Référence de configuration OmniSEPP

Vue d'ensemble | Guide des opérations | Métriques et surveillance | Dépannage

Toute la configuration d'OmniSEPP se trouve sous la clé d'application `:omnisepp`. Un sous-ensemble de clés peut être remplacé par des variables d'environnement, mais cela n'entre en vigueur que dans la **configuration d'exécution de production**. Les cartes imbriquées (`roaming_partners`, `topology_hiding_map`) et un petit nombre d'autres clés n'ont pas de variable d'environnement et sont définies uniquement via le fichier de configuration de l'application.

Structure de configuration

```
config :omnisepp,
  # Identité de l'auditeur SBI/N32 (annoncée au NRF)
  sbi_scheme: "http",
  sbi_addr: "127.0.0.22",
  sbi_port: 7777,

  # Matériel TLS pour l'auditeur N32 (utilisé uniquement lorsque
sbi_scheme est "https")
  sbi_certfile: nil,
  sbi_keyfile: nil,
  sbi_cacertfile: nil,

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

  # PLMN servi (remplacement par déploiement)
  mcc: "999",
  mnc: "70",

  # Identité propre de ce SEPP et capacités négociées
  sepp_fqdn: "sepp.5gc.mnc70.mcc999.3gppnetwork.org",
  supported_sec_capabilities: ["TLS"],

  # Persistance du contexte d'association N32 (fichier de
configuration uniquement)
  n32_context_path: "<priv>/data/n32_context.dets",

  # Roaming et masquage topologique (fichier de configuration
uniquement)
  roaming_partners: %{},
  topology_hiding_map: %{}
```

Chaque paramètre ci-dessus est documenté ci-dessous.

Paramètres principaux

Paramètre	Type	Requis	Par défaut
`sbi_scheme`	String	Non	`http`
`sbi_addr`	String	Non	`127.0.0.22`
`sbi_port`	Integer	Non	`7777`
`sbi_certfile`	String (path)	Conditionnel	(aucun)

Paramètre	Type	Requis	Par défaut
`sbi_keyfile`	String (path)	Conditionnel	(aucun)
`sbi_cacertfile`	String (path)	Non	(aucun)
`nrf_uri`	String	Non	`http://127.0.0.1`
`mcc`	String	Non	`999`

Paramètre	Type	Requis	Par défaut
`mnc`	String	Non	`70`
`heartbeat_interval`	Integer (ms)	Non	`10000`
`sepp_fqdn`	String	Non	dérivé (voir ci-dess
`supported_sec_capabilities`	Liste de String	Non	`["TLS"]`

Paramètre	Type	Requis	Par défaut
`n32_context_path`	String (path)	Non	dérivé (voir ci-dess
`roaming_partners`	Map	Non	`%{}`
`topology_hiding_map`	Map	Non	`%{}`

sepp_fqdn

Lorsque `sepp_fqdn` n'est pas défini, il est dérivé du PLMN servi comme suit :

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

Pour le PLMN par défaut `999-70`, cela donne `sepp.5gc.mnc70.mcc999.3gppnetwork.org`. Ce FQDN est envoyé comme identité `sender` dans les demandes et réponses de handshake N32-c (TS 29.573). Remplacez-le explicitement lorsque la forme dérivée ne correspond pas au FQDN que vos partenaires de roaming attendent.

TLS de l'auditeur N32

Lorsque `sbi_scheme` est `https`, l'auditeur N32 termine lui-même TLS plutôt que de s'appuyer sur un terminateur externe. C'est le mode TLS N32-f (TS 33.501 §13.1), dans lequel deux SEPP protègent l'interface avec TLS entre eux.

- `sbi_certfile` et `sbi_keyfile` sont **tous deux requis** lorsque `sbi_scheme` est `https`. Si l'un d'eux est manquant, le SEPP refuse de démarrer plutôt que de rétrograder silencieusement en texte clair.
- Lorsque `sbi_cacertfile` est également défini, l'auditeur exige et vérifie le certificat client du SEPP pair contre cette CA, offrant un TLS mutuellement authentifié. Sans CA configurée, seul le TLS côté serveur est terminé.
- Lorsque `sbi_scheme` est `http` (la valeur par défaut), ces clés sont ignorées et l'auditeur sert en texte clair.

Le schéma annoncé dans l'enregistrement NRF suit `sbi_scheme`, il reflète donc maintenant le transport réel de l'auditeur.

capacités_sec_soutenus

Les capacités de sécurité N32-f que ce SEPP prend en charge, dans **ordre de préférence local** (le plus préféré en premier). Pendant le handshake N32-c, OmniSEPP sélectionne la première entrée de cette liste que le pair propose également (TS 29.573 §5.2.3.2.2).

Valeur	Signification	Référence
`TLS`	Protection au niveau du transport entre les SEPP.	TS 33.501 §13.1
`PRINS`	Protection avec insertion de sécurité intermédiaire (protection au niveau de l'application JOSE via un hub de roaming).	TS 33.501 §13.2

Seules ces deux valeurs sont reconnues ; toute autre entrée est ignorée. La valeur par défaut est `["TLS"]`; gardez-la à `["TLS"]` pour un fonctionnement interopérable.

Lors du remplacement via la variable d'environnement `SEPP_SEC_CAPABILITIES`, fournissez une liste séparée par des virgules dans l'ordre de préférence, par exemple `TLS,PRINS`. Les espaces autour de chaque entrée sont supprimés.

Persistance du contexte N32

Les associations N32 établies sont persistées dans un fichier DETS à `n32_context_path`, de sorte qu'elles survivent à un redémarrage de processus ou de nœud (TS 29.573). Au démarrage, le magasin recharge les associations persistées, de sorte qu'un partenaire n'a pas à relancer le handshake N32-c après un redémarrage d'OmniSEPP.

