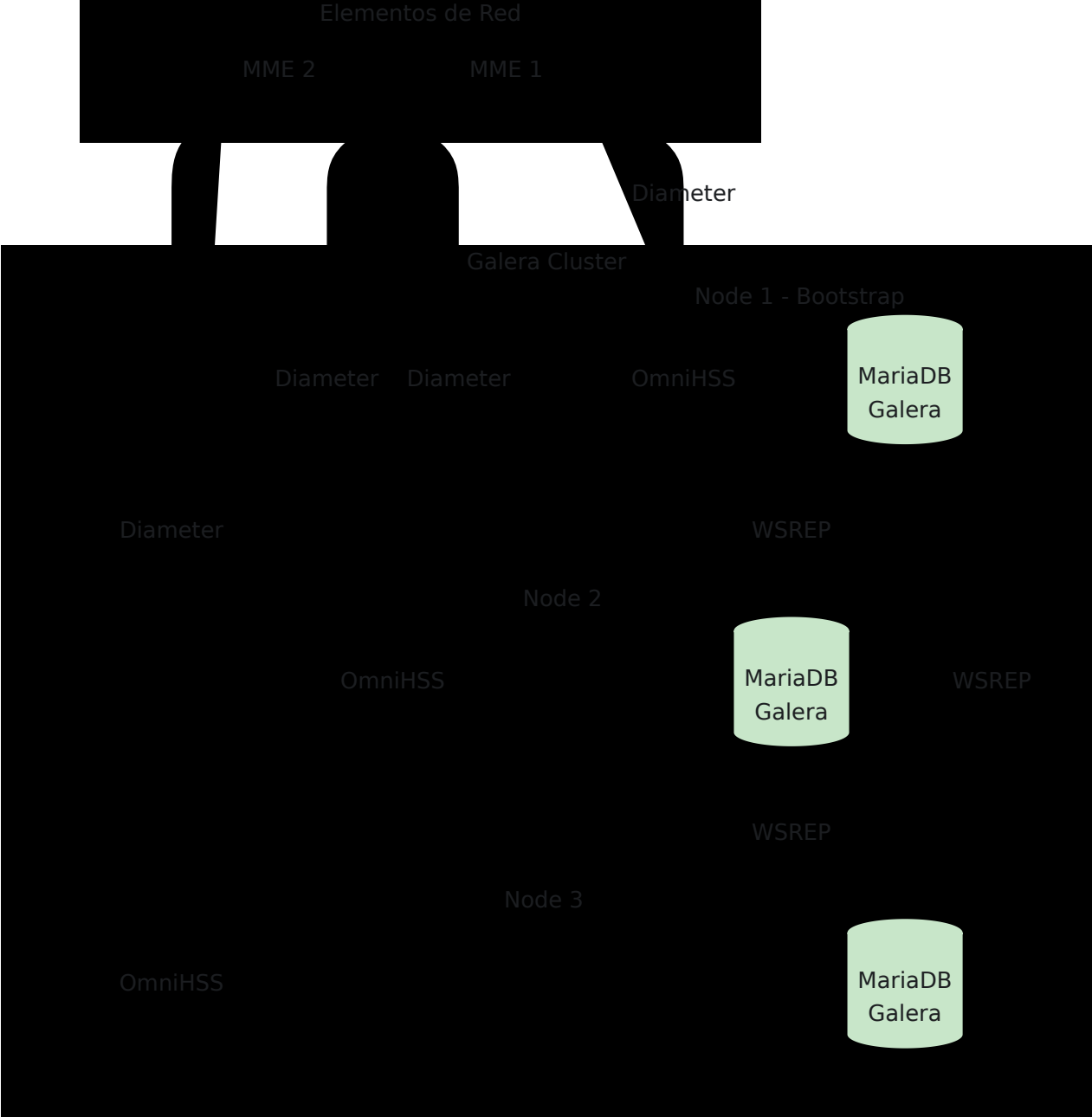
Método	Tipo	Caso de Uso
IST (Incremental)	Sincronización delta	Nodo desconectado brevemente, se pone al día con transacciones perdidas
SST (Instantánea)	Sincronización completa	Nodo nuevo o nodo desconectado durante mucho tiempo, recibe una copia completa de la base de datos

OmniHSS utiliza `rsync` para SST:

```
wsrep_sst_method=rsync
```

Arquitectura de Implementación

Clúster Multi-Nodo



Requisitos de Red

Puerto	Protocolo	Propósito
3306	TCP	Conexiones de cliente MySQL
4567	TCP/UDP	Comunicación del clúster Galera
4568	TCP	Transferencia de Estado Incremental (IST)
4444	TCP	Transferencia de Instantánea de Estado (SST)

Configuración del Cortafuegos

```
# Entre nodos Galera
ufw allow from <node2_ip> to any port 3306,4567,4568,4444 proto
tcp
ufw allow from <node2_ip> to any port 4567 proto udp
ufw allow from <node3_ip> to any port 3306,4567,4568,4444 proto
tcp
ufw allow from <node3_ip> to any port 4567 proto udp
```

Referencia de Configuración

Variables de Ansible

Configure Galera en los `group_vars` de su inventario:

```
omnihss:
  database_host: "localhost"
  database_username: "hss"
  database_password: "secure_password"
  mysql:
    replication_mode: "galera"           # Habilitar Galera
    bootstrap_host: "hss01"             # Primer nodo para iniciar
    el clúster
    run_bootstrap: false                 # Establecer en true solo
    para la configuración inicial
    reinstall: false                     # Establecer en true para
    reinstalar MariaDB
```

Archivo de Configuración de Galera

La configuración de Galera se encuentra en `/etc/mysql/my.cnf`:

```
[mysqld]
# Configuraciones Básicas
pid-file          = /var/run/mysqld/mysqld.pid
socket            = /var/run/mysqld/mysqld.sock
datadir           = /var/lib/mysql
log-error         = /var/log/mysql/error.log

# Requerido para Galera
binlog_format=ROW
default-storage-engine=innodb
innodb_autoinc_lock_mode=2
bind-address=0.0.0.0

# Proveedor de Galera
wsrep_on=ON
wsrep_provider=/usr/lib/galera/libgalera_smm.so

# Configuración del Clúster
wsrep_cluster_name="omnihss_galera"
wsrep_cluster_address="gcomm://10.4.10.140,10.4.10.141,10.4.10.142"

# Transferencia de Estado
wsrep_sst_method=rsync

# Identidad del Nodo
wsrep_node_address="10.4.10.140"
wsrep_node_name="hss01"
```

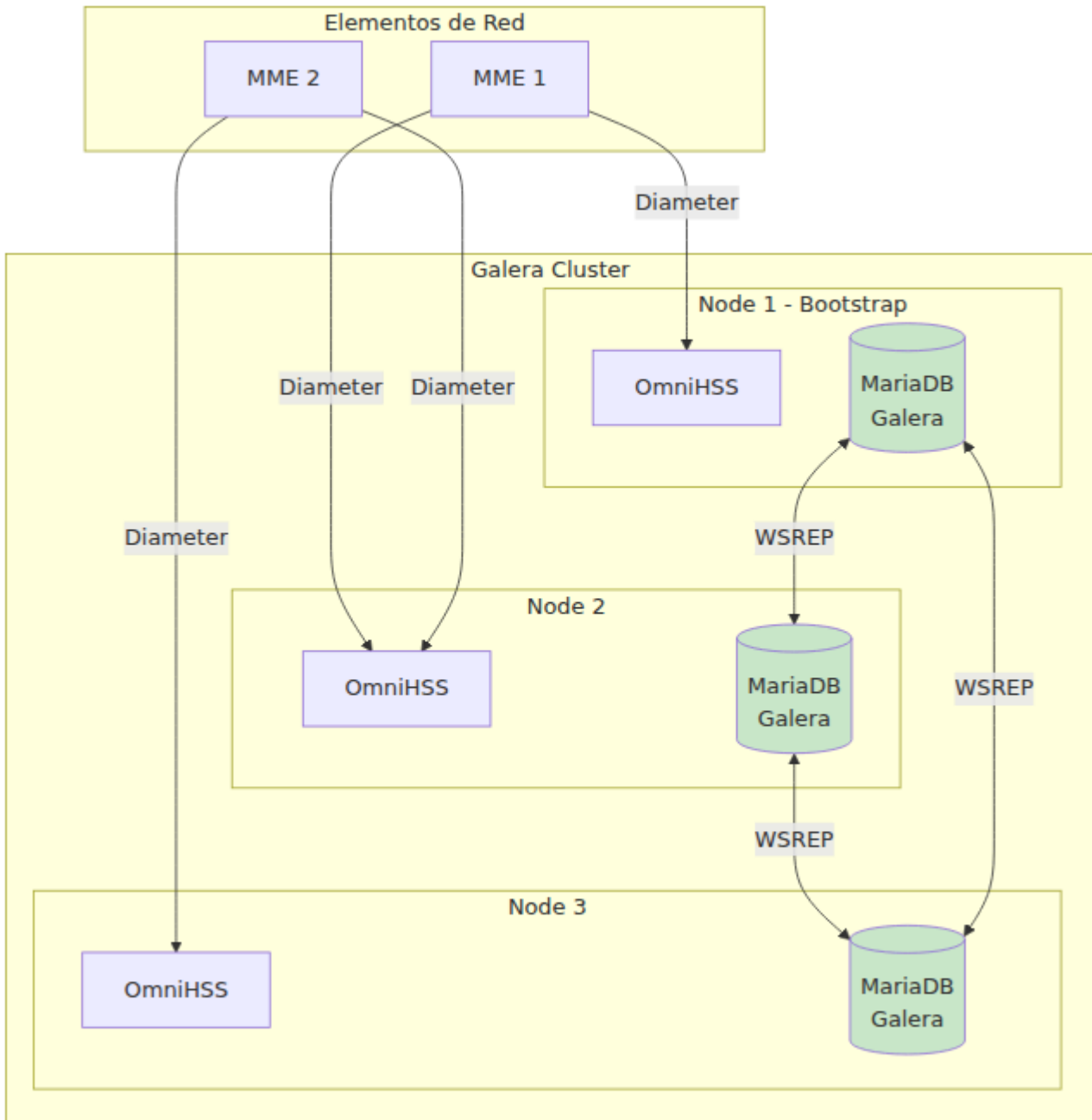
Parámetros de Configuración Explicados

Parámetro	Valor	Propósito
<code>binlog_format</code>	<code>ROW</code>	Requerido - registro basado en filas para replicación
<code>innodb_autoinc_lock_mode</code>	<code>2</code>	Requerido - permite auto-incremento concurrente
<code>wsrep_on</code>	<code>ON</code>	Habilita replicación WSREP
<code>wsrep_provider</code>	Ruta a libgalera	Ubicación de la biblioteca Galera
<code>wsrep_cluster_name</code>	<code>"omnihss_galera"</code>	Todos los nodos deben usar el mismo nombre
<code>wsrep_cluster_address</code>	<code>gcomm://ip1,ip2,ip3</code>	Lista de todas las IPs de nodos del clúster
<code>wsrep_sst_method</code>	<code>rsync</code>	Método de transferencia de estado completo
<code>wsrep_node_address</code>	IP del Nodo	IP del clúster de este nodo
<code>wsrep_node_name</code>	Nombre del Nodo	Identificador de este nodo

Proceso de Bootstrap

Configuración Inicial del Clúster

El proceso de bootstrap crea un nuevo clúster Galera:



Pasos de Bootstrap

1. Designar el Host de Bootstrap

```
omnihss:
  mysql:
    replication_mode: "galera"
    bootstrap_host: "hss01"
    run_bootstrap: true
```

2. Ejecutar el Playbook de Ansible

```
ansible-playbook -i hosts/your_site/inventory.ini
services/omnihss.yml
```

3. Qué Sucede:

- AppArmor se desactiva (requerido para Galera)
- Se instalan paquetes de Galera en todos los nodos
- El nodo de bootstrap establece `safe_to_bootstrap=1` en `/var/lib/mysql/grastate.dat`
- El nodo de bootstrap ejecuta el comando `mysqld_bootstrap`
- Otros nodos reinician MariaDB y se unen a través de la dirección `gcomm://`
- Las migraciones de base de datos se ejecutan solo en el nodo de bootstrap (los cambios se replican)

4. Después del Bootstrap

```
omnihss:
  mysql:
    run_bootstrap: false # Desactivar bootstrap para futuras
ejecuciones
```

Archivo Grastate

El estado del clúster se rastrea en `/var/lib/mysql/grastate.dat`:

```
# Estado guardado de GALERA
version: 2.1
uuid:    abc12345-6789-def0-1234-567890abcdef
seqno:   1234567
safe_to_bootstrap: 0
```

- `uuid`: Identificador único del clúster
 - `seqno`: Número de secuencia de la última transacción comprometida
 - `safe_to_bootstrap`: Solo se establece en 1 en el nodo que debe iniciar el clúster
-

Operaciones

Agregar un Nuevo Nodo

1. Configure el nuevo nodo en el inventario con el grupo `hss`
2. Actualice `wsrep_cluster_address` para incluir todos los nodos
3. Ejecute el playbook de OmniHSS - el nodo se unirá automáticamente:
 - Instalará paquetes de Galera
 - Obtendrá configuración con direcciones de clúster
 - Se unirá al clúster a través de SST

Eliminar un Nodo

1. Detenga OmniHSS y MariaDB en el nodo a eliminar
2. Elimine el nodo del inventario
3. Actualice `wsrep_cluster_address` en los nodos restantes
4. Reinicie MariaDB en los nodos restantes

Reinicio Controlado

Para mantenimiento, reinicie los nodos uno a la vez:

```
# En cada nodo, uno a la vez
systemctl stop omnihss
systemctl stop mysql
# Realizar mantenimiento
systemctl start mysql
systemctl start omnihss
```

Espera a que cada nodo se reincorpore completamente antes de reiniciar el siguiente.

Recuperación de Emergencia

Si todo el clúster se detiene (corte de energía, etc.):

1. Identificar el Nodo Más Reciente

```
# Ver seqno en cada nodo
cat /var/lib/mysql/grastate.dat
```

2. Bootstrap desde el Más Reciente

```
# En el nodo con el seqno más alto
sed -i "/safe_to_bootstrap/s/0/1/" /var/lib/mysql/grastate.dat
mysqld_bootstrap
```

3. Iniciar Otros Nodos

```
# En otros nodos
systemctl start mysql
```

Monitoreo

Estado del Clúster

Consulta el estado del clúster en cualquier nodo:

```
-- Tamaño del clúster (número de nodos)
SHOW STATUS LIKE 'wsrep_cluster_size';

-- Estado del clúster
SHOW STATUS LIKE 'wsrep_cluster_status';

-- Estado del nodo
SHOW STATUS LIKE 'wsrep_local_state_comment';

-- Todas las variables WSREP
SHOW STATUS LIKE 'wsrep_%';
```

Métricas Clave

Métrica	Valor Saludable	Descripción
<code>wsrep_cluster_size</code>	Conteo esperado de nodos	Número de nodos en el clúster
<code>wsrep_cluster_status</code>	Primary	El clúster tiene quórum
<code>wsrep_local_state</code>	4	El nodo está sincronizado
<code>wsrep_local_state_comment</code>	Synced	Descripción del estado del nodo
<code>wsrep_ready</code>	ON	El nodo acepta consultas
<code>wsrep_connected</code>	ON	El nodo está conectado al clúster

Estados de Nodo

Estado	Valor	Descripción
Uniéndose	1	El nodo se está uniendo al clúster
Donante/Desincronizado	2	El nodo está proporcionando SST a otro
Unido	3	El nodo se ha unido, sincronizando
Sincronizado	4	El nodo está completamente sincronizado

Métricas de Prometheus

OmniHSS expone métricas de Galera a través del punto de métricas estándar al usar MariaDB Galera.

Solución de Problemas

El Nodo No Se Une al Clúster

Síntomas: El nodo se inicia pero no se une al clúster

Verifique:

```
# Ver el registro de errores de MariaDB
tail -f /var/log/mysql/error.log

# Verifique si wsrep está en funcionamiento
mysql -e "SHOW STATUS LIKE 'wsrep_on';"
```

Causas Comunes:

- Cortafuegos bloqueando puertos 4567, 4568, 4444
- IP incorrecta en `wsrep_cluster_address`
- AppArmor aún habilitado
- Desajuste de UUID del clúster

Solución:

```
# Asegúrese de que AppArmor esté deshabilitado
systemctl status apparmor
# Si está activo: systemctl stop apparmor && systemctl disable
apparmor

# Verifique que los puertos estén abiertos
ss -tlnp | grep -E '4567|4568|4444|3306'
```

Split-Brain / Estado No Primario

Síntomas: `wsrep_cluster_status` muestra `non-Primary`

Esto sucede cuando:

- El clúster pierde quórum (mayoría de nodos caídos)
- Una partición de red aísla nodos

Recuperación:

```
-- En el nodo con los datos más recientes  
SET GLOBAL wsrep_provider_options='pc.bootstrap=YES';
```

Fallo de SST

Síntomas: El nuevo nodo no puede completar la transferencia de estado

Verifique:

```
# Espacio en disco en el donante y el que se une  
df -h /var/lib/mysql  
  
# Proceso rsync  
ps aux | grep rsync
```

Causas Comunes:

- Espacio en disco insuficiente
- rsync no instalado
- Cortafuegos bloqueando el puerto 4444

Nodo Desincronizado Después de Donante

Síntomas: `wsrep_local_state_comment` muestra `Donor/Desynced`

Esto es normal durante SST. El nodo reanuda el estado normal después de completar la transferencia de estado al nodo que se une.

Si se queda atascado:

```
# Verifique si rsync está atascado
ps aux | grep rsync
# Matar si está atascado
pkill rsync
systemctl restart mysql
```

Grastate Corrupto

Síntomas: MariaDB no se inicia, error sobre grastate

Solución:

```
# Eliminar grastate corrupto
rm /var/lib/mysql/grastate.dat

# Iniciar como nuevo nodo (se SST desde el clúster existente)
systemctl start mysql
```

Degradación del Rendimiento

Síntomas: Escrituras lentas, alta `wsrep_local_send_queue`

Verifique:

```
SHOW STATUS LIKE 'wsrep_local_send_queue%';
SHOW STATUS LIKE 'wsrep_flow_control%';
```

Causas Comunes:

- Latencia de red entre nodos
- Un nodo significativamente más lento (I/O de disco)
- Transacciones muy grandes

Mitigación:

- Asegúrese de que haya una red de baja latencia entre nodos
 - Use hardware similar para todos los nodos
 - Evite operaciones de lote muy grandes
-

Mapeo de Datos de Respuesta de Diameter

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

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

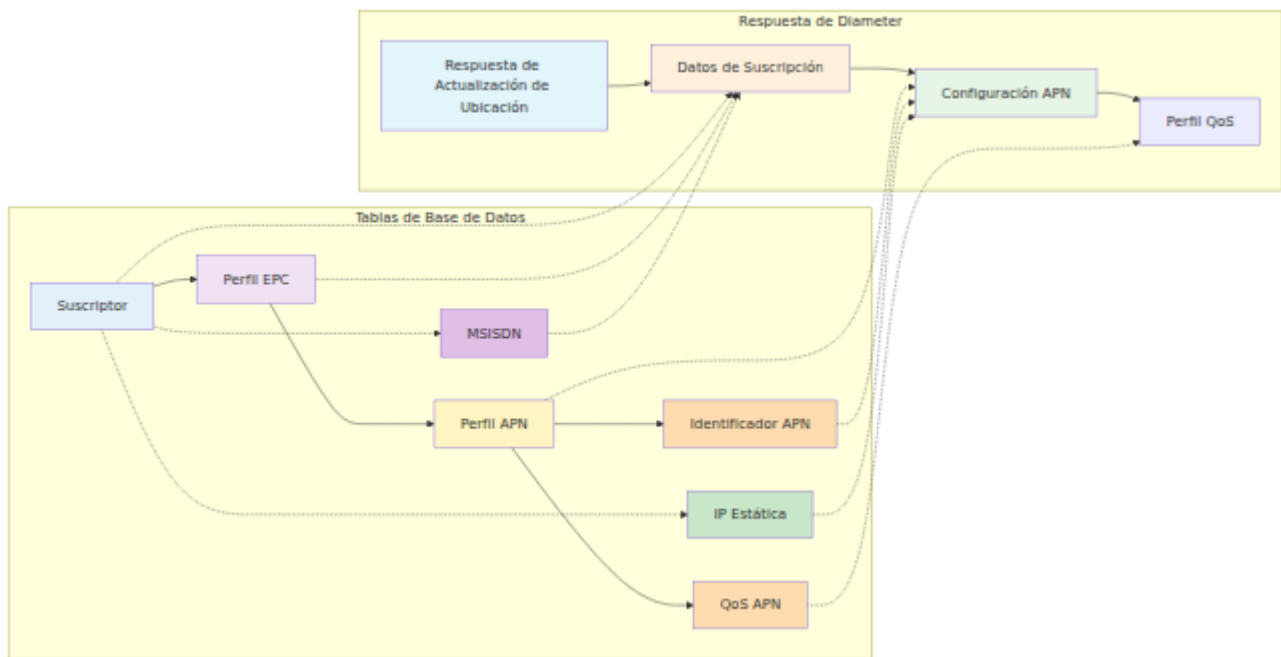
Tabla de Contenidos

- [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 del 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 de datos completo desde las tablas de la base de datos hasta los AVPs de Diameter.

Mapeo de Fuentes de Datos



Mapeo Detallado de Campos

Fuente de Base de Datos	Campo	D
subscriber.enabled	true/false	Su St
msisdn.msisdn	'14155551234'	MS
epc_profile.ue_ambr_ul_kbps	50000	Ma Re Ba UL
epc_profile.ue_ambr_dl_kbps	100000	Ma Re Ba DL
epc_profile.network_access_mode	'packet_only'	Ne Ac Mo
apn_identifier.apn	'internet'	Se Se
apn_identifier.ip_version	'ipv4v6'	PD
apn_qos_profile.qci	9	Qc Id

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, Diameter espera en bps (multiplicar por 1000)
- Codificación de Versión IP:** 0=IPv4, 1=IPv6, 2=IPv4v6, 3=IPv4_or_IPv6

- Estado del Suscriptor:** `enabled: true → 0 (SERVICE_GRANTED)`,
`enabled: false → 1 (OPERATOR_DETERMINED_BARRING)`
- Context-Identifer:** Numeración secuencial (0, 1, 2...) para cada APN en el perfil
- IP Estática:** Solo incluida si se asigna a través de `static_ips` relación muchos a muchos

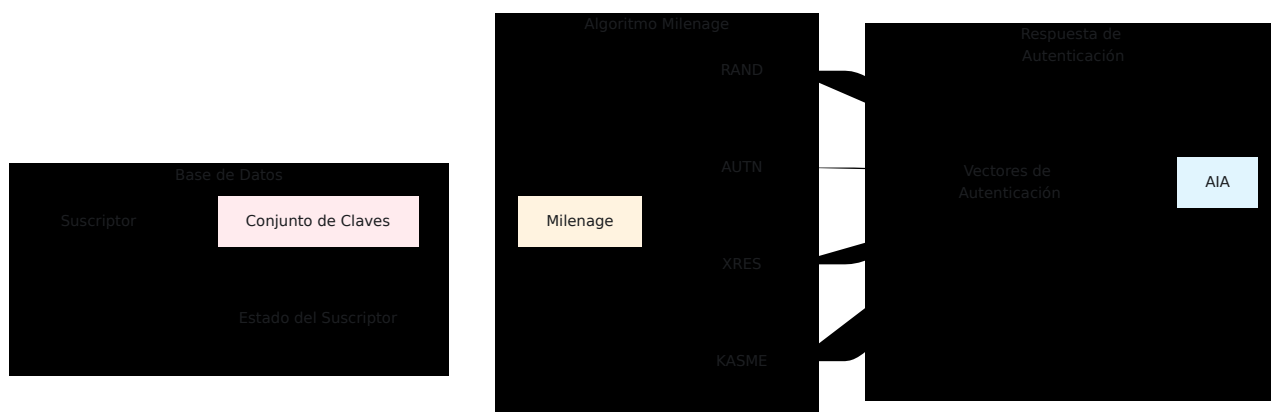
Validación de Lógica de Negocio:

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

Respuesta de Información de Autenticación (S6a AIA)

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

Mapeo de Fuentes de Datos



Componentes Clave:

- Claves Criptográficas:** Todas las claves almacenadas 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

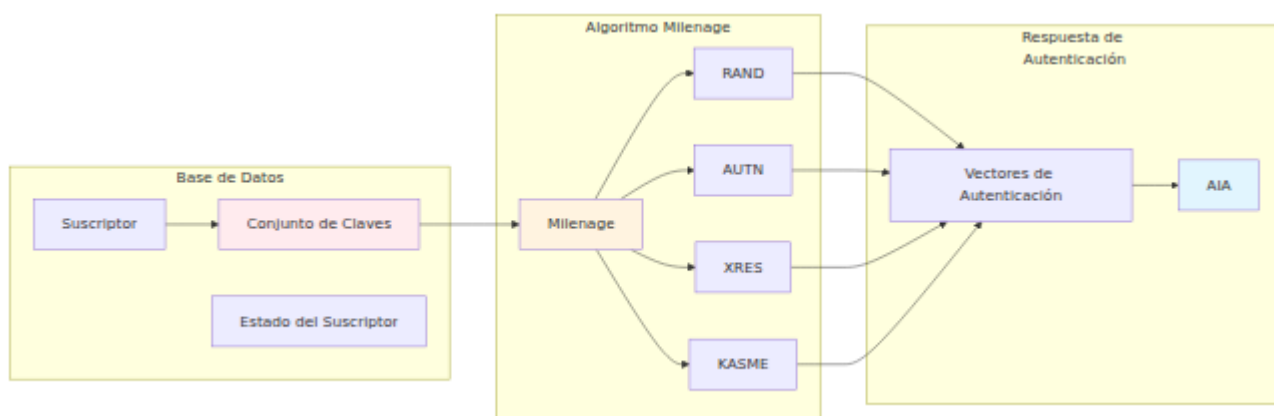
Características de Seguridad:

- 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.

Mapeo 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 S-CSCF:** Almacena S-CSCF asignado en

`subscriber_state.assigned_scscf`

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

`{msisdn}`

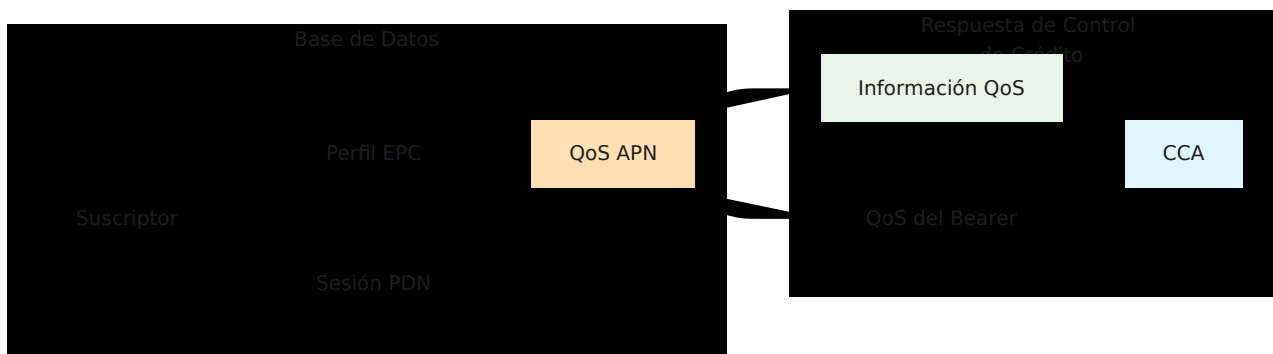
Parámetros de Plantilla IFC:

- `{{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 desde el perfil QoS APN

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

Gestión del Estado de la 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.

