Referência de Configuração do OmniSEPP

Visão Geral | Guia de Operações | Métricas e Monitoramento | Solução de Problemas

Toda a configuração do OmniSEPP vive sob a chave de aplicativo `:omnisepp`. Um subconjunto de chaves pode ser substituído por variáveis de ambiente, mas isso só tem efeito na **configuração de tempo de execução de produção**. Os mapas aninhados (`roaming_partners`, `topology_hiding_map`) e um pequeno número de outras chaves não têm variável de ambiente e são configurados apenas através do arquivo de configuração do aplicativo.

Estrutura da Configuração

```
config :omnisepp,
  # Identidade do listener SBI/N32 (anunciada para o NRF)
  sbi_scheme: "http",
  sbi_addr: "127.0.0.22",
  sbi_port: 7777,

  # Material TLS para o listener N32 (usado apenas quando
sbi_scheme é "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 (substituir por implantação)
  mcc: "999",
  mnc: "70",

  # Identidade própria deste SEPP e capacidades negociadas
  sepp_fqdn: "sepp.5gc.mnc70.mcc999.3gppnetwork.org",
  supported_sec_capabilities: ["TLS"],

  # Persistência do contexto de associação N32 (apenas arquivo de
configuração)
  n32_context_path: "<priv>/data/n32_context.dets",

  # Roaming e ocultação de topologia (apenas arquivo de
configuração)
  roaming_partners: %{},
  topology_hiding_map: %{}
```

Cada parâmetro acima é documentado abaixo.

Parâmetros Principais

Parâmetro	Tipo	Requerido	Padrão
`sbi_scheme`	String	Não	`http`
`sbi_addr`	String	Não	`127.0.0.22`
`sbi_port`	Inteiro	Não	`7777`
`sbi_certfile`	String (caminho)	Condicional	(nenhum)

Parâmetro	Tipo	Requerido	Padrão
`sbi_keyfile`	String (caminho)	Condicional	(nenhum)
`sbi_cacertfile`	String (caminho)	Não	(nenhum)
`nrf_uri`	String	Não	`http://127.0.0.`

Parâmetro	Tipo	Requerido	Padrão
`mcc`	String	Não	`999`
`mnc`	String	Não	`70`
`heartbeat_interval`	Inteiro (ms)	Não	`10000`
`sepp_fqdn`	String	Não	derivado (veja ab

Parâmetro	Tipo	Requerido	Padrão
`supported_sec_capabilities`	Lista de String	Não	`["TLS"]`
`n32_context_path`	String (caminho)	Não	derivado (veja ab
`roaming_partners`	Mapa	Não	`%{}`

Parâmetro	Tipo	Requerido	Padrão
`topology_hiding_map`	Mapa	Não	`%{}`

sepp_fqdn

Quando `sepp_fqdn` não está definido, ele é derivado do PLMN servido como:

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

Para o PLMN padrão `999-70`, isso resulta em `sepp.5gc.mnc70.mcc999.3gppnetwork.org`. Este FQDN é enviado como a identidade `sender` em solicitações e respostas de handshake N32-c (TS 29.573). Substitua-o explicitamente quando a forma derivada não corresponder ao FQDN que seus parceiros de roaming esperam.

TLS do Listener N32

Quando `sbi_scheme` é `https`, o listener N32 termina o TLS por conta própria, em vez de depender de um terminador externo. Este é o modo TLS N32-f (TS 33.501 §13.1), no qual dois SEPPs protegem a interface com TLS entre eles.

- `sbi_certfile` e `sbi_keyfile` são **ambos obrigatórios** quando `sbi_scheme` é `https`. Se algum deles estiver ausente, o SEPP se recusa a iniciar em vez de rebaixar silenciosamente para texto simples.

- Quando `sbi_cacertfile` também está definido, o listener requer e verifica o certificado do cliente do SEPP par contra essa CA, proporcionando TLS mutuamente autenticado. Sem CA configurada, apenas o TLS do lado do servidor é terminado.
- Quando `sbi_scheme` é `http` (o padrão), essas chaves são ignoradas e o listener serve texto simples.

O esquema anunciado no registro NRF segue `sbi_scheme`, portanto, agora reflete o transporte real do listener.

capacidades_sec_suportadas

As capacidades de segurança N32-f que este SEPP suporta, na **ordem de preferência local** (mais preferido primeiro). Durante o handshake N32-c, o OmniSEPP seleciona a primeira entrada nesta lista que o par também oferece (TS 29.573 §5.2.3.2.2).

Valor	Significado	Referência
`TLS`	Proteção na camada de transporte entre SEPPs.	TS 33.501 §13.1
`PRINS`	PRoteção com Inserção de Segurança Intermediária (proteção na camada de aplicação JOSE via um hub de roaming).	TS 33.501 §13.2

Apenas esses dois valores são reconhecidos; qualquer outra entrada é ignorada. O padrão é `["TLS"]`; mantenha-o em `["TLS"]` para operação interoperável.

Ao substituir via a variável de ambiente `SEPP_SEC_CAPABILITIES`, forneça uma lista separada por vírgulas na ordem de preferência, por exemplo `TLS,PRINS`. O espaço em branco ao redor de cada entrada é removido.

Persistência do Contexto N32

Associações N32 estabelecidas são persistidas em um arquivo DETS em `n32_context_path`, para que sobrevivam a uma reinicialização de processo ou nó (TS 29.573). Na inicialização, o armazenamento recarrega as associações persistidas, para que um parceiro não precise reexecutar o handshake N32-c após uma reinicialização do OmniSEPP.