- Lorsqu'il n'est pas défini, le chemin par défaut est `n32_context.dets` sous le répertoire de données `priv` de l'application OTP. Le répertoire parent est créé au démarrage s'il n'existe pas.
- Si le fichier ne peut pas être ouvert (par exemple en cas de corruption), le magasin enregistre un avertissement et démarre avec une table en mémoire vide plutôt que de planter au démarrage ; les associations sont ensuite rétablies par handshake.
- Cette clé n'a pas de variable d'environnement et est définie uniquement via le fichier de configuration de l'application.

Partenaires de roaming

La carte `roaming_partners` est la liste blanche statique des PLMN partenaires de roaming. Elle est indexée par l'identifiant PLMN du partenaire sous la forme `"mcc-mnc"`, et chaque valeur est une spécification de partenaire.

```
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"
    }
  }
```

Structure de niveau supérieur :

Forme de clé	Type	Description
`"mcc-mnc"`	String (clé de carte)	Identifiant PLMN du partenaire, par exemple `"001-01"`.
valeur	Map	Spécification du partenaire (voir ci-dessous).

Spécification du partenaire :

Paramètre	Type	Requis	Par défaut	
`sepp_uri`	String	Oui	-	La r par aut N32
`sec_capabilities`	Liste de String	Non	hérite de `supported_sec_capabilities`	Cap aut par om des `sup` de

Une carte `roaming_partners` vide (la valeur par défaut) signifie qu'aucun partenaire de roaming n'est configuré, et le transfert N32-f refuse tous les PLMN inconnus. Cette carte n'a pas de variable d'environnement et est définie uniquement via le fichier de configuration de l'application.

Carte de masquage topologique

La carte `topology_hiding_map` implémente la réécriture FQDN pour le masquage topologique (TS 33.501 §13.2). Elle associe chaque FQDN NF interne au FQDN externe présenté aux partenaires 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"
  }
```

Forme de clé	Type	Description
`internal_fqdn`	String (clé de carte)	Le FQDN NF interne à masquer, par exemple un FQDN AMF ou UDM.
`external_fqdn`	String (valeur)	Le FQDN externe présenté aux partenaires à sa place.

La correspondance est appliquée sortante (interne à externe) sur les valeurs d'en-tête `3gpp-Sbi-Target-apiRoot`, `Location`, et producer-id, et inversée entrante (externe à interne) afin que les apiRoots présentés par le partenaire se résolvent à nouveau sur le véritable FQDN interne. Une carte vide (la valeur par défaut) signifie qu'aucune réécriture n'est effectuée. Cette carte n'a pas de variable d'environnement et est définie uniquement via le fichier de configuration de l'application.

Résumé des variables d'environnement

Les variables d'environnement s'appliquent uniquement dans la configuration d'exécution de production. Les clés non listées ici sont uniquement pour le fichier de configuration.

Variable d'environnement	Paramètre	Remarques
`SEPP_SBI_SCHEME`	`sbi_scheme`	`http` ou `https`.
`SEPP_SBI_ADDR`	`sbi_addr`	
`SEPP_SBI_PORT`	`sbi_port`	Interprété comme un entier.
`SEPP_SBI_CERTFILE`	`sbi_certfile`	Requis lorsque le schéma est `https`.
`SEPP_SBI_KEYFILE`	`sbi_keyfile`	Requis lorsque le schéma est `https`.
`SEPP_SBI_CACERTFILE`	`sbi_cacertfile`	Défini pour activer le TLS mutuel N32-f (vérification du certificat client pair).
`SEPP_NRF_URI`	`nrf_uri`	
`SEPP_MCC`	`mcc`	
`SEPP_MNC`	`mnc`	
`SEPP_FQDN`	`sepp_fqdn`	Lorsqu'il n'est pas défini, le FQDN est

Variable d'environnement	Paramètre	Remarques
		dérivé du PLMN.
`SEPP_SEC_CAPABILITIES`	`supported_sec_capabilities`	Liste séparée par des virgules, ordre de préférence.

Exemple de configuration

Un remplacement réaliste par déploiement pour un PLMN domestique `310-260` avec un seul partenaire 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"
  }
```

Comment ça fonctionne : OmniSEPP se présente au NRF à `10.20.0.5:7777` en tant que type NF `SEPP` pour le PLMN `310-260`, envoyant des heartbeats toutes les 10 secondes. Comme `sbi_scheme` est `https`, l'auditeur N32 termine TLS avec `sepp.crt` / `sepp.key`, et comme `sbi_cacertfile` est défini, il exige et vérifie le certificat client du SEPP partenaire contre `partner-ca.crt` (TLS mutuel). Il accepte les handshakes N32-c en tant que `sepp.5gc.mnc260.mcc310.3gppnetwork.org`, négociant TLS comme la seule capacité N32-f, et au démarrage, initie le handshake sortant vers le partenaire `001-01`. Le trafic N32-f est relayé uniquement vers et depuis le PLMN partenaire `001-01`, et le FQDN AMF interne est masqué derrière le FQDN SEPP vers ce partenaire.

Métriques et Surveillance d'OmniSEPP

Vue d'ensemble | Guide des opérations | Référence de configuration | Dépannage

Observabilité

L'observabilité est fournie par des **journaux d'application structurés** et un journal de requêtes standard. Les opérateurs surveillent OmniSEPP à travers ses journaux, qui capturent les événements de poignée de main, de transfert et de requête décrits ci-dessous.

Ce qu'il faut surveiller dans les journaux

Les journaux d'application sont le signal principal pour faire fonctionner OmniSEPP. Les classes d'événements suivantes sont enregistrées et valent la peine d'être surveillées.

Résultats de la poignée de main N32-c

Chaque négociation de capacité enregistre son résultat, y compris l'identité SEPP distante et la capacité de sécurité N32-f sélectionnée en cas de succès. Surveillez-les pour confirmer que :

- Les partenaires de roaming attendus complètent la poignée de main.
- La capacité sélectionnée correspond à votre intention (par exemple `TLS`).
- Un partenaire est rejeté car aucune capacité commune n'a pu être sélectionnée.

