OmniSEP Configuration Reference

Complete configuration reference for OmniSEP Service Endpoint Platform.

Table of Contents

Configuration Structure

HTTP Server Configuration

Controls the HTTP endpoint where devices connect.

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

Parameters

Parameter	Type	Required	Default	
`http_port`	Integer	No	9014	TCP port for HTTP terminator in prod
`http_ip`	Tuple	No	`{0, 0, 0, 0}`	IP address to bind. Use specific IP for
`server_fqdn`	String	Yes	-	Server's fully qual `aes.mnc<MNC>.` per GSMA TS.43 S
`entitlement_version`	String	No	"2.0"	TS.43 protocol ver "2.0".

FQDN Format

The server FQDN follows the 3GPP naming convention:

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

Component	Description	Example
`aes`	Application Entitlement Server prefix	`aes`
`mnc<MNC>`	Mobile Network Code (3 digits, zero-padded)	`mnc001`
`mcc<MCC>`	Mobile Country Code (3 digits)	`mcc310`
`pub.3gppnetwork.org`	Standard 3GPP domain suffix	-

Example: For MCC 310 (USA), MNC 410 (AT&T):

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

Storage Configuration

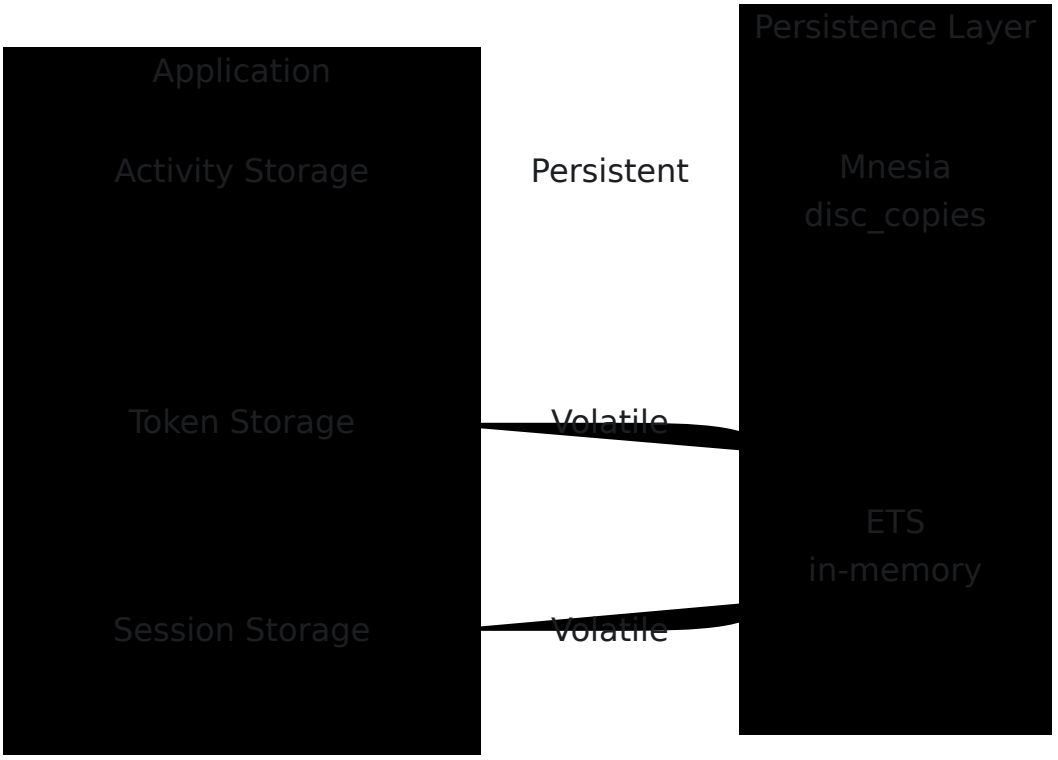
Controls persistent data storage using Mnesia for audit-compliant activity logging.

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

Parameters

Parameter	Type	Required	Default	Description
`data_dir`	String	No	"priv/data"	Directory for Mnesia database files. Activity logs are persisted here and survive application restarts.

Storage Architecture



Mnesia Tables

Activity logging uses Mnesia `disc_copies` tables for persistence:

Table	Purpose	Persistence
`activity`	Activity records (audit log)	Mnesia disc_copies
`activity_by_imsi`	IMSI index for fast lookup	Mnesia disc_copies
`activity_by_terminal`	Terminal ID index	Mnesia disc_copies

Data Directory Structure

```
priv/data/
└── mnesia/
    ├── schema.DAT         # Mnesia schema
    ├── activity.DCD       # Activity table data
    ├── activity.DCL       # Activity transaction log
    ├── activity_by_imsi.DCD
    ├── activity_by_imsi.DCL
    ├── activity_by_terminal.DCD
    ├── activity_by_terminal.DCL
    ├── DECISION_TAB.LOG
    └── LATEST.LOG
```

Production Considerations

For production deployments:

1. **Data Directory Permissions**: Ensure the data directory is writable by the application user
2. **Disk Space**: Monitor disk usage as activity logs grow
3. **Backup**: Include the Mnesia directory in backup procedures
4. **Recovery**: Mnesia automatically recovers from transaction logs on startup

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

Default Entitlements

Defines the entitlement status returned to subscribers who have no custom configuration.

```
config :omni_sep, :default_entitlements,
  # VoWiFi (ap2004) defaults
  vowifi: %{
    entitlement_status: 1,           # ENABLED
    addr_status: 2,                  # NOT_REQUIRED
    tc_status: 2,                    # NOT_REQUIRED
    prov_status: 1,                  # PROVISIONED
    service_flow_url: "",
    service_flow_user_data: "",
    message_for_incompatible: "VoWiFi service is not available for
your subscription."
  },

  # Voice-over-Cellular (ap2003) defaults
  volte: %{
    entries: [
      %{
        access_type: 1,              # 4G/LTE
        home_roaming_nw_type: 1,     # Home & Roaming
        entitlement_status: 1        # ENABLED
      },
      %{
        access_type: 2,              # 5G/NR
        home_roaming_nw_type: 1,     # Home & Roaming
        entitlement_status: 1,       # ENABLED
        network_voice_irat_capability: "EPS-Fallback"
      }
    ]
  },

  # SMSoIP (ap2005) defaults
  smsoip: %{
    entitlement_status: 1            # ENABLED
  },

  # Data Plan (ap2010) defaults
  data_plan: %{
    entitlement_status: 1
  },

  # Direct Carrier Billing (ap2012) defaults
  dcb: %{
    entitlement_status: 0,           # DISABLED by default
```

```
  tc_status: 2                      # NOT_REQUIRED
},

# Satellite Mode (ap2016) defaults
satmode: %{
  entitlement_status: 0             # DISABLED by default
}
```

VoWiFi Parameters (ap2004)

Parameter	Type	Values	Description
`entitlement_status`	Integer	0=Disabled, 1=Enabled, 2=Incompatible, 3=Provisioning	Service availabilit status
`addr_status`	Integer	0=Not Available, 1=Available, 2=Not Required, 3=In Progress	Address verificati status
`tc_status`	Integer	0=Not Available, 1=Available, 2=Not Required, 3=In Progress	Terms & Condition acceptance statu
`prov_status`	Integer	0=Not Provisioned, 1=Provisioned, 2=Not Required, 3=In Progress	Provisioning statu
`service_flow_url`	String	URL	URL for service flo (address verificat T&C)
`service_flow_user_data`	String	-	User data passed service flow

Parameter	Type	Values	Description
`message_for_incompatible`	String	-	Message shown w `entitlement_sta`

VoLTE Parameters (ap2003)

VoLTE configuration uses an array of entries, one per access technology:

Parameter	Type	Values	Description
`access_type`	Integer	1=4G/LTE, 2=5G/NR	Radio access technology
`home_roaming_nw_type`	Integer	1=Home & Roaming, 2=Home Only, 3=Roaming Only	Network scope
`entitlement_status`	Integer	0=Disabled, 1=Enabled	Service availability
`network_voice_irat_capability`	String	"EPS-Fallback", "VoNR"	5G voice capability

Entitlement Status Values

Value	Name	Description
0	DISABLED	Service not available
1	ENABLED	Service available and ready
2	INCOMPATIBLE	Device or subscription incompatible
3	PROVISIONING	Provisioning in progress

Token Configuration

Controls authentication token generation and validation.

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

Parameters

Parameter	Type	Required	Default	Description
`validity_seconds`	Integer	No	86400	Token lifetime in seconds. Default is 24 hours.
`signing_secret`	String	Yes	-	Secret key for token signing. **Must be changed in production.** Use a cryptographically random string of at least 32 characters.

Security Considerations

- Generate a unique `signing_secret` for each deployment
- Rotate secrets periodically
- Use environment variables for secrets in production:

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

EAP-AKA Configuration

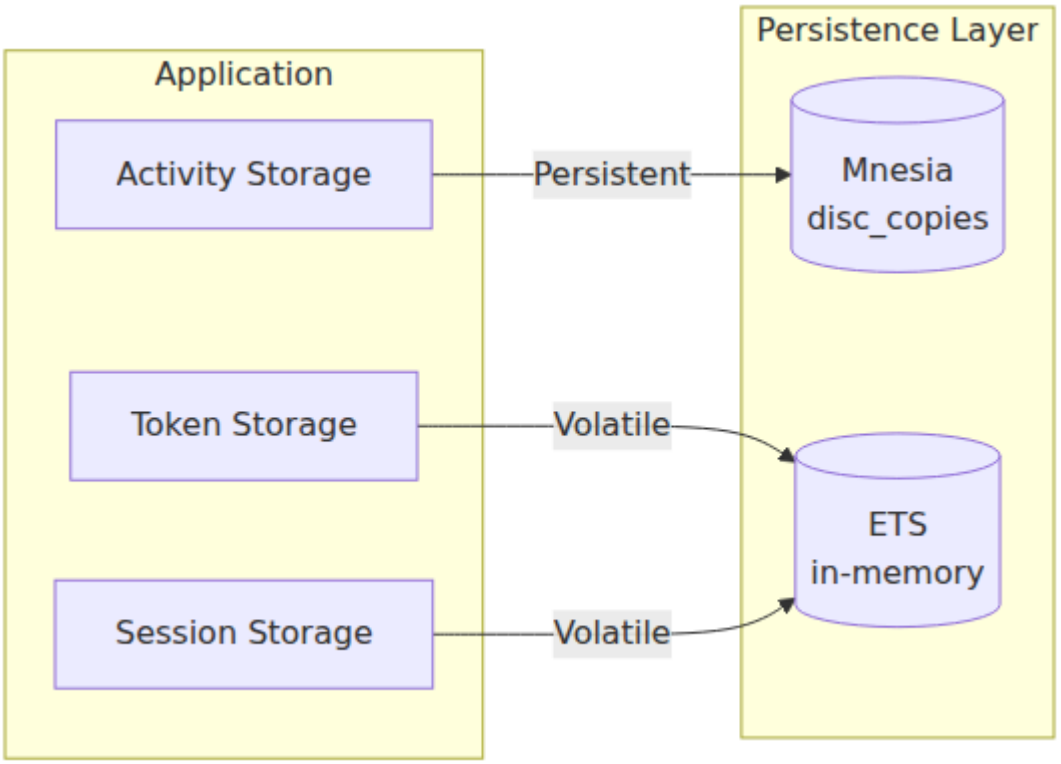
Controls EAP-AKA authentication behavior for initial device authentication.

