Referencia de Configuración de OmniSEPP

Descripción general | Guía de Operaciones | Métricas y Monitoreo | Solución de Problemas

Toda la configuración de OmniSEPP se encuentra bajo la clave de aplicación `:omnisepp`. Un subconjunto de claves puede ser sobrescrito por variables de entorno, pero eso solo tiene efecto en la **configuración de tiempo de ejecución de producción**. Los mapas anidados (`roaming_partners`, `topology_hiding_map`) y un pequeño número de otras claves no tienen variable de entorno y se establecen únicamente a través del archivo de configuración de la aplicación.

Estructura de Configuración

```
config :omnisepp,
  # Identidad del oyente SBI/N32 (anunciada al NRF)
  sbi_scheme: "http",
  sbi_addr: "127.0.0.22",
  sbi_port: 7777,

  # Material TLS para el oyente N32 (utilizado solo cuando
sbi_scheme es "https")
  sbi_certfile: nil,
  sbi_keyfile: nil,
  sbi_cacertfile: nil,

  # Registro NRF
  nrf_uri: "http://127.0.0.10:7777",
  heartbeat_interval: 10_000,

  # PLMN servido (sobrescribir por implementación)
  mcc: "999",
  mnc: "70",

  # Identidad propia de este SEPP y capacidades negociadas
  sepp_fqdn: "sepp.5gc.mnc70.mcc999.3gppnetwork.org",
  supported_sec_capabilities: ["TLS"],

  # Persistencia del contexto de asociación N32 (solo archivo de
configuración)
  n32_context_path: "<priv>/data/n32_context.dets",

  # Roaming y ocultación de topología (solo archivo de
configuración)
  roaming_partners: %{},
  topology_hiding_map: %{}
```

Cada parámetro anterior se documenta a continuación.

Parámetros Principales

Parámetro	Tipo	Requerido	Predeterminad
`sbi_scheme`	String	No	`http`
`sbi_addr`	String	No	`127.0.0.22`
`sbi_port`	Integer	No	`7777`
`sbi_certfile`	String (ruta)	Condicional	(ninguno)

Parámetro	Tipo	Requerido	Predeterminad
`sbi_keyfile`	String (ruta)	Condicional	(ninguno)
`sbi_cacertfile`	String (ruta)	No	(ninguno)
`nrf_uri`	String	No	`http://127.0.0.10`
`mcc`	String	No	`999`

Parámetro	Tipo	Requerido	Predeterminad
`mnc`	String	No	`70`
`heartbeat_interval`	Integer (ms)	No	`10000`
`sepp_fqdn`	String	No	derivado (ver más a
`supported_sec_capabilities`	Lista de String	No	`["TLS"]`

Parámetro	Tipo	Requerido	Predeterminad
`n32_context_path`	String (ruta)	No	derivado (ver más a
`roaming_partners`	Mapa	No	`%{}`
`topology_hiding_map`	Mapa	No	`%{}`

Parámetro	Tipo	Requerido	Predeterminad

sepp_fqdn

Cuando `sepp_fqdn` no está establecido, se deriva del PLMN servido como:

```
sepp.5gc.mnc<mnc>.mcc<mcc>.3gppnetwork.org
```

Para el PLMN predeterminado `999-70`, esto produce `sepp.5gc.mnc70.mcc999.3gppnetwork.org`. Este FQDN se envía como la identidad `sender` en las solicitudes y respuestas de apretón de manos N32-c (TS 29.573). Sobrescríbalo explícitamente cuando la forma derivada no coincida con el FQDN que sus socios de roaming esperan.

TLS del Oyente N32

Cuando `sbi_scheme` es `https`, el oyente N32 termina TLS por sí mismo en lugar de depender de un terminador externo. Este es el modo TLS N32-f (TS 33.501 §13.1), en el que dos SEPPs protegen la interfaz con TLS entre ellos.

- `sbi_certfile` y `sbi_keyfile` son **ambos requeridos** cuando `sbi_scheme` es `https`. Si alguno falta, el SEPP se niega a iniciar en lugar de degradar silenciosamente a texto plano.
- Cuando `sbi_cacertfile` también está establecido, el oyente requiere y verifica el certificado del cliente del SEPP par contra esa CA, proporcionando TLS mutuamente autenticado. Sin una CA configurada, solo se termina TLS del lado del servidor.
- Cuando `sbi_scheme` es `http` (el predeterminado), estas claves se ignoran y el oyente sirve texto plano.

El esquema anunciado en el registro NRF sigue `sbi_scheme`, por lo que ahora refleja el transporte real del oyente.

capacidades_sec_soportadas

Las capacidades de seguridad N32-f que este SEPP soporta, en **orden de preferencia local** (más preferido primero). Durante el apretón de manos N32-c, OmniSEPP selecciona la primera entrada en esta lista que el par también ofrece (TS 29.573 §5.2.3.2.2).

Valor	Significado	Referencia
`TLS`	Protección a nivel de transporte entre SEPPs.	TS 33.501 §13.1
`PRINS`	Protección con Inserción de Seguridad Intermedia (protección a nivel de aplicación JOSE a través de un hub de roaming).	TS 33.501 §13.2

Solo se reconocen estos dos valores; cualquier otra entrada se ignora. El predeterminado es `["TLS"]`; manténgalo en `["TLS"]` para una operación interoperable.

Al sobrescribir a través de la variable de entorno `SEPP_SEC_CAPABILITIES`, proporcione una lista separada por comas en orden de preferencia, por ejemplo `TLS,PRINS`. Se recorta el espacio en blanco alrededor de cada entrada.

Persistencia del Contexto N32

Las asociaciones N32 establecidas se persisten en un archivo DETS en `n32_context_path`, de modo que sobrevivan a un reinicio de proceso o nodo (TS 29.573). Al iniciar, el almacenamiento recarga las asociaciones persistidas, por lo que un socio no tiene que volver a ejecutar el apretón de manos N32-c después de un reinicio de OmniSEPP.

