

Référence de Configuration OmniSEP

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

Table des Matières

- Configuration du Serveur HTTP
- Configuration du Stockage
- Droits par Défaut
- Configuration du Jeton
- 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",
  entitlement_version: "2.0"

```

Paramètres

Paramètre	Type	Requis	Par Défaut	Description
<code>http_port</code>	Entier	Non	9014	Port TCP pour les connexions à un terminator TLS en
<code>http_ip</code>	Tuple	Non	<code>{0, 0, 0, 0}</code>	Adresse IP à lier. Utilisez une IP spécifique hébergés.
<code>server_fqdn</code>	Chaîne	Oui	-	Nom de domaine entier Format : <code>aes.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org</code> selon GSMA TS.43 Sec
<code>entitlement_version</code>	Chaîne	Non	"2.0"	Version du protocole T défaut à "2.0".

Format FQDN

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

```

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

```

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

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

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

Configuration du Stockage

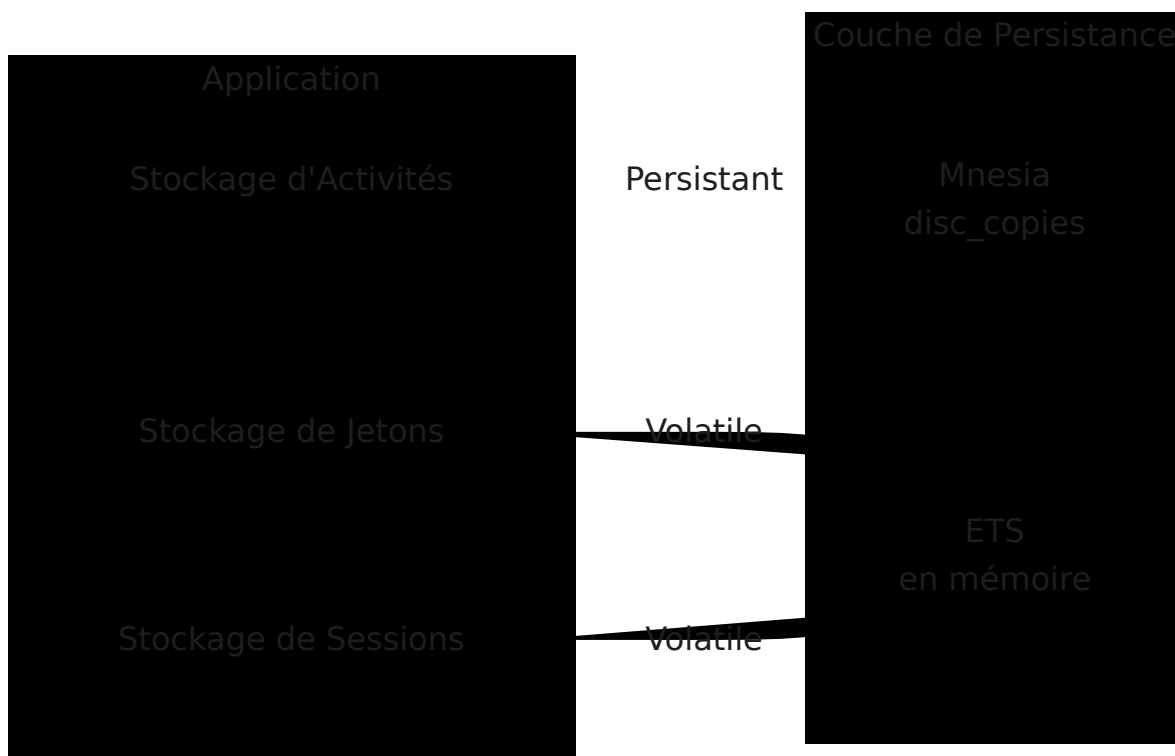
Contrôle le stockage de données persistantes en utilisant Mnesia pour une journalisation des activités conforme aux audits.

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

Paramètres

Paramètre	Type	Requis	Par Défaut	Description
<code>data_dir</code>	Chaîne	Non	"priv/data"	Répertoire pour les fichiers de base de données Mnesia. Les journaux d'activités sont conservés 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	Objectif	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 & Roaming
        entitlement_status: 1      # ACTIVÉ
      },
      %{
        access_type: 2,            # 5G/NR
        home_roaming_nw_type: 1,   # Domicile & Roaming
        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
<code>entitlement_status</code>	Entier	0=Désactivé, 1=Activé, 2=Incompatible, 3=Provisionnement	État de disponi service
<code>addr_status</code>	Entier	0=Non Disponible, 1=Disponible, 2=Non Requis, 3=En Cours	État de vérifica d'adresse
<code>tc_status</code>	Entier	0=Non Disponible, 1=Disponible, 2=Non Requis, 3=En Cours	État d'acceptat Termes & Conc
<code>prov_status</code>	Entier	0=Non Provisionné, 1=Provisionné, 2=Non Requis, 3=En Cours	État de provisionneme
<code>service_flow_url</code>	Chaîne	URL	URL pour le flu service (vérific d'adresse, T&C
<code>service_flow_user_data</code>	Chaîne	-	Données utilis transmises au service
<code>message_for_incompatible</code>	Chaîne	-	Message affich lorsque <code>entitlement_s</code>

Paramètres VoLTE (ap2003)

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

Paramètre	Type	Valeurs	Description
<code>access_type</code>	Entier	1=4G/LTE, 2=5G/NR	Technologie d'accès radio
<code>home_roaming_nw_type</code>	Entier	1=Domicile & Roaming, 2=Domicile Seulement, 3=Roaming Seulement	Portée du réseau
<code>entitlement_status</code>	Entier	0=Désactivé, 1=Activé	Disponibilité du service
<code>network_voice_irat_capability</code>	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 du Jeton

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
<code>validity_seconds</code>	Entier	Non	86400	Durée de vie du jeton en secondes. Par défaut, 24 heures.
<code>signing_secret</code>	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

- Générer un `signing_secret` unique pour chaque déploiement
- Faire tourner les secrets périodiquement
- Utiliser 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

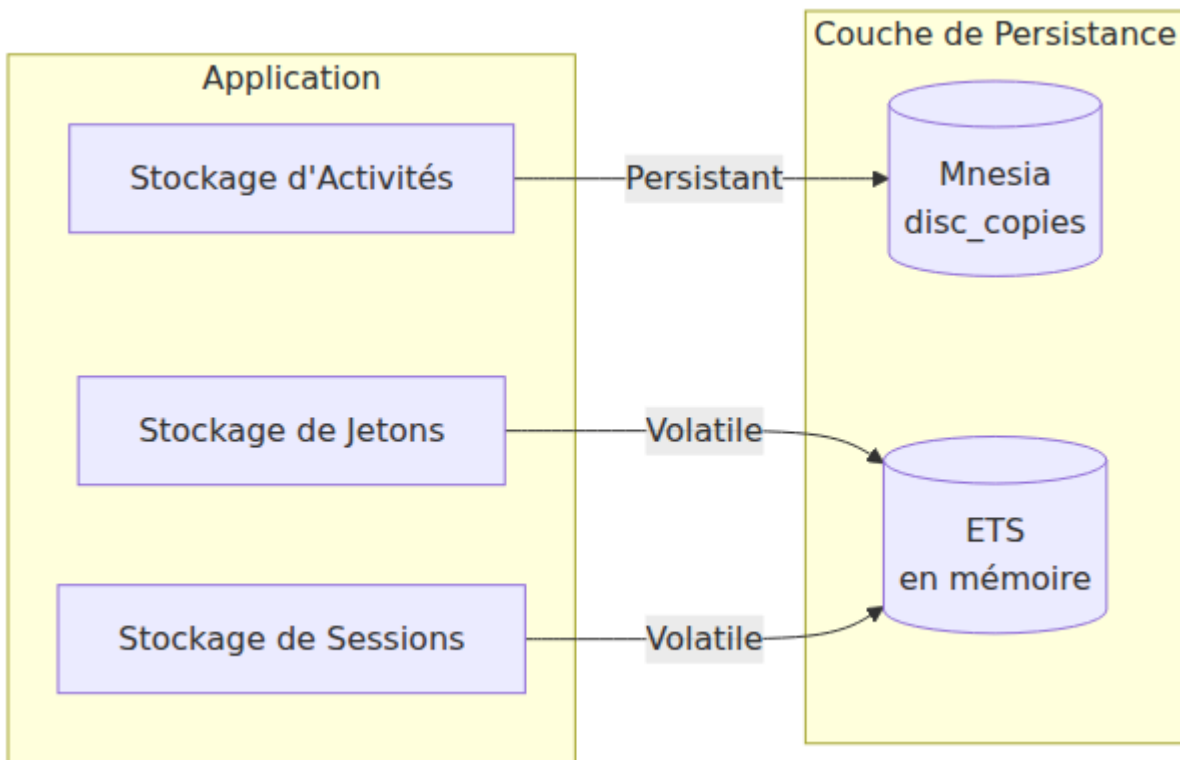
Contrôle le comportement d'authentification EAP-AKA pour l'authentification initiale des appareils.

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

Paramètres

Paramètre	Type	Requis	Par Défaut	Description
<code>enabled</code>	Booléen	Non	true	Activer l'authentification EAP-AKA. Lorsque faux, seule l'authentification par jeton est acceptée.
<code>session_timeout_ms</code>	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	Descriptif
<code>service_name</code>	Atome	Oui	-	Identifie le service interne
<code>host</code>	Chaîne	Oui	-	Diameter Host. Doit être un FQDN résolvable selon RFC 6733
<code>realm</code>	Chaîne	Oui	-	Diameter Realm. Utilisé pour le routage selon RFC 6733
<code>vendor_id</code>	Entier	Oui	10415	ID de fournisseur 3GPP selon TS 29.230
<code>auth_application_ids</code>	Liste	Oui	-	Liste des IDs d'applications d'authentification supportées. La valeur par défaut est 16777215
<code>request_timeout</code>	Entier	Non	5000	Délai d'attente de la requête en millisecondes
<code>peer_selection_algorithm</code>	Atome	Non	<code>:round_robin</code>	Sélection de l'algorithme de pair : <code>:round_robin</code> <code>:failover</code>

Paramètres Réseau