Un pair qui sélectionne une capacité que ce SEPP n'a pas offerte (sur le chemin de l'initiateur) est enregistré comme un avertissement et rejeté.

Décisions et Échecs de Transfert N32-f

Le relais N32-f enregistre ses décisions de transfert et ses échecs, y compris :

- Refus de transférer à un PLMN qui n'est pas un partenaire de roaming configuré. Un taux croissant de ces refus suggère une entrée `roaming_partners` manquante ou mal configurée.
- Cibles de relais entrantes et sortantes (l'URL résolue et la direction).
- Échecs de transfert, qui apparaissent pour le partenaire comme `502 TARGET_NF_NOT_REACHABLE` et indiquent que le NF interne adressé était injoignable.

Journalisation des Requêtes

La journalisation standard des requêtes couvre chaque requête SBI traitée par l'auditeur, y compris les points de terminaison de la poignée de main et le relais N32-f catch-all. Utilisez-le pour observer le volume de requêtes, les méthodes et les chemins, et pour corréler l'activité des partenaires avec les événements de poignée de main et de transfert.

Vérification de l'état

La santé est évaluée en combinant :

- **Véracité :** `GET /n32c-handshake/v1/status` retourne `200 {"status":"UP"}` lorsque l'auditeur SBI est opérationnel. Voir le Guide des opérations.
- **Enregistrement NRF :** confirmer qu'OmniSEPP apparaît dans le NRF en tant qu'instance NF `SEPP` et envoie des signaux de vie. Le comportement d'enregistrement est décrit dans le Guide des opérations.
- **Signaux de journaux :** les événements de poignée de main et de transfert décrits ci-dessus.

Guide des opérations OmniSEPP

Vue d'ensemble | Référence de configuration | Métriques et surveillance | Dépannage

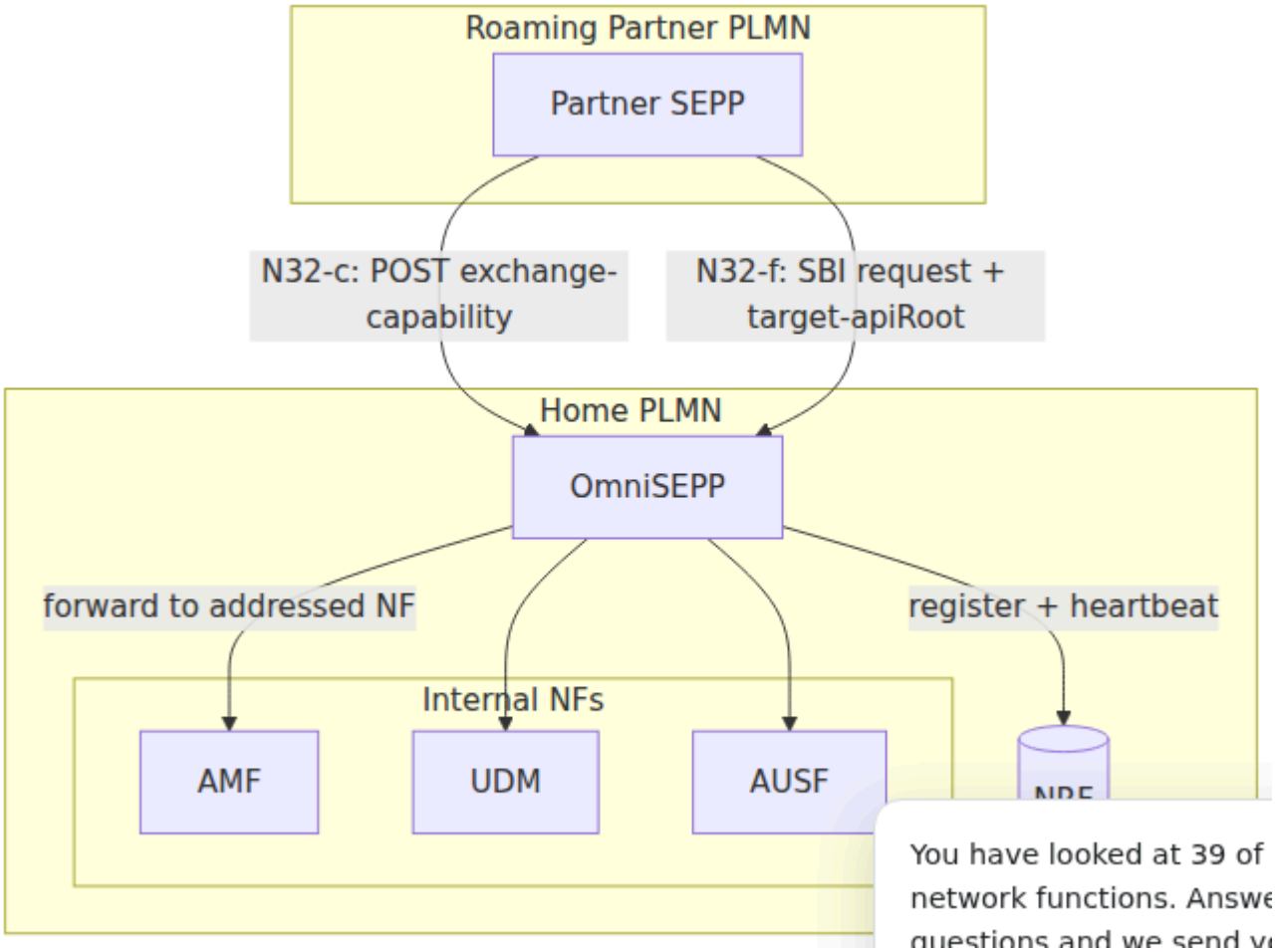
Ce guide décrit comment OmniSEPP se comporte sur l'interface N32 inter-PLMN et comment l'exploiter. OmniSEPP est le Security Edge Protection Proxy défini dans 3GPP TS 23.501 §6.2.17, avec un comportement de sécurité provenant de 3GPP TS 33.501 et l'interface N32 de 3GPP TS 29.573.