- Cuando no está establecido, la ruta predeterminada es `n32_context.dets` bajo el directorio de datos `priv` de la aplicación OTP. El directorio padre se crea al iniciar si no existe.
- Si no se puede abrir el archivo (por ejemplo, por corrupción), el almacenamiento registra una advertencia y comienza con una tabla en

memoria vacía en lugar de fallar en el arranque; las asociaciones se restablecen mediante apretón de manos.
- Esta clave no tiene variable de entorno y se establece únicamente a través del archivo de configuración de la aplicación.

Socios de Roaming

El mapa `roaming_partners` es la lista estática de socios de roaming PLMNs. Se indexa por el identificador del PLMN socio en forma de `"mcc-mnc"`, y cada valor es una especificación de socio.

```
config :omnisepp,
  roaming_partners: %{
    "001-01" => %{
      sepp_uri: "https://sepp.partner-a.example:7777",
      sec_capabilities: ["TLS"]
    },
    "310-260" => %{
      sepp_uri: "https://sepp.partner-b.example:7777"
    }
  }
```

Estructura de nivel superior:

Forma de clave	Tipo	Descripción
`"mcc-mnc"`	String (clave del mapa)	Identificador del PLMN socio, por ejemplo `"001-01"`.
valor	Mapa	Especificación del socio (ver más abajo).

Especificación del socio:

Parámetro	Tipo	Requerido	Predeterminado
`sepp_uri`	String	Sí	-
`sec_capabilities`	Lista de String	No	hereda `supported_sec_capabilities`

Un mapa `roaming_partners` vacío (el predeterminado) significa que no hay socios de roaming configurados, y el reenvío N32-f rechaza todos los PLMNs desconocidos. Este mapa no tiene variable de entorno y se establece únicamente a través del archivo de configuración de la aplicación.

Mapa de Ocultación de Topología

El `topology_hiding_map` implementa la reescritura de FQDN para la ocultación de topología (TS 33.501 §13.2). Mapea cada FQDN NF interno al FQDN externo presentado a los socios de roaming.

```
config :omnisepp,
  topology_hiding_map: %{
    "amf1.5gc.mnc070.mcc999.3gppnetwork.org" =>
      "sepp.5gc.mnc070.mcc999.3gppnetwork.org",
    "udm1.5gc.mnc070.mcc999.3gppnetwork.org" =>
      "sepp.5gc.mnc070.mcc999.3gppnetwork.org"
  }
```

Forma de clave	Tipo	Descripción
`internal_fqdn`	String (clave del mapa)	El FQDN NF interno que se debe enmascarar, por ejemplo un FQDN de AMF o UDM.
`external_fqdn`	String (valor)	El FQDN externo presentado a los socios en su lugar.

La asignación se aplica hacia afuera (de interno a externo) en los valores de `3gpp-Sbi-Target-apiRoot`, `Location`, y los valores de encabezado producer-id, y se invierte hacia adentro (de externo a interno) para que los apiRoots presentados por el socio se resuelvan de nuevo al verdadero FQDN interno. Un mapa vacío (el predeterminado) significa que no hay reescritura. Este mapa no tiene variable de entorno y se establece únicamente a través del archivo de configuración de la aplicación.

Resumen de Variables de Entorno

Las variables de entorno se aplican solo en la configuración de tiempo de ejecución de producción. Las claves no listadas aquí son solo de archivo de configuración.

Variable de Entorno	Parámetro	Notas
`SEPP_SBI_SCHEME`	`sbi_scheme`	`http` o `https`.
`SEPP_SBI_ADDR`	`sbi_addr`	
`SEPP_SBI_PORT`	`sbi_port`	Analizado como un entero.
`SEPP_SBI_CERTFILE`	`sbi_certfile`	Requerido cuando el esquema es `https`.
`SEPP_SBI_KEYFILE`	`sbi_keyfile`	Requerido cuando el esquema es `https`.
`SEPP_SBI_CACERTFILE`	`sbi_cacertfile`	Establecer para habilitar TLS mutuo N32-f (verificación del certificado del cliente par).
`SEPP_NRF_URI`	`nrf_uri`	
`SEPP_MCC`	`mcc`	
`SEPP_MNC`	`mnc`	
`SEPP_FQDN`	`sepp_fqdn`	Cuando no está establecido, el FQDN se deriva del PLMN.

Variable de Entorno	Parámetro	Notas
`SEPP_SEC_CAPABILITIES`	`supported_sec_capabilities`	Separado por comas, orden de preferencia.

Ejemplo de Configuración

Una sobrescritura realista por implementación para un PLMN local `310-260` con un solo socio de roaming:

```
config :omnisepp,
  sbi_scheme: "https",
  sbi_addr: "10.20.0.5",
  sbi_port: 7777,
  sbi_certfile: "/etc/omnisepp/tls/sepp.crt",
  sbi_keyfile: "/etc/omnisepp/tls/sepp.key",
  sbi_cacertfile: "/etc/omnisepp/tls/partner-ca.crt",
  nrf_uri: "http://10.20.0.1:7777",
  heartbeat_interval: 10_000,
  mcc: "310",
  mnc: "260",
  sepp_fqdn: "sepp.5gc.mnc260.mcc310.3gppnetwork.org",
  supported_sec_capabilities: ["TLS"],
  roaming_partners: %{
    "001-01" => %{
      sepp_uri: "https://sepp.partner-a.example:7777",
      sec_capabilities: ["TLS"]
    }
  },
  topology_hiding_map: %{
    "amf1.5gc.mnc260.mcc310.3gppnetwork.org" =>
      "sepp.5gc.mnc260.mcc310.3gppnetwork.org"
  }
```

Cómo funciona: OmniSEPP se anuncia al NRF en `10.20.0.5:7777` como NFType `SEPP` para PLMN `310-260`, enviando latidos cada 10 segundos. Debido a que `sbi_scheme` es `https`, el oyente N32 termina TLS con `sepp.crt` /

`sepp.key`, y debido a que `sbi_cacertfile` está establecido, requiere y verifica el certificado del cliente del SEPP socio contra `partner-ca.crt` (mutual TLS). Acepta apretón de manos N32-c como `sepp.5gc.mnc260.mcc310.3gppnetwork.org`, negociando TLS como la única capacidad N32-f, y al iniciar inicia el apretón de manos saliente hacia el socio `001-01`. El tráfico N32-f se reenvía solo hacia y desde el PLMN socio `001-01`, y el FQDN interno de AMF está enmascarado detrás del FQDN SEPP hacia ese socio.