- Quando não definido, o caminho padrão é `n32_context.dets` sob o diretório de dados `priv` do aplicativo OTP. O diretório pai é criado na inicialização se não existir.
- Se o arquivo não puder ser aberto (por exemplo, em caso de corrupção), o armazenamento registra um aviso e inicia com uma tabela em memória vazia em vez de falhar na inicialização; as associações são então restabelecidas por handshake.
- Esta chave não tem variável de ambiente e é configurada apenas através do arquivo de configuração do aplicativo.

Parceiros de Roaming

O mapa `roaming_partners` é a lista estática de permissão de PLMNs de parceiros de roaming. Ele é indexado pelo identificador do PLMN parceiro na forma `"mcc-mnc"`, e cada valor é uma especificação de parceiro.

```
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"
    }
  }
```

Estrutura de nível superior:

Forma da Chave	Tipo	Descrição
`"mcc-mnc"`	String (chave do mapa)	Identificador do PLMN parceiro, por exemplo `"001-01"`.
valor	Mapa	Especificação do parceiro (veja abaixo).

Especificação do parceiro:

Parâmetro	Tipo	Requerido	Padrão
`sepp_uri`	String	Sim	-
`sec_capabilities`	Lista de String	Não	herda `supported_sec_capabilities`

Um mapa `roaming_partners` vazio (o padrão) significa que nenhum parceiro de roaming está configurado, e o encaminhamento N32-f recusa todos os PLMNs desconhecidos. Este mapa não tem variável de ambiente e é configurado apenas através do arquivo de configuração do aplicativo.

Mapa de Ocultação de Topologia

O `topology_hiding_map` implementa a reescrita de FQDN para ocultação de topologia (TS 33.501 §13.2). Ele mapeia cada FQDN NF interno para o FQDN externo apresentado aos parceiros 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 da Chave	Tipo	Descrição
`internal_fqdn`	String (chave do mapa)	O FQDN NF interno a ser mascarado, por exemplo, um FQDN AMF ou UDM.
`external_fqdn`	String (valor)	O FQDN externo apresentado aos parceiros em seu lugar.

O mapeamento é aplicado para fora (interno para externo) nos valores de `3gpp-Sbi-Target-apiRoot`, `Location`, e cabeçalhos producer-id, e revertido para dentro (externo para interno) para que os apiRoots apresentados pelo parceiro resolvam de volta para o verdadeiro FQDN interno. Um mapa vazio (o padrão) significa que não há reescrita. Este mapa não tem variável de ambiente e é configurado apenas através do arquivo de configuração do aplicativo.

Resumo das Variáveis de Ambiente

As variáveis de ambiente se aplicam apenas na configuração de tempo de execução de produção. Chaves não listadas aqui são apenas para arquivo de configuração.

Variável de Ambiente	Parâmetro	Notas
`SEPP_SBI_SCHEME`	`sbi_scheme`	`http` ou `https`.
`SEPP_SBI_ADDR`	`sbi_addr`	
`SEPP_SBI_PORT`	`sbi_port`	Interpretado como um inteiro.
`SEPP_SBI_CERTFILE`	`sbi_certfile`	Requerido quando o esquema é `https`.
`SEPP_SBI_KEYFILE`	`sbi_keyfile`	Requerido quando o esquema é `https`.
`SEPP_SBI_CACERTFILE`	`sbi_cacertfile`	Definido para habilitar o TLS mútuo N32-f (verificação do certificado do cliente par).
`SEPP_NRF_URI`	`nrf_uri`	
`SEPP_MCC`	`mcc`	
`SEPP_MNC`	`mnc`	
`SEPP_FQDN`	`sepp_fqdn`	Quando não definido, o FQDN é

Variável de Ambiente	Parâmetro	Notas
		derivado do PLMN.
`SEPP_SEC_CAPABILITIES`	`supported_sec_capabilities`	Separado por vírgulas, ordem de preferência.