Table des matières

- Vue d'ensemble de l'architecture
- L'interface N32
- Cycle de vie de l'association N32
- Négociation des capacités
- Contrôle des partenaires de roaming
- Masquage de la topologie
- Flux de messages
- Points de terminaison SBI
- Enregistrement NRF
- Notes opérationnelles

Vue d'ensemble de l'architecture

OmniSEPP termine l'interface N32 vers les SEPPs partenaires de roaming et relaye le trafic vers les fonctions réseau internes dans le PLMN d'origine. Il s'enregistre auprès du NRF local en tant que NFType `SEPP` afin que les consommateurs locaux et le SCP puissent le découvrir ; le SEPP pair distant et la carte de masquage de topologie sont une configuration statique par accord de roaming (les SEPPs pairs ne sont pas découverts via le NRF).



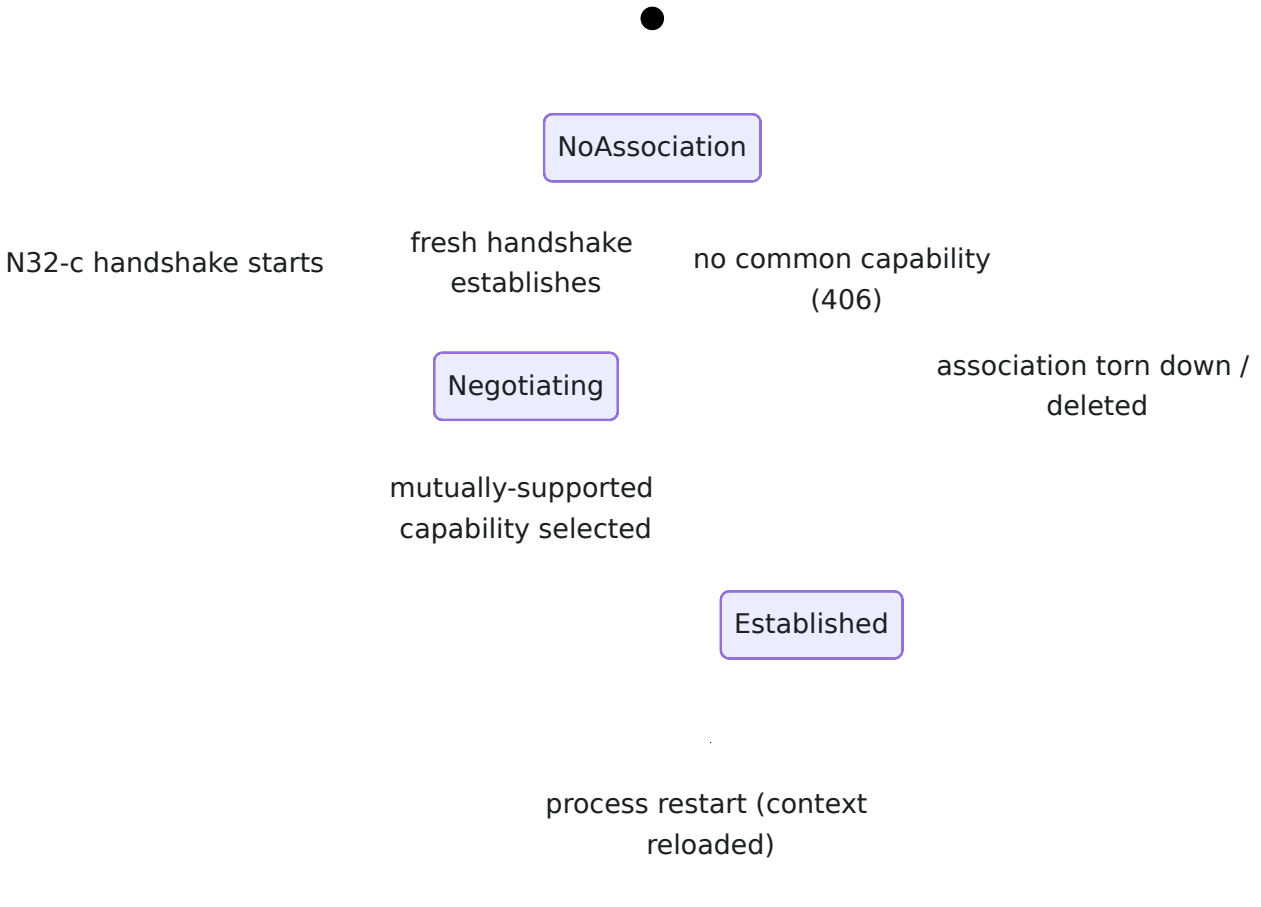
L'interface N32

N32 a deux canaux logiques (TS 29.573) :

- **N32-c (canal de contrôle)** - La poignée de main utilisée pour négocier la capacité de sécurité N32-f et établir l'association entre les deux SEPPs. OmniSEPP expose cela comme le `/n32c-handshake/v1/exchange-capability` point de terminaison (rôle de répondant) et initie également la poignée de main vers chaque partenaire de roaming configuré au démarrage (rôle d'initiateur).
- **N32-f (canal de transfert)** - L'échange continu de messages basés sur les services (SBI) entre les deux PLMNs. OmniSEPP relaie ces messages en **mode TLS** : le message est transféré en grande partie tel quel, avec une hygiène des en-têtes par saut et un masquage de topologie appliqué.

Cycle de vie de l'association N32

Chaque négociation N32-c réussie enregistre une association dans un **magasin de contexte persistant** (une table DETS devant un cache en mémoire), indexée par le FQDN du SEPP distant. Le contexte stocké inclut la capacité de sécurité N32-f sélectionnée et la liste d'identité du PLMN partenaire.