Mapeo de Fuentes de Datos



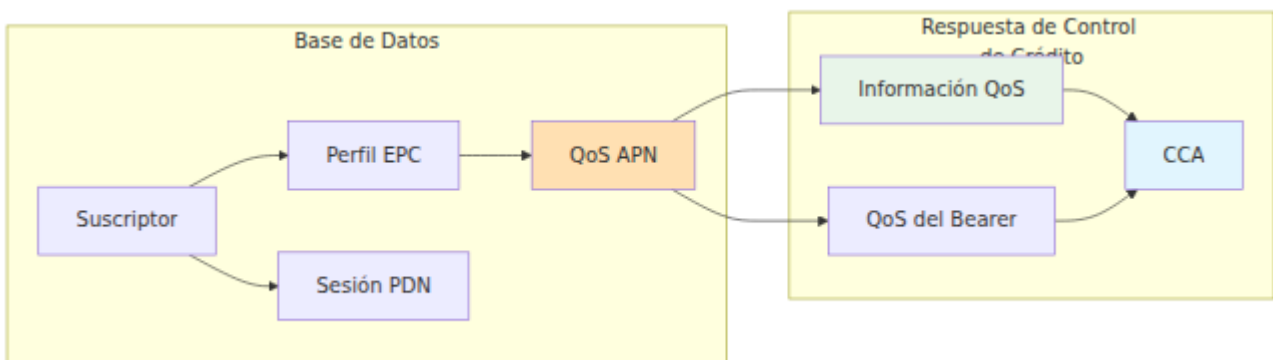
Características Clave:

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, referencia y transparente
-

Respuesta de Verificación de Identidad del ME (S13 ECA)

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

Mapeo de Fuentes de Datos



Características Clave:

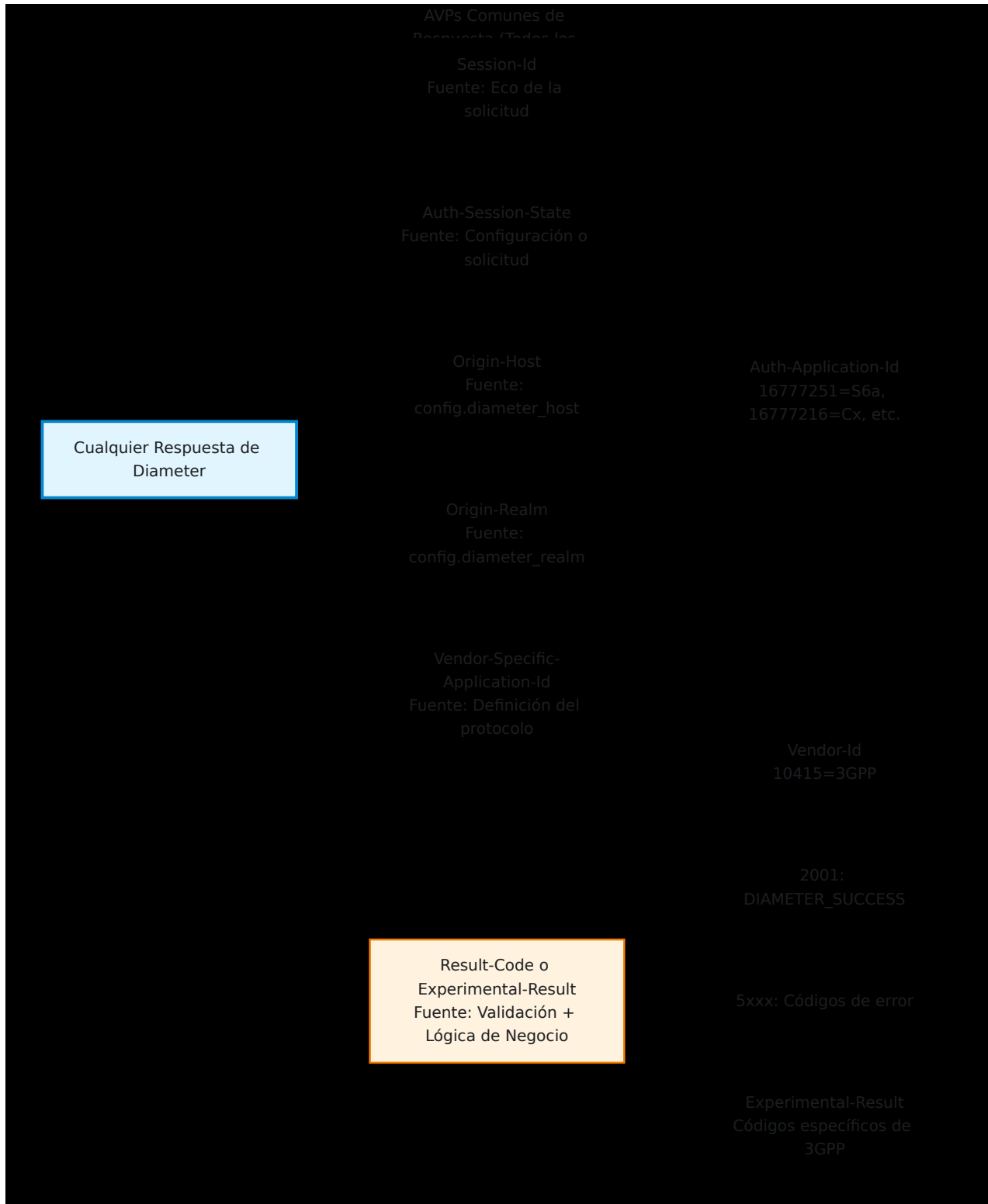
1. **Coincidencia de Regex de IMEI:** Las reglas utilizan expresiones regulares para coincidencias flexibles
2. **Reglas basadas en TAC:** Puede coincidir con el Código de Asignación de Tipo (primeros 8 dígitos)
3. **Comportamiento Predeterminado:** Configurable para IMEIs desconocidos (aceptar o rechazar)
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 en la lista blanca
- Rastrear dispositivos del mercado gris

Elementos Comunes de Respuesta

Todas las respuestas de Diameter comparten estos AVPs comunes:

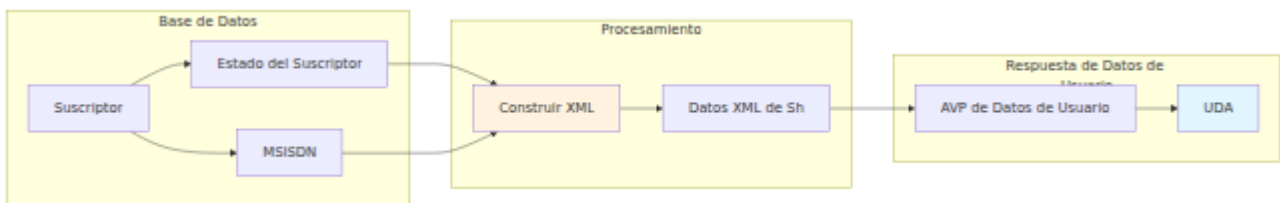


Ejemplo de Configuración:

```
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 Diameter:

- **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 carga
- **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 Roaming** - Reglas y restricciones de roaming
 - **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](#)

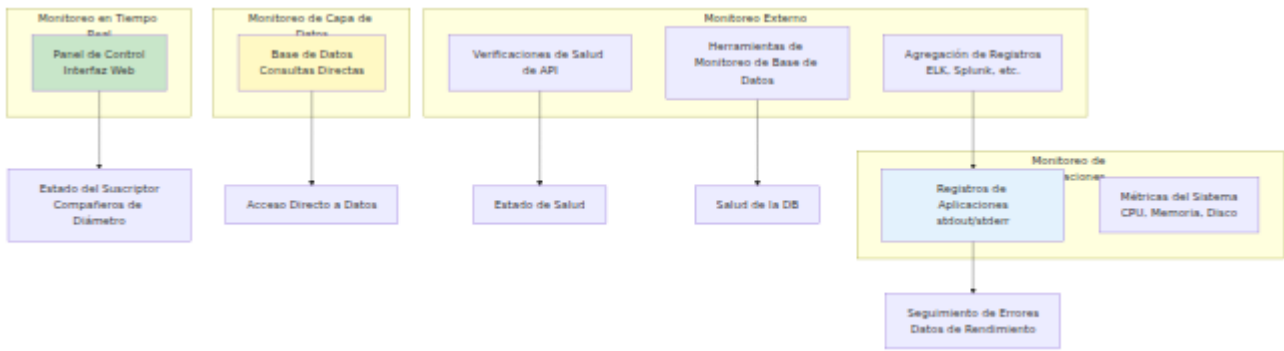
Tabla de Contenidos

- [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 Desempeño](#)
 - [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 integral.

Capas de Monitoreo



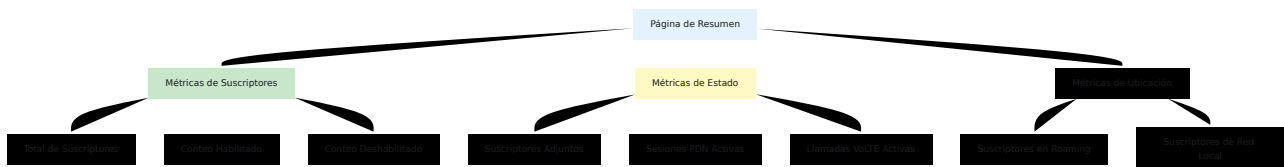
Monitoreo del Panel de Control

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	Qué 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

Aunque 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 expandibles** para información de estado
4. **Anotar marcas de tiempo de última vista** para la capacidad de respuesta

Monitoreo de la Página de Diámetro

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

Métricas Clave



Monitoreo de Compañeros Críticos

Identifica compañeros críticos y monitorea su estado:

Tipo de Compañero	Criticidad	Impacto si Está Caído
MME	Alta	Sin nuevos adjuntos LTE
P-GW	Alta	Sin sesiones de datos
S-CSCF	Alta	Sin registros IMS
P-CSCF	Alta	Sin llamadas VoLTE
I-CSCF	Media	Problemas de enrutamiento IMS
AS	Baja-Media	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	Rastrear 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 de 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:

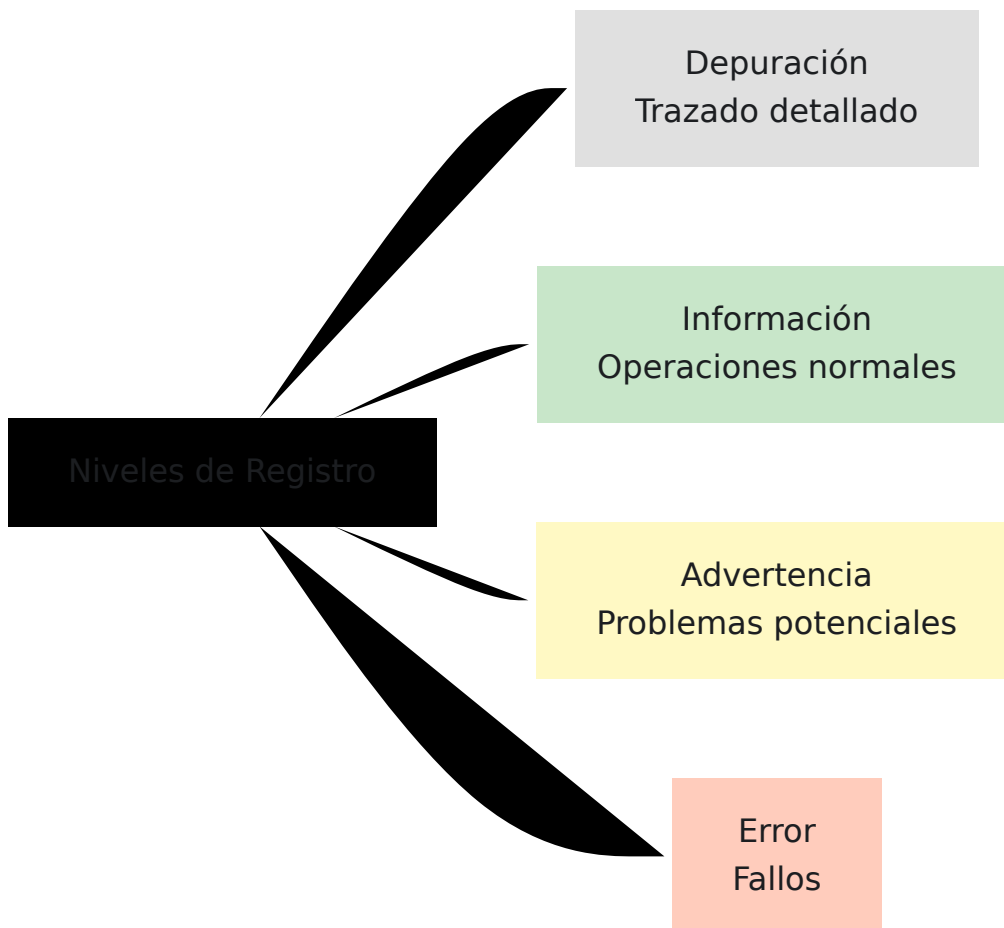
- Tamaño total de la base de datos y tendencias de crecimiento
 - Tamaños de tablas individuales y conteos de filas
 - Conteo actual de conexiones a la base de datos
 - Rendimiento de consultas y uso de recursos
-

Monitoreo de Registros

Salida de Registros

OmniHSS envía registros a **stdout/stderr**, que deben ser capturados por tu administrador de procesos.

Niveles de Registro



Patrones Clave de Registro a Monitorear

Eventos de Compañeros de Diámetro:

```
[info] Compañero de Diámetro conectado: mme01.epc.example.com  
[warn] Compañero de Diámetro desconectado: pgw01.epc.example.com  
[error] Fallo en la conexión del compañero de Diámetro: 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 a la base de datos fallida: interbloqueo 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 Registro

Agregador de Registros

Pila ELK

Splunk

Registro en la Nube
CloudWatch, Stackdriver

Tableros

Integración de Monitoreo Externo

Endpoint de Verificación de Salud

Verificación 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 respondiendo (HTTP
$response)"
    exit 2
fi
```

Integración con Prometheus

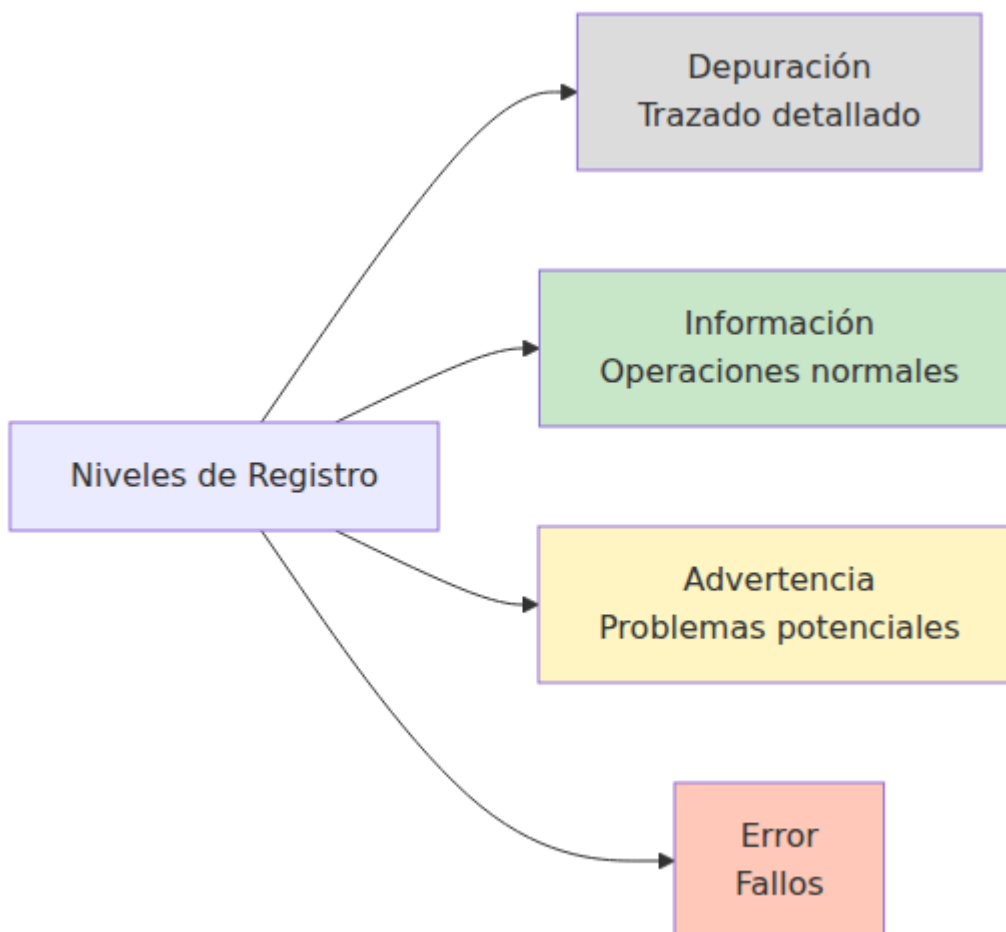
Se pueden crear exportadores personalizados para exportar métricas de OmniHSS a Prometheus consultando la API y la base de datos.

Integración SNMP

Para 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 Desempeño

KPIs Operacionales



Umbrales de KPI Recomendados

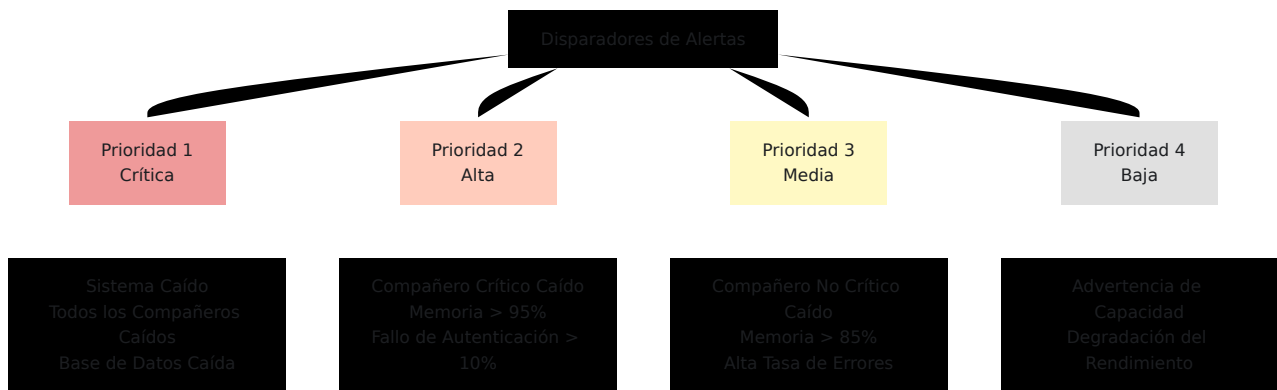
KPI	Objetivo	Advertencia	Crítico
Tiempo de Actividad del Sistema	99.99%	< 99.95%	< 99.9%
Tiempo de Actividad de Compañeros de Diámetro	99.9%	< 99.5%	< 99%
Tasa de Éxito de Autenticación	> 99%	< 99%	< 95%
Tiempo de Respuesta de Diámetro	< 100ms	> 200ms	> 500ms
Tiempo de Consulta de Base de Datos	< 50ms	> 100ms	> 500ms
Tasa de Errores	< 0.1%	> 0.5%	> 1%

KPIs de Capacidad

Métrica	Monitorear	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 verificación de salud de la API falla
- Panel de Control inaccesible
- Fallo de conexión a la base de datos
- Acción: Investigación y escalamiento inmediato

Todos los Compañeros de Diámetro Desconectados:

- Cero compañeros 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)

Compañero Crítico Caído:

- MME principal desconectado
- P-GW principal desconectado
- S-CSCF principal desconectado
- Acción: Investigar conectividad del compañero dentro de 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 aprovisionamiento de suscriptores, investigar causa

Alertas de Prioridad Media (P3)

Compañero No Crítico Caído:

- Compañero 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:

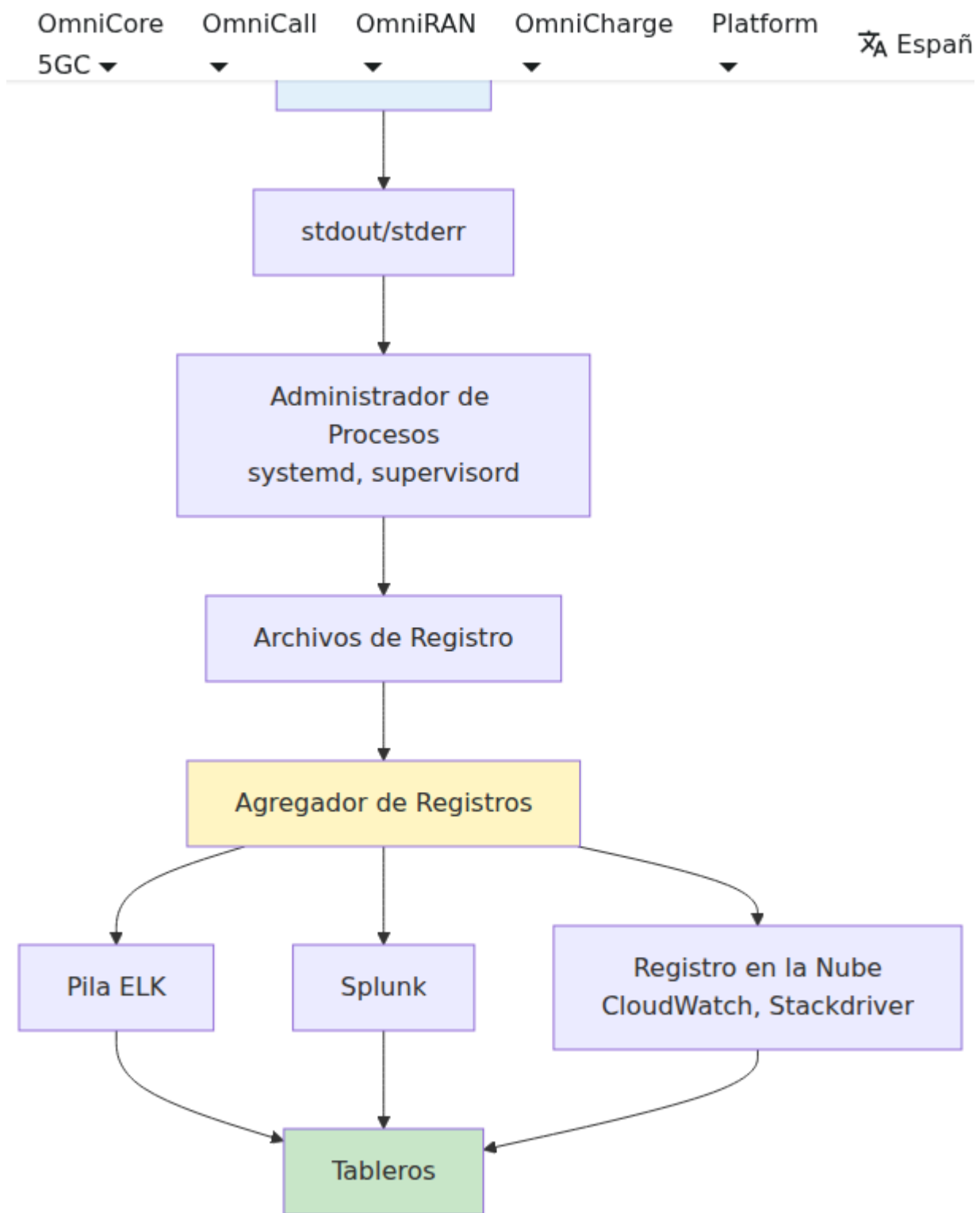
- Suscriptores > 80% de la capacidad
- Base de Datos > 80% del almacenamiento asignado

- 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

Chequesos Diarios

- Revisar Resumen del Panel de Control - conteos de suscriptores normales
- Revisar página de Diámetro - todos los compañeros críticos conectados
- Revisar página de Aplicaciones - memoria y procesos dentro de límites
- Verificar registros de errores - sin errores críticos en las últimas 24 horas
- Verificar que la copia de seguridad se completó con éxito

Chequesos 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

Chequesos Mensuales

- Revisión de planificación de capacidad - proyectar 6 meses adelante
- Revisión de optimización de rendimiento - identificar consultas lentas
- Revisión de seguridad - expiración de certificados, vulnerabilidades
- Revisión de documentación - actualizar manuales de procedimientos
- Prueba de recuperación ante desastres - verificar que las copias de seguridad se restauren correctamente

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

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](#)
-

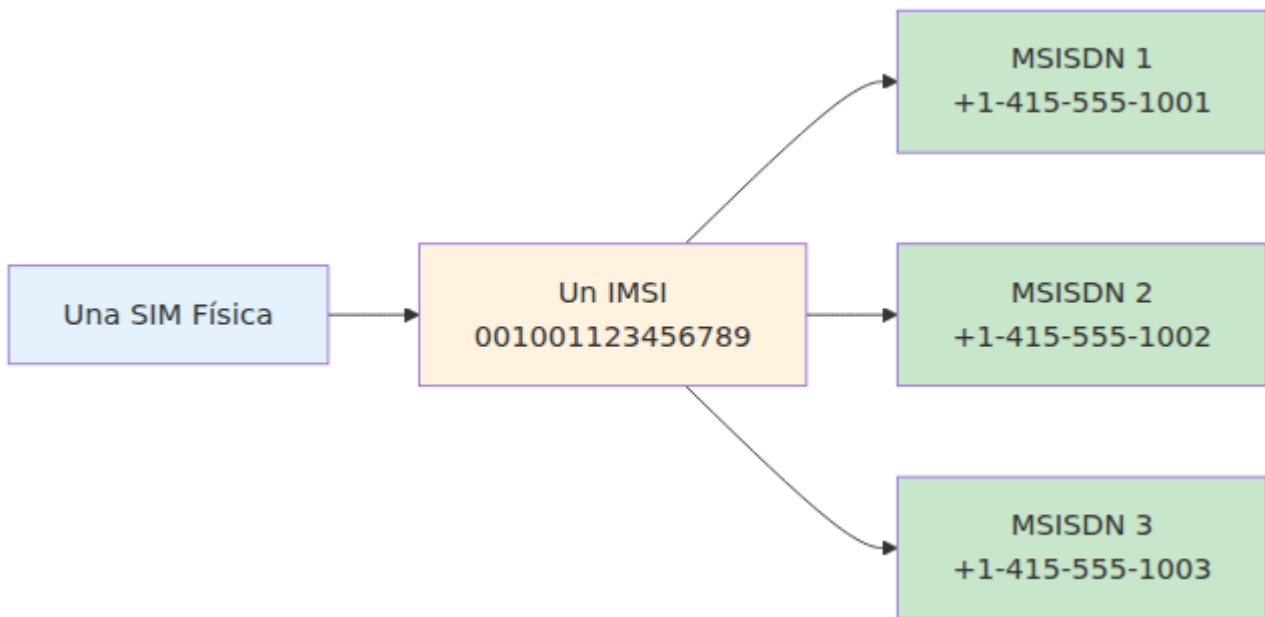
Descripción General

OmniHSS soporta capacidades avanzadas de aprovisionamiento que permiten configuraciones de servicio flexibles:

Soporte Multi-MSISDN

Un IMSI → Múltiples Números de Teléfono

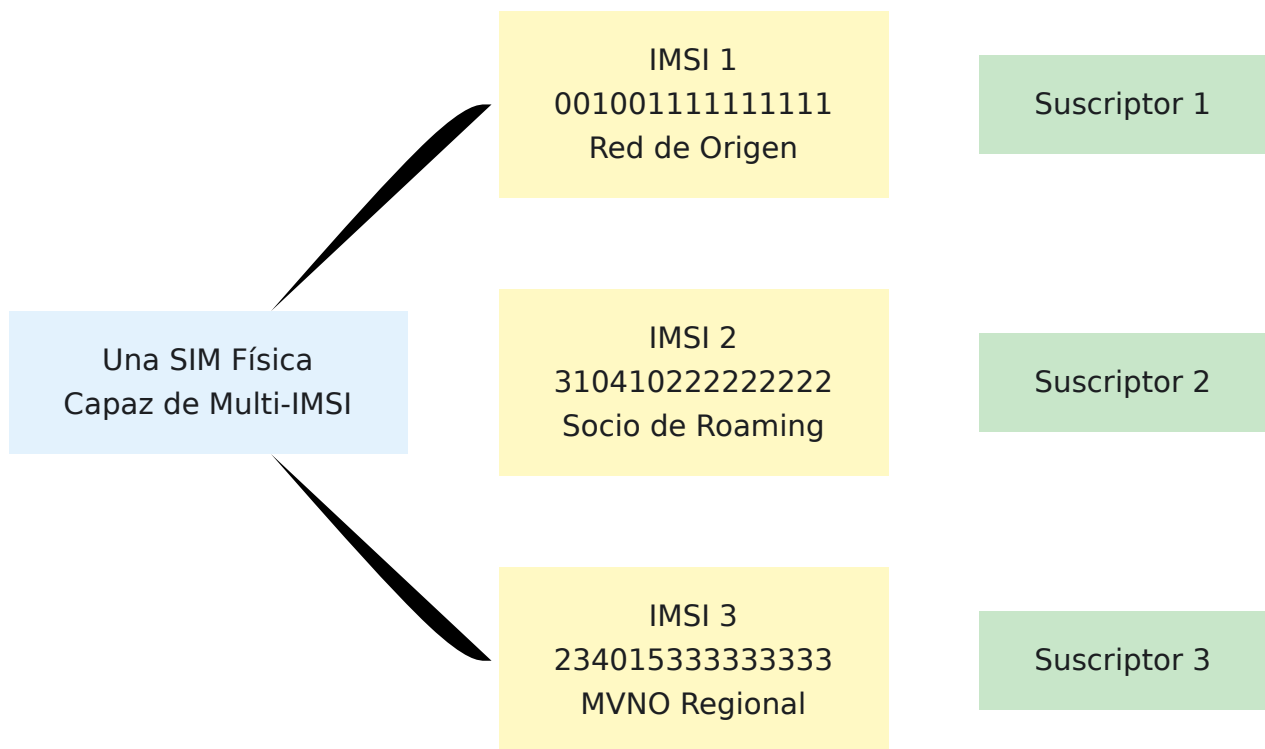
Un único suscriptor (identificado por un IMSI) puede tener múltiples MSISDN (números de teléfono) asignados. Todos los números suenan en el mismo dispositivo y comparten los mismos perfiles de servicio.



Soporte SIM Multi-IMSI

Una SIM → Múltiples IMSIs

Una única tarjeta SIM física puede contener múltiples IMSIs, permitiendo 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

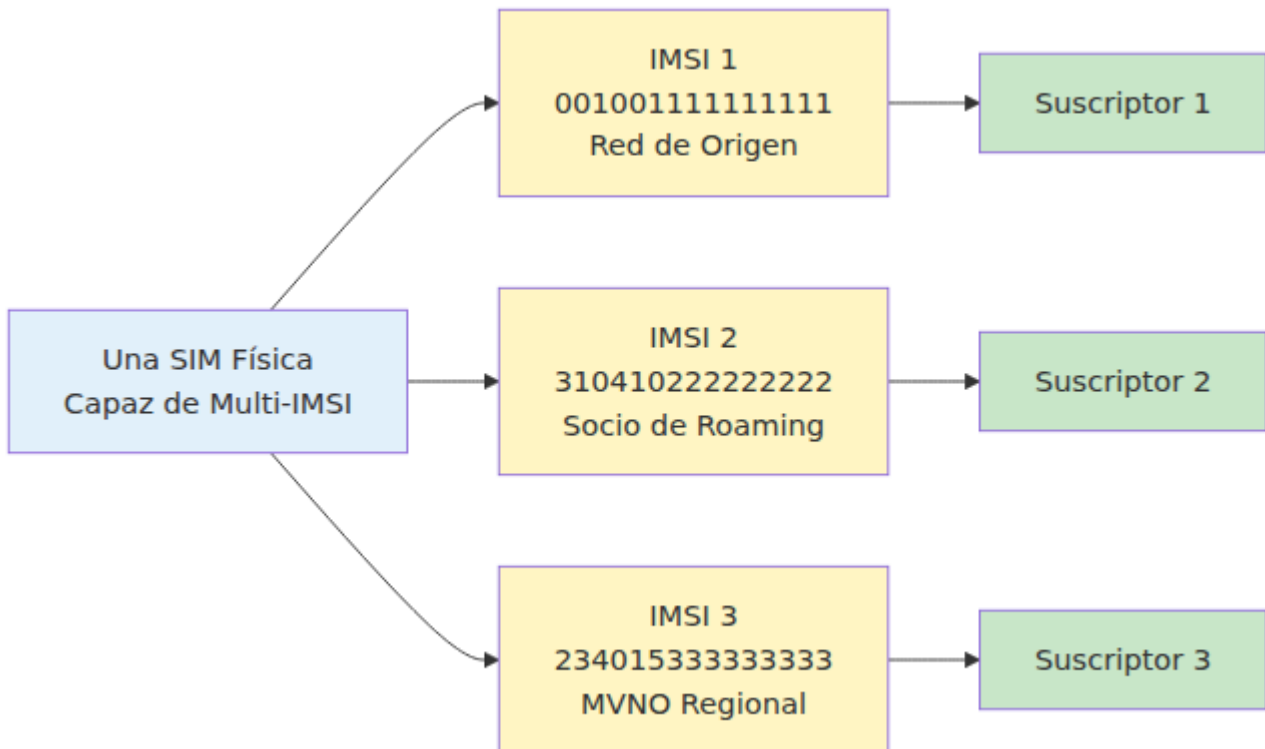
Cómo Funciona

Un registro de suscriptor en el HSS tiene múltiples MSISDNs vinculados a través de una tabla de unión. Cuando el suscriptor se registra en IMS, todos los MSISDNs se incluyen en el perfil 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 MSISDNs están registrados en IMS
- **Servicio Compartido** - Todos los números comparten los mismos perfiles de servicio (EPC, IMS, Roaming)

Modelo de Datos

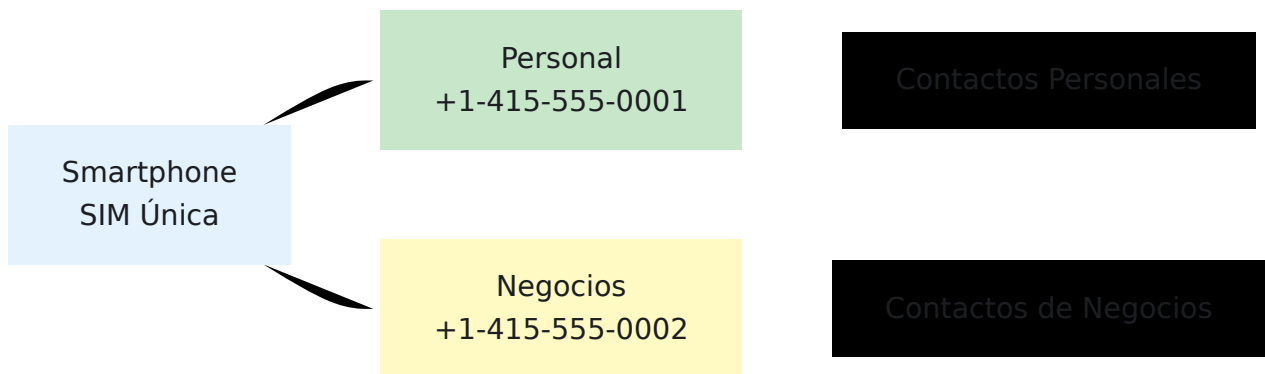


Importante: Un MSISDN solo puede ser asignado a UN suscriptor a la vez. Sin embargo, un suscriptor puede tener MUCHOS MSISDNs.

Casos de Uso

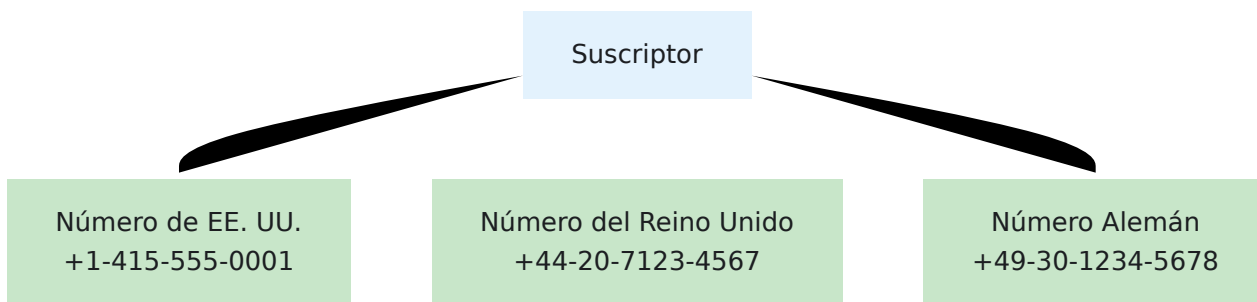
1. Líneas de Negocios y Personales

Un suscriptor tiene tanto números de teléfono de negocios como personales en el mismo dispositivo:



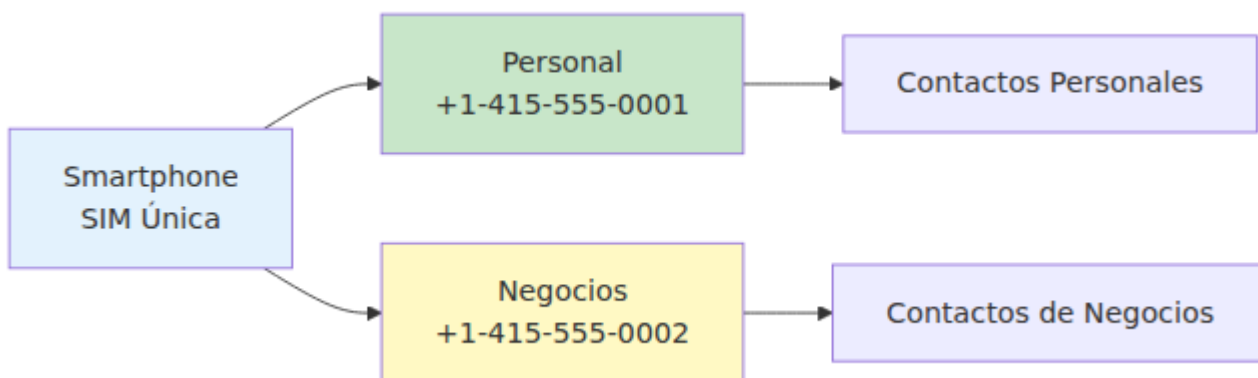
2. Números Internacionales

Un suscriptor que viaja con frecuencia tiene números en múltiples países:



3. Planes Familiares

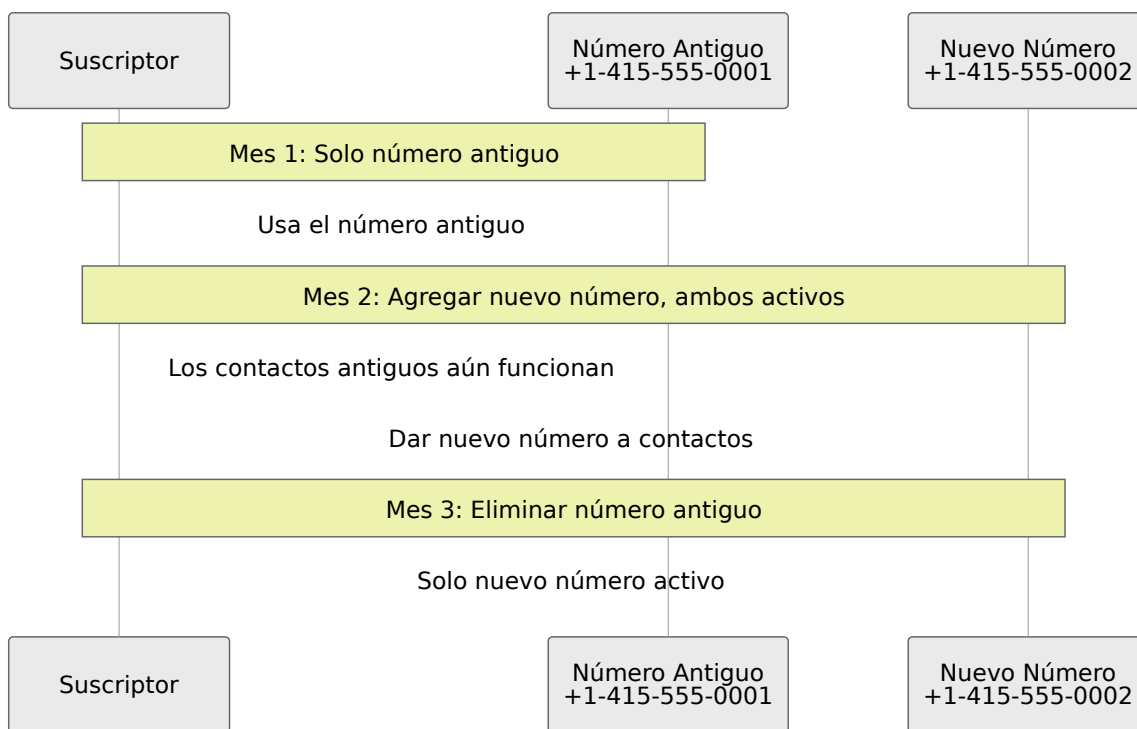
Un padre gestiona múltiples números de miembros de la familia:



Nota: En OmniHSS, esto requeriría múltiples suscriptores (uno por SIM/IMSI), cada uno potencialmente teniendo múltiples MSISDNs.

4. Portabilidad de Línea Legada

Cuando un suscriptor cambia de número pero quiere mantener el número antiguo 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

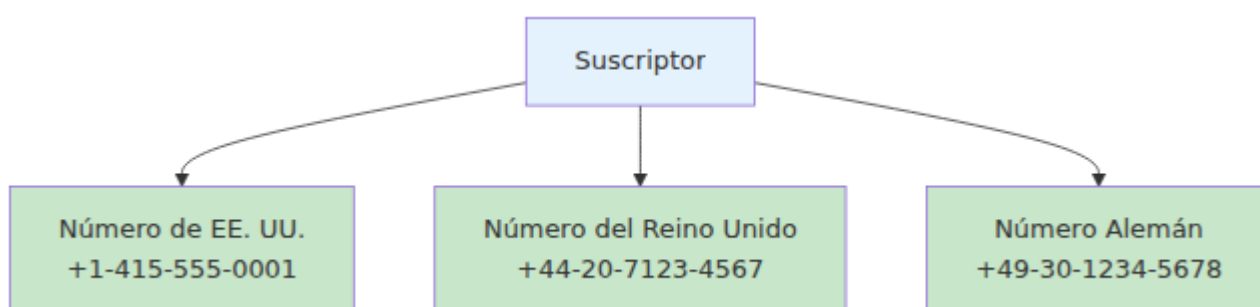
La asignación se realiza a través de la tabla de unión en la base de datos.

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 MSISDNs vinculados mediante:

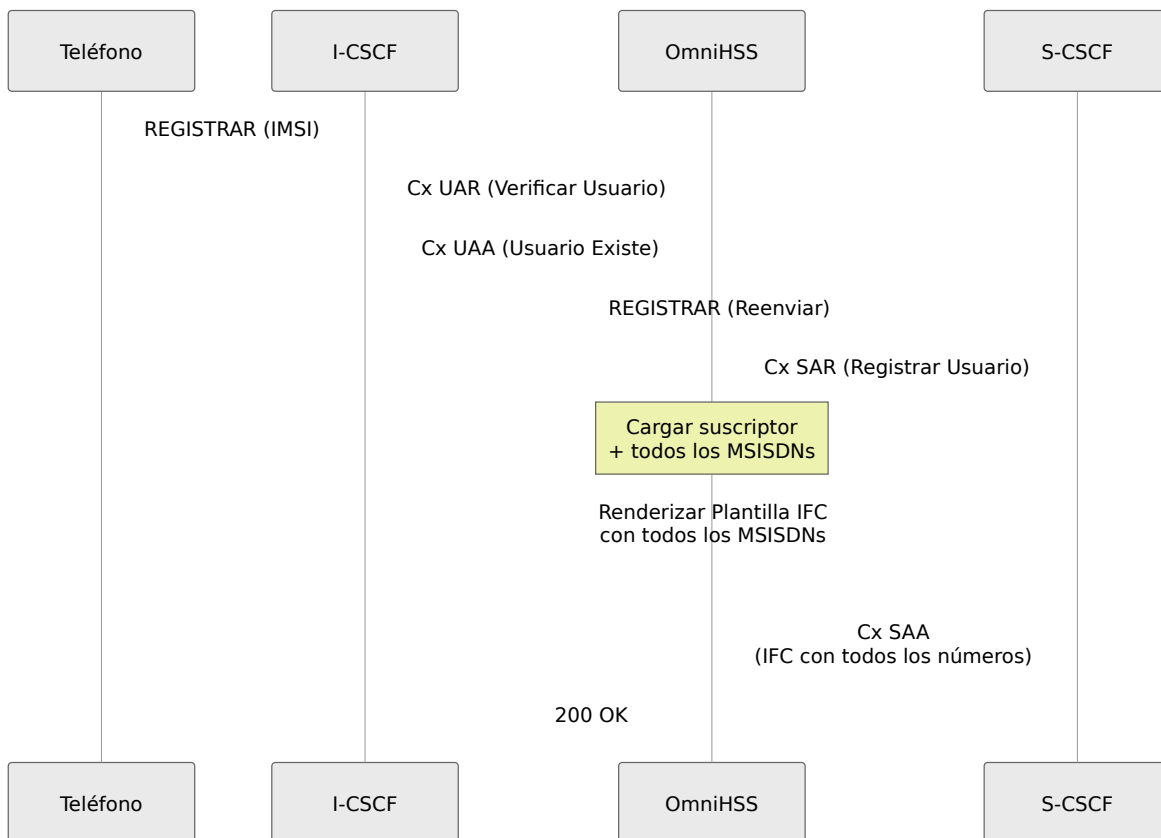
- Uniendo la tabla de suscriptores con la tabla de unión
- Uniendo la tabla de unión con la tabla de msisdn
- Agrupando los resultados por suscriptor para ver todos los números de teléfono juntos

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 IMS enviado al S-CSCF.



Renderización de Plantilla IFC

La plantilla IFC de IMS puede hacer referencia a todos los MSISDNs usando 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

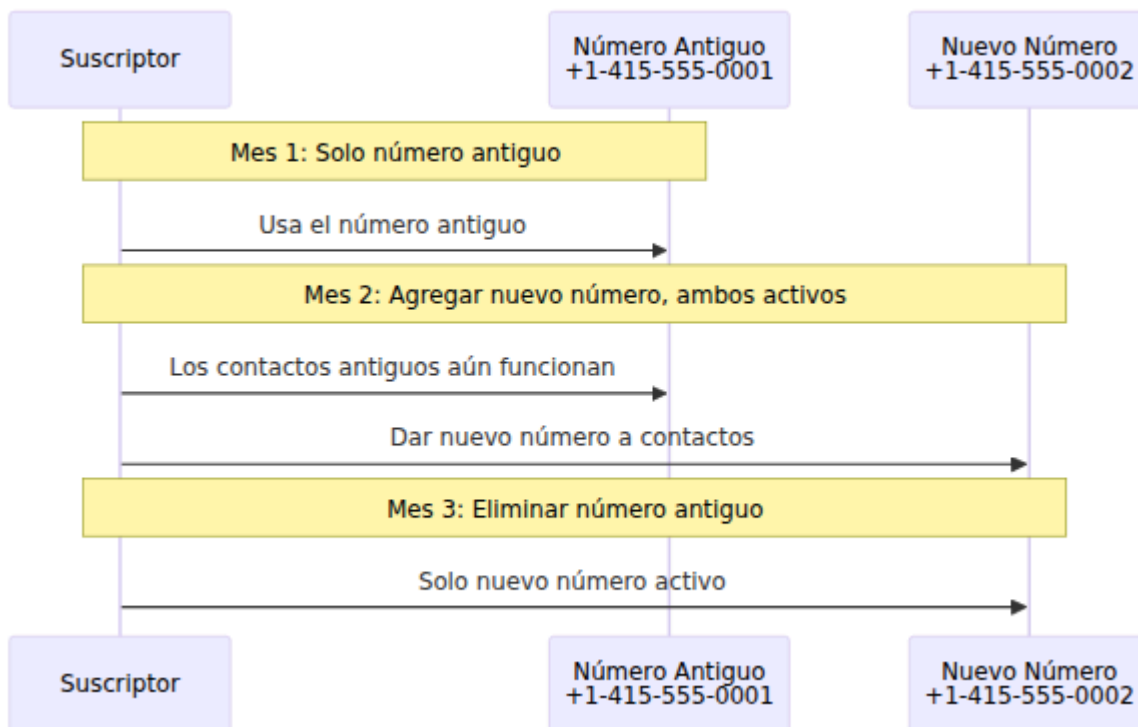
Identidades Públicas

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 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
- 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 del 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 registros S-CSCF para identidades públicas registradas

Problema: No se Puede Asignar MSISDN a Suscriptor

Síntomas:

- Fallo en la inserción de la base de datos
- 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 el registro de MSISDN primero a través de la API o inserción en la base de datos

Problema: Las Llamadas a Un Número Funcionan, Otras 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 enrutamiento especial

3. Probar Ambos Números:

```
# Probar desde 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 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 necesitan ser corregidos.

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 interrupción del 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 llamadas salientes

Migración

Al migrar de un solo a multi-MSISDN:

El suscriptor tiene 1 MSISDN

Agregar segundo MSISDN

Probar ambos números

¿Ambos funcionan?

Sí

No

Activar para el cliente

Depurar problema

Completo

SIM Multi-IMSI: Múltiples Identidades de Red

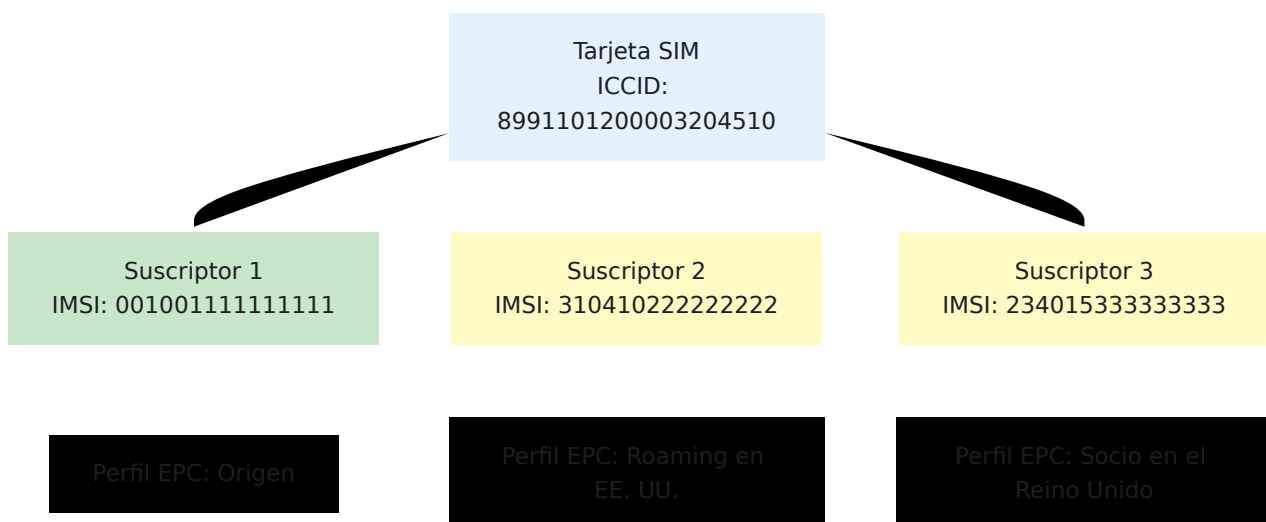
Cómo Funciona

Una SIM multi-IMSI contiene múltiples perfiles completos de suscriptor, 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 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/costo bajo
- Dispositivos críticos mantienen conectividad

4. Cumplimiento Regulatorio

- Diferentes IMSIs para diferentes zonas regulatorias
- Cumplir con los requisitos de residencia de datos locales
- 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)
- 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 deciden qué IMSI usar
- Basado en redes disponibles, ubicación, política
- El HSS autentica el IMSI que el dispositivo presenta

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": "\0010011111111111",
    "sim_id": $SIM_ID,
    "key_set_id": $KEYSET1,
    "epc_profile_id": 1
  }}'

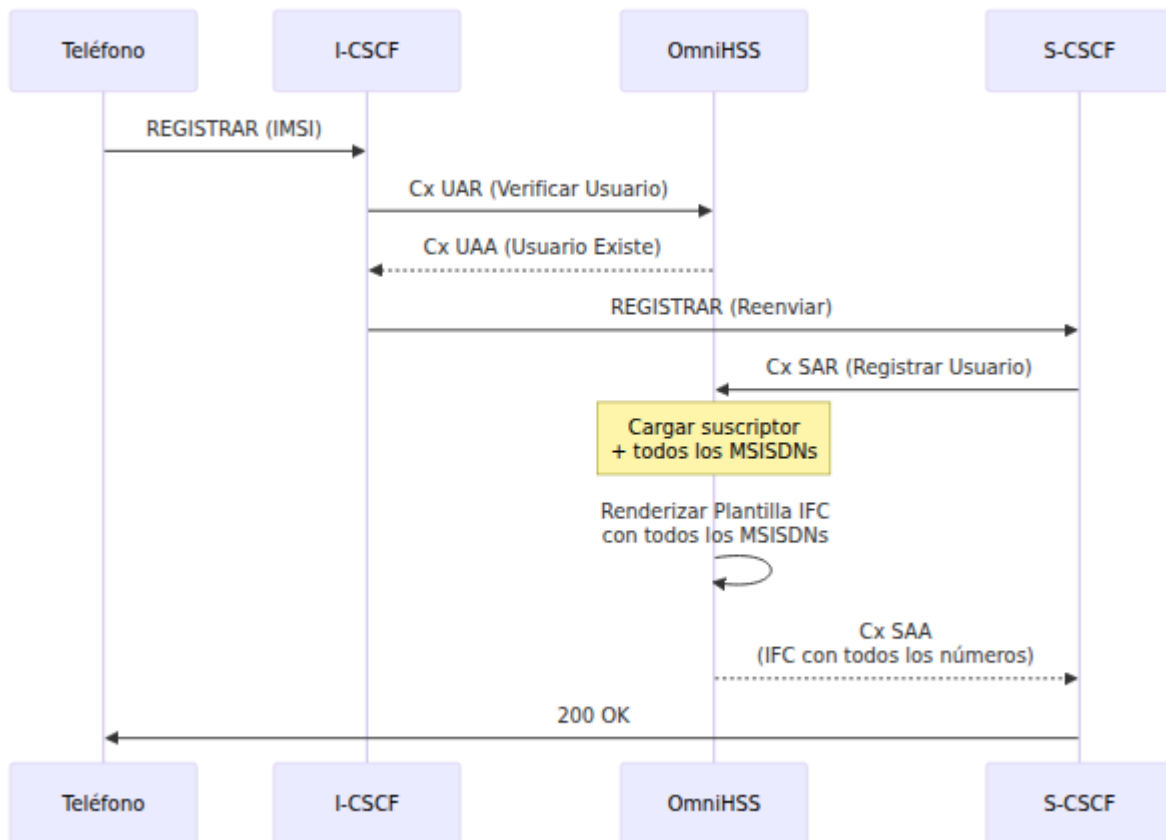
# 4. Crear conjunto de claves para IMSI 2 (socio de roaming)
KEYSET2=$(curl -k -X POST https://hss.example.com:8443/api/key_set \
  \
  -d '{"key_set": {"ki": "1111111111111111...", "opc": \
  "2222222222..."}}' \
  | jq -r '.data.id')

# 5. Crear suscriptor 2 (IMSI de roaming)
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -d '{"subscriber": {
    "imsi": "\3104102222222222",
    "sim_id": $SIM_ID,
    "key_set_id": $KEYSET2,
    "epc_profile_id": 2
  }}'

# 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; simplemente 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

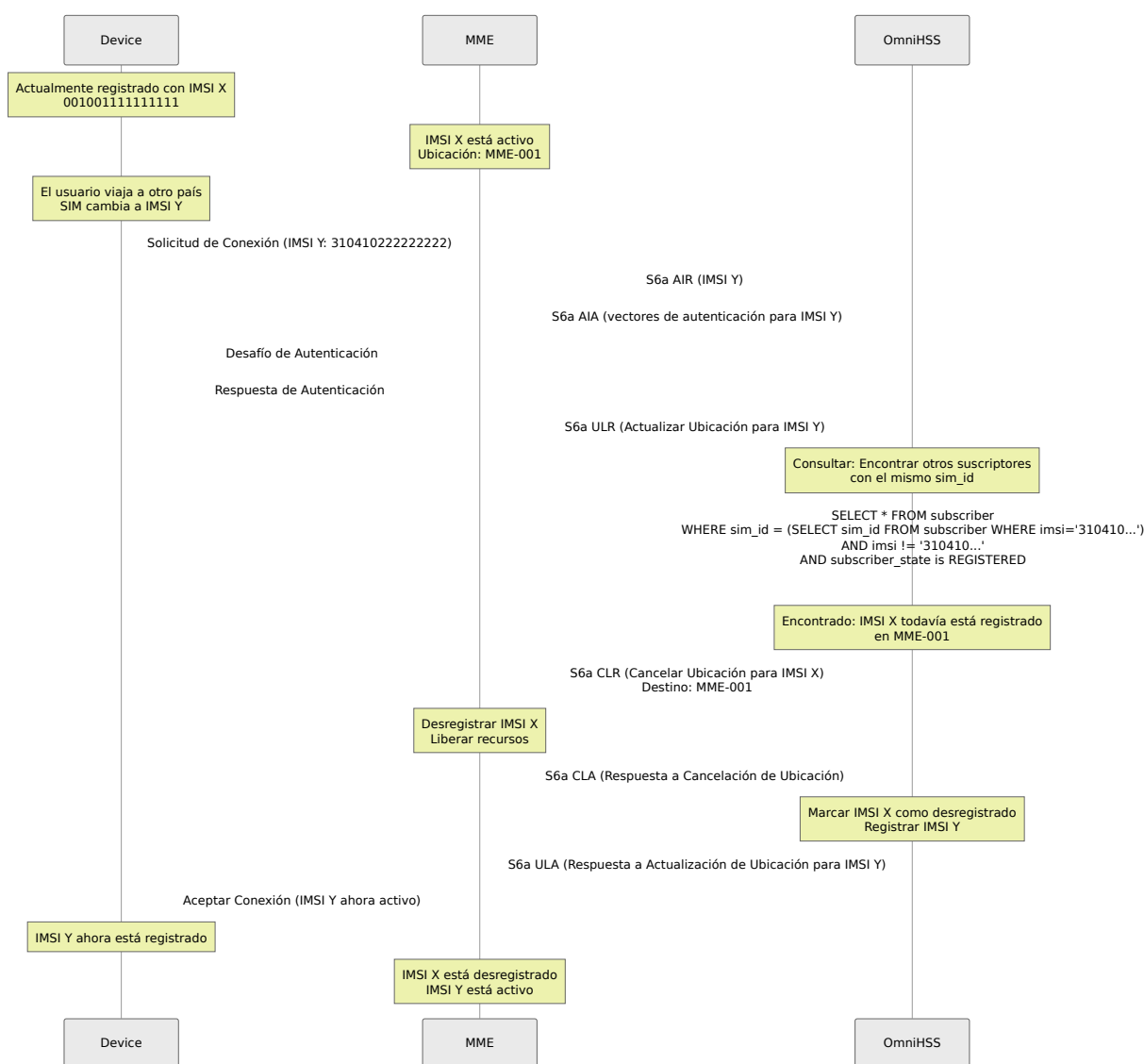
Concepto Clave: Solo un suscriptor (IMSI) por tarjeta SIM puede estar activo en un momento dado.

- Si un suscriptor está registrado en un MME usando **IMSI X**

- Y el HSS recibe una Solicitud de Actualización de Ubicación para **IMSI Y** (en la misma SIM que IMSI X)
- El HSS envía automáticamente una **Solicitud de Cancelación de Ubicación** para desregistrar **IMSI X**

Esto asegura una transferencia limpia entre IMSIs y previene conflictos en la red.

Flujo de Cambio de IMSI



Por Qué Esto Importa

Integridad de la Red:

- Previene registros duplicados desde la misma SIM física

- Asegura que los recursos de la red se liberen adecuadamente
- Mantiene datos de ubicación de suscriptor precisos

Precisión de Facturación:

- Solo un IMSI se cobra 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:

- Se liberan recursos MME para el IMSI antiguo
- Se limpian los contextos PDP y portadores
- El seguimiento de ubicación sigue siendo preciso

Disparadores de Cambio de IMSI

El dispositivo/SIM decide cuándo cambiar IMSIs basado en:

1. Disponibilidad de Red

- Red de 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

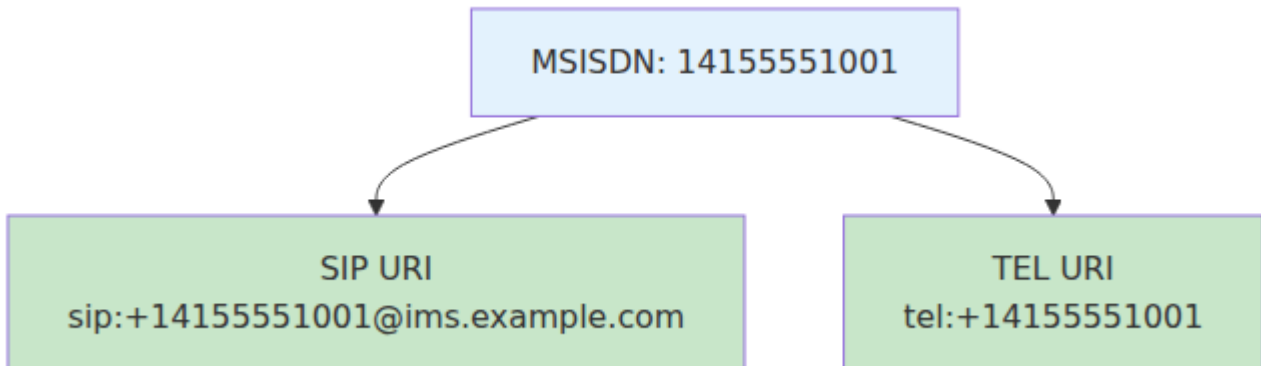
- La tarjeta SIM tiene reglas internas (por ejemplo, preferir IMSI local en ciertos países)
- Cambio automático basado en MCC/MNC

4. Optimización de Costos

- Cambiar a IMSI con tarifas de roaming más bajas
- Usar IMSI local para evitar cargos de roaming

Consideraciones IMS

El mismo comportamiento de Solicitud de Cancelación de Ubicación se aplica al registro IMS:



Impacto Operativo

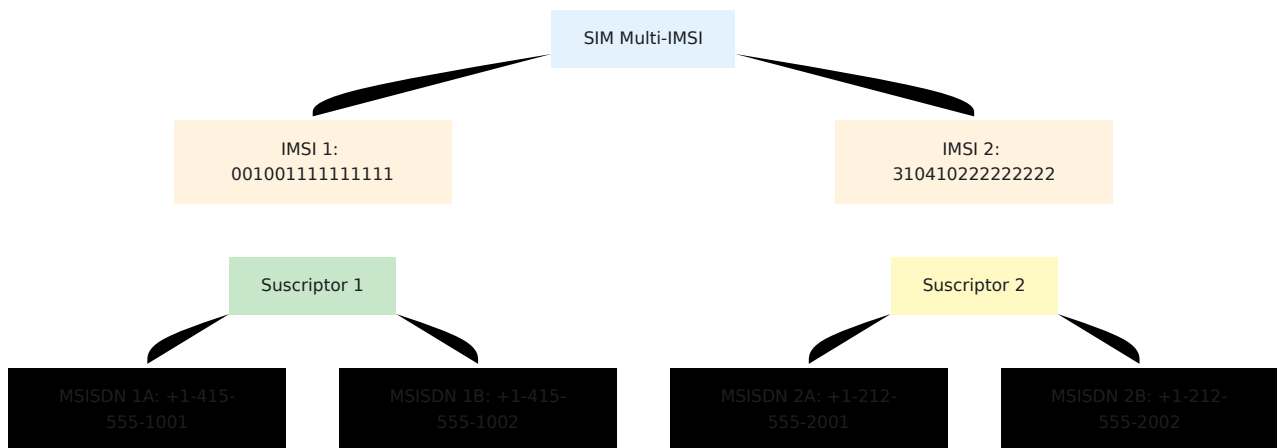
Para el Personal de Operaciones:

- 1. El suscriptor aparece fuera de línea:** Cuando cambia IMSI, el IMSI antiguo mostrará como "desregistrado" 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 cambia IMSI, la ubicación antigua se borra.
 - 4. Solución de Problemas:** Si un dispositivo no puede ser alcanzado:
 - Verificar qué IMSI está actualmente registrado
 - Confirmar que se está utilizando el IMSI correcto para la red actual
 - Asegurarse de que solo un IMSI por SIM esté en estado registrado
-

Escenarios Combinados

Multi-IMSI + Multi-MSISDN

Puedes combinar ambas funciones: múltiples IMSIs en una SIM, cada una con múltiples MSISDNs.



Ejemplo de Caso de Uso:

- **Red de Origen (IMSI 1):**
 - Número personal: +1-415-555-1001
 - Número de negocios: +1-415-555-1002
- **Red de Roaming en EE. UU. (IMSI 2):**
 - Número personal: +1-212-555-2001
 - Número de negocios: +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 Operativos

Gestión de Suscriptores Multi-MSISDN

Ver todos los MSISDNs para un suscriptor:

```
Consulta a través de API: GET /api/subscriber/imsi/:imsi
```

La respuesta incluye todos los MSISDNs vinculados.

