OmniSEPP □置参考

□述 | 操作指南 | 指标与监控 | 故障排除

所有 OmniSEPP 配置都在 `:omnisepp` 应用程序键下。部分键可以通过环境变量进行覆盖，但这仅在 生产运行时□置 中生效。嵌套映射（`roaming_partners`，`topology_hiding_map`）和少量其他键没有环境变量，仅通过应用程序配置文件设置。

□置结构

```
config :omnisepp,
  # SBI/N32 □听器身份（向 NRF 广告）
  sbi_scheme: "http",
  sbi_addr: "127.0.0.22",
  sbi_port: 7777,

  # N32 □听器的 TLS 材料（仅在 sbi_scheme 为 "https" 时使用）
  sbi_certfile: nil,
  sbi_keyfile: nil,
  sbi_cacertfile: nil,

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

  # 提供的 PLMN（按部署覆盖）
  mcc: "999",
  mnc: "70",

  # 此 SEPP 的身份和协商能力
  sepp_fqdn: "sepp.5gc.mnc70.mcc999.3gppnetwork.org",
  supported_sec_capabilities: ["TLS"],

  # N32 关联上下文持久性（仅配置文件）
  n32_context_path: "<priv>/data/n32_context.dets",

  # 漫游和拓扑隐藏（仅配置文件）
  roaming_partners: %{},
  topology_hiding_map: %{}
```

以上每个参数在下面都有文档说明。

□□□□

□□	□□	□□	□□	
`sbi_scheme`	□□□	□	`http`	`SEPP_S`
`sbi_addr`	□□□	□	`127.0.0.22`	`SEPP_S`
`sbi_port`	□□	□	`7777`	`SEPP_S`
`sbi_certfile`	□□□ □□□	□□□	(□)	`SEPP_S`
`sbi_keyfile`	□□□ □□□	□□□	(□)	`SEPP_S`

□□	□□	□□	□□	
`sbi_cacertfile`	□□□□□□□	□	(□)	`SEPP_S`
`nrf_uri`	□□□	□	`http://127.0.0.10:7777`	`SEPP_N`
`mcc`	□□□	□	`999`	`SEPP_N`
`mnc`	□□□	□	`70`	`SEPP_N`
`heartbeat_interval`	□□□□□□	□	`10000`	(□)
`sepp_fqdn`	□□□	□	□□□□□□□	`SEPP_F`
`supported_sec_capabilities`	□□□□□□	□	`["TLS"]`	`SEPP_S`
`n32_context_path`	□□□	□	□□□□□□□	(□)

参数	类型	必需	默认	
	（路径）			
`roaming_partners`	映射	否	`%{}`	（无）
`topology_hiding_map`	映射	否	`%{}`	（无）

sepp_fqdn

当 `sepp_fqdn` 未设置时，它是从提供的 PLMN 派生的：

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

对于默认 PLMN `999-70`，这将产生 `sepp.5gc.mnc70.mcc999.3gppnetwork.org`。此 FQDN 作为 `sender` 身份在 N32-c 握手请求和响应中发送（TS 29.573）。当派生形式与漫游伙伴期望的 FQDN 不匹配时，请显式覆盖它。

N32 监听器 TLS

当 `sbi_scheme` 为 `https` 时，N32 监听器自行终止 TLS，而不是依赖外部终止器。这是 N32-f TLS 模式（TS 33.501 §13.1），其中两个 SEPP 通过 TLS 保护它们之间的接口。

- 当 `sbi_scheme` 为 `https` 时，`sbi_certfile` 和 `sbi_keyfile` 都是必需的。如果缺少任何一个，SEPP 将拒绝启动，而不是静默降级为明文。
- 当 `sbi_cacertfile` 也设置时，监听器要求并验证对等 SEPP 的客户端证书与该 CA 的匹配，从而实现双向认证的 TLS。如果未配置 CA，则仅终止服务器端 TLS。
- 当 `sbi_scheme` 为 `http`（默认值）时，这些密钥将被忽略，监听器提供明文服务。

在 NRF 注册中广告的方案遵循 `sbi_scheme`，因此它现在反映了监听器的实际传输。

supported_sec_capabilities

此 SEPP 支持的 N32-f 安全能力，按本地优先顺序（优先级最高的在前）。在 N32-c 握手期间，OmniSEPP 选择此列表中第一个对等方也提供的条目（TS 29.573 §5.2.3.2.2）。