Métricas y Monitoreo de OmniSEPP

Resumen | Guía de Operaciones | Referencia de Configuración | Solución de Problemas

Observabilidad

La observabilidad se proporciona a través de **registros de aplicación estructurados** y registro de solicitudes estándar. Los operadores monitorean OmniSEPP a través de sus registros, que capturan el apretón de manos, el reenvío y los eventos de solicitud descritos a continuación.

Qué Observar en los Registros

Los registros de la aplicación son la señal principal para operar OmniSEPP. Las siguientes clases de eventos se registran y valen la pena observar.

Resultados del Apretón de Manos N32-c

Cada negociación de capacidad registra su resultado, incluyendo la identidad del SEPP remoto y la capacidad de seguridad N32-f seleccionada en caso de éxito. Observa estos para confirmar que:

- Los socios de roaming esperados están completando el apretón de manos.
- La capacidad seleccionada coincide con tu intención (por ejemplo `TLS`).
- Un socio está siendo rechazado porque no se pudo seleccionar una capacidad común.

Un par que selecciona una capacidad que este SEPP no ofreció (en la ruta del iniciador) se registra como una advertencia y se rechaza.

Decisiones y Fallos de Reenvío N32-f

El N32-f relay registra sus decisiones y fallos de reenvío, incluyendo:

- Rechazos para reenviar a un PLMN que no es un socio de roaming configurado. Una tasa creciente de estos sugiere una entrada `roaming_partners` faltante o mal configurada.
- Objetivos de reenvío entrantes y salientes (la URL resuelta y la dirección).
- Fallos de reenvío, que se presentan al socio como `502 TARGET_NF_NOT_REACHABLE` e indican que el NF interno dirigido no era accesible.

Registro de Solicitudes

El registro de solicitudes estándar cubre cada solicitud SBI manejada por el listener, incluyendo los puntos finales de apretón de manos y el relay de captura N32-f. Úsalo para observar el volumen de solicitudes, métodos y rutas, y para correlacionar la actividad del socio con eventos de apretón de manos y reenvío.

Verificación de Salud

La salud se evalúa combinando:

- **Vitalidad:** `GET /n32c-handshake/v1/status` devuelve `200 {"status":"UP"}` cuando el listener SBI está en funcionamiento. Consulta la Guía de Operaciones.
- **Registro en NRF:** confirma que OmniSEPP aparece en el NRF como una instancia NF `SEPP` y está enviando latidos. El comportamiento de registro se describe en la Guía de Operaciones.
- **Señales de Registro:** los eventos de apretón de manos y reenvío descritos anteriormente.

Guía de Operaciones de OmniSEPP

Resumen | Referencia de Configuración | Métricas y Monitoreo | Solución de Problemas

Esta guía describe cómo se comporta OmniSEPP en el borde inter-PLMN N32 y cómo operarlo. OmniSEPP es el Proxy de Protección de Seguridad en el Borde definido en 3GPP TS 23.501 §6.2.17, con comportamiento de seguridad de 3GPP TS 33.501 y la interfaz N32 de 3GPP TS 29.573.