Propriétés opérationnelles clés :

- Le magasin est **persistant** : les associations sont écrites dans le fichier DETS à `n32_context_path` et rechargées au démarrage, de sorte qu'elles survivent à un redémarrage de processus ou de nœud. Un partenaire n'a pas à refaire la poignée de main après un redémarrage d'OmniSEPP.
- Il n'y a **pas de TTL** : une association persiste jusqu'à ce qu'elle soit explicitement détruite (supprimée) ou remplacée par une nouvelle négociation.
- Si le fichier DETS ne peut pas être ouvert (par exemple en cas de corruption), le magasin commence vide et enregistre un avertissement ; les associations sont alors rétablies par poignée de main.

Négociation des capacités

Lors de la poignée de main N32-c, les deux SEPPs s'accordent sur une seule capacité de sécurité N32-f. Les capacités valides sont `TLS` et `PRINS` (TS 33.501 §13.1).

La règle de sélection (TS 29.573 §5.2.3.2.2) est **préférence-locale-d'abord** : OmniSEPP parcourt sa propre liste configurée de `supported_sec_capabilities` dans l'ordre et choisit la première entrée que le pair offre également. Si les deux ensembles de capacités sont disjoints, la négociation échoue avec `INSUFFICIENT_RESOURCES` (HTTP 406) et aucune association n'est enregistrée.

Seules les capacités bien formées et reconnues (`TLS`, `PRINS`) sont annoncées. Gardez `supported_sec_capabilities` à `["TLS"]` pour un fonctionnement interopérable. Voir la Référence de configuration pour savoir comment définir l'ordre de préférence.

Contrôle des partenaires de roaming

Le **registre des partenaires de roaming** est une liste d'autorisation statique indexée par le PLMN partenaire (`"mcc-mnc"`). Il régit le transfert N32-f :

- Seuls les PLMNs présents dans le registre sont relayés vers ou depuis.
- Un registre vide (par défaut) signifie que le transfert N32-f refuse tous les PLMNs inconnus.
- Chaque entrée partenaire contient l'API root du SEPP partenaire et, en option, les capacités de sécurité N32-f autorisées avec ce partenaire. Lorsque la liste des capacités est omise, le partenaire hérite des `supported_sec_capabilities` de ce SEPP.

Voir Référence de configuration - Partenaires de roaming pour la structure de la carte.

Masquage de la topologie

Le masquage de la topologie (TS 33.501 §13.2) masque les identités des NF internes des partenaires de roaming en réécrivant les FQDN. OmniSEPP applique une carte configurée par l'opérateur de `internal_fqdn => external_fqdn` :

- **Sortant** (vers un partenaire) : les FQDN internes dans les valeurs d'en-tête `3gpp-Sbi-Target-apiRoot`, `Location` et `producer-id` sont réécrits en leurs équivalents externes.
- **Entrant** (d'un partenaire) : le mappage inverse est appliqué afin que l'apiRoot présenté extérieurement soit résolu en arrière vers le vrai FQDN interne avant que la demande ne soit routée vers le NF interne.

Les réécritures sont ancrées à des **tokens FQDN entiers** : un FQDN mappé est réécrit uniquement lorsqu'il apparaît comme un hôte complet (délimité par des délimiteurs d'URL tels que `/`, `:`, `@`, ou la fin de la valeur), jamais comme une sous-chaîne d'un nom d'hôte plus long. Cela empêche un mappage de corrompre un hôte non lié qui contient simplement le nom mappé, et empêche qu'une valeur produite par un mappage soit réappariée par une autre entrée de mappage.

À chaque relais, les en-têtes par saut (`host`, `content-length`, `connection`) sont supprimés. Sur le chemin entrant, l'en-tête `3gpp-Sbi-Target-apiRoot` (maintenant consommé) est également supprimé avant que la demande n'atteigne le NF interne.

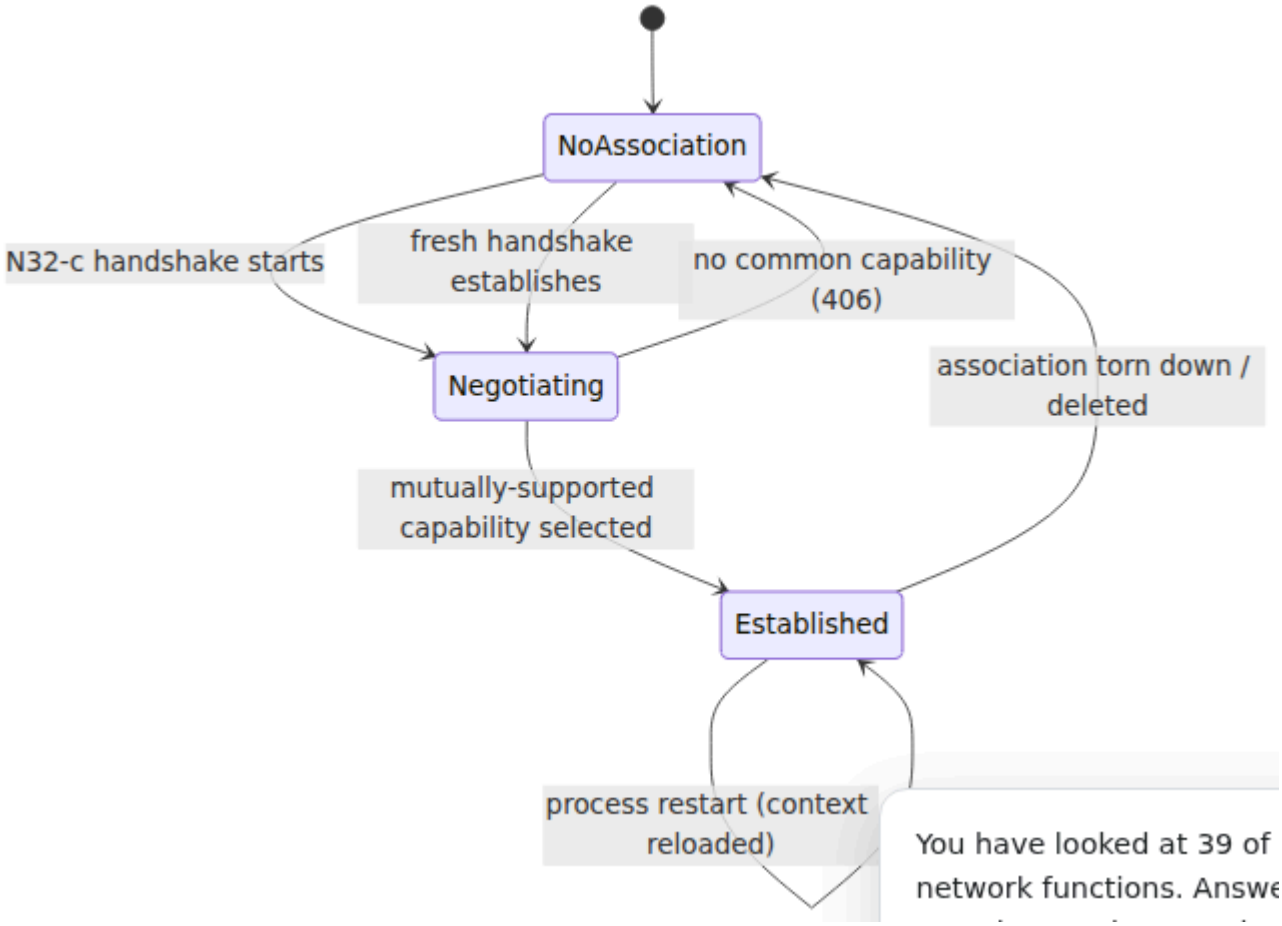
Une carte de masquage de topologie vide (par défaut) signifie qu'aucune réécriture n'est effectuée. Voir Référence de configuration - Carte de masquage de topologie.