值	意义	参考
`TLS`	SEPP 之间的传输层保护。	TS 33.501 §13.1
`PRINS`	通过插入中间安全性进行保护（通过漫游中心的 JOSE 应用层保护）。	TS 33.501 §13.2

仅识别这两个值；任何其他条目将被忽略。默认值为 `["TLS"]`；为了互操作性，请保持为 `["TLS"]`。

通过 `SEPP_SEC_CAPABILITIES` 环境变量进行覆盖时，请提供一个以逗号分隔的优先顺序列表，例如 `TLS,PRINS`。每个条目周围的空格将被修剪。

N32 上下文持久性

已建立的 N32 关联被持久化到 `n32_context_path` 的 DETS 文件中，���此它们在进程或节点重启后仍然存在（TS 29.573）。在启动时，存储会重新加载持久化的关联，因此合作伙伴在 OmniSEPP 重启后无需重新运行 N32-c 握手。

- 当未设置时，路径默认为 OTP 应用程序的 `priv` 数据目录下的 `n32_context.dets`。如果该父目录不存在，则在启动时会创建。
- 如果文件无法打开（例如由于损坏），存储会记录警告并以空的内存表启动，而不是崩溃启动；然后通过握手重新建立关联。
- 此键没有环境变量，仅通过应用程序配置文件设置。

漫游伙伴

`roaming_partners` 映射是漫游伙伴 PLMN 的静态允许列表。它以 `"mcc-mnc"` 形式的伙伴 PLMN 标识符为键，每个值是一个伙伴规范。

```
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"
    }
  }
```

顶级结构：

键形式	类型	描述
`"mcc-mnc"`	字符串（映射键）	伙伴 PLMN 标识符，例如 `"001-01"`。
值	映射	伙伴规范（见下文）。

伙伴规范：

参数	类型	必需	默认	
`sepp_uri`	字符串	是	-	伙伴 SEPP 的 API [N32-f 流量转发到此。
`sec_capabilities`	字符串列表	否	继承 `supported_sec_capabilities`	与此伙伴允许的 N32-f 承此 SEPP 的 `supported_sec`

空的 `roaming_partners` 映射（默认值）表示未配置任何漫游伙伴，N32-f 转发拒绝所有未知 PLMN。此映射没有环境变量，仅通过应用程序配置文件设置。

拓扑隐藏映射

`topology_hiding_map` 实现 FQDN 重写以进行拓扑隐藏 (TS 33.501 §13.2)。它将每个内部 NF FQDN 映射到呈现给漫游伙伴的外部 FQDN。

```
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"
  }
```

键形式	类型	描述
`internal_fqdn`	字符串（映射键）	要被掩盖的内部 NF FQDN，例如 AMF 或 UDM FQDN。
`external_fqdn`	字符串（值）	代替��呈现给伙伴的外部 FQDN。

该映射在 `3gpp-Sbi-Target-apiRoot`、`Location` 和 producer-id 头值的出站（内部到外部）上应用，并在入站（外部到内部）上反转，以便伙伴呈现的 apiRoots 能够解析回真实的内部 FQDN。空映射（默认值）表示没有重写。此映射没有环境变量，仅通过应用程序配置文件设置。

环境变量摘要

环境变量仅适用于生产运行时配置。未在此列出的键仅适用于配置文件。

环境变量	参数	备注
`SEPP_SBI_SCHEME`	`sbi_scheme`	`http` 或 `https`。
`SEPP_SBI_ADDR`	`sbi_addr`	
`SEPP_SBI_PORT`	`sbi_port`	解析为整数。
`SEPP_SBI_CERTFILE`	`sbi_certfile`	当方案为 `https` 时必需。
`SEPP_SBI_KEYFILE`	`sbi_keyfile`	当方案为 `https` 时必需。
`SEPP_SBI_CACERTFILE`	`sbi_cacertfile`	设置以启用 N32-f 双向 TLS（对等客户端证书验证）。
`SEPP_NRF_URI`	`nrf_uri`	
`SEPP_MCC`	`mcc`	
`SEPP_MNC`	`mnc`	
`SEPP_FQDN`	`sepp_fqdn`	当未设置时，FQDN 从 PLMN 派生。
`SEPP_SEC_CAPABILITIES`	`supported_sec_capabilities`	以逗号分隔的优先顺序。

