OmniSEP - Plateforme de Point de Service

OmniSEP est une plateforme de point de service unifiée fournissant des implémentations de qualité opérateur des protocoles de provisionnement des appareils mobiles. Elle gère la configuration des droits TS.43, les services supplémentaires XCAP et la messagerie vocale visuelle depuis une seule plateforme.

Liens Rapides

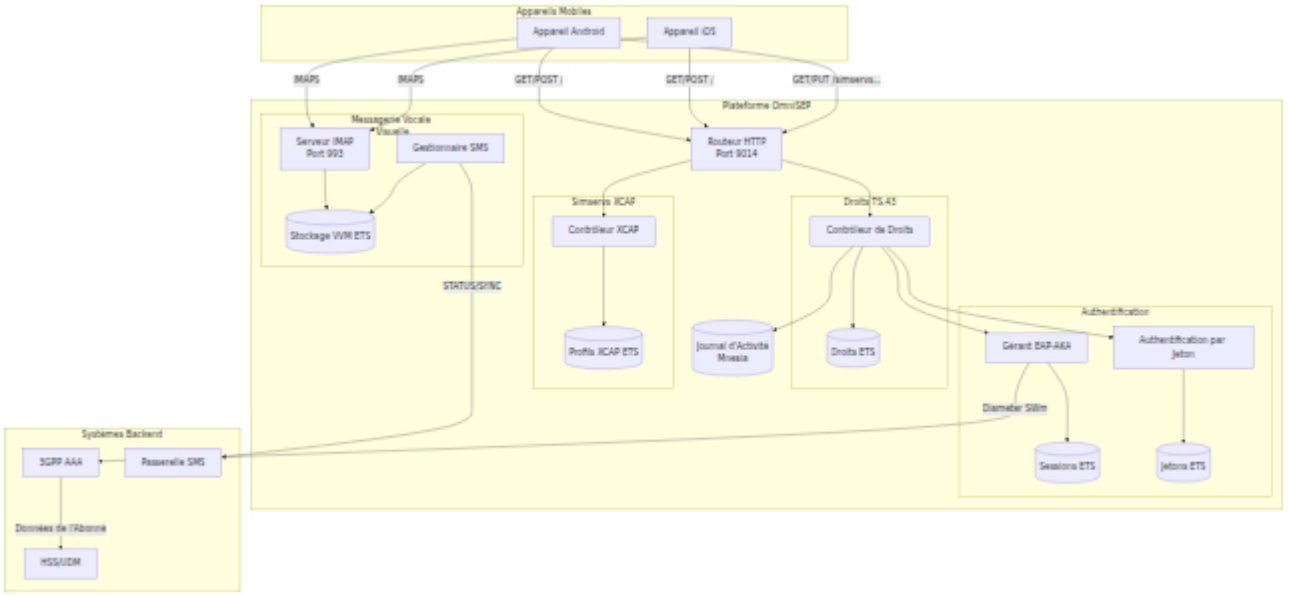
Opérations & Surveillance

- **Référence de Configuration** - Documentation complète des paramètres pour tous les services
- **API de Gestion** - Référence de l'API REST pour la surveillance et l'administration (port 8443)
- **Dépannage** - Problèmes courants et résolutions

Documentation des Services

- **Droits TS.43** - Configuration des droits de service TS.43 de la GSMA
- **Simservs XCAP** - Services supplémentaires ETSI TS 183 023 (Transfert d'Appel, Blocage d'Appel, Identification de l'Appelant)
- **Messagerie Vocale Visuelle** - Serveur de Messagerie Vocale Visuelle OMTP VVM v1.3 / GSMA TS.46

Aperçu de l'Architecture



Services Supportés

Configuration des Droits TS.43

Implémente la norme GSMA TS.43 pour les requêtes de droits de service des appareils :

ID App	Service	Description
ap2003	Voix sur Cellulaire	Statut des droits VoLTE/VoNR
ap2004	VoWiFi	Droits d'appel Voix sur WiFi
ap2005	SMSoIP	Droits SMS sur IP
ap2006	Compagnon ODSA	Activation de Service sur Appareil (compagnon)
ap2009	Principal ODSA	Activation de Service sur Appareil (principal)
ap2010	Boost de Plan de Données	Informations sur le plan de données
ap2012	Facturation Directe par Opérateur	Statut du service DCB
ap2016	Mode Satellite	Droits de connectivité satellite

Services Supplémentaires XCAP

Implémente la norme ETSI TS 183 023 pour la configuration des services supplémentaires IMS :

Service	Description	Référence
Diversion de Communication	Transfert d'appel (CFU, CFB, CFNA, CFNRC)	ETSI TS 183 004
Blocage d'Appels Entrants	Bloquer les appels entrants par type	ETSI TS 183 023
Blocage d'Appels Sortants	Bloquer les appels sortants par type	ETSI TS 183 023
OIP/OIR	Présentation et restriction de l'identification de l'appelant	ETSI TS 183 023

Messagerie Vocale Visuelle

Implémente la Spécification OMTP VVM v1.3 et GSMA TS.46 :

Composant	Description	Référence
Serveur IMAP	Récupération et gestion des messages	RFC 3501
Protocole SMS	Messages de provisionnement SYNC/STATUS	OMTP VVM v1.3
Gestion des Salutations	Salutations personnelles et d'absence prolongée	GSMA TS.46
Transcription	Support de la messagerie vocale en texte	OMTP VVM v1.3

Aperçu des Points de Terminaison



Point de Terminaison	Méth
`/`	GET/POS
`/simservs.ngn.etsi.org/users/{sip}/simservs.xml`	GET/PUT
`/simservs.ngn.etsi.org/users/{sip}/simservs.xml/~~/{xpath}`	GET/PUT/
`/api/activity`	GET
`/api/entitlements/{imsi}`	GET/POS
`/api/xcap/{msisdn}`	GET/POS
`/health`	GET

Interface Web

OmniSEP comprend une interface web en temps réel pour la surveillance et la gestion, construite avec Phoenix LiveView. Accédez à l'UI à `http://<host>:9014/`.

Gestion des Profils Simservs XCAP montrant la configuration des services supplémentaires de l'abonné

Tableaux de Bord

Tableau de Bord	Chemin	Description
Statut	`/`	État du système, statut des services, utilisation de la mémoire, statistiques de stockage
Droits	`/entitlements`	Voir et gérer les droits personnalisés TS.43 par IMSI
Sessions	`/sessions`	Surveiller les sessions EAP-AKA et les jetons d'authentification actifs
Activité	`/activity`	Parcourir les journaux d'activité TS.43 avec filtrage et pagination
Profils XCAP	`/xcap`	Gérer les profils Simservs XCAP, synchroniser avec HSS
Diameter	`/diameter`	Surveiller les connexions et l'état des pairs Diameter
Journaux	`/logs`	Visionneuse de journaux système en temps réel avec filtrage par niveau

Tableau de Bord de Statut

Le tableau de bord de statut principal fournit un aperçu de la santé du système :

- **Statut des Services** : Serveur HTTP, EAP-AKA, indicateurs de service VVM
- **Compteurs de Stockage** : Droits, profils XCAP, sessions, jetons, enregistrements d'activité

- **Utilisation de la Mémoire** : Total, processus et répartition de la mémoire ETS
- **Temps de Fonctionnement** : Affichage du temps de fonctionnement du système

Tous les indicateurs se rafraîchissent automatiquement toutes les 5 secondes.

Gestion des Profils XCAP

Le tableau de bord XCAP permet aux opérateurs de :

- Rechercher et visualiser les profils des abonnés par MSISDN
- Modifier les paramètres des services supplémentaires (OIP/OIR, transfert d'appel, blocage d'appel)
- Récupérer des profils depuis HSS via l'interface Sh Diameter
- Pousser des modifications locales vers HSS
- Voir les métadonnées de modification (timestamp, IP du client, User-Agent)

Surveillance de l'Activité

Le tableau de bord d'activité fournit une visibilité en temps réel sur toutes les requêtes des appareils :

Journal d'activité montrant les requêtes XCAP et de droits avec les détails de la requête/réponse

Fonctionnalités :

- Filtrer par type de requête (XCAP, Requête de Droits, Défi EAP, etc.)
- Rechercher par IMSI, MSISDN, ID de Terminal ou IP du Client
- Voir les données détaillées de la requête/réponse y compris les en-têtes, le corps et le chemin
- Suivre la méthode HTTP et les codes d'état de réponse

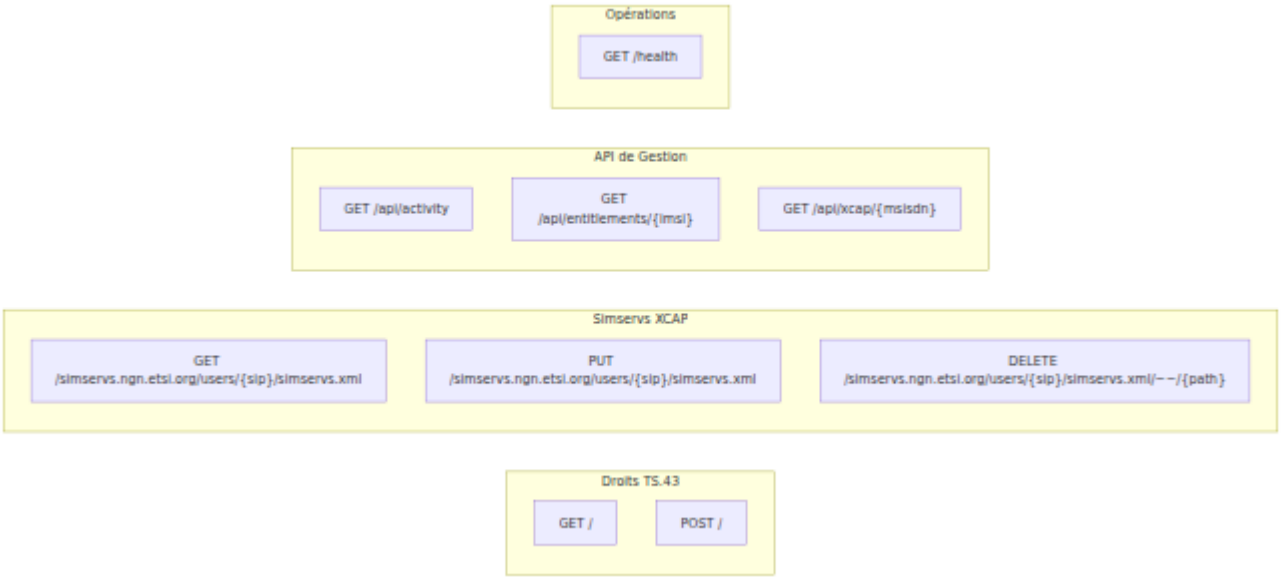
Surveillance des Sessions

Le tableau de bord des sessions affiche :

- **Onglet Sessions** : Sessions EAP-AKA actives avec état (en attente, défi envoyé, authentifié, échoué)
- **Onglet Jetons** : Jetons d'authentification actifs avec le temps restant jusqu'à l'expiration

Les deux vues prennent en charge la révocation manuelle des sessions/jetons.

Flux d'Authentification



Configuration de Démarrage Rapide

Configuration Minimale

```
# config/config.exs
import Config

config :omni_sep,
  http_port: 9014,
  http_ip: {0, 0, 0, 0},
  server_fqdn: "sep.mnc001.mcc001.pub.3gppnetwork.org",
  entitlement_version: "2.0"

# Droits par défaut pour tous les abonnés
config :omni_sep, :default_entitlements,
  vowifi: %{
    entitlement_status: 1,
    addr_status: 2,
    tc_status: 2,
    prov_status: 1
  },
  volte: %{
    entries: [
      %{access_type: 1, home_roaming_nw_type: 1,
entitlement_status: 1}
    ]
  }

# Paramètres des jetons
config :omni_sep, :token,
  validity_seconds: 86400,
  signing_secret: "votre-secret-de-production-ici"

# Paramètres EAP-AKA
config :omni_sep, :eap_aka,
  enabled: true,
  session_timeout_ms: 30_000
```

Voir Référence de Configuration pour la documentation complète des paramètres.

Structure de la Documentation

Par Rôle

Opérateurs de Réseau :

1. Commencez par cet aperçu
2. Consultez Référence de Configuration pour les paramètres de déploiement
3. Consultez Dépannage pour les problèmes courants

Configuration des Services :

1. Droits TS.43 pour le provisionnement VoWiFi/VoLTE
2. Simservs XCAP pour le transfert/bloquage d'appel

Dépannage :

1. Guide de Dépannage pour les problèmes courants
2. Vérifiez Journal d'Activité pour le suivi des requêtes

Par Protocole

GSMA TS.43 :

- Droits TS.43 - Documentation complète des droits de service
- Spécification : GSMA TS.43

ETSI XCAP :

- Simservs XCAP - Documentation des services supplémentaires
- Spécifications :
  - ETSI TS 183 023 - Cadre XCAP
  - ETSI TS 183 004 - Diversion de Communication
  - RFC 4825 - Protocole XCAP

Référence de Configuration OmniSEP

Référence complète de configuration pour la plateforme de point de service OmniSEP.

Table des Matières

- Configuration du Serveur HTTP
- Configuration du Stockage
- Droits par Défaut
- Configuration des Jetons
- Configuration EAP-AKA
- Configuration Diameter
- Journalisation des Activités
- Configuration Spécifique à l'Environnement

Structure de Configuration



Configuration du Serveur HTTP

Contrôle le point de terminaison HTTP où les appareils se connectent.

```
config :omni_sep,
  http_port: 9014,
  http_ip: {0, 0, 0, 0},
  server_fqdn: "sep.mnc001.mcc001.pub.3gppnetwork.org",
  vers_version: 1,
  vers_validity_seconds: 172_800
```

Paramètres

Paramètre	Type	Requis	Par Défaut	
`http_port`	Entier	Non	9014	Port TCP pour les avec un terminat
`http_ip`	Tuple	Non	`{0, 0, 0, 0}`	Adresse IP à lier. interfaces. Utilise hôtes multi-homé
`server_fqdn`	Chaîne	Oui	-	Nom de domaine serveur. Format : `aes.mnc<MNC>.mc` selon GSMA TS.4
`vers_version`	Entier	Oui	-	Version de config caractéristique V pour que les appa configuration.
`vers_validity_seconds`	Entier	Oui	-	Durée, en second appareil peut me (VALIDITÉ VERS).
`min_entitlement_version`	Chaîne	Non	"1.0"	Plus basse versio qu'un client peut inférieure obtient Samsung envoier
`max_entitlement_version`	Chaîne	Non	"13.0"	Plus haute versio qu'un client peut supérieure obtier

Format FQDN

Le FQDN du serveur suit la convention de nommage 3GPP :

```
aes.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org
```

Composant	Description	Exemple
`aes`	Préfixe du Serveur d'Accès aux Droits d'Application	`aes`
`mnc<MNC>`	Code de Réseau Mobile (3 chiffres, complété par des zéros)	`mnc001`
`mcc<MCC>`	Code de Pays Mobile (3 chiffres)	`mcc310`
`pub.3gppnetwork.org`	Suffixe de domaine standard 3GPP	-

Exemple : Pour MCC 310 (USA), MNC 410 (AT&T) :

```
aes.mnc410.mcc310.pub.3gppnetwork.org
```

Configuration du Stockage

Contrôle le stockage de données persistantes en utilisant Mnesia pour une journalisation des activités conforme aux audits.

```
config :omni_sep, :storage,
  data_dir: "priv/data"
```

Paramètres

Paramètre	Type	Requis	Par Défaut	Description
`data_dir`	Chaîne	Non	"priv/data"	Répertoire pour les fichiers de base de données Mnesia. Les journaux d'activités sont persistés ici et survivent aux redémarrages de l'application.

