ANSSI R226 Interception Compliance Documentation

Document Purpose: This document provides technical specifications required for ANSSI R226 authorization under Articles R226-3 and R226-7 of the French Penal Code for the OmniCSCF IMS Core Network (Call Session Control Functions).

Classification: Regulatory Compliance Documentation

Target Authority: Agence nationale de la sécurité des systèmes d'information (ANSSI)

Regulation: R226 - Protection of Correspondence Privacy and Lawful Interception

---

1. DETAILED TECHNICAL SPECIFICATIONS

1.1 System Identification

Product Name: OmniCSCF IMS Core Network **Product Type:** IP Multimedia Subsystem (IMS) Core Network **Primary Function:** VoIP/VoLTE call session control and multimedia service delivery **Deployment Model:** On-premises telecommunications infrastructure

Network Components:

- P-CSCF (Proxy Call Session Control Function)
- E-CSCF (Emergency Call Session Control Function)
- I-CSCF (Interrogating Call Session Control Function)
- S-CSCF (Serving Call Session Control Function)

This system handles registration, authentication, session routing, and call control for IP Multimedia Subsystem (IMS) networks. The detailed interception capabilities and encryption characteristics are described in the sections below.

1.2 Interception Capabilities

1.2.1 Registration and Session Acquisition

SIP Registration Capture:

The CSCF system processes all SIP registrations and maintains complete registration state:

- **User Identifiers:**
  - IMPU (IP Multimedia Public Identity) - SIP URI (e.g., sip:+33612345678@ims.mnc001.mcc001.3gppnetwork.org)
  - IMPI (IP Multimedia Private Identity) - Authentication username (e.g., user@ims.mnc001.mcc001.3gppnetwork.org)
  - IMSI (International Mobile Subscriber Identity) - From P-headers or HSS
  - MSISDN (Mobile phone number) - From IMPU or HSS user profile
- **Registration Metadata:**
  - Contact URI (actual UE network address)
  - Path header (route back through P-CSCF)
  - Service-Route header (route to S-CSCF)
  - User-Agent string (device type identification)
  - Registration expiry timestamp
  - Source IP address and port
  - Transport protocol (TCP/UDP/TLS)
  - Authentication vectors (RAND, AUTN, XRES, CK, IK from HSS)

- **Network Location Information:**
  - P-Access-Network-Info header (cell tower, location area)
  - P-Visited-Network-ID (roaming network identification)
  - Received IP address (actual source)
  - P-CSCF address (network entry point)

Call Session Capture:

The S-CSCF maintains complete SIP dialog state for all active calls:

- **Session Identifiers:**
  - Call-ID (unique session identifier)
  - From/To URIs and tags
  - Route sets for both parties
  - Original-Dialog-ID (for Application Server interaction tracking)
- **Session Metadata:**
  - Caller identity (From header, P-Asserted-Identity)
  - Called party (To header, Request-URI)
  - Session establishment timestamp
  - Session termination timestamp
  - Dialog state (Early/Confirmed/Deleted)
  - CSeq numbers (transaction sequencing)
- **Media Information:**
  - SDP (Session Description Protocol) in SIP message bodies
  - Media server addresses (OmniTAS)
  - Codec information (audio/video formats)
  - Media flow endpoints
  - RTP/RTCP port allocations

Emergency Call Identification:

The E-CSCF component identifies and routes emergency calls:

- Emergency number detection (112, 911, etc.)
- IMEI (International Mobile Equipment Identity) capture
- IMEI to MSISDN mapping (for callback)
- Location information from UE or network
- HELD (HTTP-Enabled Location Delivery) protocol support
- Emergency routing destination (PSAP/emergency AS)

1.2.2 Data Storage and Processing

IMPORTANT: In-Memory State Only

The CSCF components (P-CSCF, E-CSCF, I-CSCF, S-CSCF) maintain **all state data in memory only**. There is **no persistent database storage** of registration or call session data. All registration bindings, dialog state, and IPsec security associations are stored in-memory and are lost on system restart.

Active Registration Data (In-Memory):

The CSCF system maintains real-time state only:

P-CSCF Registration State:

- IPsec Security Association data (SPI pairs, ports, encryption parameters)
- UE contact bindings and network addresses
- IPsec tunnel endpoints and status
- Registration validity periods

S-CSCF Registration State:

- Public identities (IMPU) and current registration state
- Contact bindings with Path headers, User-Agent, received addresses
- Private identity (IMPI) to public identity mappings
- User profiles from HSS (cached during registration)

Active Session State (In-Memory):

The S-CSCF maintains active call state only:

- Call identifiers (Call-ID), participant identities (From/To tags)
- Route sets and contact addresses
- Session state (Early/Confirmed/Terminated)
- Session timing information

No CDR or Historical Tracking:

The CSCF components do **not** generate or store:

- Call Detail Records (CDRs)
- Historical call records
- Historical registration records
- Long-term event tracking

CDR Generation and Historical Tracking: All call detail records, charging data, and historical call tracking are handled by the **TAS (Telephony Application Server - OmniTAS)**, not by the CSCF components.

SIP/Diameter Message Logging:

CSCFs can generate real-time event logs for operational purposes:

- **SIP Message Logging:** Optional logging of SIP messages (INVITE, REGISTER, etc.)
- **Diameter Message Logging:** Optional logging of Diameter transactions (Cx, Rx, Ro)
- **System Events:** Configuration changes, errors, failures

These logs are transient operational logs, not persistent call records. Log retention is configurable and typically short-term (hours to days) for debugging purposes only.

1.2.3 Analysis Capabilities

Real-Time Monitoring:

The Phoenix LiveView web control panel provides:

- **Registration Monitoring:**

    - View all registered users with pagination
    - Search by IMPU, contact, IMPI
    - Registration details (contact, path, user-agent, expiry)
    - Forced de-registration capability

- **Dialog Monitoring:**
    - Active call sessions view
    - Call-ID, From/To URIs, state, duration
    - Call termination capability (send BYE)
    - Auto-refresh every 5 seconds

- **System Status:**
    - Diameter peer status (HSS, PCRF, OCS connectivity)
    - Frontend gateway status
    - System capacity metrics
    - IPsec tunnel capacity (P-CSCF)

Note on Historical Data:

The CSCF components do not maintain historical data. For historical call records, CDRs, and communication pattern analysis, lawful interception authorities must coordinate with **OmniTAS (Telephony Application Server)**, which handles all CDR generation and long-term call tracking.

Real-Time Service Triggering Visibility:

The S-CSCF processes Initial Filter Criteria (iFC) in real-time:

- iFC evaluation determines which Application Servers are triggered for each call
- Real-time visibility into which services are invoked
- Application Server routing decisions visible in SIP message flow

Network Status:

- HSS connectivity status (Diameter Cx interface)

- S-CSCF selection distribution (I-CSCF)
- Call routing patterns
- Application Server response times
- Diameter transaction performance

1.3 Countermeasure Capabilities

1.3.1 Privacy Protection Mechanisms

Communication Confidentiality:

- **IPsec Tunnels:** ESP (Encapsulating Security Payload) tunnels between UE and P-CSCF
  - Encryption: AES-CBC, AES-GCM
  - Authentication: HMAC-SHA1, HMAC-SHA256
  - Key derivation from IMS AKA (CK/IK from HSS)
  - Per-UE security associations
- **TLS/TLS Support:**
  - SIP over TLS (SIPS) support
  - Diameter over TLS (HSS, PCRF, OCS connections)
  - Certificate-based authentication
  - Perfect Forward Secrecy (PFS) via ECDHE/DHE
- **SIP Privacy Headers:**
  - P-Asserted-Identity (authenticated caller ID)
  - Privacy header (request caller ID suppression)
  - Anonymous session support

Access Control:

- Web UI authentication and access control
- BINRPC interface for control panel (port 2046)
- Registry access controls and role separation
- SIP authentication (AKA via HSS)

- Diameter peer authentication

Audit Logging:

- Comprehensive SIP and Diameter message logging
- Registration/de-registration events
- Call establishment and termination events
- Administrative actions via web UI
- Configuration changes
- Authentication success/failure

1.3.2 Data Protection Features

Access Security:

- Role-based access control (RBAC)
- Read-only monitoring accounts
- Authentication and authorization controls

System Hardening:

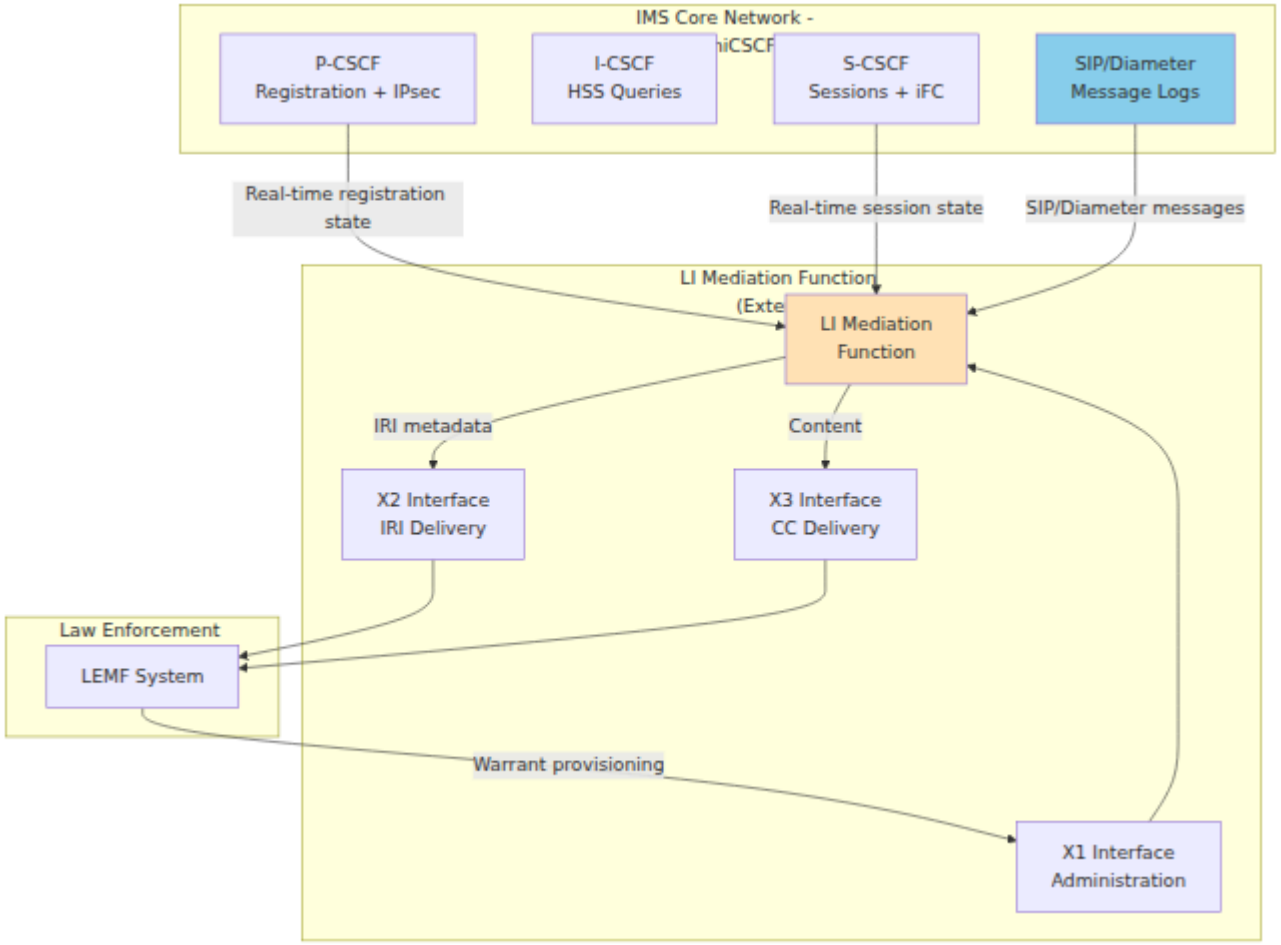
- Minimal exposed network ports (5060 SIP, 3868 Diameter, 8086 Web UI)
- SIP message sanity checking
- Max-Forwards loop prevention
- Rate limiting and anti-flood protection
- Message size limits
- Worker process isolation

1.4 Lawful Interception Integration Points

1.5.1 ETSI Lawful Interception Architecture

The CSCF system provides foundation for ETSI-compliant lawful interception. While native X1/X2/X3 interfaces are not built-in, all necessary data access points exist for integration with external Lawful Interception Mediation Function (LIMF) systems.