置示例

一个现实的每个部署覆盖示例，适用于家庭 PLMN `310-260`，并有一个���游伙伴：

```
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"
  }
```

工作原理：OmniSEPP 向 NRF 广告其在 `10.20.0.5:7777` 的身份为 NFType `SEPP`，适用于 PLMN `310-260`，每 10 秒进行一次心跳。由于 `sbi_scheme` 为 `https`，N32 监听器使用 `sepp.crt` / `sepp.key` 终止 TLS，并且由于 `sbi_cacertfile` 已设置，它要求并验证伙伴 SEPP 的客户端证书与 `partner-ca.crt` 的匹配（双向 TLS）。它接受 N32-c 握手作为 `sepp.5gc.mnc260.mcc310.3gppnetwork.org`，协商 TLS 作为唯一的 N32-f 能力，并在启动时发起与伙伴 `001-01` 的出站握手。N32-f 流量仅在伙伴 PLMN `001-01` 之间转发，内部 AMF FQDN 在该伙伴面前被隐藏在 SEPP FQDN 后面。

OmniSEPP 指标和监控

□述 | 操作指南 | 配置参考 | 故障排除

可观察性

可观察性通过 结构化应用日志 和标准请求日志提供。操作员通过日志监控 OmniSEPP，这些日志捕获了下面描述的握手、转发和请求事件。

日志中需要关注的内容

应用日志是操作 OmniSEPP 的主要信号。以下类别的事件被记录，值得关注。

N32-c 握手结果

每次能力协商都会记录其结果，包括远程 SEPP 身份和成功时选择的 N32-f 安全能力。关注这些以确认：

- 预期的漫游合作伙伴正在完成握手。
- 选择的能力符合您的意图（例如 `TLS`）。
- 由于无法选择共同能力而拒绝了一个合作伙伴。

选择了此 SEPP 未提供的能力（在发起者路径上）的对等方将被记录为警告并被拒绝。

N32-f 转发决策和失败

N32-f 中继记录其转发决策和失败，包括：

- 拒绝转发到未配置的漫游合作伙伴的 PLMN。此类事件的上升率表明缺少或配置错误的 `roaming_partners` 条目。
- 入站和出站中继目标（解析的 URL 和方向）。
- 转发失败，这会以 `502 TARGET_NF_NOT_REACHABLE` 的形式浮现给合作伙伴，表示目标内部 NF 无法访问。

请求日志

标准请求日志涵盖了监听器处理的每个 SBI 请求，包括握手端点和 N32-f 捕获所有的中继。使用它来观察请求量、方法和路径，并将合作伙伴活动与握手和转发事件关联起来。

健康检查

健康状态通过以下方式评估：

- 存活性：`GET /n32c-handshake/v1/status` 返回 `200 {"status":"UP"}` 当 SBI 监听器正在服务时。请参见 操作指南。
- **NRF** 注册：确认 OmniSEPP 作为 `SEPP` NF 实例出现在 NRF 中并正在发送心跳。注册行为在 操作指南 中描述。
- 日志信号：上述握手和转发事件。

OmniSEPP 操作指南

□述 | 配置参考 | 指标和监控 | 故障排除

本指南描述了 OmniSEPP 在 N32 互 PLMN 边缘的行为以及如何操作它。OmniSEPP 是在 3GPP TS 23.501 §6.2.17 中定义的安全边缘保护代理，具有来自 3GPP TS 33.501 的安全行为和来自 3GPP TS 29.573 的 N32 接口。

目录

- 架构□述
- N32 接口
- N32 关联生命周期
- 能力协商
- 漫游伙伴限制
- 拓扑隐藏
- 消息流
- SBI 端点
- NRF 注册
- 操作说明

架构概述

OmniSEPP 终止与漫游伙伴 SEPP 的 N32 接口，并将流量转发到本地 PLMN 的内部网络功能。它以 NFType `SEPP` 向本地 NRF 注册，以便本地消费者和 SCP 可以发现它；远程对等 SEPP 和拓扑隐藏映射是根据漫游协议的静态配置（对等 SEPP 不通过 NRF 发现）。

N32 接口

N32 有两个逻辑通道 (TS 29.573):