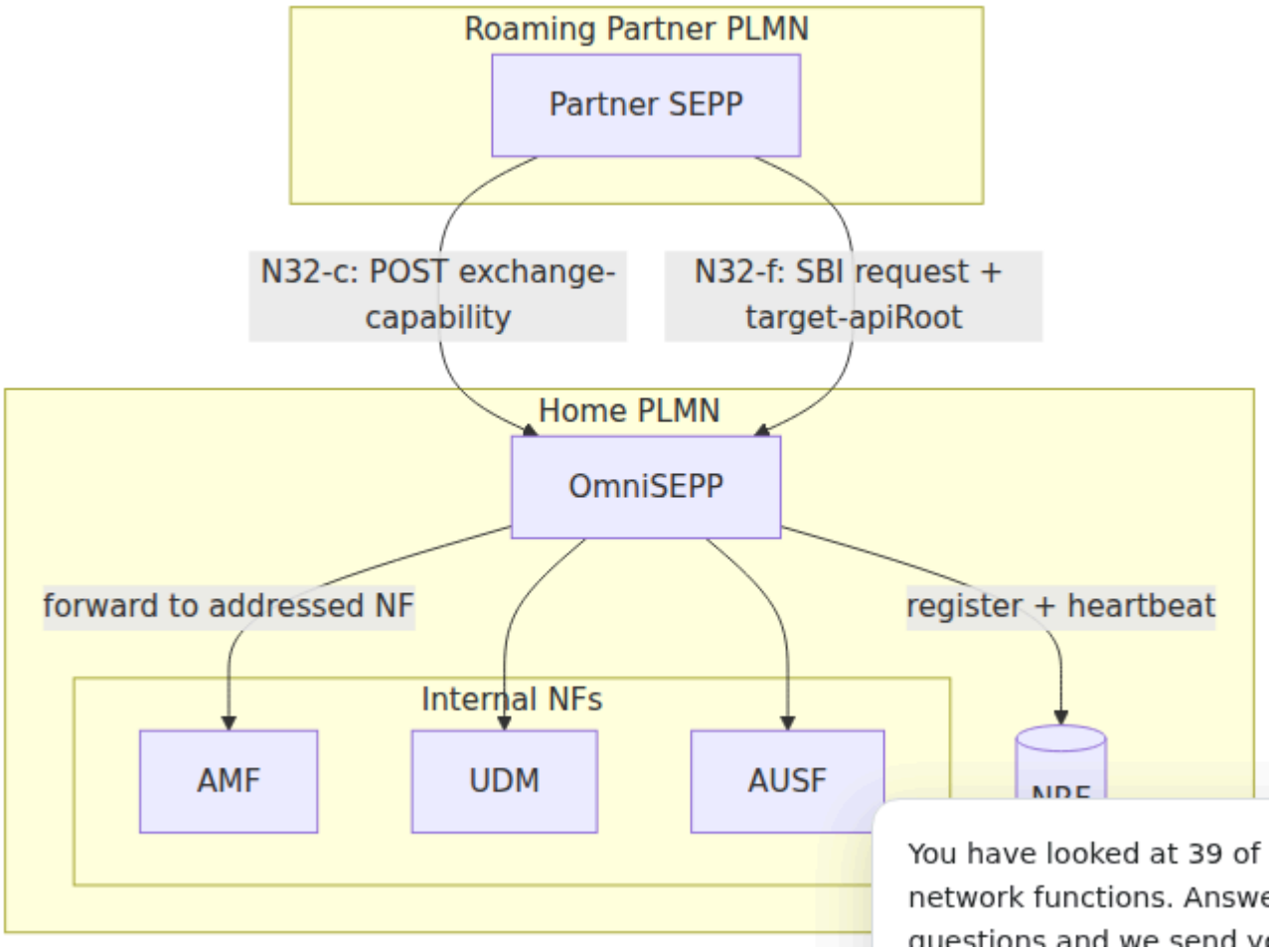
Tabla de Contenidos

- Descripción General de la Arquitectura
- La Interfaz N32
- Ciclo de Vida de la Asociación N32
- Negociación de Capacidades
- Control de Socios de Roaming
- Ocultación de Topología
- Flujos de Mensajes
- Puntos de Acceso SBI
- Registro NRF
- Notas Operativas

Descripción General de la Arquitectura

OmniSEPP termina la interfaz N32 hacia los SEPPs socios de roaming y reenvía el tráfico a las funciones de red internas en el PLMN de origen. Se registra con el NRF local como NFType `SEPP` para que los consumidores locales y el SCP puedan descubrirlo; el SEPP remoto y el mapa de ocultación de topología son

configuración estática por acuerdo de roaming (los SEPPs pares no se descubren a través del NRF).



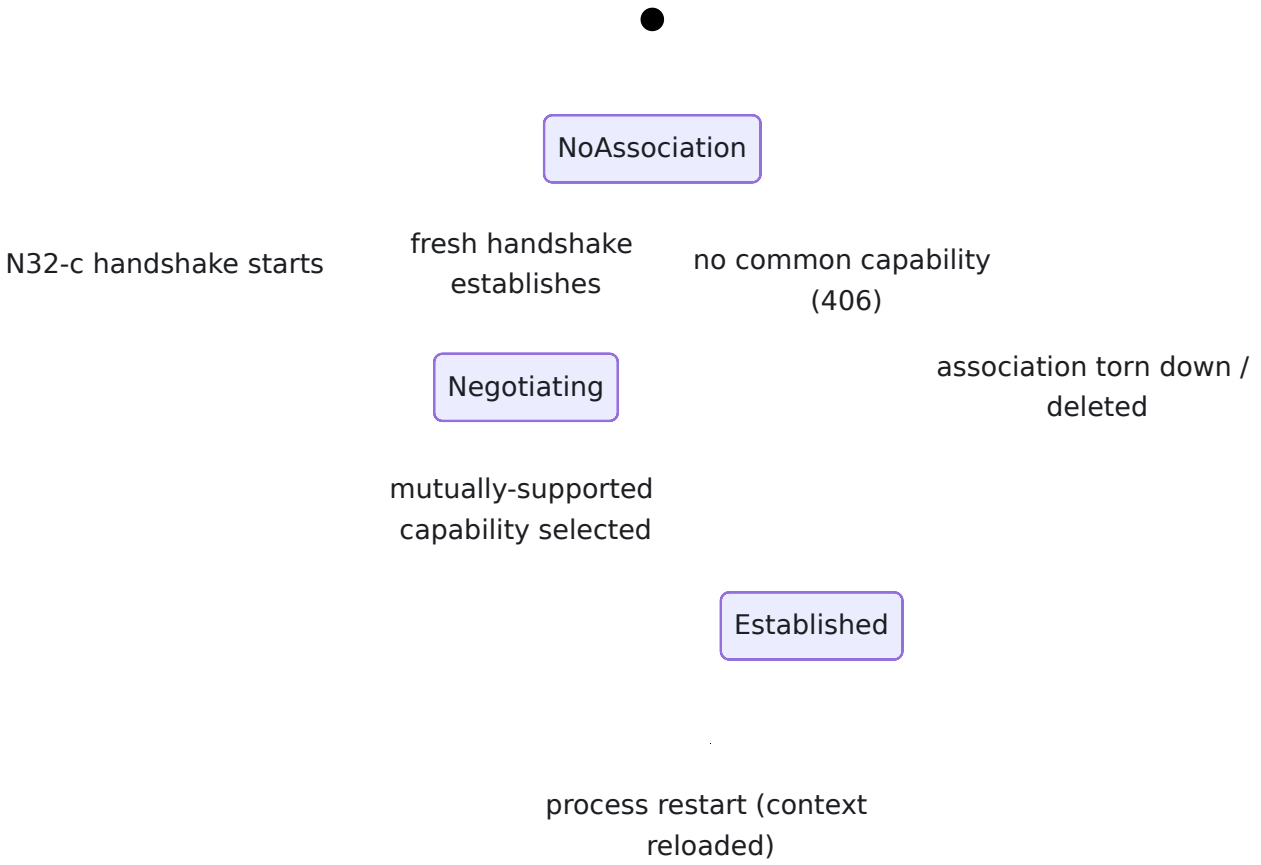
La Interfaz N32

N32 tiene dos canales lógicos (TS 29.573):

- **N32-c (canal de control)** - El apretón de manos utilizado para negociar la capacidad de seguridad N32-f y establecer la asociación entre los dos SEPPs. OmniSEPP expone esto como el `/n32c-handshake/v1/exchange-capability` endpoint (rol de respondedor) y también inicia el apretón de manos hacia cada socio de roaming configurado al inicio (rol de iniciador).
- **N32-f (canal de reenvío)** - El intercambio continuo de mensajes basados en servicios (SBI) entre los dos PLMNs. OmniSEPP reenvía estos en **modo TLS**: el mensaje se reenvía en gran medida de forma literal, con higiene de encabezados hop-by-hop y ocultación de topología aplicada.