Architecture de Stockage



Tables Mnesia

La journalisation des activités utilise des tables Mnesia `disc_copies` pour la persistance :

Table	But	Persistance
`activity`	Enregistrements d'activités (journal d'audit)	Mnesia disc_copies
`activity_by_imsi`	Index IMSI pour une recherche rapide	Mnesia disc_copies
`activity_by_terminal`	Index ID de terminal	Mnesia disc_copies

Structure du Répertoire de Données

```
priv/data/
└── mnesia/
    ├── schema.DAT         # Schéma Mnesia
    ├── activity.DCD       # Données de la table d'activités
    ├── activity.DCL       # Journal des transactions d'activités
    ├── activity_by_imsi.DCD
    ├── activity_by_imsi.DCL
    ├── activity_by_terminal.DCD
    ├── activity_by_terminal.DCL
    ├── DECISION_TAB.LOG
    └── LATEST.LOG
```

Considérations de Production

Pour les déploiements en production :

1. **Permissions du Répertoire de Données** : Assurez-vous que le répertoire de données est accessible en écriture par l'utilisateur de l'application
2. **Espace Disque** : Surveillez l'utilisation du disque à mesure que les journaux d'activités augmentent
3. **Sauvegarde** : Incluez le répertoire Mnesia dans les procédures de sauvegarde

4. **Récupération** : Mnesia récupère automatiquement à partir des journaux de transactions au démarrage

```
# config/prod.exs
config :omni_sep, :storage,
  data_dir: "/var/lib/omni_sep/data"
```

Droits par Défaut

Définit l'état des droits retourné aux abonnés qui n'ont pas de configuration personnalisée.

```
config :omni_sep, :default_entitlements,
  # Defaults VoWiFi (ap2004)
  vowifi: %{
    entitlement_status: 1,           # ACTIVÉ
    addr_status: 2,                  # NON REQUIS
    tc_status: 2,                    # NON REQUIS
    prov_status: 1,                  # PROVISIONNÉ
    service_flow_url: "",
    service_flow_user_data: "",
    message_for_incompatible: "Le service VoWiFi n'est pas
disponible pour votre abonnement."
  },

  # Defaults Voix sur Cellulaire (ap2003)
  volte: %{
    entries: [
      %{
        access_type: 1,              # 4G/LTE
        home_roaming_nw_type: 1,     # Domicile & Itinérance
        entitlement_status: 1        # ACTIVÉ
      },
      %{
        access_type: 2,              # 5G/NR
        home_roaming_nw_type: 1,     # Domicile & Itinérance
        entitlement_status: 1,       # ACTIVÉ
        network_voice_irat_capability: "EPS-Fallback"
      }
    ]
  },

  # Defaults SMSoIP (ap2005)
  smsoip: %{
    entitlement_status: 1            # ACTIVÉ
  },

  # Defaults Plan de Données (ap2010)
  data_plan: %{
    entitlement_status: 1
  },

  # Defaults Facturation Directe par Opérateur (ap2012)
  dcb: %{
    entitlement_status: 0,           # DÉSACTIVÉ par défaut
```

```
  tc_status: 2                    # NON REQUIS
},

# Defaults Mode Satellite (ap2016)
satmode: %{
  entitlement_status: 0           # DÉSACTIVÉ par défaut
}
```

Paramètres VoWiFi (ap2004)

Paramètre	Type	Valeurs	Descript
`entitlement_status`	Entier	0=Désactivé, 1=Activé, 2=Incompatible, 3=Provisionnement	État de disponi service
`addr_status`	Entier	0=Non Disponible, 1=Disponible, 2=Non Requis, 3=En Cours	État de vérifica l'adresse
`tc_status`	Entier	0=Non Disponible, 1=Disponible, 2=Non Requis, 3=En Cours	État d'acceptat Termes et Cond
`prov_status`	Entier	0=Non Provisionné, 1=Provisionné, 2=Non Requis, 3=En Cours	État de provisionneme
`service_flow_url`	Chaîne	URL	URL pour le flu service (vérific d'adresse, T&C
`service_flow_user_data`	Chaîne	-	Données utilisa transmises au service
`message_for_incompatible`	Chaîne	-	Message affich lorsque `entitlement_s`

Paramètres VoLTE (ap2003)

La configuration VoLTE utilise un tableau d'entrées, une par technologie d'accès :

Paramètre	Type	Valeurs	Description
`access_type`	Entier	1=4G/LTE, 2=5G/NR	Technologie d'accès radio
`home_roaming_nw_type`	Entier	1=Domicile & Itinérance, 2=Domicile Seulement, 3=Itinérance Seulement	Portée du réseau
`entitlement_status`	Entier	0=Désactivé, 1=Activé	Disponibilité du service
`network_voice_irat_capability`	Chaîne	"EPS-Fallback", "VoNR"	Capacité vocale 5G

Valeurs d'État des Droits

Valeur	Nom	Description
0	DÉSACTIVÉ	Service non disponible
1	ACTIVÉ	Service disponible et prêt
2	INCOMPATIBLE	Appareil ou abonnement incompatible
3	PROVISIONNEMENT	Provisionnement en cours

Configuration des Jetons

Contrôle la génération et la validation des jetons d'authentification.

```
config :omni_sep, :token,
  validity_seconds: 86400,
  signing_secret: "change_me_in_production"
```

Paramètres

Paramètre	Type	Requis	Par Défaut	Description
`validity_seconds`	Entier	Non	86400	Durée de vie du jeton en secondes. Par défaut, 24 heures.
`signing_secret`	Chaîne	Oui	-	Clé secrète pour la signature du jeton. **Doit être changée en production.** Utilisez une chaîne aléatoire cryptographiquement sécurisée d'au moins 32 caractères.

Considérations de Sécurité

- Générez un `signing_secret` unique pour chaque déploiement
- Faites tourner les secrets périodiquement
- Utilisez des variables d'environnement pour les secrets en production :

```
# config/prod.exs
config :omni_sep, :token,
  signing_secret: System.get_env("OMNI_SEP_TOKEN_SECRET")
```

Configuration EAP-AKA

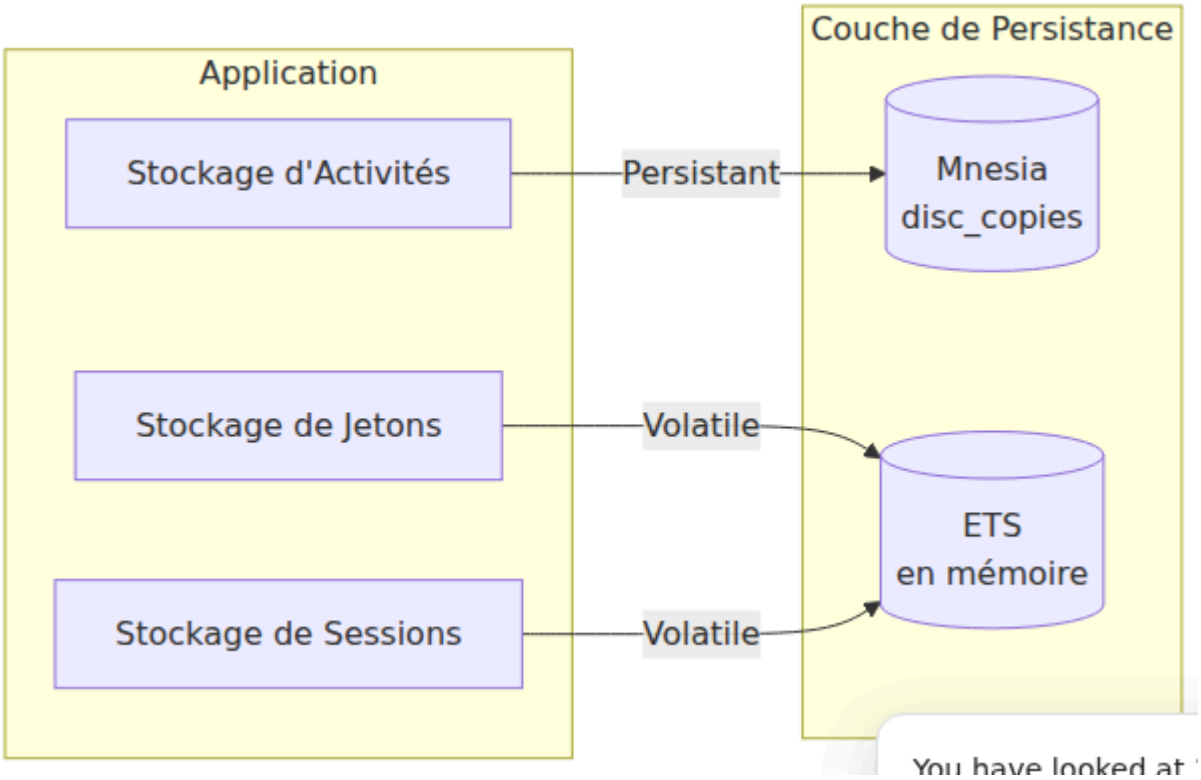
Contrôle le comportement d'authentification EAP-AKA pour l'authentification initiale des appareils.

```
config :omni_sep, :eap_aka,
  enabled: true,
  session_timeout_ms: 30_000
```

Paramètres

Paramètre	Type	Requis	Par Défaut	Description
`enabled`	Booléen	Non	true	Activer l'authentification EAP-AKA. Lorsque faux, seule l'authentification par jeton est acceptée.
`session_timeout_ms`	Entier	Non	30000	Temps d'expiration de la session EAP en millisecondes. La session expire si le client ne répond pas dans ce délai.

Flux EAP-AKA



Configuration Diameter

Configure le client Diameter pour l'authentification EAP-AKA via l'interface SWm.

```
config :diameter_ex, :diameter,
  service_name: :omni_sep_aaa,
  listen_ip: {127, 0, 0, 1},
  listen_port: 3868,
  host: "omnisep.example.com",
  realm: "example.com",
  product_name: "OmniSep",
  vendor_id: 10415,
  auth_application_ids: [16777265],
  acct_application_ids: [],
  supported_vendor_ids: [10415],
  request_timeout: 5000,
  allow_undefined_peers_to_connect: true,
  peer_selection_algorithm: :round_robin,
  control_module: OmniSep.Diameter.Control,
  processor_module: OmniSep.Diameter.Processor,
  applications: [
    %{
      alias: :swm,
      dictionary: :diameter_gen_base_rfc6733,
      module: OmniSep.Diameter.Swm
    }
  ],
  peers: [
    %{
      host: "aaa01.example.com",
      ip: "192.168.1.10",
      port: 3868,
      transport: :tcp
    }
  ]
```

Paramètres Principaux

Paramètre	Type	Requis	Par Défaut	Descri
`service_name`	Atome	Oui	-	Identifian service in
`host`	Chaîne	Oui	-	Origin-Ho Diameter être un F résolvabl RFC 6733
`realm`	Chaîne	Oui	-	Origin-Re Diameter pour le rc selon RFC
`vendor_id`	Entier	Oui	10415	ID de fou 3GPP selc TS 29.23(
`auth_application_ids`	Liste	Oui	-	Liste des d'applicat d'authent supportés est 1677
`request_timeout`	Entier	Non	5000	Délai d'at de la requ millisecor
`peer_selection_algorithm`	Atome	Non	`:round_robin`	Sélection pairs : `:round_r` `:failove`

Paramètres Réseau

Paramètre	Type	Requis	Par Défaut	Description
`listen_ip`	Tuple	Non	`{127, 0, 0, 1}`	IP à lier pour les connexions Diameter entrantes
`listen_port`	Entier	Non	3868	Port Diameter selon RFC 6733

Paramètres des Pairs

Chaque pair dans la liste `peers` :

Paramètre	Type	Requis	Par Défaut	Description
`host`	Chaîne	Oui	-	Identité Diameter du pair (doit correspondre exactement à l'Origin-Host du pair)
`ip`	Chaîne	Oui	-	Adresse IP du pair pour la connexion TCP/SCTP
`port`	Entier	Non	3868	Port Diameter du pair
`transport`	Atome	Non	`:tcp`	Transport : `:tcp` ou `:sctp`

Application SWm

L'interface SWm (ID d'application 16777265) est utilisée pour l'authentification EAP-AKA selon 3GPP TS 29.273.

Message	Code	Description
DER	268	Diameter-EAP-Request - Transporte la charge utile EAP vers AAA
DEA	268	Diameter-EAP-Answer - Retourne la réponse EAP de AAA

Aucun AAA Disponible

Si aucun pair Diameter n'est configuré ou connecté, OmniSEP n'authentifie pas l'abonné. La requête EAP-AKA est rejetée avec HTTP 511 (ou 503 lorsque EAP-AKA est désactivé), et une erreur est enregistrée.

Journalisation des Activités

Contrôle la journalisation des activités des abonnés pour les audits et le dépannage.

```
config :omni_sep, :activity,
  max_records_per_subscriber: 1000,
  retention_seconds: 2_592_000
```

Paramètres

Paramètre	Type	Requis	Par Défaut	Descriptio
`max_records_per_subscriber`	Entier	Non	1000	Nombre maximum d'enregistrem d'activités conservés pa abonné. Les enregistreme les plus ancie sont supprim lorsque la lim est dépassée
`retention_seconds`	Entier	Non	2592000	Période de conservation activités en secondes. Par défaut, 30 jou Les enregistreme plus anciens s automatiquer nettoyés.

Contenu des Enregistrements d'Activités

Chaque enregistrement d'activité contient :

Champ	Description
`imsi`	IMSI de l'abonné
`terminal_id`	IMEI/ID de terminal de l'appareil
`timestamp`	Horodatage de la requête
`client_ip`	Adresse IP du client
`user_agent`	En-tête HTTP User-Agent
`app_ids`	IDs d'application demandés
`auth_method`	Méthode d'authentification utilisée (EAP-AKA, JETON)
`response_code`	Code d'état de la réponse HTTP

Configuration Spécifique à l'Environnement

Développement

```
# config/dev.exs
import Config

config :omni_sep,
  http_port: 9014

config :omni_sep, :eap_aka,
  enabled: true

config :logger, :console,
  level: :debug
```

Production

```
# config/prod.exs
import Config

config :omni_sep,
  http_port: 9014,
  http_ip: {0, 0, 0, 0},
  server_fqdn: System.get_env("OMNI_SEP_FQDN")

config :omni_sep, :token,
  validity_seconds: 86400,
  signing_secret: System.get_env("OMNI_SEP_TOKEN_SECRET")

config :diameter_ex, :diameter,
  host: System.get_env("DIAMETER_HOST"),
  realm: System.get_env("DIAMETER_REALM"),
  peers: [
    %{
      host: System.get_env("AAA_PEER_HOST"),
      ip: System.get_env("AAA_PEER_IP"),
      port: 3868,
      transport: :tcp
    }
  ]

config :logger, :console,
  level: :info
```

Variables d'Environnement

Variable	Description
`OMNI_SEP_FQDN`	FQDN du serveur pour TS.43
`OMNI_SEP_TOKEN_SECRET`	Secret de signature du jeton
`DIAMETER_HOST`	Origin-Host Diameter
`DIAMETER_REALM`	Origin-Realm Diameter
`AAA_PEER_HOST`	Nom d'hôte du pair AAA
`AAA_PEER_IP`	Adresse IP du pair AAA

Configuration du Journal

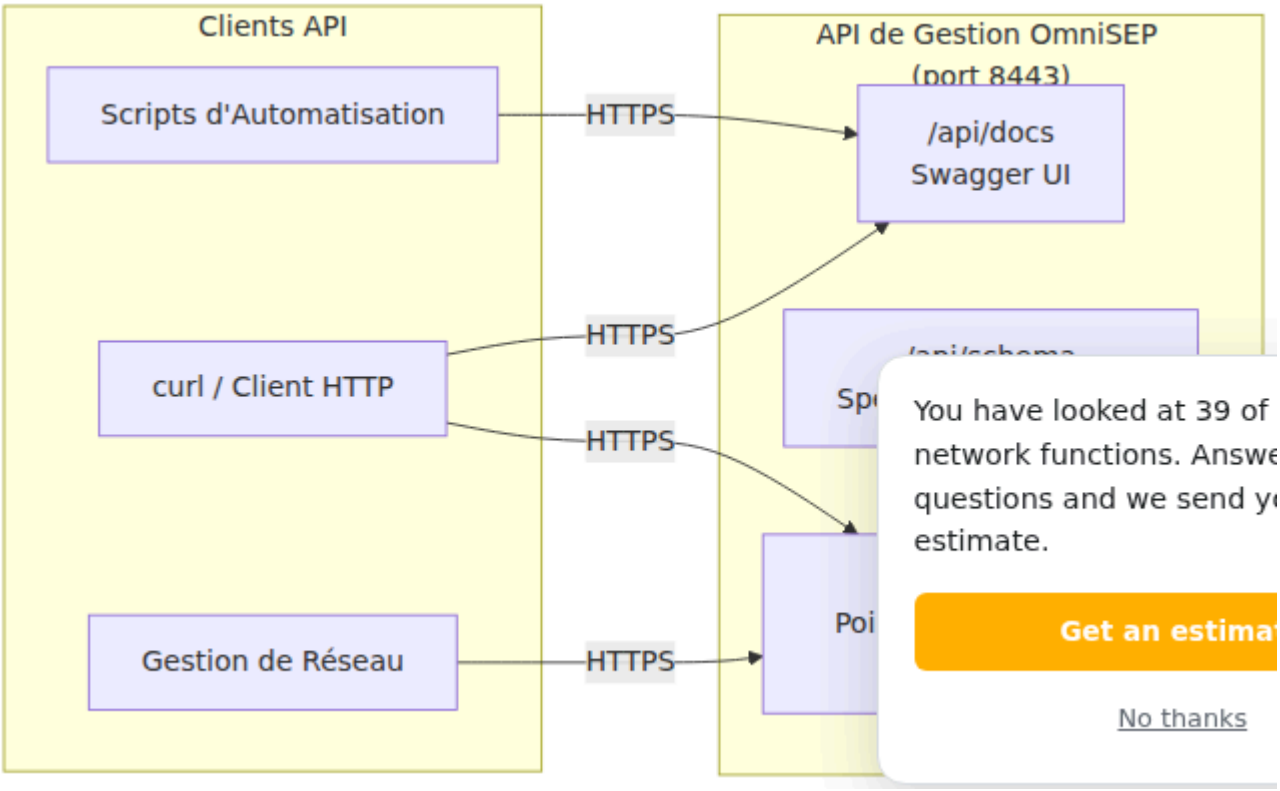
```
config :logger, :console,
  format: "$time $metadata[$level] $message\n",
  metadata: [:request_id, :imsi, :terminal_id]
```

Métadonnées	Description
`request_id`	Identifiant unique de la requête (UUID)
`imsi`	IMSI de l'abonné (lorsqu'authentifié)
`terminal_id`	ID de terminal de l'appareil provenant de la requête

API de Gestion

OmniSEP fournit une API de gestion RESTful pour surveiller et administrer la plateforme. L'API sert des réponses JSON sur HTTPS sur le port 8443 et inclut une documentation Swagger/OpenAPI auto-générée.

Aperçu



Résumé des Points de Terminaison

Point de Terminaison	Méthodes	Description
`/api/docs`	GET	Swagger UI (documentation API interactive)
`/api/schema`	GET	Spécification OpenAPI 3.0 (JSON)
`/api/status`	GET	État du système, temps de fonctionnement, mémoire, comptes de stockage
`/api/activity`	GET	Journal d'activité avec filtrage et pagination
`/api/activity/:id`	GET	Détail d'un enregistrement d'activité unique
`/api/entitlements`	GET	Liste des abonnés avec des droits personnalisés
`/api/entitlements/:id`	GET, DELETE	Obtenir ou supprimer des droits par IMSI
`/api/sessions`	GET	Liste des sessions EAP-AKA actives
`/api/sessions/:id`	GET, DELETE	Obtenir ou expirer une session
`/api/tokens`	GET	Liste des jetons d'authentification actifs
`/api/tokens/:id`	GET, DELETE	Obtenir ou révoquer un jeton

Point de Terminaison	Méthodes	Description
`/api/diameter`	GET	État de la connexion de pair Diameter
`/api/xcap`	GET	Liste des profils Simservs XCAP
`/api/xcap/:id`	GET, DELETE	Obtenir ou supprimer un profil par MSISDN

Authentification

L'API de gestion écoute sur un port TLS séparé (8443) du port HTTP destiné aux abonnés. Le contrôle d'accès est géré au niveau du réseau - restreindre l'accès au port de gestion à l'aide de règles de pare-feu ou se lier uniquement à une interface de gestion.