- **N32-c**（控制通道） - 用于协商 N32-f 安全能力并建立两个 SEPP 之间的关联的握手。OmniSEPP 将其公开为 `/n32c-handshake/v1/exchange-capability` 端点（响应者角色），并在启动时向每个配置的漫游伙伴发起握手（发起者角色）。
- **N32-f**（转发通道） - 两个 PLMN 之间基于服务的（SBI）消息的持续交换。OmniSEPP 在 **TLS** 模式下转发这些消息：消息基本上逐字转发，应用逐跳头部卫生和拓扑隐藏。

N32 关联生命周期

每次成功的 N32-c 协商都会在 持久上下文存储（由内存缓存前端的 DETS 表）中记录一个关联，使用远程 SEPP FQDN 作为键。存储的上下文包括所选的 N32-f 安全能力和合作 PLMN 身份列表。

关键操作属性：

- 存储是 持久的：关联写入 `n32_context_path` 的 DETS 文件，并在启动时重新加载，因此它们在进程或节点重启后仍然存在。合作伙伴在 OmniSEPP 重启后不必重新握手。
- 没有 **TTL**：关联持续存在，直到显式拆除（删除）或被新的协商替换。
- 如果 DETS 文件无法打开（例如由于损坏），存储将为空并记录警告；然后通过握手重新建立关联。

能力协商

在 N32-c 握手期间��两个 SEPP 同意一个 N32-f 安全能力。有效的能力是 `TLS` 和 `PRINS` (TS 33.501 §13.1)。

选择规则 (TS 29.573 §5.2.3.2.2) 是 本地优先：OmniSEPP 按顺序遍历其配置的 `supported_sec_capabilities` 列表，并选择第一个对等方也提供的条目。如果两个能力集不相交，则协商失败，返回 `INSUFFICIENT_RESOURCES`（HTTP 406），并且不记录关联。

仅广告格式正确、被认可的能力（`TLS`，`PRINS`）。保持 `supported_sec_capabilities` 为 `["TLS"]` 以实现互操作性。有关如何设置优先顺序，请参见 配置参考。

漫游伙伴限制

漫游伙伴注册表是一个静态允许列表，以合作 PLMN（`"mcc-mnc"`）为键。它控制 N32-f 转发：

- 仅转发注册表中存在的 PLMN。
- 空注册表（默认）意味着 N32-f 转发拒绝所有未知 PLMN。
- 每个合作伙伴条目携带合作伙伴 SEPP API 根，并可选地携带与该合作伙伴允许的 N32-f 安全能力。当省略能力列表时，合作伙伴继承该 SEPP 的 `supported_sec_capabilities`。

有关映射结构，请参见 配置参考 - 漫游伙伴。

拓扑隐藏

拓扑隐藏 (TS 33.501 §13.2) 通过重写 FQDN 来掩盖内部 NF 身份，以防止漫游伙伴识别。OmniSEPP 应用运营商配置的 `internal_fqdn => external_fqdn` 映射：

- 出站（朝向合作伙伴）：`3gpp-Sbi-Target-apiRoot`、`Location` 和生产者 ID 头部值中的内部 FQDN 被重写为其外部等价物。
- 入站（来自合作伙伴）：应用反向映射，以便外部呈现的 apiRoot 在请求路由到内部 NF 之前解析回真实的内部 FQDN。

重写锚定到 完整 **FQDN** 令牌：仅当映射的 FQDN 作为完整主机出现（由 URL 分隔符如 `/`、`:`、`@` 或值的结尾界定）时，才会进行重写，而不会作为较长主机名的子字符串出现。这防止了映射损坏与映射名称无关的主机，并阻止了一个映射产生的值被另一个映射条目重新匹配。