Solución de Problemas Multi-IMSI

Dispositivo no se conecta con el segundo IMSI:

1. Verificar que exista el segundo registro de suscriptor para ese IMSI
2. Comprobar que el conjunto de claves esté configurado correctamente para ese IMSI
3. Verificar que el perfil EPC esté asignado
4. Confirmar que las reglas de roaming permitan la conexión

Dispositivo cambia IMSIs inesperadamente:

- Esto es controlado por la lógica del dispositivo/SIM, no por el HSS
- El HSS autentica cualquier IMSI que se presente
- Verificar la configuración de selección de IMSI del dispositivo

Solución de Problemas Multi-MSISDN

El segundo número no suena:

1. Verificar que el MSISDN esté vinculado en la tabla de unión
2. Comprobar que la plantilla de perfil IMS incluya la variable `{{msisdns}}`
3. Confirmar que el registro IMS incluya todas las identidades públicas
4. Revisar los registros S-CSCF para identidades registradas

Las llamadas salientes solo muestran un número:

- El dispositivo selecciona qué número presentar como ID de llamada
 - Esto es configuración del dispositivo, no del HSS
 - El HSS proporciona todas las identidades; el dispositivo elige
-

Resumen de Beneficios

Beneficios Multi-MSISDN

- ✓ Una SIM, múltiples números de teléfono
- ✓ Líneas de negocios y personales separadas
- ✓ Presencia local internacional
- ✓ Gestión simplificada del dispositivo
- ✓ 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 failover
- ✓ 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 de negocio complejos
 - ✓ Optimización internacional y local
-

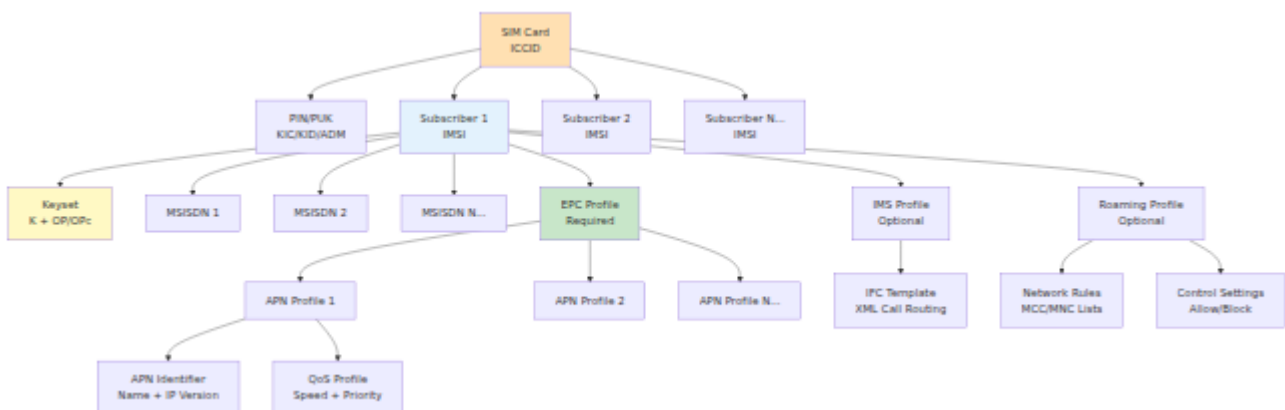
[← Volver a la Guía de Operaciones](#)

Gestión de Perfiles de OmniHSS

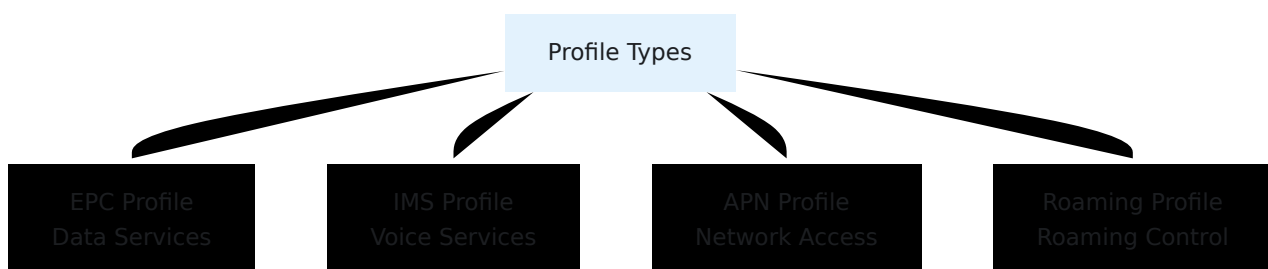
[← Volver a la Guía de Operaciones](#)

Descripción General

OmniHSS utiliza **perfiles** para definir las características del servicio para los suscriptores. Los perfiles permiten crear plantillas de servicio reutilizables que se pueden asignar a múltiples suscriptores, simplificando la provisión y asegurando 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
<code>ue_ambr_dl_kbps</code>	Límite de velocidad de descarga	10,000 - 1,000,000 Kbps
<code>ue_ambr_ul_kbps</code>	Límite de velocidad de carga	5,000 - 500,000 Kbps
<code>network_access_mode</code>	Tipo de servicio	"packet_only" o "packet_and_circuit"
<code>tracking_area_update_interval_seconds</code>	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 de país de origen

- `{{mnc}}` - Código de 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>"
  }
}'
```

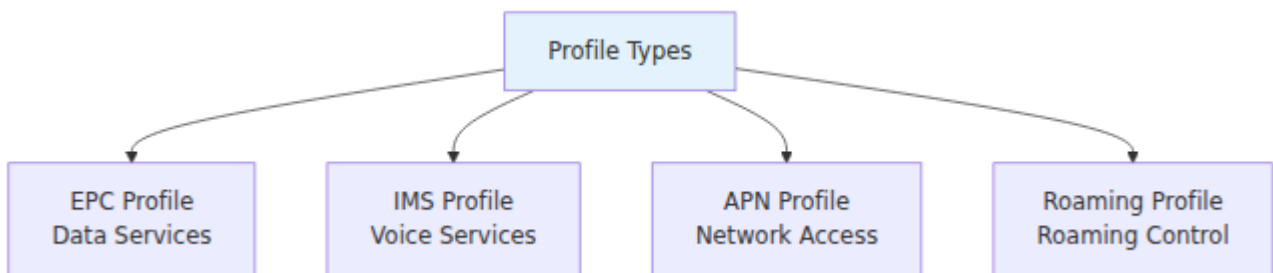
Ejemplo de Plantilla IFC

```
<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 del 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 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	Transmisión de video	Alto
5	Non-GBR	Señalización IMS	Medio
9	Non-GBR	Internet (predeterminado)	Más bajo

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`.

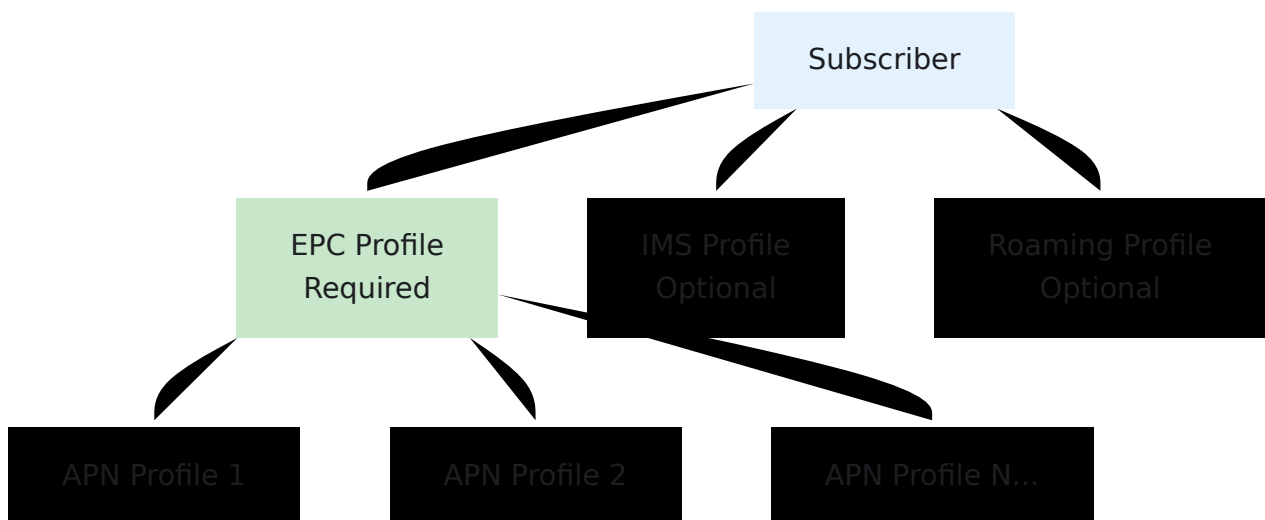
Inserte registros en la tabla de unión para vincular los IDs de perfil APN al ID de perfil EPC. Se pueden asignar múltiples perfiles APN a un perfil EPC.

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": 1,
      "epc_profile_id": 1,
      "ims_profile_id": 1,
      "roaming_profile_id": 1
    }
  }'
```