Configuration TLS

L'API utilise le même certificat TLS que les autres interfaces de gestion :

```
priv/cert/omnitouch.crt   # Certificat TLS
priv/cert/omnitouch.pem   # Clé privée TLS
```

Tous les exemples dans ce document utilisent `curl -k` pour ignorer la vérification du certificat pour les certificats auto-signés. En production, utilisez des certificats signés par une CA appropriée et retirez le drapeau `-k`.

État

Retourne des informations sur la santé du système, y compris le temps de fonctionnement, l'utilisation de la mémoire, les comptes de stockage et l'état des services.

```
GET /api/status
```

```
curl -sk https://localhost:8443/api/status
```

Réponse


```
{
  "status": "ok",
  "application": "OmniSEP",
  "version": "1.0.0",
  "uptime": "2d 5h 32m",
  "uptime_seconds": 193920,
  "memory": {
    "total_mb": 118.3,
    "processes_mb": 42.9,
    "ets_mb": 3.4
  },
  "storage": {
    "custom_entitlements": 12,
    "xcap_profiles": 45,
    "eap_aka_sessions": 3,
    "active_tokens": 8,
    "activity_records": 1267
  },
  "services": {
    "http_port": 80,
    "eap_aka_enabled": true,
    "vvm_enabled": false
  },
  "timestamp": "2026-04-11T10:35:24.794331Z"
}
```

Champs de Réponse

Champ	Type	Description
`status`	String	Toujours `"ok"` lorsque le service fonctionne
`application`	String	Nom de l'application
`version`	String	Version de l'application
`uptime`	String	Temps de fonctionnement lisible par l'homme (par exemple, `"2d 5h 32m"`)
`uptime_seconds`	Integer	Temps de fonctionnement en secondes
`memory.total_mb`	Float	Utilisation totale de la mémoire BEAM en mégaoctets
`memory.processes_mb`	Float	Mémoire utilisée par les processus Erlang
`memory.ets_mb`	Float	Mémoire utilisée par les tables ETS
`storage.custom_entitlements`	Integer	Nombre d'abonnés avec des droits personnalisés
`storage.xcap_profiles`	Integer	Nombre de profils Simservs XCAP stockés
`storage.eap_aka_sessions`	Integer	Nombre de sessions d'authentification EAP-AKA actives

Champ	Type	Description
`storage.active_tokens`	Integer	Nombre de jetons d'authentification actifs
`storage.activity_records`	Integer	Total des enregistrements du journal d'activité
`services.http_port`	Integer	Port HTTP destiné aux abonnés
`services.eap_aka_enabled`	Boolean	Indique si l'authentification EAP-AKA est activée
`services.vvm_enabled`	Boolean	Indique si la messagerie vocale visuelle est activée
`timestamp`	String	Heure actuelle du serveur (ISO 8601)

Activité

Interrogez le journal d'activité pour l'historique des demandes des abonnés. Le journal d'activité enregistre toutes les requêtes de droits TS.43, les opérations XCAP et les événements d'authentification EAP-AKA.

Lister les Enregistrements d'Activité

```
GET /api/activity
```

```
# Par défaut : les 50 premiers enregistrements
curl -sk https://localhost:8443/api/activity

# Avec pagination
curl -sk "https://localhost:8443/api/activity?page=2&limit=25"

# Filtrer par type de demande
curl -sk "https://localhost:8443/api/activity?
type=entitlement_query"

# Rechercher par IMSI
curl -sk "https://localhost:8443/api/activity?query=001010555"
```

Paramètres de Requête

Paramètre	Type	Par défaut	Description
`limit`	Integer	50	Nombre d'enregistrements par page (max 1000)
`page`	Integer	1	Numéro de page
`type`	String	`"all"`	Filtrer par type de demande
`query`	String	-	Rechercher dans IMSI, MSISDN, ID de terminal et IP du client (correspondance partielle)

Valeurs de Filtre de Type

Valeur	Description
`all`	Tous les types d'activité (par défaut)
`entitlement_query`	Requêtes de droits TS.43
`xcap`	Opérations Simservs XCAP
`eap_challenge`	Requêtes de défi EAP-AKA
`eap_response`	Soumissions de réponse EAP-AKA
`token_auth`	Requêtes authentifiées par jeton

Réponse

```
{
  "count": 25,
  "total": 1267,
  "page": 1,
  "page_size": 25,
  "activities": [
    {
      "id": "72420db8-c328-46bd-9878-2a9f3f0d2b88",
      "timestamp": "2026-03-09T04:19:19.461325Z",
      "request_type": "entitlement_query",
      "request_method": "GET",
      "request_path": "/",
      "imsi": "001010555555558",
      "msisdn": null,
      "terminal_id": "terminal_001",
      "terminal_vendor": "Samsung",
      "terminal_model": "SM-S928B",
      "terminal_sw_version": "1.0",
      "client_ip": "10.0.0.1",
      "user_agent": "SEC TS.43/2.0",
      "auth_method": "EAP-AKA",
      "response_status": 200,
      "response_code": 200,
      "app_ids": ["ap2004"],
      "request_headers": {},
      "request_body": null,
      "response_body": null,
      "response_summary": {}
    }
  ]
}
```


Champs d'Enregistrement d'Activité

Champ	Type	Description
`id`	String	ID d'enregistrement d'activité unique (UUID)
`timestamp`	String	Horodatage de la demande (ISO 8601)
`request_type`	String	Type de demande (voir valeurs de filtre de type)
`request_method`	String	Méthode HTTP (GET, POST, PUT, DELETE)
`request_path`	String	Chemin de la demande HTTP
`imsi`	String	IMSI de l'abonné
`msisdn`	String	MSISDN de l'abonné (si disponible)
`terminal_id`	String	Identifiant de terminal de l'appareil/IMEI
`terminal_vendor`	String	Fabricant de l'appareil
`terminal_model`	String	Modèle de l'appareil
`terminal_sw_version`	String	Version du logiciel de l'appareil
`client_ip`	String	Adresse IP du client
`user_agent`	String	En-tête HTTP User-Agent
`auth_method`	String	Méthode d'authentification utilisée (EAP-AKA, TOKEN)
`response_status`	Integer	Code d'état de la réponse HTTP
`response_code`	Integer	Code de réponse de l'application

Champ	Type	Description
`app_ids`	Array	IDs d'application demandés (par exemple, `["ap2004"]`)
`request_headers`	Object	En-têtes de la demande HTTP
`request_body`	String	Corps de la demande HTTP
`response_body`	String	Corps de la réponse HTTP
`response_summary`	Object	Données de réponse résumées

Obtenir un Enregistrement d'Activité

```
GET /api/activity/:id
```

```
curl -sk https://localhost:8443/api/activity/72420db8-c328-46bd-9878-2a9f3f0d2b88
```

Retourne un seul enregistrement d'activité avec tous les champs. Retourne `404` si l'enregistrement n'existe pas.

Droits

Gérez les droits TS.43 personnalisés par abonné. Les abonnés sans droits personnalisés reçoivent la configuration de droits par défaut.

Lister les Abonnés avec des Droits Personnalisés

```
GET /api/entitlements
```

```
# Lister tous
curl -sk https://localhost:8443/api/entitlements

# Rechercher par IMSI
curl -sk "https://localhost:8443/api/entitlements?query=31038"
```

Paramètres de Requête

Paramètre	Type	Par défaut	Description
`query`	String	-	Filtrer par IMSI (correspondance partielle, insensible à la casse)

Réponse


```
{
  "count": 2,
  "entitlements": [
    {
      "imsi": "310380100000001",
      "app_ids": ["ap2003", "ap2004"],
      "services": ["VoLTE/VoNR", "VoWiFi"]
    },
    {
      "imsi": "310380100000042",
      "app_ids": ["ap2004", "ap2005"],
      "services": ["VoWiFi", "SMSoIP"]
    }
  ]
}
```

Référence ID d'Application

ID d'Application	Nom du Service
`ap2003`	VoLTE/VoNR
`ap2004`	VoWiFi
`ap2005`	SMSoIP
`ap2006`	Compagnon ODSA
`ap2009`	Principal ODSA
`ap2010`	Forfait de Données
`ap2012`	DCB (Facturation Directe par Opérateur)
`ap2016`	Satellite

Obtenir les Droits pour un Abonné

```
GET /api/entitlements/:imsi
```

```
curl -sk https://localhost:8443/api/entitlements/310380100000001
```

Réponse

```
{
  "imsi": "310380100000001",
  "entitlements": {
    "ap2003": {
      "service_name": "VoLTE/VoNR",
      "data": {
        "entries": [
          {
            "access_type": 1,
            "home_roaming_nw_type": 1,
            "entitlement_status": 1
          }
        ]
      }
    },
    "ap2004": {
      "service_name": "VoWiFi",
      "data": {
        "entitlement_status": 1,
        "addr_status": 2,
        "tc_status": 2,
        "prov_status": 1
      }
    }
  }
}
```


Retourne `404` si aucun droit personnalisé n'existe pour l'IMSI donné.

Supprimer les Droits pour un Abonné

```
DELETE /api/entitlements/:imsi
```

```
curl -sk -X DELETE
https://localhost:8443/api/entitlements/310380100000001
```

Supprime tous les droits personnalisés pour l'abonné. L'abonné reviendra à recevoir des droits par défaut.

Réponse

```
{
  "status": "ok",
  "imsi": "310380100000001"
}
```

Sessions

Affichez et gérez les sessions d'authentification EAP-AKA actives. Les sessions sont créées lorsqu'un appareil initie une authentification EAP-AKA et sont de courte durée (généralement 30 secondes).

Lister les Sessions

```
GET /api/sessions
```

```
curl -sk https://localhost:8443/api/sessions
```

Réponse

```
{
  "count": 1,
  "sessions": [
    {
      "session_id": "a1b2c3d4-e5f6-7890-abcd-ef1234567890",
      "imsi": "310380100000001",
      "state": "challenge_sent",
      "created_at": 1712834400000,
      "eap_id": 1,
      "aaa_session_id": "dra01-sess-001",
      "completed_at": null
    }
  ]
}
```

Valeurs d'État de Session

État	Description
`pending`	Session créée, en attente de réponse Diameter
`challenge_sent`	Défi EAP-AKA envoyé à l'appareil
`authenticated`	Appareil authentifié avec succès
`failed`	Échec de l'authentification
`completed`	Session terminée et jeton émis

Obtenir une Session

```
GET /api/sessions/:id
```

```
curl -sk https://localhost:8443/api/sessions/a1b2c3d4-e5f6-7890-abcd-ef1234567890
```

Retourne `404` si la session n'existe pas.

Expirer une Session

```
DELETE /api/sessions/:id
```

```
curl -sk -X DELETE https://localhost:8443/api/sessions/a1b2c3d4-e5f6-7890-abcd-ef1234567890
```

Expire immédiatement la session. L'appareil devra redémarrer l'authentification.

Réponse

```
{
  "status": "ok",
  "session_id": "a1b2c3d4-e5f6-7890-abcd-ef1234567890"
}
```


Jetons

Affichez et gérez les jetons d'authentification actifs. Les jetons sont émis après une authentification EAP-AKA réussie et sont utilisés pour les requêtes de droits suivantes.

Lister les Jetons

```
GET /api/tokens
```

```
curl -sk https://localhost:8443/api/tokens
```

Réponse


```
{
  "count": 1,
  "tokens": [
    {
      "token_id": "f8e7d6c5-b4a3-2190-fedc-ba0987654321",
      "imsi": "310380100000001",
      "created_at": 1712834400,
      "expires_at": 1712920800,
      "expires_in_seconds": 72340,
      "validity": 86400,
      "terminal_id": "terminal_001",
      "app_name": null,
      "auth_method": "EAP-AKA"
    }
  ]
}
```

Champs de Jeton

Champ	Type	Description
`token_id`	String	Identifiant unique du jeton
`imsi`	String	IMSI de l'abonné
`created_at`	Integer	Heure de création du jeton (secondes d'époque Unix)
`expires_at`	Integer	Heure d'expiration du jeton (secondes d'époque Unix)
`expires_in_seconds`	Integer	Secondes restantes avant l'expiration
`validity`	Integer	Durée totale de validité du jeton en secondes
`terminal_id`	String	ID de terminal de l'appareil qui possède ce jeton
`app_name`	String	Nom de l'application (si limité)
`auth_method`	String	Comment le jeton a été émis (par exemple, `"EAP-AKA"`)

Obtenir un Jeton

```
GET /api/tokens/:id
```

```
curl -sk https://localhost:8443/api/tokens/f8e7d6c5-b4a3-2190-
fedc-ba0987654321
```

Retourne `404` si le jeton n'existe pas ou a expiré.

Révoquer un Jeton

```
DELETE /api/tokens/:id
```

```
curl -sk -X DELETE https://localhost:8443/api/tokens/f8e7d6c5-b4a3-2190-fedc-ba0987654321
```

Révoque immédiatement le jeton. L'appareil devra se ré-authentifier via EAP-AKA.

Réponse

```
{
  "status": "ok",
  "token_id": "f8e7d6c5-b4a3-2190-fedc-ba0987654321"
}
```

Diameter

Retourne l'état de connexion de pair Diameter pour surveiller la connectivité AAA 3GPP.

```
GET /api/diameter
```

```
curl -sk https://localhost:8443/api/diameter
```

Réponse


```
{
  "status": "configured",
  "connected_count": 1,
  "disconnected_count": 0,
  "peers": [
    {
      "host": "dra01.epc.mnc001.mcc001.3gppnetwork.org",
      "status": "Connected",
      "ip": "10.179.2.233",
      "port": 3868,
      "transport": "tcp",
      "connection_initiation": "OmniSEP -> Peer",
      "realm": "epc.mnc001.mcc001.3gppnetwork.org",
      "product_name": "OmniDRA",
      "application_ids": {}
    }
  ]
}
```


Champs de Réponse

Champ	Type	Description
`status`	String	État de Diameter : `"configured"`, `"not_configured"`, ou `"no_peers"`
`connected_count`	Integer	Nombre de pairs connectés
`disconnected_count`	Integer	Nombre de pairs déconnectés
`peers`	Array	Détails des pairs (voir ci-dessous)

Champs de Pair

Champ	Type	Description
`host`	String	Origine-Hôte Diameter du pair
`status`	String	État de la connexion : `"Connected"`, `"Disconnected"`, ou `"Unknown"`
`ip`	String	Adresse IP du pair
`port`	Integer	Port Diameter du pair
`transport`	String	Protocole de transport (`"tcp"` ou `"sctp"`)
`connection_initiation`	String	Qui initie la connexion (par exemple, `"OmniSEP -> Peer"`)
`realm`	String	Domaine Diameter du pair
`product_name`	String	Nom du produit annoncé par le pair
`application_ids`	Object	IDs d'application Diameter annoncés par le pair

Valeurs d'État de Diameter

État	Description
`configured`	Diameter est configuré avec un ou plusieurs pairs
`not_configured`	Aucune configuration Diameter présente. Les demandes EAP-AKA sont rejetées.
`no_peers`	Diameter est configuré mais aucun pair n'est défini

XCAP

Gérez les profils de Services Supplémentaires XCAP (Simservs). Les profils contiennent des paramètres de renvoi d'appel, de barring d'appel et d'identification de l'appelant par abonné.

Lister les Profils

```
GET /api/xcap
```

```
# Lister tous
curl -sk https://localhost:8443/api/xcap

# Rechercher par MSISDN
curl -sk "https://localhost:8443/api/xcap?query=61400"
```

Paramètres de Requête

Paramètre	Type	Par défaut	Description
`query`	String	-	Filtrer par MSISDN (correspondance partielle, insensible à la casse)

Réponse

```
{
  "count": 1,
  "profiles": [
    {
      "msisdn": "61400000001",
      "profile": {
        "originating_identity_presentation": {"active": true},
        "originating_identity_presentation_restriction":
{"active": false},
        "communication_waiting": {"active": true},
        "communication_diversion": {
          "active": true,
          "rules": []
        },
        "incoming_communication_barring": {"active": false},
        "outgoing_communication_barring": {"active": false}
      }
    }
  ]
}
```


Obtenir un Profil

```
GET /api/xcap/:msisdn
```

```
curl -sk https://localhost:8443/api/xcap/61400000001
```

Retourne `404` si aucun profil n'existe pour le MSISDN donné.

Supprimer un Profil

```
DELETE /api/xcap/:msisdn
```

```
curl -sk -X DELETE https://localhost:8443/api/xcap/61400000001
```

Supprime le profil XCAP du stockage local. Cela n'affecte pas le profil stocké dans le HSS.

Réponse

```
{
  "status": "ok",
  "msisdn": "61400000001"
}
```

Réponses d'Erreur

Tous les points de terminaison retournent des erreurs dans un format cohérent :

```
{
  "error": "Enregistrement d'activité non trouvé"
}
```

Codes d'État HTTP

Code	Signification
200	Succès
404	Ressource non trouvée
422	Entité non traitable (erreur de validation)

Configuration

L'API de gestion est configurée dans `config.exs` au moment de la compilation pour les définitions de routes, et peut être remplacée à l'exécution pour les paramètres réseau.