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

Parameters

Parameter	Type	Required	Default	Description
`enabled`	Boolean	No	true	Enable EAP-AKA authentication. When false, only token-based auth is accepted.
`session_timeout_ms`	Integer	No	30000	EAP session timeout in milliseconds. Session expires if client doesn't respond within this time.

EAP-AKA Flow



Diameter Configuration

Configures the Diameter client for EAP-AKA authentication via SWm interface.

```
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
    }
  ]
```

Core Parameters

Parameter	Type	Required	Default	Desc
`service_name`	Atom	Yes	-	Interna service identif
`host`	String	Yes	-	Diame Origin- Must b resolva FQDN 6733.
`realm`	String	Yes	-	Diame Origin- Used f routing RFC 67
`vendor_id`	Integer	Yes	10415	3GPP V ID per TS 29.
`auth_application_ids`	List	Yes	-	List of suppor auth applica IDs. SV 16777
`request_timeout`	Integer	No	5000	Reque timeou millise

Parameter	Type	Required	Default	Desc
`peer_selection_algorithm`	Atom	No	`:round_robin`	Peer selecti `:roun` or `:fa`

Network Parameters

Parameter	Type	Required	Default	Description
`listen_ip`	Tuple	No	`{127, 0, 0, 1}`	IP to bind for incoming Diameter connections
`listen_port`	Integer	No	3868	Diameter port per RFC 6733

Peer Parameters

Each peer in the `peers` list:

Parameter	Type	Required	Default	Description
`host`	String	Yes	-	Peer's Diameter Identity (must match peer's Origin-Host exactly)
`ip`	String	Yes	-	Peer's IP address for TCP/SCTP connection
`port`	Integer	No	3868	Peer's Diameter port
`transport`	Atom	No	`:tcp`	Transport: `:tcp` or `:sctp`

SWm Application

The SWm interface (Application ID 16777265) is used for EAP-AKA authentication per 3GPP TS 29.273.

Message	Code	Description
DER	268	Diameter-EAP-Request - Carries EAP payload to AAA
DEA	268	Diameter-EAP-Answer - Returns EAP response from AAA

Mock Mode

If no Diameter peers are configured, OmniSEP operates in mock mode:

- EAP-AKA challenges are simulated
- IMSI is extracted from EAP_ID
- Authentication always succeeds
- Useful for development and testing

Activity Logging

Controls subscriber activity logging for audit and troubleshooting.

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

Parameters

Parameter	Type	Required	Default	Descript
`max_records_per_subscriber`	Integer	No	1000	Maximum activity records ke per subscribe Oldest records ar deleted w limit is exceeded
`retention_seconds`	Integer	No	2592000	Activity retention period in seconds. Default is days. Records older thar this are automatic cleaned u

Activity Record Contents

Each activity record contains:

Field	Description
`imsi`	Subscriber IMSI
`terminal_id`	Device IMEI/terminal ID
`timestamp`	Request timestamp
`client_ip`	Client IP address
`user_agent`	HTTP User-Agent header
`app_ids`	Requested application IDs
`auth_method`	Authentication method used (EAP-AKA, TOKEN)
`response_code`	HTTP response status code

Environment-Specific Configuration

Development

```
# config/dev.exs
import Config

config :omni_sep,
  http_port: 9014

config :omni_sep, :eap_aka,
  enabled: true  # Mock mode - no AAA peers

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
```

Environment Variables

Variable	Description
`OMNI_SEP_FQDN`	Server FQDN for TS.43
`OMNI_SEP_TOKEN_SECRET`	Token signing secret
`DIAMETER_HOST`	Diameter Origin-Host
`DIAMETER_REALM`	Diameter Origin-Realm
`AAA_PEER_HOST`	AAA peer hostname
`AAA_PEER_IP`	AAA peer IP address

Logger Configuration

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

Metadata	Description
`request_id`	Unique request identifier (UUID)
`imsi`	Subscriber IMSI (when authenticated)
`terminal_id`	Device terminal ID from request

OmniSEP Troubleshooting Guide

Common issues and resolutions for OmniSEP Service Endpoint Platform.

Table of Contents

Activity Log

The Activity Log provides a real-time view of all requests to OmniSEP, including TS.43 entitlement queries and XCAP operations.

Features:

- Filter by request type (XCAP, Entitlement Query, EAP Challenge, etc.)
- Search by IMSI, MSISDN, Terminal ID, or Client IP
- View HTTP method (GET, PUT, POST, DELETE) and response status
- Click any row to see detailed information

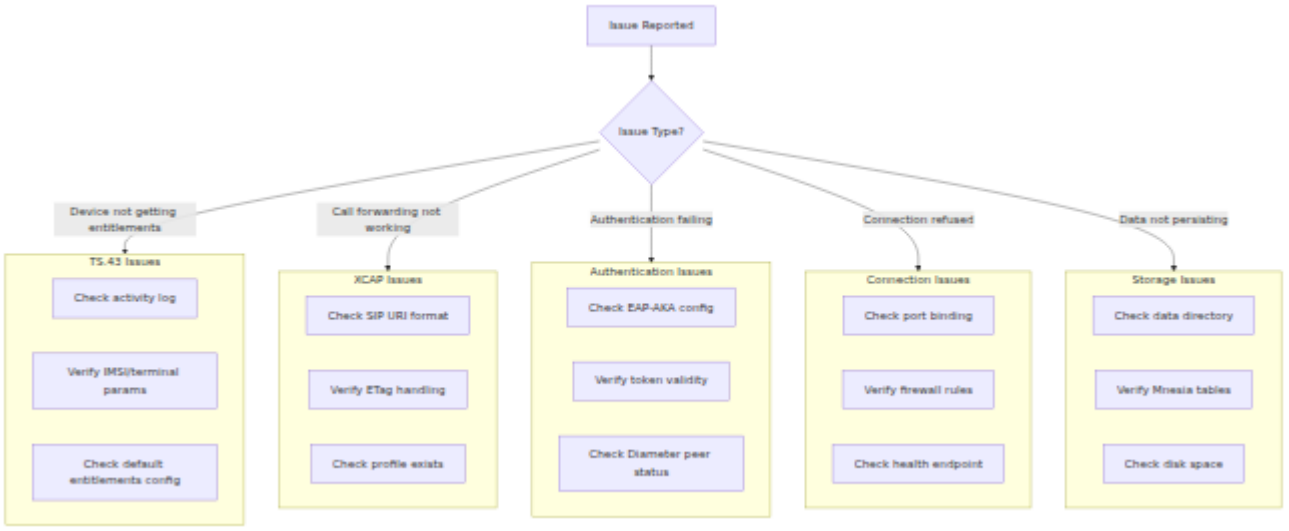
Activity Details Panel

Selecting an activity record shows comprehensive request/response details:

Captured Information:

- **Timestamp and Client IP**: When and where the request originated
- **Request Type and HTTP Method**: XCAP, entitlement query, etc.
- **Subscriber Info**: IMSI, MSISDN (when available)
- **Terminal Info**: Device ID, Vendor, Model (extracted from User-Agent)
- **Request Path**: Full XCAP path or entitlement endpoint
- **User-Agent**: Raw User-Agent header
- **Request Headers**: Content-Type, If-Match, 3GPP headers, etc.
- **Request/Response Body**: XML content for XCAP operations
- **Response Status**: Success, Server Error, Client Error with HTTP code

Diagnostic Workflow



TS.43 Entitlement Issues

Device Reports "Service Not Available"

Symptoms: Device shows VoWiFi/VoLTE as unavailable despite correct subscription

Possible causes:

- Default entitlements configured with `entitlement_status: 0`
- Custom entitlement set for subscriber with disabled status
- Device sending incorrect IMSI or terminal parameters

Resolution:

1. Check the activity log for the subscriber's requests:

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

2. Verify the entitlement response in activity records

3. Check default entitlements configuration:

```
config :omni_sep, :default_entitlements,
  vowifi: %{
    entitlement_status: 1,  # Should be 1 for enabled
    ...
  }
```

4. Check for custom entitlements overriding defaults:

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

Device Gets Wrong Entitlement Status

Symptoms: Device receives different entitlement values than expected

Possible causes:

- Custom entitlement configured for subscriber
- Wrong app_id being queried
- Configuration mismatch between environments

Resolution:

1. Verify which app_id the device is requesting (check activity log)

2. Common app IDs:

App ID	Service
ap2003	VoLTE/VoNR
ap2004	VoWiFi
ap2005	SMSoIP

3. Check custom entitlements:

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

4. Remove unwanted custom entitlement:

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

Missing Parameters in Request

Symptoms: HTTP 400 Bad Request with "Missing parameters" error

Possible causes:

- Device not sending required TS.43 parameters
- Parameters in wrong format
- URL encoding issues

Required parameters:

Parameter	Description
`terminal_id`	Device IMEI (15 digits)
`terminal_vendor`	Manufacturer (max 4 chars)
`terminal_model`	Model name (max 10 chars)
`terminal_sw_version`	Software version
`entitlement_version`	Protocol version (typically "2.0")
`app`	Application ID(s) to query

Resolution:

1. Check activity log for raw request details
2. Verify device is sending all required parameters

3. For Android, ensure User-Agent follows format:

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

Version Mismatch (HTTP 406)

Symptoms: Device receives HTTP 406 Not Acceptable

Possible causes:

- Device sending unsupported `entitlement_version`
- Server configured with incompatible version

Resolution:

1. Check server's configured version:

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

2. Android devices typically use version "2.0"

3. Ensure server version matches expected device version

XCAP Simservs Issues

Profile Not Found (HTTP 404)

Symptoms: XCAP GET request returns 404

Possible causes:

- Profile never created for subscriber
- Wrong SIP URI format
- MSISDN not linked to profile

Resolution:

1. Check SIP URI format in request:

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

2. Verify profile exists via management API:

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

3. Create profile if missing:

```
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": {}
}
```

ETag Mismatch (HTTP 412)

Symptoms: PUT or DELETE request returns HTTP 412 Precondition Failed

Possible causes:

- Client using stale ETag
- Concurrent modification by another client
- ETag not sent with conditional request

Resolution:

1. Fetch current document to get fresh ETag:

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

2. Use returned ETag in `If-Match` header:

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

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

3. For unconditional updates (testing only), omit `If-Match` header

Invalid XML (HTTP 400)