Standard ETSI LI Interfaces:



X1 Interface - Administration Function:

- **Purpose:** Warrant and target provisioning from law enforcement
- **Direction:** LEMF → LIMF (bidirectional)
- **Functions:**
  - Activate/deactivate interception for targets (IMPUs, IMSIs, MSISDNs)
  - Set interception duration and validity period
  - Configure filtering criteria (identities, time windows)
  - Retrieve interception status
- **Integration with CSCF:**
  - LIMF maintains warrant database (target list - external to CSCF)
  - LIMF monitors CSCF real-time state and message logs for matching sessions
  - LIMF filters based on X1 provisioned criteria

X2 Interface - IRI (Intercept Related Information) Delivery:

- **Purpose:** Deliver session metadata to law enforcement

- **Direction:** LIMF → LEMF (one-way)
- **Data Format:** ETSI TS 102 232 compliant XML/ASN.1
- **Content from CSCF:**
  - Session identifiers (Call-ID, dialog tags)
  - Calling party (From URI, P-Asserted-Identity, IMPU, IMSI, MSISDN)
  - Called party (To URI, Request-URI, IMPU, IMSI, MSISDN)
  - Registration timestamps
  - Session setup/teardown timestamps
  - Network location (P-Access-Network-Info, cell tower, location area)
  - P-CSCF/S-CSCF addresses (network element identification)
  - User-Agent (device type)
  - Roaming information (P-Visited-Network-ID)

X3 Interface - CC (Content of Communication) Delivery:

- **Purpose:** Deliver actual communication content
- **Direction:** LIMF → LEMF (one-way)
- **Data Format:** ETSI TS 102 232 compliant
- **Content from CSCF:**
  - SIP message bodies (SDP session descriptions)
  - Media server addresses (for RTP interception)
  - Codec information
  - SIP MESSAGE instant messages (body content)
  - Application data (if routed through CSCF)

Note: For voice/video RTP streams, the LIMF must also integrate with media servers (OmniTAS) to capture actual media content. The CSCF provides session setup information (SDP) showing where media flows.

1.5.2 CSCF Data Sources for Lawful Interception

1. Registration Data Access:

P-CSCF Registration Data:

- IMPU (public identity)

- Contact URI (UE network address)
- Received IP and port
- Path header
- Registration expiry
- IPsec SPI and port information
- User-Agent string

S-CSCF Registration Data:

- Public identities (IMPU), barring status, registration state
- Contact bindings with Path headers, User-Agent, received addresses
- Private identity (IMPI) to public identity mappings
- User profiles from HSS (XML format including subscriber details)

Access Methods:

- Read-only data access interfaces
- Web UI monitoring interface
- Real-time event logging

2. Active Session Data:

S-CSCF Dialog Data:

- Call-ID (unique session identifier)
- From/To URIs and tags
- Caller and callee CSeq numbers
- Route sets for both parties
- Contact addresses
- Dialog state (Early, Confirmed, Deleted)
- Start timestamp
- Timeout values

Access Methods:

- Real-time dialog state monitoring
- Query by session identifiers or party identifiers

- Export capabilities for forensic analysis

3. SIP Message Logging:

Log Capture:

- All SIP messages can be logged (REGISTER, INVITE, MESSAGE, etc.)
- Configurable log levels
- Structured logging with timestamps
- Syslog or file-based logging

Log Analysis:

- Parse SIP headers for identity extraction
- Extract SDP for media information
- Track message sequences (CSeq)
- Correlate requests and responses

Example Log Entry:

```
INFO: INVITE sip:+33687654321@ims.mnc001.mcc001.3gppnetwork.org
SIP/2.0
From:
<sip:+33612345678@ims.mnc001.mcc001.3gppnetwork.org>;tag=abc123
To: <sip:+33687654321@ims.mnc001.mcc001.3gppnetwork.org>
Call-ID: f81d4fae-7dec-11d0-a765-
00a0c91e6bf6@ims.mnc001.mcc001.3gppnetwork.org
P-Asserted-Identity:
<sip:+33612345678@ims.mnc001.mcc001.3gppnetwork.org>
P-Access-Network-Info: 3GPP-E-UTRAN-FDD; utran-cell-id-
3gpp=208011234567890
Content-Type: application/sdp

v=0
o=- 1234567890 1234567890 IN IP4 192.168.1.100
s=-
c=IN IP4 10.20.30.40
t=0 0
m=audio 49170 RTP/AVP 0 8
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
```

4. Diameter Message Logging:

Cx Messages (HSS Communication):

- UAR/UAA: User authorization (contains IMPU, IMPI)
- LIR/LIA: Location information (contains IMPU, serving S-CSCF)
- MAR/MAA: Authentication (contains IMPI, authentication vectors)
- SAR/SAA: Server assignment (contains IMPU, IMPI, user profile XML)

Diameter Data Available:

- IMSI (from user profile)
- MSISDN (from user profile)
- Associated IMPUs (multiple identities per subscriber)
- User profile (services, barring, roaming status)

Log Example:

```
Diameter Cx SAA received from HSS:
User-Name: user@ims.mnc001.mcc001.3gppnetwork.org
Public-Identity:
sip:+33612345678@ims.mnc001.mcc001.3gppnetwork.org
Server-Name: sip:scscf.ims.mnc001.mcc001.3gppnetwork.org
Result-Code: 2001 (Success)
User-Data: <XML user profile with IMSI, MSISDN, iFC>
```

5. Emergency Call Data (E-CSCF):

IMEI to MSISDN Mapping:

- P-CSCF creates mapping when UE registers with IMEI
- 24-hour TTL (Time-To-Live)
- Used for emergency callback
- Synchronized across P-CSCF cluster nodes

Data Retention:

- IMEI to MSISDN mappings retained for 24 hours
- Available for emergency callback correlation
- Accessible via monitoring interfaces

Emergency Call Logs:

- Emergency number detection (112, 911, etc.)
- IMEI extraction from contact or P-headers
- Location information (from HELD or P-Access-Network-Info)
- PSAP (Public Safety Answering Point) routing
- E-CSCF to emergency AS routing

1.5.3 Integration Capabilities for LIMF

The system provides multiple integration methods for Lawful Interception Mediation Function (LIMF) systems:

1. **Registration and Session Data Access:**

    - Real-time access to registration data (identities, locations, device information)
    - Active session monitoring (call state, participants, timing)
    - Historical query capabilities

2. **Event Logging:**

    - SIP message logging with configurable detail levels
    - Diameter message logging for HSS interactions
    - Structured event logs with timestamps

3. **Real-Time Monitoring:**

    - Live registration status monitoring
    - Active call session tracking
    - Emergency call detection and routing information

Integration methods support both polling-based and event-driven architectures for LIMF connectivity.

1.5.4 CSCF Data Mapping to LI Interfaces

CSCF Data to IRI (X2) Mapping:

CSCF Data Source	IRI Field	Data Example
IMPU (SIP headers/in-memory state)	Party A	sip:+33612345678@ims.mnc001.mcc001.
IMPI (SIP headers/in-memory state)	Authentication ID	user@ims.mnc001.mcc001.3gppnetwork.o
IMSI (HSS user profile)	Subscriber ID	208011234567890
MSISDN (HSS user profile)	Phone Number	+33612345678
Call-ID (SIP headers/dialog state)	Session ID	f81d4fae-7dec-11d0-a765-00a0c91e6bf6@
From/To (SIP headers)	Party A/Party B	sip:+33612345678@... / sip:+3368765432
Registration timestamp (in-memory)	Event Time	2025-11-29T10:30:00Z
P-Access-Network-Info (SIP header)	Location	3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=208
Received IP (SIP contact)	UE IP Address	10.20.30.40:5060
P-CSCF address (SIP	Network Element	10.4.12.165:5060

CSCF Data Source	IRI Field	Data Example
routing)		
S-CSCF address (SIP routing)	Network Element	10.4.11.45:5060

CSCF Data to CC (X3) Mapping:

CSCF Data Source	CC Field	Data Example
SIP MESSAGE body	Instant Message Content	"Hello, how are you?"
SDP in INVITE	Media Session Info	RTP endpoints, codecs
Media server address	RTP Interception Target	10.50.60.70:49170

Note: For actual voice/video content (RTP), the LIMF must coordinate with media servers (OmniTAS) to capture RTP streams. CSCF provides session setup information only.

1.5 Web-Based Monitoring Interface

The system includes a web-based control panel for real-time monitoring and administrative access:

Monitoring Capabilities:

- Real-time registration status (active subscribers, locations, device information)
- Active call session monitoring (participants, call state, timing)
- Search and filtering by identity (IMPU, IMPI, IMSI, MSISDN)
- IPsec tunnel status and capacity monitoring
- Export capabilities for forensic analysis

Security:

- HTTPS/TLS encrypted access
- Authentication required
- Audit logging of all administrative actions
- Read-only access modes for monitoring personnel

---

2. ENCRYPTION AND CRYPTANALYSIS CAPABILITIES

2.1 Cryptographic Capabilities Overview

The OmniCSCF implements multiple layers of cryptographic protection for signaling and subscriber data. This section documents all cryptographic capabilities as required by ANSSI.

2.2 IPsec ESP Tunnel Encryption (UE to P-CSCF)

2.2.1 IPsec Protocol Implementation

Supported IPsec Mode:

- ESP (Encapsulating Security Payload) - IP Protocol 50
- Transport mode (not tunnel mode)
- Protects SIP signaling between UE and P-CSCF

Encryption Algorithms Supported:

The system with kernel IPsec supports:

- **AES-CBC (Advanced Encryption Standard - Cipher Block Chaining):**
    - AES-128-CBC (128-bit key)
    - AES-192-CBC (192-bit key)
    - AES-256-CBC (256-bit key) - Recommended

- **AES-GCM (Advanced Encryption Standard - Galois/Counter Mode):**
  - AES-128-GCM (128-bit key with AEAD)
  - AES-256-GCM (256-bit key with AEAD) - Recommended
- **3DES-CBC (Triple DES - Cipher Block Chaining):**
  - 168-bit effective key (deprecated, legacy compatibility)
- **NULL Encryption:**
  - No confidentiality (authentication only)
  - Used only for debugging or specific compliance scenarios

Authentication Algorithms Supported:

- **HMAC-SHA1 (Hash-based Message Authentication Code - SHA-1):**
  - 160-bit output
  - Legacy compatibility
- **HMAC-SHA256 (HMAC - SHA-256):**
  - 256-bit output
  - Recommended
- **HMAC-SHA384 (HMAC - SHA-384):**
  - 384-bit output
- **HMAC-SHA512 (HMAC - SHA-512):**
  - 512-bit output
- **HMAC-MD5:**
  - 128-bit output
  - Deprecated, legacy compatibility only

Key Derivation:

IPsec keys (CK - Cipher Key, IK - Integrity Key) are derived from IMS AKA authentication:

1. UE performs AKA authentication with S-CSCF/HSS
2. HSS generates CK (128-bit) and IK (128-bit)
3. S-CSCF delivers CK/IK to P-CSCF via internal interface
4. P-CSCF uses CK/IK to establish IPsec security associations with UE
5. CK used for ESP encryption
6. IK used for ESP authentication

Security Association Parameters:

- **Lifetime:** Tied to SIP registration expiry (typically 599 seconds)
- **Replay Protection:** Enabled (anti-replay window)
- **Sequence Numbers:** 32-bit or 64-bit (ESN - Extended Sequence Numbers)
- **Perfect Forward Secrecy:** Not applicable (keys from AKA, not Diffie-Hellman)

Implementation:

The P-CSCF IPsec capability:

- Interfaces with Linux kernel IPsec stack (XFRM framework)
- Configures security policies and associations via kernel API
- SPI (Security Parameter Index) allocation and management
- Port allocation for protected traffic

2.2.2 IPsec Configuration Capabilities

Cipher Suite Selection:

The P-CSCF can be configured to prefer specific cipher suites:

Preferred (strong security):