Configuration au Moment de la Compilation (config.exs)

```
config :api_ex,
  api: %{
    port: 8443,
    listen_ip: "0.0.0.0",
    product_name: "OmniSEP",
    title: "API - OmniSEP",
    hostname: "localhost",
    enable_tls: true,
    tls_cert_path: "priv/cert/omnitouch.crt",
    tls_key_path: "priv/cert/omnitouch.pem",
    routes: [...]
  }
```

Remplacements à l'Exécution (runtime.exs)

Le port, l'IP d'écoute et les chemins TLS peuvent être remplacés à l'exécution :

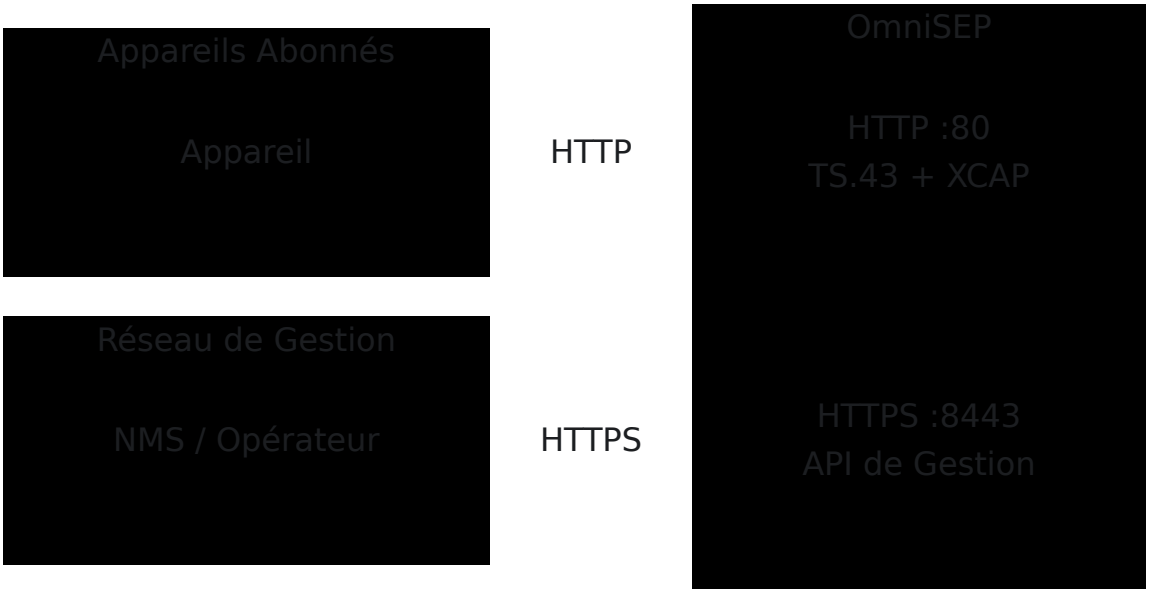
```
config :api_ex,
  api: %{
    port: 8443,
    listen_ip: "0.0.0.0",
    enable_tls: true,
    tls_cert_path: "priv/cert/omnitouch.crt",
    tls_key_path: "priv/cert/omnitouch.pem"
  }
```

Paramètres de Configuration

Paramètre	Type	Par défaut	Description
`port`	Integer	8443	Port HTTPS pour l'API de gestion
`listen_ip`	String	`"0.0.0.0"`	Adresse IP à lier. Utilisez une IP d'interface de gestion pour restreindre l'accès.
`product_name`	String	`"OmniSEP"`	Nom du produit affiché dans les réponses API et Swagger UI
`title`	String	`"API - OmniSEP"`	Titre affiché dans Swagger UI
`hostname`	String	`"localhost"`	Nom d'hôte pour la spécification OpenAPI
`enable_tls`	Boolean	`true`	Activer TLS. Doit toujours être `true` en production.

Paramètre	Type	Par défaut	Description
`tls_cert_path`	String	`"priv/cert/omnitouch.crt"`	Chemin vers le fichier de certificat TLS
`tls_key_path`	String	`"priv/cert/omnitouch.pem"`	Chemin vers le fichier de clé privée TLS
`routes`	List	-	Définitions de routes API (uniquement au moment de la compilation)

Ports Réseau



Port	Protocole	But
80 (configurable)	HTTP	Droits TS.43 et XCAP destinés aux abonnés
8443 (configurable)	HTTPS	API de Gestion (ce document)
3868	TCP	Diameter (interface SWm vers AAA/DRA)

Guide de dépannage OmniSEP

Problèmes courants et résolutions pour la plateforme de point de service OmniSEP.

Table des matières

- Journal d'activité
- Problèmes d'attribution TS.43
- Problèmes de Simservs XCAP
- Problèmes d'authentification
- Problèmes de connectivité
- Problèmes de stockage

Journal d'activité

Le journal d'activité fournit une vue en temps réel de toutes les demandes à OmniSEP, y compris les requêtes d'attribution TS.43 et les opérations XCAP.

Fonctionnalités :

- Filtrer par type de demande (XCAP, requête d'attribution, défi EAP, etc.)
- Rechercher par IMSI, MSISDN, ID de terminal ou IP client
- Voir la méthode HTTP (GET, PUT, POST, DELETE) et le statut de la réponse
- Cliquez sur n'importe quelle ligne pour voir des informations détaillées

Panneau de détails de l'activité

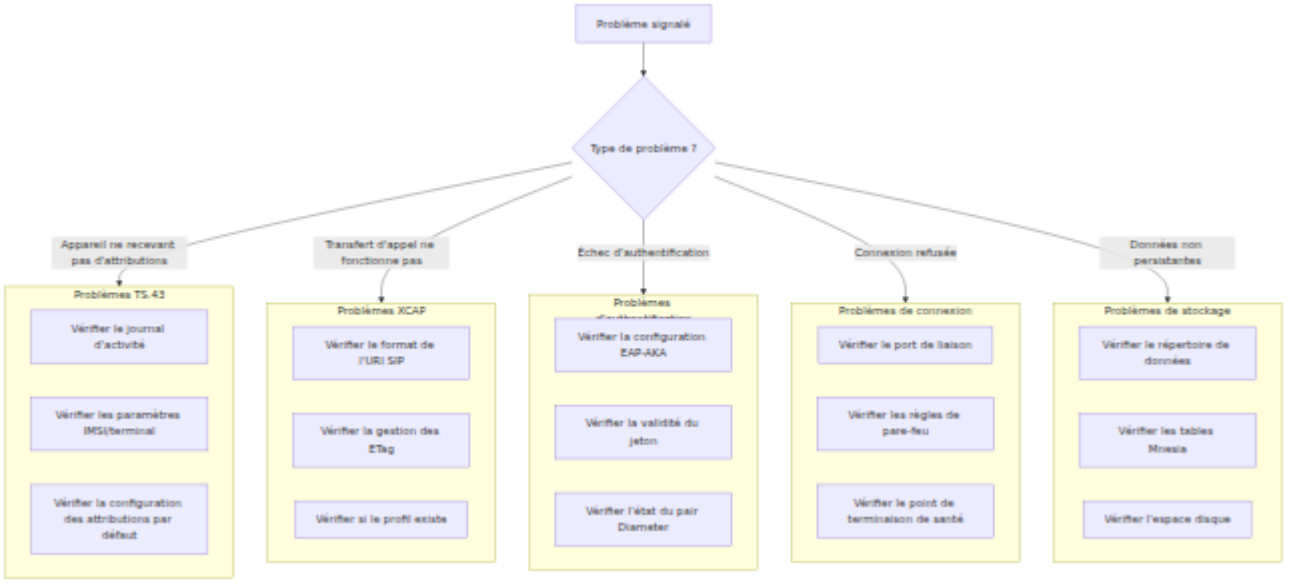
Sélectionner un enregistrement d'activité montre des détails complets de la demande/réponse :

Informations capturées :

- **Horodatage et IP client** : Quand et où la demande a été faite
- **Type de demande et méthode HTTP** : XCAP, requête d'attribution, etc.
- **Informations sur l'abonné** : IMSI, MSISDN (lorsqu'elles sont disponibles)
- **Informations sur le terminal** : ID de l'appareil, fournisseur, modèle (extrait de l'User-Agent)
- **Chemin de la demande** : Chemin XCAP complet ou point de terminaison d'attribution
- **User-Agent** : En-tête User-Agent brut
- **En-têtes de demande** : Content-Type, If-Match, en-têtes 3GPP, etc.

- **Corps de la demande/réponse** : Contenu XML pour les opérations XCAP
- **Statut de la réponse** : Succès, erreur serveur, erreur client avec code HTTP

Flux de travail de diagnostic



Problèmes d'attribution TS.43

L'appareil signale "Service non disponible"

Symptômes : L'appareil affiche VoWiFi/VoLTE comme indisponible malgré un abonnement correct

Causes possibles :

- Attributions par défaut configurées avec `entitlement_status: 0`
- Attribution personnalisée définie pour l'abonné avec un statut désactivé
- Appareil envoyant un IMSI ou des paramètres de terminal incorrects

Résolution :

1. Vérifiez le journal d'activité pour les demandes de l'abonné :

```
GET /api/activity?imsi=<subscriber_imsi>
```

2. Vérifiez la réponse d'attribution dans les enregistrements d'activité

3. Vérifiez la configuration des attributions par défaut :

```
config :omni_sep, :default_entitlements,
  vowifi: %{
    entitlement_status: 1,  # Doit être 1 pour activé
    ...
  }
```

4. V��rifiez les attributions personnalisées qui remplacent les valeurs par défaut :

```
GET /api/entitlements/<imsi>
```

L'appareil reçoit un mauvais statut d'attribution

Symptômes : L'appareil reçoit des valeurs d'attribution différentes de celles attendues

Causes possibles :

- Attribution personnalisée configurée pour l'abonné
- Mauvais app_id étant interrogé
- Incompatibilité de configuration entre les environnements

Résolution :

1. Vérifiez quel app_id l'appareil demande (vérifiez le journal d'activité)

2. App IDs courants :

App ID	Service
ap2003	VoLTE/VoNR
ap2004	VoWiFi
ap2005	SMSoIP

3. Vérifiez les attributions personnalisées :

```
GET /api/entitlements/<imsi>
```

4. Supprimez l'attribution personnalisée indésirable :

```
DELETE /api/entitlements/<imsi>/<app_id>
```

Paramètres manquants dans la demande

Symptômes : HTTP 400 Bad Request avec erreur "Paramètres manquants"

Causes possibles :

- Appareil ne pas envoyant les paramètres TS.43 requis
- Paramètres dans un format incorrect
- Problèmes d'encodage d'URL

Paramètres requis :

Paramètre	Description
`terminal_id`	IMEI de l'appareil (15 chiffres)
`terminal_vendor`	Fabricant (max 4 caractères)
`terminal_model`	Nom du modèle (max 10 caractères)
`terminal_sw_version`	Version du logiciel
`entitlement_version`	Version du protocole (les clients Samsung envoient "1.0", les autres "2.0" ou supérieur)
`app`	ID(s) de l'application à interroger

Résolution :

1. Vérifiez le journal d'activité pour les détails de la demande brute
2. Vérifiez que l'appareil envoie tous les paramètres requis
3. Pour Android, assurez-vous que l'User-Agent suit le format :

```
PRD-TS43 term-<vendor>/<model> client-IMS-Entitlement/1.0 OS-Android/<version>
```

Incompatibilité de version (HTTP 406)

Symptômes : L'appareil reçoit HTTP 406 Not Acceptable

Causes possibles :

- Appareil envoyant un `entitlement_version` en dehors de la plage supportée

Résolution :

1. Vérifiez le `entitlement_version` que l'appareil a envoyé dans le journal d'activité

2. Vérifiez la plage supportée (`min_entitlement_version`, par défaut "1.0", et `max_entitlement_version`, par défaut "13.0")

Problèmes de Simservs XCAP

Profil non trouvé (HTTP 404)

Symptômes : La demande GET XCAP retourne 404

Causes possibles :

- Profil jamais créé pour l'abonné
- Mauvais format d'URI SIP
- MSISDN non lié au profil

R��solution :

1. Vérifiez le format de l'URI SIP dans la demande :

```
/simservs.ngn.etsi.org/users/sip:+
<msisdn>@<domain>/simservs.xml
```

2. Vérifiez si le profil existe via l'API de gestion :

```
GET /api/xcap/<msisdn>
```

3. Créez le profil s'il est manquant :

```
POST /api/xcap/<msisdn>
Content-Type: application/json

{
  "oip": {"active": true},
  "oir": {"active": true, "default_behaviour": "presentation-
not-restricted"},
  "no_reply_timer": 20,
  "call_forwarding": {},
  "call_barring_incoming": {},
  "call_barring_outgoing": {}
}
```

Incompatibilité d'ETag (HTTP 412)

Symptômes : La demande PUT ou DELETE retourne HTTP 412 Precondition Failed

Causes possibles :

- Client utilisant un ETag obsolète
- Modification concurrente par un autre client
- ETag non envoyé avec la demande conditionnelle

Résolution :

1. Récupérez le document actuel pour obtenir un nouvel ETag :

```
GET /simservs.ngn.etsi.org/users/<sip_uri>/simservs.xml
```

2. Utilisez l'ETag retourné dans l'en-tête `If-Match` :

```
PUT /simservs.ngn.etsi.org/users/<sip_uri>/simservs.xml
If-Match: "<etag_value>"
Content-Type: application/xcap-el+xml

<simservs>...</simservs>
```

3. Pour des mises à jour inconditionnelles (test uniquement), omettez l'en-tête `If-Match`

XML invalide (HTTP 400)

Symptômes : La demande PUT retourne HTTP 400 Bad Request

Causes possibles :

- XML mal formé dans le corps de la demande
- Espaces de noms requis manquants
- Structure d'élément invalide

Espaces de noms requis :

Préfixe	Namespace
(par défaut)	`http://uri.etsi.org/ngn/params/xml/simservs/xcap`
cp	`urn:ietf:params:xml:ns:common-policy`

Résolution :

1. Validez la structure XML
2. Assurez-vous que l'élément racine inclut les espaces de noms requis :

```
<simservs
xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
          xmlns:cp="urn:ietf:params:xml:ns:common-policy">
```

3. Vérifiez que les noms d'éléments correspondent à la spécification ETSI TS 183 023

Le transfert d'appel ne s'active pas

Symptômes : Paramètres de transfert d'appel enregistrés mais les appels ne sont pas transférés

Causes possibles :

- Règle désactivée dans le profil
- Mauvais type de condition
- Format de numéro cible incorrect

Résolution :

1. Vérifiez que `communication-diversion` est actif :

   ```
   <communication-diversion active="true">
   ```

2. Vérifiez que la règle est correctement structurée :

   ```
   <cp:rule id="cfb">
     <cp:conditions>
       <busy/>
     </cp:conditions>
     <cp:actions>
       <forward-to>
         <target>tel:+15557654321</target>
       </forward-to>
     </cp:actions>
   </cp:rule>
   ```

3. Identifiants de règle et conditions valides :

ID de règle	Condition	Description
`cfu`	(aucun)	Inconditionnel
`cfb`	`busy`	En cas d'occupation
`cfna`	`no-answer`	En cas de non-réponse
`cfnrc`	`not-reachable`	Non joignable
`cfnl`	`not-logged-in`	Non connecté

4. La cible doit utiliser le format URI `tel:` avec un numéro E.164

Problèmes d'authentification

Défi EAP-AKA non retourné

Symptômes : Demande initiale avec EAP_ID retourne une erreur au lieu d'un défi

Causes possibles :

- EAP-AKA désactivé dans la configuration
- Format EAP_ID invalide
- Problèmes de connectivité avec le pair Diameter

Résolution :

1. Vérifiez que EAP-AKA est activé :

```
config :omni_sep, :eap_aka,
  enabled: true
```

2. Vérifiez le format EAP_ID (NAI racine) :

```
0<IMSI>@nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
```

   Exemple : `0310410123456789@nai.epc.mnc410.mcc310.3gppnetwork.org`

3. Si des pairs Diameter sont configurés, vérifiez la connectivité
4. Si aucun pair AAA n'est connecté, EAP-AKA est rejeté (HTTP 511, ou 503 lorsque EAP-AKA est désactivé)

Jeton invalide (HTTP 511)

Symptômes : Demande avec jeton retourne HTTP 511 Network Authentication Required

Causes possibles :

- Jeton expiré
- Secret de signature du jeton changé
- Jeton généré par une instance différente

Résolution :

1. Vérifiez la période de validité du jeton :

   ```
   config :omni_sep, :token,
     validity_seconds: 86400  # 24 heures par défaut
   ```

2. Si le secret a été tourné, tous les jetons existants sont invalidés
3. L'appareil doit revenir à l'authentification EAP-AKA pour obtenir un nouveau jeton
4. Vérifiez que toutes les instances utilisent le même `signing_secret`

Incompatibilité de signature de jeton

Symptômes : Jeton ayant l'air valide rejeté

Causes possibles :

- Jeton provenant d'un environnement différent
- Incompatibilité de secret de signature entre les instances
- Jeton altéré

Résolution :

1. Assurez-vous que `signing_secret` est cohérent entre toutes les instances :

   ```
   config :omni_sep, :token,
     signing_secret: System.get_env("OMNI_SEP_TOKEN_SECRET")
   ```

2. Utilisez une variable d'environnement pour le secret en production

3. Tournez les secrets entre toutes les instances simultanément

Problèmes de connectivité

Service non joignable

Symptômes : Connexion refusée ou délai d'attente

Causes possibles :

- Service non en cours d'exécution
- Mauvaise configuration de port
- Pare-feu bloquant le trafic

Résolution :

1. Vérifiez la santé du service :

   ```
   curl http://<host>:9014/health
   ```

2. Vérifiez la configuration du port :

```
config :omni_sep,
  http_port: 9014,
  http_ip: {0, 0, 0, 0}
```

3. Vérifiez que les règles de pare-feu autorisent le trafic sur le port configuré
4. Vérifiez que le service écoute :

```
netstat -tlnp | grep 9014
```

Le contrôle de santé retourne non sain

Symptômes : Le point de terminaison `/health` retourne un statut non-200

Causes possibles :

- Service dépendant indisponible
- Tables de stockage non initialisées
- Démarrage de l'application incomplet
- Répertoire de données Mnesia non accessible en écriture

Résolution :

1. Vérifiez les journaux de l'application pour des erreurs de démarrage
2. Vérifiez l'initialisation du stockage :
    - Tables Mnesia (journal d'activité)
    - Tables ETS (attributions, jetons, sessions, profils XCAP)
3. Vérifiez les permissions du répertoire de données Mnesia :

```
ls -la priv/data/mnesia/
```

4. Si Mnesia échoue à démarrer, vérifiez les fichiers corrompus et envisagez de vider le répertoire de données

5. Redémarrez l'application si des tables manquent

Temps de réponse lents

Symptômes : Les demandes prennent plus de temps que prévu

Causes possibles :

- Délais d'attente des pairs Diameter
- Arriéré de journalisation d'activité
- Charge concurrente élevée

Résolution :