Flux de messages

Poignée de main N32-c (Répondant)

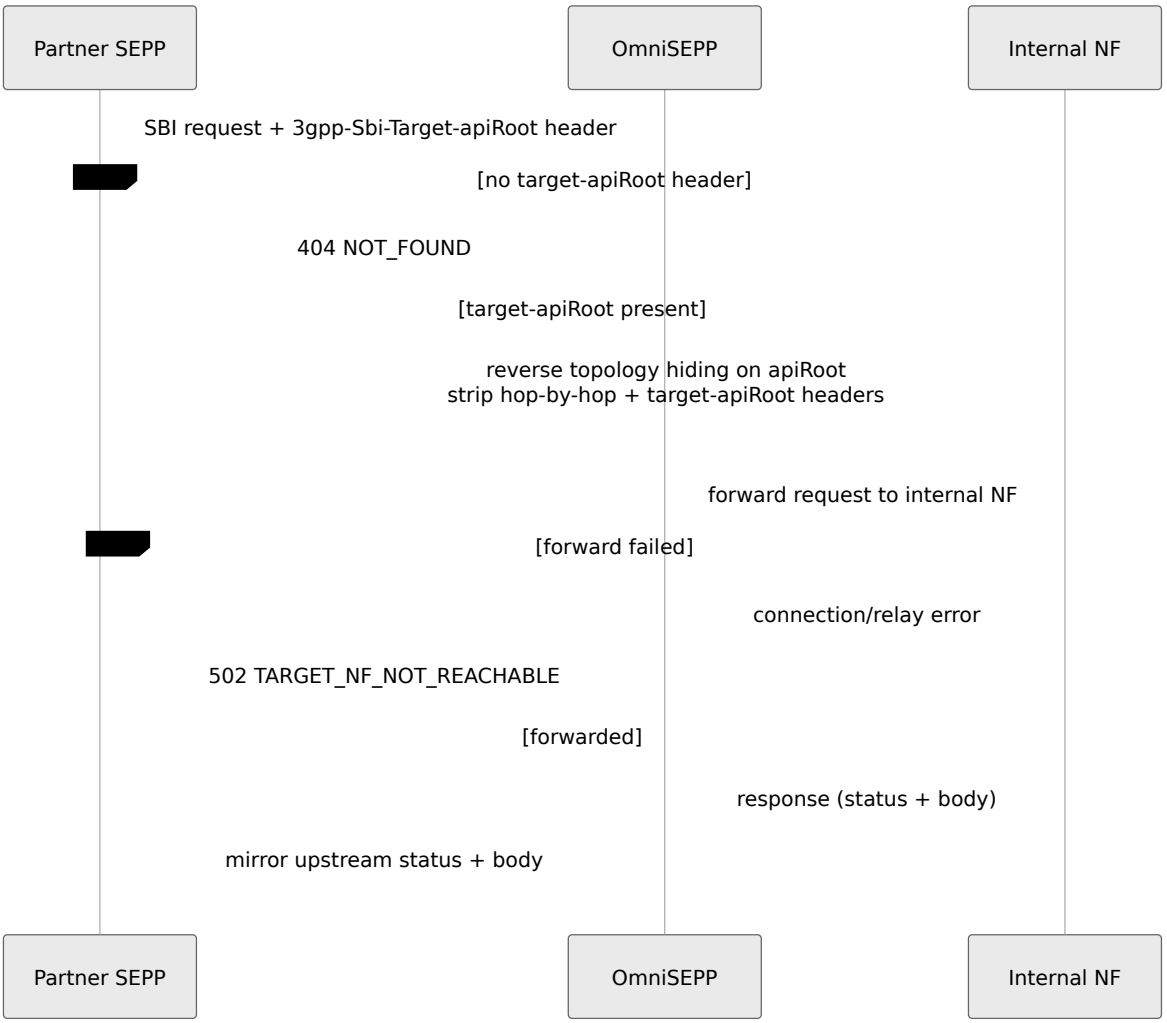
Un SEPP partenaire de roaming initie la poignée de main en envoyant une demande de négociation de capacité par POST. OmniSEPP sélectionne une

capacité mutuellement supportée, enregistre l'association et répond.