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

Paramètres de Pair

Chaque paire dans la liste `peers` :

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

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

Mode Mock

Si aucune paire Diameter n'est configurée, OmniSEP fonctionne en mode mock :

- Les défis EAP-AKA sont simulés
- L'IMSI est extrait de l'EAP_ID
- L'authentification réussit toujours
- Utile pour le développement et les tests

Journalisation des Activités

Contrôle la journalisation des activités des abonnés pour l'audit et le dépannage.

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

Paramètres

Paramètre	Type	Requis	Par Défaut	Description
<code>max_records_per_subscriber</code>	Entier	Non	1000	Nombre maximum d'enregistrements d'activités conservés par abonné. Les enregistrements les plus anciens sont supprimés lorsque la limite est dépassée.
<code>retention_seconds</code>	Entier	Non	2592000	Période de conservation des activités en secondes. Par défaut, 30 jours. Les enregistrements plus anciens que cela sont automatiquement 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, TOKEN)
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 # Mode mock - pas de pairs AAA

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	Diameter Origin-Host
DIAMETER_REALM	Diameter Origin-Realm
AAA_PEER_HOST	Nom d'hôte de la paire AAA
AAA_PEER_IP	Adresse IP de la paire AAA

Configuration du Logger

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

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

Guide de Dépannage OmniSEP

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

Table des Matières

- [Journal d'Activité](#)
- [Problèmes d'Entitlement TS.43](#)
- [Problèmes de Sirmservs 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'entitlement TS.43 et les opérations XCAP.

Fonctionnalités :

- Filtrer par type de demande (XCAP, Requête d'Entitlement, 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

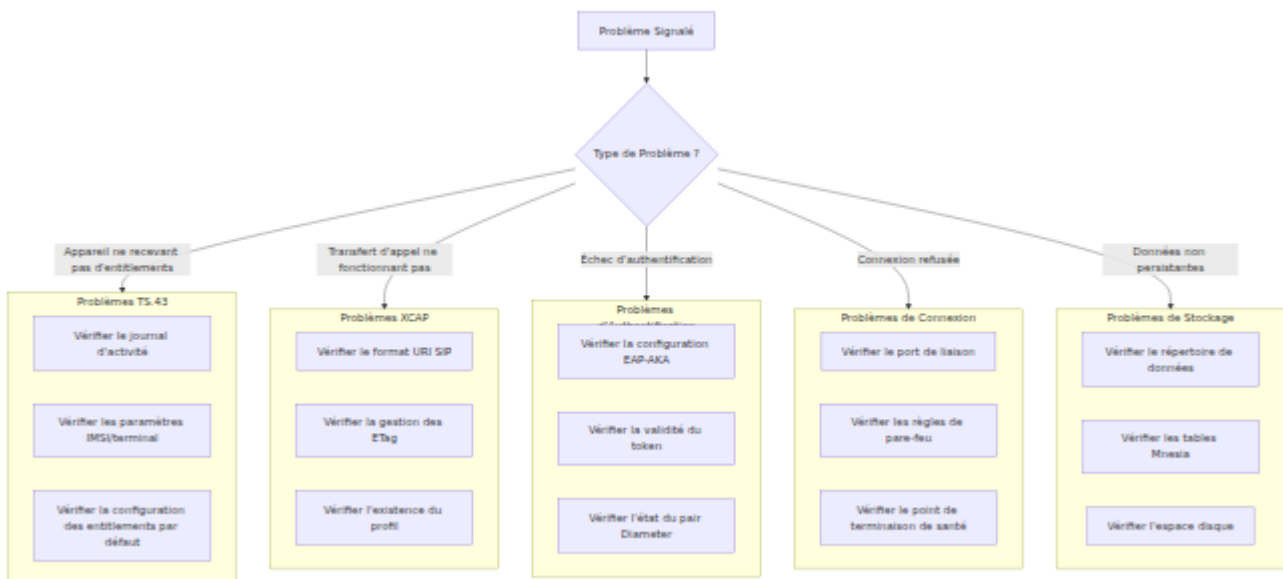
Sélectionner un enregistrement d'activité montre des détails complets de la demande/réponse :

Informations Capturées :

- **Horodatage et IP Client** : Quand et où la demande a été émise
- **Type de Demande et Méthode HTTP** : XCAP, requête d'entitlement, etc.
- **Informations sur l'Abonné** : IMSI, MSISDN (lorsqu'elles sont disponibles)
- **Informations sur le Terminal** : ID de l'appareil, Fabricant, Modèle (extrait de l'User-Agent)
- **Chemin de la Demande** : Chemin XCAP complet ou point de terminaison d'entitlement
- **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'Entitlementement TS.43

L'Appareil Signale "Service Non Disponible"

Symptômes : L'appareil indique que VoWiFi/VoLTE est indisponible malgré un abonnement correct

Causes possibles :

- Entitlements par défaut configurés avec `entitlement_status: 0`
- Entitlement 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'entitlement dans les enregistrements d'activité
3. Vérifiez la configuration des entitlements par défaut :

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

4. Vérifiez les entitlements personnalisées qui remplacent les valeurs par défaut :

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

L'Appareil Obtient un Mauvais Statut d'Entitlement

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

Causes possibles :

- Entitlement personnalisée configurée pour l'abonné
- Mauvais app_id interrogé
- Mismatch 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 entitlements personnalisés :

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

4. Supprimez l'entitlement personnalisé indésirable :

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

Paramètres Manquants dans la Demande

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

Causes possibles :

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

Paramètres requis :

Paramètre	Description
<code>terminal_id</code>	IMEI de l'appareil (15 chiffres)
<code>terminal_vendor</code>	Fabricant (max 4 caractères)
<code>terminal_model</code>	Nom du modèle (max 10 caractères)
<code>terminal_sw_version</code>	Version du logiciel
<code>entitlement_version</code>	Version du protocole (typiquement "2.0")
<code>app</code>	ID(s) d'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>
```

Mismatch de Version (HTTP 406)

Symptômes : L'appareil reçoit HTTP 406 Not Acceptable

Causes possibles :

- Appareil envoyant une `entitlement_version` non prise en charge
- Serveur configuré avec une version incompatible

Résolution :

1. Vérifiez la version configurée du serveur :

```
config :omni_sep,  
  entitlement_version: "2.0"
```

2. Les appareils Android utilisent généralement la version "2.0"
3. Assurez-vous que la version du serveur correspond à la version attendue de l'appareil

Problèmes de Sirmservs XCAP

Profil Non Trouvé (HTTP 404)