Ciclo de Vida de la Asociación N32

Cada negociación N32-c exitosa registra una asociación en un **almacenamiento de contexto persistente** (una tabla DETS precedida por una caché en memoria), indexada por el FQDN del SEPP remoto. El contexto almacenado incluye la capacidad de seguridad N32-f seleccionada y la lista de identidades de PLMN socio.



Propiedades operativas clave:

- El almacenamiento es **persistente**: las asociaciones se escriben en el archivo DETS en `n32_context_path` y se recargan al inicio, por lo que sobreviven a un reinicio de proceso o nodo. Un socio no tiene que re-hacer el apretón de manos después de un reinicio de OmniSEPP.
- No hay **TTL**: una asociación persiste hasta que se elimina explícitamente (borrada) o se reemplaza por una nueva negociación.
- Si no se puede abrir el archivo DETS (por ejemplo, por corrupción), el almacenamiento comienza vacío y registra una advertencia; las asociaciones se restablecen mediante el apretón de manos.

Negociación de Capacidades

Durante el apretón de manos N32-c, los dos SEPPs acuerdan una única capacidad de seguridad N32-f. Las capacidades válidas son `TLS` y `PRINS` (TS 33.501 §13.1).

La regla de selección (TS 29.573 §5.2.3.2.2) es **preferencia-local-primer**: OmniSEPP recorre su propia lista configurada de `supported_sec_capabilities` en orden y elige la primera entrada que el par también ofrece. Si los dos conjuntos de capacidades son disjuntos, la negociación falla con `INSUFFICIENT_RESOURCES` (HTTP 406) y no se registra ninguna asociación.

Solo se publican capacidades bien formadas y reconocidas (`TLS`, `PRINS`). Mantenga `supported_sec_capabilities` en `["TLS"]` para una operación interoperable. Consulte la Referencia de Configuración para saber cómo establecer el orden de preferencia.

Control de Socios de Roaming

El **registro de socios de roaming** es una lista de permitidos estática indexada por PLMN socio (`"mcc-mnc"`). Gobierna el reenvío N32-f:

- Solo los PLMNs presentes en el registro se reenvían hacia o desde.
- Un registro vacío (el predeterminado) significa que el reenvío N32-f rechaza todos los PLMNs desconocidos.
- Cada entrada de socio lleva la raíz de la API del SEPP socio y, opcionalmente, las capacidades de seguridad N32-f permitidas con ese socio. Cuando se omite la lista de capacidades, el socio hereda las `supported_sec_capabilities` de este SEPP.

Consulte Referencia de Configuración - Socios de Roaming para la estructura del mapa.

Ocultación de Topología

La ocultación de topología (TS 33.501 §13.2) oculta las identidades de NF internas de los socios de roaming reescribiendo FQDNs. OmniSEPP aplica un mapa configurado por el operador de `internal_fqdn => external_fqdn`:

- **Saliente** (hacia un socio): los FQDN internos en los valores de encabezado `3gpp-Sbi-Target-apiRoot`, `Location` y `producer-id` se reescriben a sus equivalentes externos.
- **Entrante** (de un socio): se aplica el mapeo inverso para que el apiRoot presentado externamente se resuelva de nuevo al verdadero FQDN interno antes de que la solicitud se dirija al NF interno.

Las reescrituras están ancladas a **tokens FQDN completos**: un FQDN mapeado se reescribe solo cuando aparece como un host completo (limitado por delimitadores de URL como `/`, `:`, `@`, o el final del valor), nunca como una subcadena de un nombre de host más largo. Esto evita que un mapeo corrompa un host no relacionado que simplemente contiene el nombre mapeado, y detiene un valor producido por un mapeo de ser re-coincidido por otra entrada de mapeo.