1. Vérifiez la configuration des pairs Diameter :

   ```
   config :diameter_ex, :diameter,
     request_timeout: 5000  # 5 secondes par défaut
   ```

2. Surveillez la taille du journal d'activité par abonné

3. Vérifiez l'utilisation de la mémoire des tables ETS

4. Envisagez une mise à l'échelle horizontale pour une charge élevée

Problèmes de stockage

Journal d'activité non persistant

Symptômes : Enregistrements d'activité perdus après redémarrage

Causes possibles :

- Répertoire de données Mnesia non accessible en écriture
- Application terminée avant que Mnesia puisse écrire sur le disque
- Disque plein

Résolution :

1. Vérifiez que le répertoire de données existe et est accessible en écriture :

   ```
   ls -la priv/data/mnesia/
   ```

2. Vérifiez les journaux de transaction Mnesia (.DCL fichiers) - ceux-ci contiennent des écritures récentes :

   ```
   ls -la priv/data/mnesia/*.DCL
   ```

3. Assurez-vous d'un arrêt gracieux pour permettre à Mnesia d'écrire :

   ```
   # N'utilisez pas kill -9, utilisez SIGTERM à la place
   kill -TERM <pid>
   ```

4. Vérifiez l'espace disque :

   ```
   df -h priv/data/
   ```

Schéma Mnesia corrompu

Symptômes : L'application échoue à démarrer avec des erreurs Mnesia

Causes possibles :

- Perte de courant ou crash pendant l'écriture
- Corruption de disque
- Versions d'Erlang mélangées

Résolution :

1. Vérifiez les journaux pour des erreurs Mnesia spécifiques

2. Si les données peuvent être perdues, videz et réinitialisez :

```
rm -rf priv/data/mnesia/*
# Redémarrez l'application - les tables seront recréées
```

3. Si les données doivent être préservées, essayez de réparer Mnesia :

```
:mnesia.stop()
:mnesia.start()
:mnesia.wait_for_tables([:activity, :activity_by_imsi,
:activity_by_terminal], 30000)
```

Journal d'activité devenant trop volumineux

Symptômes : Utilisation du disque augmentant, requêtes lentes

Causes possibles :

- Volume de demandes élevé
- Période de conservation trop longue
- Limite par abonné trop élevée

Résolution :

1. Vérifiez les paramètres de conservation actuels :

```
config :omni_sep, :activity,
  max_records_per_subscriber: 1000,  # Réduisez si nécessaire
  retention_seconds: 2_592_000       # 30 jours, réduisez si
nécessaire
```

2. Surveillez la taille de la table :

```
ls -lh priv/data/mnesia/activity.*
```

3. Envisagez de réduire la période de conservation pour les déploiements à fort volume

Commandes de diagnostic

Vérification de la santé

```
curl -s http://localhost:9014/health | jq
```

Réponse attendue :

```
{
  "status": "ok",
  "service": "omni-sep",
  "version": "0.1.0",
  "services": ["entitlements", "xcap"]
}
```

Requête de journal d'activité

```
# Activité récente pour l'abonné
curl "http://localhost:9014/api/activity?imsi=<imsi>&limit=10"

# Activité par terminal
curl "http://localhost:9014/api/activity?terminal_id=
<imei>&limit=10"

# Activité dans une plage de temps
curl "http://localhost:9014/api/activity?from=<unix_ts>&to=
<unix_ts>"
```

Vérification des attributions

```
# Obtenir des attributions personnalisées
curl http://localhost:9014/api/entitlements/<imsi>

# Définir une attribution personnalisée
curl -X POST http://localhost:9014/api/entitlements/<imsi> \
  -H "Content-Type: application/json" \
  -d '{"app_id": "ap2004", "entitlement": {"entitlement_status":
1}}'
```

Vérification du profil XCAP

```
# Obtenir le profil
curl http://localhost:9014/api/xcap/<msisdn>

# Obtenir le document simservs complet
curl "http://localhost:9014/simservs.ngn.etsi.org/users/sip:+
<msisdn>@domain/simservs.xml"
```

Analyse des journaux

Modèles de journaux clés

Modèle	Signification
`[info] GET / ...`	Demande d'attribution entrante
`[info] POST / ...`	Demande POST entrante (EAP ou attribution)
`[warning] Missing parameters`	Validation de la demande échouée
`[error] EAP session timeout`	EAP-AKA non terminé à temps
`[debug] Token validated`	Authentification du jeton réussie

Activation de la journalisation de débogage

```
# config/dev.exs ou runtime
config :logger, :console,
  level: :debug,
  metadata: [:request_id, :imsi, :terminal_id]
```

Spécifications de référence

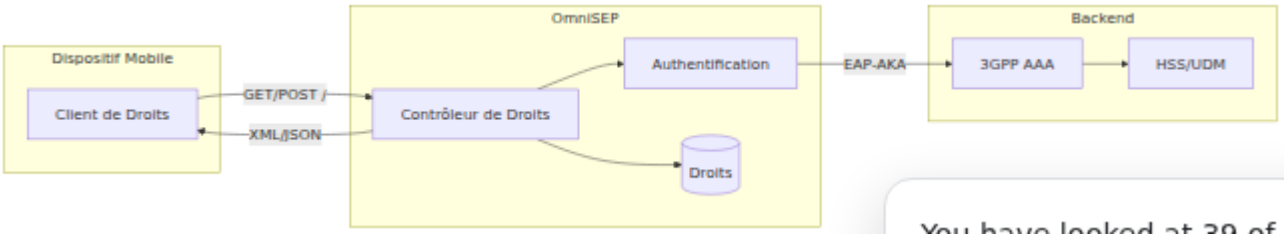
Pour le dépannage spécifique aux protocoles, référez-vous à :

Protocole	Spécification
TS.43	GSMA TS.43
XCAP	RFC 4825
Simservs	ETSI TS 183 023
EAP-AKA	RFC 4187
Diameter	RFC 6733

TS.43 Configuration des Droits

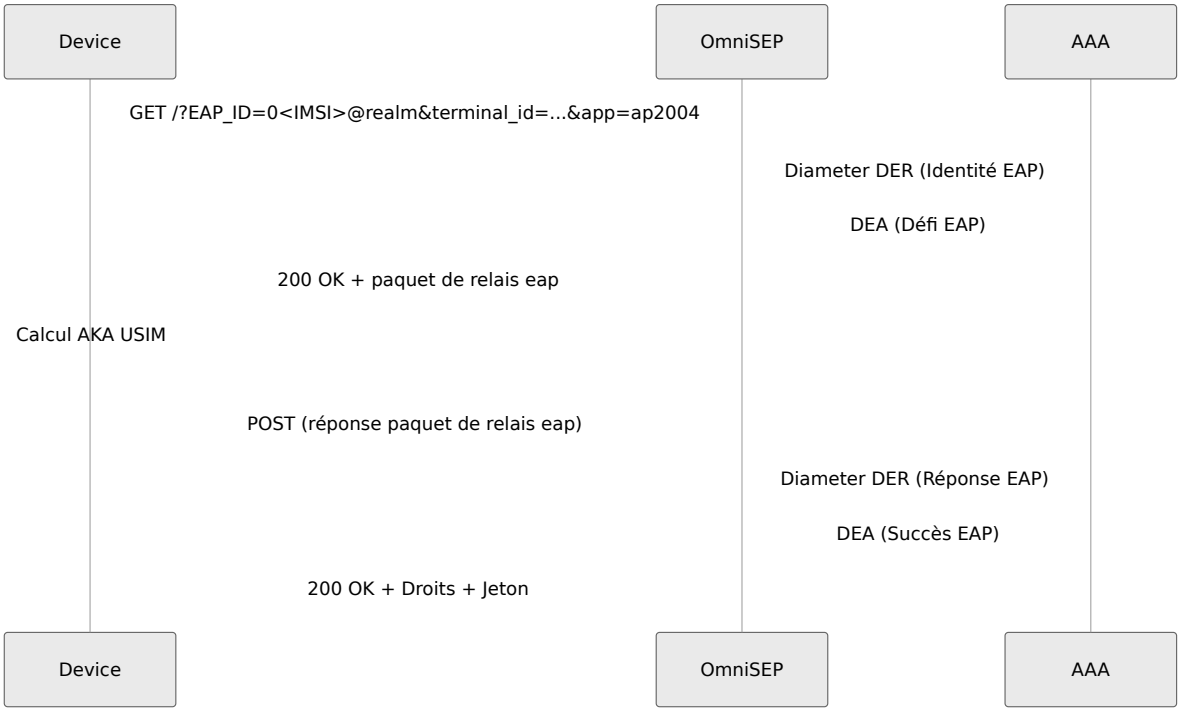
OmniSEP implémente la Configuration des Droits de Service GSMA TS.43, permettant aux dispositifs mobiles de consulter leurs droits de service (VoWiFi, VoLTE, SMS, etc.) depuis le réseau de l'opérateur.

Aperçu

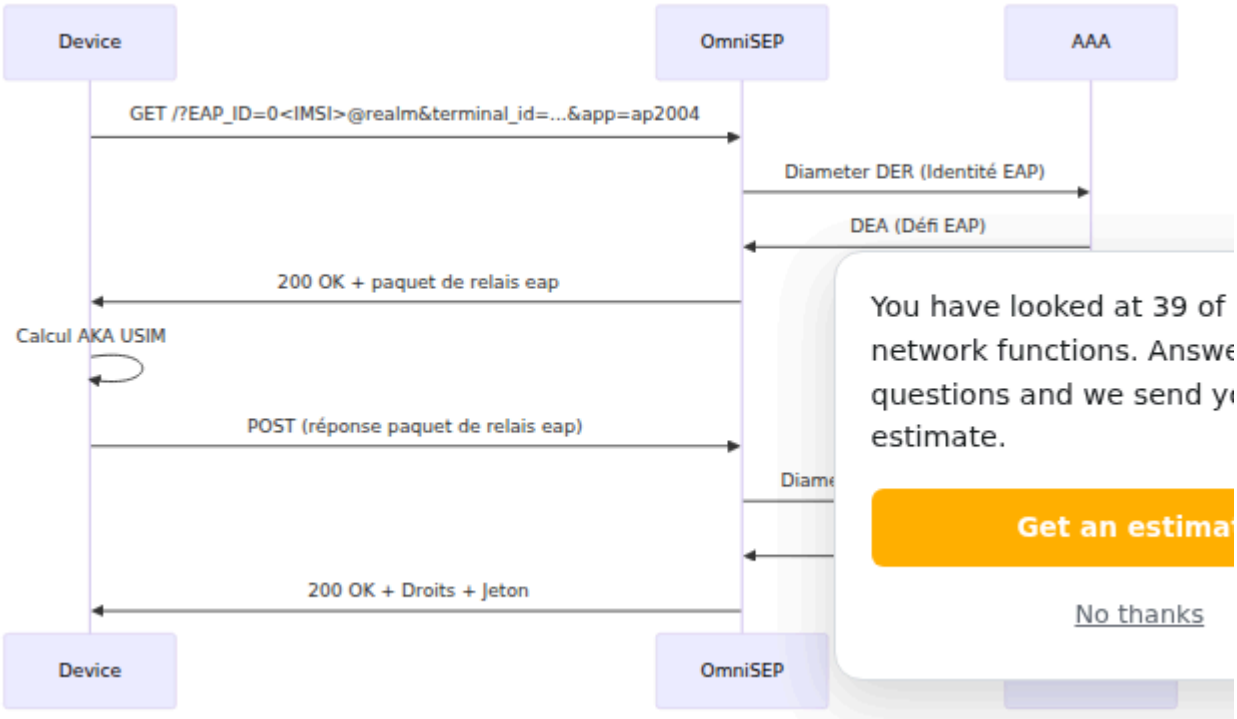


Flux de Demande

Authentification Initiale (EAP-AKA)



Ré-authentification Rapide (Jeton)



Interface HTTP

Point de Terminaison

Méthode	Chemin	Type de Contenu
GET	`/`	Paramètres de requête
POST	`/`	`application/json`

Paramètres Requis

Paramètre	Type	Description
`terminal_id`	String	IMEI du dispositif (15 chiffres)
`terminal_vendor`	String	Fabricant du dispositif (max 4 caractères par RCC.14)
`terminal_model`	String	Modèle du dispositif (max 10 caractères par RCC.14)
`terminal_sw_version`	String	Version du logiciel (max 20 caract��res par RCC.14)
`entitlement_version`	String	Version du protocole (par exemple, "2.0")
`app`	String/Liste	ID(s) de l'application à interroger

Paramètres d'Authentification

L'une de ces méthodes d'authentification est requise :

Paramètre	Description
`EAP_ID`	NAI racine pour EAP-AKA : `0<IMSI>@nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org`
`token`	Jeton d'authentification de la réponse précédente
`temporary_token`	Jeton temporaire
`operator_token`	Jeton émis par l'opérateur

Paramètres Optionnels

Paramètre	Type	Description
`IMSI`	String	Requis avec `token` pour la ré-auth rapide
`app_name`	String	Nom de l'application
`app_version`	String	Version de l'application
`notif_action`	Integer	Action de notification (0=désactiver, 1=GCM, 2=FCM)
`notif_token`	String	Jeton de notification push
`vers`	Integer	Version de configuration pour la détection de changement

Exemples de Demande

GET avec Jeton :

```
GET /?
terminal_id=123456789012345&terminal_vendor=Goog&terminal_model=Pixel
```

POST avec EAP-AKA :

```
{
  "terminal_id": "123456789012345",
  "terminal_vendor": "Goog",
  "terminal_model": "Pixel8",
  "terminal_sw_version": "14.0",
  "entitlement_version": "2.0",
  "app": "[ap2003,ap2004]",
  "EAP_ID":
"0310410123456789@nai.epc.mnc410.mcc310.3gppnetwork.org"
}
```

Formats de Réponse

En-tête Accept

En-tête Accept	Format de Réponse
`text/vnd.wap.connectivity-xml`	XML (par défaut)
`application/json`	JSON
`application/vnd.gsma.eap-relay.v1.0+json`	JSON de relais EAP

Réponse XML

```xml
<?xml version="1.0"?>
<wap-provisioningdoc version="1.1">
  <characteristic type="VERS">
    <parm name="version" value="2"/>
    <parm name="validity" value="86400"/>
  </characteristic>
  <characteristic type="TOKEN">
    <parm name="token" value="eyJ0eXAi..."/>
    <parm name="validity" value="86400"/>
  </characteristic>
  <characteristic type="APPLICATION">
    <parm name="AppID" value="ap2004"/>
    <characteristic type="ap2004">
      <parm name="EntitlementStatus" value="1"/>
      <parm name="AddrStatus" value="2"/>
      <parm name="TC_Status" value="2"/>
      <parm name="ProvStatus" value="1"/>
    </characteristic>
  </characteristic>
</wap-provisioningdoc>
```

Réponse JSON


```
{
  "Vers": {
    "version": "2",
    "validity": "86400"
  },
  "Token": {
    "token": "eyJ0eXAi...",
    "validity": "86400"
  },
  "ap2004": {
    "EntitlementStatus": "1",
    "AddrStatus": "2",
    "TC_Status": "2",
    "ProvStatus": "1"
  }
}
```


Réponse de Défi EAP

Lorsque l'authentification EAP-AKA est en cours :


```
{
  "eap-relay-packet": "AQEALBcBAAAn..."
}
```

IDs d'Application

Applications Supportées

ID d'App	Service	Référence
ap2003	Voix sur Cellulaire (VoLTE/VoNR)	TS.43 Section 4
ap2004	Voix sur WiFi (VoWiFi)	TS.43 Section 3
ap2005	SMS sur IP	TS.43 Section 5
ap2006	Compagnon ODSA	TS.43 Section 6
ap2009	ODSA Principal	TS.43 Section 6
ap2010	Augmentation de Plan de Données	TS.43 Section 7
ap2011	Demandes Initiées par le Serveur	TS.43 Section 8
ap2012	Facturation Directe par l'Opérateur	TS.43 Section 9
ap2013	Identité Utilisateur Privée	TS.43 Section 10
ap2014	Informations sur le Numéro de Téléphone	TS.43 Section 11
ap2016	Droit Satellite	TS.43 Section 12

Champs de Réponse VoWiFi (ap2004)

Champ	Type	Valeurs	Description
`EntitlementStatus`	Integer	0-3	Disponibilité du service
`AddrStatus`	Integer	0-3	Statut de vérification d'adresse E911
`TC_Status`	Integer	0-3	Statut des Termes & Conditions
`ProvStatus`	Integer	0-3	Statut de Provisioning
`ServiceFlow_URL`	String	URL	URL du flux de service
`ServiceFlow_UserData`	String	-	Données pour le flux de service

Valeurs de Statut :

Valeur	EntitlementStatus	AddrStatus/TC_Status/ProvStatus
0	Désactivé	Non Disponible
1	Activé	Disponible
2	Incompatible	Non Requis
3	Provisioning	En Cours

Champs de Réponse VoLTE (ap2003)

VoLTE utilise un tableau d'entrées par technologie d'accès :

Champ	Type	Valeurs	Description
`AccessType`	Integer	1=LTE, 2=NR	Technologie d'accès radio
`HomeRoamingNWType`	Integer	1-3	Portée du réseau
`EntitlementStatus`	Integer	0-1	Disponibilité du service
`NetworkVoiceIRATCapability`	String	-	Capacité vocale (5G uniquement)

Valeurs de HomeRoamingNWType :

Valeur	Signification
1	Domicile et Roaming
2	Domicile Seulement
3	Roaming Seulement

Réponses d'Erreur

Statut HTTP	Signification	Description
400	Mauvaise Requête	Paramètres requis manquants
403	Interdit	Échec de l'authentification
406	Non Acceptable	Version de protocole non supportée
511	Authentification Réseau Requise	Jeton invalide ou EAP-AKA requis

Format de Réponse d'Erreur

```
HTTP/1.1 400 Bad Request
Content-Type: text/plain

Bad Request: Missing parameters ["terminal_id"]
```

Droits Personnalisés

Définir des Droits Personnalisés

Utilisez l'API de gestion pour définir des droits personnalisés pour des abonnés spécifiques :

```
POST /api/entitlements/{imsi}
Content-Type: application/json

{
  "app_id": "ap2004",
  "entitlement": {
    "entitlement_status": 0,
    "addr_status": 1,
    "tc_status": 1,
    "prov_status": 0,
    "service_flow_url": "https://activate.example.com/vowifi",
    "message_for_incompatible": "VoWiFi nécessite une vérification
d'adresse"
  }
}
```

Récupérer des Droits

```
GET /api/entitlements/{imsi}
```

Renvoie tous les droits personnalisés pour l'abonné :

```
{
  "imsi": "310410123456789",
  "entitlements": {
    "ap2004": {
      "entitlement_status": 1,
      "addr_status": 2,
      "tc_status": 2,
      "prov_status": 1
    }
  }
}
```

Journalisation des Activités

Toutes les demandes de droits sont enregistrées à des fins d'audit.