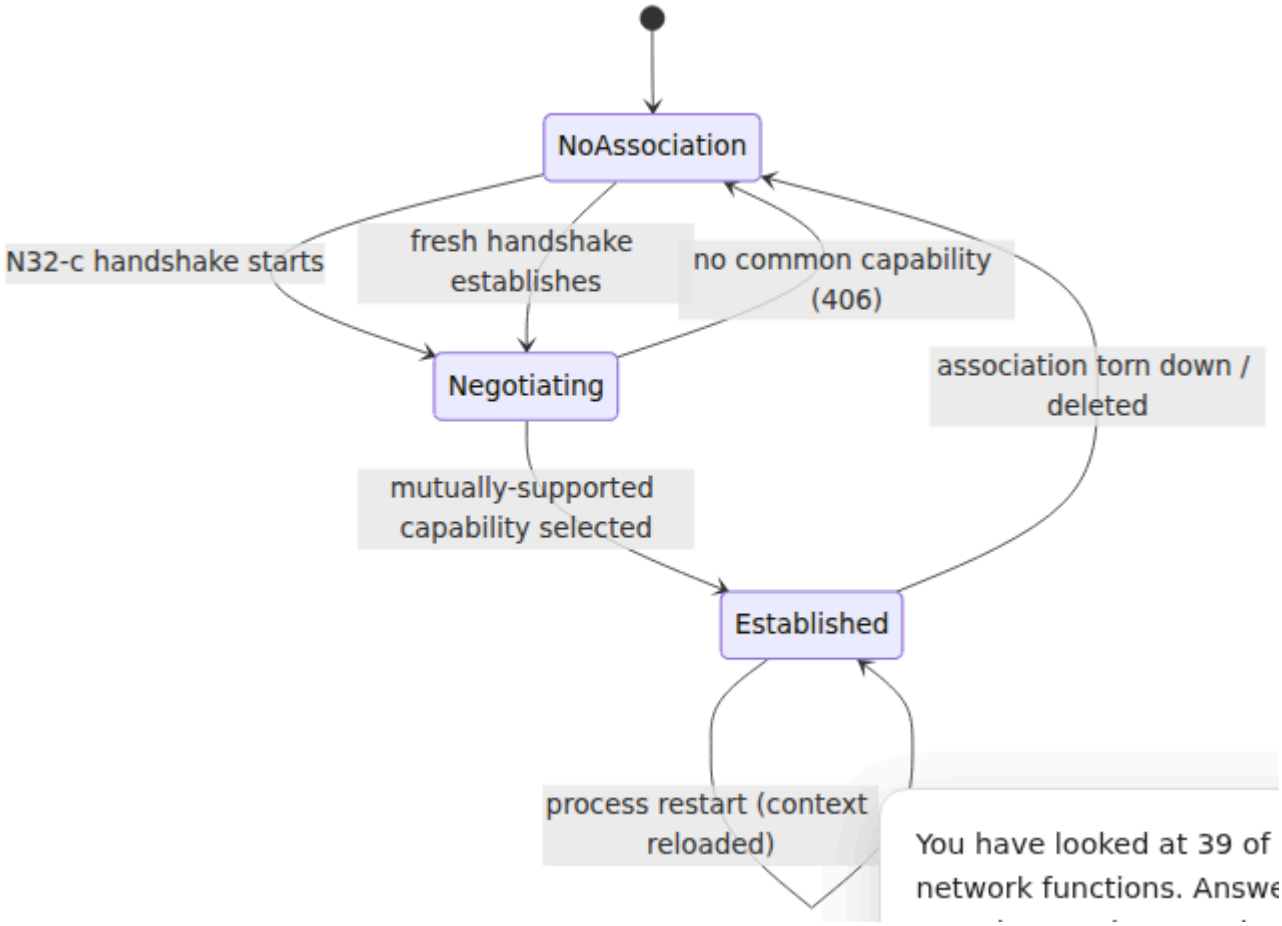
在每次转发时，逐跳头部（`host`、`content-length`、`connection`）被剥离。在入站路径上，(现已消耗的) `3gpp-Sbi-Target-apiRoot` 头部在请求到达内部 NF 之前也被丢弃。