```
# Actualizar perfil del suscriptor
curl -k -X PUT https://hss.example.com:8443/api/subscriber/1 \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "epc_profile_id": 2
    }
  }'
```

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

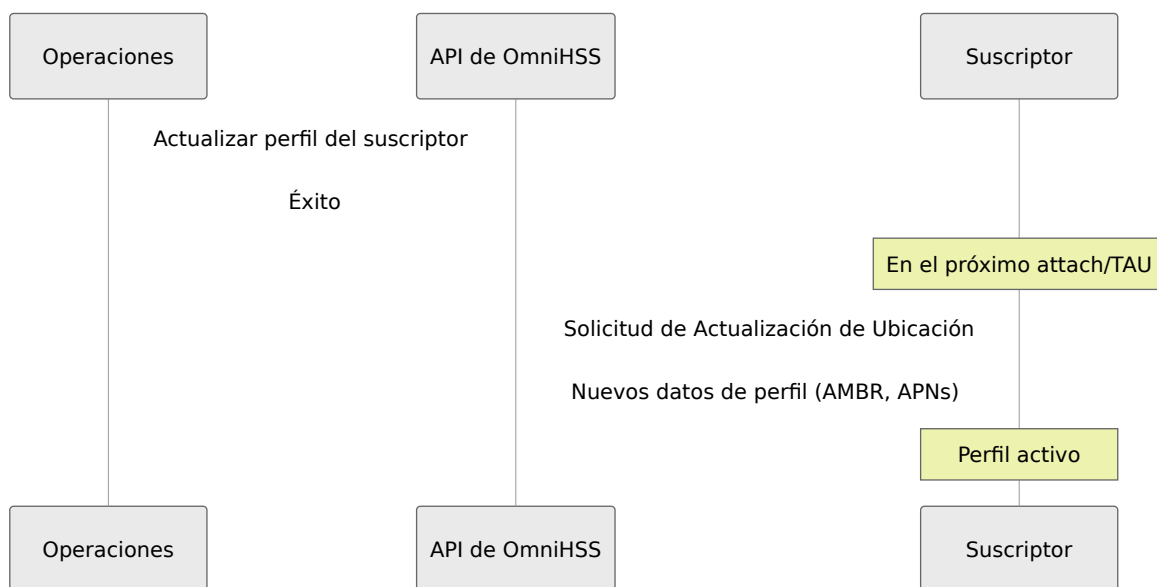
[Nivel de Servicio]-[Velocidad]-[Características]

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 vigor en el siguiente:

- Actualización de Área de Seguimiento (TAU)
- Attach
- Registro IMS (para cambios de 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 en busca de errores de 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 desde el UE

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

Flujos de Protocolo OmniHSS

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

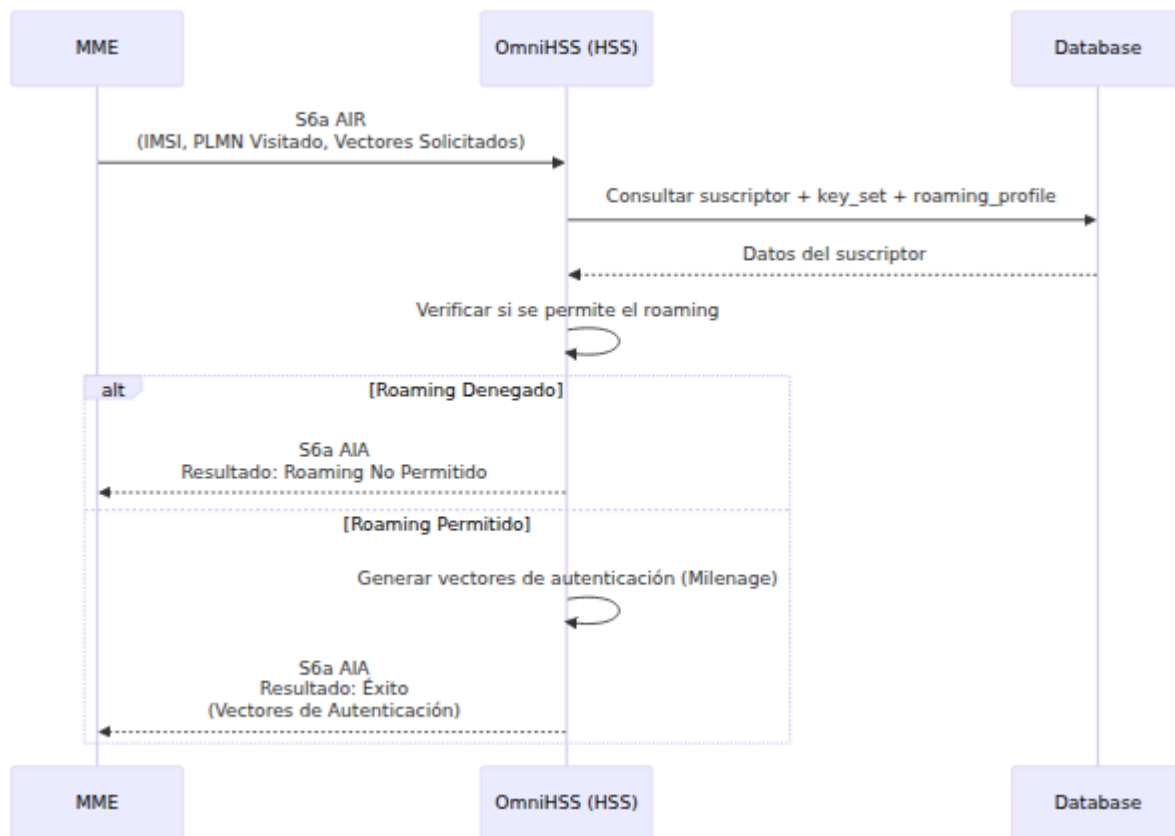
Descripción General

Este documento detalla los flujos de mensajes del protocolo Diameter soportados por OmniHSS. Comprender 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.

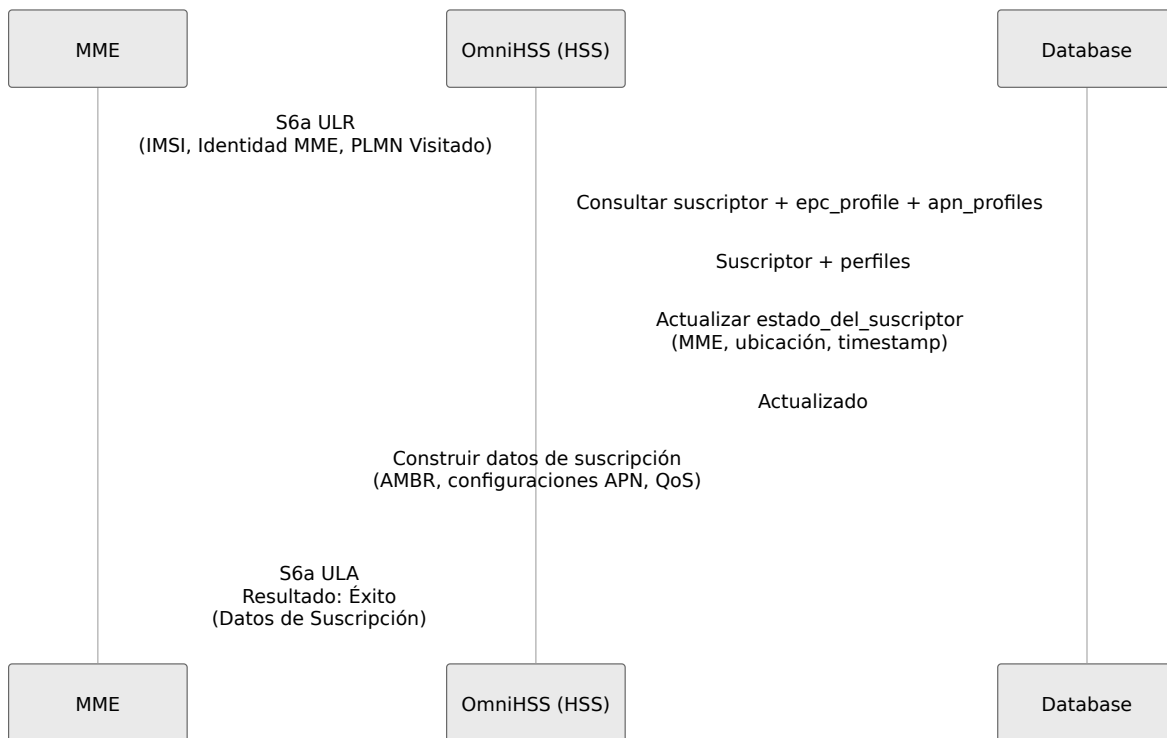


AVPs Clave:

- 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.

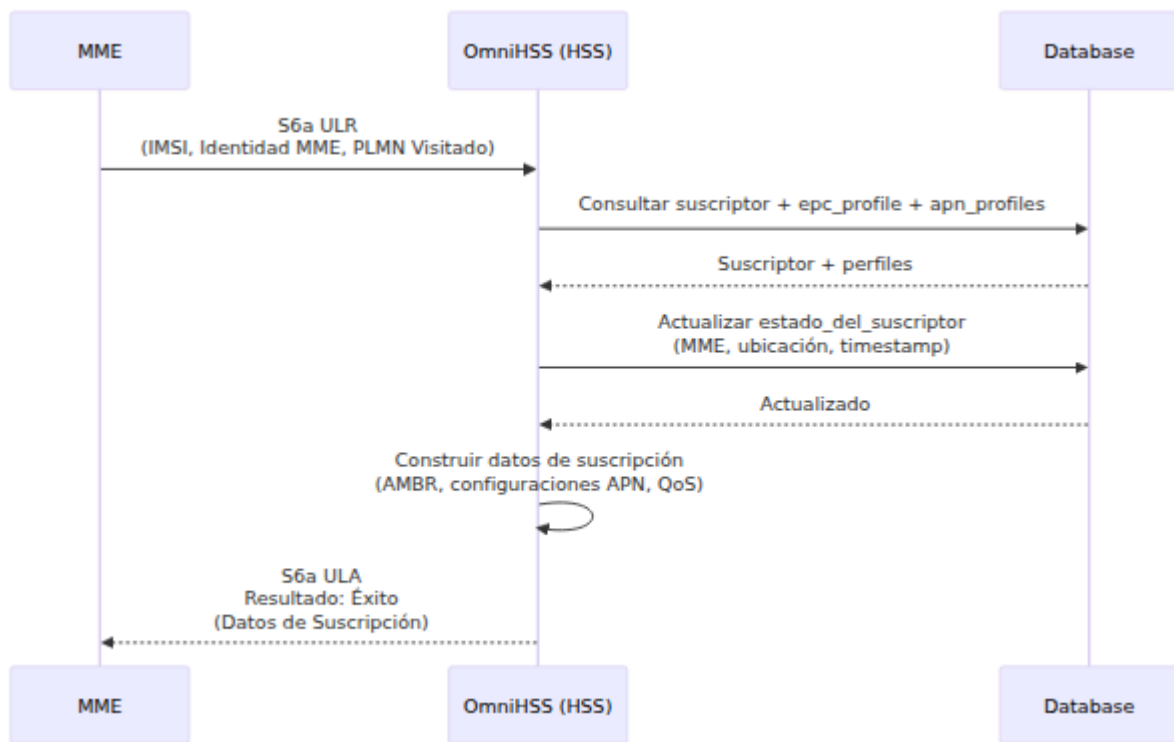


AVPs Clave:

- Solicitud: User-Name (IMSI), RAT-Type, ULR-Flags, Visited-PLMN-Id, UE-SRVCC-Capability
- Respuesta: Subscription-Data (AMBR, APN-Configuration, Network-Access-Mode)

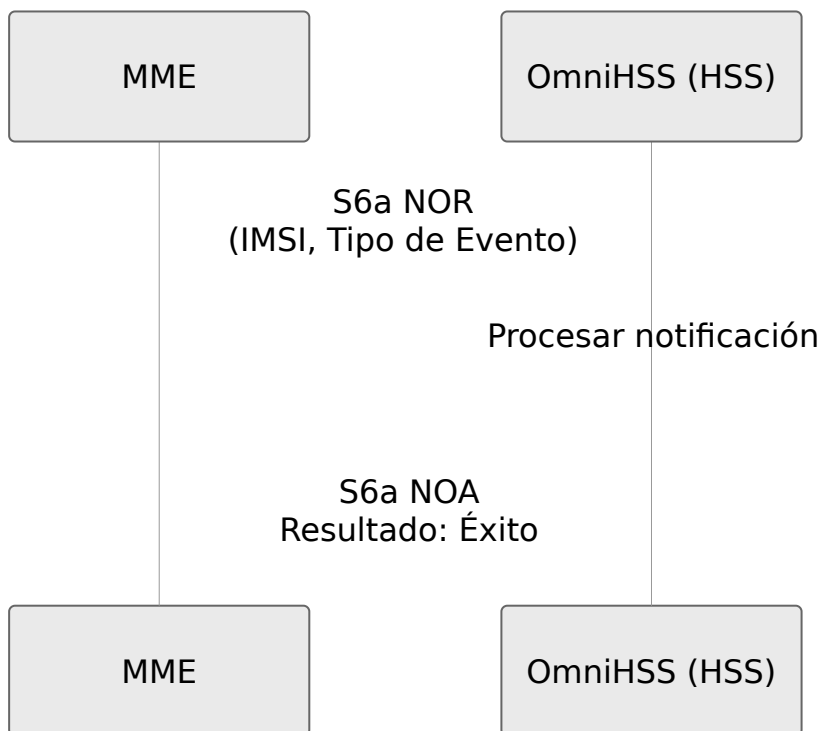
Solicitud de Purga de UE (PUR/PUA)

MME notifica a HSS cuando se elimina el contexto del suscriptor.



Solicitud de Notificación (NOR/NOA)

MME informa a HSS sobre varios eventos.

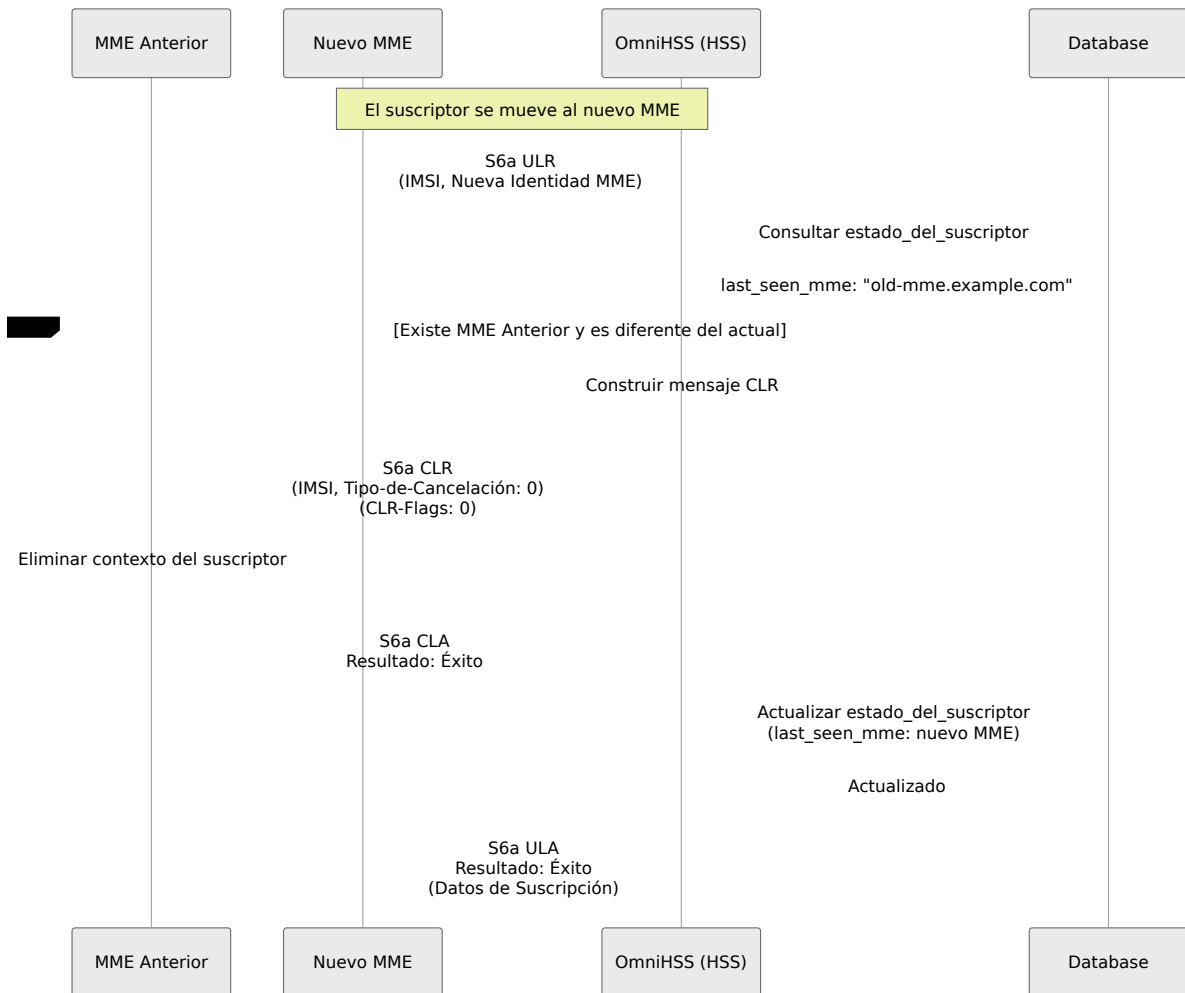


Solicitud de Cancelación de Ubicación (CLR/CLA)

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.



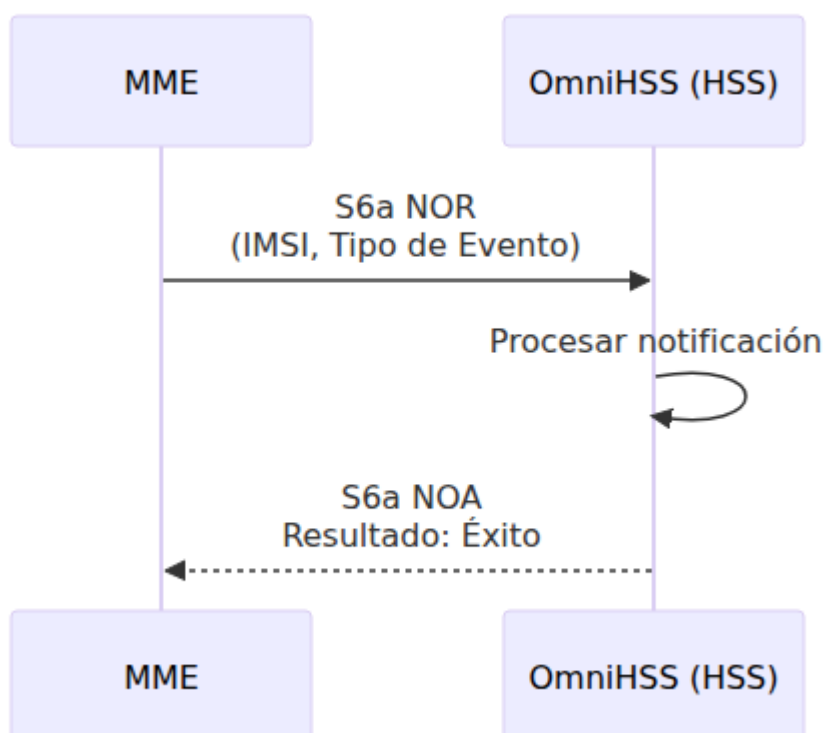
AVPs Clave (CLR Automático):

- User-Name: IMSI del suscriptor
- Destination-Host: Nombre del host del MME anterior
- Destination-Realm: Dominio 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 desasociar forzosamente a los 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 del host del último MME visto
- Destination-Realm: Dominio del último MME visto
- Cancellation-Type: `:subscription_withdrawal` (codificado como entero según 3GPP TS 29.272)
- CLR-Flags:
 - s6a_indicator: 1 (indica interfaz S6a)
 - reattach_required: 1 (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 Adición 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 = Se utilizó la interfaz S6a
Reasociación Requerida	1	1 = UE debe realizar nueva asociación

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 MSISDN, 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:

- **Se envía un CLR** a "mme01.operator.com" con IMSI 999000123456789
- Ambos MSISDNs se ven afectados (mismo suscriptor, misma SIM)
- El AVP User-Name contiene el IMSI, no los MSISDNs

Escenario 2: Múltiples Suscriptores (Diferentes IMSIs), Mismo MSISDN

OmniHSS impone una **restricción de MSISDN único** (un MSISDN no puede pertenecer a múltiples suscriptores simultáneamente). Sin embargo, durante la portabilidad/migración:

Suscriptor A:

- IMSI: 999000111111111
- MSISDN: "+1234567890"
- last_seen_mme: "mme01.operator.com"

Suscriptor B (después de la portabilidad):

- IMSI: 999000222222222
- MSISDN: "+1234567890" # Mismo MSISDN, diferente SIM/IMSI
- last_seen_mme: "mme02.operator.com"

Cuando el Suscriptor B se registra:

- **No se envía CLR** (diferente IMSI = diferente suscriptor)
- El Suscriptor A permanece registrado en mme01
- El Suscriptor B se registra en mme02
- Ambos pueden estar activos simultáneamente (diferentes dispositivos físicos)

Escenario 3: CLR Programático para Suscriptor Multi-MSISDN

Resultado:

- **Se envía un CLR** al last_seen_mme del suscriptor
- **Todos los MSISDNs** asociados con ese IMSI son 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 `estado_del_suscriptor` 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. **Sin CLR si No Hay MME Anterior:** Si `last_seen_mme` es `nil` (el suscriptor nunca se registró), no se envía CLR durante ULR.

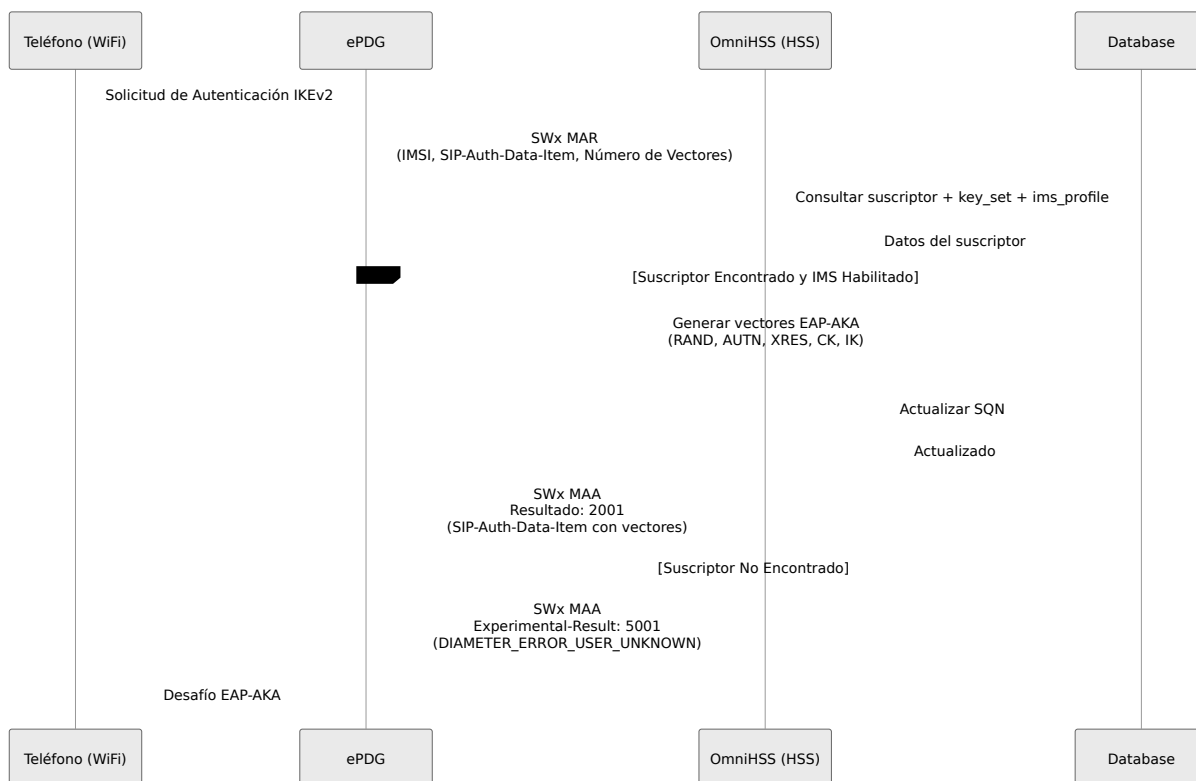
4. **Datos de Suscripción Incluidos:** El CLR automático (durante ULR) incluye el AVP completo `Subscription-Data` para ayudar al antiguo MME a limpiar correctamente el contexto.
 5. **Asincrónico:** El CLR se envía de manera asincrónica (fire-and-forget). La respuesta ULA al nuevo MME no espera por CLA del antiguo MME.
 6. **Manejo de CLA:** OmniHSS recibe respuestas CLA pero actualmente las descarta (`:discard` en la línea 398). Esto previene bucles de mensajes y es un comportamiento estándar de HSS.
-

Interfaz SWx (Acceso No 3GPP / Llamadas WiFi)

La interfaz SWx habilita las llamadas WiFi conectando el ePDG (Gateway de Datos de Paquete Evolucionado) al HSS para la autenticación y autorización del suscriptor sobre redes de acceso no 3GPP.

Solicitud de Autenticación Multimedia (MAR/MAA)

ePDG solicita vectores de autenticación EAP-AKA para el registro de llamadas WiFi.



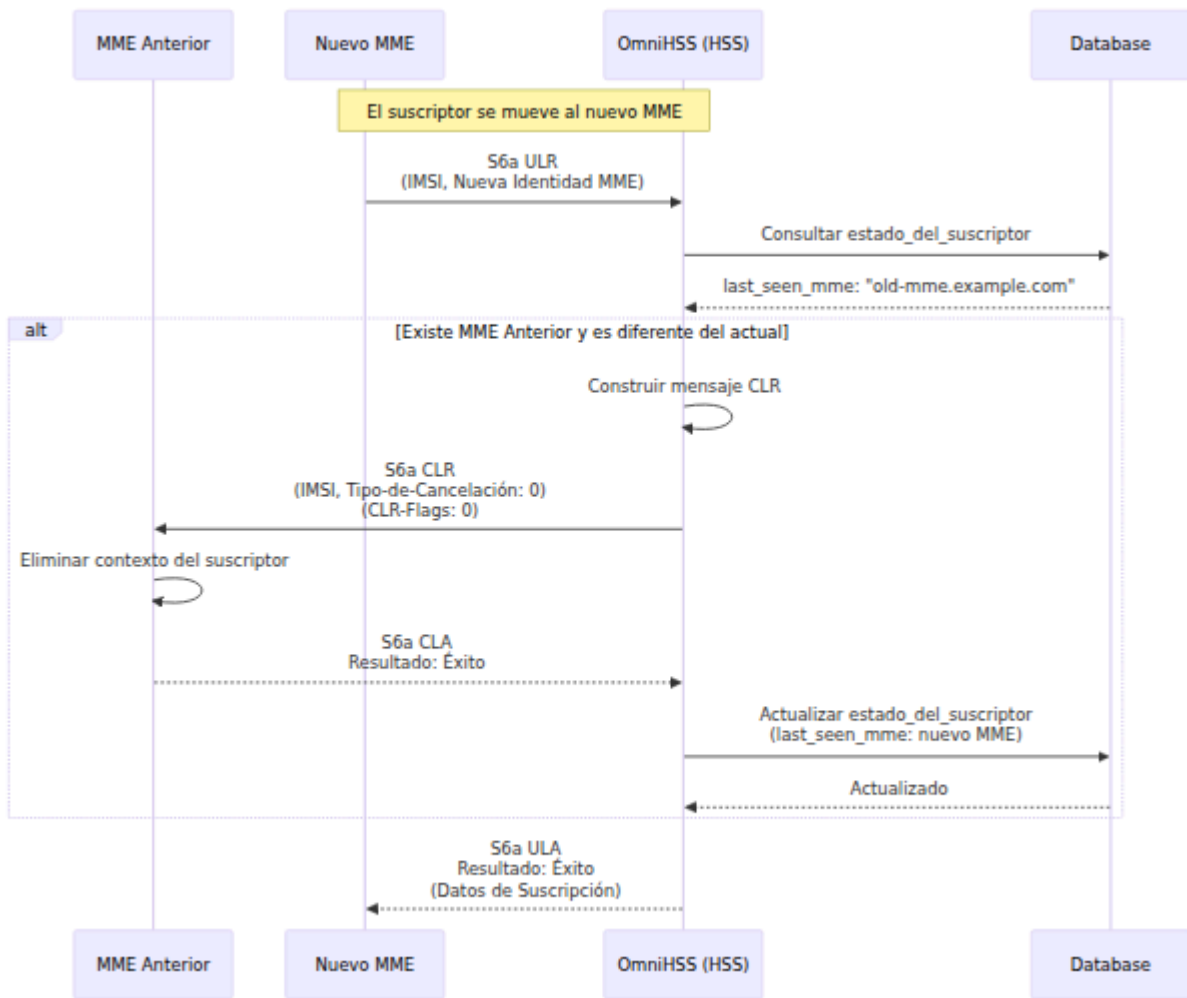
AVPs Clave:

- 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 el 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:

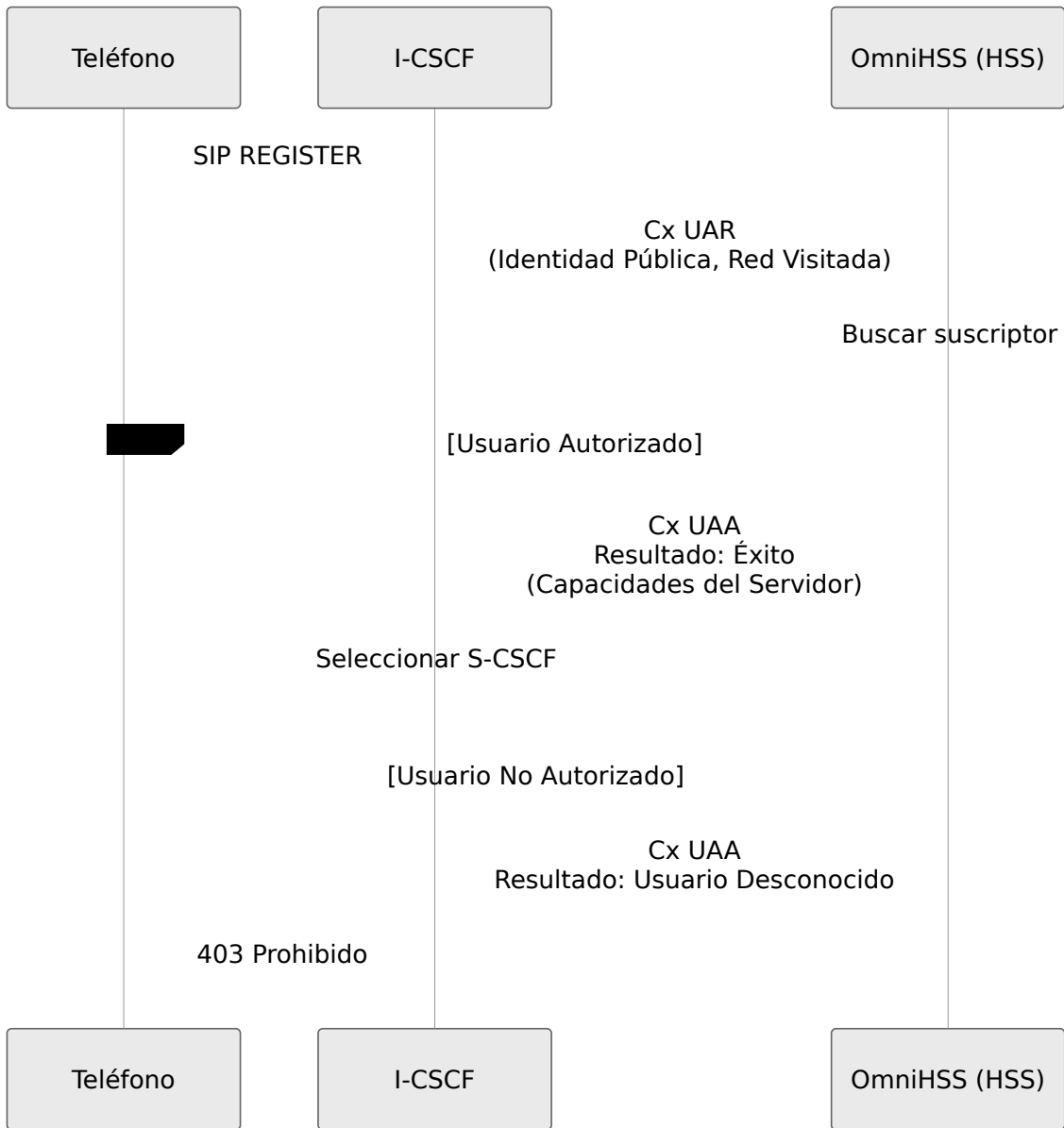
Tipo	Valor	Descripción
NO_ASSIGNMENT	0	Solo consulta, sin cambio de estado
REGISTRATION	1	Registro inicial de llamadas WiFi
RE_REGISTRATION	2	Actualización de registro
UNREGISTERED_USER	3	Servicios para usuario no registrado
TIMEOUT_DEREGISTRATION	4	Tiempo de espera de registro
USER_DEREGISTRATION	5	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), Tipo-de-Asignación-Servidor, Nombre-Servidor (identidad de ePDG), Service-Selection (APN)
- Respuesta: User-Data (XML del perfil IFC), Non-3GPP-User-Data

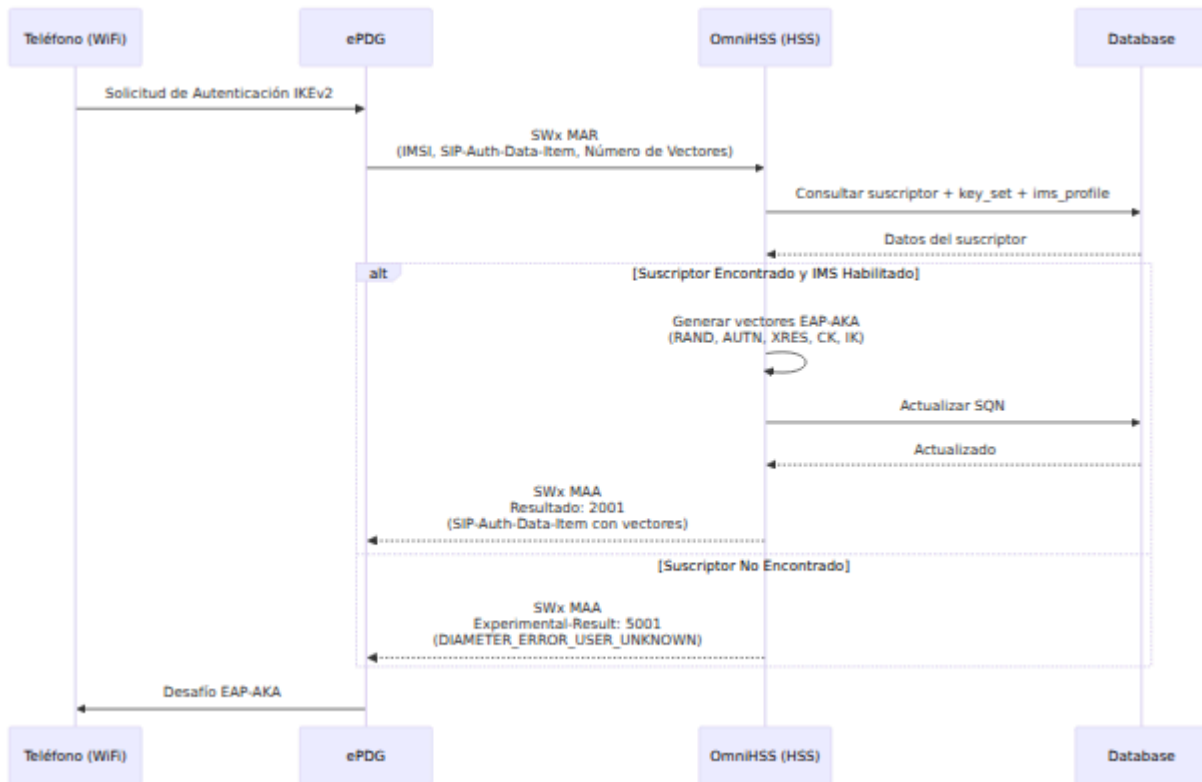
Flujo de Registro de Llamadas WiFi

Registro completo de llamadas WiFi de extremo a extremo.



Solicitud de Asignación de Servidor (SAR/SAA)

S-CSCF registra/desregistra al usuario y recupera el perfil IMS.

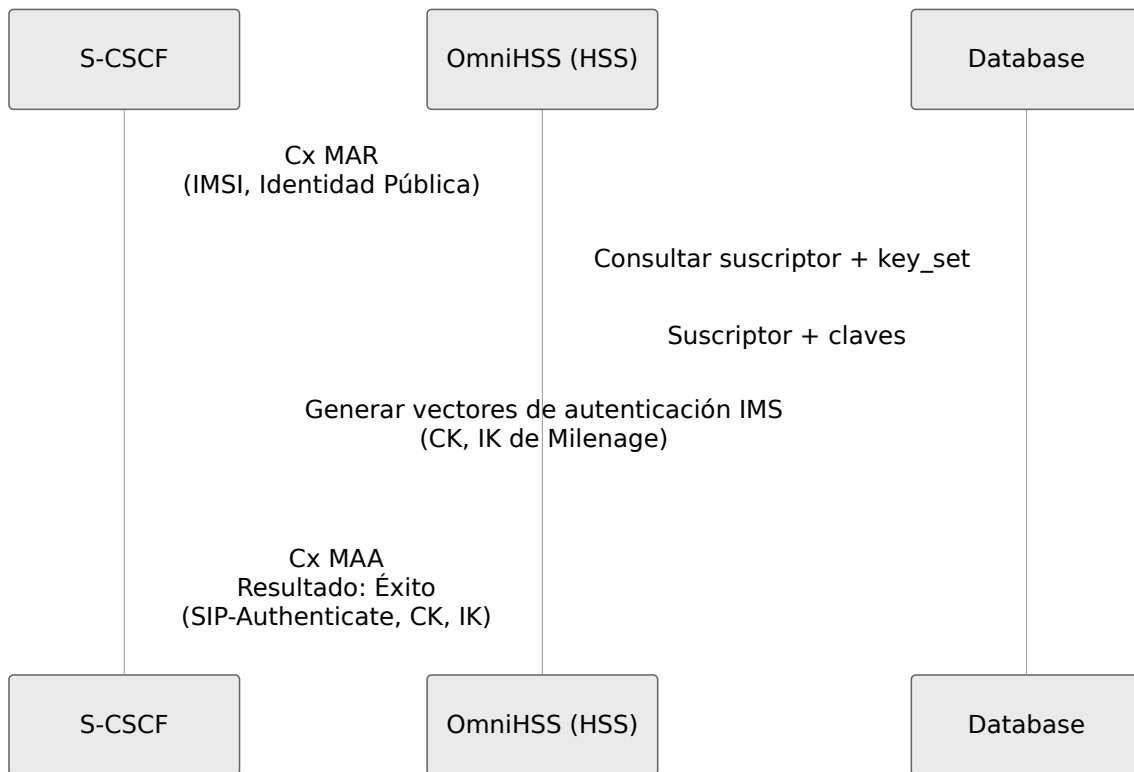


Renderización de Plantilla IFC:

- `{{imsi}}` → IMSI real
- `{{msisdns}}` → Lista de números de teléfono
- `{{mcc}}`, `{{mnc}}` → Códigos PLMN de origen

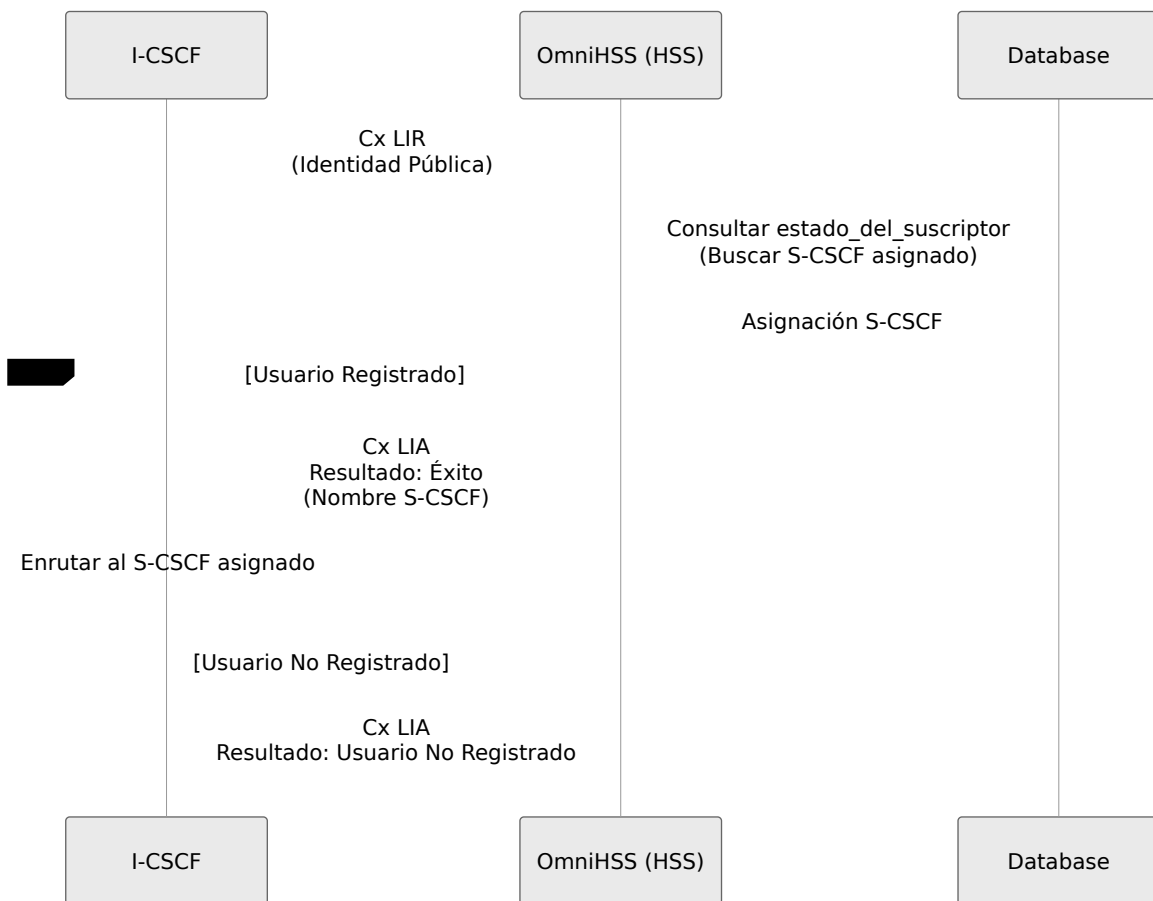
Solicitud de Autenticación Multimedia (MAR/MAA)