Recherche d'Activité

```
GET /api/activity?
imsi=310410123456789&from=1704067200&to=1704153600&limit=100
```

Paramètre	Type	Description
`imsi`	String	Filtrer par IMSI de l'abonné
`terminal_id`	String	Filtrer par ID de terminal de dispositif
`from`	Integer	Horodatage de début (époque Unix)
`to`	Integer	Horodatage de fin (époque Unix)
`limit`	Integer	Nombre maximum d'enregistrements à retourner
`offset`	Integer	Décalage de pagination

Enregistrement d'Activité


```
{
  "id": "550e8400-e29b-41d4-a716-446655440000",
  "timestamp": "2024-01-15T10:30:00Z",
  "imsi": "310410123456789",
  "terminal_id": "123456789012345",
  "terminal_vendor": "Google",
  "terminal_model": "Pixel8",
  "app_ids": ["ap2003", "ap2004"],
  "client_ip": "192.168.1.100",
  "user_agent": "PRD-TS43 Goog/Pixel8 client-IMS-Entitlement/1.0
OS-Android/14.0",
  "auth_method": "TOKEN",
  "response_code": 200
}
```

Compatibilité du Client Android

OmniSEP est testé avec la bibliothèque `service_entitlement` d'Android AOSP.

Format de User-Agent

Les dispositifs Android utilisent ce format de User-Agent :

```
PRD-TS43 term-<vendor>/<model> <client_ts43>/<app_version> OS-Android/<sw_version>
```

Exemple :

```
PRD-TS43 term-Google/Pixel8 client-IMS-Entitlement/1.0 OS-Android/14.0
```

Plusieurs IDs d'Application

Android envoie plusieurs IDs d'application dans les requêtes POST sous forme de chaîne entre crochets :

```
{
  "app": "[ap2003,ap2004]"
}
```

OmniSEP analyse les deux formats :

- `"ap2003,ap2004"` - Séparé par des virgules
- `"[ap2003,ap2004]"` - Enclavé entre crochets (format Android)
- `["ap2003", "ap2004"]` - Tableau JSON

Spécifications de Référence

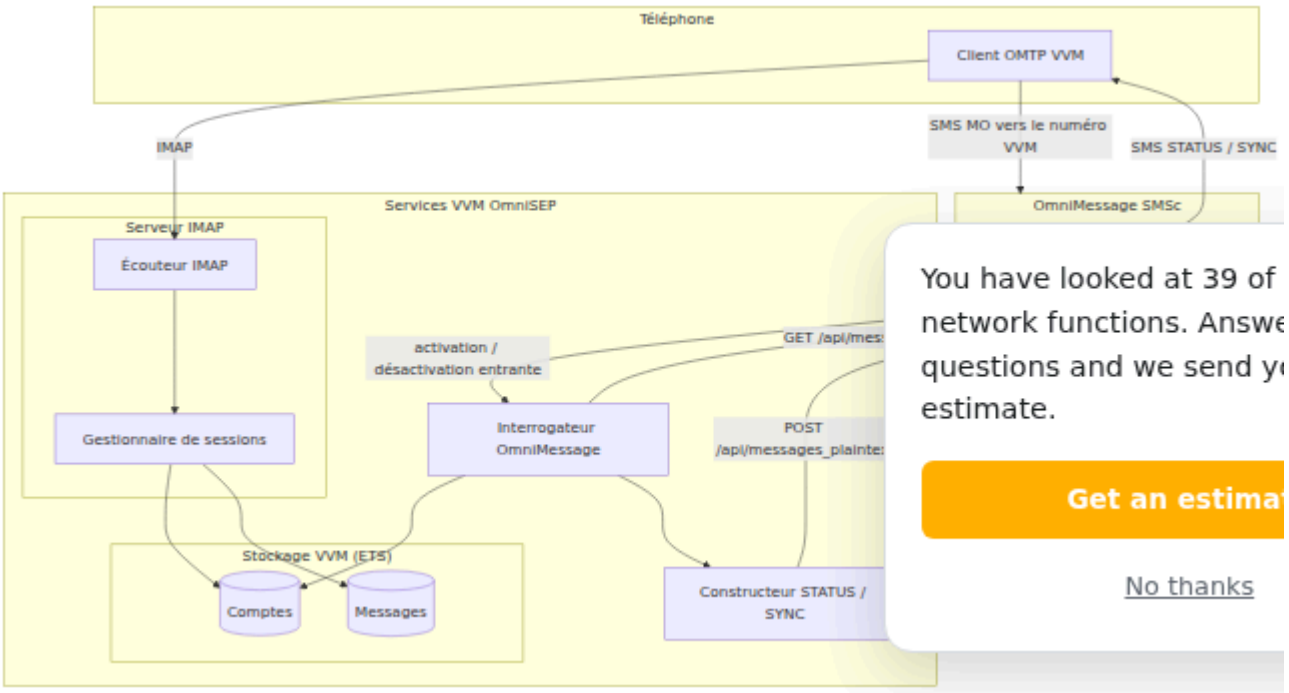
Spécification	Description
GSMA TS.43	Configuration des Droits de Service
GSMA RCC.14	Directives de Configuration des Dispositifs IMS
3GPP TS 33.220	Architecture de Démarrage Générique (GBA)
3GPP TS 29.273	Interfaces EPS AAA (SWm)

Messagerie Vocale Visuelle (VVM)

OmniSEP fournit un serveur de Messagerie Vocale Visuelle. Il implémente la spécification OMTP VVM et la GSMA TS.46. Le service permet à un téléphone de gérer la messagerie vocale via une interface IMAP. OmniSEP provisionne chaque téléphone par SMS et livre l'audio de la messagerie vocale et la transcription via IMAP.

OmniSEP ne se connecte pas directement au SMSC. Il utilise l'API HTTP OmniMessage pour tous les SMS. OmniSEP interroge OmniMessage pour les SMS VVM entrants des téléphones. OmniSEP envoie des SMS `STATUS` et `SYNC` aux téléphones via la même API.

Vue d'ensemble de l'architecture



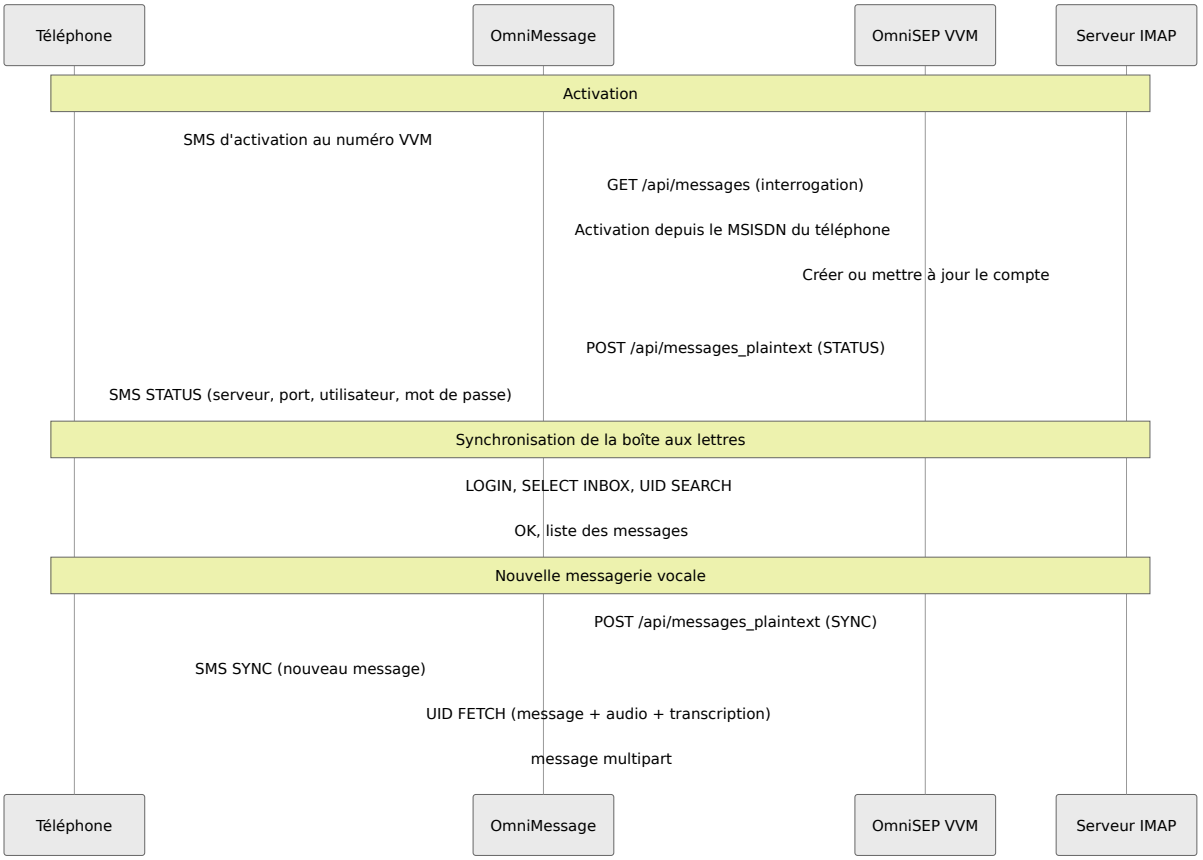
Le service se compose de trois parties :

- **Interrogateur OmniMessage** lit les SMS VVM entrants d'OmniMessage et provisionne les comptes.

- **Constructeur STATUS / SYNC** envoie des SMS OMTP au téléphone via OmniMessage.
- **Serveur IMAP** gère la boîte aux lettres, l'audio de la messagerie vocale et la transcription.

Flux de Provisionnement

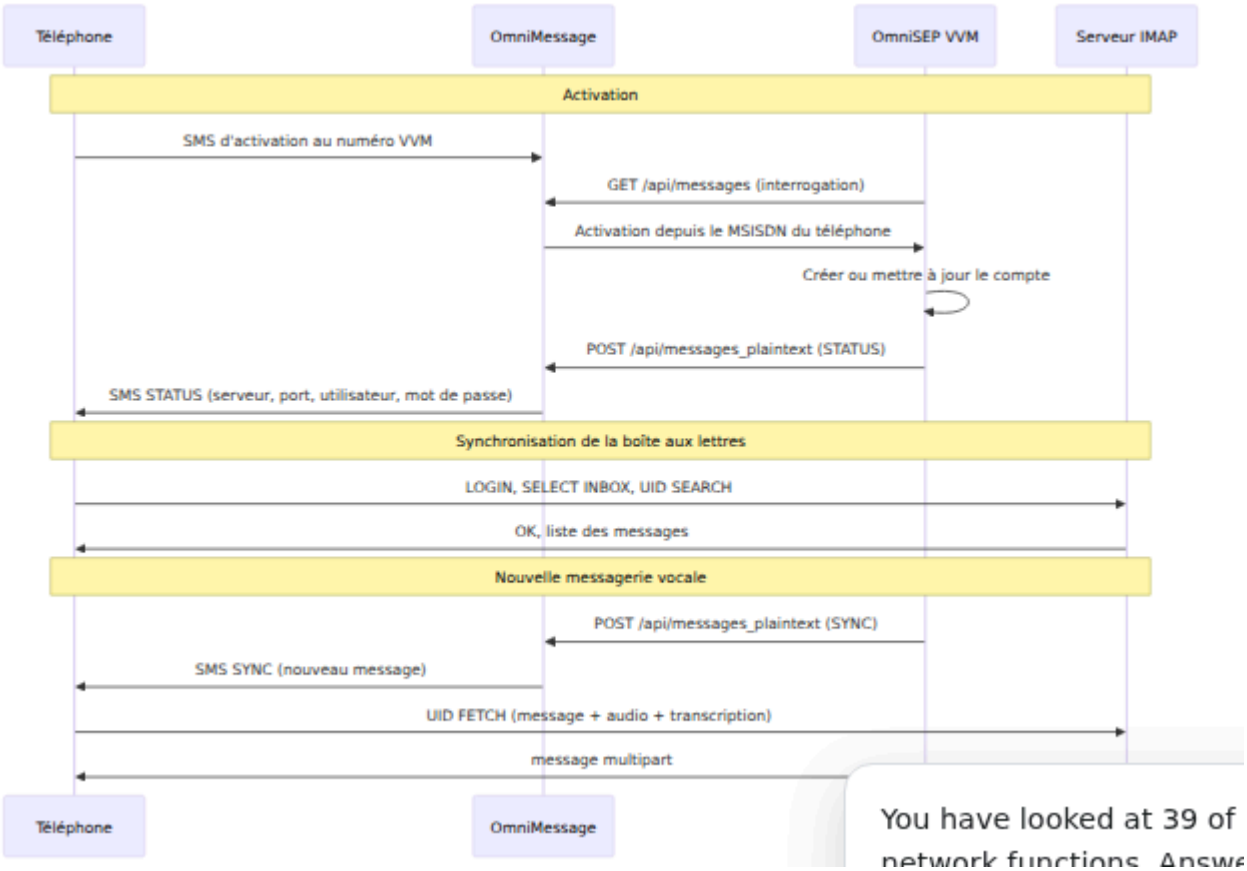
Le téléphone envoie un SMS `Activate` au numéro VVM. OmniSEP lit ce SMS depuis OmniMessage, crée le compte et envoie un SMS `STATUS` avec les identifiants IMAP. Le téléphone se connecte ensuite via IMAP.



États de Provisionnement

Le service suit un état de provisionnement pour chaque abonné. L'état suit la spécification OMTP.

État	Code	Description
Inconnu	U	État initial. Aucun provisionnement tenté.
Nouveau	N	Compte créé. Le service attend la première connexion du client.
Prêt	R	Entièrement provisionné et opérationnel.
Provisionné	P	Identifiants envoyés. Le service attend la vérification du client.
Bloqué	B	Service désactivé ou suspendu.



Intégration OmniMessage

OmniSEP utilise l'API HTTP OmniMessage pour tous les SMS VVM. Voir l'API OmniMessage pour le schéma complet.

SMS entrants (interrogation)

OmniSEP interroge `GET /api/messages` à intervalles fixes. Il sélectionne les messages dont le `destination_msisdn` est le numéro VVM configuré. Il traite les messages dont le texte commence par `Activate:`, `Deactivate:`, ou `//VVM`. Il enregistre chaque ID de message traité, afin de ne pas traiter un message deux fois. Si un message échoue à être traité, OmniSEP le réessaie lors de la prochaine interrogation.

Un message `Activate` entrant du téléphone ressemble à ceci :

```
Activate:pv=11;ct=samsung.SM-A536E.13
```

SMS sortants (envoi)

OmniSEP envoie des SMS `STATUS` et `SYNC` avec `POST /api/messages_plaintext`. Le corps de la requête contient le numéro source (le numéro VVM), le numéro de destination (le MSISDN du téléphone), et le texte du message.

```
{
  "source_msisdn": "123",
  "destination_msisdn": "15551234212",
  "message":
"//VVM:STATUS:st=R;rc=0;srv=10.179.4.165;ipt=9143;..."
}
```

Protocole SMS

Message STATUS (serveur vers téléphone)

OmniSEP envoie un message `STATUS` après activation. Le message contient les identifiants IMAP.

```
//VVM:STATUS:st=R;rc=0;srv=10.179.4.165;ipt=9143;spt=8025;u=155512342
15;pm=N;gm=N;vtc=A
```

Champ	Description
`st`	État de provisionnement. R=Prêt, B=Bloqué, N=Nouveau, P=Provisionné, U=Inconnu.
`rc`	Code de retour. 0 est un succès.
`srv`	Adresse du serveur IMAP. Le téléphone se connecte à cette adresse.
`ipt`	Port IMAP.
`spt`	Port SMTP.
`u`	Nom d'utilisateur IMAP.
`pw`	Mot de passe IMAP.
`tui`	Numéro d'interface utilisateur téléphonique.
`dn`	Numéro de destination pour les réponses SMS du client.
`lang`	Code de langue.
`g_len`	Durée maximale de salutation en secondes.
`vs_len`	Durée maximale de signature vocale en secondes.
`pw_len`	Plage de longueur du PIN.
`pm`	PIN requis. Y ou N.
`gm`	Mode de réinitialisation de la salutation. G=salutation, V=signature vocale, B=les deux, N=aucun.
`vtc`	Capacité de transcription. A=automatique, D=à la demande, B=les deux, N=aucun.

Message SYNC (serveur vers téléphone)

OmniSEP envoie un message `SYNC` lorsque le contenu de la boîte aux lettres change.

```
//VVM:SYNC:ev=NM;id=1;c=1;t=v;s=15551234567;dt=19/08/2026 01:39
+0000;l=8
```

Champ	Description
`ev`	Type d'événement. NM=nouveau message, MBU=mise à jour de la boîte aux lettres, GU=mise à jour de la salutation.
`id`	ID du message.
`c`	Nombre de messages non lus.
`t`	Type de message. v=voix, o=vidéo, f=fax, i=infotainment, e=ECC.
`s`	Numéro de l'expéditeur.
`dt`	Horodatage de dépôt.
`l`	Durée du message en secondes.

Message Activate (téléphone vers serveur)

Le téléphone envoie un message `Activate` pour activer VVM.

```
Activate:pv=11;ct=samsung.SM-A536E.13
```

Champ	Description
`pv`	Version du protocole.
`ct`	Type de client. Le format est fournisseur.modèle.version_os.