Exemplo de Configuração

Uma substituição realista por implantação para um PLMN doméstico `310-260` com um único parceiro 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"
  }
```

Como funciona: O OmniSEPP se anuncia para o NRF em `10.20.0.5:7777` como NFType `SEPP` para PLMN `310-260`, enviando heartbeats a cada 10 segundos. Como `sbi_scheme` é `https`, o listener N32 termina o TLS com `sepp.crt` / `sepp.key`, e como `sbi_cacertfile` está definido, ele requer e verifica o certificado do cliente do SEPP parceiro contra `partner-ca.crt` (mutual TLS). Ele aceita handshakes N32-c como `sepp.5gc.mnc260.mcc310.3gppnetwork.org`, negociando TLS como a única capacidade N32-f, e na inicialização inicia o handshake de saída em direção ao parceiro `001-01`. O tráfego N32-f é retransmitido apenas para e a partir do PLMN parceiro `001-01`, e o FQDN interno do AMF é mascarado atrás do FQDN do SEPP em direção a esse parceiro.

Métricas e Monitoramento do OmniSEPP

Visão Geral | Guia de Operações | Referência de Configuração | Solução de Problemas

Observabilidade

A observabilidade é fornecida por **logs de aplicação estruturados** e registro padrão de requisições. Os operadores monitoram o OmniSEPP através de seus logs, que capturam o handshake, o encaminhamento e os eventos de requisição descritos abaixo.

O que Observar nos Logs

Os logs da aplicação são o sinal principal para operar o OmniSEPP. As seguintes classes de eventos são registradas e valem a pena serem monitoradas.

Resultados do Handshake N32-c

Cada negociação de capacidade registra seu resultado, incluindo a identidade do SEPP remoto e a capacidade de segurança N32-f selecionada em caso de sucesso. Observe estes para confirmar que:

- Os parceiros de roaming esperados estão completando o handshake.
- A capacidade selecionada corresponde à sua intenção (por exemplo `TLS`).
- Um parceiro está sendo rejeitado porque nenhuma capacidade comum pôde ser selecionada.

Um par que seleciona uma capacidade que este SEPP não ofereceu (no caminho do iniciador) é registrado como um aviso e rejeitado.

Decisões e Falhas de Encaminhamento N32-f

O relay N32-f registra suas decisões de encaminhamento e falhas, incluindo:

- Recusas de encaminhar para um PLMN que não é um parceiro de roaming configurado. Uma taxa crescente desses sugere uma entrada `roaming_partners` ausente ou mal configurada.
- Alvos de relay de entrada e saída (a URL resolvida e a direção).
- Falhas de encaminhamento, que aparecem para o parceiro como `502 TARGET_NF_NOT_REACHABLE` e indicam que o NF interno endereçado estava inacessível.

Registro de Requisições

O registro padrão de requisições cobre cada requisição SBI tratada pelo listener, incluindo os endpoints de handshake e o relay N32-f catch-all. Use-o para observar o volume de requisições, métodos e caminhos, e para correlacionar a atividade do parceiro com eventos de handshake e encaminhamento.

Verificação de Saúde

A saúde é avaliada combinando:

- **Vigência:** `GET /n32c-handshake/v1/status` retorna `200 {"status":"UP"}` quando o listener SBI está ativo. Veja o Guia de Operações.
- **Registro NRF:** confirme que o OmniSEPP aparece no NRF como uma instância NF `SEPP` e está enviando batimentos cardíacos. O comportamento de registro é descrito no Guia de Operações.