空拓扑隐藏映射（默认）意味着不执行重写。有关详细信息，请参见 配置参考 - 拓扑隐藏映射。

消息流

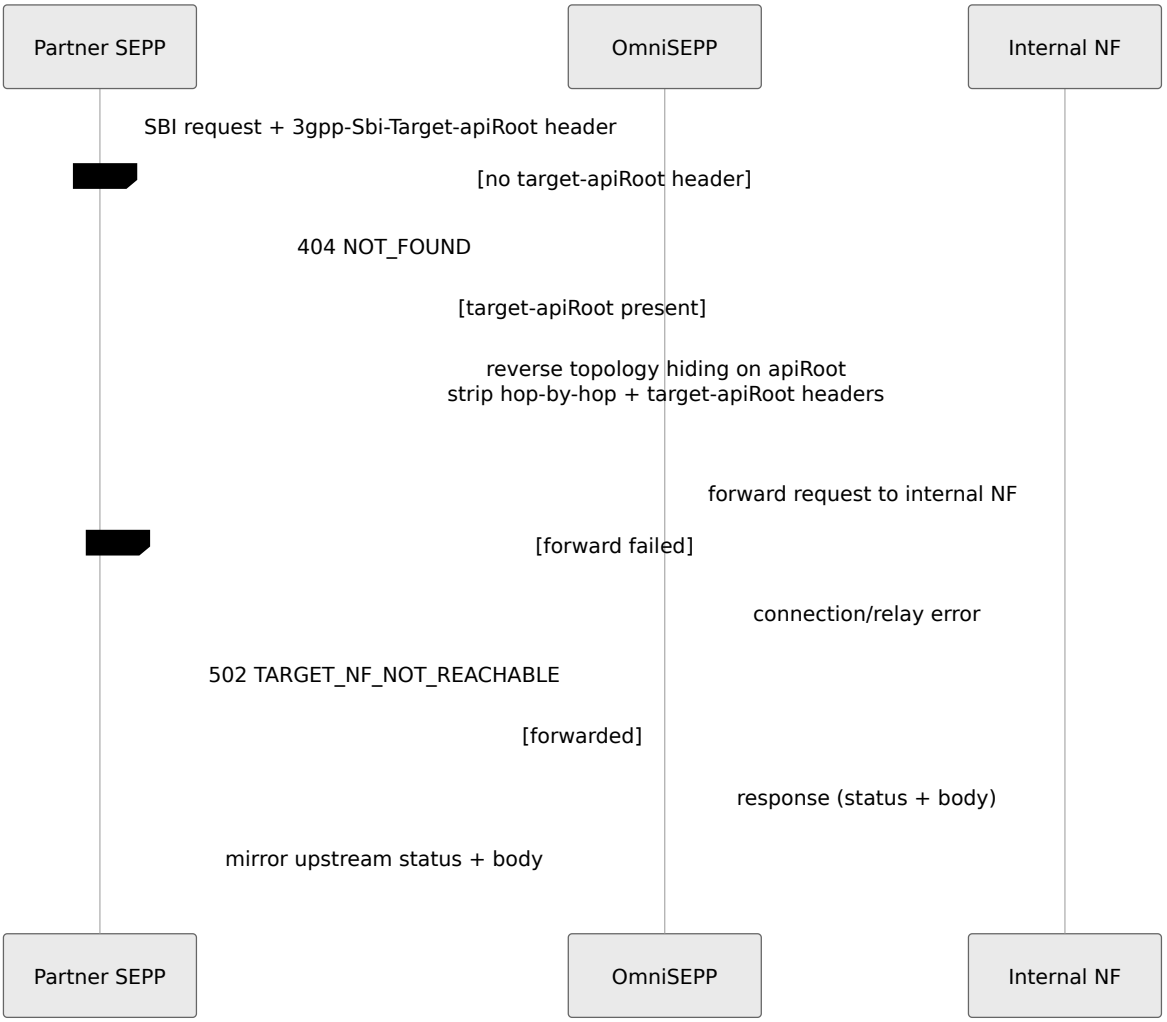
N32-c 握手（响应者）

漫游伙伴 SEPP 通过 POST 发送能力协商请求来发起握手。OmniSEPP 选择一个共同支持的能力，记录关联并回复。



N32-f 入站转发

合作伙伴 SEPP 发送一个携带 `3gpp-Sbi-Target-apiRoot` 头部的 SBI 请求，标识内部 NF。OmniSEPP 反转拓扑隐藏，剥离逐跳和路由头部，并转发请求，镜像上游响应。



SBI 端点

OmniSEPP 通过其 SBI HTTP 监听器公开以下内容。N32-c 握手广告一个 NRF 服务，`n32c-handshake` 版本 `v1`。

方法	路径	目的
POST	`/n32c-handshake/v1/exchange-capability`	N32-c 安全能力协商（响应者）。
GET	`/n32c-handshake/v1/status`	存活探测。
(任何)	任何其他路径	N32-f 转发。当请求命名一个合作伙伴 PLMN 时，路由到漫游伙伴 SEPP，否则路由到由 `3gpp-Sbi-Target-apiRoot` 命名的内部 NF。