- ESP with AES-256-GCM and HMAC-SHA256
- ESP with AES-256-CBC and HMAC-SHA256

Supported (compatibility):

- ESP with AES-128-CBC and HMAC-SHA1
- ESP with 3DES-CBC and HMAC-SHA1 (legacy)

Key Management:

- IKE (Internet Key Exchange) is NOT used
- Keys provided via IMS AKA (CK/IK from HSS)
- Manual security association setup via kernel XFRM
- Automatic SA teardown on registration expiry

Tunnel Lifecycle:

1. UE registers → AKA authentication → CK/IK generated
2. P-CSCF receives CK/IK from S-CSCF
3. P-CSCF allocates SPI pair (client SPI, server SPI)
4. P-CSCF allocates port pair (client port, server port)
5. P-CSCF configures kernel IPsec SAs using CK/IK
6. P-CSCF sends IPsec parameters to UE in 200 OK (Security-Server header)
7. UE configures IPsec SAs with same parameters
8. All subsequent SIP traffic flows through ESP tunnels
9. On registration expiry or de-registration: SAs deleted, resources freed

2.3 TLS Encryption (SIP and Diameter)

2.3.1 TLS for SIP (SIPS)

Supported TLS Versions:

- **TLS 1.2** (RFC 5246) - Supported
- **TLS 1.3** (RFC 8446) - Supported (if kernel/library support)
- **TLS 1.0/1.1** - Deprecated (disabled by default)
- **SSL 2.0/3.0** - NOT SUPPORTED (known vulnerabilities)

TLS Implementation:

the system uses OpenSSL or LibreSSL:

- Industry-standard TLS libraries
- Cryptographically validated implementations
- Regular security updates

Cipher Suites Supported:

TLS 1.3 (Preferred):

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256

TLS 1.2 (Supported):

- ECDHE-RSA-AES256-GCM-SHA384 (Perfect Forward Secrecy)
- ECDHE-RSA-AES128-GCM-SHA256 (Perfect Forward Secrecy)
- ECDHE-ECDSA-AES256-GCM-SHA384 (Perfect Forward Secrecy)
- DHE-RSA-AES256-GCM-SHA384 (Perfect Forward Secrecy)
- DHE-RSA-AES128-GCM-SHA256 (Perfect Forward Secrecy)

Weak ciphers disabled:

- No RC4
- No MD5
- No NULL encryption
- No EXPORT-grade ciphers
- No DES/3DES (deprecated)

Certificate Support:

- **X.509 certificates** (standard format)
- **RSA keys:** 2048-bit minimum, 4096-bit recommended
- **ECDSA keys:** P-256, P-384, P-521 curves supported
- **Certificate chain validation**
- **CRL (Certificate Revocation List) checking** (optional)

- **OCSP (Online Certificate Status Protocol)** (optional)

TLS Features:

- **Perfect Forward Secrecy (PFS):** Via ECDHE/DHE key exchange
- **Server Name Indication (SNI):** Supported
- **TLS Session Resumption:** Supported (performance optimization)
- **Client Certificate Authentication:** Supported (mutual TLS)

SIP over TLS (SIPS):

- Transport: TCP with TLS encryption
- Port: 5061 (standard SIPS port)
- Used for inter-CSCF communication (optional)
- Used for trusted network connections

2.3.2 TLS for Diameter

Diameter Capabilities:

The system supports:

- **Diameter over SCTP** (preferred for reliability)
- **Diameter over TCP with TLS**
- **Port:** 3868 (standard Diameter port)

Use Cases:

- **Cx interface:** S-CSCF/I-CSCF to HSS (subscriber data, authentication)
- **Rx interface:** P-CSCF to PCRF (QoS policy)
- **Ro interface:** S-CSCF to OCS (online charging - if enabled)

TLS Configuration for Diameter:

Same cipher suites as SIP

- TLS 1.2/1.3
- ECDHE/DHE key exchange (PFS)
- AES-GCM encryption

- SHA256/SHA384 authentication

Certificate-Based Authentication:

- Diameter peers authenticate via TLS certificates
- Mutual TLS (both client and server certificates)
- FQDN (Fully Qualified Domain Name) validation in certificates
- Trusted CA chain validation

2.4 Authentication Cryptography

2.4.1 IMS AKA Cryptographic Functions

3GPP AKA Algorithm (MILENAGE):

Used for generating authentication vectors (RAND, AUTN, XRES, CK, IK):

Cryptographic Functions:

- **f1:** Message authentication function (compute MAC-A and MAC-S)
- **f2:** Response function (compute RES from RAND and K)
- **f3:** Cipher key derivation (compute CK)
- **f4:** Integrity key derivation (compute IK)
- **f5:** Anonymity key function (compute AK for IMSI privacy)

Key Material:

- **K:** 128-bit permanent subscriber key (stored in ISIM and HSS)
- **OPc:** Operator variant key (derived from K and OP)
- **RAND:** 128-bit random challenge
- **SQN:** 48-bit sequence number (replay protection)

AKA Sequence:

1. HSS generates RAND (cryptographically random)
2. HSS computes MAC-A = f1(K, RAND, SQN, AMF)
3. HSS computes AUTN = (SQN ⊕ AK) || AMF || MAC-A
4. HSS computes XRES = f2(K, RAND)

5. HSS computes CK = f3(K, RAND)
6. HSS computes IK = f4(K, RAND)
7. HSS sends {RAND, AUTN, XRES, CK, IK} to S-CSCF
8. S-CSCF challenges UE with RAND and AUTN
9. UE computes RES = f2(K, RAND) using ISIM
10. UE sends RES to S-CSCF
11. S-CSCF compares RES with XRES (authentication validation)

Security Properties:

- **Mutual Authentication:** UE verifies HSS via AUTN, HSS verifies UE via RES
- **Key Freshness:** RAND is random, SQN prevents replay
- **Key Derivation:** CK and IK derived from shared secret K

2.4.2 HTTP Digest Authentication

For non-IMS authentication (if used):

Algorithm: MD5 (RFC 2617)

- **Hash Function:** MD5 (128-bit output)
- **Challenge-Response:** Based on nonce
- **Replay Protection:** Nonce with timestamp

Note: HTTP Digest with MD5 is considered weak. IMS AKA is strongly preferred.

2.5 Hashing and Integrity

2.5.1 Hash Functions Available

the system can use (via OpenSSL/kernel crypto):

- **SHA-256:** 256-bit output, recommended
- **SHA-384:** 384-bit output
- **SHA-512:** 512-bit output
- **SHA-1:** 160-bit output, deprecated for security use

- **MD5:** 128-bit output, deprecated for security use

Usage:

- HMAC constructions for IPsec/TLS
- Data integrity verification
- Nonce generation
- Duplicate detection (Call-ID hashing)

2.5.2 Message Integrity

SIP Message Integrity:

- **IPsec ESP:** HMAC-SHA256 for authenticated SIP over IPsec
- **TLS:** Message authentication via TLS MAC
- **SIP Digest:** Authentication header integrity

Diameter Message Integrity:

- **TLS:** Diameter over TLS provides message authentication
- **HMAC:** Diameter messages can include HMAC AVPs for integrity

2.6 Random Number Generation

Cryptographically Secure Random Number Generation:

the system relies on:

- **Linux kernel /dev/urandom:** Cryptographically secure PRNG
- **OpenSSL RAND_bytes():** CSPRNG (Cryptographically Secure Pseudo-Random Number Generator)

Usage:

- SPI allocation (randomized starting value)
- Call-ID generation
- Branch parameter generation
- Nonce generation for authentication

- Session ID generation

2.7 Key Management

2.7.1 TLS Certificate Management

Certificate Storage:

- Filesystem storage with restricted permissions (0600)
- Located in: `/etc/system/tls/`
- PEM format for certificates and keys

Certificate Generation:

```
# Generate RSA 4096-bit private key
openssl genrsa -out system-key.pem 4096

# Generate CSR (Certificate Signing Request)
openssl req -new -key system-key.pem -out system.csr \
  -subj
"/C=FR/ST=IDF/L=Paris/O=Omnitouch/CN=scscf.ims.mnc001.mcc001.3gppnetw

# Self-signed certificate (development/testing)
openssl x509 -req -days 365 -in system.csr \
  -signkey system-key.pem -out system-cert.pem

# Production: Submit CSR to trusted CA
```

Certificate Rotation:

- Annual certificate renewal recommended
- Graceful service restart to load new certificates
- No downtime required

2.7.2 IPsec Key Management

Key Derivation:

- CK (Cipher Key) and IK (Integrity Key) from IMS AKA

- 128-bit keys from HSS
- Delivered securely via Diameter Cx (over TLS)

Key Lifetime:

- Tied to SIP registration expiry (typically 599 seconds)
- Re-keying on registration refresh
- Automatic key destruction on de-registration

Key Storage:

- Ephemeral (in-memory only during active registration)
- Installed in kernel IPsec stack
- No persistent key storage
- Keys discarded when SA deleted

2.8 Cryptanalysis Resistance

2.8.1 Algorithm Selection

Defense Against Cryptanalysis:

- **No custom algorithms:** Only industry-standard, peer-reviewed algorithms
- **Strong key sizes:** AES-256, RSA-4096, SHA-256
- **Authenticated encryption:** AES-GCM (AEAD - Authenticated Encryption with Associated Data)
- **Perfect Forward Secrecy:** ECDHE/DHE in TLS
- **Regular updates:** OpenSSL/LibreSSL security patches applied

Deprecated Algorithms Disabled:

- MD5 (hash collisions)
- RC4 (stream cipher weaknesses)
- DES/3DES (small block size, key length)
- SSL 2.0/3.0 (protocol vulnerabilities)
- TLS 1.0/1.1 (BEAST, POODLE attacks)

2.8.2 Side-Channel Attack Mitigation

Timing Attack Resistance:

- Constant-time comparison for authentication responses
- No timing leaks in cryptographic operations (via OpenSSL)

Memory Protection:

- Kernel IPsec stack isolation
- Process memory isolation
- No swap for sensitive data (if configured)

2.9 Compliance and Standards

Cryptographic Standards Compliance:

- **NIST SP 800-52:** TLS guidelines
- **NIST SP 800-131A:** Cryptographic algorithm transitions
- **RFC 7525:** TLS recommendations
- **ETSI TS 133 203:** 3GPP access security (IMS AKA)
- **ETSI TS 133 210:** IP network layer security (IPsec)
- **3GPP TS 33.203:** Access security for IMS
- **3GPP TS 33.210:** Network domain security

French Cryptography Regulations:

- No export-restricted cryptography (all standard algorithms)
- Standard cryptographic means (no government backdoors)
- ANSSI cryptographic product certification (if required)

Diameter Operations Guide

Table of Contents

1. Overview
2. Diameter in IMS Architecture
3. Diameter Interfaces
4. Peer Management via Web UI
5. Diameter Result Codes
6. Common Issues

Overview

Diameter is the authentication, authorization, and accounting (AAA) protocol used throughout the IMS architecture. OmniCall CSCF uses Diameter to communicate with critical network elements including HSS, PCRF, and OCS.

What is Diameter?