- **Sinais de Log:** os eventos de handshake e encaminhamento descritos acima.

Guia de Operações do OmniSEPP

Visão Geral | Referência de Configuração | Métricas e Monitoramento | Solução de Problemas

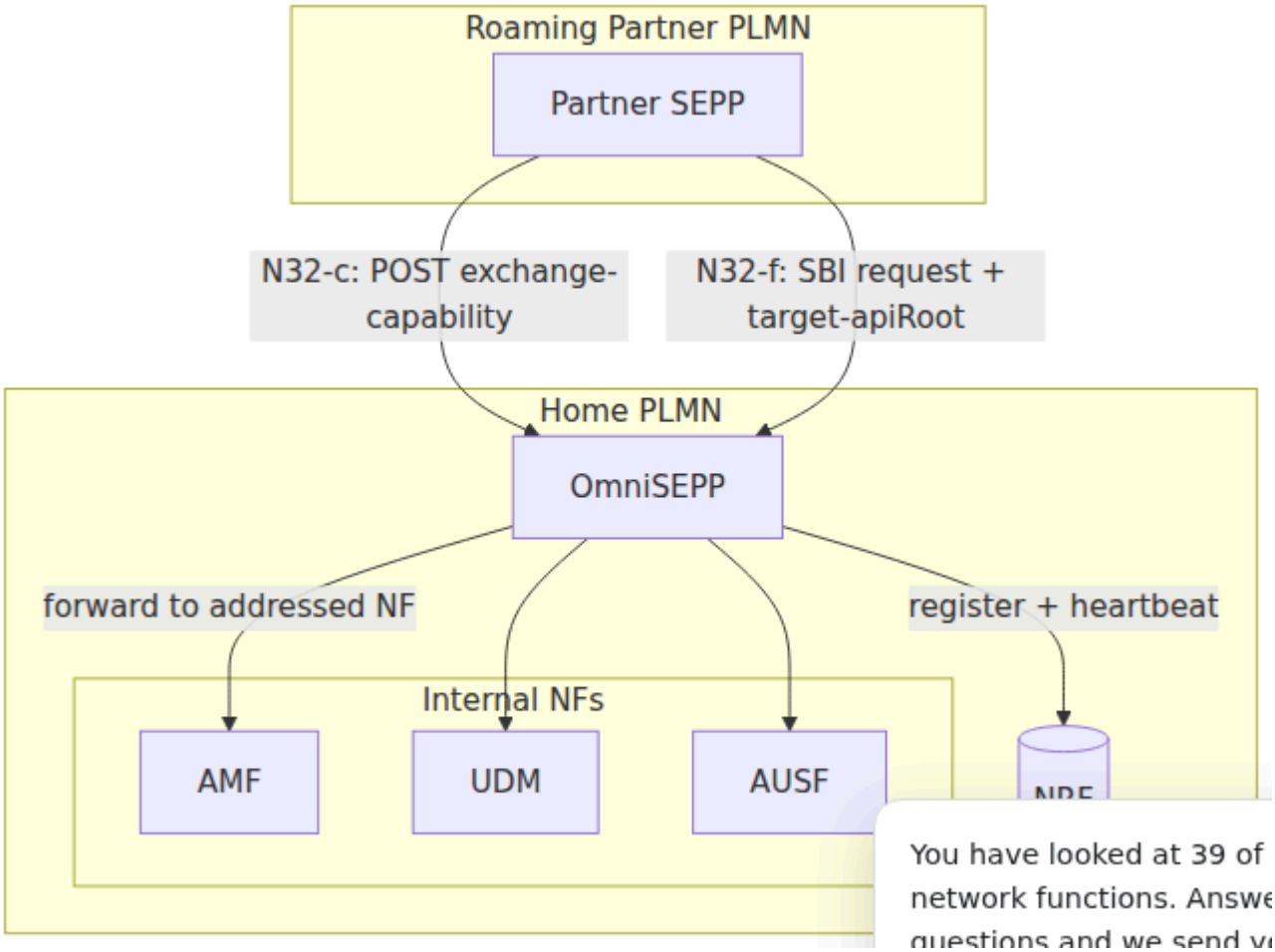
Este guia descreve como o OmniSEPP se comporta na borda inter-PLMN N32 e como operá-lo. O OmniSEPP é o Proxy de Proteção de Borda de Segurança definido em 3GPP TS 23.501 §6.2.17, com comportamento de segurança de 3GPP TS 33.501 e a interface N32 de 3GPP TS 29.573.

Índice

- Visão Geral da Arquitetura
- A Interface N32
- Ciclo de Vida da Associação N32
- Negociação de Capacidade
- Controle de Parceiro de Roaming
- Ocultação de Topologia
- Fluxos de Mensagens
- Endpoints SBI
- Registro NRF
- Notas Operacionais

Visão Geral da Arquitetura

O OmniSEPP termina a interface N32 em direção aos SEPPs de parceiros de roaming e retransmite o tráfego para funções de rede internas no PLMN de origem. Ele se registra no NRF local como NFType `SEPP`, para que consumidores locais e o SCP possam descobri-lo; o SEPP remoto e o mapa de ocultação de topologia são configurações estáticas por acordo de roaming (SEPPs pares não são descobertos via NRF).



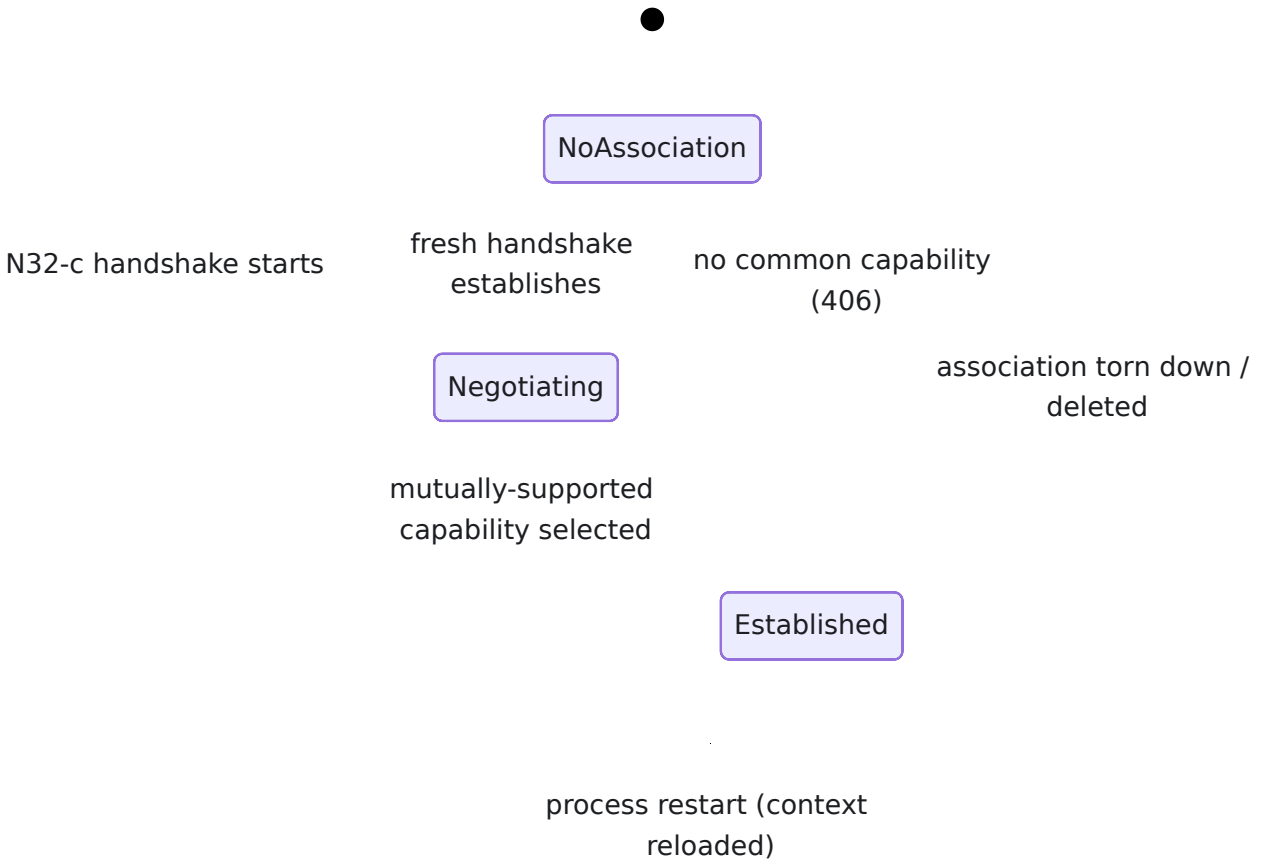
A Interface N32

N32 possui dois canais lógicos (TS 29.573):

- **N32-c (canal de controle)** - O handshake usado para negociar a capacidade de segurança N32-f e estabelecer a associação entre os dois SEPPs. O OmniSEPP expõe isso como o `/n32c-handshake/v1/exchange-capability` endpoint (papel de respondedor) e também inicia o handshake em direção a cada parceiro de roaming configurado na inicialização (papel de iniciador).
- **N32-f (canal de encaminhamento)** - A troca contínua de mensagens baseadas em serviço (SBI) entre os dois PLMNs. O OmniSEPP retransmite essas mensagens em **modo TLS**: a mensagem é retransmitida em grande parte de forma literal, com higiene de cabeçalho hop-by-hop e ocultação de topologia aplicadas.

Ciclo de Vida da Associação N32

Cada negociação N32-c bem-sucedida registra uma associação em um **armazenamento de contexto persistente** (uma tabela DETS com um cache em memória), indexada pelo FQDN do SEPP remoto. O contexto armazenado inclui a capacidade de segurança N32-f selecionada e a lista de identidade do PLMN parceiro.



Propriedades operacionais principais:

- O armazenamento é **persistente**: associações são gravadas no arquivo DETS em `n32_context_path` e recarregadas na inicialização, de modo que sobrevivam a uma reinicialização de processo ou nó. Um parceiro não precisa re-handsake após uma reinicialização do OmniSEPP.
- Não há **TTL**: uma associação persiste até que seja explicitamente desfeita (excluída) ou substituída por uma nova negociação.
- Se o arquivo DETS não puder ser aberto (por exemplo, devido a corrupção), o armazenamento começa vazio e registra um aviso; associações são então restabelecidas por handshake.

Negociação de Capacidade

Durante o handshake N32-c, os dois SEPPs concordam em uma única capacidade de segurança N32-f. As capacidades válidas são `TLS` e `PRINS` (TS 33.501 §13.1).