Symptômes : La requête GET XCAP retourne 404

Causes possibles :

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

Résolution :

1. Vérifiez le format URI SIP dans la demande :

```
/sirmservs.ngn.etsi.org/users/sip:+  
<msisdn>@<domain>/sirmservs.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": {}
}
```

Mismatch d'ETag (HTTP 412)

Symptômes : La requête 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 requête 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)	<code>http://uri.etsi.org/ngn/params/xml/simservs/xcap</code>
cp	<code>urn:ietf:params:xml:ns:common-policy</code>

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 des éléments correspondent à la spécification ETSI TS 183 023

Le Transfert d'Appel Ne S'Active Pas

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

Causes possibles :

- Règle désactivée dans le profil
- Mauvais type de condition
- Format du 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. IDs de règles et conditions valides :

ID de Règle	Condition	Description
cfu	(aucune)	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 Retourne

Symptômes : La 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 (Root NAI) :

```
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 n'est configuré, le mode simulé doit accepter tout format valide

Token Invalide (HTTP 511)

Symptômes : La demande avec token retourne HTTP 511 Network Authentication Required

Causes possibles :

- Token expiré
- Secret de signature du token changé
- Token généré par une instance différente

Résolution :

1. Vérifiez la période de validité du token :

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

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

Mismatch de Signature de Token

Symptômes : Token ayant l'air valide rejeté

Causes possibles :

- Token provenant d'un environnement différent
- Mismatch de secret de signature entre les instances
- Token altéré

Résolution :

1. Assurez-vous que le `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
```

La Vérification 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 (journalisation d'activité)
 - Tables ETS (entitlements, tokens, 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 sont manquantes

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 du pair 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 files) - ceux-ci contiennent les écritures récentes :

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

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

```
# Ne pas utiliser kill -9, utiliser 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 puissance 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, effacez et réinitialisez :

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

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 Grand

Symptômes : Utilisation du disque en augmentation, 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, # Réduire si nécessaire  
    retention_seconds: 2_592_000     # 30 jours, réduire si  
nécessaire
```

2. Surveillez la taille des tables :

```
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 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 Entitlements

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

# Définir une entitlement 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 sirmservs complet
curl "http://localhost:9014/sirmservs.ngn.etsi.org/users/sip:+<msisdn>@domain/sirmservs.xml"
```

Analyse des Journaux

Modèles de Journaux Clés

Modèle	Signification
<code>[info] GET / ...</code>	Demande d'entitlement entrante
<code>[info] POST / ...</code>	Demande POST entrante (EAP ou entitlement)
<code>[warning] Missing parameters</code>	Échec de la validation de la demande
<code>[error] EAP session timeout</code>	EAP-AKA non complété à temps
<code>[debug] Token validated</code>	Authentification de token 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

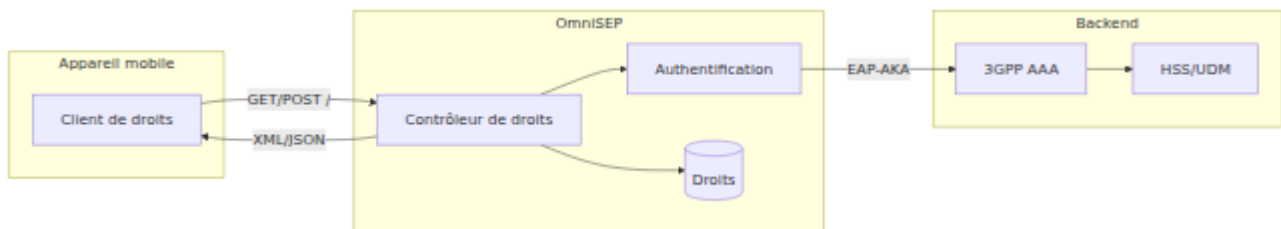
Pour le dépannage spécifique au protocole, référez-vous à :

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

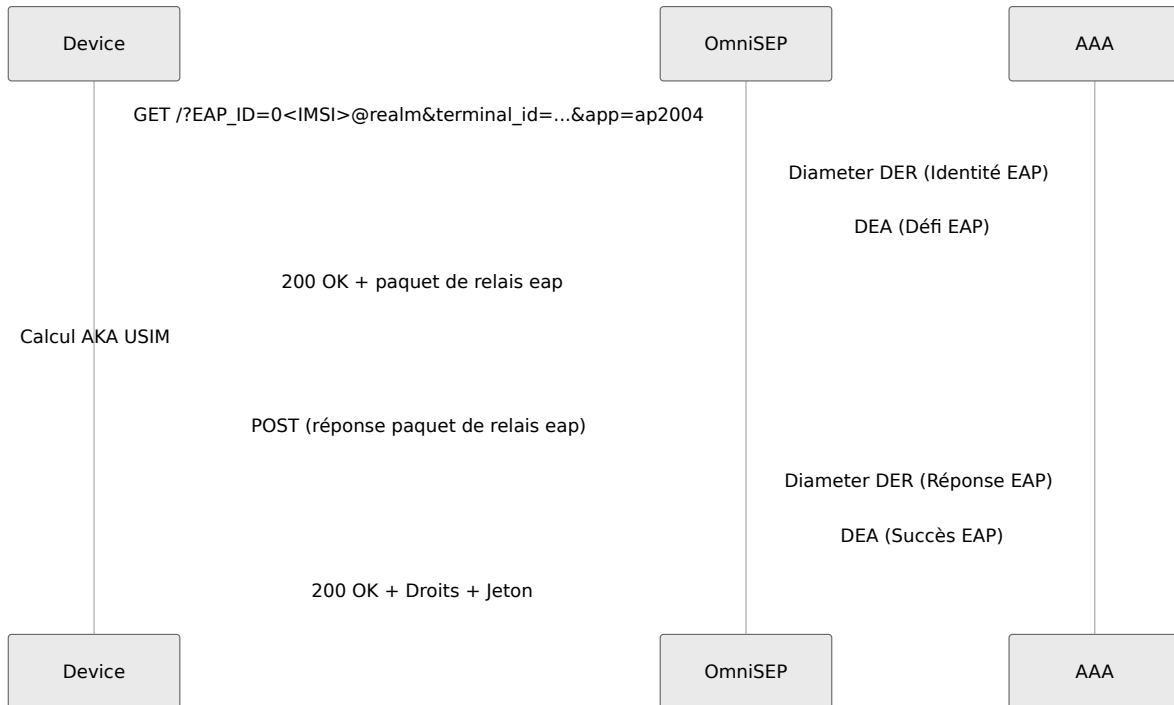
OmniSEP implémente la configuration des droits de service GSMA TS.43, permettant aux appareils mobiles de consulter leurs droits de service (VoWiFi, VoLTE, SMS, etc.) depuis le réseau de l'opérateur.