Transfert N32-f entrant

Un SEPP partenaire envoie une demande SBI portant un en-tête `3gpp-Sbi-Target-apiRoot` identifiant le NF interne. OmniSEPP inverse le masquage de topologie, supprime les en-têtes par saut et de routage, et transfère la demande, en miroir de la réponse en amont.



Points de terminaison SBI

OmniSEPP expose les éléments suivants via son écouteur HTTP SBI. La poignée de main N32-c annonce un service NRF, `n32c-handshake` version `v1`.

Méthode	Chemin	But
POST	`/n32c-handshake/v1/exchange-capability`	Négociation de la capacité de sécurité N32-c (répondant).
GET	`/n32c-handshake/v1/status`	Sonde de vivacité.
(tout)	tout autre chemin	Transfert N32-f. Routé vers l'extérieur vers le SEPP partenaire de roaming lorsque la demande nomme un PLMN partenaire, sinon entrant vers le NF interne nommé par `3gpp-Sbi-Target-apiRoot`.

POST /n32c-handshake/v1/exchange-capability

Négocie la capacité de sécurité N32-f avec un SEPP partenaire initiant.

Statut	Cause	Condition
200	-	Négociation réussie. La réponse contient `sender` et `selectedSecCapability`.
400	`MANDATORY_IE_MISSING`	La demande manque de `sender`, ou `supportedSecCapabilityList` est absente ou vide.
406	`INSUFFICIENT_RESOURCES`	Aucune capacité de sécurité N32-f mutuellement supportée.

GET /n32c-handshake/v1/status

Retourne `200` avec le corps `{"status":"UP"}`. Convient comme sonde de vivacité.

Transfert N32-f (catch-all)

Toute demande qui n'est pas l'un des points de terminaison de la poignée de main est traitée comme un trafic de transfert N32-f. La demande est routée **vers l'extérieur** (vers le SEPP partenaire de roaming) lorsqu'elle nomme un PLMN partenaire comme son sélecteur de sortie, sinon **entrant** (vers le NF interne nommé par `3gpp-Sbi-Target-apiRoot`).

Statut	Cause	Condition
(miroité)	-	Le statut et le corps en amont sont renvoyés en miroir en cas de succès (entrant ou sortant).
404	`NOT_FOUND`	Entrant : l'en-tête `3gpp-Sbi-Target-apiRoot` est absent, donc il n'y a pas de cible de routage.
403	`TARGET_PLMN_NOT_A_PARTNER`	Sortant : le PLMN cible nommé n'est pas un partenaire de roaming configuré.
502	`TARGET_NF_NOT_REACHABLE`	Le transfert vers le NF interne (entrant) ou le SEPP partenaire (sortant) a échoué.

Enregistrement NRF

Au démarrage, OmniSEPP s'enregistre auprès du NRF en tant que NFType `SEPP` (TS 23.501 §6.2.17) et envoie des battements de cœur à l'intervalle configuré.

L'enregistrement annonce l'adresse SBI, le port et le schéma, le PLMN desservi, et le service unique `n32c-handshake` `v1`.

S'enregistrer auprès du NRF local permet aux consommateurs locaux et au SCP de découvrir ce SEPP (TS 29.573 cl 4.2.1). Le SEPP pair **distant**, en revanche, est résolu à partir de la configuration statique `roaming_partners` par accord de roaming : c'est le modèle prévu pour la résolution des pairs inter-PLMN, puisque un SEPP dans un PLMN ne peut pas rechercher un SEPP dans le NRF d'un autre PLMN. Le masquage de la topologie est également une configuration statique.

Les paramètres d'enregistrement et de battement de cœur sont documentés dans la Référence de configuration.

Poignée de main sortante au démarrage

OmniSEPP agit en tant que **SEPP initiateur** ainsi que répondant. Au démarrage, une fois que le magasin de contexte est prêt, il initie une négociation de capacité N32-c vers chaque partenaire de roaming configuré (`roaming_partners`) qui a un `sepp_uri` (TS 29.573 §5.2.3.2). C'est **un meilleur effort** : un partenaire injoignable ou rejetant est enregistré et ignoré plutôt que de faire planter le démarrage, et la tâche s'exécute une fois sans redémarrage. Un partenaire qui était injoignable au démarrage peut toujours établir l'association plus tard en envoyant sa propre poignée de main (côté répondant), ou lors du prochain redémarrage.

Notes opérationnelles

- **Comportement de redémarrage :** le magasin d'associations N32 est persistant (soutenu par DETS). Les associations sont rechargées au redémarrage, donc les partenaires n'ont pas à relancer la poignée de main N32-c pour que le relais reprenne.
- **PLMNs inconnus :** avec un registre de partenaires de roaming vide, le transfert N32-f refuse les PLMNs inconnus. Remplissez le registre avant de vous attendre à ce que le trafic des partenaires soit relayé.

- **Terminaison TLS :** lorsque `sbi_scheme` est `https`, l'écouteur N32 termine TLS lui-même en utilisant le certificat et la clé configurés, et impose un TLS mutuel (certificat client) lorsqu'une CA est configurée. Voir Référence de configuration - TLS de l'écouteur N32.
- **PLMN par défaut :** le PLMN desservi par défaut expédié (`999-70`) est une valeur de test et doit être remplacé par déploiement.
- **Observabilité :** opérez contre des journaux d'application structurés ; voir Métriques et surveillance.

Dépannage d'OmniSEPP

Vue d'ensemble | Guide des opérations | Référence de configuration | Métriques et surveillance

Ce guide couvre les problèmes opérationnels courants et leurs résolutions. Le diagnostic repose sur des journaux structurés ; voir Métriques et surveillance.