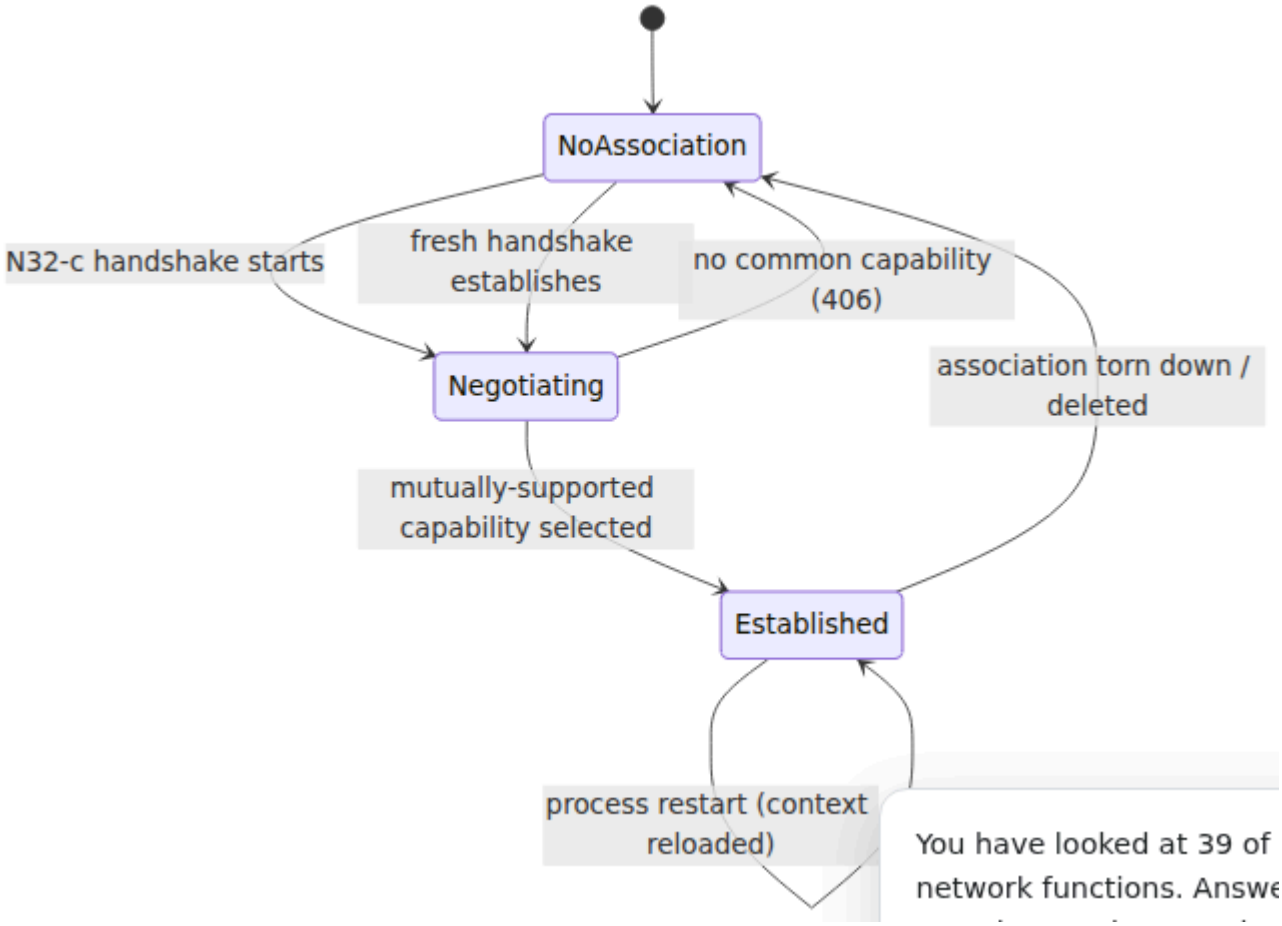
En cada reenvío, se eliminan los encabezados hop-by-hop (`host`, `content-length`, `connection`). En la ruta entrante, el encabezado (ahora consumido) `3gpp-Sbi-Target-apiRoot` también se elimina antes de que la solicitud llegue al NF interno.

Un mapa de ocultación de topología vacío (el predeterminado) significa que no se realiza ninguna reescritura. Consulte Referencia de Configuración - Mapa de Ocultación de Topología.

Flujos de Mensajes

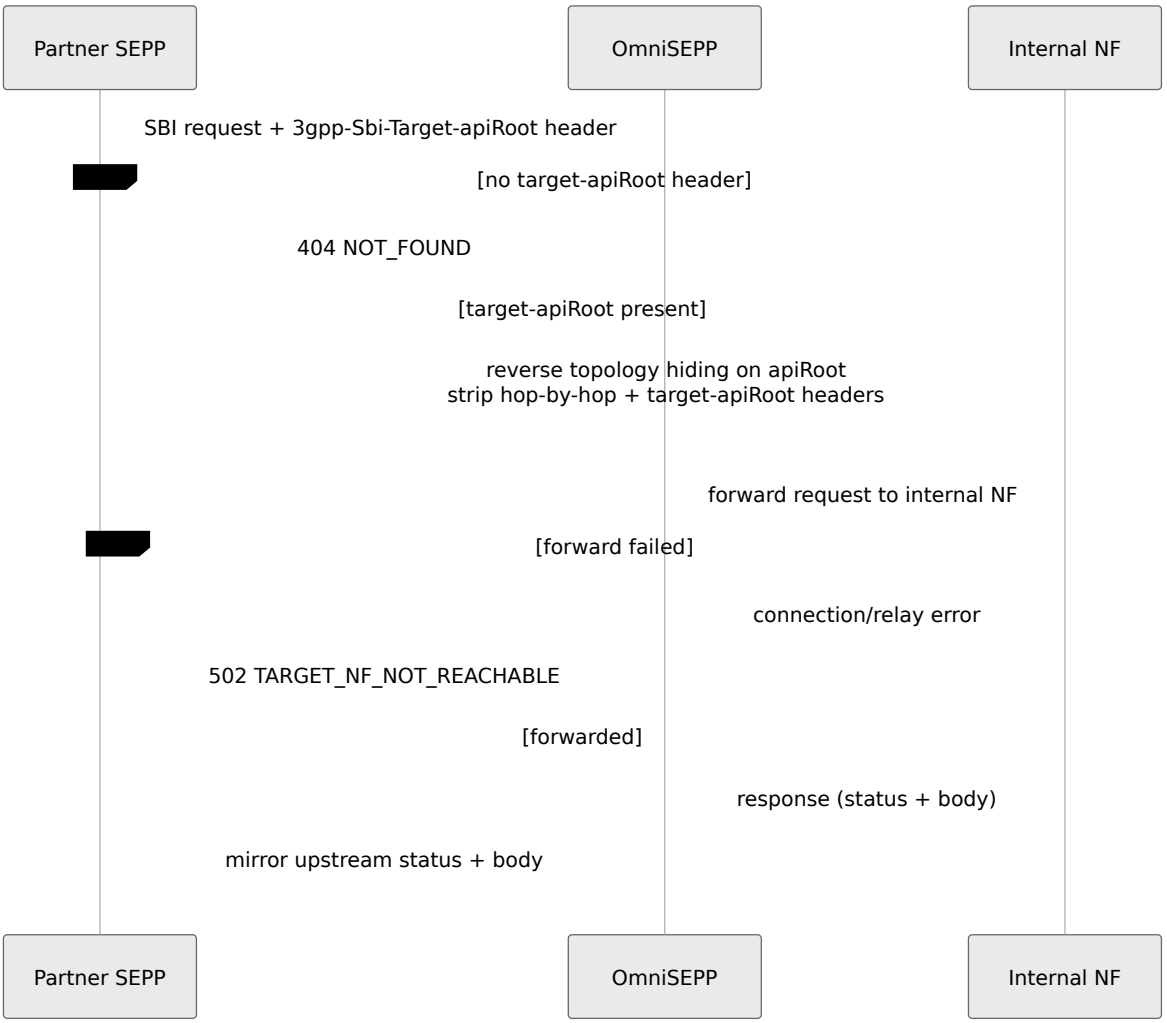
Apretón de Manos N32-c (Respondedor)

Un SEPP socio de roaming inicia el apretón de manos enviando una solicitud de negociación de capacidad por POST. OmniSEPP selecciona una capacidad mutuamente soportada, registra la asociación y responde.