Aperçu

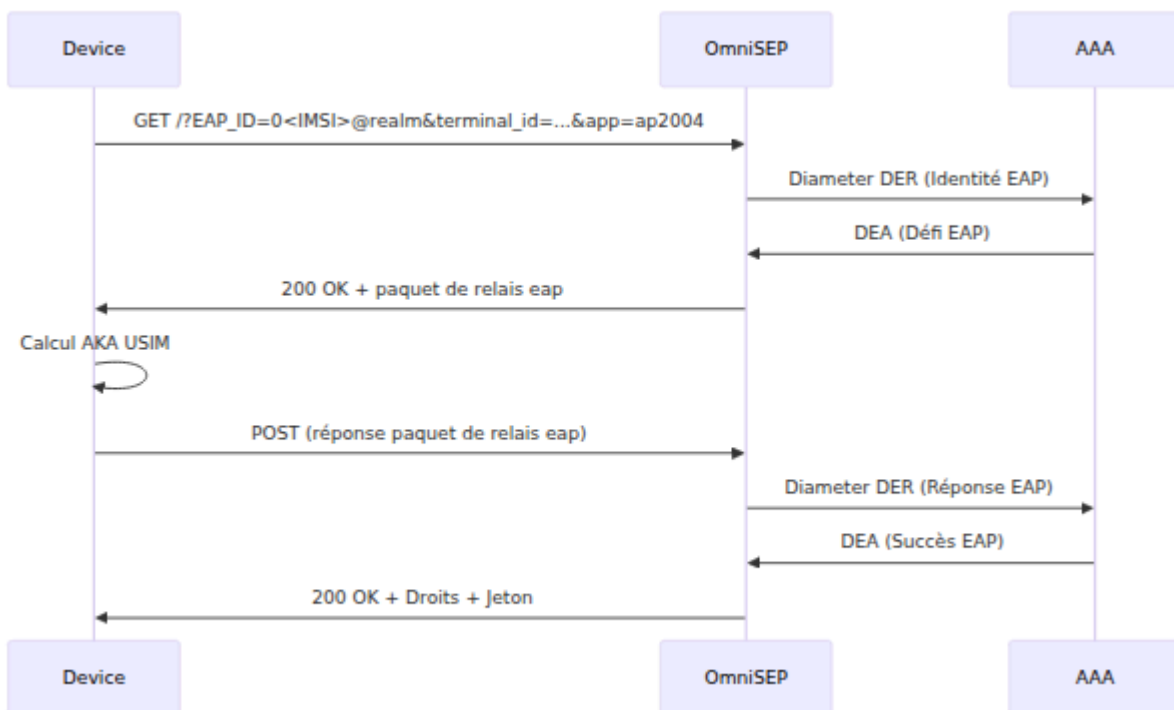


Flux de demande

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 de l'appareil (15 chiffres)
terminal_vendor	String	Fabricant de l'appareil (max 4 chars par RCC.14)
terminal_model	String	Modèle de l'appareil (max 10 chars par RCC.14)
terminal_sw_version	String	Version logicielle (max 20 chars par RCC.14)
entitlement_version	String	Version du protocole (par ex., "2.0")
app	String/Liste	ID(s) de l'application à interroger

Paramètres d'authentification

Un de ces méthodes d'authentification est requise :

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

Paramètres optionnels

Paramètre	Type	Description
<code>IMSI</code>	String	Requis avec <code>token</code> pour la ré-auth rapide
<code>app_name</code>	String	Nom de l'application
<code>app_version</code>	String	Version de l'application
<code>notif_action</code>	Integer	Action de notification (0=désactiver, 1=GCM, 2=FCM)
<code>notif_token</code>	String	Jeton de notification push
<code>vers</code>	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 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 prises en charge

ID d'application	Service	Référence
ap2003	Voix sur réseau cellulaire (VoLTE/VoNR)	TS.43 Section 4
ap2004	Voix sur Wi-Fi (VoWiFi)	TS.43 Section 3
ap2005	SMS sur IP	TS.43 Section 5
ap2006	Compagnon ODSA	TS.43 Section 6
ap2009	Primaire ODSA	TS.43 Section 6
ap2010	Amélioration du 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 et conditions
ProvStatus	Integer	0-3	Statut de provisionnement
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	Provisionnement	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 itinérance
2	Domicile uniquement
3	Itinérance uniquement

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 prise en charge
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
```

```
Mauvaise requête : Paramètres manquants ["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'activités

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

Paramètre	Type	Description
<code>imsi</code>	String	Filtrer par IMSI de l'abonné
<code>terminal_id</code>	String	Filtrer par ID de terminal de l'appareil
<code>from</code>	Integer	Horodatage de début (époque Unix)
<code>to</code>	Integer	Horodatage de fin (époque Unix)
<code>limit</code>	Integer	Nombre maximum d'enregistrements à retourner
<code>offset</code>	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 contre la bibliothèque `service_entitlement` d'Android AOSP.

Format de User-Agent

Les appareils 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]"` - Entre crochets (format Android)
- `["ap2003", "ap2004"]` - Tableau JSON

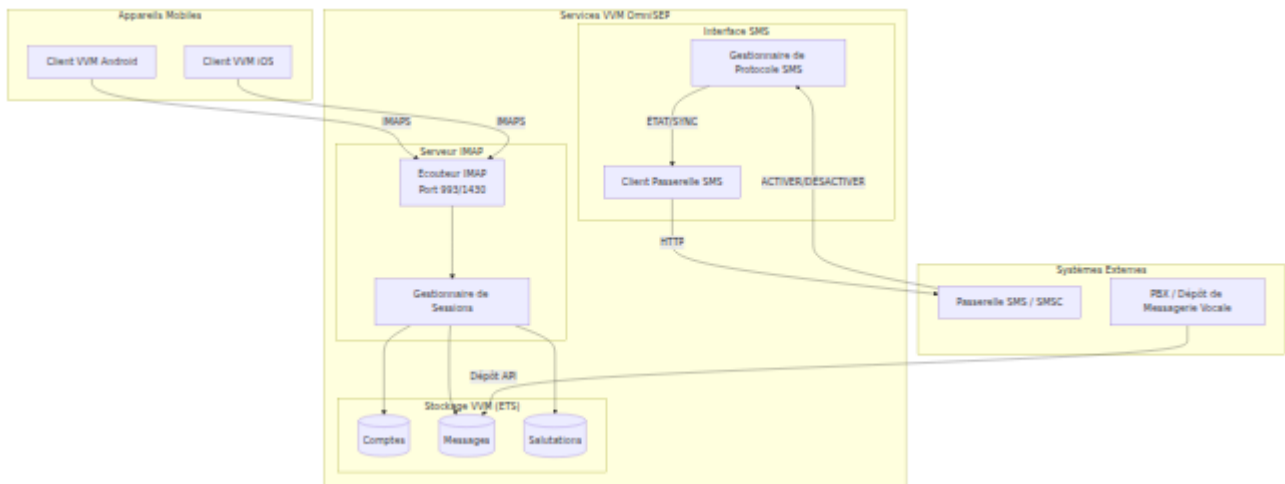
Spécifications de référence

Spécification	Description
GSMA TS.43	Configuration des droits de service
GSMA RCC.14	Directives de configuration des appareils IMS
3GPP TS 33.220	Architecture de démarrage générique (GBA)
3GPP TS 29.273	Interfaces AAA EPS (SWm)

Messagerie Vocale Visuelle (VVM)

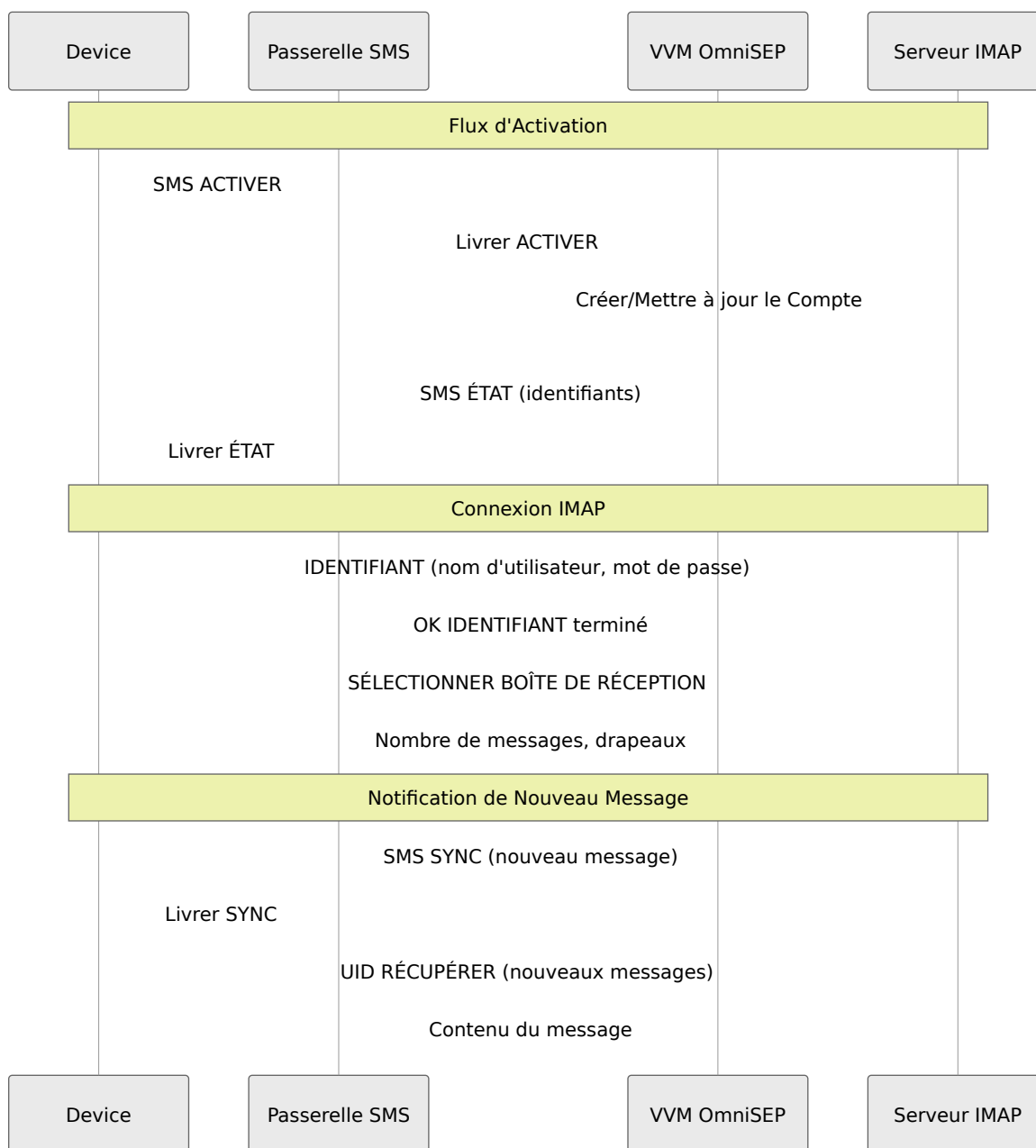
OmniSEP fournit un serveur de Messagerie Vocale Visuelle implémentant la Spécification OMTP VVM v1.3 et GSMA TS.46. Le service VVM permet aux smartphones de gérer les messages vocaux via une interface IMAP, avec un provisionnement géré par SMS.