POST /n32c-handshake/v1/exchange-capability

与发起的合作伙伴 SEPP 协商 N32-f 安全能力。

状态	原因	条件
200	-	协商成功。响应携带 `sender` 和 `selectedSecCapability`。
400	`MANDATORY_IE_MISSING`	请求缺少 `sender`，或 `supportedSecCapabilityList` 缺失或为空。
406	`INSUFFICIENT_RESOURCES`	没有共同支持的 N32-f 安全能力。

GET /n32c-handshake/v1/status

返回 `200` 和主体 `{"status":"UP"}`。适合作为存活探测。

N32-f 转发（捕获所有）

任何不是握手端点的请求都被视为 N32-f 转发流量。当请求将合作伙伴 PLMN 作为其出口选择器命名时，请求被路由 出站（到漫游伙伴 SEPP），否则 入站（到由 `3gpp-Sbi-Target-apiRoot` 命名的内部 NF）。

状态	原因	条件
(镜像)	-	上游状态和主体在成功时（入站或出站）被镜像返回。
404	`NOT_FOUND`	入站：缺少 `3gpp-Sbi-Target-apiRoot` 头部，因此没有路由目标。
403	`TARGET_PLMN_NOT_A_PARTNER`	出站：命名的目标 PLMN 不是配置的漫游伙伴。
502	`TARGET_NF_NOT_REACHABLE`	转发到内部 NF（入站）或合作伙伴 SEPP（出站）失败。

NRF 注册

在启动时，OmniSEPP 作为 NFType `SEPP` 向 NRF 注册 (TS 23.501 §6.2.17)，并在配置的间隔上进行心跳。注册广告 SBI 地址、端口和方案、服务的 PLMN，以及单个 `n32c-handshake` `v1` 服务。

向本地 NRF 注册使本地消费者和 SCP 可以发现此 SEPP (TS 29.573 cl 4.2.1)。远程对等 SEPP 则通过静态 `roaming_partners` 配置根据漫游协议解析：这是跨 PLMN 对等解析的预期模型，因为一个 PLMN 中的 SEPP 无法查找另一个 PLMN 的 NRF 中的 SEPP。拓扑隐藏同样是静态配置。

注册和心跳参数在 配置参考 中有文档说明。

启动时的出站握手

OmniSEPP 既充当 发起 **SEPP** 也充当响应者。在启动时，一旦上下文存储准备就绪，它会向每个配置的漫游伙伴（`roaming_partners`）发起 N32-c 能力协商，该伙伴具有 `sepp_uri` (TS 29.573 §5.2.3.2)。这是 尽力而为：无法到达或拒绝的合作伙伴会被记录并跳过，而不会导致启动崩溃，任务运行一次而不重启。在启动时无法到达的合作伙伴仍然可以通过发送自己的（响应者侧）握手或在下次重启时建立关联。

操作说明

- 重启行为： N32 关联存储是持久的（基于 DETS）。关联在重启时重新加载，因此合作伙伴不必重新运行 N32-c 握手以恢复转发。

- 未知 **PLMN**：在空漫游伙伴注册表中，N32-f 转发拒绝未知 PLMN。在期望合作伙伴流量被转发之前，请填充注册表。
- **TLS** 终止：当 `sbi_scheme` 为 `https` 时，N32 监听器使用配置的证书和密钥自行终止 TLS，并在配置 CA 时强制执行双向（客户端证书）TLS。有关详细信息，请参见 配置参考 - N32 监听器 TLS。
- 默认 **PLMN**：随附的默认服务 PLMN（`999-70`）是测试值，必须根据部署进行覆盖。
- 可观察性：通过结构化应用日志进行操作；请参见 指标和监控。

OmniSEPP 故障排除

□述 | 操作指南 | 配置参考 | 指标与监控

本指南涵盖常见的操作问题及其解决方案。诊断依赖于结构化日志；请参见 指标与监控。

常见问题

N32-c 握手被拒绝，状态码 400

症状：伙伴 SEPP 的能力协商请求以 `400 MANDATORY_IE_MISSING` 回应。

可能原因：

- 请求缺少 `sender` 身份。
- `supportedSecCapabilityList` 缺失或为空。

解决方案：

1. 确认伙伴发送了格式正确的 `SecNegotiateReqData`，并且 `sender` 不为空。
2. 确认伙伴在 `supportedSecCapabilityList` 中至少包含一个 N32-f 安全能力。