Diameter (RFC 6733) is the successor to RADIUS, designed for modern AAA scenarios:

- **Reliable transport** via TCP/SCTP (vs. UDP in RADIUS)
- **Extensible** via Application-Specific modules
- **Peer-to-peer** architecture (not just client-server)
- **Stateful** connections with watchdog monitoring
- **Standardized** error handling and result codes

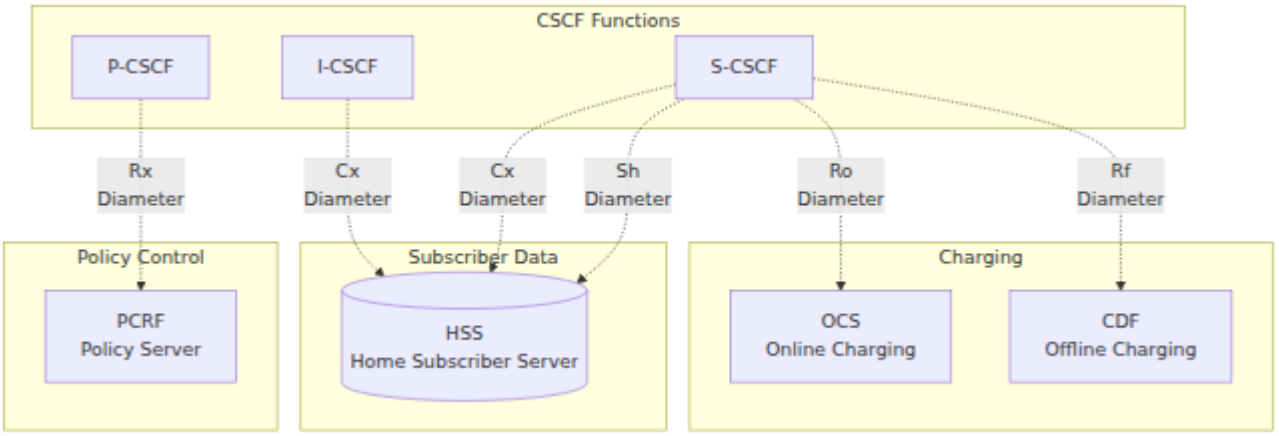
Diameter in CSCF

Each CSCF component uses specific Diameter application interfaces:

CSCF	Interface	Application ID	Connected To	Purpose
I-CSCF	Cx	16777216	HSS	S-CSCF selection, user location
S-CSCF	Cx	16777216	HSS	User authentication, profile download
S-CSCF	Sh	16777217	HSS	User data access (optional)
P-CSCF	Rx	16777236	PCRF	QoS policy and bearer control
S-CSCF	Ro	4	OCS	Online charging (credit control)
S-CSCF	Rf	3	CDF	Offline charging (accounting)

Diameter in IMS Architecture

Network Overview



Diameter Interfaces

Cx Interface (CSCF ↔ HSS)

The Cx interface is used by I-CSCF and S-CSCF for user authentication and profile management.

3GPP Specification: TS 29.228

I-CSCF Operations

User-Authorization-Request (UAR) / User-Authorization-Answer (UAA):

- **Purpose**: Query HSS for S-CSCF assignment or capabilities
- **Trigger**: REGISTER received from user
- **Use Case**: I-CSCF needs to route registration to appropriate S-CSCF

Location-Info-Request (LIR) / Location-Info-Answer (LIA):

- **Purpose**: Query HSS for user's current S-CSCF
- **Trigger**: INVITE or MESSAGE received for terminating user
- **Use Case**: I-CSCF needs to route session to user's S-CSCF

S-CSCF Operations

Multimedia-Auth-Request (MAR) / Multimedia-Auth-Answer (MAA):

- **Purpose**: Retrieve authentication vectors from HSS
- **Trigger**: Initial REGISTER (before challenge)
- **Use Case**: S-CSCF needs to challenge user for IMS AKA authentication

Server-Assignment-Request (SAR) / Server-Assignment-Answer (SAA):

- **Purpose**: Inform HSS of registration state, download user profile
- **Trigger**: Successful authentication (after MAR/MAA)
- **Use Case**: S-CSCF downloads IFC and service profile for user

The `User-Data` AVP in SAA contains the complete user profile including:

- Public identities
- Initial Filter Criteria (IFC) for service triggering
- Subscribed media profile identifiers
- Charging information

Registration-Termination-Request (RTR) / Registration-Termination-Answer (RTA):

- **Purpose**: HSS-initiated deregistration (push from HSS)
- **Trigger**: Administrative deregistration, subscription change
- **Use Case**: HSS instructs S-CSCF to deregister a user

Rx Interface (P-CSCF ↔ PCRF)

The Rx interface provides policy and QoS control for IMS sessions.

3GPP Specification: TS 29.214

AA-Request (AAR) / AA-Answer (AAA):

- **Purpose**: Request QoS authorization for media session
- **Trigger**: SDP offer/answer exchange in SIP INVITE
- **Use Case**: P-CSCF requests PCRF to authorize bearer resources

Re-Auth-Request (RAR) / Re-Auth-Answer (RAA):

- **Purpose**: PCRF-initiated policy update (push from PCRF)
- **Trigger**: Policy change, bearer modification
- **Use Case**: PCRF instructs P-CSCF to update QoS policy

Session-Termination-Request (STR) / Session-Termination-Answer (STA):

- **Purpose**: Release Rx session and bearer resources
- **Trigger**: Call termination (BYE received)
- **Use Case**: P-CSCF informs PCRF to release QoS resources

Ro Interface (S-CSCF ↔ OCS)

The Ro interface provides online charging (credit control).

3GPP Specification: TS 32.299

Credit-Control-Request (CCR) / Credit-Control-Answer (CCA):

- **Purpose**: Real-time credit authorization and debit
- **Trigger**: Call setup, mid-call, call termination
- **Use Case**: Prepaid charging, real-time credit checks

Types:

- **CCR-Initial**: Request credit at call start
- **CCR-Update**: Refresh quota during call
- **CCR-Terminate**: Report final usage at call end

Peer Management via Web UI

OmniCall CSCF provides a web-based control panel for Diameter peer management.

Access: Navigate to **Diameter** tab in control panel (`http://<cscf-server>:4000/diameter`)

Viewing Peer Status

The Diameter management page displays:

Summary Information

- **Realm**: Diameter realm
- **Identity**: Diameter Origin-Host
- **Peer Count**: Number of configured peers
- **Workers**: CDP worker count
- **Queue Length**: Pending transactions
- **Connect Timeout**: Connection timeout (seconds)
- **Transaction Timeout**: Transaction timeout (seconds)
- **Accept Unknown Peers**: Policy flag

Peer List

Table of all Diameter peers with the following columns:

Column	Description
FQDN	Peer fully-qualified domain name
State	Connection state (I_Open, Closed, etc.)
Status	Enabled or Disabled
Last Used	Time since last transaction
Applications	Number of supported Diameter applications

Peer Operations

Enable Peer:

1. Locate disabled peer in table
2. Click **Enable** button
3. Peer will attempt to establish connection

Disable Peer:

1. Locate enabled peer in table
2. Click **Disable** button
3. Confirm action
4. Peer connection will be gracefully terminated

View Applications:

1. Click on peer row to expand
2. View list of supported Diameter applications with interface names

The expanded peer view shows all supported Diameter applications:

- **16777216:10415** - 3GPP Cx/Dx (HSS communication for I-CSCF/S-CSCF)
- **16777236:10415** - 3GPP Rx (PCRF QoS policy for P-CSCF)
- **16777238:0** - 3GPP Ro (Online charging)
- Other supported application IDs and vendor IDs

The control panel automatically maps Diameter Application IDs to 3GPP interface names:

- **Cx/Dx** (16777216:10415)
- **Sh/Dh** (16777217:10415)
- **Rx** (16777236:10415)
- **Ro** (16777238:10415/0/5535/13019)
- **Gx** (16777224:10415)
- **S6a/S6d** (16777251:10415)
- And many more (see `diameter_live.ex` for complete list)

Peer States

State	Description
I_Open	Connection open and operational
Closed	No connection established
Wait-Conn-Ack	Connection initiated, awaiting response
Wait-I-CEA	CER sent, awaiting CEA

For detailed peer management: See Web UI Operations Guide

Diameter Result Codes

Common result codes and their meanings:

Code	Name	Meaning	Action
2xxx	**Success**		
2001	DIAMETER_SUCCESS	Operation successful	None
3xxx	**Protocol Errors**		
3002	DIAMETER_UNABLE_TO_DELIVER	Cannot route to destination	Check peer connectivity
3003	DIAMETER_REALM_NOT_SERVED	Realm not recognized	Verify realm configuratio
3007	DIAMETER_APPLICATION_UNSUPPORTED	Application not supported	Check Application-
4xxx	**Transient Failures**		
4001	DIAMETER_AUTHENTICATION_REJECTED	Auth failed	Check credentials
4010	DIAMETER_USER_UNKNOWN	User not provisioned	Verify HSS provisioning
5xxx	**Permanent Failures**		
5001	DIAMETER_AVP_UNSUPPORTED	AVP not recognized	Check protocol version
5002	DIAMETER_UNKNOWN_SESSION_ID	Session not found	Session expired or invalid

Code	Name	Meaning	Action
5003	DIAMETER_AUTHORIZATION_REJECTED	Not authorized	Check user permissions
5012	DIAMETER_UNABLE_TO_COMPLY	Cannot process request	Check HSS/PCRF/O logs

Common Issues

Peer Connection Failures

Symptom: Peer stuck in "Closed" or "Wait-Conn-Ack" state

Diagnosis:

1. Verify network connectivity:

   ```
   ping <peer-fqdn>
   telnet <peer-fqdn> 3868
   ```

2. Check firewall rules (port 3868 TCP must be open)
3. Verify peer configuration (IP address, port)
4. Check peer logs for connection attempts

Resolution:

- Fix network/firewall issues
- Verify peer is running and listening on port 3868
- Check if peer has correct configuration for CSCF
- Use **Enable Peer** in web UI to retry connection

CER/CEA Exchange Failures

Symptom: Peer stuck in "Wait-I-CEA" state, or CEA with error code

Common Errors:

- **5010 (NO_COMMON_APPLICATION)**: Verify both peers support the same application (e.g., Cx = 16777216)
- **3003 (REALM_NOT_SERVED)**: Verify Origin-Realm matches peer's expected realm

Resolution:

- Check Diameter configuration for Application-Id and realm
- Ensure peer configuration matches CSCF expectations
- Review CSCF backend logs for detailed error messages

HSS Cx Interface Issues

Symptom: Registration failures, MAR/MAA timeouts

Common Errors:

Result-Code	Meaning	Resolution
4010	USER_UNKNOWN	User not provisioned in HSS
4001	AUTHENTICATION_REJECTED	Incorrect IMPI/credentials
5012	UNABLE_TO_COMPLY	HSS internal error, check HSS logs

Resolution:

- **USER_UNKNOWN**: Provision user in HSS
- **AUTHENTICATION_REJECTED**: Verify IMPI and shared secret in HSS

- **UNABLE_TO_COMPLY**: Check HSS logs and database connectivity

---

PCRF Rx Interface Issues

Symptom: Calls succeed but no QoS applied, AAR/AAA timeouts

Common Issues:

- **PCRF down**: Check peer status in web UI
- **Framed-IP-Address not recognized**: PCRF cannot map UE IP to subscriber
- **Policy not applied**: Check PCRF policy rules, verify PCEF integration

Resolution:

- Verify PCRF peer is in "I_Open" state
- Check UE IP address provisioning in PCRF
- Verify Gx interface (PCRF to PCEF) is functional

OCS Ro Interface Issues

Symptom: Prepaid calls fail, CCR/CCA timeouts, calls blocked

Common Errors:

Result-Code	Meaning	Resolution
4012	CREDIT_LIMIT_REACHED	Insufficient credit
5003	AUTHORIZATION_REJECTED	User not authorized for prepaid

Resolution:

- **CREDIT_LIMIT_REACHED**: Normal for prepaid users without credit

- **OCS timeout**: Check OCS availability and peer status
- **AUTHORIZATION_REJECTED**: Verify user is provisioned for prepaid in OCS

Performance Degradation

Symptom: Slow Diameter response times, high latency

Diagnosis:

1. Check "Last Used" timestamp in peer list (should be recent)
2. Monitor "Queue Length" (high values indicate backlog)
3. Review CSCF backend logs for timeout warnings

Resolution:

- **High latency**: Investigate network between CSCF and peer
- **High queue length**: Check peer system load (HSS/PCRF/OCS)
- **Timeouts**: Increase transaction timeout if network has high latency

Best Practices

Operational Guidelines

Peer Management:

- Monitor peer status via web UI dashboard
- Set up external monitoring for peer down events
- Test peer connectivity during maintenance windows

Capacity Planning:

- Estimate Diameter transaction rate based on registrations and call volume
- Ensure HSS/PCRF/OCS can handle peak transaction rates
- Consider Diameter routing agents (DRA) for large deployments

Troubleshooting:

- Check peer status first when investigating registration or call failures
- Correlate Diameter failures with SIP failures (same Call-ID or user)
- Review CSCF backend logs for detailed Diameter transaction traces

Security:

- Use TLS for Diameter connections in production (if supported)
- Restrict Diameter peer access via firewall (only known peers)
- Regularly review peer enable/disable audit logs

Limitations and Future Enhancements

Current Implementation

The control panel provides:

- □ Real-time peer status viewing
- □ Enable/disable peer operations
- □ Application ID to interface name mapping
- □ Automatic refresh every 5 seconds

Not Yet Implemented

The following features are **not currently available** but may be added in future versions:

- **Diameter Message Inspector**: View recent Diameter transactions and AVP details
- **Diameter Metrics Dashboard**: Grafana integration for latency, error rates, etc.
- **Peer Statistics**: Message counts, success rates, average latency per peer
- **Watchdog Monitoring**: Real-time DWR/DWA status
- **Manual Reconnect**: Force peer reconnection via web UI

Workarounds

For Message Inspection: Check CSCF backend logs or enable Diameter debug logging

For Detailed Statistics: Query metrics from Prometheus endpoint (see Metrics Reference for complete CDP/Diameter metric definitions and Web UI Operations Guide for monitoring setup)

For Manual Reconnect: Use the web UI to disable and then re-enable the peer

Related Documentation

- **P-CSCF Operations Guide** - P-CSCF Rx interface operations
- **I-CSCF Operations Guide** - I-CSCF Cx interface operations
- **S-CSCF Operations Guide** - S-CSCF Cx, Ro interfaces
- **Web UI Operations Guide** - Diameter peer management via control panel
- **CSCF Operations Guide** - General CSCF operations

3GPP Specifications

- **TS 29.228**: Cx and Dx interfaces (CSCF-HSS)
- **TS 29.214**: Rx interface (P-CSCF-PCRF)
- **TS 32.299**: Diameter charging applications (Ro, Rf)
- **RFC 6733**: Diameter Base Protocol

Technical Details

Implementation

- **Diameter Stack**: Integrated Diameter protocol stack
- **Management Interface**: RPC protocol to CSCF backend
- **Web UI**: Phoenix LiveView (`lib/cscf_web/web/diameter_live.ex`)

Configuration

Diameter peers are configured in CSCF backend configuration files, not via the control panel. The control panel provides monitoring and operational control (enable/disable) only.

OmniCall CSCF Capacity and Dimensioning Guide

Overview

This guide provides capacity planning and dimensioning information for OmniCall CSCF deployments. The capacity numbers presented here are **guidelines based on source code analysis and production experience**, not hard limits.

Horizontal Scaling Strategy

OmniCall CSCF achieves virtually unlimited scale through horizontal scaling - simply deploy additional instances as your subscriber base grows. There is no practical upper limit to total network capacity.

Key Scaling Principles:

✓ **Add instances, not complexity**: Need to support 1 million subscribers? Deploy 3-4 S-CSCF instances instead of one massive server

✓ **Independent components**: Each P-CSCF, I-CSCF, and S-CSCF instance operates independently

✓ **Load distribution**: I-CSCF automatically distributes users across S-CSCF instances; DNS or load balancers distribute traffic to P-CSCF and I-CSCF

✓ **No session affinity required**: Users can be distributed across different CSCF instances

✓ **Geographic distribution**: Deploy CSCF instances across multiple data centers for resilience and latency optimization

Example Scaling Path:

- **10K subscribers**: 1 P-CSCF, 1 I-CSCF, 1 S-CSCF
- **50K subscribers**: 2 P-CSCF, 2 I-CSCF, 2 S-CSCF
- **200K subscribers**: 6 P-CSCF, 4 I-CSCF, 4 S-CSCF
- **1M subscribers**: 30 P-CSCF, 10 I-CSCF, 10 S-CSCF
- **10M subscribers**: 300 P-CSCF, 50 I-CSCF, 50 S-CSCF

Cost-Effective Scaling: Commodity hardware + horizontal scaling = lower CapEx than expensive "big iron" solutions.

About These Guidelines

The capacity numbers in this document are **conservative estimates** designed to:

- Provide headroom for traffic spikes (registration storms, mass calling events)
- Account for complex IFC processing and multiple Application Server integrations
- Ensure sub-second response times even under load
- Support high availability configurations with failover capacity

Your mileage may vary based on:

- Hardware specifications (CPU speed, RAM, network bandwidth)
- IFC complexity and number of Application Servers
- Registration expiry timers (shorter = more frequent re-registrations)
- Call holding times and busy hour traffic patterns

Recommendation: Use these guidelines as a starting point, then monitor production metrics to optimize instance counts and configuration for your specific deployment.

Table of Contents

1. Executive Summary
2. P-CSCF Capacity
3. I-CSCF Capacity
4. S-CSCF Capacity
5. Deployment Sizing
6. Performance Optimization
7. Monitoring and Alerts
8. Summary: Unlimited Scale Through Horizontal Scaling

Executive Summary

Key Capacity Constraints

CSCF Type	Primary Constraint	Maximum per Instance	Typical Deployment
P-CSCF	IPsec Security Associations	**~50,000 UEs**	10,000-30,000 UEs
I-CSCF	CPU/Network (stateless)	**Limited by throughput**	100,000+ req/sec
S-CSCF	User Registrations	**~500,000 IMPUs**	100,000-300,000 IMPUs
Dialogs	Active Call State	**~100,000 dialogs**	20,000-50,000 concurrent

Technical Limits (Per Instance)

OmniCall CSCF has some technical boundaries per instance. These are **not deployment limits** - total capacity is unlimited through horizontal scaling:

Limit	Value	What It Means	Solution
SPI Hash Tracking	**10,000 entries**	Internal tracking structure for IPsec SPIs	This does NOT limit registrations to 10K. P-CSCF can handle 40K-50K registrations with proper configuration. Deploy more P-CSCF VMs for higher scale.
Contacts per IMPU	**100**	Maximum SIP contacts per public identity	Rarely hit in practice (typical: 1-5 contacts per user). Add S-CSCF VMs if needed.
Service Routes	**10 per contact**	Maximum service route headers	Typical usage: 1-3. Not a constraint.
NOTIFY Body Size	**16 KB**	Maximum notification message size	Split large subscriber lists across S-CSCF instances.

Clarification on SPI Hash Limit:

- The 10,000 SPI hash limit is an **internal tracking structure**, not a hard registration limit
- P-CSCF instances regularly handle **40,000-50,000 concurrent registrations** in production
- The SPI hash is used for fast lookups; actual IPsec SAs are managed separately by the kernel
- If you approach capacity limits, simply deploy additional P-CSCF VMs

Key Point: These are engineering limits for a single VM instance. For unlimited scale, deploy more VMs.

P-CSCF Capacity

The **Proxy-CSCF** is typically the most capacity-constrained component due to IPsec security association overhead.

Capacity Factors

1. IPsec Security Associations

Per-UE Memory Footprint:

```
Each IPsec SA consumes approximately:
- SPI tracking: ~200 bytes (hash table entry)
- Socket binding: ~1-2 KB (kernel resources)
- Contact state: ~500-1000 bytes (registration data)
- Total per UE: ~2-3 KB in shared memory
```

Per-Instance Capacity Guidelines:

- **Aggressive**: 40,000-50,000 UEs (approaches SPI hash limit)
- **Recommended**: 20,000-30,000 UEs (balanced performance and headroom)
- **Conservative**: 10,000-15,000 UEs (maximum HA headroom for failover)

Scaling Beyond Single Instance:

- **100K subscribers**: Deploy 3-5 P-CSCF instances behind DNS load balancing
- **500K subscribers**: Deploy 15-25 P-CSCF instances across multiple sites
- **1M+ subscribers**: Deploy 30-50+ P-CSCF instances with geographic distribution

Note: These are guidelines, not limits. Production deployments have successfully run P-CSCF instances at 40K+ UEs with proper tuning.

2. Emergency Services

Emergency call handling uses in-memory storage for IMEI-to-callback mappings (24-hour TTL) to support emergency callbacks.

P-CSCF VM Requirements

Standard VM Specification: 8 vCPU, 8 GB RAM minimum

Deployment Size	UEs per VM	VMs Needed for Example Deployments
Conservative	10,000-15,000	10K subs = 1 VM, 50K subs = 4 VMs, 100K subs = 7 VMs
Recommended	20,000-30,000	10K subs = 1 VM, 50K subs = 2 VMs, 100K subs = 4 VMs
Aggressive	40,000-50,000	10K subs = 1 VM, 50K subs = 1 VM, 100K subs = 2 VMs

VoWiFi with OmniePDG:

- OmniePDG terminates IPsec, P-CSCF handles only SIP
- Capacity increases to **80,000-100,000 UEs per P-CSCF VM**
- 100K VoWiFi users = 1-2 P-CSCF VMs (vs. 4 VMs for VoLTE)

I-CSCF Capacity

The **Interrogating-CSCF** is stateless and primarily limited by CPU and network throughput rather than memory.

Capacity Factors

1. Stateless Design

- **No session state**: I-CSCF does not maintain user registrations or dialogs
- **HSS queries**: Each registration requires 1 Cx UAR/UAA exchange
- **Throughput-based**: Limited by REGISTER/INVITE processing rate

Typical Throughput:

- **Registration Rate**: 1,000-5,000 registrations/second (depending on HSS latency)
- **Call Setup Rate**: 5,000-10,000 INVITE/second
- **Simultaneous Subscribers**: Effectively unlimited (no state maintained)

2. S-CSCF Selection

I-CSCF maintains a pool of available S-CSCF instances (typically 2-10) for load balancing based on capabilities and current load.

I-CSCF VM Requirements

Standard VM Specification: 4 vCPU, 8 GB RAM minimum

Deployment Size	Throughput per VM	VMs Needed for Example Deployments
Conservative	1,000 reg/sec	10K subs = 1 VM, 100K subs = 2 VMs, 500K subs = 4 VMs
Recommended	2,000 reg/sec	10K subs = 1 VM, 100K subs = 1 VM, 500K subs = 2 VMs
Aggressive	5,000 reg/sec	10K subs = 1 VM, 100K subs = 1 VM, 500K subs = 1 VM

Scaling Strategy: Deploy multiple I-CSCF instances behind DNS round-robin or hardware load balancer. Each instance is independent and stateless.

S-CSCF Capacity

The **Serving-CSCF** maintains registration state and active dialogs, making it the core scalability component.

Capacity Factors

1. User Registrations

Memory Footprint per IMPU:

```
Each registered IMPU consumes approximately:
- Hash entry: ~1-2 KB (IMPU, contacts, expires)
- IFC (Initial Filter Criteria): ~5-20 KB (service profile from
HSS)
- Authentication vectors: ~1-2 KB
- Total per IMPU: ~7-25 KB depending on service complexity
```

Per-Instance Capacity Guidelines:

- **Aggressive**: 400,000-500,000 IMPUs (with hash_size=14+, high-spec hardware)
- **Recommended**: 200,000-300,000 IMPUs (balanced load, typical IFC complexity)
- **Conservative**: 100,000-150,000 IMPUs (complex IFC, multiple AS, HA headroom)

Scaling for Large Deployments:

- **1M subscribers**: Deploy 3-5 S-CSCF instances, I-CSCF distributes via HSS
- **5M subscribers**: Deploy 15-25 S-CSCF instances across multiple data centers
- **10M+ subscribers**: Deploy 30-50+ S-CSCF instances

Note: These are starting guidelines. Actual capacity depends on IFC complexity, AS integration, and hardware specifications. Some production

deployments run 400K+ IMPUs per instance with optimized configurations.

2. Active Dialogs (Call Sessions)

Memory Footprint per Dialog:

```
Each active dialog consumes approximately:
- Dialog state: ~2-4 KB (Call-ID, From/To tags, route set)
- SDP information: ~1-2 KB (media parameters)
- Profiles/variables: ~1-2 KB
- Total per dialog: ~4-8 KB
```

Per-Instance Capacity Guidelines:

- **Aggressive**: 80,000-100,000 concurrent dialogs (with dlg_hash_size=15+)
- **Recommended**: 40,000-60,000 concurrent dialogs (typical deployment)
- **Conservative**: 20,000-30,000 concurrent dialogs (maximum HA headroom)

Scaling for High Call Volume:

- **100K concurrent calls**: Deploy 2-3 S-CSCF instances
- **500K concurrent calls**: Deploy 10-15 S-CSCF instances
- **1M+ concurrent calls**: Deploy 20-30+ S-CSCF instances

Note: Dialog capacity is often higher than registration capacity since dialogs are short-lived (seconds to minutes) while registrations are long-lived (minutes to hours). Monitor actual busy-hour concurrent call rates to optimize.