A regra de seleção (TS 29.573 §5.2.3.2.2) é **preferência-local-primeiro**: o OmniSEPP percorre sua própria lista configurada de `supported_sec_capabilities` em ordem e escolhe a primeira entrada que o par também oferece. Se os dois conjuntos de capacidade forem disjuntos, a negociação falha com `INSUFFICIENT_RESOURCES` (HTTP 406) e nenhuma associação é registrada.

Apenas capacidades bem formadas e reconhecidas (`TLS`, `PRINS`) são anunciadas. Mantenha `supported_sec_capabilities` em `["TLS"]` para operação interoperável. Consulte a Referência de Configuração para saber como definir a ordem de preferência.

Controle de Parceiro de Roaming

O **registro de parceiros de roaming** é uma lista de permissão estática indexada por PLMN parceiro (`"mcc-mnc"`). Ele governa o encaminhamento N32-f:

- Apenas PLMNs presentes no registro são retransmitidos para ou a partir de.
- Um registro vazio (o padrão) significa que o encaminhamento N32-f recusa todos os PLMNs desconhecidos.
- Cada entrada de parceiro contém a raiz da API do SEPP parceiro e, opcionalmente, as capacidades de segurança N32-f permitidas com esse parceiro. Quando a lista de capacidades é omitida, o parceiro herda as `supported_sec_capabilities` deste SEPP.

Consulte Referência de Configuração - Parceiros de Roaming para a estrutura do mapa.

Ocultação de Topologia

A ocultação de topologia (TS 33.501 §13.2) mascara as identidades internas de NF dos parceiros de roaming reescrevendo FQDNs. O OmniSEPP aplica um mapa configurado pelo operador de `internal_fqdn => external_fqdn`:

- **Outbound** (em direção a um parceiro): FQDNs internos nos valores de cabeçalho `3gpp-Sbi-Target-apiRoot`, `Location` e `producer-id` são reescritos para seus equivalentes externos.
- **Inbound** (de um parceiro): o mapeamento reverso é aplicado para que o apiRoot apresentado externamente resolva de volta para o verdadeiro FQDN interno antes que a solicitação seja roteada para o NF interno.

As reescritas são ancoradas em **tokens FQDN inteiros**: um FQDN mapeado é reescrito apenas quando aparece como um host completo (limitado por delimitadores de URL, como `/`, `:`, `@` ou o final do valor), nunca como uma substring de um nome de host mais longo. Isso impede que um mapeamento corrompa um host não relacionado que apenas contém o nome mapeado e impede que um valor produzido por um mapeamento seja re-mapeado por outra entrada de mapeamento.

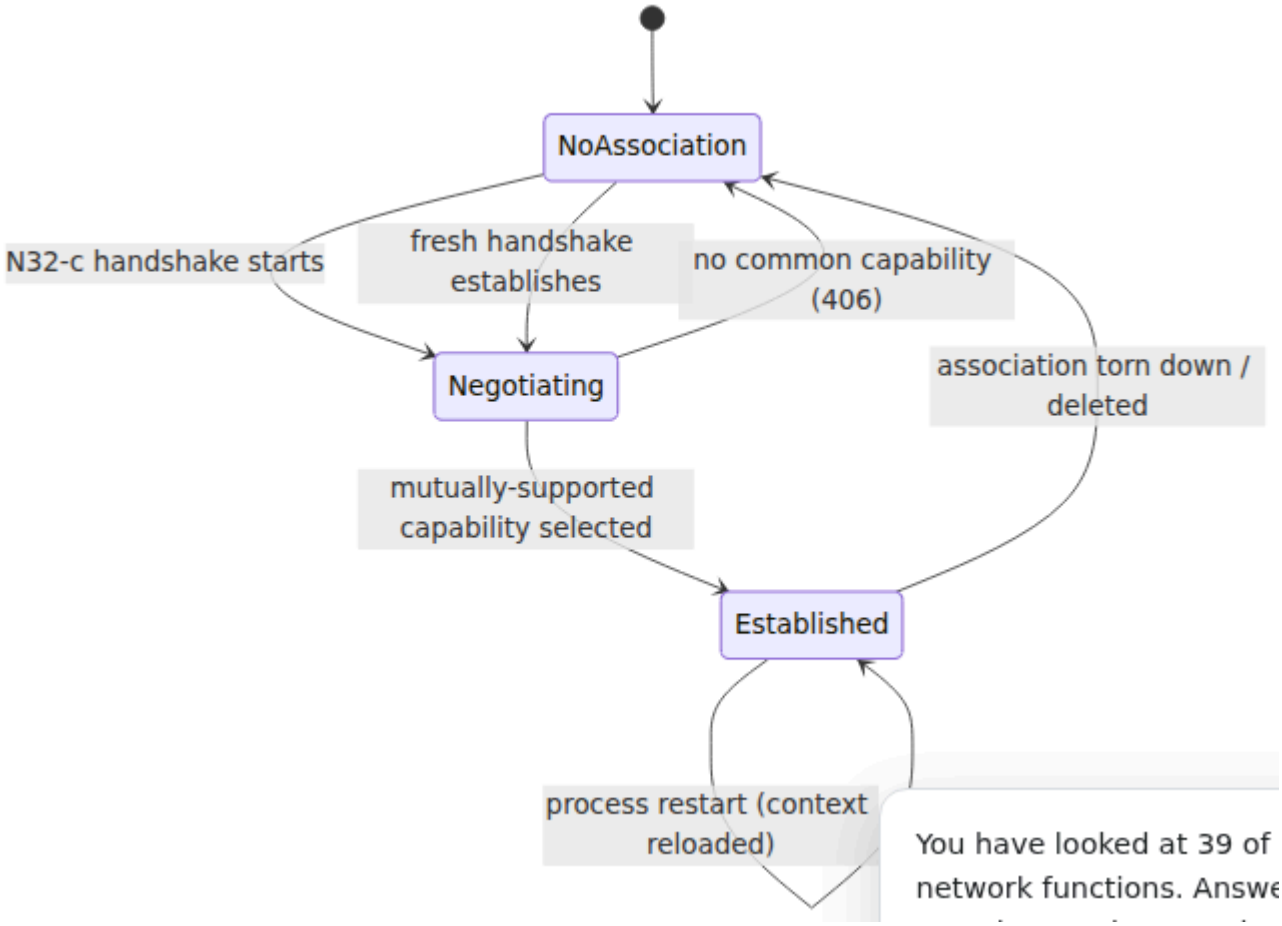
Em cada retransmissão, cabeçalhos hop-by-hop (`host`, `content-length`, `connection`) são removidos. No caminho de entrada, o cabeçalho `3gpp-Sbi-Target-apiRoot` (agora consumido) também é descartado antes que a solicitação alcance o NF interno.

Um mapa de ocultação de topologia vazio (o padrão) significa que nenhuma reescrita é realizada. Consulte Referência de Configuração - Mapa de Ocultação de Topologia.

Fluxos de Mensagens

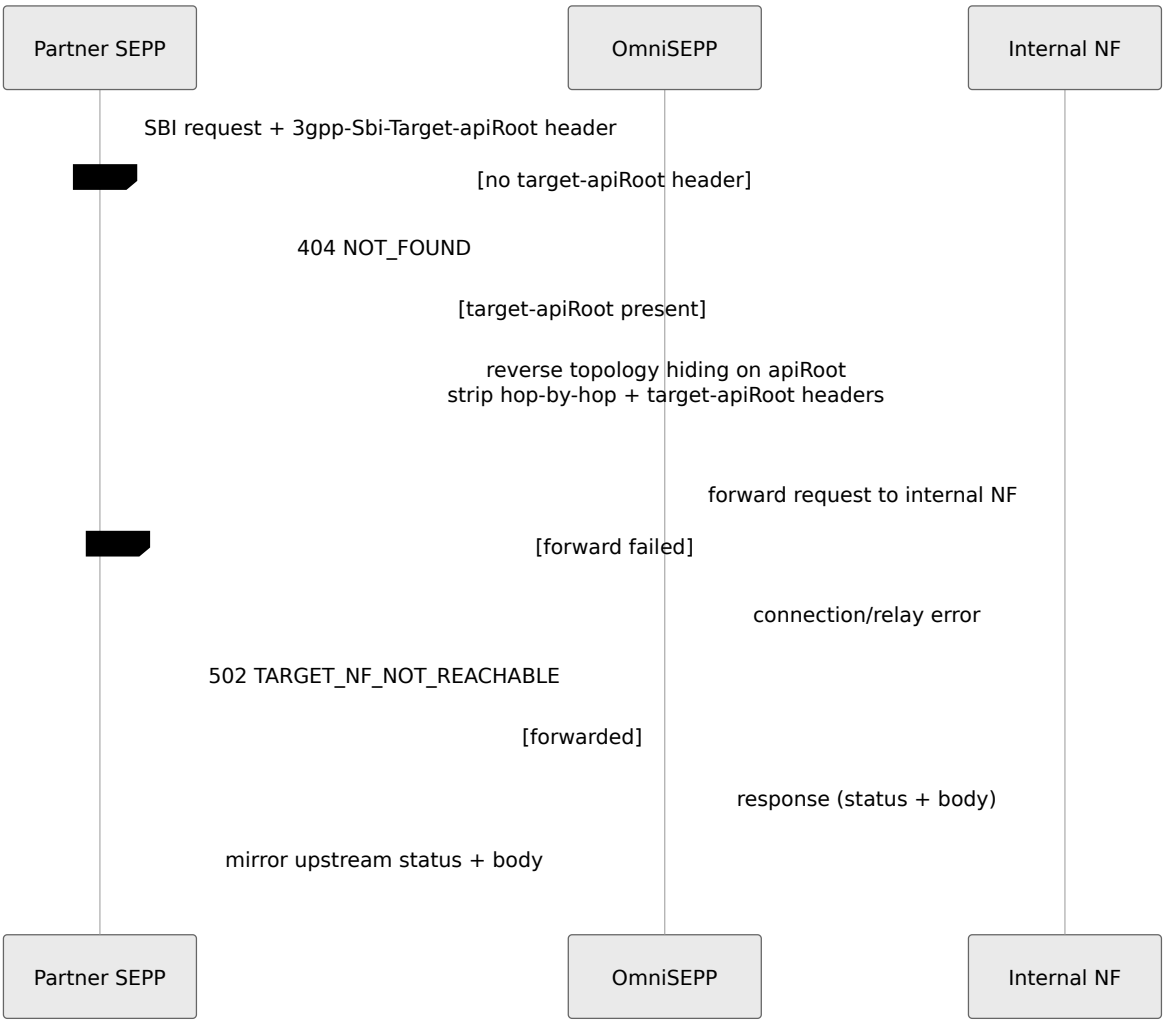
Handshake N32-c (Respondedor)

Um SEPP parceiro de roaming inicia o handshake enviando uma solicitação de negociação de capacidade. O OmniSEPP seleciona uma capacidade suportada mutuamente, registra a associação e responde.



Retransmissão N32-f Inbound

Um SEPP parceiro envia uma solicitação SBI contendo um cabeçalho `3gpp-Sbi-Target-apiRoot` que identifica o NF interno. O OmniSEPP reverte a ocultação de topologia, remove cabeçalhos hop-by-hop e de roteamento, e retransmite a solicitação, espelhando a resposta upstream.