Vue d'ensemble de l'architecture



Flux de Provisionnement

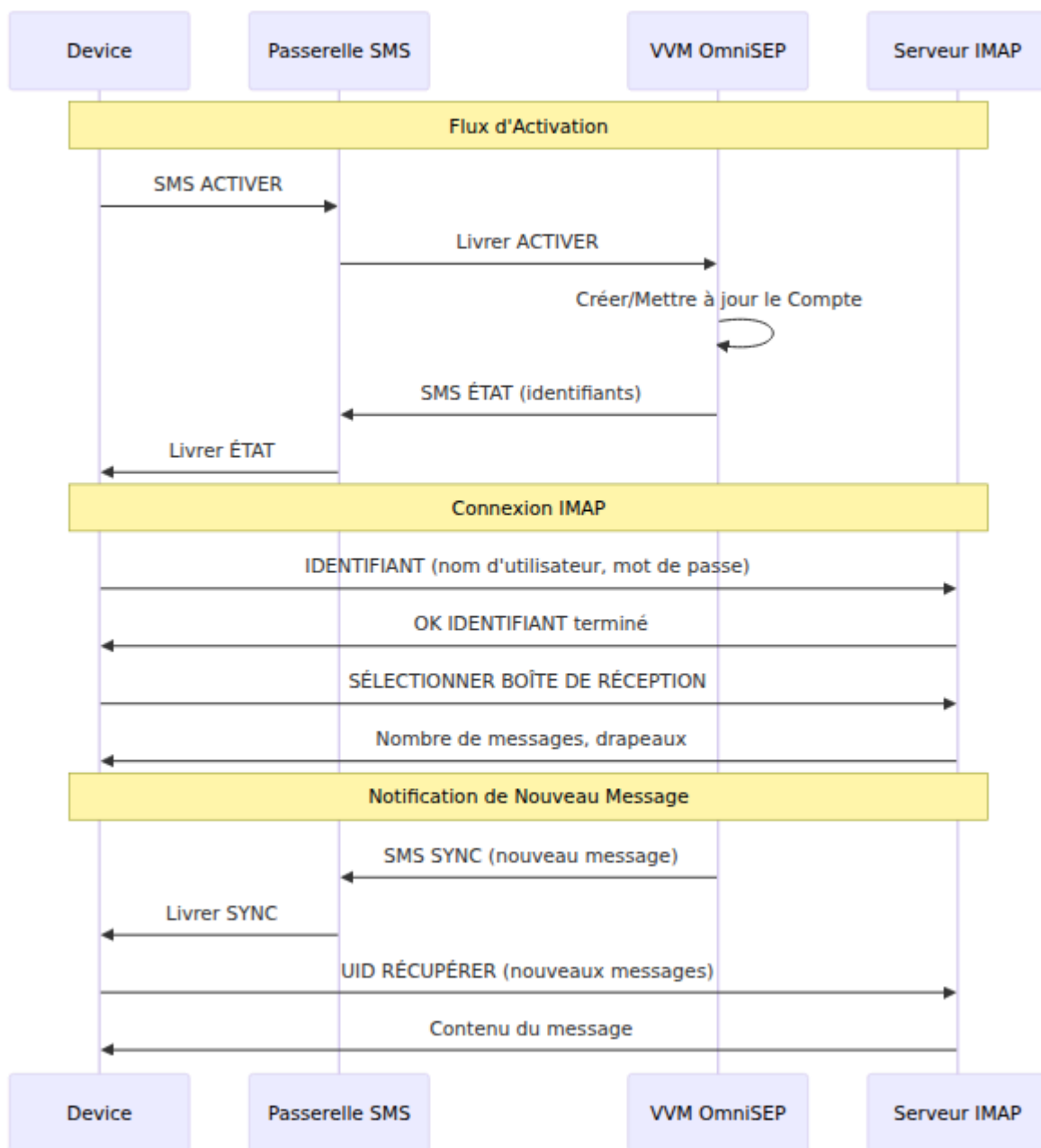
Le provisionnement VVM suit la machine d'état de la spécification OMTP. Lorsqu'un appareil active VVM, il envoie un SMS ACTIVER, reçoit des identifiants via un SMS ÉTAT, puis se connecte via IMAP.



États de Provisionnement

Le service VVM suit l'état de provisionnement des abonnés selon la spécification OMTP :

État	Code	Description
Inconnu	U	État initial, aucun provisionnement tenté
Nouveau	N	Compte créé, en attente de la première connexion client
Prêt	R	Entièrement provisionné et opérationnel
Provisionné	P	Identifiants envoyés, en attente de vérification par le client
Bloqué	B	Service désactivé ou suspendu



Protocole SMS

Message ÉTAT (Serveur vers Client)

Envoyé après l'activation pour fournir les identifiants IMAP :

```
//VVM:STATUS:st=R;rc=0;srv=vvm.example.com;ipt=993;spt=587;u=5050100015;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=succès)
srv	Nom d'hôte du serveur IMAP
ipt	Port IMAP
spt	Port SMTP (le cas échéant)
u	Nom d'utilisateur (basé sur l'IMSI)
pw	Mot de passe
tui	Numéro d'accès TUI
dn	Numéro de destination SMS (pour les réponses des clients)
lang	Code de langue
g_len	Durée maximale de la salutation en secondes
vs_len	Durée maximale de la signature vocale en secondes
pw_len	Plage de longueur du code PIN
pm	Code PIN requis (Y/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 Client)

Envoyé lorsque le contenu de la boîte aux lettres change :

```
//VVM:SYNC:ev=NM;id=123;c=5;t=v;s=+61400123456;dt=15/01/2024 10:30+0000;l=30
```

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=infodivertissement, e=ECC)
s	Numéro de l'expéditeur
dt	Horodatage du dépôt
l	Durée du message en secondes

Message ACTIVER (Client vers Serveur)

Envoyé par l'appareil pour activer VVM :

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

Champ	Description
pv	Version du protocole
ct	Type de client (vendeur.modèle.version_os)

Message DÉSACTIVER (Client vers Serveur)

Envoyé par l'appareil pour désactiver VVM :