Reenvío N32-f Entrante

Un SEPP socio envía una solicitud SBI que lleva un encabezado `3gpp-Sbi-Target-apiRoot` que identifica el NF interno. OmniSEPP revierte la ocultación de topología, elimina los encabezados hop-by-hop y de enrutamiento, y reenvía la solicitud, reflejando la respuesta ascendente.



Puntos de Acceso SBI

OmniSEPP expone lo siguiente a través de su oyente HTTP SBI. El apretón de manos N32-c publicita un servicio NRF, `n32c-handshake` versión `v1`.

Método	Ruta	Propósito
POST	`/n32c-handshake/v1/exchange-capability`	Negociación de Capacidad de Seguridad N32-c (respondedor).
GET	`/n32c-handshake/v1/status`	Sonda de disponibilidad.
(cualquiera)	cualquier otra ruta	Reenvío N32-f. Enrutado saliente al SEPP socio de roaming cuando la solicitud nombra un PLMN socio, de lo contrario entrante al NF interno nombrado por `3gpp-Sbi-Target-apiRoot`.

POST /n32c-handshake/v1/exchange-capability

Negocia la capacidad de seguridad N32-f con un SEPP socio iniciador.

Estado	Causa	Condición
200	-	Negociación exitosa. La respuesta lleva `sender` y `selectedSecCapability`.
400	`MANDATORY_IE_MISSING`	La solicitud carece de `sender`, o `supportedSecCapabilityList` está ausente o vacía.
406	`INSUFFICIENT_RESOURCES`	No hay capacidad de seguridad N32-f mutuamente soportada.

GET /n32c-handshake/v1/status

Devuelve `200` con el cuerpo `{"status":"UP"}`. Adecuado como sonda de disponibilidad.

Reenvío N32-f (catch-all)

Cualquier solicitud que no sea uno de los puntos finales de apretón de manos se trata como tráfico de reenvío N32-f. La solicitud se enruta **saliente** (hacia el SEPP socio de roaming) cuando nombra un PLMN socio como su selector de salida, de lo contrario **entrante** (hacia el NF interno nombrado por `3gpp-Sbi-Target-apiRoot`).

Estado	Causa	Condición
(reflejado)	-	El estado y el cuerpo ascendentes se reflejan de nuevo en caso de éxito (entrante o saliente).
404	`NOT_FOUND`	Entrante: el encabezado `3gpp-Sbi-Target-apiRoot` está ausente, por lo que no hay objetivo de enrutamiento.
403	`TARGET_PLMN_NOT_A_PARTNER`	Saliente: el PLMN objetivo nombrado no es un socio de roaming configurado.
502	`TARGET_NF_NOT_REACHABLE`	El reenvío al NF interno (entrante) o al SEPP socio (saliente) falló.

Registro NRF

Al iniciar, OmniSEPP se registra con el NRF como NFType `SEPP` (TS 23.501 §6.2.17) y envía latidos en el intervalo configurado. El registro publicita la dirección SBI, el puerto y el esquema, el PLMN servido y el único servicio `n32c-handshake` `v1`.

Registrarse con el NRF local permite a los consumidores locales y al SCP descubrir este SEPP (TS 29.573 cl 4.2.1). El SEPP **remoto**, en cambio, se resuelve a partir de la configuración estática `roaming_partners` por acuerdo de roaming: este es el modelo previsto para la resolución de pares inter-PLMN, ya que un SEPP en un PLMN no puede buscar un SEPP en el NRF de otro PLMN. La ocultación de topología también es una configuración estática.

Los parámetros de registro y latido están documentados en la Referencia de Configuración.

Apretón de Manos Saliente al Inicio

OmniSEPP actúa como el **SEPP iniciador** así como el respondedor. Al arrancar, una vez que el almacenamiento de contexto está listo, inicia una negociación de capacidad N32-c hacia cada socio de roaming configurado (`roaming_partners`) que tenga un `sepp_uri` (TS 29.573 §5.2.3.2). Esto es **mejor esfuerzo**: un socio inalcanzable o que rechaza se registra y se omite en lugar de hacer que el inicio falle, y la tarea se ejecuta una vez sin reinicio. Un socio que fue inalcanzable al inicio aún puede establecer la asociación más tarde enviando su propio apretón de manos (lado respondedor), o en el próximo reinicio.

Notas Operativas

- **Comportamiento de reinicio:** el almacenamiento de asociación N32 es persistente (respaldado por DETS). Las asociaciones se recargan al reiniciar, por lo que los socios no tienen que volver a ejecutar el apretón de manos N32-c para que el reenvío se reanude.

- **PLMNs desconocidos:** con un registro de socios de roaming vacío, el reenvío N32-f rechaza PLMNs desconocidos. Pueble el registro antes de esperar que el tráfico de socios sea reenviado.
- **Terminación TLS:** cuando `sbi_scheme` es `https`, el oyente N32 termina TLS por sí mismo utilizando el certificado y la clave configurados, y aplica TLS mutuo (certificado de cliente) cuando se configura un CA. Consulte Referencia de Configuración - TLS del Oyente N32.
- **PLMN predeterminado:** el PLMN servido predeterminado enviado (`999-70`) es un valor de prueba y debe ser sobrescrito por implementación.
- **Observabilidad:** opere contra registros de aplicación estructurados; consulte Métricas y Monitoreo.