Symptoms: PUT request returns HTTP 400 Bad Request

Possible causes:

- Malformed XML in request body
- Missing required namespaces
- Invalid element structure

Required namespaces:

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

Resolution:

1. Validate XML structure

2. Ensure root element includes required namespaces:

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

3. Verify element names match ETSI TS 183 023 specification

Call Forwarding Not Activating

Symptoms: Call forwarding settings saved but calls not forwarded

Possible causes:

- Rule disabled in profile
- Wrong condition type
- Target number format incorrect

Resolution:

1. Verify `communication-diversion` is active:

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

2. Check rule is correctly structured:

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

3. Valid rule IDs and conditions:

Rule ID	Condition	Description
`cfu`	(none)	Unconditional
`cfb`	`busy`	On Busy
`cfna`	`no-answer`	On No Answer
`cfnrc`	`not-reachable`	Not Reachable
`cfnl`	`not-logged-in`	Not Logged In

4. Target must use `tel:` URI format with E.164 number

Authentication Issues

EAP-AKA Challenge Not Returned

Symptoms: Initial request with EAP_ID returns error instead of challenge

Possible causes:

- EAP-AKA disabled in configuration
- Invalid EAP_ID format
- Diameter peer connectivity issues

Resolution:

1. Verify EAP-AKA is enabled:

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

2. Check EAP_ID format (Root NAI):

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

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

3. If Diameter peers configured, check connectivity
4. If no peers configured, mock mode should accept any valid format

Token Invalid (HTTP 511)

Symptoms: Request with token returns HTTP 511 Network Authentication Required

Possible causes:

- Token expired
- Token signing secret changed
- Token was generated by different instance

Resolution:

1. Check token validity period:

   ```
   config :omni_sep, :token,
     validity_seconds: 86400  # 24 hours default
   ```

2. If secret was rotated, all existing tokens are invalidated
3. Device should fall back to EAP-AKA authentication to get new token
4. Verify all instances use same `signing_secret`

Token Signature Mismatch

Symptoms: Valid-looking token rejected

Possible causes:

- Token from different environment
- Signing secret mismatch between instances
- Token tampered

Resolution:

1. Ensure consistent `signing_secret` across all instances:

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

2. Use environment variable for secret in production

3. Rotate secrets across all instances simultaneously

Connectivity Issues

Service Not Reachable

Symptoms: Connection refused or timeout

Possible causes:

- Service not running
- Wrong port configuration
- Firewall blocking traffic

Resolution:

1. Check service health:

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

2. Verify port configuration:

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

3. Check firewall rules allow traffic on configured port
4. Verify service is listening:

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

Health Check Returns Unhealthy

Symptoms: `/health` endpoint returns non-200 status

Possible causes:

- Dependent service unavailable
- Storage tables not initialized
- Application startup incomplete
- Mnesia data directory not writable

Resolution:

1. Check application logs for startup errors
2. Verify storage initialization:
    - Mnesia tables (activity logging)
    - ETS tables (entitlements, tokens, sessions, XCAP profiles)
3. Check Mnesia data directory permissions:

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

4. If Mnesia fails to start, check for corrupted files and consider clearing the data directory

5. Restart application if tables missing

Slow Response Times

Symptoms: Requests taking longer than expected

Possible causes:

- Diameter peer timeouts
- Activity logging backlog
- High concurrent load

Resolution:

1. Check Diameter peer configuration:

   ```
   config :diameter_ex, :diameter,
     request_timeout: 5000  # 5 seconds default
   ```

2. Monitor activity log size per subscriber

3. Check ETS table memory usage

4. Consider horizontal scaling for high load

Storage Issues

Activity Log Not Persisting

Symptoms: Activity records lost after restart

Possible causes:

- Mnesia data directory not writable
- Application terminated before Mnesia could flush to disk
- Disk full

Resolution:

1. Verify data directory exists and is writable:

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

2. Check for Mnesia transaction logs (.DCL files) - these contain recent writes:

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

3. Ensure graceful shutdown to allow Mnesia to flush:

```
# Don't use kill -9, use SIGTERM instead
kill -TERM <pid>
```

4. Check disk space:

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

Mnesia Schema Corrupted

Symptoms: Application fails to start with Mnesia errors

Possible causes:

- Power loss or crash during write
- Disk corruption
- Mixed Erlang versions

Resolution:

1. Check logs for specific Mnesia error

2. If data can be lost, clear and reinitialize:

```
rm -rf priv/data/mnesia/*
# Restart application - tables will be recreated
```

3. If data must be preserved, try Mnesia repair:

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

Activity Log Growing Too Large

Symptoms: Disk usage increasing, slow queries

Possible causes:

- High request volume
- Retention period too long
- Per-subscriber limit too high

Resolution:

1. Check current retention settings:

```
config :omni_sep, :activity,
  max_records_per_subscriber: 1000,  # Reduce if needed
  retention_seconds: 2_592_000       # 30 days, reduce if
needed
```

2. Monitor table size:

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

3. Consider reducing retention period for high-volume deployments

Diagnostic Commands

Health Check

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

Expected response:

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

Activity Log Query

```
# Recent activity for subscriber
curl "http://localhost:9014/api/activity?imsi=<imsi>&limit=10"

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

# Activity in time range
curl "http://localhost:9014/api/activity?from=<unix_ts>&to=
<unix_ts>"
```

Entitlements Check

```
# Get custom entitlements
curl http://localhost:9014/api/entitlements/<imsi>

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

XCAP Profile Check

```
# Get profile
curl http://localhost:9014/api/xcap/<msisdn>

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

Log Analysis

Key Log Patterns

Pattern	Meaning
`[info] GET / ...`	Incoming entitlement request
`[info] POST / ...`	Incoming POST request (EAP or entitlement)
`[warning] Missing parameters`	Request validation failed
`[error] EAP session timeout`	EAP-AKA not completed in time
`[debug] Token validated`	Successful token authentication

Enabling Debug Logging

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

Reference Specifications

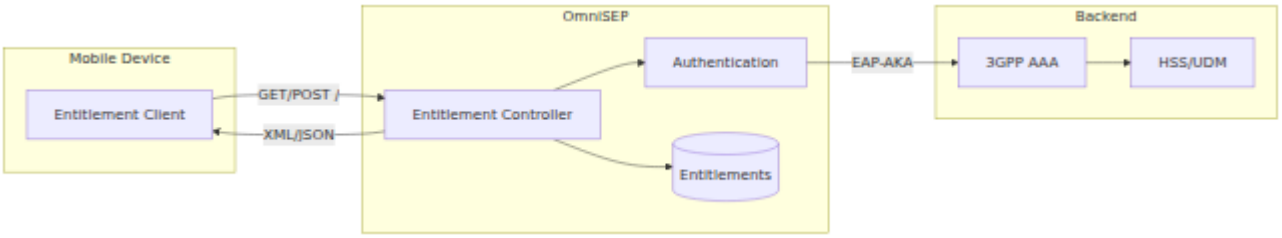
For protocol-specific troubleshooting, refer to:

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

TS.43 Entitlement Configuration

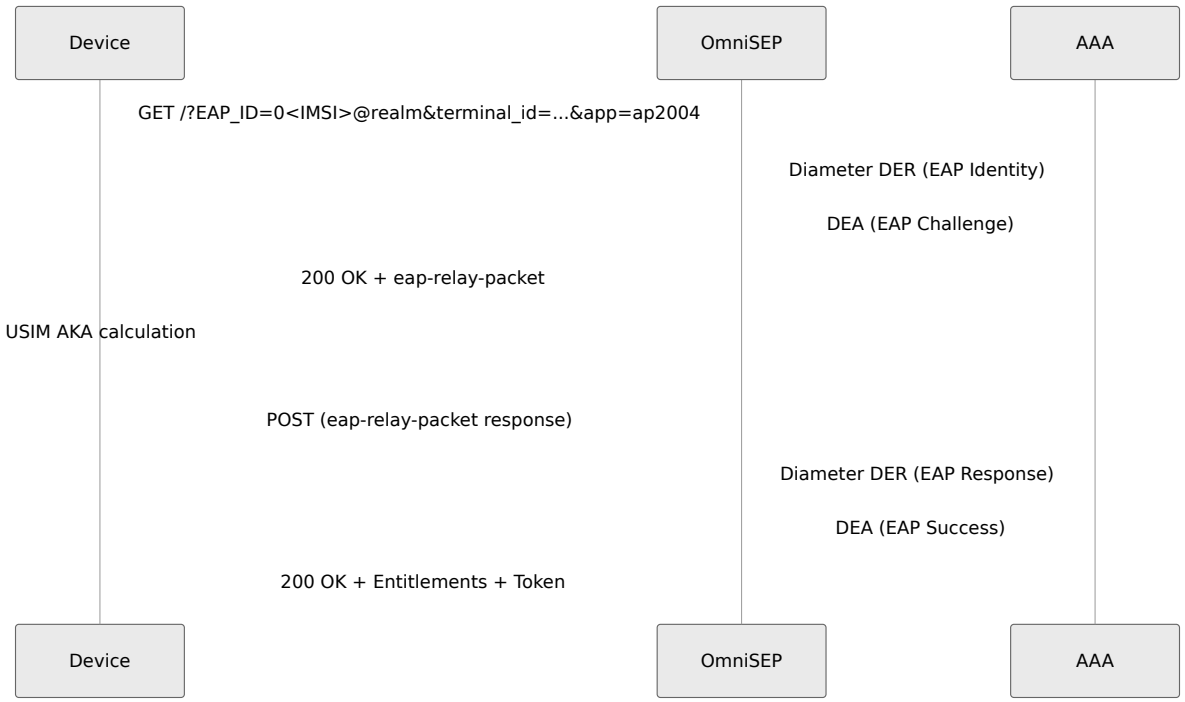
OmniSEP implements GSMA TS.43 Service Entitlement Configuration, enabling mobile devices to query their service entitlements (VoWiFi, VoLTE, SMS, etc.) from the carrier network.