Message Deactivate (téléphone vers serveur)

Le téléphone envoie un message `Deactivate` pour désactiver VVM.

```
Deactivate:pv=11
```

Serveur IMAP

Le serveur IMAP implémente un sous-ensemble d'IMAP4rev1 (RFC 3501) pour la messagerie vocale. Il accepte IMAP simple ou IMAPS.

Capacités

```
IMAP4rev1 AUTH=PLAIN AUTH=LOGIN UIDPLUS MOVE QUOTA
```

Commandes Supportées

Commande	Description
CAPABILITY	Lister les capacités du serveur.
LOGIN	Authentifier avec nom d'utilisateur et mot de passe.
LOGOUT	Terminer la session.
SELECT	Ouvrir une boîte aux lettres.
EXAMINE	Ouvrir une boîte aux lettres en lecture seule.
LIST	Lister les boîtes aux lettres disponibles.
STATUS	Obtenir l'état de la boîte aux lettres.
FETCH	Récupérer le contenu du message.
UID FETCH	Récupérer par UID.
STORE	Mettre à jour les indicateurs de message.
UID STORE	Mettre à jour les indicateurs par UID.
SEARCH	Rechercher des messages.
UID SEARCH	Rechercher par UID.
COPY	Copier des messages entre boîtes aux lettres.
EXPUNGE	Supprimer les messages marqués.
CLOSE	Fermer la boîte aux lettres et expurger.
GETQUOTAROOT	Obtenir le quota de stockage.

Commande	Description
NOOP	Garder la connexion active.

Format de Message

OmniSEP présente chaque message vocal comme un message MIME `multipart/mixed`. La partie 1 est l'audio. La partie 2 est la transcription. Le téléphone lit l'en-tête `Content-Type` de niveau supérieur pour confirmer que le message est multipart. Le téléphone extrait ensuite la partie `audio/*`.

```
Content-Type: multipart/mixed; boundary="----=_Part_0"

------=_Part_0
Content-Type: audio/amr
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="voicemail.amr"

[base64 audio]
------=_Part_0
Content-Type: text/plain; charset="UTF-8"

[texte de transcription]
------=_Part_0--
```

Récupération de la Messagerie Vocale

Le téléphone récupère une messagerie vocale en plusieurs étapes. Les commandes exactes dépendent du client. Le client OMTP sur Android utilise cette séquence :

1. `UID SEARCH UID <id>` pour confirmer que le message existe.
2. `UID FETCH <id> (UID BODY.PEEK[])` pour lire le message complet.
3. `UID FETCH <id> (... BODY.PEEK[HEADER.FIELDS (...)] BODYSTRUCTURE)` pour lire les en-têtes et la structure.
4. `UID FETCH <id> (UID BODY.PEEK[<n>])` pour lire une partie, par exemple la transcription.

Le client nécessite que l'en-tête `Content-Type` commence par `multipart/`. Si l'en-tête est absent, le client consigne "Message non multipart ignoré" et abandonne la messagerie vocale. OmniSEP renvoie donc le message multipart complet pour la récupération des en-têtes, afin que le client voie le bon `Content-Type`.

Configuration

Exemple de Configuration

```
config :omni_sep, :vvm,
  # Interrupteur principal
  enabled: true,

  # Serveur IMAP
  imap_port: 9143,
  imap_ssl: false,
  imap_server: "10.179.4.165",
  imap_cert: "priv/cert/server.crt",
  imap_key: "priv/cert/server.key",

  # SMTP (dépôt de messagerie vocale, utilisation future)
  smtp_port: 8025,
  smtp_server: nil,

  # Interface utilisateur téléphonique
  tui_number: "*86",

  # SMS via OmniMessage
  sms_source_number: "123",
  vvm_number: "123",
  omnimessage_url: "https://10.179.3.219:8443",
  sms_gateway: "https://10.179.3.219:8443/api/messages_plaintext",
  poll_interval_ms: 5000,

  # PIN
  min_pin_length: 4,
  max_pin_length: 15,

  # Limites des abonnés
  default_max_messages: 100,
  default_storage_limit_kb: 50_000,
  default_max_greeting_seconds: 60
```

Paramètres de Configuration

Paramètre	Type	Requis	Par défaut
`enabled`	Boolean	Non	false
`imap_port`	Integer	Non	993
`imap_ssl`	Boolean	Non	true
`imap_server`	String	Oui	-
`imap_cert`	String	Non	priv/cert/server.crt
`imap_key`	String	Non	priv/cert/server.key
`smtp_port`	Integer	Non	587
`smtp_server`	String	Non	nil
`tui_number`	String	Non	*86
`sms_source_number`	String	Oui	-

Paramètre	Type	Requis	Par défaut
`vvm_number`	String	Non	123
`omnimessage_url`	String	Oui	nil
`sms_gateway`	String	Oui	nil
`poll_interval_ms`	Integer	Non	5000
`min_pin_length`	Integer	Non	4
`max_pin_length`	Integer	Non	15
`default_max_messages`	Integer	Non	100
`default_storage_limit_kb`	Integer	Non	50000
`default_max_greeting_seconds`	Integer	Non	60

Accessibilité

Le téléphone se connecte au serveur IMAP via le support de données mobiles. Définissez `imap_server` sur une adresse que le réseau de données UE peut atteindre. Dans le laboratoire, l'hôte OmniSEP sur le P-CSCF est accessible depuis les pools UE.

Activation du Téléphone

Le téléphone active VVM à partir de sa configuration de l'opérateur. Définissez les clés OMTP dans CarrierConfig. Le téléphone envoie ensuite le SMS `Activate` au numéro de destination.

Clé CarrierConfig	Valeur	Description
`vvm_type_string`	`vvm_type_omtp`	Sélectionnez le protocole OMTP.
`vvm_destination_number_string`	`123`	Le numéro court VVM. Faites correspondre cette valeur à `vvm_number`.
`vvm_ssl_enabled_bool`	`false`	Utilisez IMAP simple. Faites correspondre cette valeur à `imap_ssl`.

Lorsque la configuration de l'opérateur change, le téléphone commence l'activation de VVM. Il envoie le SMS `Activate` au numéro de destination. OmniSEP lit le SMS depuis OmniMessage, provisionne le compte et renvoie le SMS `STATUS`.

Expérience du Téléphone

Après activation, le téléphone reçoit le SMS `SYNC` pour chaque nouvelle messagerie vocale. Le client de messagerie vocale natif se synchronise via IMAP, télécharge l'audio et affiche la messagerie vocale dans l'application Téléphone. Les captures d'écran suivantes montrent un téléphone Samsung qui exécute le client OMTP natif contre OmniSEP.

La boîte de réception de la messagerie vocale liste chaque message avec le numéro de l'appelant et l'heure de dépôt.

La vue détaillée de la messagerie vocale lit l'audio téléchargé. Le téléphone diffuse la partie audio que OmniSEP sert via IMAP.

Les numéros d'appelants dans ces captures d'écran utilisent la plage fictive nord-américaine (555-0100 à 555-0199).

Métriques

Métriques de Session IMAP

Métrique: `vvm_imap_sessions_total` **Type**: Compteur **Description**: Nombre total de sessions IMAP VVM. **Étiquettes**:

- `result` - Résultat de la session : `success`, `auth_failed`, `timeout`.

Métrique: `vvm_imap_active_sessions` **Type**: Jauge **Description**: Nombre de sessions IMAP actives.

Métrique: `vvm_imap_commands_total` **Type**: Compteur **Description**: Total des commandes IMAP traitées. **Étiquettes**:

- `command` - Commande IMAP, par exemple `LOGIN`, `SELECT`, `FETCH`.

- `result` - Résultat de la commande : `ok`, `no`, `bad`.

Métriques de Message

Métrique: `vvm_messages_total` **Type**: Compteur **Description**: Total des opérations de message VVM. **Étiquettes**:

- `operation` - Type d'opération : `deposit`, `read`, `delete`, `move`.

Métrique: `vvm_messages_stored` **Type**: Jauge **Description**: Nombre de messages vocaux dans le stockage.

Métrique: `vvm_message_duration_seconds` **Type**: Histogramme **Description**: Durée des messages vocaux en secondes. **Seaux**: 5, 10, 15, 30, 60, 120, 180, 300.

Métriques SMS

Métrique: `vvm_sms_total` **Type**: Compteur **Description**: Total des messages SMS VVM. **Étiquettes**:

- `type` - Type de SMS : `status`, `sync`, `activate`, `deactivate`.
- `result` - Résultat de la livraison : `success`, `failed`, `no_gateway`.

Exemples de Requêtes Prometheus

```
# Taux de session IMAP
rate(vvm_imap_sessions_total[5m])

# Taux d'échec d'authentification
sum(rate(vvm_imap_sessions_total{result="auth_failed"}[5m]))
  / sum(rate(vvm_imap_sessions_total[5m]))

# Taux de succès de livraison des SMS
sum(rate(vvm_sms_total{result="success"}[5m]))
  / sum(rate(vvm_sms_total[5m]))
```

Dépannage

Le Téléphone Ne Peut Pas Activer VVM

Symptômes: Le téléphone affiche "Messagerie vocale visuelle indisponible", ou l'activation ne se termine pas.

Causes possibles:

- Le service VVM est désactivé.
- `omnimessage_url` est incorrect ou l'API est inaccessible.
- Le téléphone n'envoie pas le SMS `Activate`.

Résolution:

1. Confirmer `enabled: true` dans la configuration VVM.
2. Confirmer que l'API OmniMessage répond à `GET /api/messages`.
3. Confirmer que les clés CarrierConfig sont définies sur le téléphone. Voir Activation du Téléphone.
4. Vérifier OmniMessage pour un message `Activate` entrant au numéro VVM.

SMS STATUS Non Livré

Symptômes: Le téléphone envoie `Activate`, mais le téléphone ne reçoit pas le SMS `STATUS`.

Causes possibles:

- `sms_gateway` est incorrect ou l'API est inaccessible.
- Le téléphone n'est pas enregistré pour SMS sur IMS.

Résolution:

1. Confirmer que `sms_gateway` pointe vers `<omnimessage_url>/api/messages_plaintext`.
2. Vérifier OmniMessage pour un message sortant du numéro VVM vers le téléphone.

3. Confirmer que le téléphone est enregistré pour la livraison des SMS.

Échec d'Authentification IMAP

Symptômes: Le téléphone reçoit le SMS `STATUS`, mais la connexion IMAP échoue.

Causes possibles:

- Le mot de passe dans le `STATUS` mis en cache diffère du mot de passe du compte.
- Le compte n'existe plus, par exemple après un redémarrage d'OmniSEP.
- Un pare-feu bloque le port IMAP.

Résolution:

1. Re-provisionner le téléphone afin qu'il reçoive un nouveau `STATUS` avec le mot de passe actuel.
2. Confirmer que le compte existe dans le stockage.
3. Confirmer que le pare-feu autorise le port IMAP depuis le réseau de données UE.

Le Téléphone Ignore la Messagerie Vocale

Symptômes: Le téléphone se synchronise, mais la messagerie vocale n'apparaît pas, ou l'audio ne se lit pas.

Causes possibles:

- Le `Content-Type` du message n'est pas `multipart/`.
- La partie audio est absente ou a le mauvais `Content-Type`.

Résolution:

1. Confirmer que le message est `multipart/mixed` avec une partie `audio/amr`.
2. Confirmer que le téléphone peut atteindre le serveur IMAP sur le port configuré.

3. Confirmer que le SMS `SYNC` rapporte le bon ID de message et le bon nombre.

Références

- Spécification OMTP VVM v1.3 - Spécification de l'Interface de Messagerie Vocale Visuelle.
- GSMA TS.46 - Spécification de l'Interface de Messagerie Vocale Visuelle.
- RFC 3501 - Protocole IMAP4rev1.
- RFC 5322 - Format de Message Internet.

Services Supplémentaires XCAP (Simservs)

OmniSEP implémente ETSI TS 183 023 XCAP (XML Configuration Access Protocol) pour gérer les services supplémentaires IMS, y compris le renvoi d'appels, le barrissement d'appels et les paramètres d'identification de l'appelant.

Interface du Panneau de Contrôle

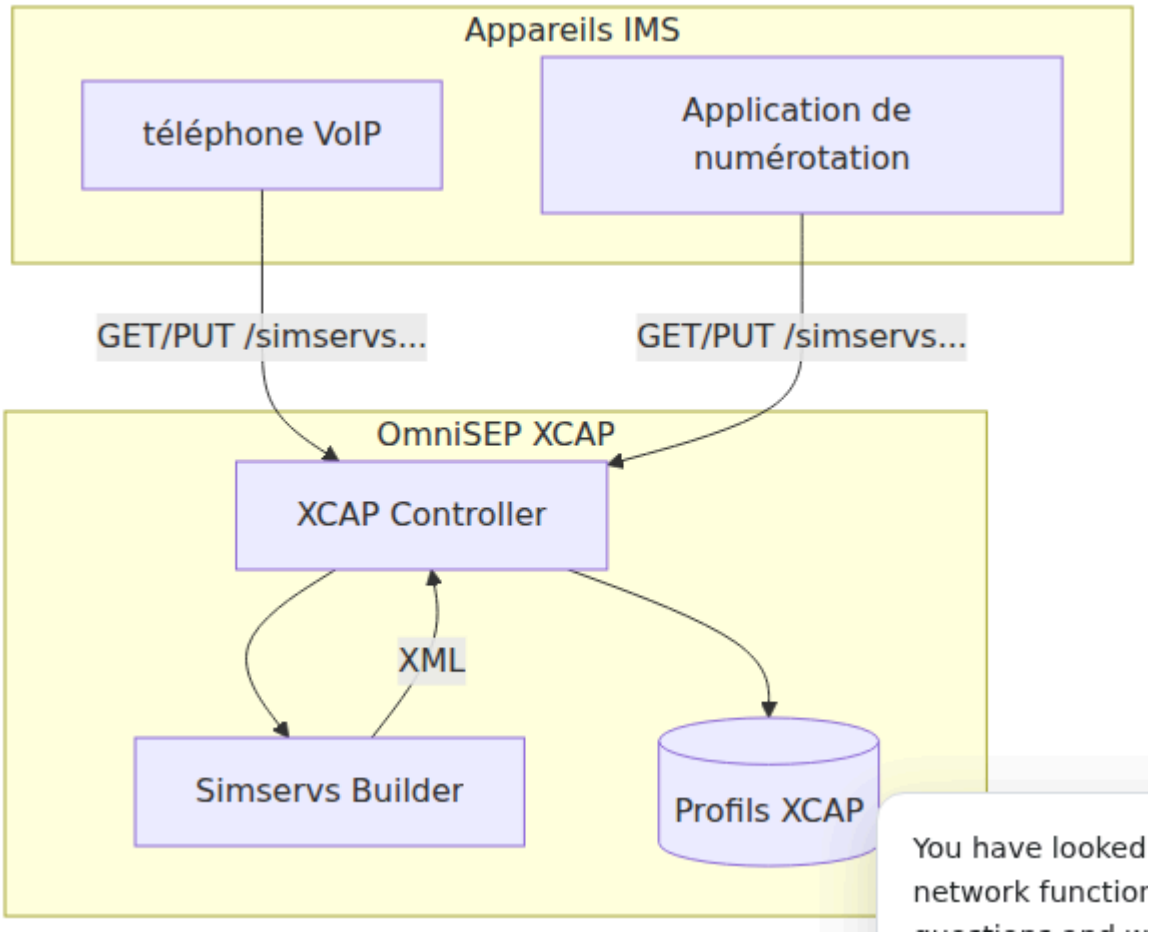
La page des Profils Simservs XCAP fournit une interface web pour visualiser et gérer les profils des abonnés :

Fonctionnalités :

- Rechercher et filtrer les profils locaux par MSISDN
- Récupérer les profils depuis HSS en utilisant l'interface Diameter Sh
- Voir les détails du profil dans une mise en page à 2 colonnes :

    - **Colonne de gauche** : Services d'identité (OIP/OIR), Autres services (Appel en attente, Mise en attente d'appel), règles de renvoi d'appels
    - **Colonne de droite** : Règles de barrissement d'appels entrants et sortants avec conditions
- Synchronisation Push/Pull avec HSS
- Mode édition pour modifier les paramètres du profil

Aperçu



Structure du Document Simservs

Le document simservs suit la structure ETSI TS 183 023 :



Interface HTTP

Format d'URL XCAP

```
/simservs.ngn.etsi.org/users/{sip_uri}/simservs.xml[/~~/{xpath}]
```

Composant	Description	Exemple
`{sip_uri}`	URI SIP avec MSISDN	`sip:+15551234567@ims.example.com`
`{xpath}`	Sélecteur XPath (optionnel)	`simservs/communication-diversion`

Opérations

Méthode	Chemin
GET	`/simservs.ngn.etsi.org/users/{sip}/simservs.xml`
PUT	`/simservs.ngn.etsi.org/users/{sip}/simservs.xml`
GET	`/simservs.ngn.etsi.org/users/{sip}/simservs.xml/~~/simser`
PUT	`/simservs.ngn.etsi.org/users/{sip}/simservs.xml/~~/simser`
DELETE	`/simservs.ngn.etsi.org/users/{sip}/simservs.xml/~~/simser`

Types de Contenu

Content-Type	Utilisation
`application/xcap-el+xml`	Opérations sur les éléments XCAP
`application/xml`	XML standard