Endpoints SBI

O OmniSEPP expõe o seguinte sobre seu ouvinte HTTP SBI. O handshake N32-c anuncia um serviço NRF, `n32c-handshake` versão `v1`.

Método	Caminho	Propósito
POST	`/n32c-handshake/v1/exchange-capability`	Negociação de Capacidade de Segurança N32-c (respondedor).
GET	`/n32c-handshake/v1/status`	Verificação de vivacidade.
(qualquer)	qualquer outro caminho	Retransmissão N32-f. Roteado para fora para o SEPP parceiro de roaming quando a solicitação nomeia um PLMN parceiro, caso contrário, para dentro para o NF interno nomeado por `3gpp-Sbi-Target-apiRoot`.

POST /n32c-handshake/v1/exchange-capability

Negocia a capacidade de segurança N32-f com um SEPP parceiro iniciador.

Status	Causa	Condição
200	-	Negociação bem-sucedida. A resposta contém `sender` e `selectedSecCapability`.
400	`MANDATORY_IE_MISSING`	A solicitação está faltando `sender`, ou `supportedSecCapabilityList` está ausente ou vazia.
406	`INSUFFICIENT_RESOURCES`	Nenhuma capacidade de segurança N32-f suportada mutuamente.

GET /n32c-handshake/v1/status

Retorna `200` com o corpo `{"status":"UP"}`. Adequado como uma verificação de vivacidade.

Retransmissão N32-f (catch-all)

Qualquer solicitação que não seja um dos endpoints de handshake é tratada como tráfego de retransmissão N32-f. A solicitação é roteada **para fora** (para o SEPP parceiro de roaming) quando nomeia um PLMN parceiro como seu seletor de saída, caso contrário, **para dentro** (para o NF interno nomeado por `3gpp-Sbi-Target-apiRoot`).

Status	Causa	Condição
(espelhado)	-	O status e o corpo upstream são espelhados de volta em caso de sucesso (inbound ou outbound).
404	`NOT_FOUND`	Inbound: o cabeçalho `3gpp-Sbi-Target-apiRoot` está ausente, então não há alvo de roteamento.
403	`TARGET_PLMN_NOT_A_PARTNER`	Outbound: o PLMN alvo nomeado não é um parceiro de roaming configurado.
502	`TARGET_NF_NOT_REACHABLE`	A retransmissão para o NF interno (inbound) ou SEPP parceiro (outbound) falhou.

Registro NRF

Na inicialização, o OmniSEPP se registra no NRF como NFType `SEPP` (TS 23.501 §6.2.17) e envia batimentos cardíacos no intervalo configurado. O registro anuncia o endereço SBI, porta e esquema, o PLMN servido e o único serviço `n32c-handshake` `v1`.

Registrar-se no NRF local permite que consumidores locais e o SCP descubram este SEPP (TS 29.573 cl 4.2.1). O SEPP **remoto**, por contraste, é resolvido a partir da configuração estática `roaming_partners` por acordo de roaming: este é o modelo pretendido para resolução de pares inter-PLMN, uma vez que um SEPP em um PLMN não pode procurar um SEPP no NRF de outro PLMN. A ocultação de topologia também é uma configuração estática.

Os parâmetros de registro e batimento cardíaco estão documentados na Referência de Configuração.

Handshake de Saída na Inicialização

O OmniSEPP atua como o **SEPP iniciador** assim como o respondedor. Na inicialização, uma vez que o armazenamento de contexto está pronto, ele inicia uma negociação de capacidade N32-c em direção a cada parceiro de roaming configurado (`roaming_partners`) que possui um `sepp_uri` (TS 29.573 §5.2.3.2). Isso é **esforço máximo**: um parceiro inatingível ou que rejeita é registrado e ignorado em vez de interromper a inicialização, e a tarefa é executada uma vez sem reinicialização. Um parceiro que estava inacessível na inicialização ainda pode estabelecer a associação mais tarde enviando seu próprio handshake (lado do respondedor), ou na próxima reinicialização.