```
Désactiver:pv=11
```

Serveur IMAP

Le serveur IMAP VVM implémente un sous-ensemble d'IMAP4rev1 (RFC 3501) adapté pour la messagerie vocale :

Commandes Supportées

Commande	Description
CAPABILITÉ	Lister les capacités du serveur
IDENTIFIANT	Authentifier avec nom d'utilisateur/mot de passe
DÉCONNECTER	Terminer la session
SÉLECTIONNER	Ouvrir la boîte aux lettres (BOÎTE DE RÉCEPTION, Corbeille, Enregistré)
EXAMINER	Ouvrir la boîte aux lettres en lecture seule
LISTE	Lister les boîtes aux lettres disponibles
ÉTAT	Obtenir l'état de la boîte aux lettres (nombre de messages)
RÉCUPÉRER	Récupérer le contenu du message
UID RÉCUPÉRER	Récupérer par UID
STOCKER	Mettre à jour les drapeaux du message
UID STOCKER	Mettre à jour les drapeaux par UID
RECHERCHER	Rechercher des messages
UID RECHERCHER	Rechercher par UID
COPIER	Copier des messages entre les boîtes aux lettres
EXPUNGER	Supprimer définitivement les messages marqués
FERMER	Fermer la boîte aux lettres et expurger

Commande	Description
OBTENIRQUOTAROOT	Obtenir le quota de stockage
NOOP	Garder la connexion active

Capacités

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

Structure de la Boîte aux Lettres

Boîte aux Lettres	Description
BOÎTE DE RÉCEPTION	Messages vocaux nouveaux et lus
Corbeille	Messages marqués pour suppression
Enregistré	Messages archivés

Format du Message

Les messages vocaux sont présentés sous forme d'e-mail RFC 5322 avec une structure MIME multipartite :

From: +61400123456 <voicemail@vvm.local>
To: 505010000000001@ims.example.com
Date: Sam, 25 Jan 2025 10:30:00 +0000
Subject: Messagerie vocale de +61400123456
Message-ID: <123@vvm.omnisep>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="-----_Part_0"
X-VVM-MessageType: voice
X-VVM-Duration: 30
X-VVM-Sender: +61400123456

-----_Part_0
Content-Type: text/plain; charset="UTF-8"

Messagerie vocale de: +61400123456
Durée: 30 secondes

Transcription:
Bonjour, ceci est un message vocal de test.

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

[Audio encodé en Base64]

-----_Part_0--

En-têtes Personnalisés

En-tête	Description
X-VVM-MessageType	Type de message (voix, vidéo, fax, infodivertissement, ecc)
X-VVM-Duration	Durée du message en secondes
X-VVM-Sender	Numéro de l'appelant d'origine

Configuration

Activation de VVM

```
# config/config.exs
config :omni_sep, :vvm,
  enabled: true,

  # Paramètres du serveur IMAP
  imap_port: 993,
  imap_ssl: true,
  imap_server: "vvm.example.com",
  imap_cert: "priv/cert/server.crt",
  imap_key: "priv/cert/server.key",

  # Numéro TUI (Interface Utilisateur Traditionnelle)
  tui_number: "*86",

  # Paramètres SMS
  sms_source_number: "+614000000000",
  sms_gateway: "https://sms-gateway.example.com/api/send",

  # Paramètres du 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
<code>enabled</code>	Booléen	Non	false
<code>imap_port</code>	Entier	Non	993
<code>imap_ssl</code>	Booléen	Non	true
<code>imap_server</code>	Chaîne	Oui	-
<code>imap_cert</code>	Chaîne	Non	priv/cert/server.crt
<code>imap_key</code>	Chaîne	Non	priv/cert/server.key
<code>smtp_port</code>	Entier	Non	587

Paramètre	Type	Requis	Par défaut
tui_number	Chaîne	Non	*86
sms_source_number	Chaîne	Oui	-
sms_gateway	Chaîne	Non	nil
min_pin_length	Entier	Non	4
max_pin_length	Entier	Non	15
default_max_messages	Entier	Non	100
default_storage_limit_kb	Entier	Non	50000

Paramètre	Type	Requis	Par défaut
default_max_greeting_seconds	Entier	Non	60

Configuration de Développement

Pour le développement, utilisez IMAP simple (sans TLS) pour faciliter les tests :

```
# config/dev.exs
config :omni_sep, :vvm,
  enabled: true,
  imap_port: 1430,
  imap_ssl: false,
  imap_server: "localhost",
  tui_number: "*86",
  sms_source_number: "+61400000000"
```

Configuration de Production

```
# config/prod.exs
config :omni_sep, :vvm,
  enabled: true,
  imap_port: 993,
  imap_ssl: true,
  imap_server: "vvm.carrier.example.com",
  imap_cert: "/etc/omnisep/certs/vvm.crt",
  imap_key: "/etc/omnisep/certs/vvm.key",
  tui_number: "*86",
  sms_source_number: "+61400000001",
  sms_gateway: "https://smc.carrier.example.com/api/v1/send"
```

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 actuellement actives

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

- `command` - Commande IMAP: `LOGIN`, `SELECT`, `FETCH`, etc.
- `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 total de messages vocaux actuellement stockés

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`

Métriques de Compte

Métrique: `vvm_accounts_total` **Type:** Compteur **Description:** Opérations sur les comptes VVM **Étiquettes:**

- `operation` - Opération: `create`, `activate`, `deactivate`, `update`
- `result` - Résultat: `success`, `error`

Métrique: `vvm_accounts_active` **Type:** Jauge **Description:** Nombre de comptes VVM actifs

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]))