S-CSCF solicita vectores de autenticación para el registro IMS.



Solicitud de Información de Ubicación (LIR/LIA)

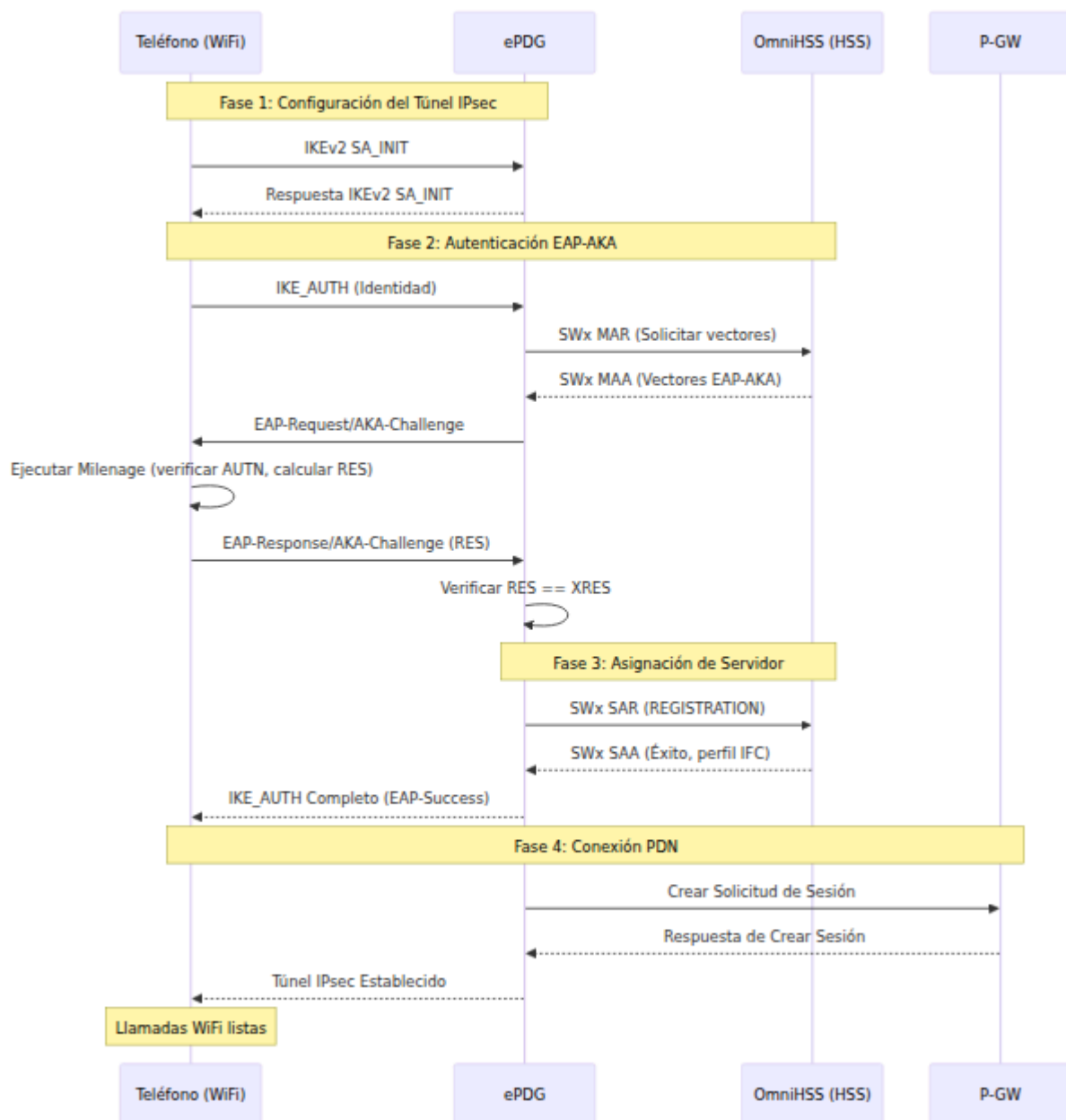
I-CSCF consulta qué S-CSCF está sirviendo al usuario.



Interfaz Sh (Datos del Perfil IMS)

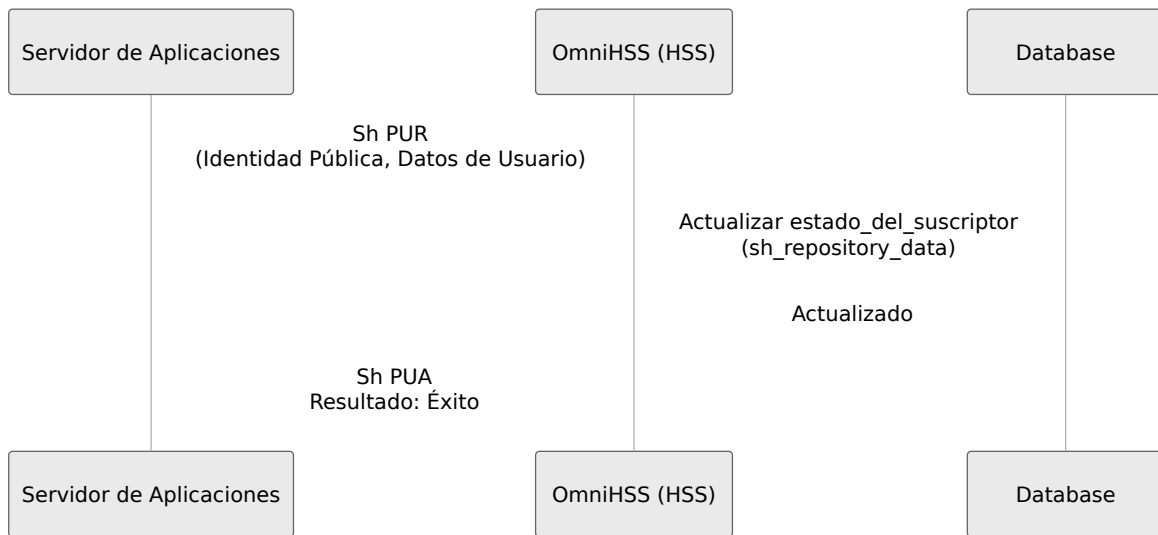
Solicitud de Datos de Usuario (UDR/UDA)

El Servidor de Aplicaciones solicita datos del perfil del suscriptor.



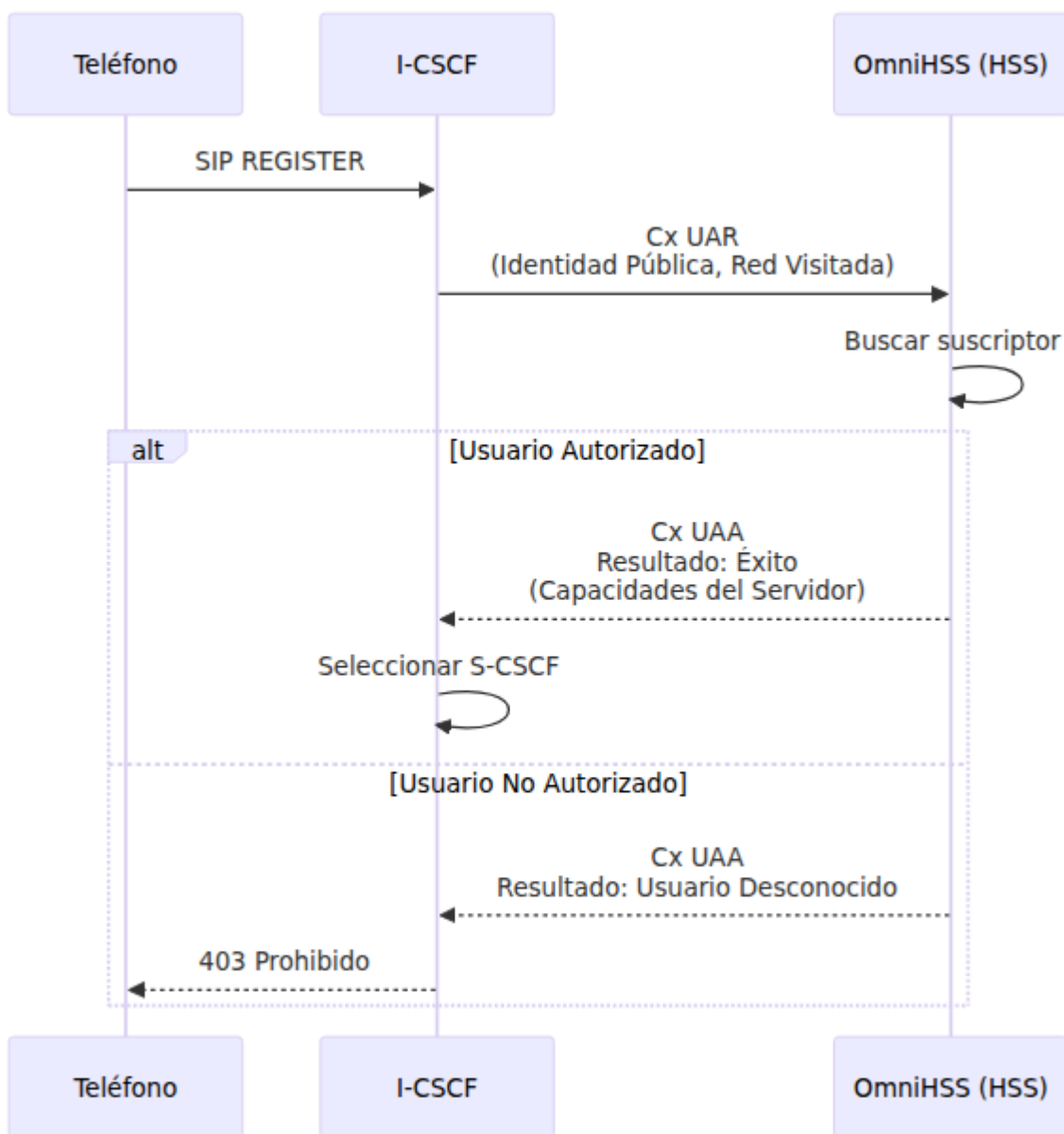
Solicitud de Actualización de Perfil (PUR/PUA)

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.



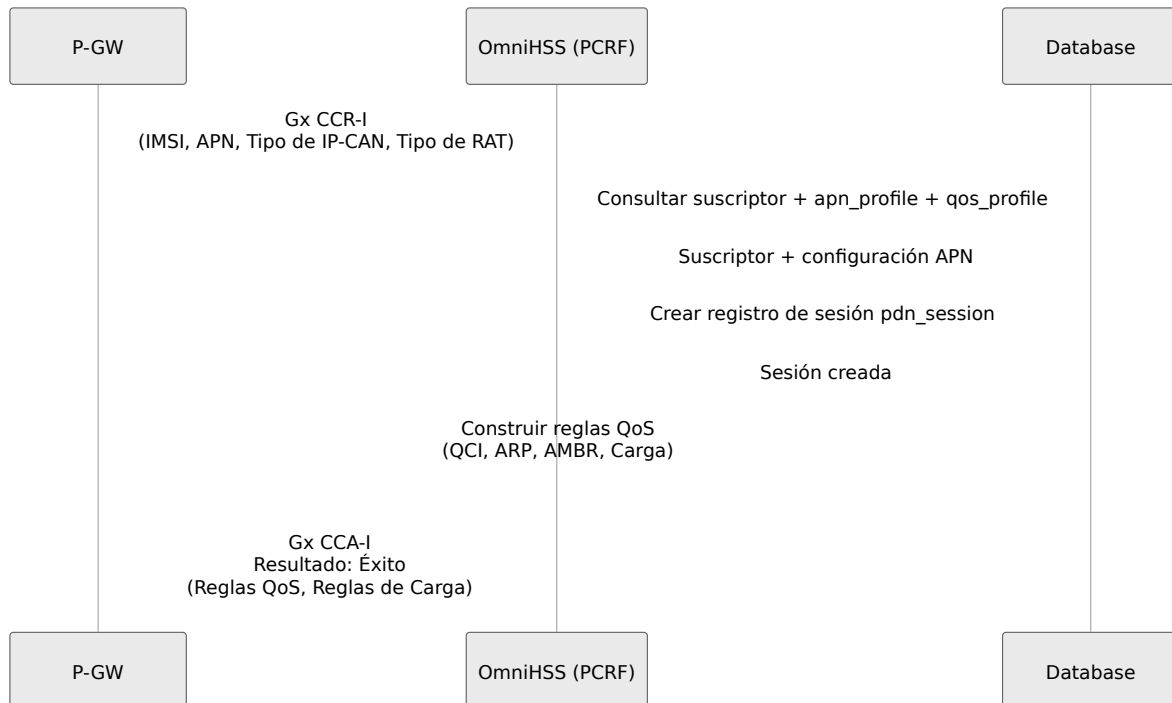
Interfaz Gx (Control de Políticas)

OmniHSS funciona como el PCRF (Función de Reglas de Políticas y Carga) a través de la interfaz Gx.

Consulte la **Documentación de PCRF** para obtener 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.

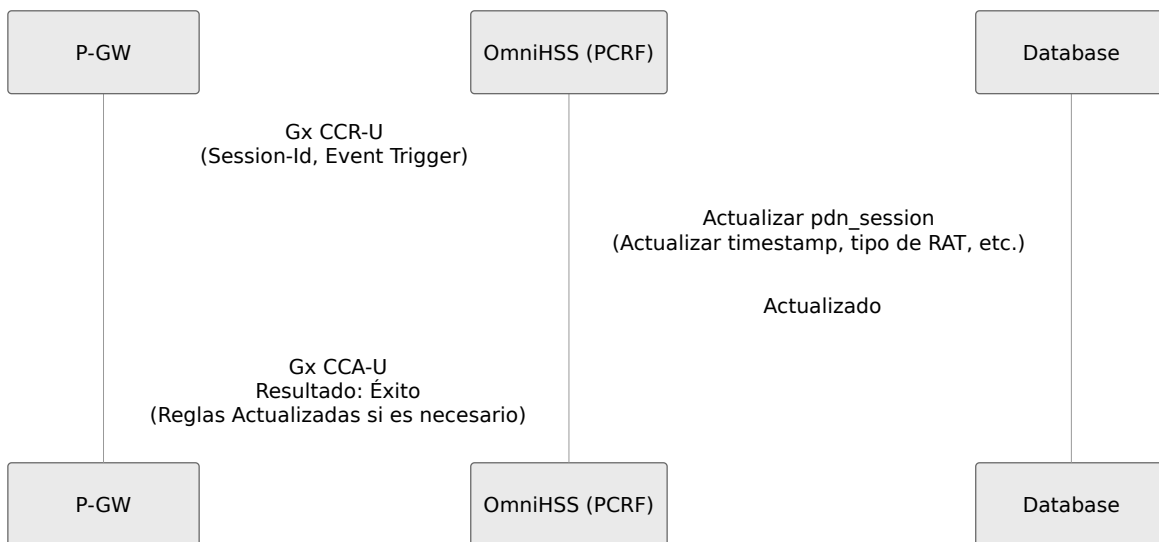


AVPs Clave:

- Solicitud: Subscription-Id (IMSI), Called-Station-Id (APN), RAT-Type, IP-CAN-Type
- Respuesta: QoS-Information (QCI, ARP, AMBR), Charging-Rule-Install

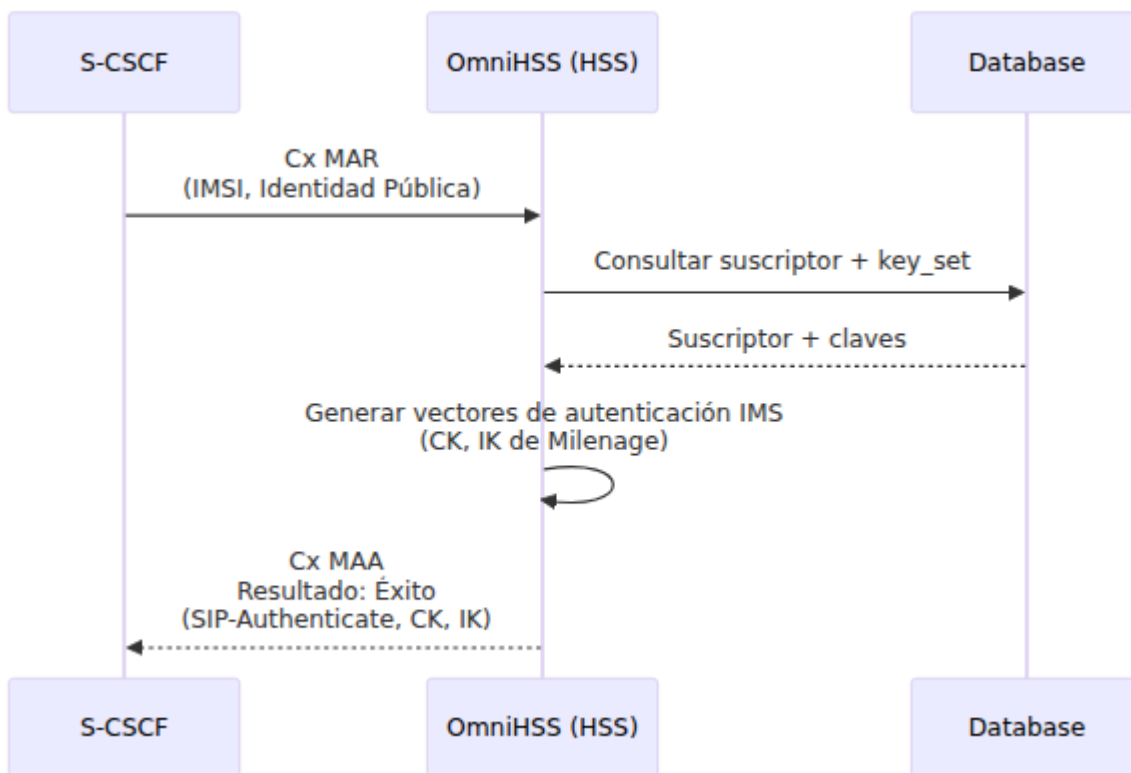
Solicitud de Control de Crédito - Actualización (CCR-U/CCA-U)

P-GW notifica cambios en la sesión.



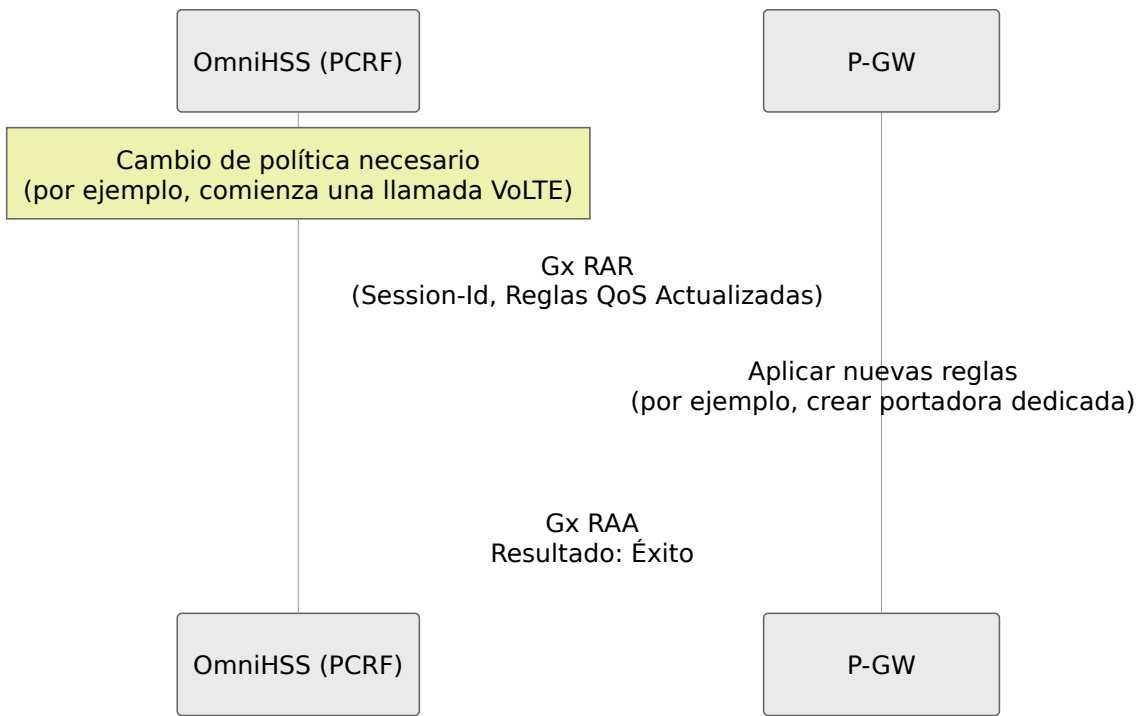
Solicitud de Control de Crédito - Terminar (CCR-T/CCA-T)

P-GW notifica cuando finaliza la sesión PDN.



Solicitud de Reautenticación (RAR/RAA)

OmniHSS (PCRF) inicia la actualización de políticas a P-GW.



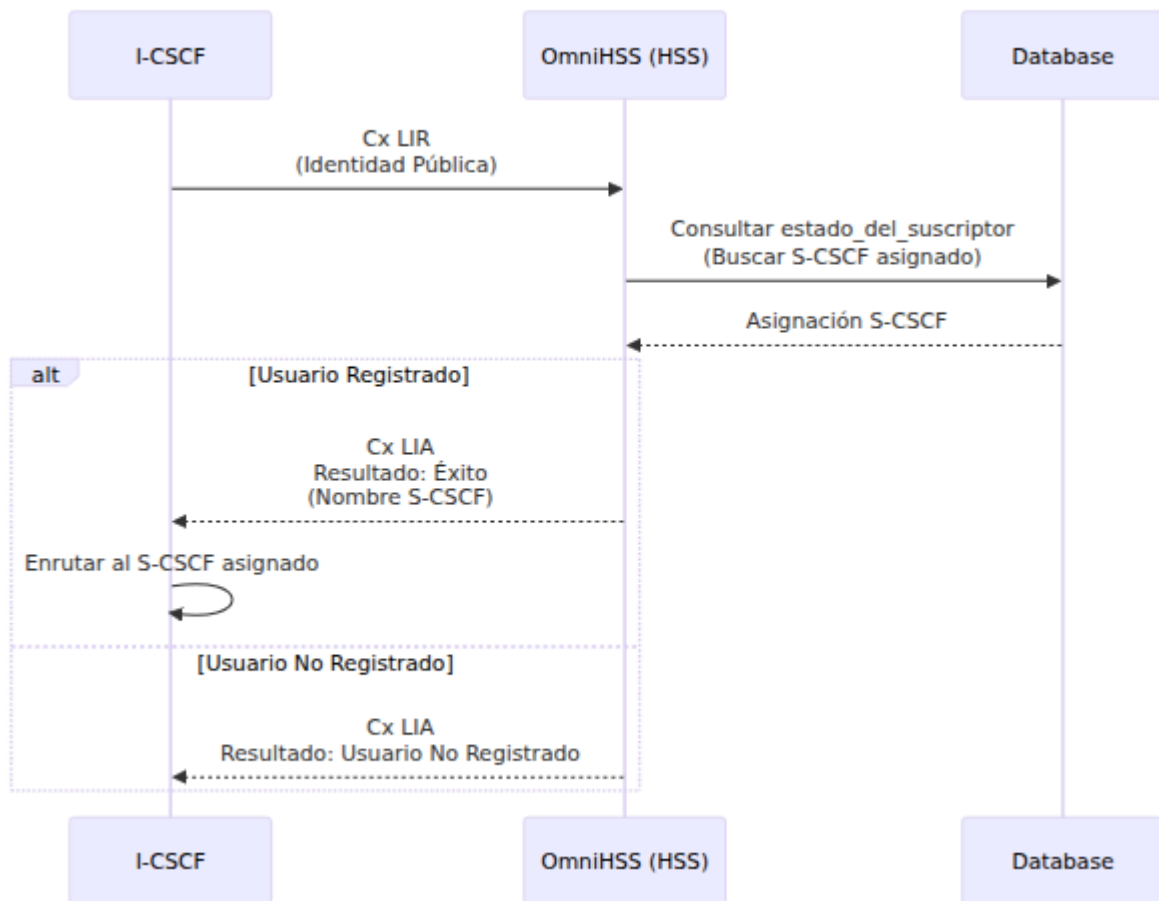
Interfaz Rx (Política de Medios IMS)

OmniHSS funciona como el PCRF a través de la interfaz Rx para la autorización de medios IMS.

Consulte la **Documentación de PCRF** para obtener flujos de llamadas VoLTE detallados y autorización de medios.

Solicitud AA (AAR/AAA)

P-CSCF solicita autorización de medios para la sesión IMS.

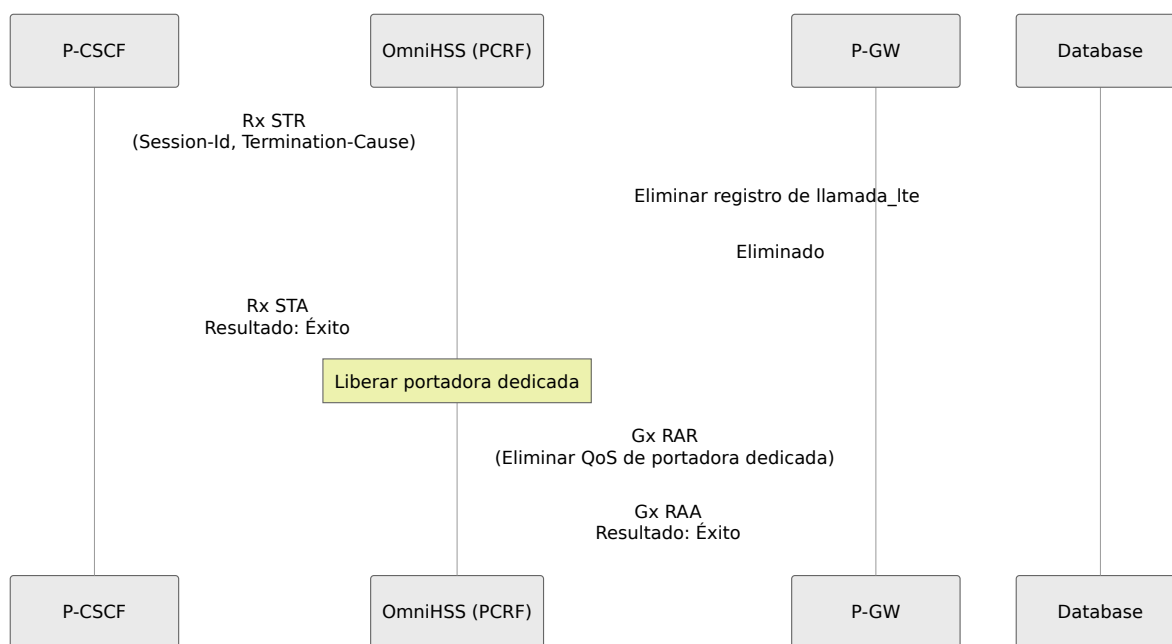


Información Clave:

- 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 finaliza la sesión IMS.



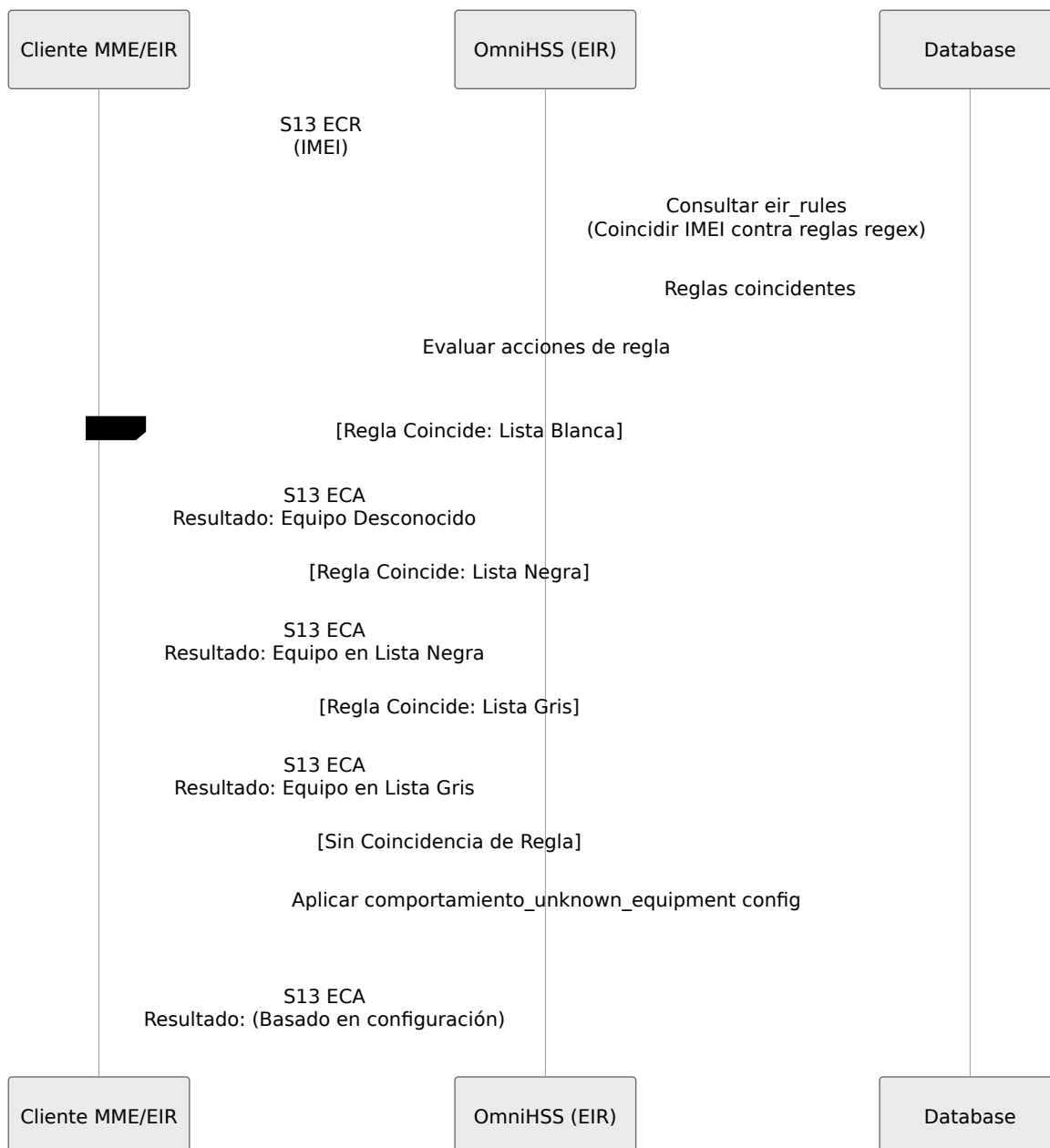
Interfaz S13 (EIR)

OmniHSS funciona como el EIR (Registro de Identidad de Equipos) a través de la interfaz S13.

Consulte la **Documentación de EIR** para obtener detalles sobre la verificación de identidad del equipo, validación de IMEI y gestión de listas negras.

Solicitud de Verificación de Identidad del ME (ECR/ECA)

Cliente EIR externo (o MME) solicita validación del equipo.

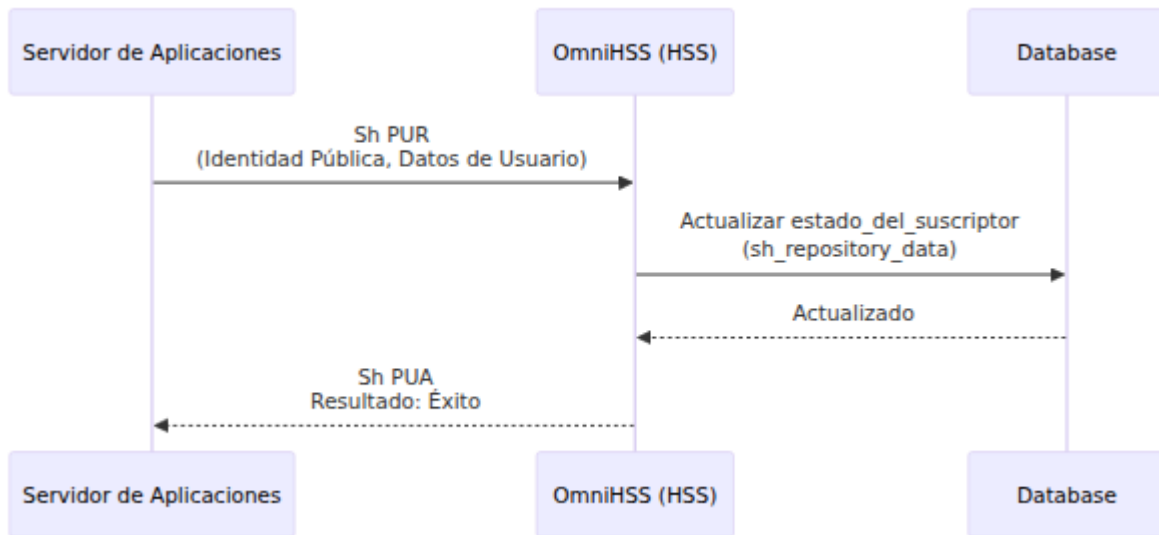


Valores de Estado del Equipo:

- **Equipo Desconocido (0)** - Dispositivo permitido (lista blanca)
- **Equipo en Lista Negra (1)** - Dispositivo bloqueado
- **Equipo en Lista Gris (2)** - Dispositivo permitido pero rastreado

Flujo de Llamada Completo: Llamada VoLTE

Configuración de llamada VoLTE de extremo a extremo que muestra múltiples interfaces.

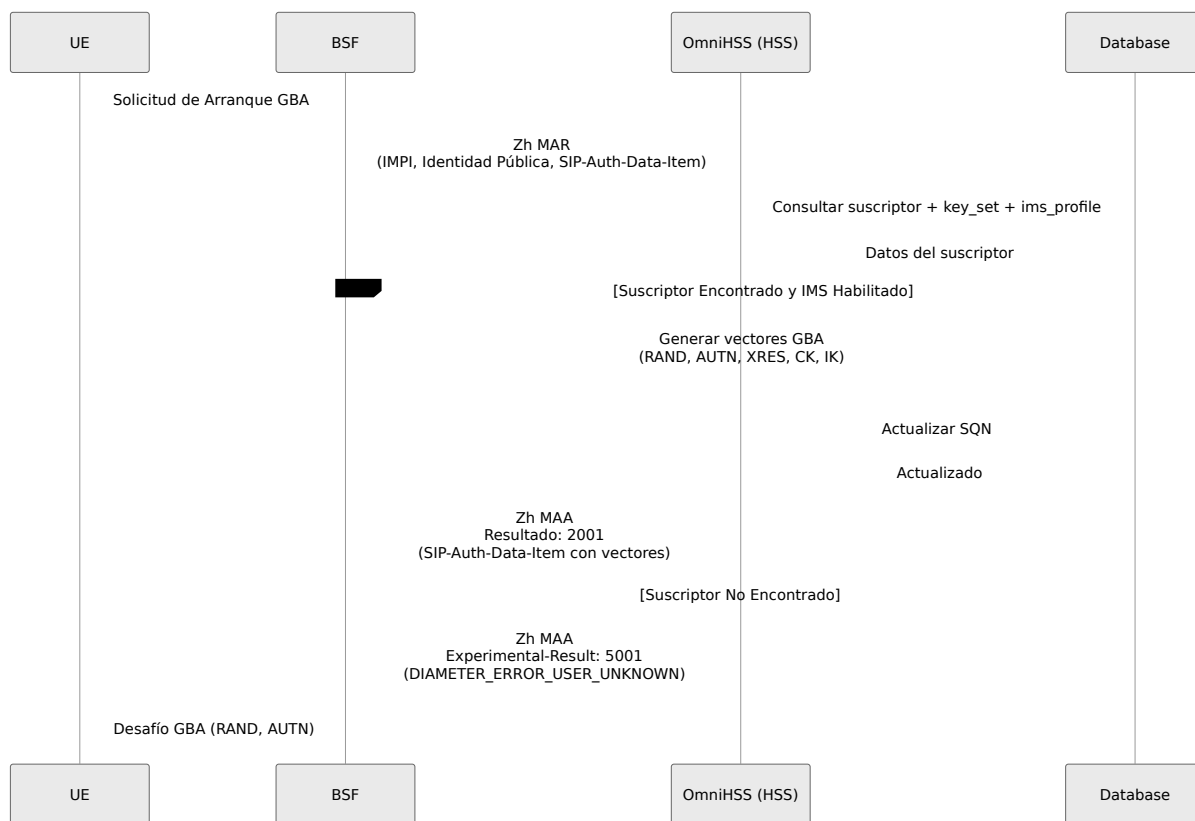


Interfaz Zh (Arquitectura de Arranque Genérico)

La interfaz Zh habilita la Arquitectura de Arranque Genérico (GBA) conectando la Función del Servidor de Arranque (BSF) al HSS para la autenticación y derivación de claves del suscriptor.

Solicitud de Autenticación Multimedia (MAR/MAA)

BSF solicita vectores de autenticación GBA para el arranque.



AVPs Clave:

- Solicitud: User-Name (IMPI), Identidad Pública, SIP-Auth-Data-Item (esquema de autenticación), Destination-Realm
- Respuesta: SIP-Auth-Data-Item (SIP-Authenticate, SIP-Authorization, Confidentiality-Key, Integrity-Key), GBA-UserSecSettings

Casos de Uso de GBA:

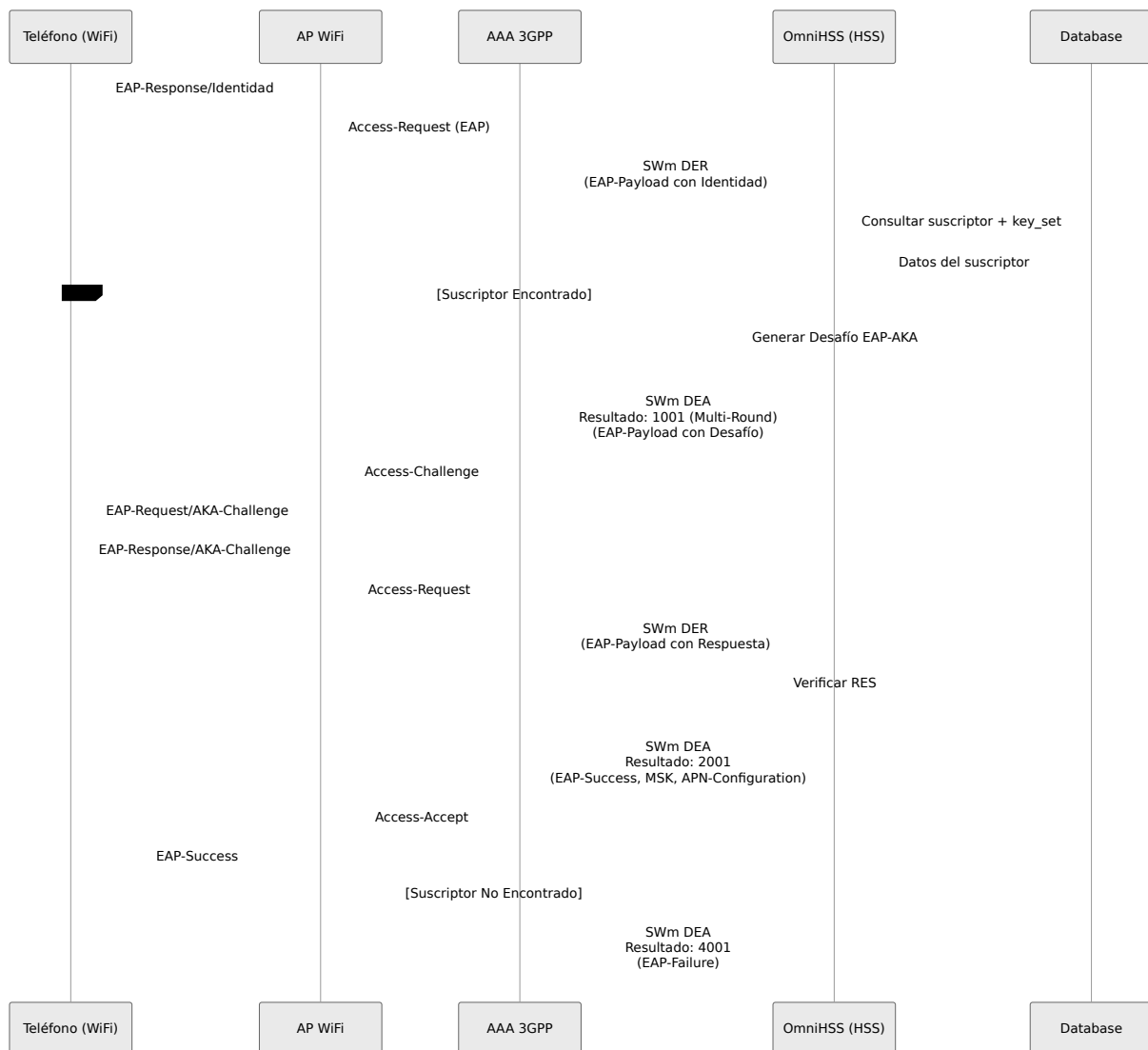
Aplicación	Descripción
MBMS	Gestión de claves del Servicio de Multicast de Difusión Móvil
HTTPS	Aprovisionamiento de certificados basado en GBA
NAF	Autenticación de Función de Aplicación de Red Genérica
Presencia	Autenticación segura del servicio de presencia

Interfaz SWm (Acceso No 3GPP No Confiable)

La interfaz SWm habilita la autenticación EAP-AKA para redes de acceso no confiables no 3GPP (por ejemplo, WiFi a través de ePDG) conectando el Servidor AAA 3GPP al HSS.

Solicitud Diameter-EAP (DER/DEA)

Intercambio de autenticación EAP para acceso WiFi.



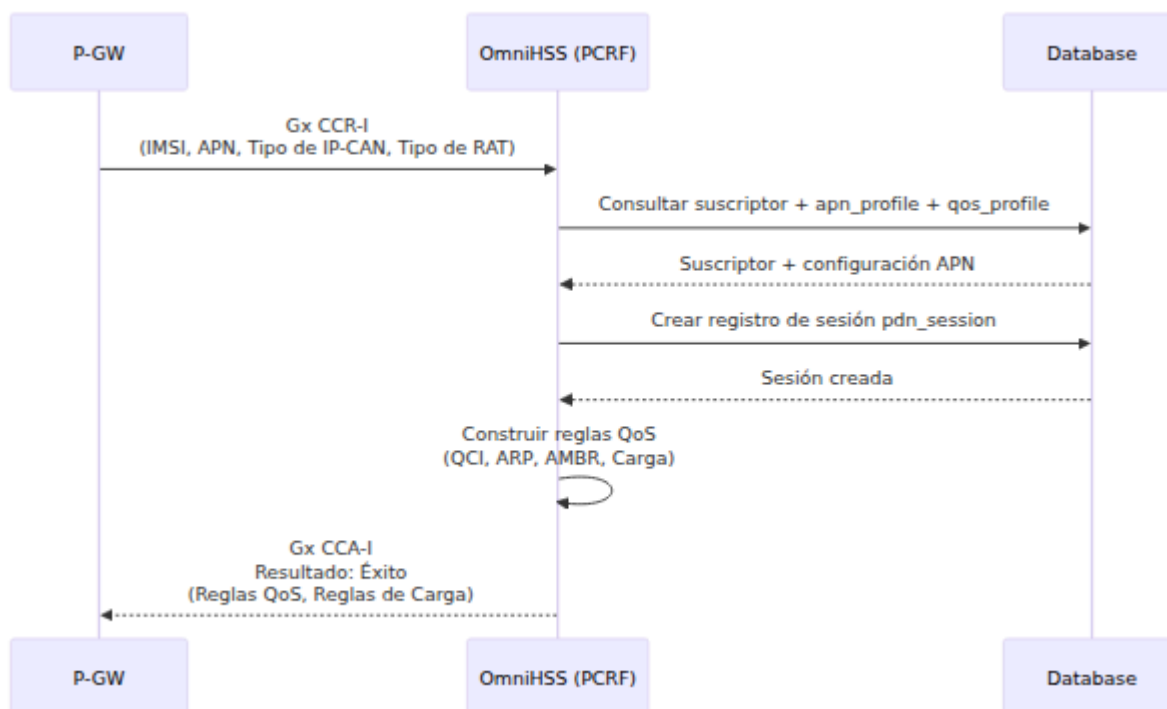
AVPs Clave:

- 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 la autenticación EAP exitosa.

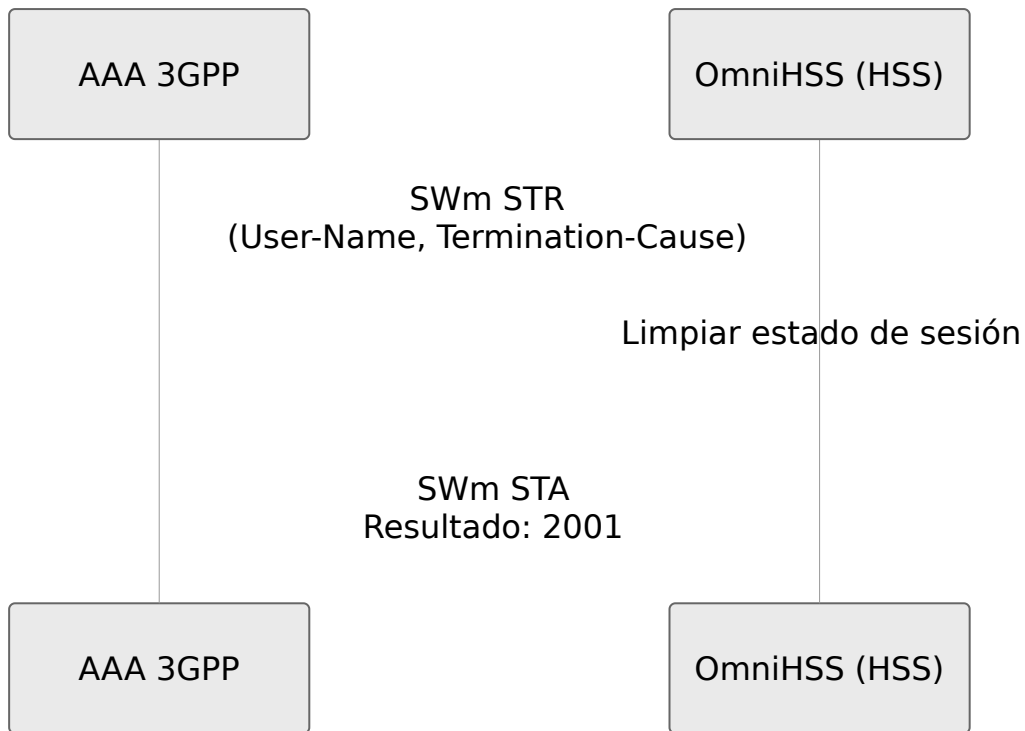


AVPs Clave:

- 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 espera de autenticación
DIAMETER_USER_MOVED	7	Usuario movido a otro acceso
DIAMETER_SESSION_TIMEOUT	8	Tiempo de espera de sesión

Solución de Problemas de Problemas de Protocolo

Fallos de Autenticación (S6a AIR)

Verificar:

1. Conjunto de claves configurado correctamente (Ki, OPC, AMF)
2. Sincronización de SQN (si hay fallos repetidos)
3. Reglas de roaming permiten la red visitada

Fallos de Actualización de Ubicación (S6a ULR)

Verificar:

1. El perfil EPC existe y tiene APNs configurados
2. Roaming permitido para servicios de datos
3. Formato de identidad MME correcto

Fallos de Registro IMS (Cx SAR)

Verificar:

1. Perfil IMS asignado al suscriptor
2. Plantilla IFC XML válida
3. Selección de S-CSCF configurada
4. MSISDNs asignados si se utilizan en la plantilla

Fallos de Conexión PDN (Gx CCR-I)

Verificar:

1. APN existe en la lista de APN del perfil EPC
2. Perfil QoS de APN configurado
3. Tabla de sesiones PDN no está llena (si existen límites)

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

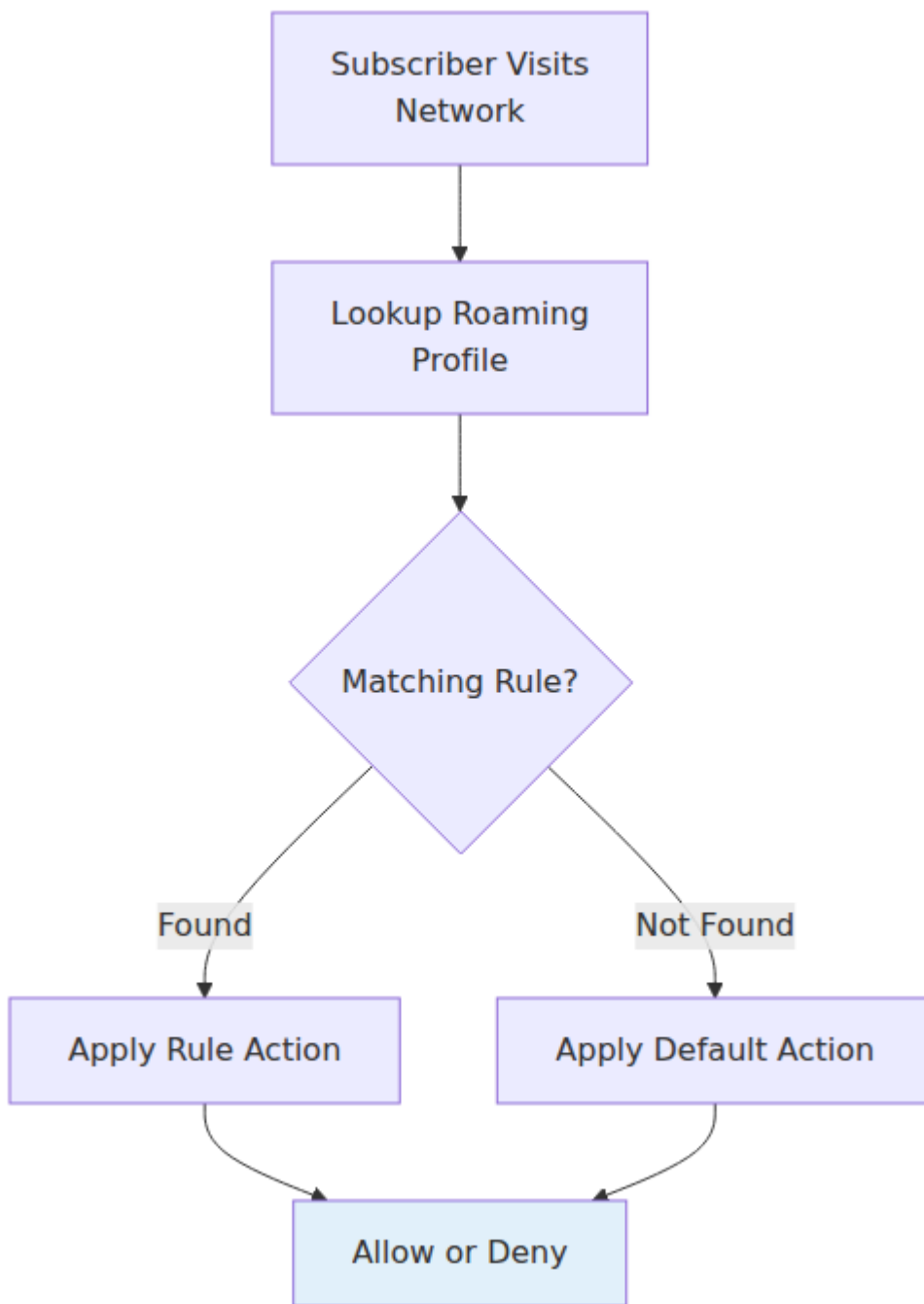
Control de Roaming de OmniHSS

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

Visión General

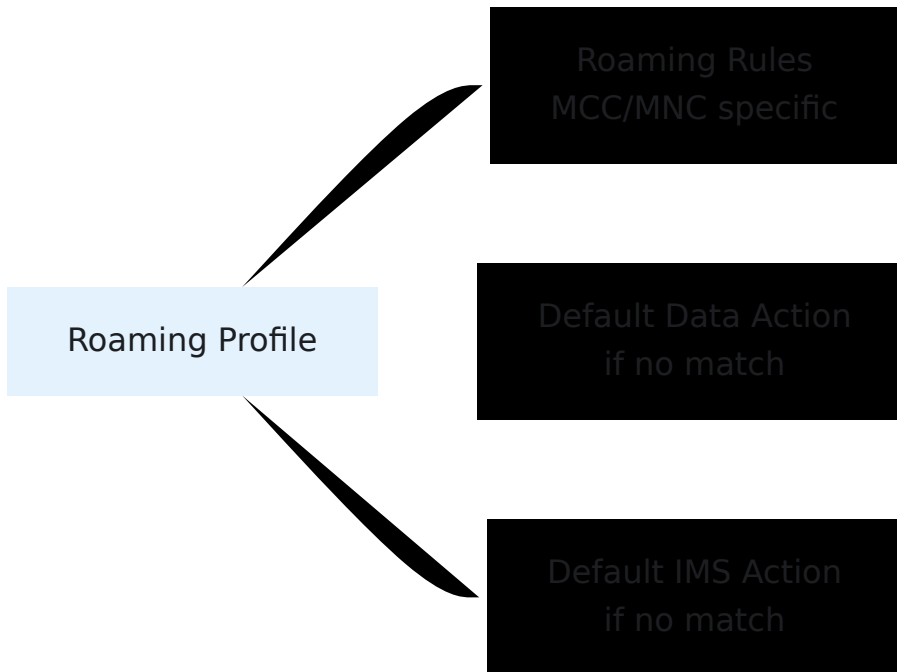
OmniHSS proporciona un control de roaming granular, permitiéndole definir qué redes pueden acceder los suscriptores tanto para servicios de datos como de IMS cuando están en roaming.

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)

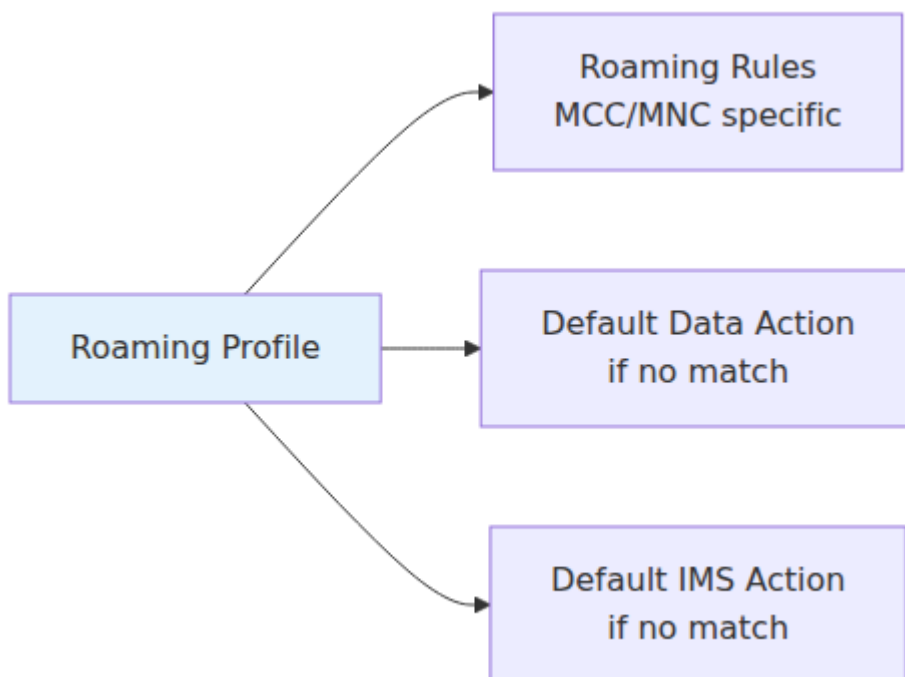
```
# Crear regla de bloqueo de red costosa
RULE=$(curl -k -X POST
https://hss.example.com:8443/api/roaming/rule \
-H "Content-Type: application/json" \
-d '{
  "roaming_rule": {
    "name": "Block Expensive Network",
    "mcc": "206",
    "mnc": "01",
    "data_action": "deny",
    "ims_action": "deny"
  }
}' | 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.