Overview

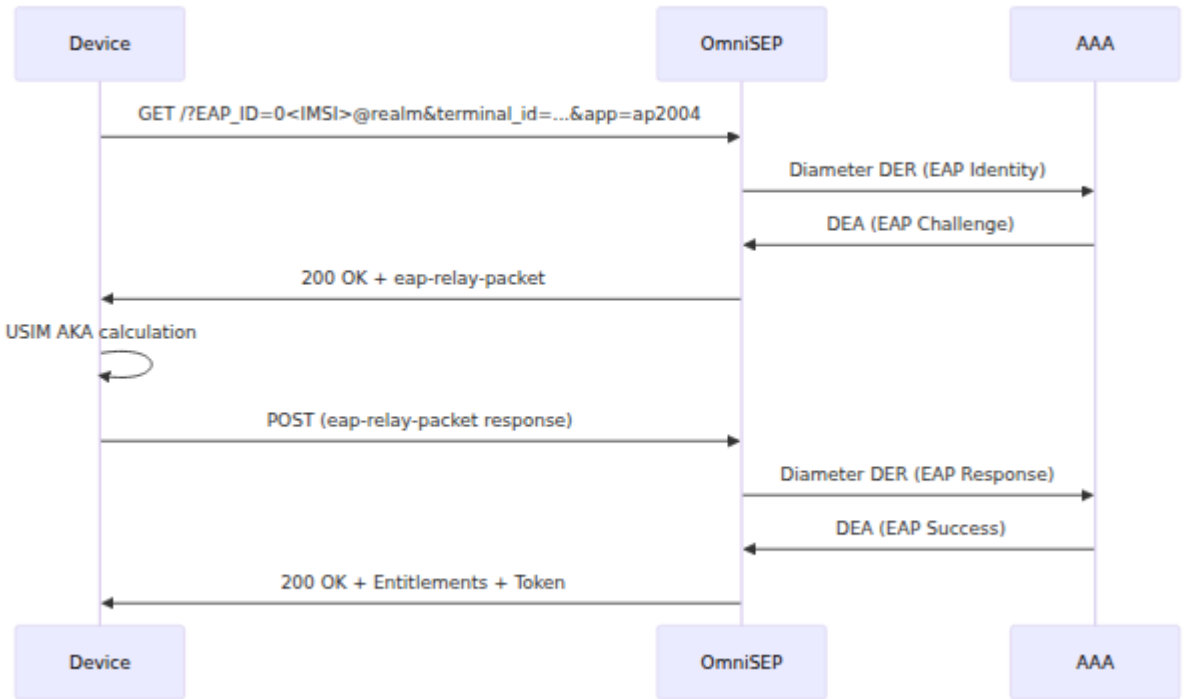


Request Flow

Initial Authentication (EAP-AKA)



Fast Re-Authentication (Token)



HTTP Interface

Endpoint

Method	Path	Content-Type
GET	`/`	Query parameters
POST	`/`	`application/json`

Required Parameters

Parameter	Type	Description
`terminal_id`	String	Device IMEI (15 digits)
`terminal_vendor`	String	Device manufacturer (max 4 chars per RCC.14)
`terminal_model`	String	Device model (max 10 chars per RCC.14)
`terminal_sw_version`	String	Software version (max 20 chars per RCC.14)
`entitlement_version`	String	Protocol version (e.g., "2.0")
`app`	String/List	Application ID(s) to query

Authentication Parameters

One of these authentication methods is required:

Parameter	Description
`EAP_ID`	Root NAI for EAP-AKA: `0<IMSI>@nai.epc.mnc<MNC>.mcc<MCC>.3gppnetv`
`token`	Authentication token from previous response
`temporary_token`	Temporary token
`operator_token`	Operator-issued token

Optional Parameters

Parameter	Type	Description
`IMSI`	String	Required with `token` for fast re-auth
`app_name`	String	Application name
`app_version`	String	Application version
`notif_action`	Integer	Notification action (0=disable, 1=GCM, 2=FCM)
`notif_token`	String	Push notification token
`vers`	Integer	Configuration version for change detection

Request Examples

GET with Token:

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

POST with 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"
}
```


Response Formats

Accept Header

Accept Header	Response Format
`text/vnd.wap.connectivity-xml`	XML (default)
`application/json`	JSON
`application/vnd.gsma.eap-relay.v1.0+json`	EAP relay JSON

XML Response

```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>
```

JSON Response


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


EAP Challenge Response

When EAP-AKA authentication is in progress:


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

Application IDs

Supported Applications

App ID	Service	Reference
ap2003	Voice-over-Cellular (VoLTE/VoNR)	TS.43 Section 4
ap2004	Voice-over-WiFi (VoWiFi)	TS.43 Section 3
ap2005	SMS-over-IP	TS.43 Section 5
ap2006	ODSA Companion	TS.43 Section 6
ap2009	ODSA Primary	TS.43 Section 6
ap2010	Data Plan Boost	TS.43 Section 7
ap2011	Server Initiated Requests	TS.43 Section 8
ap2012	Direct Carrier Billing	TS.43 Section 9
ap2013	Private User Identity	TS.43 Section 10
ap2014	Phone Number Information	TS.43 Section 11
ap2016	Satellite Entitlement	TS.43 Section 12

VoWiFi (ap2004) Response Fields

Field	Type	Values	Description
`EntitlementStatus`	Integer	0-3	Service availability
`AddrStatus`	Integer	0-3	E911 address verification status
`TC_Status`	Integer	0-3	Terms & Conditions status
`ProvStatus`	Integer	0-3	Provisioning status
`ServiceFlow_URL`	String	URL	Service flow URL
`ServiceFlow_UserData`	String	-	Data for service flow

Status Values:

Value	EntitlementStatus	AddrStatus/TC_Status/ProvStatus
0	Disabled	Not Available
1	Enabled	Available
2	Incompatible	Not Required
3	Provisioning	In Progress

VoLTE (ap2003) Response Fields

VoLTE uses an array of entries per access technology:

Field	Type	Values	Description
`AccessType`	Integer	1=LTE, 2=NR	Radio access technology
`HomeRoamingNWType`	Integer	1-3	Network scope
`EntitlementStatus`	Integer	0-1	Service availability
`NetworkVoiceIRATCapability`	String	-	Voice capability (5G only)

HomeRoamingNWType Values:

Value	Meaning
1	Home and Roaming
2	Home Only
3	Roaming Only

Error Responses

HTTP Status	Meaning	Description
400	Bad Request	Missing required parameters
403	Forbidden	Authentication failed
406	Not Acceptable	Unsupported protocol version
511	Network Authentication Required	Token invalid or EAP-AKA required

Error Response Format

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

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

Custom Entitlements

Setting Custom Entitlements

Use the management API to set custom entitlements for specific subscribers:

```
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 requires address
verification"
  }
}
```

Retrieving Entitlements

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

Returns all custom entitlements for the subscriber:

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

Activity Logging

All entitlement requests are logged for audit purposes.

Searching Activity

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

Parameter	Type	Description
`imsi`	String	Filter by subscriber IMSI
`terminal_id`	String	Filter by device terminal ID
`from`	Integer	Start timestamp (Unix epoch)
`to`	Integer	End timestamp (Unix epoch)
`limit`	Integer	Maximum records to return
`offset`	Integer	Pagination offset

Activity Record