Notas Operacionais

- **Comportamento de reinicialização:** o armazenamento de associação N32 é persistente (apoiado por DETS). As associações são recarregadas na

reinicialização, de modo que os parceiros não precisam reexecutar o handshake N32-c para que a retransmissão seja retomada.

- **PLMNs desconhecidos:** com um registro de parceiros de roaming vazio, o encaminhamento N32-f recusa PLMNs desconhecidos. Preencha o registro antes de esperar que o tráfego do parceiro seja retransmitido.
- **Terminação TLS:** quando `sbi_scheme` é `https`, o ouvinte N32 termina o TLS usando o certificado e chave configurados e impõe TLS mútuo (certificado do cliente) quando uma CA está configurada. Consulte Referência de Configuração - TLS do Ouvinte N32.
- **PLMN padrão:** o PLMN servido padrão enviado (`999-70`) é um valor de teste e deve ser substituído por implantação.
- **Observabilidade:** opere contra logs de aplicativo estruturados; veja Métricas e Monitoramento.

Solução de Problemas do OmniSEPP

Visão Geral | Guia de Operações | Referência de Configuração | Métricas e Monitoramento

Este guia cobre problemas operacionais comuns e suas resoluções. O diagnóstico depende de logs estruturados; veja Métricas e Monitoramento.

Problemas Comuns

N32-c Handshake Rejeitado Com 400

Sintomas: A solicitação de negociação de capacidade de um SEPP parceiro é respondida com `400 MANDATORY_IE_MISSING`.

Possíveis causas:

- A solicitação está faltando a identidade `sender`.
- A `supportedSecCapabilityList` está ausente ou vazia.

Resolução:

1. Confirme que o parceiro está enviando um `SecNegotiateReqData` bem formado com um `sender` não vazio.
2. Confirme que o parceiro inclui pelo menos uma capacidade de segurança N32-f em `supportedSecCapabilityList`.

N32-c Handshake Rejeitado Com 406

Sintomas: O handshake de um parceiro é respondido com `406 INSUFFICIENT_RESOURCES` e nenhuma associação é registrada.

Possíveis causas:

- Não há capacidade comum entre as `supported_sec_capabilities` deste SEPP e a lista oferecida pelo parceiro. Por exemplo, o parceiro oferece apenas `PRINS`, enquanto este SEPP oferece apenas `TLS`.

Resolução:

1. Compare as capacidades oferecidas pelo parceiro com as `supported_sec_capabilities` deste SEPP.
2. Certifique-se de que ambos os lados compartilhem pelo menos uma capacidade. Na prática, isso significa que ambos devem suportar `TLS`; mantenha `supported_sec_capabilities` em `["TLS"]` para operação interoperável.

Tráfego N32-f Recusado para um PLMN

Sintomas: O relé N32-f é recusado, e os logs mostram uma recusa em encaminhar para um PLMN não parceiro.

Possíveis causas:

- O PLMN parceiro não está presente no registro `roaming_partners`.
- O registro está vazio (o padrão), então todos os PLMNs desconhecidos são recusados.

Resolução:

1. Adicione o PLMN parceiro a `roaming_partners`, indexado por `"mcc-mnc"`, com o `sepp_uri` do SEPP parceiro.
2. Confirme que a chave do PLMN corresponde exatamente ao `mcc-mnc` do parceiro.