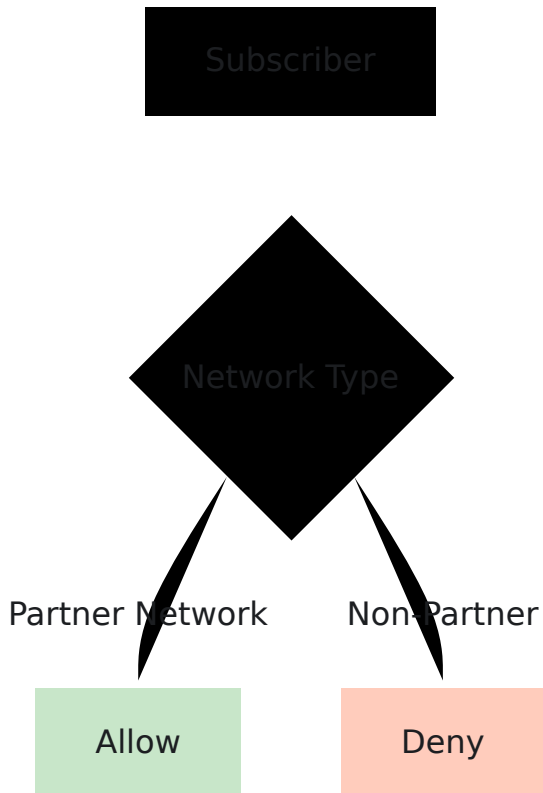


Configuración:

- 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.

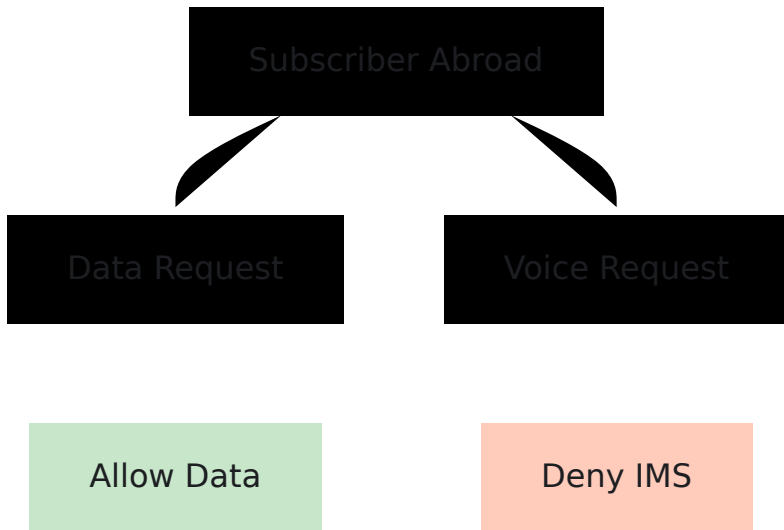


Configuración:

- 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 se realiza típicamente a nivel de MME/red. Las reglas de roaming de OmniHSS se aplican a los 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

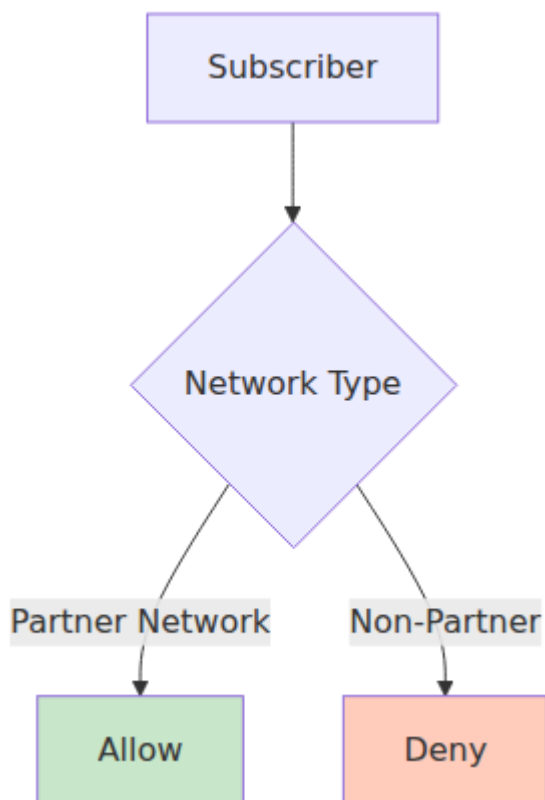
Operadores Comunes de EE. UU. (MCC 310-316)

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 de Roaming

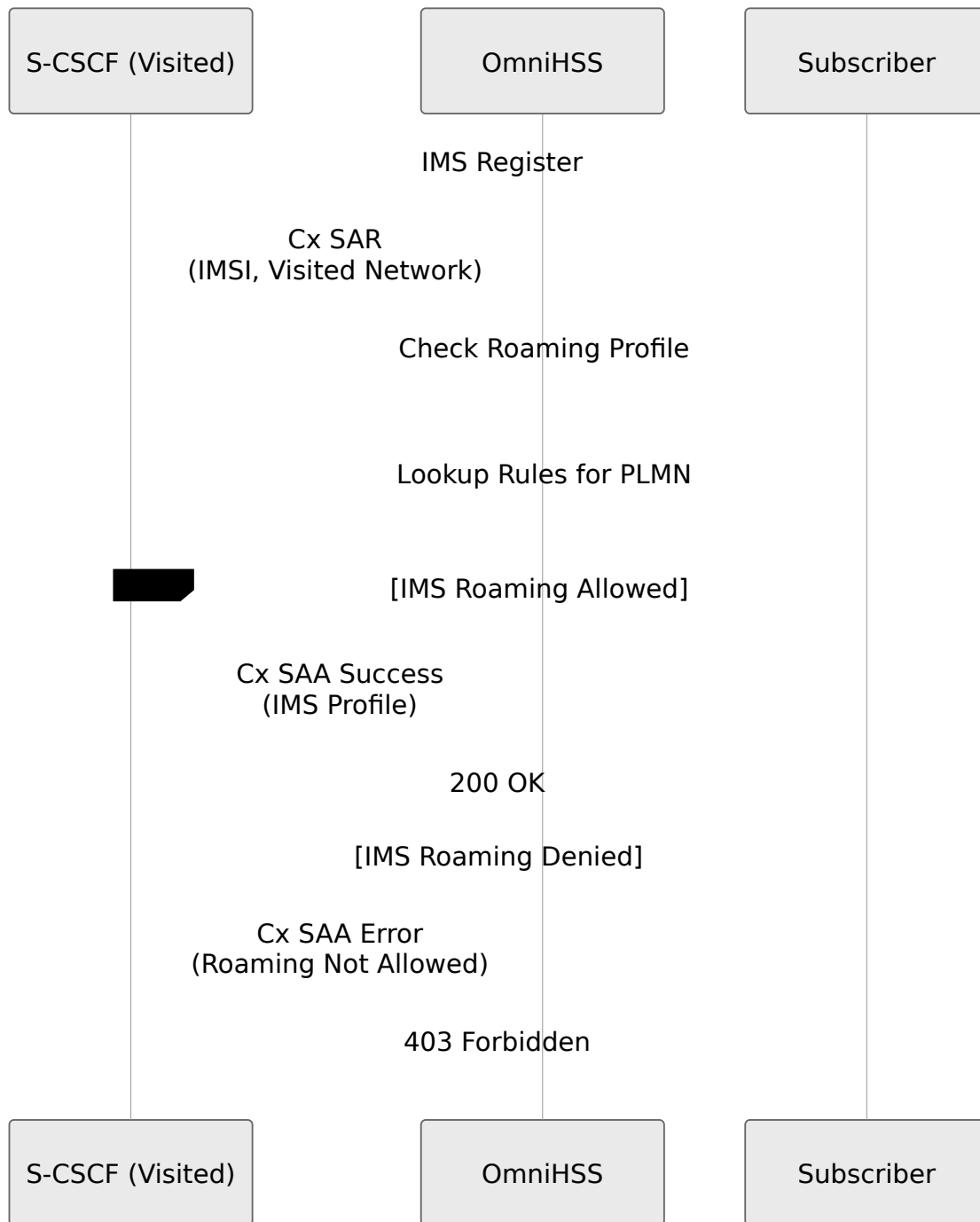
Interfaz S6a (Datos)

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

Verifique la asignación del perfil de roaming:

- Consulte la base de datos para ver el perfil de roaming asignado al suscriptor
- Verifique el nombre del perfil y la configuración de acciones predeterminadas

Verifique si existe una regla para la red visitada:

- Consulte la base de datos para obtener reglas de roaming que coincidan con el MCC/MNC de la red visitada
- Verifique si existe una regla para el perfil de roaming del suscriptor
- Verifique el valor de `data_action` para esa red específica

El Suscriptor Puede Conectarse Pero No Registrar IMS

Verifique la acción de IMS por separado:

- Consulte las reglas de roaming para la red visitada
- Verifique los valores de `data_action` y `ims_action`
- Busque casos donde los datos están permitidos pero IMS está denegado

Comportamiento de Roaming Inesperado

Revise los registros para verificar los controles 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. **Comience restrictivo** - Denegar por defecto, permitir explícitamente a los socios
2. **Pruebe a fondo** - Verifique las reglas en el laboratorio antes de la producción
3. **Documente las reglas** - Mantenga una lista de redes permitidas y por qué
4. **Revise regularmente** - Actualice a medida que cambien los acuerdos de roaming

Gestión de Reglas

1. **Use nombres descriptivos** - "Allow-ATT-Data-Only" no "Rule1"
2. **Verifique MCC/MNC** - Verifique los códigos contra bases de datos oficiales
3. **Considere ambos servicios** - Piense en datos e IMS por separado
4. **Monitoree el uso** - Realice un seguimiento de qué redes visitan realmente los suscriptores

Procedimientos Operativos

1. **Cambios de Emergencia** - Tener un procedimiento para habilitar/deshabilitar rápidamente el roaming
2. **Actualizaciones Masivas** - Planifique la actualización de los perfiles de roaming de múltiples suscriptores
3. **Informes** - Realice un seguimiento del uso de roaming y de los intentos denegados
4. **Comunicación con el Cliente** - Notifique a los clientes sobre cambios en la política de roaming

Guía de Solución de Problemas de OmniHSS

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

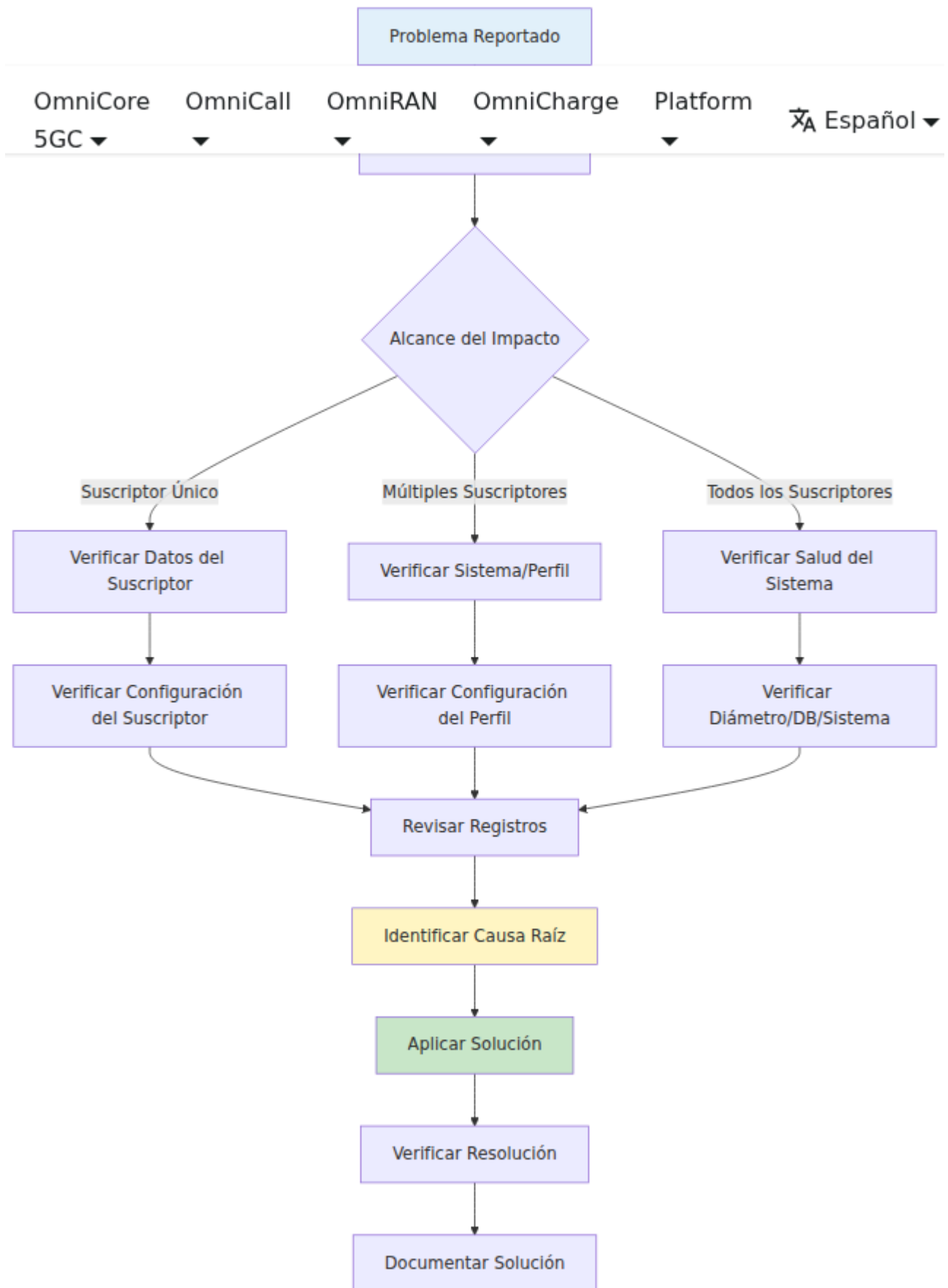
Tabla de Contenidos

- [Descripción General de la Solución de Problemas](#)
 - [Fallos de Autenticación](#)
 - [Problemas de Conectividad de Diámetro](#)
 - [Problemas de Base de Datos](#)
 - [Fallos en el Registro EPC](#)
 - [Fallos en el Registro IMS](#)
 - [Fallos en 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, recopila:

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 múltiples?
- ¿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 la conectividad de la base de datos

Fallos de Autenticación

Síntomas

- El suscriptor no puede conectarse 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 consistente 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 haber funcionado 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 conectar)

Advertencia: Restablecer SQN puede causar problemas de seguridad. Solo hacerlo 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 Faltante

Síntomas:

- La búsqueda del suscriptor tiene éxito, pero la autenticación falla
- Error: "No se asignó perfil EPC"

Pasos de Diagnóstico:

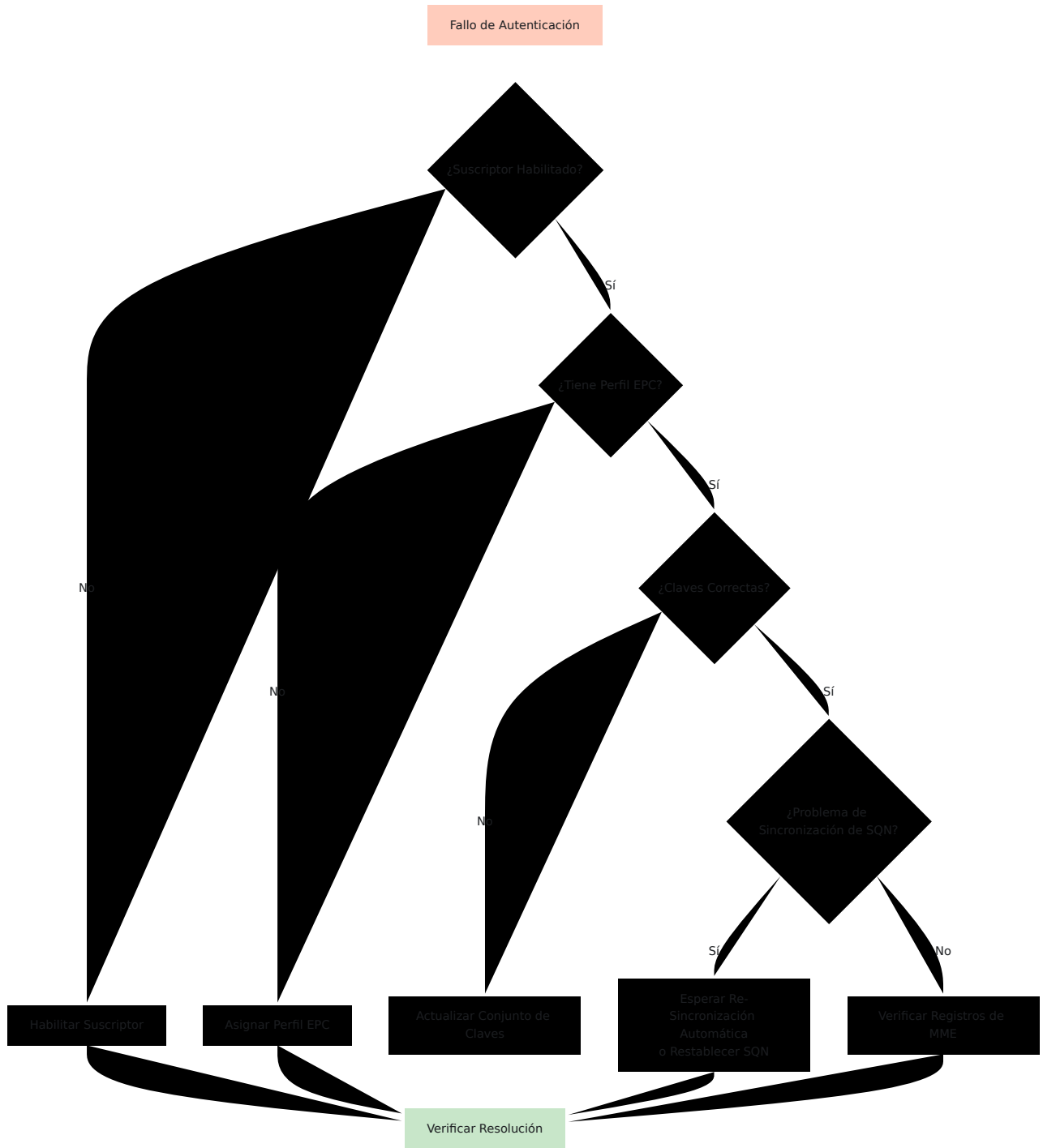
1. Verificar el campo `epc_profile_id` del suscriptor
2. Verificar que el perfil EPC exista:

```
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
- El ping falla al par

Pasos de Diagnóstico:

1. Verificar la 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 el tráfico de Diámetro (puerto 3868)

Solución:

- Corregir el enrutamiento de la red

- Actualizar las reglas del firewall
- Verificar que el par esté funcionando 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 de 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 certificados
- Errores de "Certificado expirado" o "Certificado inválido"

Pasos de Diagnóstico:

1. Verificar que los archivos de certificados 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 en el 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:

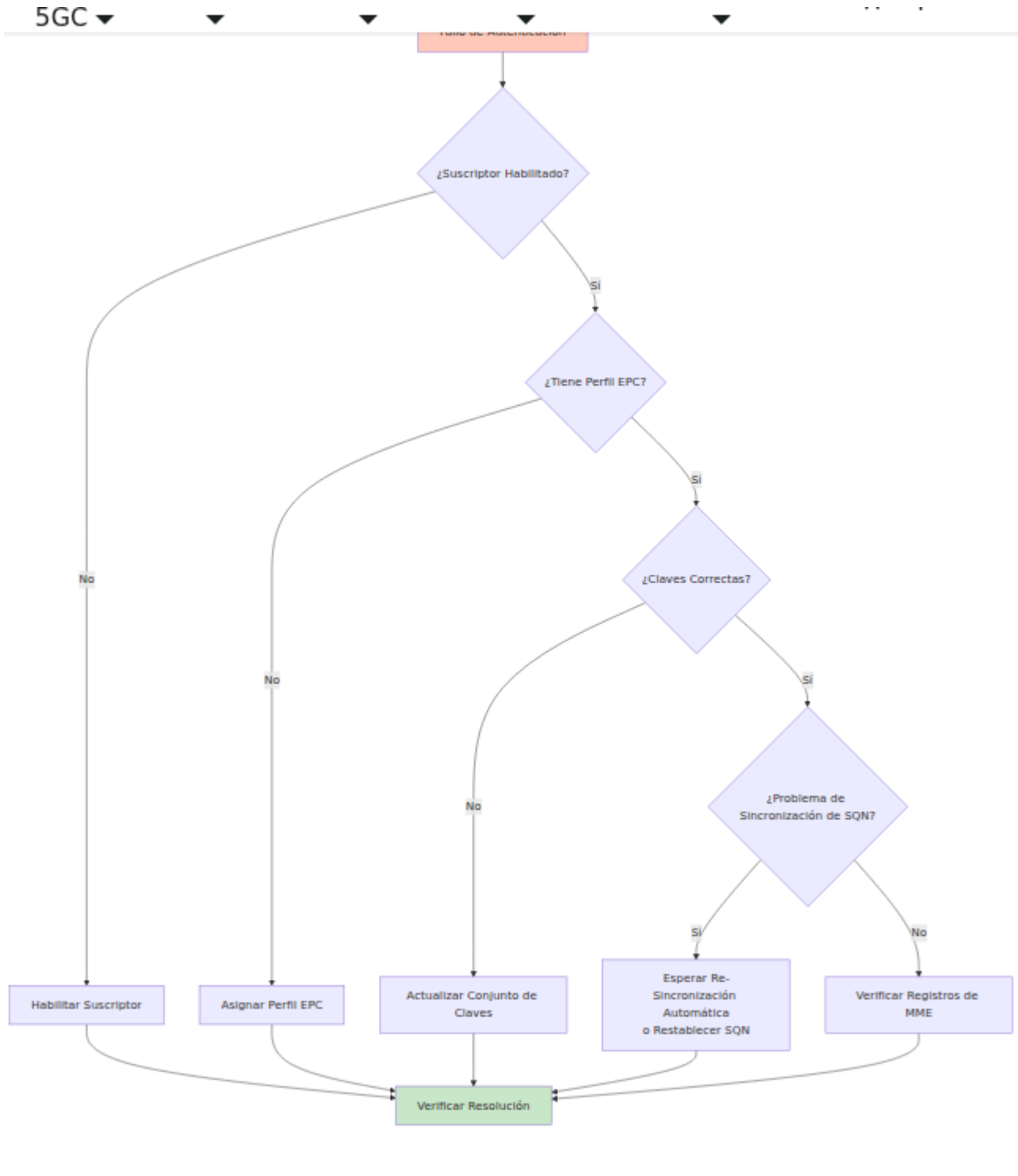
1. Verificar la [página de Diámetro del Panel de Control](#) para las aplicaciones del par
2. Verificar que el par soporte la aplicación requerida (S6a, Cx, Sh, etc.)
3. Revisar el intercambio CER/CEA en los registros

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 "Fallo de conexión a la base de datos"
- Rendimiento de consulta lento

Causas Comunes y Soluciones

Causa 1: Servidor de Base de Datos Apagado

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:

```
# Si se usa PostgreSQL
psql -h [DB_HOST] -U [DB_USER] -d [DB_NAME]

# Si se usa MySQL
mysql -h [DB_HOST] -u [DB_USER] -p [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 en el 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 inicio

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
- Conceder 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 "No hay conexiones disponibles"
- Los 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 conexión 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 la API muy lentas
- Tiempo de espera en búsquedas de suscriptores
- Alta CPU en la base de datos