N32-c 握手被拒绝，状态码 406

症状：伙伴的握手以 `406 INSUFFICIENT_RESOURCES` 回应，并且没有记录关联。

可能原因：

- 该 SEPP 的 `supported_sec_capabilities` 和伙伴提供的列表之间没有共同的能力。例如，伙伴只提供 `PRINS`，��该 SEPP 只提供 `TLS`。

解决方案：

1. 将伙伴提供的能力与该 SEPP 的 `supported_sec_capabilities` 进行比较。
2. 确保双方至少共享一个能力。在实践中，这意味着双方都必须支持 `TLS`；将 `supported_sec_capabilities` 保持为 `["TLS"]` 以实现互操作。

N32-f 流量被拒绝，针对某个 PLMN

症状： N32-f 中继被拒绝，日志显示拒绝转发到非伙伴 PLMN。

可能原因：

- 伙伴 PLMN 不在 `roaming_partners` 注册表中。
- 注册表为空（默认情况），因此所有未知 PLMN 都被拒绝。

解决方案：

1. 将伙伴 PLMN 添加到 `roaming_partners`，以 `"mcc-mnc"` 为键，值为伙伴 SEPP 的 `sepp_uri`。
2. 确认 PLMN 键与伙伴的 `mcc-mnc` 完全匹配。

入站中继返回 404 NOT_FOUND

症状：伙伴请求以 `404 NOT_FOUND` 回应，而不是被中继。

可能原因：

- 请求未携带 `3gpp-Sbi-Target-apiRoot` 头，因此 OmniSEPP 没有路由目标。

解决方案：

1. 确认伙伴设置了 `3gpp-Sbi-Target-apiRoot` 头以识别内部 NF。
2. 如果使用了拓扑隐藏，确认伙伴提供的外部 apiRoot 在 `topology_hiding_map` 中有匹配的反向条目。

入站中继返回 502 TARGET_NF_NOT_REACHABLE

症状：伙伴请求以 `502 TARGET_NF_NOT_REACHABLE` 回应。

可能原因：

- 指定的内部 NF 已关闭或从 OmniSEPP 无法访问。
- 拓扑隐藏未能将外部 apiRoot 解析为可访问的内部 FQDN。

解决方案：

1. 确认从（反向）apiRoot 解析的内部 NF 正在运行并且可访问。

2. 检查 `topology_hiding_map` 条目是否将外部 FQDN 映射到正确的、可解析的内部 FQDN。

重启后关联消失

症状：重启 OmniSEPP 后，之前建立的伙伴被视为没有关联，N32-f 中继失败，直到它们再次握手。

可能原因：

- `n32_context_path` 处的 DETS 文件无法打开（例如由于损坏或权限问题），因此存储从空开始并记录了警告。
- 在运行之间配置的 `n32_context_path` 发生了变化，因此未读取之前的文件。

解决方案：

1. 关联通常是持久的，并在重启时重新加载，因此仅重启不应清除它们。如果缺失，请检查启动日志中是否有关于打开 DETS 的 N32Context 警告。
2. 确认 `n32_context_path` 指向一个稳定的、可写的位置，该位置在重启之间保持不变（而不是每次运行的临时目录��。

伙伴无法建立相互认证的 **TLS**

症状：伙伴期望通过相互认证的 TLS 进行 N32，但连接被拒绝、是明文 HTTP，或伙伴的客户端证书未被验证。

可能原因：

- `sbi_scheme` 为 `http`，因此监听器提供明文服务。
- `sbi_scheme` 为 `https`，但未设置 `sbi_cacertfile`，因此仅服务器端 TLS 被终止，且不需要对等方的客户端证书。
- `sbi_scheme` 为 `https`，但未配置 `sbi_certfile` / `sbi_keyfile`，在这种情况下，OmniSEPP 拒绝启动，而不是降级为明文。

解决方案：

1. 将 `sbi_scheme` 设置为 `https`，并配置 `sbi_certfile` 和 `sbi_keyfile`，以便监听器自行终止 TLS。
2. 要求并验证对等 SEPP 的客户端证书（相互 TLS），请将 `sbi_cacertfile` 设置为签署对等证书的 CA。请参见 配置参考 - N32 监听器 TLS。

参考

主题	规范
SEPP 网络功能	3GPP TS 23.501 §6.2.17
N32-f TLS 模式和拓扑隐藏	3GPP TS 33.501 §13.1, §13.2
N32 握手和 N32-f 转发	3GPP TS 29.573 §5.2.3, §5.3, §6.1.5.2