```
{
  "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
}
```

Android Client Compatibility

OmniSEP is tested against the Android AOSP `service_entitlement` library.

User-Agent Format

Android devices use this User-Agent format:

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

Example:

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

Multiple App IDs

Android sends multiple app IDs in POST requests as a bracket-enclosed string:

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

OmniSEP parses both formats:

- `"ap2003,ap2004"` - Comma-separated
- `"[ap2003,ap2004]"` - Bracket-enclosed (Android format)
- `["ap2003", "ap2004"]` - JSON array

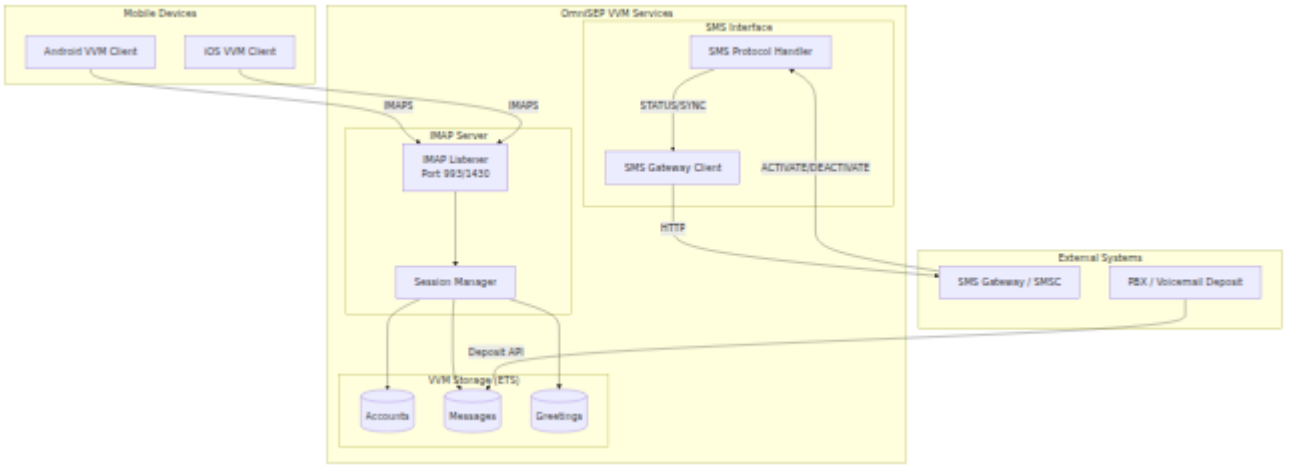
Reference Specifications

Specification	Description
GSMA TS.43	Service Entitlement Configuration
GSMA RCC.14	IMS Device Configuration Guidelines
3GPP TS 33.220	Generic Bootstrapping Architecture (GBA)
3GPP TS 29.273	EPS AAA Interfaces (SWm)

Visual Voicemail (VVM)

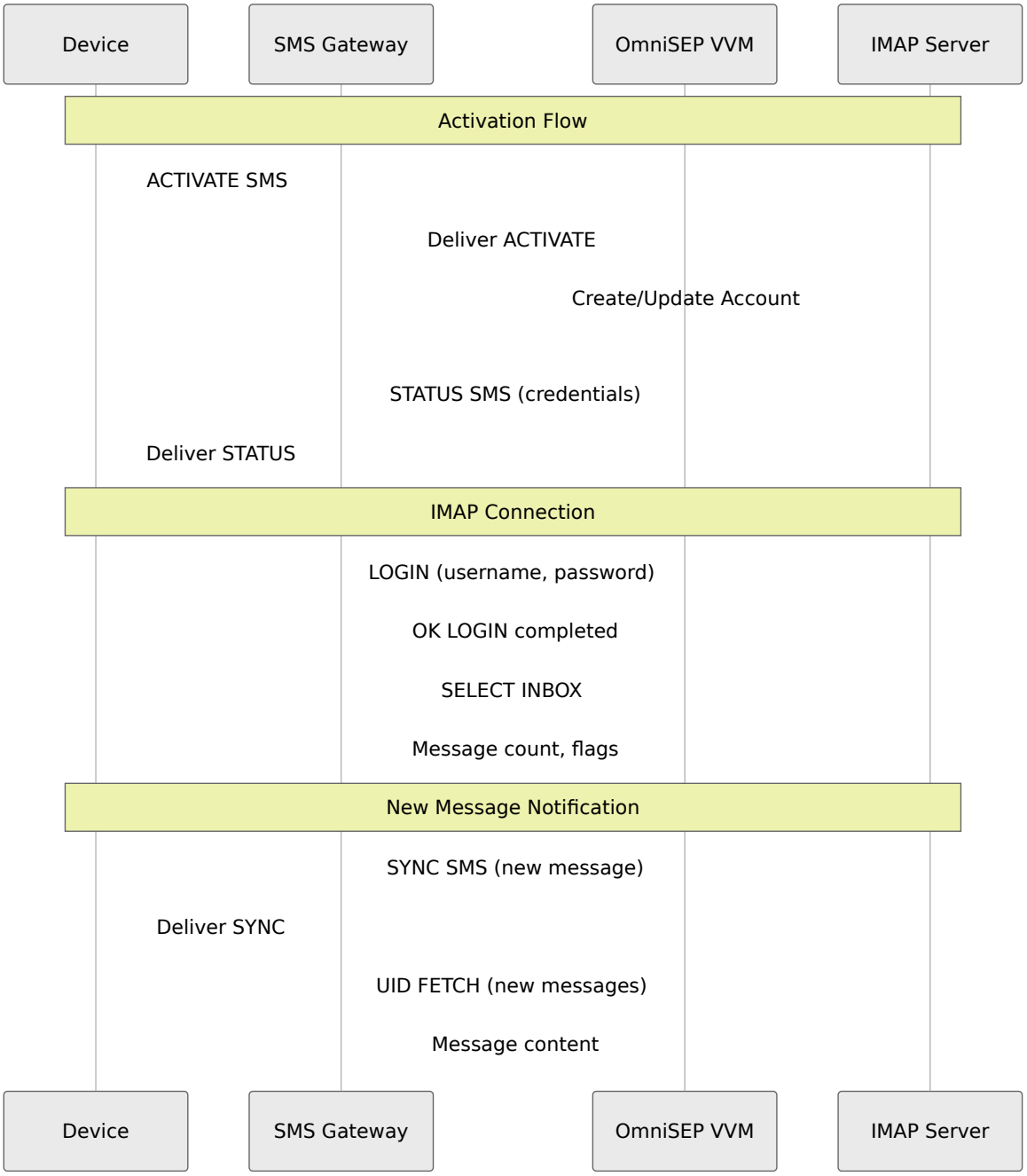
OmniSEP provides a Visual Voicemail server implementing the OMTP VVM Specification v1.3 and GSMA TS.46. The VVM service enables smartphones to manage voicemail messages through an IMAP interface, with provisioning handled via SMS.

Architecture Overview



Provisioning Flow

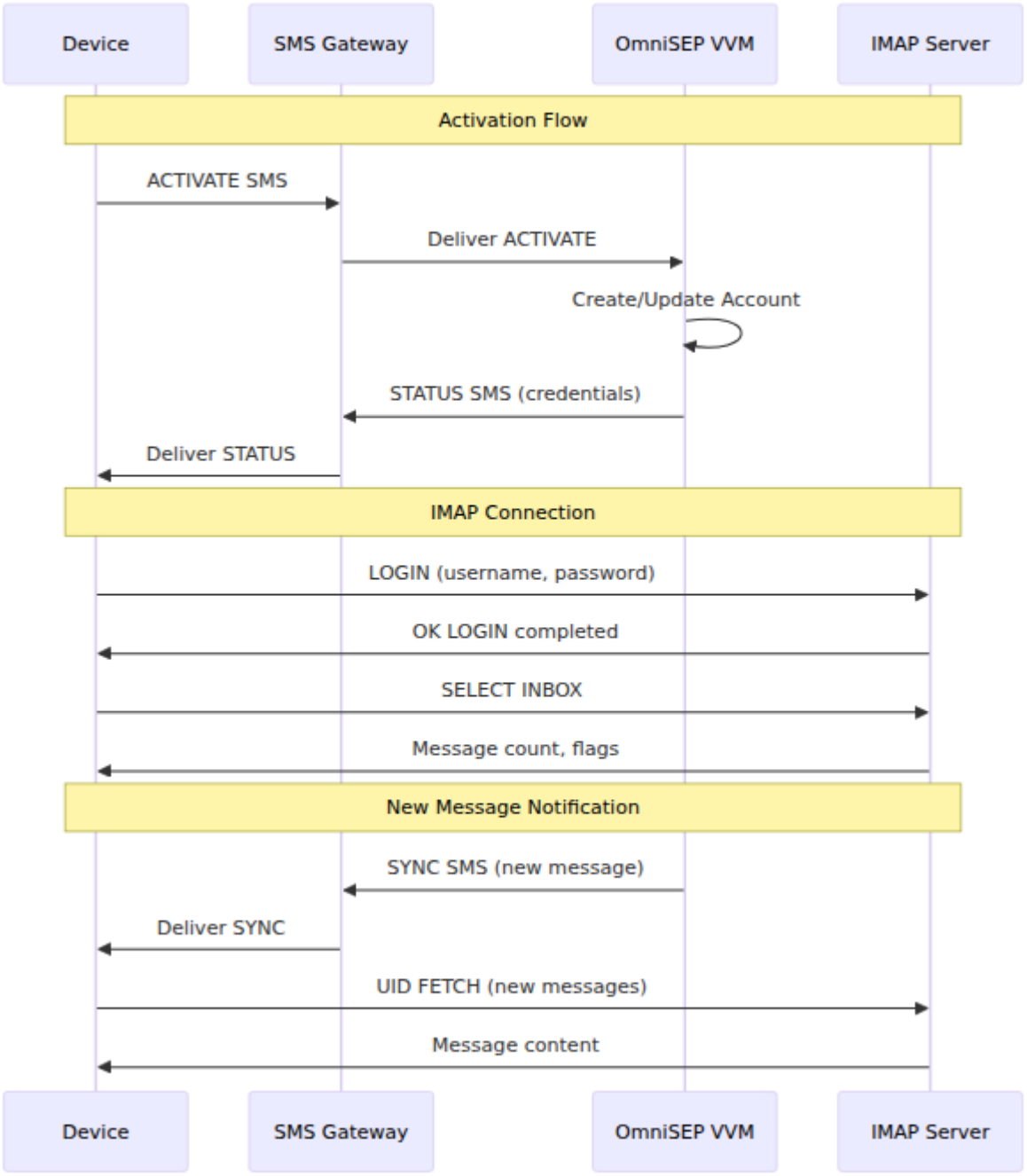
VVM provisioning follows the OMTP specification state machine. When a device activates VVM, it sends an ACTIVATE SMS, receives credentials via STATUS SMS, then connects via IMAP.



Provisioning States

The VVM service tracks subscriber provisioning state per the OMTP specification:

State	Code	Description
Unknown	U	Initial state, no provisioning attempted
New	N	Account created, awaiting first client connection
Ready	R	Fully provisioned and operational
Provisioned	P	Credentials sent, awaiting client verification
Blocked	B	Service deactivated or suspended



SMS Protocol

STATUS Message (Server to Client)

Sent after activation to provide IMAP credentials:

```
//VVM:STATUS:st=R;rc=0;srv=vvm.example.com;ipt=993;spt=587;u=5050100
15;pm=N;gm=N;vtc=A
```

Field	Description
`st`	Provisioning state (R=Ready, B=Blocked, N=New, P=Provisioned, U=Unknown)
`rc`	Return code (0=success)
`srv`	IMAP server hostname
`ipt`	IMAP port
`spt`	SMTP port (if applicable)
`u`	Username (IMSI-based)
`pw`	Password
`tui`	TUI access number
`dn`	SMS destination number (for client replies)
`lang`	Language code
`g_len`	Maximum greeting length in seconds
`vs_len`	Maximum voice signature length in seconds
`pw_len`	PIN length range
`pm`	PIN required (Y/N)
`gm`	Greeting reset mode (G=greeting, V=voice signature, B=both, N=none)
`vtc`	Transcription capability (A=automatic, D=on-demand, B=both, N=none)

SYNC Message (Server to Client)

Sent when mailbox content changes:

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

Field	Description
`ev`	Event type (NM=new message, MBU=mailbox update, GU=greeting update)
`id`	Message ID
`c`	Unread message count
`t`	Message type (v=voice, o=video, f=fax, i=infotainment, e=ECC)
`s`	Sender number
`dt`	Deposit timestamp
`l`	Message length in seconds

ACTIVATE Message (Client to Server)

Sent by device to enable VVM:

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

Field	Description
`pv`	Protocol version
`ct`	Client type (vendor.model.os_version)

DEACTIVATE Message (Client to Server)

Sent by device to disable VVM:

```
Deactivate:pv=11
```

IMAP Server

The VVM IMAP server implements a subset of IMAP4rev1 (RFC 3501) tailored for voicemail:

Supported Commands

Command	Description
CAPABILITY	List server capabilities
LOGIN	Authenticate with username/password
LOGOUT	End session
SELECT	Open mailbox (INBOX, Trash, Saved)
EXAMINE	Open mailbox read-only
LIST	List available mailboxes
STATUS	Get mailbox status (message counts)
FETCH	Retrieve message content
UID FETCH	Retrieve by UID
STORE	Update message flags
UID STORE	Update flags by UID
SEARCH	Search messages
UID SEARCH	Search by UID
COPY	Copy messages between mailboxes
EXPUNGE	Permanently delete flagged messages
CLOSE	Close mailbox and expunge
GETQUOTAROOT	Get storage quota

Command	Description
NOOP	Keep-alive

Capabilities

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

Mailbox Structure

Mailbox	Description
INBOX	New and read voicemail messages
Trash	Messages marked for deletion
Saved	Archived messages

Message Format

Voicemail messages are presented as RFC 5322 email with multipart MIME structure:

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

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

Voicemail from: +61400123456
Duration: 30 seconds

Transcription:
Hello, this is a test voicemail message.

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

[Base64 encoded audio]
------=_Part_0--
```

Custom Headers

Header	Description
`X-VVM-MsgType`	Message type (voice, video, fax, infotainment, ecc)
`X-VVM-Duration`	Message duration in seconds
`X-VVM-Sender`	Original caller number

Configuration

Enabling VVM

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

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

  # TUI (Traditional User Interface) number
  tui_number: "*86",

  # SMS settings
  sms_source_number: "+61400000000",
  sms_gateway: "https://sms-gateway.example.com/api/send",

  # PIN settings
  min_pin_length: 4,
  max_pin_length: 15,

  # Subscriber limits
  default_max_messages: 100,
  default_storage_limit_kb: 50_000,
  default_max_greeting_seconds: 60
```

Configuration Parameters

Parameter	Type	Required	Default
`enabled`	Boolean	No	false
`imap_port`	Integer	No	993
`imap_ssl`	Boolean	No	true
`imap_server`	String	Yes	-
`imap_cert`	String	No	priv/cert/server.crt
`imap_key`	String	No	priv/cert/server.key
`smtp_port`	Integer	No	587
`tui_number`	String	No	*86
`sms_source_number`	String	Yes	-

Parameter	Type	Required	Default
`sms_gateway`	String	No	nil
`min_pin_length`	Integer	No	4
`max_pin_length`	Integer	No	15
`default_max_messages`	Integer	No	100
`default_storage_limit_kb`	Integer	No	50000
`default_max_greeting_seconds`	Integer	No	60

Development Configuration

For development, use plain IMAP (no TLS) for easier testing:

```
# 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"
```

Production Configuration

```
# 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://smsc.carrier.example.com/api/v1/send"
```

Metrics

IMAP Session Metrics

Metric: `vvm_imap_sessions_total` **Type**: Counter **Description**: Total number of VVM IMAP sessions **Labels**:

- `result` - Session outcome: `success`, `auth_failed`, `timeout`

Metric: `vvm_imap_active_sessions` **Type**: Gauge **Description**: Number of currently active IMAP sessions

Metric: `vvm_imap_commands_total` **Type**: Counter **Description**: Total IMAP commands processed **Labels**:

- `command` - IMAP command: `LOGIN`, `SELECT`, `FETCH`, etc.
- `result` - Command result: `ok`, `no`, `bad`

Message Metrics

Metric: `vvm_messages_total` **Type**: Counter **Description**: Total VVM message operations **Labels**:

- `operation` - Operation type: `deposit`, `read`, `delete`, `move`

Metric: `vvm_messages_stored` **Type**: Gauge **Description**: Total number of voicemail messages currently stored

Metric: `vvm_message_duration_seconds` **Type**: Histogram **Description**: Duration of voicemail messages in seconds **Buckets**: 5, 10, 15, 30, 60, 120, 180, 300

SMS Metrics

Metric: `vvm_sms_total` **Type**: Counter **Description**: Total VVM SMS messages **Labels**:

- `type` - SMS type: `status`, `sync`, `activate`, `deactivate`
- `result` - Delivery result: `success`, `failed`, `no_gateway`

Account Metrics

Metric: `vvm_accounts_total` **Type**: Counter **Description**: VVM account operations **Labels**:

- `operation` - Operation: `create`, `activate`, `deactivate`, `update`
- `result` - Result: `success`, `error`

Metric: `vvm_accounts_active` **Type**: Gauge **Description**: Number of active VVM accounts

Example Prometheus Queries

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

# Authentication failure rate
sum(rate(vvm_imap_sessions_total{result="auth_failed"}[5m]))
  / sum(rate(vvm_imap_sessions_total[5m]))

# Average message duration
histogram_quantile(0.5,
rate(vvm_message_duration_seconds_bucket[5m]))

# SMS delivery success rate
sum(rate(vvm_sms_total{result="success"}[5m]))
  / sum(rate(vvm_sms_total[5m]))

# Active sessions over time
vvm_imap_active_sessions
```

Greeting Management

VVM supports multiple greeting types per subscriber:

Greeting Type	Description
`normal`	Standard personal greeting
`busy`	Played when subscriber is busy
`extended_absence`	Vacation or out-of-office greeting
`voice_signature`	Voice signature for name announcement

Greetings are stored and retrieved via the storage API. The IMAP server includes greeting metadata in the account quota response.

Troubleshooting

Client Cannot Activate VVM

Symptoms: Device shows "Visual Voicemail unavailable" or activation fails

Possible causes:

- SMS gateway not configured or unreachable
- Source number not whitelisted at SMSC
- VVM service disabled in configuration

Resolution:

1. Verify `sms_gateway` is configured and reachable
2. Check SMS gateway logs for delivery status
3. Confirm `enabled: true` in VVM configuration
4. Review metrics: `vvm_sms_total{type="status"}`

IMAP Authentication Failures

Symptoms: Client cannot connect after receiving STATUS SMS

Possible causes:

- Username/password mismatch
- TLS certificate issues
- Firewall blocking IMAP port

Resolution:

1. Verify credentials match between STATUS SMS and account storage
2. Check TLS certificate validity and trust chain
3. Confirm firewall allows traffic on configured IMAP port
4. Test with telnet/openssl: `openssl s_client -connect vvm.example.com:993`

Messages Not Syncing

Symptoms: New voicemails not appearing on device

Possible causes:

- SYNC SMS not being sent
- IMAP session disconnected
- Message deposit failing

Resolution:

1. Check `vvm_sms_total{type="sync"}` metrics
2. Verify SMS gateway connectivity
3. Check `vvm_messages_total{operation="deposit"}` for deposit failures
4. Review IMAP session metrics for disconnections

High Storage Usage

Symptoms: Subscribers hitting quota limits

Resolution:

1. Review quota settings: `default_storage_limit_kb`, `default_max_messages`
2. Check `vvm_messages_stored` gauge
3. Consider implementing automatic message expiration
4. Review greeting storage: `get_greetings/1` returns audio sizes

References

- OMTP VVM Specification v1.3 - Visual Voicemail Interface Specification
- GSMA TS.46 - Visual Voicemail Interface Specification
- RFC 3501 - IMAP4rev1 Protocol
- RFC 5322 - Internet Message Format

XCAP Supplementary Services (Simservs)

OmniSEP implements ETSI TS 183 023 XCAP (XML Configuration Access Protocol) for managing IMS supplementary services including call forwarding, call barring, and caller ID settings.

Control Panel UI

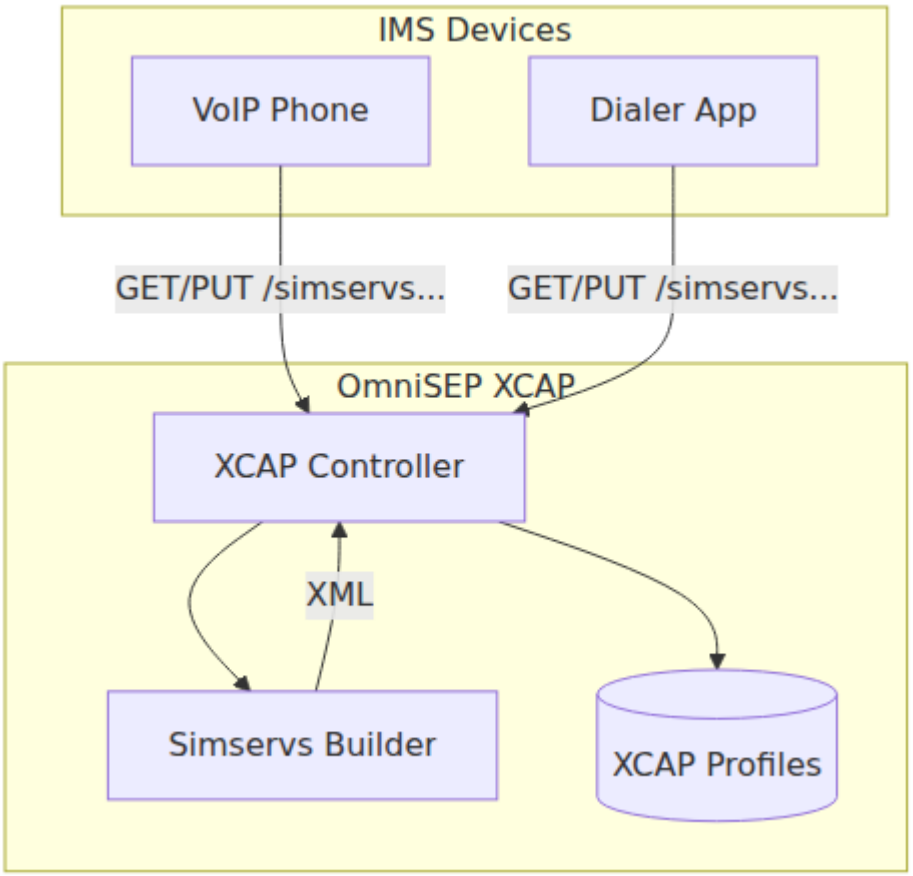
The XCAP Simservs Profiles page provides a web-based interface for viewing and managing subscriber profiles:

Features:

- Search and filter local profiles by MSISDN
- Fetch profiles from HSS using Diameter Sh interface
- View profile details in a 2-column layout:
  - **Left column**: Identity Services (OIP/OIR), Other Services (Call Waiting, Call Hold), Call Forwarding rules

    - **Right column**: Incoming and Outgoing Call Barring rules with conditions
- Push/Pull synchronization with HSS
- Edit mode for modifying profile settings

Overview



Simservs Document Structure

The simservs document follows ETSI TS 183 023 structure:

HTTP Interface

XCAP URL Format

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

Component	Description	Example
`{sip_uri}`	SIP URI with MSISDN	`sip:+15551234567@ims.example.com`
`{xpath}`	XPath selector (optional)	`simservs/communication-diversion`

Operations

Method	Path
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/~~/simservs`
PUT	`/simservs.ngn.etsi.org/users/{sip}/simservs.xml/~~/simservs`
DELETE	`/simservs.ngn.etsi.org/users/{sip}/simservs.xml/~~/simservs`

Content Types

Content-Type	Usage
`application/xcap-el+xml`	XCAP element operations
`application/xml`	Standard XML