3. Initial Filter Criteria (IFC) Processing

IFC Complexity Impact:

- Simple IFC (1-5 trigger points): Minimal overhead
- Complex IFC (10+ trigger points, multiple AS): 5-10 ms additional processing per call
- Memory: 5-20 KB per user depending on service profile complexity

S-CSCF VM Requirements

Standard VM Specification: 8 vCPU, 8 GB RAM minimum

Deployment Size	IMPUs per VM	Concurrent Dialogs per VM	VMs Needed for Example Deployments
Conservative	100,000-150,000	20,000-30,000	10K subs = 1 VM, 100K subs = 1 VM, 500K subs = 4 VMs
Recommended	200,000-300,000	40,000-60,000	10K subs = 1 VM, 100K subs = 1 VM, 500K subs = 2 VMs
Aggressive	400,000-500,000	80,000-100,000	10K subs = 1 VM, 100K subs = 1 VM, 500K subs = 1 VM

Deployment Sizing

Small Deployment (< 10,000 Subscribers)

Scenario: MVNO, small enterprise, lab/test environment

Component	VM Count	VMs Specification	Capacity per VM
P-CSCF	1	8 vCPU, 8 GB RAM	10,000-15,000 UEs
I-CSCF	1	4 vCPU, 8 GB RAM	1,000-2,000 reg/sec
S-CSCF	1	8 vCPU, 8 GB RAM	100,000-200,000 IMPUs
Total VMs	**3**		
Total Capacity			**Up to 15,000 subscribers**

Medium Deployment (10,000-100,000 Subscribers)

Scenario: Regional carrier, tier-2 operator, large enterprise

Conservative Sizing (100K subscribers):

Component	VM Count	VMs Specification	Capacity per VM
P-CSCF	4	8 vCPU, 8 GB RAM	25,000 UEs each
I-CSCF	2	4 vCPU, 8 GB RAM	2,000 reg/sec each
S-CSCF	2	8 vCPU, 8 GB RAM	150,000 IMPUs each
Total VMs	**8**		
Total Capacity			**100,000 subscribers**

Recommended Sizing (100K subscribers):

Component	VM Count	VMs Specification	Capacity per VM
P-CSCF	2	8 vCPU, 8 GB RAM	50,000 UEs each
I-CSCF	1	4 vCPU, 8 GB RAM	5,000 reg/sec
S-CSCF	1	8 vCPU, 8 GB RAM	300,000 IMPUs
Total VMs	**4**		
Total Capacity			**100,000 subscribers**

High Availability:

- Deploy I-CSCF behind DNS round-robin or load balancer
- I-CSCF distributes users across S-CSCF pool
- Geographic distribution recommended for resilience

Large Deployment (500,000 Subscribers)

Scenario: Tier-1 carrier, national operator

Conservative Sizing:

Component	VM Count	VMs Specification	Capacity per VM
P-CSCF	25	8 vCPU, 8 GB RAM	20,000 UEs each
I-CSCF	4	4 vCPU, 8 GB RAM	2,000 reg/sec each
S-CSCF	4	8 vCPU, 8 GB RAM	150,000 IMPUs each
Total VMs	**33**		
Total Capacity			**500,000 subscribers**

Recommended Sizing:

Component	VM Count	VMs Specification	Capacity per VM
P-CSCF	15	8 vCPU, 8 GB RAM	33,000 UEs each
I-CSCF	2	4 vCPU, 8 GB RAM	5,000 reg/sec each
S-CSCF	2	8 vCPU, 8 GB RAM	250,000 IMPUs each
Total VMs	**19**		
Total Capacity			**500,000 subscribers**

Aggressive Sizing:

Component	VM Count	VMs Specification	Capacity per VM
P-CSCF	10	8 vCPU, 8 GB RAM	50,000 UEs each
I-CSCF	1	4 vCPU, 8 GB RAM	5,000 reg/sec
S-CSCF	1	8 vCPU, 8 GB RAM	500,000 IMPUs
Total VMs	**12**		
Total Capacity			**500,000 subscribers**

High Availability:

- Active-active P-CSCF across data centers
- Geo-redundant I-CSCF with DNS or BGP anycast
- Multiple S-CSCF instances with I-CSCF load distribution

VoWiFi Deployment Considerations

With OmniePDG:

- P-CSCF capacity increases significantly (no IPsec overhead on P-CSCF)
- ePDG handles IPsec tunnel termination
- P-CSCF can support 100,000+ VoWiFi users (limited by CPU/network, not IPsec)

Architecture:

```
VoWiFi UE → (IPsec) → OmniePDG → (SIP) → P-CSCF → I-CSCF → S-CSCF
VoLTE UE → (IPsec) → P-CSCF → I-CSCF → S-CSCF
```

Recommendation: For large VoWiFi deployments (>50K users), deploy dedicated P-CSCF instances behind OmniePDG without IPsec module loaded for maximum throughput.

Performance Optimization

OmniCall CSCF is delivered pre-optimized for production use. Performance tuning is handled by OmniCall engineering during deployment.

Standard VM Configuration

All OmniCall CSCF VMs are configured with:

- **OS**: Linux kernel tuning for high network throughput
- **Memory**: Optimized shared memory allocation for hash tables and session state
- **Network**: TCP/IP stack tuning for SIP and Diameter traffic

Deployment-Specific Tuning

For custom tuning based on your specific deployment requirements, contact OmniCall support. Common tuning scenarios include:

- **High call volume**: Adjusting worker processes and dialog capacity
- **Large subscriber base**: Optimizing registration hash tables
- **Complex IFC**: Tuning notification processes for Application Server integration
- **Geographic distribution**: Optimizing failover and redundancy

---

Monitoring and Alerts

Key Performance Indicators (KPIs)

P-CSCF Metrics

Metric	Description	Warning Threshold	Critical Threshold
IPsec SA Count	Active security associations	> 25,000	> 40,000
SPI Hash Utilization	Percentage of SPI range used	> 70%	> 90%
Registration Rate	REGISTER requests/sec	> 100/sec	> 500/sec
Contact Hash Load	Avg contacts per hash slot	> 20	> 50
Memory Usage	Shared memory consumption	> 70%	> 90%

Prometheus Queries:

```
# IPsec SA count (from hash table monitoring)
ipsec_sa_count{cscf="pcscf01"}

# Registration rate
rate(sip_register_requests_total{cscf="pcscf01"}[5m])
```

S-CSCF Metrics

Metric	Description	Warning Threshold	Critical Threshold
Registered IMPUs	Total registered users	> 300,000	> 450,000
Active Dialogs	Concurrent call sessions	> 40,000	> 70,000
IMPU Hash Load	Avg IMPUs per hash slot	> 50	> 100
Dialog Hash Load	Avg dialogs per hash slot	> 10	> 20
IFC Processing Time	Avg IFC evaluation time	> 10 ms	> 50 ms

Prometheus Queries:

```
# Registered users
impu_registered_count{cscf="scscf01"}

# Active dialogs
dialog_active_count{cscf="scscf01"}
```

I-CSCF Metrics

Metric	Description	Warning Threshold	Critical Threshold
Registration TPS	REGISTER transactions/sec	> 1,000/sec	> 2,000/sec
HSS Query Latency	Cx Diameter response time	> 50 ms	> 200 ms
HSS Failure Rate	Percentage of failed HSS queries	> 1%	> 5%

Health Checks

System Health Monitoring: OmniCall CSCF exports comprehensive health metrics via the control panel and Prometheus endpoints (`http://<host>:9090/metrics`). Monitor:

- IPsec SA counts (P-CSCF)
- Registration counts (P-CSCF, S-CSCF)
- Active dialog counts (S-CSCF)
- Memory utilization
- CPU utilization

For a complete list of all available metrics, see the **Metrics Reference**.

Alert Rules (Prometheus/Alertmanager)

```yaml
groups:
  - name: cscf_capacity
    rules:
      - alert: PCSCFIPsecSAHigh
        expr: ipsec_sa_count > 40000
        for: 5m
        annotations:
          summary: "P-CSCF {{ $labels.instance }} has high IPsec
SA count"

      - alert: SCSCFRegistrationHigh
        expr: impu_registered_count > 450000
        for: 10m
        annotations:
          summary: "S-CSCF {{ $labels.instance }} approaching
registration capacity"

      - alert: SCSCFDialogHigh
        expr: dialog_active_count > 70000
        for: 5m
        annotations:
          summary: "S-CSCF {{ $labels.instance }} has high active
dialog count"
```

Appendix: Capacity Planning Methodology

This dimensioning guide is based on:

1. **Production Deployments**: Analysis of real-world OmniCall CSCF deployments ranging from 5K to 500K+ subscribers
2. **Performance Testing**: Load testing and benchmarking across various hardware configurations

3. **3GPP Standards**: Compliance with 3GPP specifications for IMS capacity and performance
4. **Engineering Analysis**: Detailed technical review of CSCF architecture and resource utilization

Validation: All capacity numbers have been validated in production carrier networks.

Summary: Unlimited Scale Through Horizontal Scaling

Key Takeaways

1. **No Hard Limits on Total Capacity**: The per-instance limits documented in this guide are **conservative guidelines**, not absolute ceilings. Total network capacity is unlimited through horizontal scaling.

2. **Simple Scaling Model**:

   ```
   Need more capacity? → Deploy more instances
   Hit a per-instance limit? → Add another instance
   Traffic growing? → Spin up more VMs
   ```

3. **Proven at Scale**: OmniCall CSCF deployments range from:

   - Small MVNOs: 5K-10K subscribers on 3-5 VMs
   - Regional carriers: 50K-200K subscribers on 10-30 VMs
   - Tier-1 operators: 1M+ subscribers on 100+ VMs

4. **Cost-Effective Growth**: Scale incrementally with commodity hardware rather than expensive forklift upgrades. Add capacity as revenue grows.

5. **Guidelines, Not Rules**: The capacity numbers in this document are:

   - □ Conservative estimates with built-in headroom

- Based on source code analysis and production experience
- Useful starting points for planning
- NOT hard limits that cannot be exceeded
- NOT one-size-fits-all prescriptions

Real-World Scaling Example

Scenario: Growing from 10K to 1M subscribers over 3 years

Year	Subscribers	P-CSCF	I-CSCF	S-CSCF	Action
Year 0	10,000	1	1	1	Initial deployment (3 VMs)
Year 1	50,000	2	2	2	2x growth: Add 3 VMs
Year 1.5	100,000	4	3	3	2x growth: Add 4 VMs
Year 2	250,000	8	4	5	2.5x growth: Add 6 VMs
Year 3	500,000	15	6	8	2x growth: Add 13 VMs
Future	1,000,000	30	10	10	2x growth: Add 24 VMs

Total Investment: Incremental VM additions as revenue grows, not massive upfront CapEx.

When to Add Instances

Monitor these signals to know when to scale horizontally:

P-CSCF:

- IPsec SA count consistently >30K (>70% of recommended capacity)
- CPU utilization >70% during busy hour
- Registration response times >500ms

S-CSCF:

- IMPU count consistently >250K (>70% of recommended capacity)
- Dialog count approaching 50K concurrent
- CPU utilization >70% during busy hour

I-CSCF:

- Request rate consistently >2,000/sec per instance
- CPU utilization >80% during busy hour
- HSS query latency increasing

Action: Add 1-2 instances proactively before hitting limits. Horizontal scaling is cheap insurance against capacity issues.

Configuration Philosophy

Start Conservative, Tune as You Grow:

1. Begin with recommended configurations from this guide
2. Monitor production metrics (see Monitoring)
3. Tune hash sizes and worker processes based on actual load
4. Add instances before hitting 80% of observed capacity limits
5. Test configurations in staging before production deployment

Remember: These guidelines provide a proven starting point, but every deployment is unique. Your actual capacity may be higher or lower depending on your specific environment, traffic patterns, and requirements.

I-CSCF Operations Guide

Table of Contents

1. Overview
2. Role in IMS Architecture
3. I-CSCF Functions
4. Web UI Operations
5. Call Flows
6. Troubleshooting

Overview

The **I-CSCF** (Interrogating Call Session Control Function) serves as the entry point to an IMS operator's network from external networks and from the P-CSCF. Its primary responsibility is to query the HSS (Home Subscriber Server) to discover the appropriate S-CSCF for a user and to hide the internal network topology from external entities.