Relé Inbound Retorna 404 NOT_FOUND

Sintomas: Uma solicitação de parceiro é respondida com `404 NOT_FOUND` em vez de ser encaminhada.

Possíveis causas:

- A solicitação não contém um cabeçalho `3gpp-Sbi-Target-apiRoot`, então o OmniSEPP não tem um alvo de roteamento.

Resolução:

1. Confirme que o parceiro define o cabeçalho `3gpp-Sbi-Target-apiRoot` identificando o NF interno.
2. Se a ocultação de topologia estiver em uso, confirme que o apiRoot externo apresentado pelo parceiro tem uma entrada reversa correspondente no `topology_hiding_map`.

Relé Inbound Retorna 502 TARGET_NF_NOT_REACHABLE

Sintomas: Uma solicitação de parceiro é respondida com `502 TARGET_NF_NOT_REACHABLE`.

Possíveis causas:

- O NF interno endereçado está fora do ar ou inacessível a partir do OmniSEPP.
- A ocultação de topologia não resolveu o apiRoot externo para um FQDN interno acessível.

Resolução:

1. Confirme que o NF interno resolvido a partir do apiRoot (reverso) está em execução e acessível.
2. Verifique se a entrada do `topology_hiding_map` mapeia o FQDN externo para o FQDN interno correto e resolvível.

Associações Desaparecem Após um Reinício

Sintomas: Após reiniciar o OmniSEPP, parceiros previamente estabelecidos são tratados como se nenhuma associação existisse, e o relé N32-f para eles falha até que eles façam handshake novamente.

Possíveis causas:

- O arquivo DETS em `n32_context_path` não pôde ser aberto (por exemplo, devido a corrupção ou um problema de permissões), então o armazenamento começou vazio e registrou um aviso.
- O `n32_context_path` configurado mudou entre execuções, então o arquivo anterior não está sendo lido.

Resolução:

1. Associações normalmente são persistentes e recarregadas ao reiniciar, então um reinício por si só não deve apagá-las. Se estiverem faltando, verifique os logs de inicialização para um aviso N32Context sobre a abertura do DETS.
2. Confirme que `n32_context_path` aponta para um local estável e gravável que é preservado entre reinícios (não um diretório temporário por execução).

Parceiro Não Consegue Estabelecer TLS Mutuamente Autenticado

Sintomas: Um parceiro espera N32 sobre TLS mutuamente autenticado, mas a conexão é recusada, é HTTP simples, ou o certificado do cliente do parceiro não está sendo verificado.

Possíveis causas:

- `sbi_scheme` é `http`, então o listener serve texto simples.
- `sbi_scheme` é `https`, mas `sbi_cacertfile` não está definido, então apenas o TLS do lado do servidor é encerrado e o certificado do cliente do par não `` exigido.
- `sbi_scheme` é `https`, mas `sbi_certfile` / `sbi_keyfile` não estão configurados, caso em que o OmniSEPP se recusa a iniciar em vez de rebaixar para texto simples.

Resolução:

1. Defina `sbi_scheme` como `https` e configure `sbi_certfile` e `sbi_keyfile` para que o listener encerre o TLS por conta própria.

2. Para exigir e verificar o certificado do cliente do SEPP par (TLS mútuo), defina `sbi_cacertfile` para a CA que assina o certificado do par. Veja Referência de Configuração - TLS do Listener N32.

Referência

Tópico	Especificação
Função de rede SEPP	3GPP TS 23.501 §6.2.17
Modo TLS N32-f e ocultação de topologia	3GPP TS 33.501 §13.1, §13.2
Handshake N32 e encaminhamento N32-f	3GPP TS 29.573 §5.2.3, §5.3, §6.1.5.2