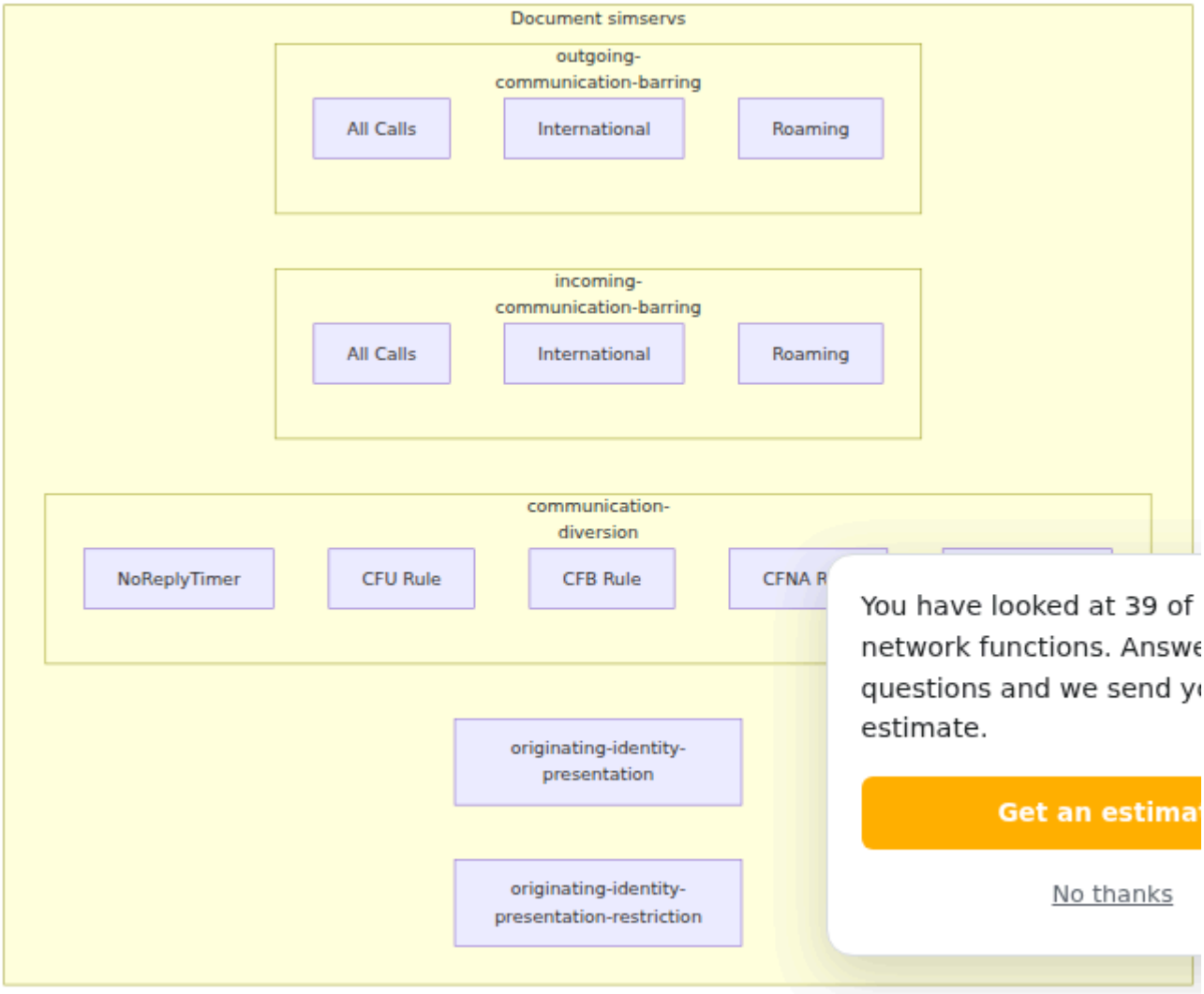
Support ETag

OmniSEP implémente le contrôle de concurrence basé sur ETag selon RFC 4825 :

En-tête	Utilisation
`ETag`	En-tête de réponse avec la version du document
`If-Match`	Mise à jour conditionnelle (PUT/DELETE)
`If-None-Match`	GET conditionnel (304 Non Modifié)

Architecture de Mise en Cache

OmniSEP utilise une stratégie de mise en cache locale avec un stockage basé sur ETS et une synchronisation asynchrone avec HSS.



Tables de Stockage

Table	Clé	Valeur	But
`xcap_profiles`	IMSI	`{profile_map, etag}`	Stockage principal des profils
`xcap_by_msisdn`	MSISDN	IMSI	Index de recherche pour les demandes XCAP

Stratégie de Mise en Cache

Opérations de Lecture (GET)

1. Interroger d'abord le cache local ETS
2. En cas de cache manquant, récupérer depuis HSS via Diameter Sh
3. Initialiser le cache local avec la réponse de HSS
4. Retourner le profil par défaut si HSS indisponible ou aucun profil n'existe

Opérations d'Écriture (PUT)

1. Valider la condition ETag par rapport à la valeur mise en cache
2. Mettre à jour le cache local immédiatement
3. Retourner une réponse au client avec un nouvel ETag
4. Pousser les modifications vers HSS de manière asynchrone (non-bloquant)

Génération d'ETag

Les ETags sont calculés comme des hachages MD5 des données du profil :

```
ETag = MD5(erlang:term_to_binary(profile))[0:16]
```

Exemple : `"a1b2c3d4e5f6g7h8"`

La chaîne hexadécimale de 16 caractères change chaque fois qu'un champ de profil est modifié, permettant une invalidation précise du cache.

Contrôle de Concurrence

Mécanisme	But
Concurrence de lecture ETS	Lectures parallèles rapides sans verrouillage
Écritures GenServer	Opérations d'écriture atomiques
Validation d'ETag	Empêche les mises à jour perdues de clients concurrents

Profil Par Défaut

Les abonnés inconnus reçoivent automatiquement un profil par défaut selon 3GPP TS 24.623 :

- Tous les services supplémentaires actifs
- OIR par défaut : `presentation-not-restricted`
- NoReplyTimer : 20 secondes
- Règles de renvoi/barrissement d'appels vides

Cela garantit que les appareils reçoivent toujours une réponse valide sans nécessiter de pré-provisionnement.

Intégration HSS

Opération	Commande Diameter	Timing
Récupérer le profil	Sh UDR (User-Data-Request)	Synchronous on cache miss
Pousser les changements	Sh PUR (Profile-Update-Request)	Asynchronous after PUT

La poussée asynchrone signifie que les mises à jour HSS ne bloquent pas les réponses des clients, améliorant la latence pour les demandes des appareils.

Document XML Simservs

Exemple de Document Complet

```xml
<?xml version="1.0" encoding="UTF-8"?>
<simservs xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
          xmlns:cp="urn:ietf:params:xml:ns:common-policy">

  <originating-identity-presentation active="true"/>

  <originating-identity-presentation-restriction active="true">
    <default-behaviour>presentation-not-restricted</default-
behaviour>
  </originating-identity-presentation-restriction>

  <communication-diversion active="true">
    <NoReplyTimer>20</NoReplyTimer>
    <cp:ruleset>
      <cp:rule id="cfb">
        <cp:conditions>
          <busy/>
        </cp:conditions>
        <cp:actions>
          <forward-to>
            <target>tel:+15557654321</target>
            <notify-caller>false</notify-caller>
          </forward-to>
        </cp:actions>
      </cp:rule>
    </cp:ruleset>
  </communication-diversion>

  <incoming-communication-barring active="false">
    <cp:ruleset/>
  </incoming-communication-barring>

  <outgoing-communication-barring active="false">
    <cp:ruleset/>
  </outgoing-communication-barring>

</simservs>
```

Espaces de Noms

Préfixe	Espace de Nom	Descript
(par défaut)	`http://uri.etsi.org/ngn/params/xml/simservs/xcap`	ETSI Simservs
cp	`urn:ietf:params:xml:ns:common-policy`	Politique Commun RFC 4745

Services

Présentation de l'Identité d'Origine (OIP)

Contrôle si l'identification de l'appelant est affichée à la partie appelée.

```
<originating-identity-presentation active="true"/>
```

Attribut	Type	Description
`active`	Booléen	Service activé/désactivé

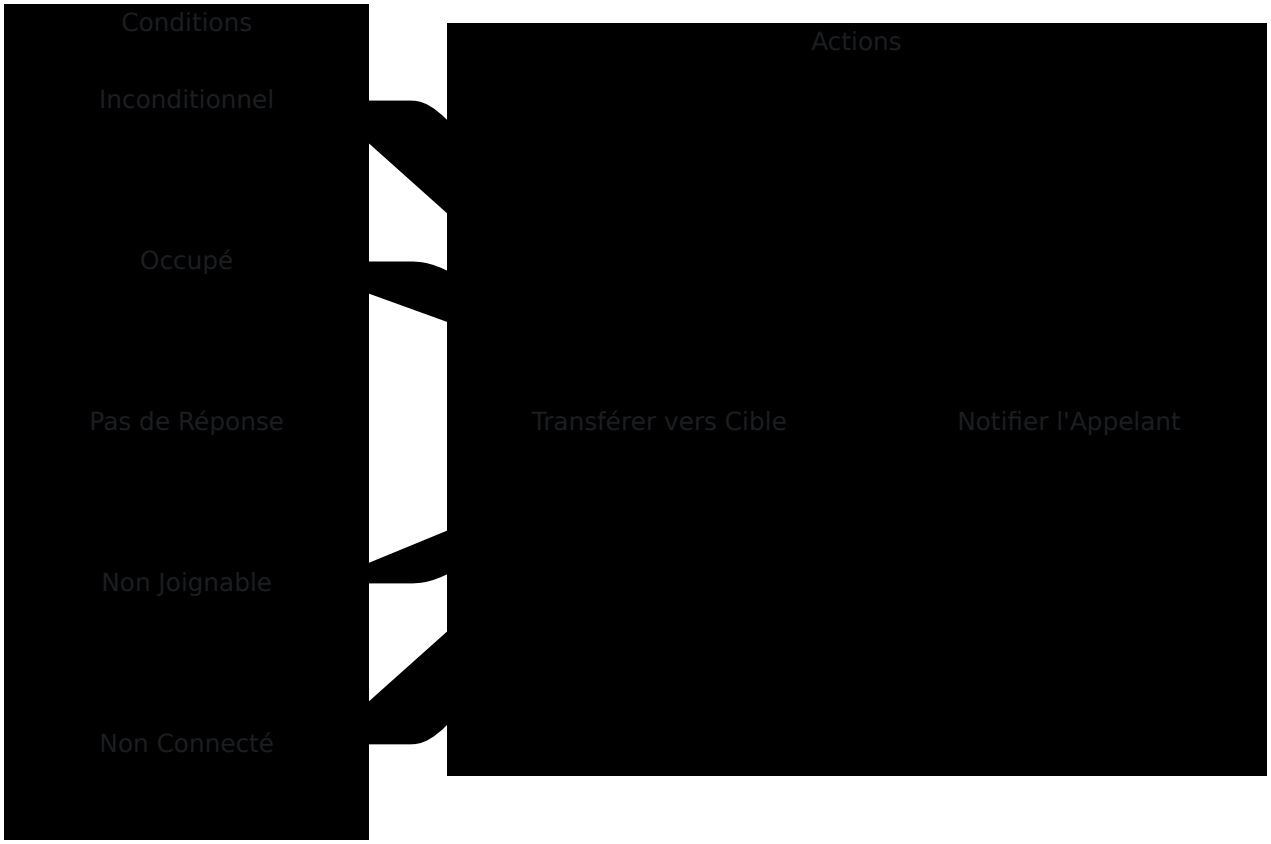
Restriction de la Présentation de l'Identité d'Origine (OIR)

Contrôle le masquage de l'identification de l'appelant.

```
<originating-identity-presentation-restriction active="true">
  <default-behaviour>presentation-not-restricted</default-
behaviour>
</originating-identity-presentation-restriction>
```

Élément	Valeurs	Description
`default-behaviour`	`presentation-restricted`, `presentation-not-restricted`	Comportement par défaut de l'identification de l'appelant

Diversion de Communication (Renvoi d'Appels)



Types de Règles

ID de Règle	Condition	Description
`cfu`	(aucune)	Renvoi d'Appels Inconditionnel - transfère tous les appels immédiatement
`cfb`	`occupé`	Renvoi d'Appels en cas d'Occupation
`cfna`	`pas-de-réponse`	Renvoi d'Appels en cas de Pas de Réponse (utilise NoReplyTimer)
`cfnrc`	`non-joignable`	Renvoi d'Appels en cas de Non Joignable
`cfnl`	`non-connecté`	Renvoi d'Appels en cas de Non Connecté

Structure de la Règle de Renvoi d'Appels

```
<communication-diversion active="true">
  <NoReplyTimer>20</NoReplyTimer>
  <cp:ruleset>
    <cp:rule id="cfna">
      <cp:conditions>
        <no-answer/>
      </cp:conditions>
      <cp:actions>
        <forward-to>
          <target>tel:+15557654321</target>
          <notify-caller>false</notify-caller>
        </forward-to>
      </cp:actions>
    </cp:rule>
  </cp:ruleset>
</communication-diversion>
```

Élément	Type	Description
`NoReplyTimer`	Entier	Secondes à attendre avant CFNA (1-300)
`cp:rule/@id`	Chaîne	Identifiant de la règle (cfu, cfb, cfna, cfnrc, cfnl)
`target`	URI tel:	Numéro de destination pour le transfert
`notify-caller`	Booléen	Jouer une annonce à l'appelant

Format de l'URI de Cible

Les cibles de transfert utilisent le format URI tel: selon RFC 3966 :

```
tel:+15557654321;phone-context=ims.mnc001.mcc310.3gppnetwork.org
```

Composant	Description
`tel:`	Schéma URI
`+15557654321`	Numéro E.164 avec code pays
`phone-context`	Domaine IMS (optionnel)

Barrissement d'Appels

Barrissement de Communication Entrante

```
<incoming-communication-barring active="true">
  <cp:ruleset>
    <cp:rule id="international">
      <cp:conditions>
        <international/>
      </cp:conditions>
      <cp:actions>
        <allow>false</allow>
      </cp:actions>
    </cp:rule>
  </cp:ruleset>
</incoming-communication-barring>
```

Barrissement de Communication Sortante

```
<outgoing-communication-barring active="true">
  <cp:ruleset>
    <cp:rule id="international">
      <cp:conditions>
        <international/>
      </cp:conditions>
      <cp:actions>
        <allow>false</allow>
      </cp:actions>
    </cp:rule>
  </cp:ruleset>
</outgoing-communication-barring>
```

Types de Règles de Barrissement

ID de Règle	Condition	Description
`all`	(aucune)	Barrer tous les appels
`international`	`international`	Barrer les appels internationaux
`international-exHC`	`international-exHC`	Barrer les appels internationaux sauf le pays d'origine
`roaming`	`roaming`	Barrer les appels pendant le roaming

Exemples d'API

Obtenir le Document Complet Simservs

```
GET
/simservs.ngn.etsi.org/users/sip:+15551234567@ims.example.com/simserv
Accept: application/xcap-el+xml
```

Réponse :

```
HTTP/1.1 200 OK
Content-Type: application/xcap-el+xml
ETag: "a1b2c3d4e5f6g7h8"

<?xml version="1.0" encoding="UTF-8"?>
<simservs
xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap"...>
  ...
</simservs>
```

Obtenir les Paramètres de Renvoi d'Appels

```
GET
/simservs.ngn.etsi.org/users/sip:+15551234567@ims.example.com/simserv
diversion
```

Activer le Renvoi d'Appels en Cas d'Occupation

```
PUT
/simservs.ngn.etsi.org/users/sip:+15551234567@ims.example.com/simserv
diversion/cp:ruleset/cfb
Content-Type: application/xcap-el+xml
If-Match: "a1b2c3d4e5f6g7h8"

<cp:rule id="cfb">
  <cp:conditions>
    <busy/>
  </cp:conditions>
  <cp:actions>
    <forward-to>
      <target>tel:+15557654321</target>
      <notify-caller>false</notify-caller>
    </forward-to>
  </cp:actions>
</cp:rule>
```

Désactiver la Règle de Renvoi d'Appels

```
DELETE
/simservs.ngn.etsi.org/users/sip:+15551234567@ims.example.com/simserv
diversion/cp:ruleset/cfb
If-Match: "a1b2c3d4e5f6g7h8"
```

Mettre à Jour le NoReplyTimer

```
PUT
/simservs.ngn.etsi.org/users/sip:+15551234567@ims.example.com/simserv
diversion/NoReplyTimer
Content-Type: application/xcap-el+xml

25
```

API de Gestion

Pour un accès administratif, utilisez l'API de gestion JSON :

Obtenir le Profil

```
GET /api/xcap/15551234567
```

Réponse :

```
{
  "oip": { "active": true },
  "oir": {
    "active": true,
    "default_behaviour": "presentation-not-restricted"
  },
  "no_reply_timer": 20,
  "call_forwarding": {
    "cfb": {
      "enabled": true,
      "target": "tel:+15557654321",
      "condition": "busy"
    }
  },
  "call_barring_incoming": {},
  "call_barring_outgoing": {}
}
```

Définir le Profil

```
POST /api/xcap/15551234567
Content-Type: application/json

{
  "no_reply_timer": 25,
  "call_forwarding": {
    "cfna": {
      "enabled": true,
      "target": "tel:+15559876543",
      "condition": "no-answer"
    }
  }
}
```

Profil Par Défaut

Les nouveaux abonnés reçoivent ce profil par défaut :

Paramètre	Par Défaut
OIP	Actif
OIR	Actif, presentation-not-restricted
NoReplyTimer	20 secondes
Renvoi d'Appels	Toutes les règles désactivées
Barrissement d'Appels (Entrants)	Tous les appels autorisés
Barrissement d'Appels (Sortants)	Tous les appels autorisés

Réponses d'Erreur

Statut HTTP	Description
200	Succès
304	Non Modifié (If-None-Match correspondant)
400	Mauvaise Demande - XML ou chemin invalide
404	Non Trouvé - Document ou élément non trouvé
405	Méthode Non Autorisée
409	Conflit - Violation de contrainte
412	Échec de la Précondition - Mismatch d'ETag

Format de Réponse d'Erreur

```
<?xml version="1.0" encoding="UTF-8"?>
<xcap-error xmlns="urn:ietf:params:xml:ns:xcap-error">
  <error-element>Élément non trouvé : simservs/unknown</error-
element>
</xcap-error>
```

Spécifications de Référence

Spécification	Description
ETSI TS 183 023	Cadre XCAP pour les Simservs NGN
ETSI TS 183 004	Diversion de Communication (CDIV)
RFC 4825	Protocole XCAP
RFC 4745	Politique Commune
RFC 3966	URI tel:
3GPP TS 24.623	XCAP sur l'interface Ut