Solución de Problemas de OmniSEPP

Resumen | Guía de Operaciones | Referencia de Configuración | Métricas y Monitoreo

Esta guía cubre problemas operativos comunes y sus resoluciones. El diagnóstico se basa en registros estructurados; consulte Métricas y Monitoreo.

Problemas Comunes

N32-c Handshake Rechazado Con 400

Síntomas: La solicitud de negociación de capacidades de un SEPP asociado se responde con `400 MANDATORY_IE_MISSING`.

Causas posibles:

- La solicitud carece de la identidad `sender`.
- La `supportedSecCapabilityList` está ausente o vacía.

Resolución:

1. Confirme que el socio esté enviando un `SecNegotiateReqData` bien formado con un `sender` no vacío.
2. Confirme que el socio incluya al menos una capacidad de seguridad N32-f en `supportedSecCapabilityList`.

N32-c Handshake Rechazado Con 406

Síntomas: El handshake de un socio se responde con `406 INSUFFICIENT_RESOURCES` y no se registra ninguna asociación.

Causas posibles:

- No hay una capacidad común entre las `supported_sec_capabilities` de este SEPP y la lista ofrecida por el socio. Por ejemplo, el socio ofrece solo `PRINS` mientras que este SEPP ofrece solo `TLS`.

Resolución:

1. Compare las capacidades ofrecidas por el socio con las `supported_sec_capabilities` de este SEPP.
2. Asegúrese de que ambos lados compartan al menos una capacidad. En la práctica, esto significa que ambos deben soportar `TLS`; mantenga `supported_sec_capabilities` en `["TLS"]` para una operación interoperable.

N32-f Tráfico Rechazado para un PLMN

Síntomas: El reenvío N32-f es rechazado, y los registros muestran un rechazo para reenviar a un PLMN no asociado.

Causas posibles:

- El PLMN asociado no está presente en el registro de `roaming_partners`.
- El registro está vacío (el valor predeterminado), por lo que todos los PLMNs desconocidos son rechazados.

Resolución:

1. Agregue el PLMN asociado a `roaming_partners`, con la clave `"mcc-mnc"`, junto con el `sepp_uri` del SEPP asociado.
2. Confirme que la clave del PLMN coincida exactamente con el `mcc-mnc` del socio.

El Relay Inbound Devuelve 404 NOT_FOUND

Síntomas: Una solicitud de un socio se responde con `404 NOT_FOUND` en lugar de ser reenviada.

Causas posibles:

- La solicitud no lleva un encabezado `3gpp-Sbi-Target-apiRoot`, por lo que OmniSEPP no tiene un objetivo de enrutamiento.

Resolución:

1. Confirme que el socio establezca el encabezado `3gpp-Sbi-Target-apiRoot` identificando el NF interno.
2. Si se está utilizando ocultación de topología, confirme que el apiRoot externo que presenta el socio tenga una entrada inversa coincidente en el `topology_hiding_map`.

El Relay Inbound Devuelve 502 TARGET_NF_NOT_REACHABLE

Síntomas: Una solicitud de un socio se responde con `502 TARGET_NF_NOT_REACHABLE`.

Causas posibles:

- El NF interno dirigido está caído o es inalcanzable desde OmniSEPP.
- La ocultación de topología no resolvió el apiRoot externo a un FQDN interno alcanzable.

Resolución:

1. Confirme que el NF interno resuelto desde el apiRoot (invertido) esté en funcionamiento y sea alcanzable.
2. Verifique que la entrada del `topology_hiding_map` mapee el FQDN externo al FQDN interno correcto y resoluble.

Las Asociaciones Desaparecen Después de un Reinicio

Síntomas: Después de reiniciar OmniSEPP, los socios previamente establecidos son tratados como si no existiera ninguna asociación, y el reenvío N32-f para ellos falla hasta que vuelven a realizar el handshake.

Causas posibles:

- El archivo DETS en `n32_context_path` no se pudo abrir (por ejemplo, debido a corrupción o un problema de permisos), por lo que el almacenamiento comenzó vacío y registró una advertencia.
- La `n32_context_path` configurada cambió entre ejecuciones, por lo que el archivo anterior no se está leyendo.

Resolución:

1. Las asociaciones son normalmente persistentes y se recargan al reiniciar, por lo que un reinicio solo no debería borrarlas. Si faltan, verifique los registros de inicio para una advertencia de N32Context sobre la apertura de DETS.
2. Confirme que `n32_context_path` apunte a una ubicación estable y escribible que se conserve entre reinicios (no a un directorio temporal por ejecución).

El Socio No Puede Establecer TLS Mutuamente Autenticado

Síntomas: Un socio espera N32 sobre TLS mutuamente autenticado, pero la conexión es rechazada, es HTTP sin cifrar, o el certificado del cliente del socio no se está verificando.

Causas posibles:

- `sbi_scheme` es `http`, por lo que el listener sirve texto sin formato.
- `sbi_scheme` es `https` pero `sbi_cacertfile` no está configurado, por lo que solo se termina TLS del lado del servidor y no se requiere el certificado del cliente del par.
- `sbi_scheme` es `https` pero `sbi_certfile` / `sbi_keyfile` no están configurados, en cuyo caso OmniSEPP se niega a iniciar en lugar de degradar a texto sin formato.

Resolución:

1. Establezca `sbi_scheme` en `https` y configure `sbi_certfile` y `sbi_keyfile` para que el listener termine TLS por sí mismo.

2. Para requerir y verificar el certificado del cliente del SEPP par (TLS mutuo), establezca `sbi_cacertfile` en la CA que firma el certificado del par. Consulte Referencia de Configuración - TLS del Listener N32.

Referencia

Tema	Especificación
Función de red SEPP	3GPP TS 23.501 §6.2.17
Modo TLS N32-f y ocultación de topología	3GPP TS 33.501 §13.1, §13.2
Handshake N32 y reenvío N32-f	3GPP TS 29.573 §5.2.3, §5.3, §6.1.5.2