# Durée moyenne des messages
histogram_quantile(0.5,
rate(vvm_message_duration_seconds_bucket[5m]))

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

# Sessions actives au fil du temps
vvm_imap_active_sessions
```

Gestion des Salutations

VVM prend en charge plusieurs types de salutations par abonné :

Type de Salutation	Description
<code>normal</code>	Salutation personnelle standard
<code>busy</code>	Joué lorsque l'abonné est occupé
<code>extended_absence</code>	Salutation de vacances ou d'absence
<code>voice_signature</code>	Signature vocale pour l'annonce du nom

Les salutations sont stockées et récupérées via l'API de stockage. Le serveur IMAP inclut les métadonnées de salutation dans la réponse de quota de compte.

Dépannage

Le Client Ne Peut Pas Activer VVM

Symptômes: L'appareil affiche "Messagerie Vocale Visuelle indisponible" ou l'activation échoue

Causes possibles:

- Passerelle SMS non configurée ou inaccessible
- Numéro source non autorisé auprès du SMSC
- Service VVM désactivé dans la configuration

Résolution:

1. Vérifiez que `sms_gateway` est configuré et accessible
2. Consultez les journaux de la passerelle SMS pour l'état de livraison
3. Confirmez `enabled: true` dans la configuration VVM
4. Examinez les métriques: `vvm_sms_total{type="status"}`

Échecs d'Authentification IMAP

Symptômes: Le client ne peut pas se connecter après avoir reçu le SMS ÉTAT

Causes possibles:

- Mismatch nom d'utilisateur/mot de passe
- Problèmes de certificat TLS
- Pare-feu bloquant le port IMAP

Résolution:

1. Vérifiez que les identifiants correspondent entre le SMS ÉTAT et le stockage de compte
2. Vérifiez la validité du certificat TLS et la chaîne de confiance
3. Confirmez que le pare-feu autorise le trafic sur le port IMAP configuré
4. Testez avec telnet/openssl: `openssl s_client -connect vvm.example.com:993`

Messages Ne Se Synchronisant Pas

Symptômes: Nouveaux messages vocaux n'apparaissant pas sur l'appareil

Causes possibles:

- SMS SYNC non envoyé
- Session IMAP déconnectée
- Échec du dépôt de message

Résolution:

1. Vérifiez les métriques `vvm_sms_total{type="sync"}`
2. Vérifiez la connectivité de la passerelle SMS
3. Vérifiez `vvm_messages_total{operation="deposit"}` pour les échecs de dépôt
4. Examinez les métriques de session IMAP pour les déconnexions

Utilisation Élevée du Stockage

Symptômes: Abonnés atteignant les limites de quota

Résolution:

1. Examinez les paramètres de quota: `default_storage_limit_kb`, `default_max_messages`
2. Vérifiez la jauge `vvm_messages_stored`
3. Envisagez de mettre en œuvre l'expiration automatique des messages
4. Examinez le stockage des salutations: `get_greetings/1` retourne les tailles audio

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 barring d'appels et les paramètres d'identification de l'appelant.

Interface du Panneau de Contrôle

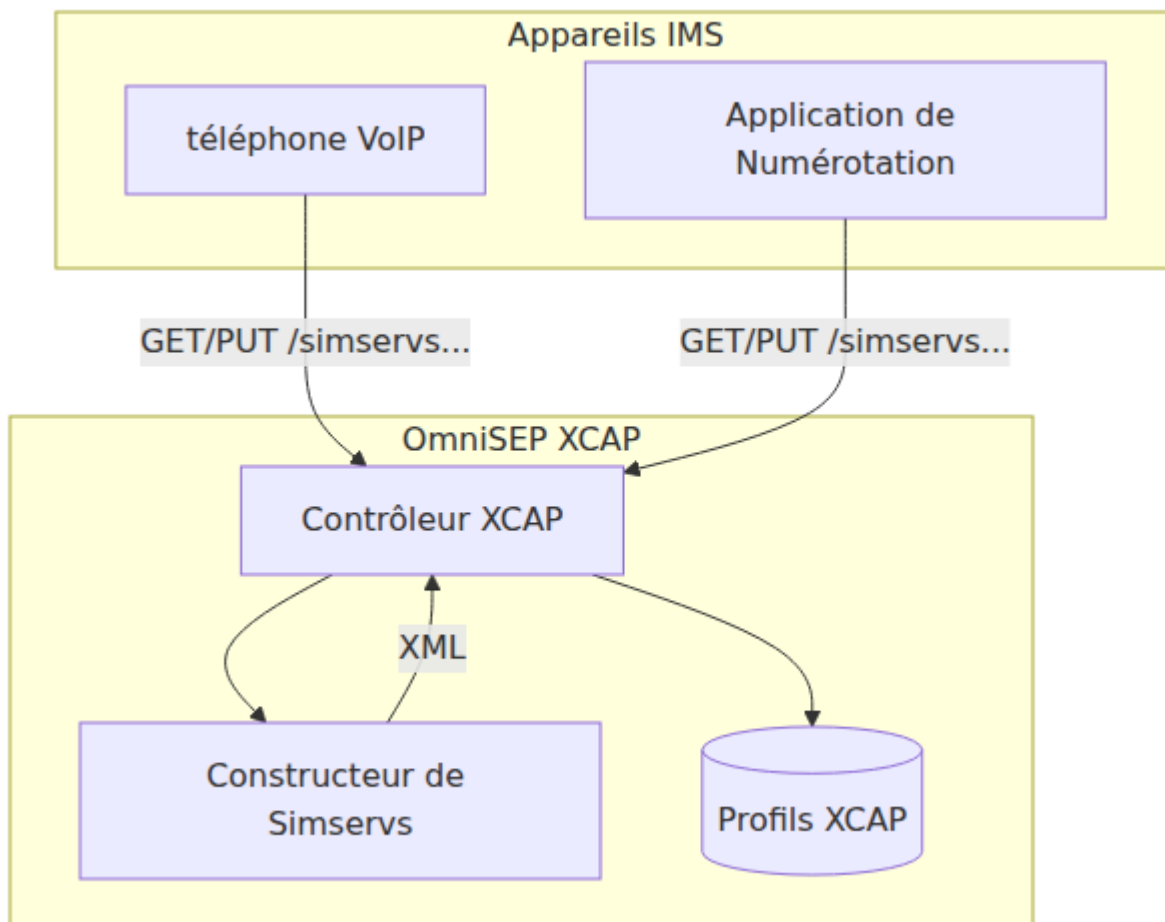
La page des Profils Simservs XCAP fournit une interface web pour visualiser et gérer les profils des abonnés :

Fonctionnalités :

- Rechercher et filtrer les profils locaux par MSISDN
- Récupérer des 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 Barring d'Appels Entrants et Sortants avec conditions
- Synchronisation Push/Pull avec HSS
- Mode d'édition pour modifier les paramètres du profil

Aperçu



Structure du Document Sivers

Le document sivers 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/~/simserv
PUT	/simservs.ngn.etsi.org/users/{sip}/simservs.xml/~/simserv
DELETE	/simservs.ngn.etsi.org/users/{sip}/simservs.xml/~/simserv

Types de Contenu

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

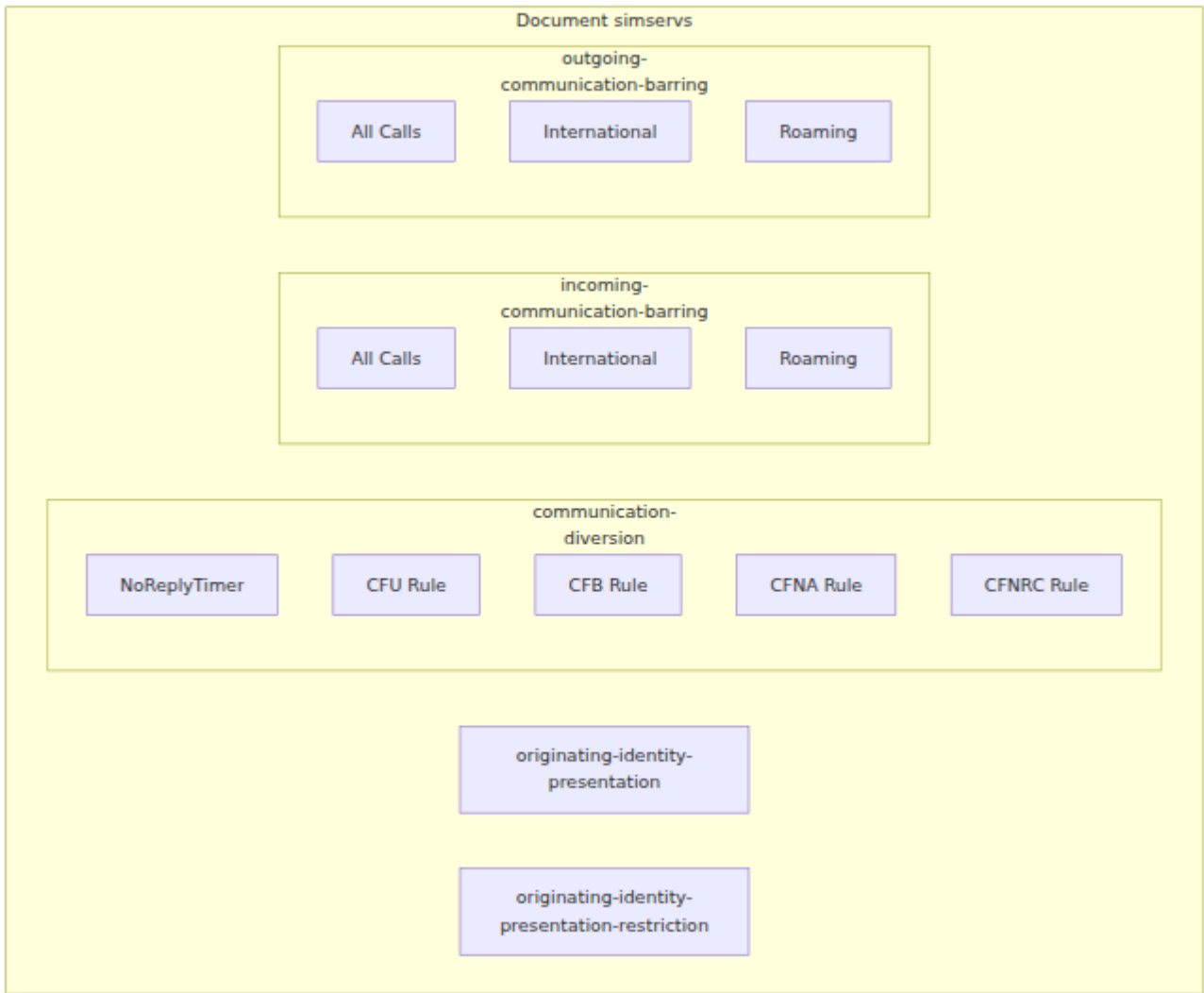
Support ETag

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 priorisant le local 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 requêtes XCAP

Stratégie de Mise en Cache

Opérations de Lecture (GET)

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

Opérations d'Écriture (PUT)

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

Génération d'ETag

Les ETags sont calculés comme des hachages MD5 des données de 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 provenant 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/barring 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)	Synchrone en cas de cache miss
Pousser les changements	Sh PUR (Profile-Update-Request)	Asynchrone après PUT

Le push asynchrone signifie que les mises à jour HSS ne bloquent pas les réponses des clients, améliorant la latence pour les requêtes des appareils.

Document XML Sirmservs

Exemple de Document Complet

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

</sirmservs>
```

Espaces de Noms

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

Services

Présentation de l'Identité de l'Appelant (OIP)

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

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

Attribut	Type	Description
<code>active</code>	Booléen	Service activé/désactivé

Restriction de la Présentation de l'Identité de l'Appelant (OIR)

Contrôle le masquage de l'identité 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, cfnc, 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)

Barring d'Appels

Barring 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>
```

Barring 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 Barring

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

Exemples d'API

Obtenir le Document Complet Sivers

```
GET
/sivers.ngn.etsi.org/users/sip:+15551234567@ims.example.com/sivers
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"?>
<sivers
xmlns="http://uri.etsi.org/ngn/params/xml/sivers/xcap"...>
  ...
</sivers>
```

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
Barring d'Appels (Entrants)	Tous les appels autorisés
Barring d'Appels (Sortants)	Tous les appels autorisés

Réponses d'Erreur

Statut HTTP	Description
200	Succès
304	Non Modifié (If-None-Match correspond)
400	Mauvaise Requête - 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 : sirmservs/unknown</error-
element>
</xcap-error>
```

Spécifications de Référence

Spécification	Description
ETSI TS 183 023	Cadre XCAP pour les Sirmservs 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

OmniSEP - Plateforme de Point de Service

OmniSEP est une plateforme unifiée de point de service fournissant des mises en œuvre de qualité opérateur des protocoles de provisionnement des appareils mobiles. Elle gère la configuration des droits d'accès TS.43, les services supplémentaires XCAP et la messagerie vocale visuelle à partir d'une seule plateforme.