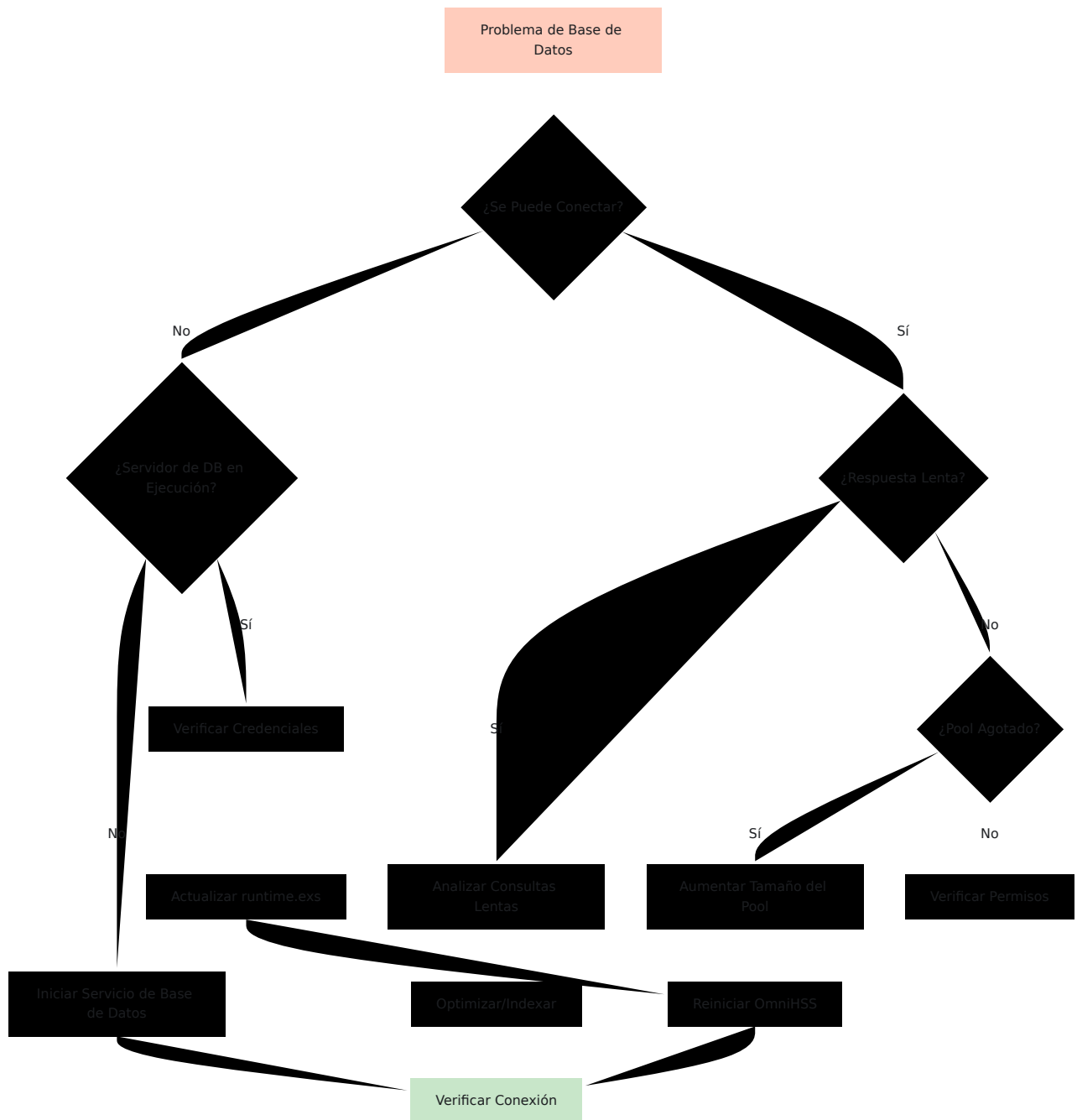
Pasos de Diagnóstico:

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 en el Registro EPC

Síntomas

- El suscriptor no puede conectarse a la red LTE

- MME rechaza la conexión
- 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. Comprobar 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 conexión 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 del 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 conectarse
- Sin comunicación con el MME
- Par de Diámetro apagado

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 conectado pero no puede volver a conectarse
- El estado no coincide con la realidad
- La desconexión y reconexión falla

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

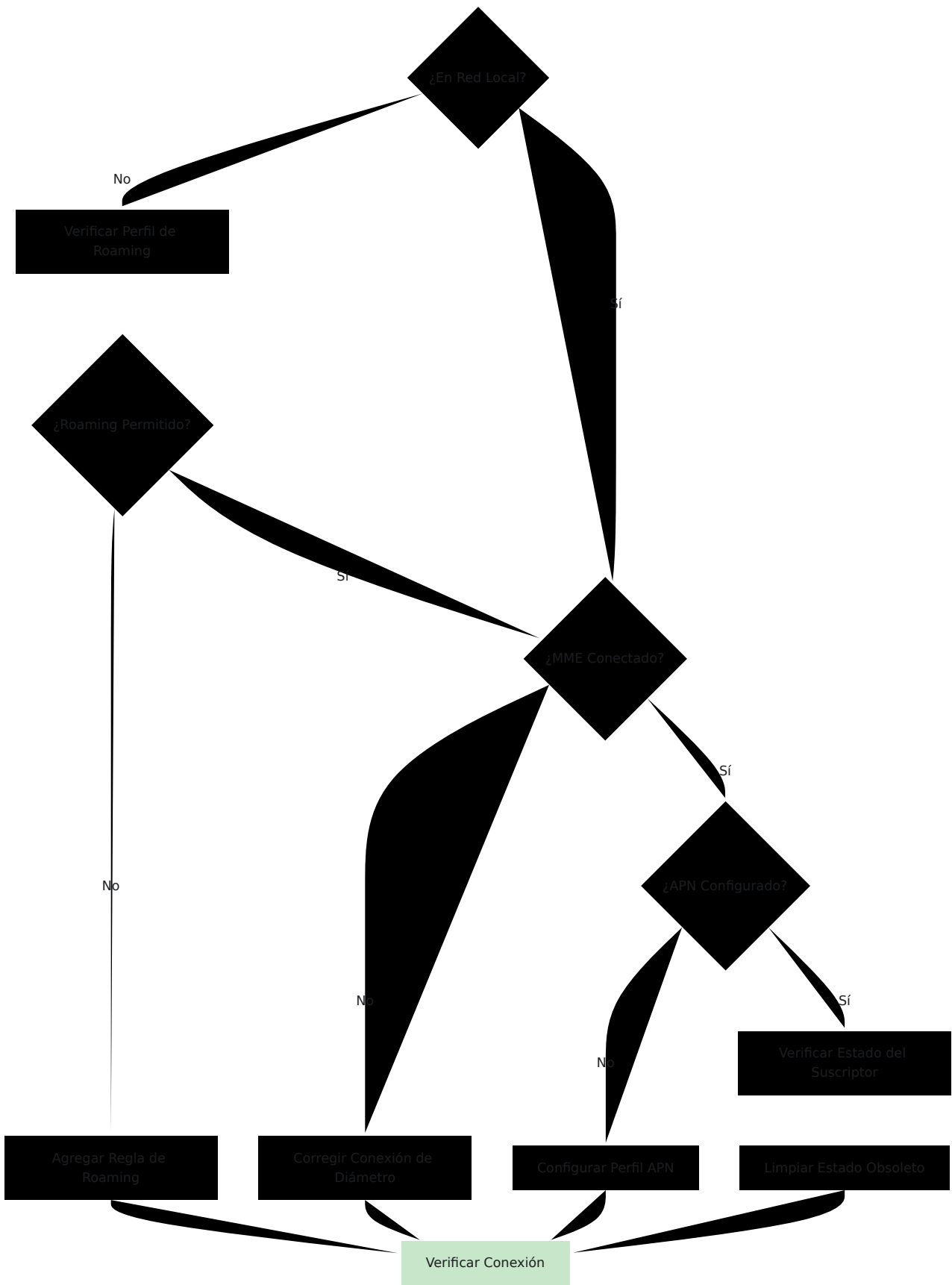
Solución:

- Limpiar el estado del suscriptor (procedimiento de desconexión)
- 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

Fallo en el Registro EPC



Fallos en el Registro IMS

Síntomas

- El suscriptor no puede registrarse para VoLTE
- "Fallo en el 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
- Sin 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 [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
- 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 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 en 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 [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

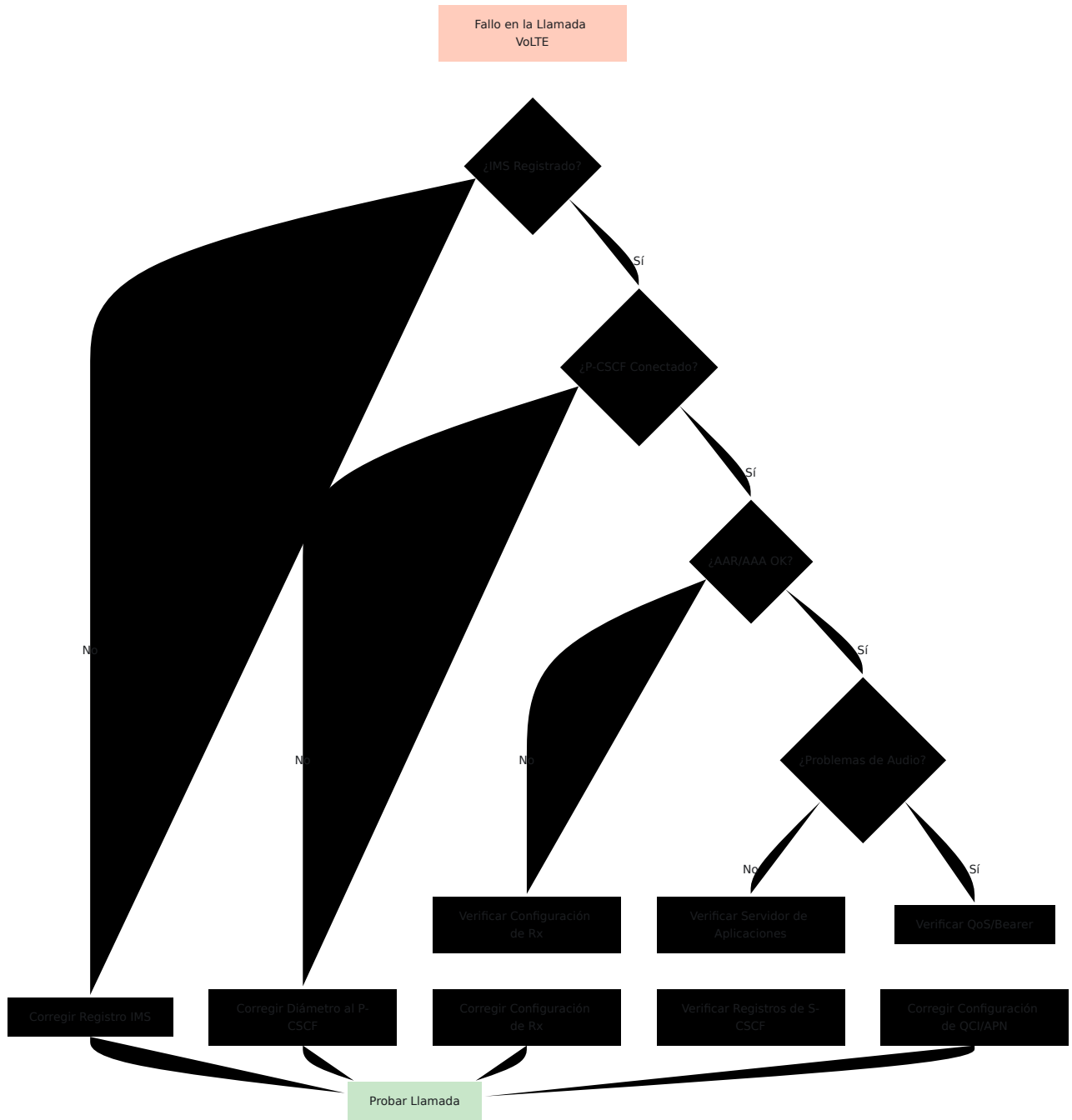
Pasos de Diagnóstico:

1. Verificar el perfil de QoS del APN de voz
2. Verificar que el 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 de IMS
- Asegurarse de que QCI 1 esté configurado para el bearer de voz
- Corregir **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
- Roaming de datos funciona pero no voz (o viceversa)

Causas Comunes y Soluciones

Causa 1: No se Asignó Perfil de Roaming

Síntomas:

- El roaming falla para el suscriptor
- Otros suscriptores hacen roaming con éxito

Pasos de Diagnóstico:

1. Consultar el campo `roaming_profile_id` del suscriptor
2. Verificar si el campo es nulo

Solución:

- Asignar un **perfil de roaming** al suscriptor

Causa 2: Roaming Denegado por Política

Síntomas:

- El roaming falla consistentemente en una red específica
- El error indica rechazo por política

Pasos de Diagnóstico:

1. Identificar el MCC/MNC de la red visitada desde el dispositivo del suscriptor o el MME
2. Consultar el perfil de roaming del suscriptor

3. Verificar las reglas de roaming para el MCC/MNC coincidente
4. Verificar la acción predeterminada del perfil

Solución:

- Agregar una **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": "Permitir Red Visitada",
    "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 de servicio dividida

Pasos de Diagnóstico:

1. Consultar las reglas de roaming para la red visitada
2. Verificar los valores de `data_action` frente a `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"`

Ver [Documentación de Roaming](#) para la configuración detallada.

Problemas de EIR

Síntomas

- Dispositivos bloqueados inesperadamente
- Dispositivos robados no bloqueados
- Fallo en la verificación de EIR

Causas Comunes y Soluciones

Causa 1: Regex IMEI Incorrecto

Síntomas:

- Dispositivos incorrectos bloqueados/permitidos
- La regla coincide incorrectamente

Pasos de Diagnóstico:

1. Consultar las 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 la **regla de EIR** con el regex correcto
- Probar el regex a fondo antes de aplicarlo
- Considerar el orden de las reglas (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 de Diámetro 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 de Diámetro 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 catch-all
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 catch-all
-

Problemas de Rendimiento

Síntomas

- Respuestas lentas de la API
- Tiempos de espera en solicitudes de Diámetro
- Alta utilización de CPU o memoria
- Panel de Control lento para cargar

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 Conteo 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 conteo 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 conjuntos de datos grandes
- Considerar la paginación para resultados grandes
- Implementar caché si es necesario

Causa 3: Problemas con el Par de Diámetro

Síntomas:

- Operaciones de Diámetro lentas
- Tiempos de espera en un par específico
- Algunos pares rápidos, otros lentos

Pasos de Diagnóstico:

1. Verificar la [página de Diámetro del Panel de Control](#)
2. Identificar el par lento
3. Probar la latencia de red al par
4. Verificar el uso de recursos del par

Solución:

- Investigar problemas de rendimiento del par
- Verificar el camino de red en busca de congestión
- Considerar agregar pares redundantes

- Aumentar el tiempo de espera de Diámetro si es necesario

Causa 4: Problemas de Memoria

Síntomas:

- Alta utilización de memoria de OmniHSS
- 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 fugas 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 alta
-

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 desconectar al suscriptor

Causas Comunes y Soluciones

Causa 1: Caída/Reinicio del MME

Síntomas:

- El suscriptor muestra un MME que ya no está sirviendo
- 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 que sirve
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 reiniciar

Causa 2: Desconexión de Red No Recibida

Síntomas:

- El suscriptor apagado pero aparece como conectado
- Las sesiones PDN permanecen en la base de datos
- La ubicación no se limpia

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 estados muy obsoletos

Causa 3: Corrupción de Base de Datos

Síntomas:

- Estado inconsistente en las 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 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 todos los campos requeridos estén incluidos
- 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 no existe"
- 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 trabajo 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. Resumen del Sistema

- URL: `https://[hostname]:7443/overview`
- Comprobar: Conteos de suscriptores, sesiones activas, estado del sistema

2. Estado de Diámetro

- URL: `https://[hostname]:7443/diameter`
- Comprobar: Todos los pares críticos conectados

3. Salud de la Aplicación

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

- Comprobar: Uso de memoria, conteo de procesos, tiempo de actividad

Comandos de Diagnóstico de API

Verificar 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/1
```

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/1

# Perfil IMS
curl -k https://hss.example.com:8443/api/ims/profile/1

# Perfil de Roaming
curl -k https://hss.example.com:8443/api/roaming/profile/1
```

Comandos de Diagnóstico de Red

Probar Conectividad del Puerto de Diámetro:

```
telnet [PEER_IP] 3868
```

Verificar Certificado TLS:

```
openssl s_client -connect [hostname]:8443 -showcerts
```

Probar Conectividad de la Base de Datos:

```
# PostgreSQL  
psql -h [DB_HOST] -U [DB_USER] -d [DB_NAME] -c "SELECT COUNT(*)  
FROM subscriber;"
```

```
# MySQL  
mysql -h [DB_HOST] -u [DB_USER] -p -e "SELECT COUNT(*) FROM  
subscriber;" [DB_NAME]
```

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 de Diámetro:

```
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. **Fallas en todo el sistema** que no se pueden resolver con procedimientos documentados
2. **Corrupción de datos** o estado de base de datos inconsistente
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 realizados** - Qué solución de problemas ya has hecho
3. **Registros** - Fragmentos de registro relevantes que muestran el problema
4. **Configuración** - Porciones relevantes de runtime.exs (redactar datos sensibles)
5. **Entorno** - Versión de OmniHSS, versión de la base de datos, versión del SO
6. **Impacto** - Cuántos suscriptores 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
"Fallo en la generación de vectores de autenticación"	Conjunto de claves faltante o inválido	Verificar configuración de conjunto de claves
"Fallo de sincronización de SQN"	SQN fuera de sincronización	Esperar re-sincronización
"Suscriptor no encontrado"	IMSI inválido	Verificar IMSI, aprovisionar suscriptor
"Suscriptor deshabilitado"	enabled=false	Habilitar suscriptor

Errores de Diámetro

Mensaje de Error	Causa	Solución
"Tiempo de espera de conexión del par de Diámetro"	Problema de red	Verificar conectividad de red
"Fallo en el intercambio CER/CEA"	Desajuste de configuración	Verificar configuración de Diámetro
"Aplicación no soportada"	El par no soporta la aplicación requerida	Verificar aplicaciones del par
"Fallo en el apretón de manos TLS"	Problema de certificado	Verificar certificados

Errores de Base de Datos

Mensaje de Error	Causa	Solución
"Conexión rechazada"	Base de datos apagada	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 no existe"	Clave foránea inválida	Crear conjunto de claves primero
"IMSI ya ha sido tomado"	IMSI duplicado	Usar un IMSI diferente o eliminar el existente
"Error de validación"	Entrada inválida	Verificar formato y requisitos del campo

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

Integración de Webhook de OmniHSS

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

Tabla de Contenidos

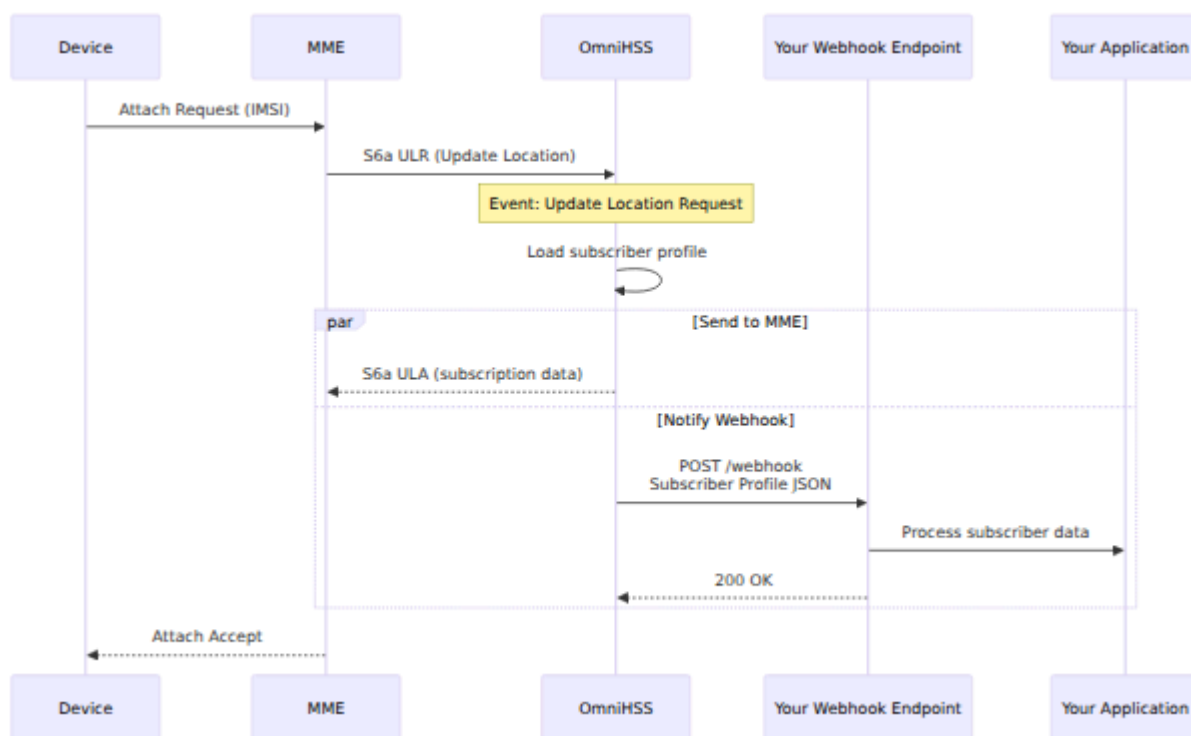
- [Descripción General](#)
 - [Cómo Funcionan los Webhooks](#)
 - [Eventos de Webhook](#)
 - [Carga Útil del Webhook](#)
 - [Configuración](#)
 - [Casos de Uso](#)
 - [Consideraciones de Seguridad](#)
 - [Solución de Problemas](#)
-

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 basado en eventos de red
- **Reducción de consultas** - No es necesario consultar continuamente la API para 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 confirmar 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 desregulación 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": 1234,
    "imsi": "001001123456789",
    "enabled": true,
    "ims_enabled": true,
    "msisdns": [
      {"id": 1, "msisdn": "14155551001"},
      {"id": 2, "msisdn": "14155551002"}
    ],
    "sim": {
      "id": 5678,
      "iccid": "8991101200003204510",
      "is_esim": false
    },
    "key_set": {
      "id": 100,
      "amf": "8000"
    },
    "epc_profile": {
      "id": 1,
      "name": "Premium 100Mbps",
      "ue_ambr_dl_kbps": 100000,
      "ue_ambr_ul_kbps": 50000
    },
    "ims_profile": {
      "id": 1,
      "name": "Standard VoLTE"
    },
    "roaming_profile": {
      "id": 1,
      "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 contextuales 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": 5678,
  "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": 1,
    "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/1 \  
-H "Content-Type: application/json" \  
-d '{  
  "webhook": {  
    "enabled": false  
  }  
'
```

Eliminar Webhook

```
curl -k -X DELETE https://hss.example.com:8443/api/webhook/1
```

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** - Para seguridad, utiliza 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 confirmar la recepción
  res.status(200).json({ received: true });

  // Manejar procesamiento asíncrono después de la respuesta
  processWebhook(req.body).catch(console.error);
});

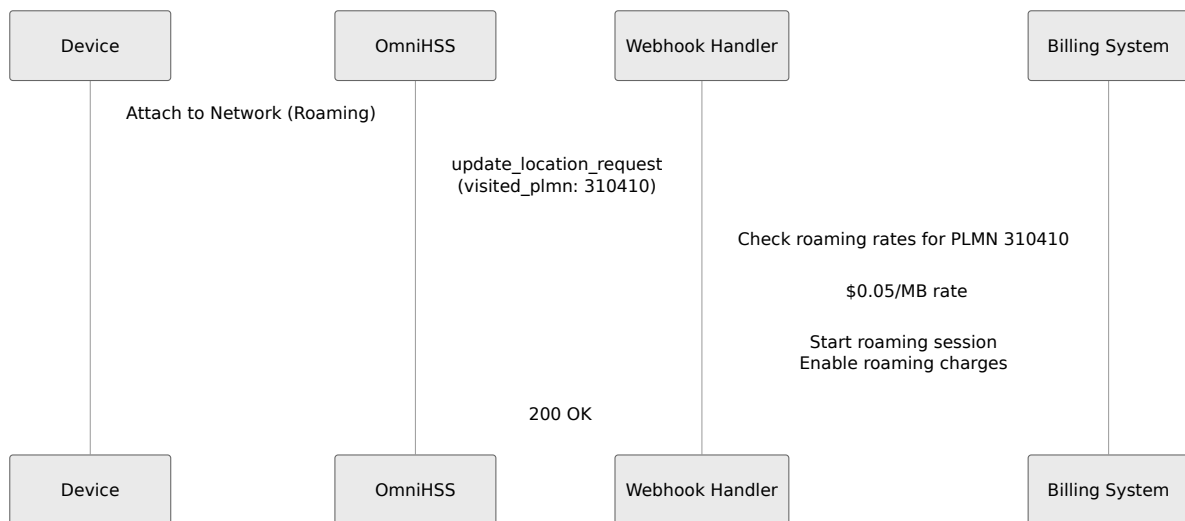
async function processWebhook(payload) {
  // Tu lógica de procesamiento asíncrono
  // por ejemplo, actualizar el sistema de facturación, activar
  análisis, etc.
}

app.listen(3000);
```

Casos de Uso

1. Facturación en Tiempo Real y Seguimiento de Uso

Rastrear el uso de la red 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 de suscriptores 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
    });
  }

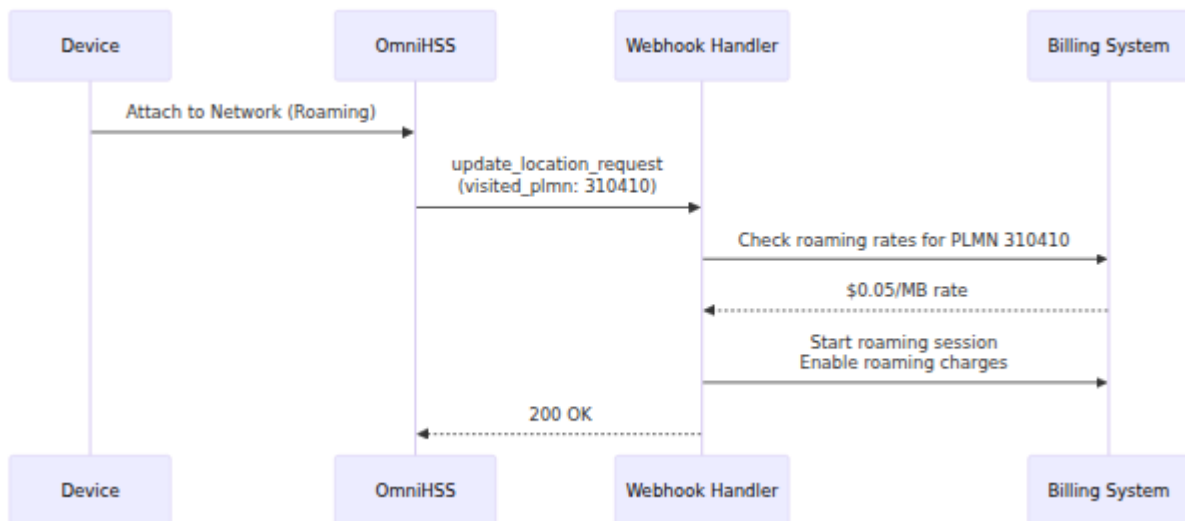
  res.status(200).send();
});
```

Panel de Control de Análisis:

- Suscriptores activos por MME
- Suscriptores en roaming por país
- Distribución de niveles de servicio
- Tasas 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 viaje imposible
        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 automáticamente IMS cuando el suscriptor usa 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']
    });
  }

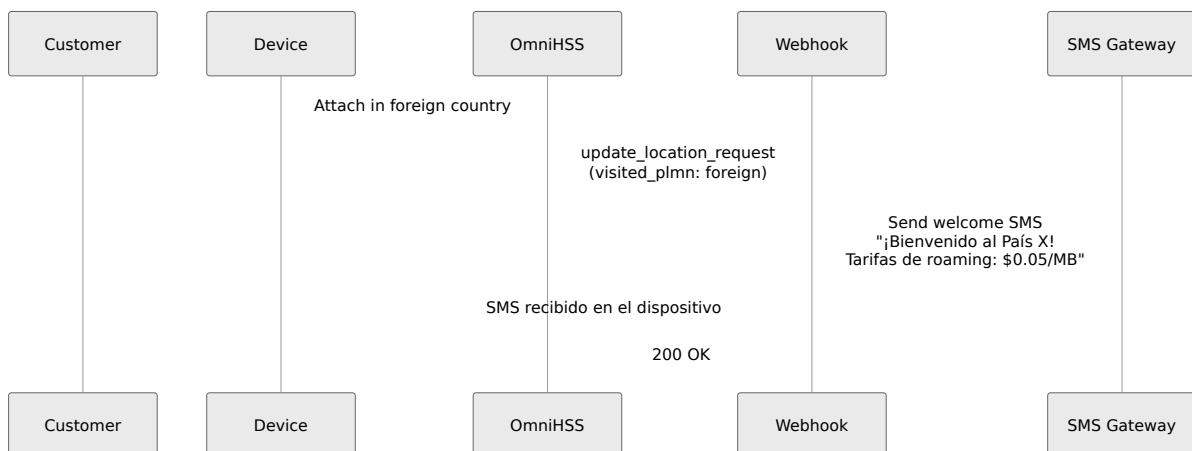
  res.status(200).send();
});

```

5. Notificaciones a Clientes

Enviar notificaciones en tiempo real a los clientes sobre su servicio.

Caso de Uso: Mensaje de bienvenida cuando viajan internacionalmente



Ejemplos 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 de 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

Verificar 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** - Verificar las firmas de los webhooks para prevenir suplantaciones
3. **Limitación de tasa** - Implementar limitación de tasa en los endpoints de webhook

4. **Lista blanca de IP** - Restringir el acceso al webhook a direcciones IP de OmniHSS
5. **Monitorear fallos** - Rastrear fallos y errores en la entrega de webhooks
6. **Sanitizar datos** - Validar y sanitizar las cargas útiles de los webhooks antes de procesarlas
7. **Proteger credenciales** - Almacenar secretos de webhook en configuraciones seguras (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 del webhook
- **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 de `ims_registration`, verifica que esté en la matriz de eventos

3. Revisar los registros de HSS:

- Comprobar errores de entrega de webhook
- Buscar problemas de conectividad de red
- Verificar que no haya fallos de resolución 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 de webhook recibe la solicitud pero HSS la marca como fallida

Solución:

1. Responder inmediatamente:

- Devolver HTTP 200 dentro de 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 asíncronamente
});
```

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 usando `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** - Falló la verificación de la firma

- 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 completo:

```
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
});
  }
});
```

Datos del Suscriptor Faltantes

Síntomas:

- Webhook recibido pero el objeto del suscriptor está incompleto
- Campos esperados son nulos o faltantes

Causas Posibles:

1. **Suscriptor no completamente provisionado** - Algunos perfiles pueden ser opcionales (IMS, roaming)
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 Roaming' };

// Manejar MSISDNs faltantes
const msisdns = subscriber.msisdns || [];
```

Monitoreo y Observabilidad

Métricas de Webhook

Rastrear el rendimiento y la confiabilidad de los webhooks:

Métricas a Monitorear:

- Tasa de entrega de webhooks (exitosos vs. fallidos)
- Latencia de webhook (tiempo desde el evento hasta la respuesta del endpoint)
- Tiempos de respuesta del endpoint
- Tasas de error por endpoint
- Eventos por segundo

Consulta de Ejemplo para el Panel (Prometheus/Grafana):

```
# Tasa de éxito de webhook
rate(omnihss_webhook_success_total[5m]) /
rate(omnihss_webhook_attempts_total[5m])

# Latencia de webhook
histogram_quantile(0.95, omnihss_webhook_duration_seconds)
```

Registros de Webhook

Habilitar registros detallados de webhook para solución de problemas:

Formato de Registro:

```
{
  "timestamp": "2025-01-15T14:30:00Z",
  "level": "info",
  "component": "webhook",
  "event_id": "550e8400-e29b-41d4-a716-446655440000",
  "webhook_id": 1,
  "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](#) →