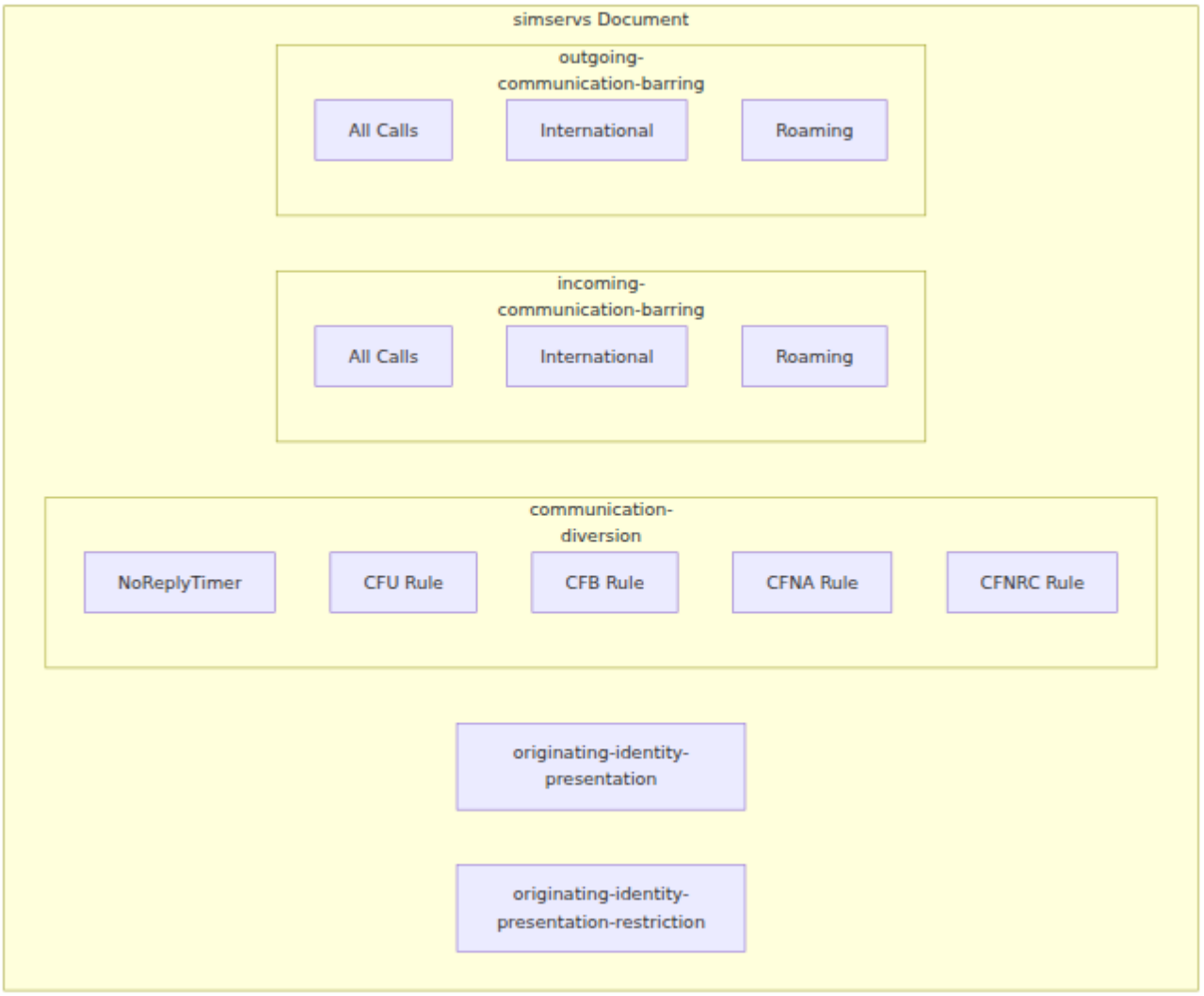
ETag Support

OmniSEP implements RFC 4825 ETag-based concurrency control:

Header	Usage
`ETag`	Response header with document version
`If-Match`	Conditional update (PUT/DELETE)
`If-None-Match`	Conditional GET (304 Not Modified)

Caching Architecture

OmniSEP uses a local-first caching strategy with ETS-based storage and asynchronous HSS synchronization.



Storage Tables

Table	Key	Value	Purpose
`xcap_profiles`	IMSI	`{profile_map, etag}`	Primary profile storage
`xcap_by_msisdn`	MSISDN	IMSI	Lookup index for XCAP requests

Caching Strategy

Read Operations (GET)

1. Query local ETS cache first
2. On cache miss, fetch from HSS via Diameter Sh
3. Seed local cache with HSS response
4. Return default profile if HSS unavailable or no profile exists

Write Operations (PUT)

1. Validate ETag precondition against cached value
2. Update local cache immediately
3. Return response to client with new ETag
4. Asynchronously push changes to HSS (non-blocking)

ETag Generation

ETags are computed as MD5 hashes of the profile data:

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

Example: `"a1b2c3d4e5f6g7h8"`

The 16-character hex string changes whenever any profile field is modified, enabling precise cache invalidation.

Concurrency Control

Mechanism	Purpose
ETS read_concurrency	Fast parallel reads without locking
GenServer writes	Atomic write operations
ETag validation	Prevents lost updates from concurrent clients

Default Profile

Unknown subscribers automatically receive a default profile per 3GPP TS 24.623:

- All supplementary services active
- OIR default: `presentation-not-restricted`
- NoReplyTimer: 20 seconds
- Empty call forwarding/barring rulesets

This ensures devices always receive a valid response without requiring pre-provisioning.

HSS Integration

Operation	Diameter Command	Timing
Fetch profile	Sh UDR (User-Data-Request)	Synchronous on cache miss
Push changes	Sh PUR (Profile-Update-Request)	Asynchronous after PUT

The asynchronous push means HSS updates don't block client responses, improving latency for device requests.

Simservs XML Document

Full Document Example

```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>
```

Namespaces

Prefix	Namespace	Descrip
(default)	`http://uri.etsi.org/ngn/params/xml/simservs/xcap`	ETSI Simservs
cp	`urn:ietf:params:xml:ns:common-policy`	RFC 474 Commor Policy

Services

Originating Identity Presentation (OIP)

Controls whether caller ID is displayed to called party.

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

Attribute	Type	Description
`active`	Boolean	Service enabled/disabled

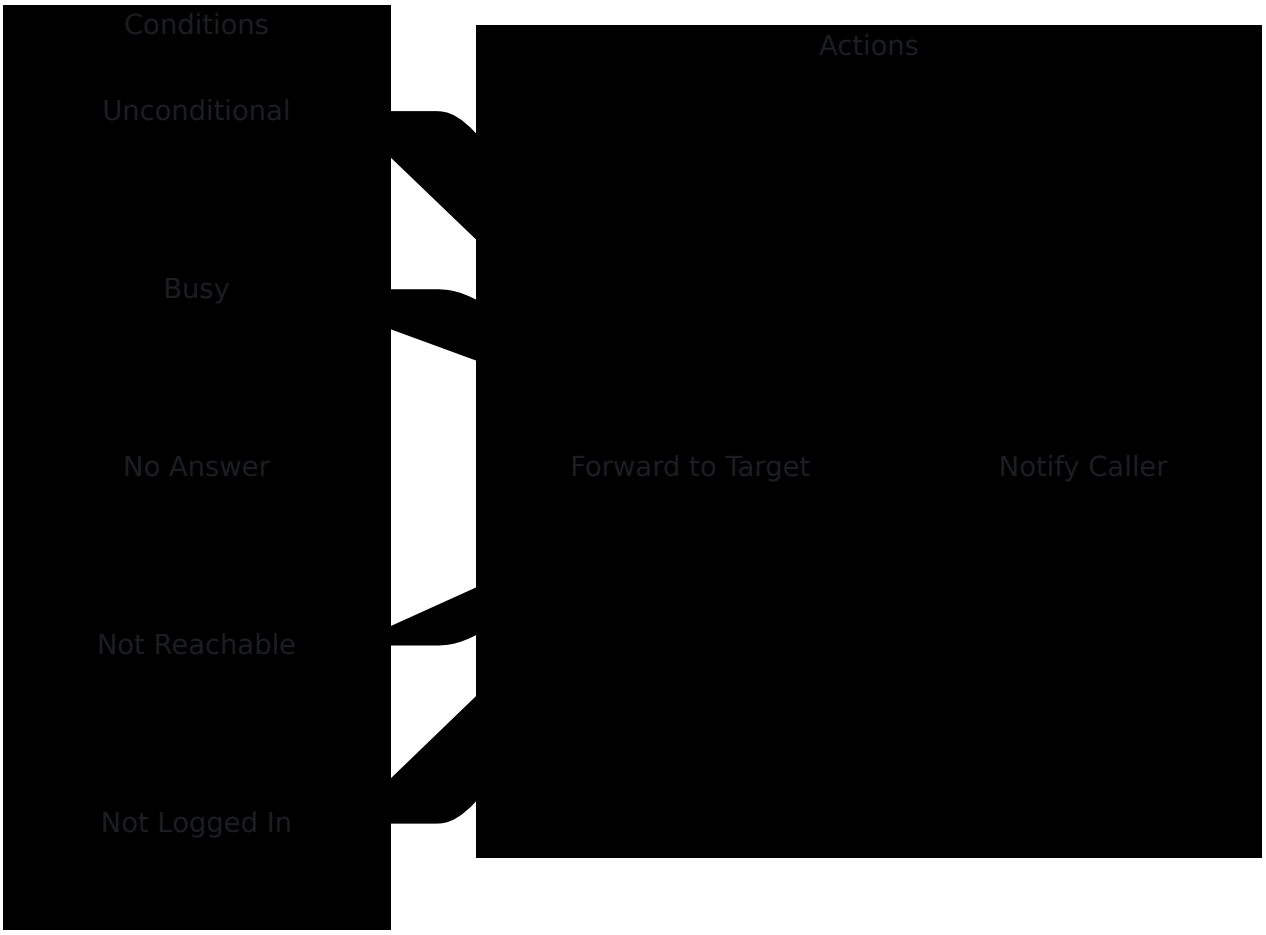
Originating Identity Presentation Restriction (OIR)

Controls caller ID hiding.

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

Element	Values	Description
`default-behaviour`	`presentation-restricted`, `presentation-not-restricted`	Default caller ID behavior

Communication Diversion (Call Forwarding)



Rule Types

Rule ID	Condition	Description
`cfu`	(none)	Call Forwarding Unconditional - forwards all calls immediately
`cfb`	`busy`	Call Forwarding on Busy
`cfna`	`no-answer`	Call Forwarding on No Answer (uses NoReplyTimer)
`cfnrc`	`not-reachable`	Call Forwarding on Not Reachable
`cfnl`	`not-logged-in`	Call Forwarding on Not Logged In

Call Forwarding Rule Structure

```
<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>
```

Element	Type	Description
`NoReplyTimer`	Integer	Seconds to wait before CFNA (1-300)
`cp:rule/@id`	String	Rule identifier (cfu, cfb, cfna, cfnrc, cfnl)
`target`	tel: URI	Forward destination number
`notify-caller`	Boolean	Play announcement to caller

Target URI Format

Forward targets use tel: URI format per RFC 3966:

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

Component	Description
`tel:`	URI scheme
`+15557654321`	E.164 number with country code
`phone-context`	IMS domain (optional)

Call Barring

Incoming Communication Barring

```
<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>
```

Outgoing Communication Barring

```
<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>
```

Barring Rule Types

Rule ID	Condition	Description
`all`	(none)	Bar all calls
`international`	`international`	Bar international calls
`international-exHC`	`international-exHC`	Bar international except home country
`roaming`	`roaming`	Bar calls while roaming

API Examples

Get Full Simservs Document

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

Response:

```
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>
```

Get Call Forwarding Settings

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

Enable Call Forwarding on Busy

```
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>
```

Disable Call Forwarding Rule

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

Update NoReplyTimer

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

25
```

Management API

For administrative access, use the JSON management API:

Get Profile

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

Response:

```
{
  "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": {}
}
```

Set Profile

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

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

Default Profile

New subscribers receive this default profile:

Setting	Default
OIP	Active
OIR	Active, presentation-not-restricted
NoReplyTimer	20 seconds
Call Forwarding	All rules disabled
Call Barring (Incoming)	All calls allowed
Call Barring (Outgoing)	All calls allowed

Error Responses

HTTP Status	Description
200	Success
304	Not Modified (If-None-Match matched)
400	Bad Request - Invalid XML or path
404	Not Found - Document or element not found
405	Method Not Allowed
409	Conflict - Constraint violation
412	Precondition Failed - ETag mismatch

Error Response Format