Liens Rapides

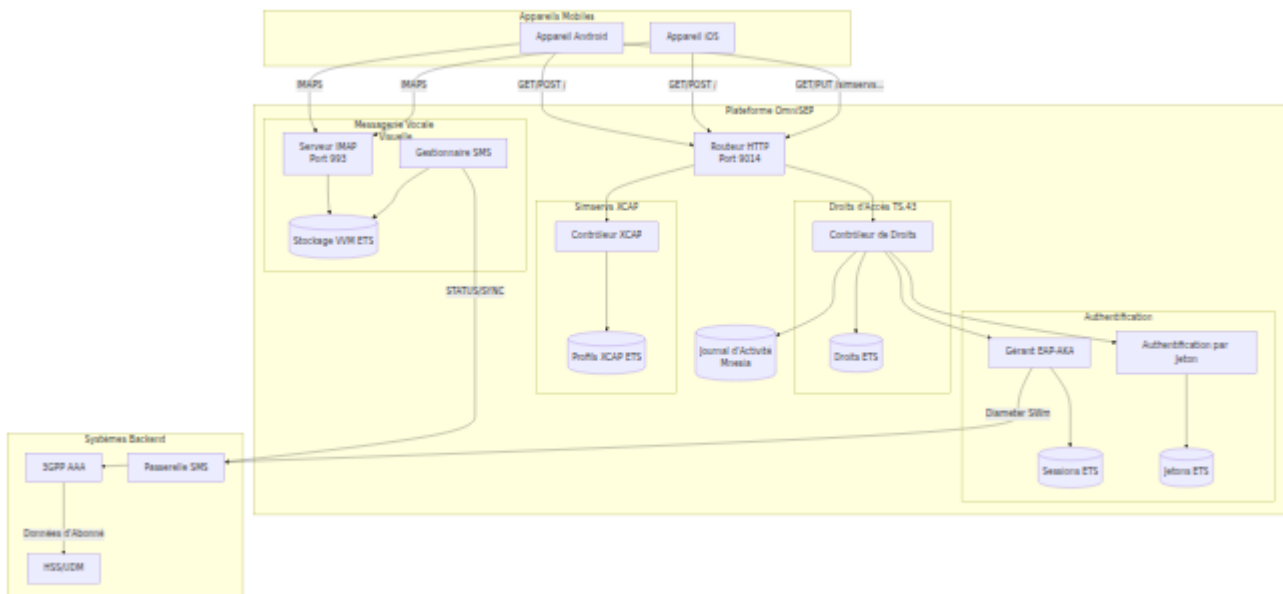
Opérations & Surveillance

- **Référence de Configuration** - Documentation complète des paramètres pour tous les services
- **Dépannage** - Problèmes courants et résolutions

Documentation des Services

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

Vue d'Ensemble de l'Architecture



Services Supportés

Configuration des Droits d'Accès TS.43

Implémente GSMA TS.43 pour les requêtes de droits d'accès au service des appareils :

ID d'App	Service	Description
ap2003	Voix sur Réseau 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	Augmentation de Forfait de Données	Informations sur le forfait de données
ap2012	Facturation Directe par Opérateur	Statut du service DCB
ap2016	Mode Satellite	Droits de connectivité satellite

Services Supplémentaires XCAP

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

Service	Description	Référence
Diversion de Communication	Renvoi 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

Vue d'Ensemble 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 inclut une interface web en temps réel pour la surveillance et la gestion, construite avec Phoenix LiveView. Accédez à l'interface 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 du service, utilisation de la mémoire, statistiques de stockage
Droits d'Accès	/entitlements	Voir et gérer les droits d'accès 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 Sirmservs XCAP, synchroniser avec HSS
Diameter	/diameter	Surveiller les connexions et l'état des pairs Diameter
Journaux	/logs	Visionneuse de journal 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 du Service** : Serveur HTTP, EAP-AKA, indicateurs de service VVM
- **Compteurs de Stockage** : Droits d'accès, 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 afficher les profils d'abonnés par MSISDN
- Modifier les paramètres des services supplémentaires (OIP/OIR, renvoi d'appel, blocage d'appel)
- Extraire des profils de HSS via l'interface Diameter Sh
- Pousser les 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 demandes des appareils :

Journal d'activité montrant les requêtes XCAP et de droits d'accès avec les détails des requêtes/réponses

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

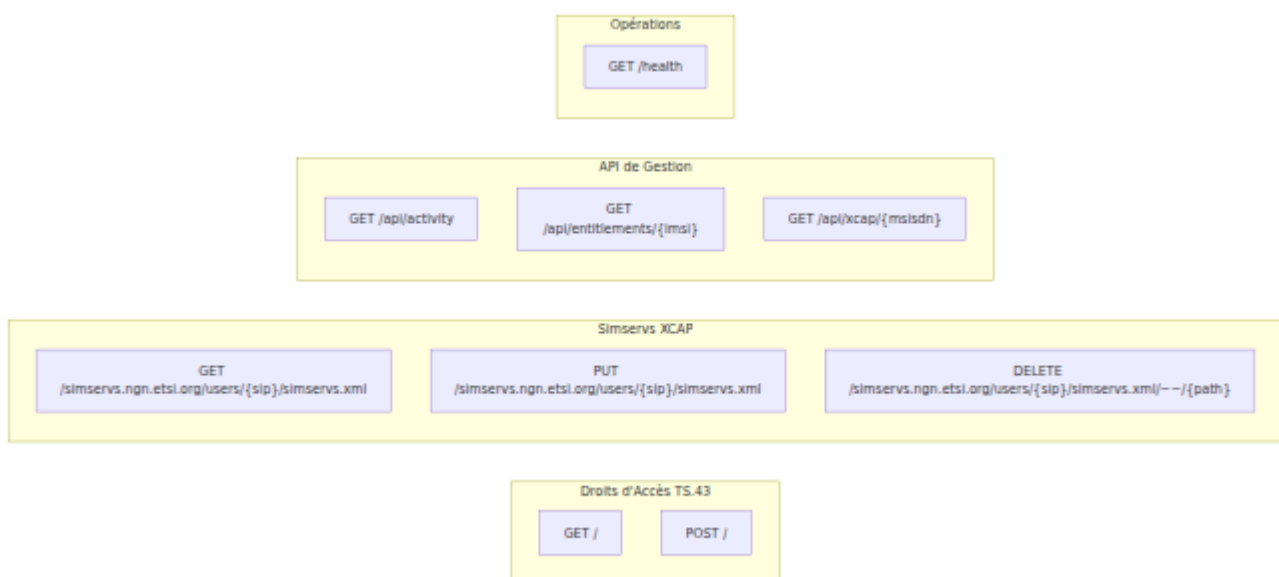
Surveillance des Sessions

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 avant 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 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 d'Accès TS.43](#) pour le provisionnement VoWiFi/VoLTE
2. [Simservs XCAP](#) pour le renvoi/bloquage d'appels

Dépannage :

1. [Guide de Dépannage](#) pour les problèmes courants
2. Vérifiez [Journal d'Activité](#) pour le suivi des demandes

Par Protocole

GSMA TS.43 :

- [Droits d'Accès TS.43](#) - Documentation complète des droits d'accès au 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