Problèmes courants

Échec de la poignée de main N32-c avec 400

Symptômes : La demande de négociation de capacité d'un SEPP partenaire est répondue par `400 MANDATORY_IE_MISSING`.

Causes possibles :

- La demande manque de l'identité `sender`.
- La `supportedSecCapabilityList` est absente ou vide.

Résolution :

1. Confirmer que le partenaire envoie un `SecNegotiateReqData` bien formé avec un `sender` non vide.
2. Confirmer que le partenaire inclut au moins une capacité de sécurité N32-f dans `supportedSecCapabilityList`.

Échec de la poignée de main N32-c avec 406

Symptômes : La poignée de main d'un partenaire est répondue par `406 INSUFFICIENT_RESOURCES` et aucune association n'est enregistrée.

Causes possibles :

- Il n'y a pas de capacité commune entre les `supported_sec_capabilities` de ce SEPP et la liste offerte par le partenaire. Par exemple, le partenaire n'offre que `PRINS` tandis que ce SEPP n'offre que `TLS`.

Résolution :

1. Comparer les capacités offertes par le partenaire avec celles de ce SEPP `supported_sec_capabilities`.
2. S'assurer que les deux parties partagent au moins une capacité. En pratique, cela signifie que les deux doivent prendre en charge `TLS` ; garder `supported_sec_capabilities` à `["TLS"]` pour un fonctionnement interopérable.

Trafic N32-f refusé pour un PLMN

Symptômes : Le relais N32-f est refusé, et les journaux montrent un refus de transmettre à un PLMN non partenaire.

Causes possibles :

- Le PLMN partenaire n'est pas présent dans le registre `roaming_partners`.
- Le registre est vide (par défaut), donc tous les PLMN inconnus sont refusés.

Résolution :

1. Ajouter le PLMN partenaire à `roaming_partners`, indexé par `"mcc-mnc"`, avec le `sepp_uri` du SEPP partenaire.
2. Confirmer que la clé PLMN correspond exactement à celle du `mcc-mnc` du partenaire.

Le relais entrant renvoie 404 NOT_FOUND

Symptômes : Une demande de partenaire est répondue par `404 NOT_FOUND` au lieu d'être relayée.

Causes possibles :

- La demande ne contient pas d'en-tête `3gpp-Sbi-Target-apiRoot`, donc OmniSEPP n'a pas de cible de routage.

Résolution :

1. Confirmer que le partenaire définit l'en-tête `3gpp-Sbi-Target-apiRoot` identifiant le NF interne.
2. Si le masquage de topologie est utilisé, confirmer que l'apiRoot externe présenté par le partenaire a une entrée inverse correspondante dans le `topology_hiding_map`.

Le relais entrant renvoie 502 TARGET_NF_NOT_REACHABLE

Symptômes : Une demande de partenaire est répondue par `502 TARGET_NF_NOT_REACHABLE`.

Causes possibles :

- Le NF interne adressé est hors service ou inaccessible depuis OmniSEPP.
- Le masquage de topologie n'a pas résolu l'apiRoot externe en un FQDN interne accessible.

Résolution :

1. Confirmer que le NF interne résolu à partir de l'apiRoot (inversé) est en cours d'exécution et accessible.
2. Vérifier que l'entrée `topology_hiding_map` associe le FQDN externe au bon FQDN interne résolvable.

Les associations disparaissent après un redémarrage

Symptômes : Après le red��marrage d'OmniSEPP, les partenaires précédemment établis sont traités comme s'il n'existait aucune association, et le relais N32-f pour eux échoue jusqu'à ce qu'ils effectuent à nouveau la poignée de main.

Causes possibles :

- Le fichier DETS à `n32_context_path` n'a pas pu être ouvert (par exemple en raison de corruption ou d'un problème de permissions), donc le stockage a commencé vide et a enregistré un avertissement.
- Le `n32_context_path` configuré a changé entre les exécutions, donc le fichier précédent n'est pas lu.

Résolution :

1. Les associations sont normalement persistantes et se rechargent au redémarrage, donc un redémarrage seul ne devrait pas les effacer. S'ils sont manquants, vérifier les journaux de démarrage pour un avertissement N32Context concernant l'ouverture de DETS.
2. Confirmer que `n32_context_path` pointe vers un emplacement stable et écrivable qui est préservé entre les redémarrages (pas un répertoire temporaire par exécution).

Le partenaire ne peut pas établir TLS mutuellement authentifié

Symptômes : Un partenaire s'attend à N32 sur TLS mutuellement authentifié mais la connexion est refusée, est en HTTP simple, ou le certificat client du partenaire n'est pas vérifié.

Causes possibles :

- `sbi_scheme` est `http`, donc l'auditeur sert du texte en clair.
- `sbi_scheme` est `https` mais `sbi_cacertfile` n'est pas défini, donc seulement le TLS côté serveur est terminé et le certificat client du pair n'est pas requis.
- `sbi_scheme` est `https` mais `sbi_certfile` / `sbi_keyfile` ne sont pas configurés, auquel cas OmniSEPP refuse de démarrer plutôt que de rétrograder vers du texte en clair.

Résolution :

1. Définir `sbi_scheme` sur `https` et configurer `sbi_certfile` et `sbi_keyfile` afin que l'auditeur termine le TLS lui-même.

2. Pour exiger et vérifier le certificat client du SEPP pair (TLS mutuel), définir `sbi_cacertfile` sur l'AC qui signe le certificat du pair. Voir Référence de configuration - TLS de l'auditeur N32.

Référence

Sujet	Spécification
Fonction réseau SEPP	3GPP TS 23.501 §6.2.17
Mode TLS N32-f et masquage de topologie	3GPP TS 33.501 §13.1, §13.2
Poignée de main N32 et transfert N32-f	3GPP TS 29.573 §5.2.3, §5.3, §6.1.5.2