```
<?xml version="1.0" encoding="UTF-8"?>
<xcap-error xmlns="urn:ietf:params:xml:ns:xcap-error">
  <error-element>Element not found: simservs/unknown</error-
element>
</xcap-error>
```

Reference Specifications

Specification	Description
ETSI TS 183 023	XCAP framework for NGN Simservs
ETSI TS 183 004	Communication Diversion (CDIV)
RFC 4825	XCAP Protocol
RFC 4745	Common Policy
RFC 3966	tel: URI
3GPP TS 24.623	XCAP over Ut interface

OmniSEP - Service Endpoint Platform

OmniSEP is a unified service endpoint platform providing carrier-grade implementations of mobile device provisioning protocols. It handles TS.43 Entitlement Configuration, XCAP Supplementary Services, and Visual Voicemail from a single platform.

Quick Links

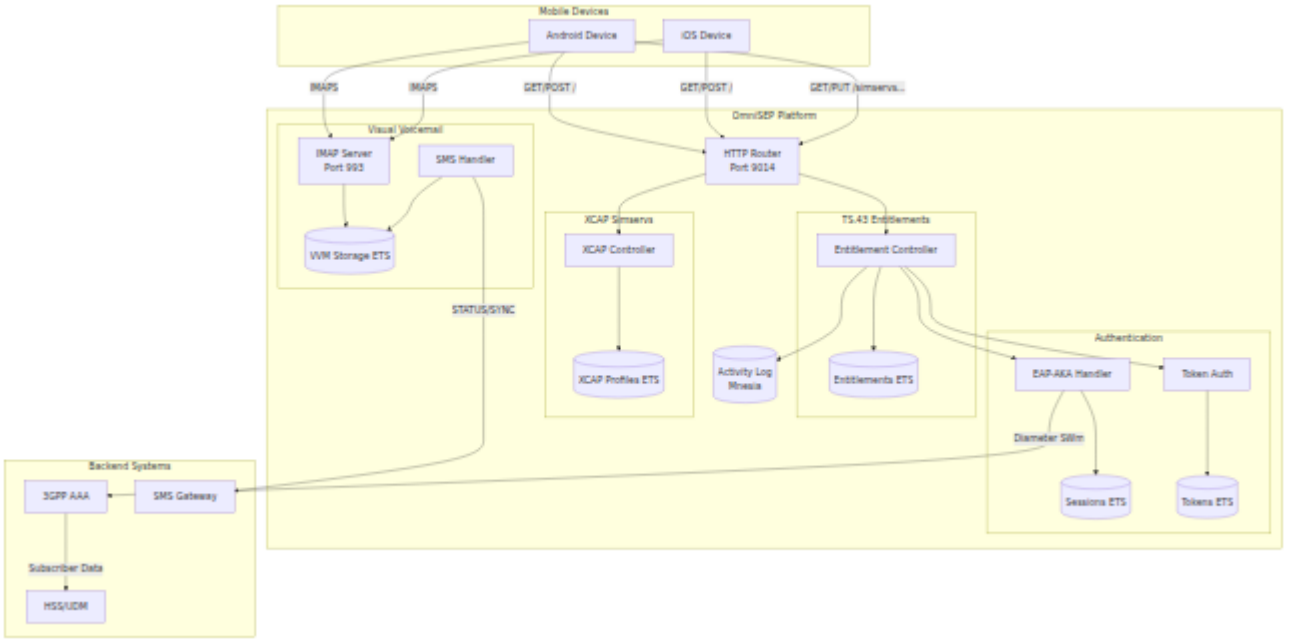
Operations & Monitoring

- **Configuration Reference** - Complete parameter documentation for all services
- **Troubleshooting** - Common issues and resolutions

Service Documentation

- **TS.43 Entitlements** - GSMA TS.43 Service Entitlement Configuration
- **XCAP Simservs** - ETSI TS 183 023 Supplementary Services (Call Forwarding, Call Barring, Caller ID)
- **Visual Voicemail** - OMTP VVM v1.3 / GSMA TS.46 Visual Voicemail Server

Architecture Overview



Supported Services

TS.43 Entitlement Configuration

Implements GSMA TS.43 for device service entitlement queries:

App ID	Service	Description
ap2003	Voice-over-Cellular	VoLTE/VoNR entitlement status
ap2004	VoWiFi	Voice over WiFi calling entitlement
ap2005	SMSoIP	SMS over IP entitlement
ap2006	ODSA Companion	On-Device Service Activation (companion)
ap2009	ODSA Primary	On-Device Service Activation (primary)
ap2010	Data Plan Boost	Data plan information
ap2012	Direct Carrier Billing	DCB service status
ap2016	Satellite Mode	Satellite connectivity entitlement

XCAP Supplementary Services

Implements ETSI TS 183 023 for IMS supplementary service configuration:

Service	Description	Reference
Communication Diversion	Call forwarding (CFU, CFB, CFNA, CFNRC)	ETSI TS 183 004
Incoming Call Barring	Block incoming calls by type	ETSI TS 183 023
Outgoing Call Barring	Block outgoing calls by type	ETSI TS 183 023
OIP/OIR	Caller ID presentation and restriction	ETSI TS 183 023

Visual Voicemail

Implements OMTP VVM Specification v1.3 and GSMA TS.46:

Component	Description	Reference
IMAP Server	Message retrieval and management	RFC 3501
SMS Protocol	SYNC/STATUS provisioning messages	OMTP VVM v1.3
Greeting Management	Personal and extended absence greetings	GSMA TS.46
Transcription	Voicemail-to-text support	OMTP VVM v1.3

Endpoints Overview

Endpoint	Met
`/`	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

Web UI

OmniSEP includes a real-time web interface for monitoring and management, built with Phoenix LiveView. Access the UI at `http://<host>:9014/`.

XCAP Simservs Profile management showing subscriber supplementary services configuration

Dashboards

Dashboard	Path	Description
Status	`/`	System health, service status, memory usage, storage statistics
Entitlements	`/entitlements`	View and manage TS.43 custom entitlements by IMSI
Sessions	`/sessions`	Monitor EAP-AKA sessions and active authentication tokens
Activity	`/activity`	Browse TS.43 activity logs with filtering and pagination
XCAP Profiles	`/xcap`	Manage XCAP Simservs profiles, sync with HSS
Diameter	`/diameter`	Monitor Diameter peer connections and status
Logs	`/logs`	Real-time system log viewer with level filtering

Status Dashboard

The main status dashboard provides at-a-glance system health:

- **Service Status**: HTTP server, EAP-AKA, VVM service indicators
- **Storage Counters**: Entitlements, XCAP profiles, sessions, tokens, activity records
- **Memory Usage**: Total, process, and ETS memory breakdown
- **Uptime**: System uptime display

All metrics auto-refresh every 5 seconds.

XCAP Profile Management

The XCAP dashboard allows operators to:

- Search and view subscriber profiles by MSISDN
- Edit supplementary service settings (OIP/OIR, call forwarding, call barring)
- Pull profiles from HSS via Diameter Sh interface
- Push local changes back to HSS
- View modification metadata (timestamp, client IP, User-Agent)

Activity Monitoring

The activity dashboard provides real-time visibility into all device requests:

Activity log showing XCAP and entitlement requests with request/response details

Features:

- Filter by request type (XCAP, Entitlement Query, EAP Challenge, etc.)
- Search by IMSI, MSISDN, Terminal ID, or Client IP
- View detailed request/response data including headers, body, and path
- Track HTTP method and response status codes

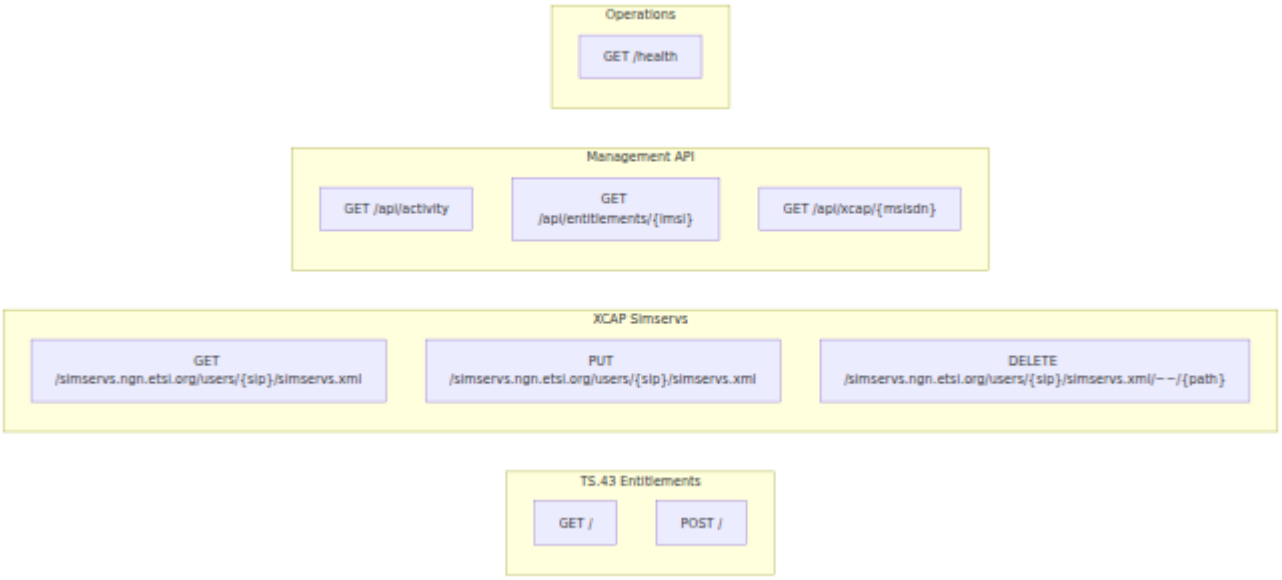
Session Monitoring

The sessions dashboard displays:

- **Sessions Tab**: Active EAP-AKA sessions with state (pending, challenge_sent, authenticated, failed)
- **Tokens Tab**: Active authentication tokens with time remaining until expiry

Both views support manual session/token revocation.

Authentication Flow



Quick Start Configuration

Minimal Configuration

```
# 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"

# Default entitlements for all subscribers
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}
    ]
  }

# Token settings
config :omni_sep, :token,
  validity_seconds: 86400,
  signing_secret: "your-production-secret-here"

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

See Configuration Reference for complete parameter documentation.

Documentation Structure

By Role

Network Operators:

1. Start with this overview
2. Review Configuration Reference for deployment settings
3. Review Troubleshooting for common issues

Service Configuration:

1. TS.43 Entitlements for VoWiFi/VoLTE provisioning
2. XCAP Simservs for call forwarding/barring

Troubleshooting:

1. Troubleshooting Guide for common issues
2. Check Activity Logging for request tracking

By Protocol

GSMA TS.43:

- TS.43 Entitlements - Complete service entitlement documentation
- Specification: GSMA TS.43

ETSI XCAP:

- XCAP Simservs - Supplementary services documentation
- Specifications:
  - ETSI TS 183 023 - XCAP framework
  - ETSI TS 183 004 - Communication Diversion
  - RFC 4825 - XCAP protocol