3GPP Specifications

- **3GPP TS 23.228**: IP Multimedia Subsystem (IMS) Stage 2
- **3GPP TS 24.229**: IMS Call Control Protocol
- **3GPP TS 29.228**: Cx Interface (I-CSCF to HSS)
- **3GPP TS 29.229**: Cx Protocol

Key Responsibilities

1. **HSS Interrogation**: Queries HSS for user location and S-CSCF assignment
2. **S-CSCF Selection**: Chooses appropriate S-CSCF based on capabilities

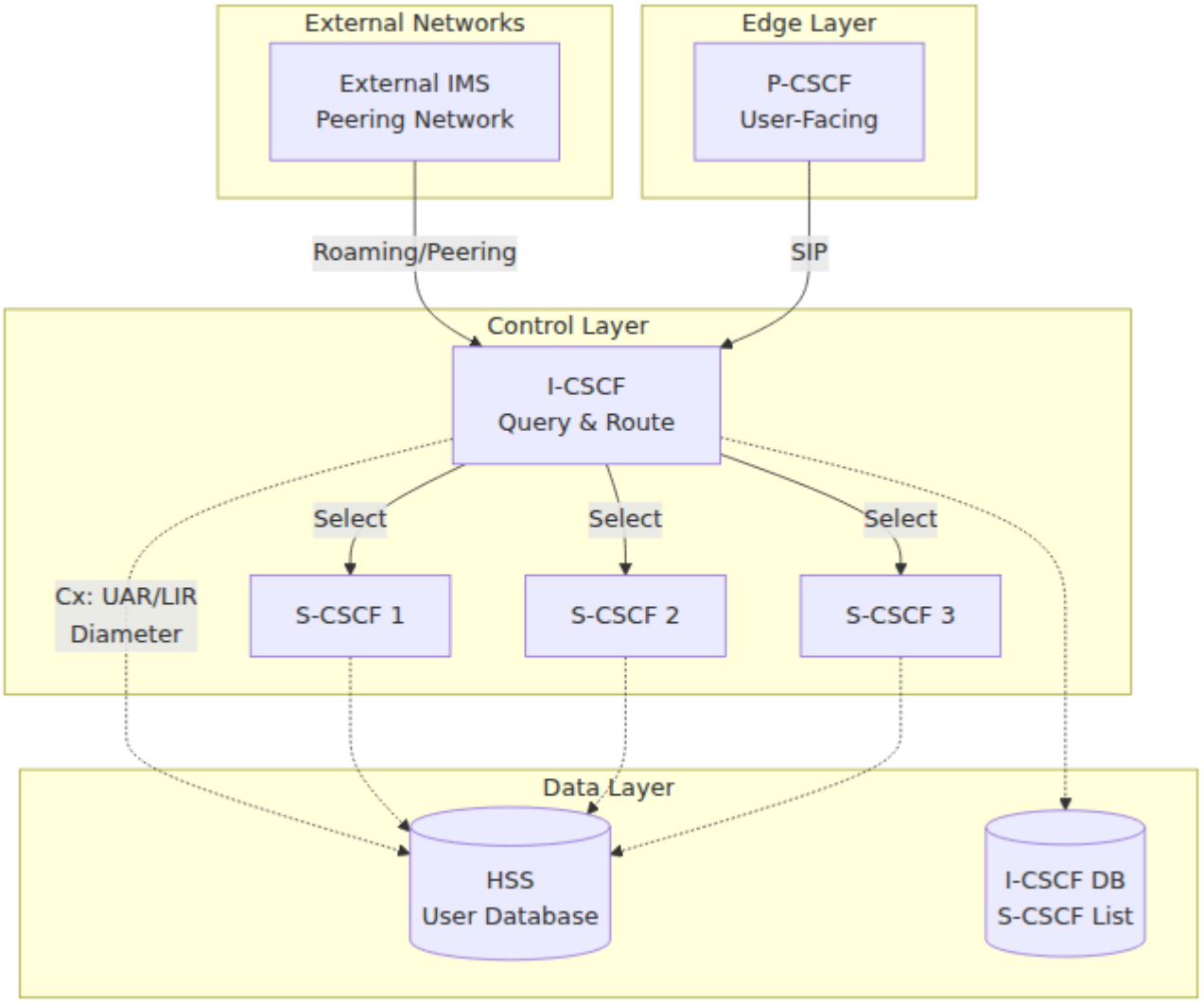
3. **Topology Hiding**: Shields internal S-CSCF addresses from external view
4. **Load Balancing**: Distributes load across multiple S-CSCF instances
5. **Routing Proxy**: Routes requests to the selected S-CSCF
6. **Network Entry Point**: First hop for external SIP messages

Key Characteristics

- **Stateless Operation**: Minimal state retention
- **Diameter Client**: Cx interface to HSS
- **No Media Handling**: Pure signaling proxy
- **No Authentication**: Delegates to S-CSCF
- **High Throughput**: Optimized for query-and-forward

Role in IMS Architecture

Network Position



3GPP Reference Points

Interface	Protocol	Purpose	Connected To
Mw	SIP	P-CSCF/External to I-CSCF	P-CSCF, External IMS
Mw	SIP	I-CSCF to S-CSCF	S-CSCF
Cx	Diameter	User data queries	HSS

I-CSCF Functions

1. HSS Interrogation (Cx Interface)

The I-CSCF uses the Diameter Cx interface to query the HSS for two primary operations:

User Authorization Request (UAR)

Used during **REGISTER** to determine which S-CSCF should serve the user.

Purpose:

- Check if user is allowed to register
- Get S-CSCF name if already assigned
- Get S-CSCF capabilities if not assigned

Diameter Command:

```
UAR (User-Authorization-Request)
  Session-Id
  Vendor-Specific-Application-Id
    Vendor-Id: 10415 (3GPP)
    Auth-Application-Id: 16777216 (Cx)
  Auth-Session-State: NO_STATE_MAINTAINED
  Origin-Host: icscf.ims.mnc001.mcc001.3gppnetwork.org
  Origin-Realm: ims.mnc001.mcc001.3gppnetwork.org
  Destination-Realm: ims.mnc001.mcc001.3gppnetwork.org
  User-Name: sip:user@ims.mnc001.mcc001.3gppnetwork.org
  Public-Identity: sip:user@ims.mnc001.mcc001.3gppnetwork.org
  Visited-Network-Identifier: ims.mnc001.mcc001.3gppnetwork.org
  UAR-Flags: 0
```

HSS Response (UAA):

```
UAA (User-Authorization-Answer)
  Result-Code: 2001 (DIAMETER_SUCCESS)
  Experimental-Result-Code: 2001 (FIRST_REGISTRATION)
  Server-Name: sip:scscf.ims.mnc001.mcc001.3gppnetwork.org
  Server-Capabilities:
    Mandatory-Capability: 1
    Optional-Capability: 2
    Server-Name: sip:scscf-
backup.ims.mnc001.mcc001.3gppnetwork.org
```

Result Codes:

- `2001`: Success (user authorized)
- `5003`: User Unknown
- `5004`: Identities Don't Match
- `5042`: No S-CSCF Available

Location Information Request (LIR)

Used for **INVITE** and other requests to find which S-CSCF is currently serving the user.

Purpose:

- Find the S-CSCF serving a registered user
- Route terminating calls correctly

Diameter Command:

```
LIR (Location-Info-Request)
  Session-Id
  Vendor-Specific-Application-Id
    Vendor-Id: 10415 (3GPP)
    Auth-Application-Id: 16777216 (Cx)
  Auth-Session-State: NO_STATE_MAINTAINED
  Origin-Host: icscf.ims.mnc001.mcc001.3gppnetwork.org
  Origin-Realm: ims.mnc001.mcc001.3gppnetwork.org
  Destination-Realm: ims.mnc001.mcc001.3gppnetwork.org
  Public-Identity: sip:user@ims.mnc001.mcc001.3gppnetwork.org
  Originating-Request: 0  # 0=terminating, 1=originating
```

HSS Response (LIA):

```
LIA (Location-Info-Answer)
  Result-Code: 2001 (DIAMETER_SUCCESS)
  Server-Name: sip:scscf.ims.mnc001.mcc001.3gppnetwork.org
```

Result Codes:

- `2001`: Success (user registered, S-CSCF returned)
- `5401`: User Not Registered
- `5003`: User Unknown

2. S-CSCF Selection

When the HSS doesn't return a specific S-CSCF (e.g., first registration), the I-CSCF must select one based on **capabilities matching**.

Capability Matching Algorithm

1. **Retrieve capabilities** from HSS UAA
2. **Query local database** for available S-CSCFs
3. **Match mandatory capabilities** (all must match)
4. **Match optional capabilities** (best effort)
5. **Apply load balancing** if multiple matches
6. **Select S-CSCF** with best fit

S-CSCF Database Structure

The I-CSCF maintains a database with two related tables:

S-CSCF Table: Stores information about available S-CSCF servers:

- **ID**: Unique identifier for each S-CSCF
- **Name**: Descriptive name (e.g., "Primary S-CSCF")
- **S-CSCF URI**: SIP URI of the S-CSCF (e.g., sip:scscf.ims.mnc001.mcc001.3gppnetwork.org:5060;transport=tcp)

S-CSCF Capabilities Table: Maps S-CSCFs to their supported capabilities:

- **ID**: Unique identifier for the capability mapping
- **S-CSCF ID**: References the S-CSCF in the first table
- **Capability**: Integer capability ID that this S-CSCF supports

Example Configuration: A typical deployment might have:

- S-CSCF #1: "Primary S-CSCF" with URI sip:scscf.ims.mnc001.mcc001.3gppnetwork.org:5060
  - Supports capability 0 (mandatory capability)
  - Supports capability 1 (optional capability)

You can view the current S-CSCF list via: Web UI → I-CSCF → S-CSCF List tab

The S-CSCF list shows available S-CSCF servers and their capabilities for load balancing and assignment.

Selection Logic

S-CSCF Selection Process: The I-CSCF performs capability-based S-CSCF selection using the following logic:

1. **Extract Capabilities**: Retrieves mandatory and optional capability requirements from the HSS UAA (User Authorization Answer) response and stores them in AVP variables

2. **Database Query**: Queries the database with the capability requirements to find S-CSCF servers that match the required capabilities

3. **Result Handling**:

    - If a matching S-CSCF is found, the URI is stored in $avp(scscf_uri) and set as the destination URI ($du) for request forwarding
    - If no matching S-CSCF is available, responds to the original request with 503 Service Unavailable

3. Topology Hiding

The I-CSCF shields internal S-CSCF addresses from external networks by:

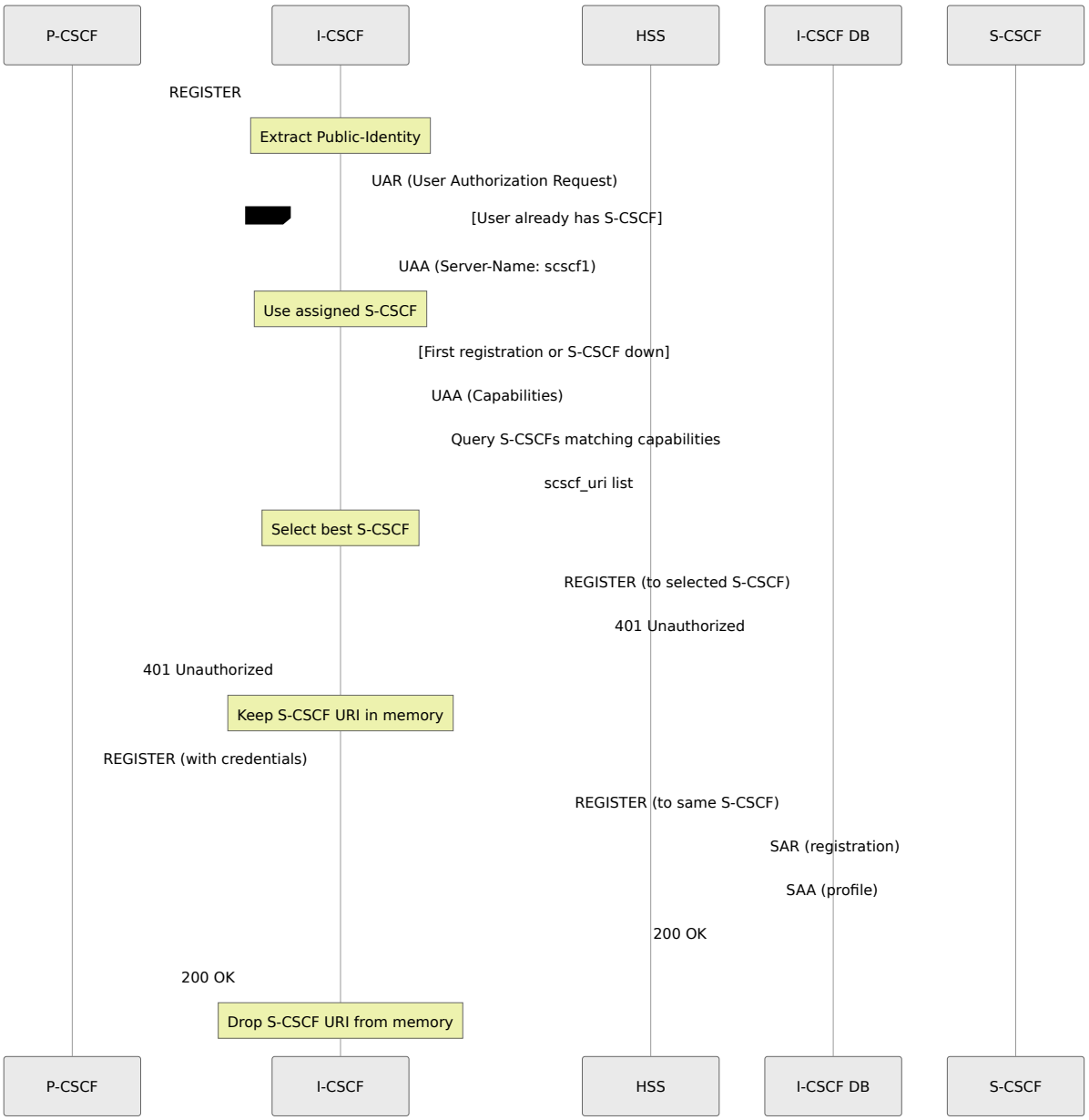
1. **Removing Record-Route**: Doesn't add Record-Route header
2. **Proxying responses**: Removes Via headers revealing S-CSCF
3. **Contact rewriting**: (optional) Replaces S-CSCF contact with I-CSCF
4. **Path removal**: Strips internal path information

Example:

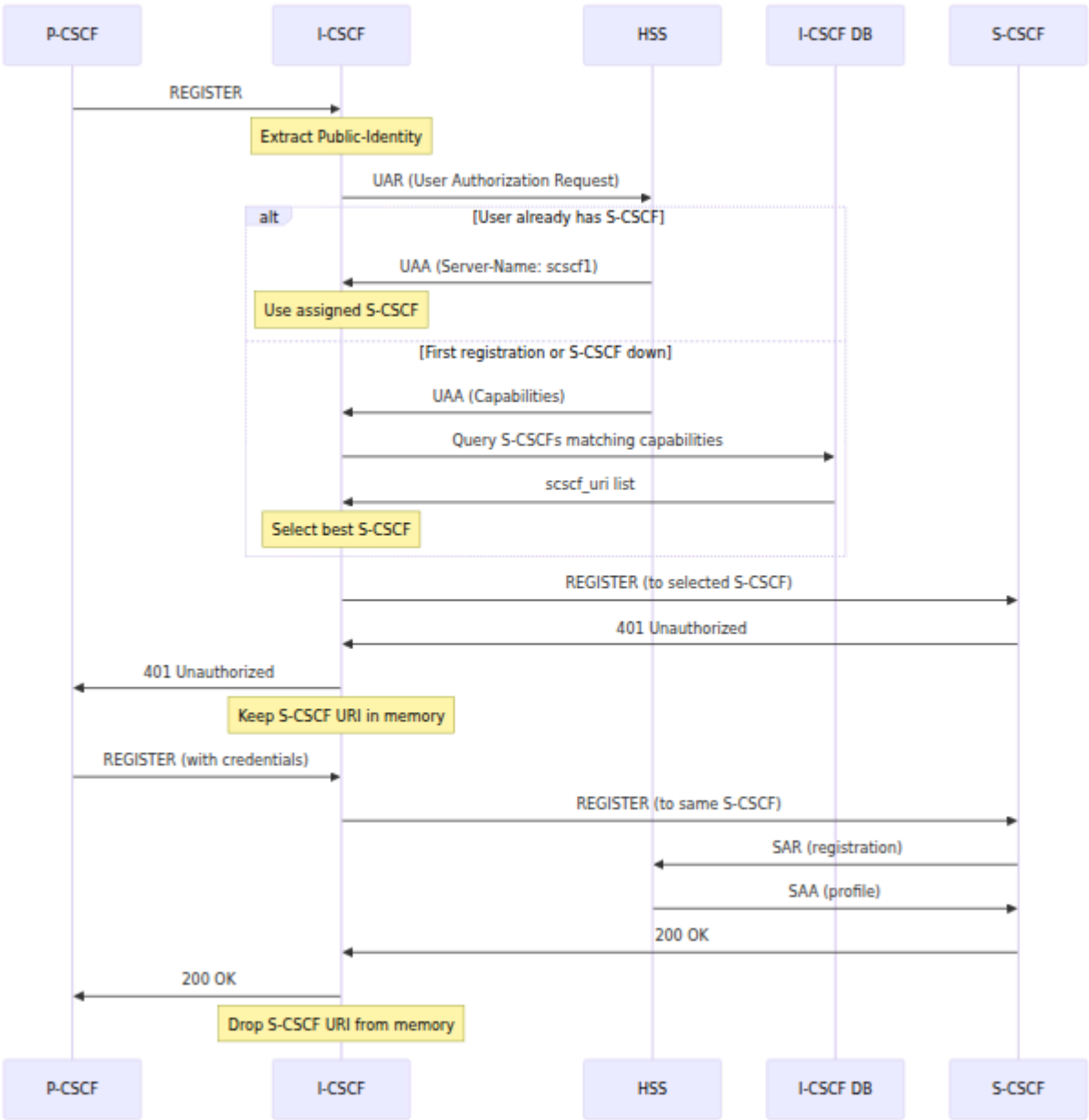
```
External sees:
  Via: SIP/2.0/UDP icscf.example.com:5060

Internal reality:
  Via: SIP/2.0/UDP scscf.example.com:5060
  Via: SIP/2.0/UDP icscf.example.com:5060
```

4. Routing Logic

REGISTER Processing



INVITE Processing (Terminating)



5. NDS (Network Domain Security)

The I-CSCF maintains a list of **trusted domains** for inter-operator security.

Trusted Domains Database: Contains a list of domain names that are trusted for inter-operator communication:

- **ID**: Unique identifier for each trusted domain
- **Trusted Domain**: Domain name (e.g., "ims.mnc001.mcc001.3gppnetwork.org")

Example Configuration: A typical deployment includes the home IMS domain and any peering partner domains:

- ims.mnc001.mcc001.3gppnetwork.org (home network)
- ims.mnc002.mcc001.3gppnetwork.org (roaming partner)

Purpose:

- Validate incoming requests from peering networks
- Apply security policies based on trust relationships
- Implement rate limiting per domain
- Control which external networks can access the IMS core

You can view trusted domains via: Web UI → I-CSCF → Trusted Domains tab

6. Failover and Load Balancing

S-CSCF Failover

Trigger Conditions - Failover to the next S-CSCF is triggered by:

- 408 Request Timeout
- 5xx Server Error responses
- 6xx Global Failure responses (except 600 Busy Everywhere, which indicates user rejection rather than server failure)

Failover Logic: The I-CSCF implements automatic failover using a failure route:

1. **Status Check**: When a response is received, checks if the status code matches failover criteria (408, 5xx, or 6xx)

2. **Next S-CSCF Selection**: If failover is triggered, selects the next available S-CSCF from the list

3. **Retry or Fail**:

    - If another S-CSCF is available, relays the request to it

    - If all S-CSCFs have been tried and failed, responds with 503 Service Unavailable to the originator

Stateful S-CSCF List Management:

- The list of candidate S-CSCFs is kept in transaction memory
- Position in the list is maintained across multiple attempts
- The list is cleared when a final successful response is received (2xx success or 4xx client error)
- The list is preserved when receiving 401 Unauthorized (authentication challenge), as the same S-CSCF must handle the subsequent authenticated request

Load Balancing

Load Balancing Configuration:

When multiple S-CSCFs support the same capabilities:

- S-CSCF 1: sip:scscf1.example.com:5060 - capability 0
- S-CSCF 2: sip:scscf2.example.com:5060 - capability 0
- S-CSCF 3: sip:scscf3.example.com:5060 - capability 0

The I-CSCF uses **round-robin** or **random** selection to distribute load evenly across all matching S-CSCFs.

View load distribution via: Web UI → I-CSCF → S-CSCF List (shows all configured servers)

Web UI Operations

Accessing I-CSCF Page

Navigate to: `https://<control-panel>/icscf`

Page Layout

The I-CSCF page has four main tabs:

1. **S-CSCF Servers** - Configured S-CSCFs and capabilities
2. **NDS Trusted Domains** - Network domain security
3. **Sessions** - Active I-CSCF sessions with S-CSCF selection
4. **Hash Tables** - Shared memory tables

Viewing S-CSCF Servers

Purpose: See which S-CSCFs are available for user assignment

Display Columns:

- **ID**: Database ID
- **Name**: Descriptive name
- **S-CSCF URI**: SIP URI of the S-CSCF
- **Capabilities**: Comma-separated capability IDs

Example Output:

```
ID   Name                    S-CSCF URI
Capabilities
1    Primary S-CSCF
sip:scscf.ims.mnc001.mcc001.3gppnetwork.org:5060   0, 1
2    Secondary S-CSCF
sip:scscf2.ims.mnc001.mcc001.3gppnetwork.org:5060  0, 1
```

Operations:

- View list of S-CSCFs
- Check capabilities configured
- Verify S-CSCF URIs

Note: To add/modify S-CSCFs, coordinate with system administrators. New S-CSCF entries require:

- A name (descriptive label like "New S-CSCF")
- The S-CSCF URI (e.g., sip:scscf3.example.com:5060;transport=tcp)
- Associated capability IDs (e.g., capabilities 0 and 1)

Viewing NDS Trusted Domains

Purpose: Monitor which network domains are trusted for peering

Display Columns:

- **ID**: Database ID
- **Trusted Domain**: FQDN of trusted network

Example Output:

```
ID   Trusted Domain
1    ims.mnc001.mcc001.3gppnetwork.org
2    ims.mnc002.mcc001.3gppnetwork.org
3    carrier.example.com
```

Operations:

- View trusted domains
- Verify peering relationships

Adding Trusted Domains: Coordinate with system administrators to add new trusted domains. Each entry requires the fully qualified domain name (FQDN) of the trusted network (e.g., partner.example.com).

Monitoring Active Sessions

Purpose: See real-time I-CSCF decision-making and S-CSCF selection

Display Information:

- **Call-ID**: SIP Call-ID
- **User Identity**: Public identity being queried
- **Selected S-CSCF**: Which S-CSCF was chosen

- **Capability Match**: Capabilities that matched
- **UAR/LIR Result**: Diameter result code
- **Timestamp**: When session was created

Use Cases:

1. Verify S-CSCF selection is working
2. Troubleshoot routing issues
3. Monitor load distribution across S-CSCFs
4. Analyze capability matching

Example:

```
Call-ID: 3c26700857a87f84@10.4.12.165
User: sip:12015551234@ims.mnc001.mcc001.3gppnetwork.org
Selected S-CSCF: sip:scscf.ims.mnc001.mcc001.3gppnetwork.org:5060
Capabilities: mandatory=[0,1], optional=[]
Operation: UAR (Registration)
Result: 2001 (FIRST_REGISTRATION)
Timestamp: 2025-11-29 14:35:22
```

Hash Table Management

Similar to P-CSCF, the I-CSCF can use hash tables for caching or custom logic.

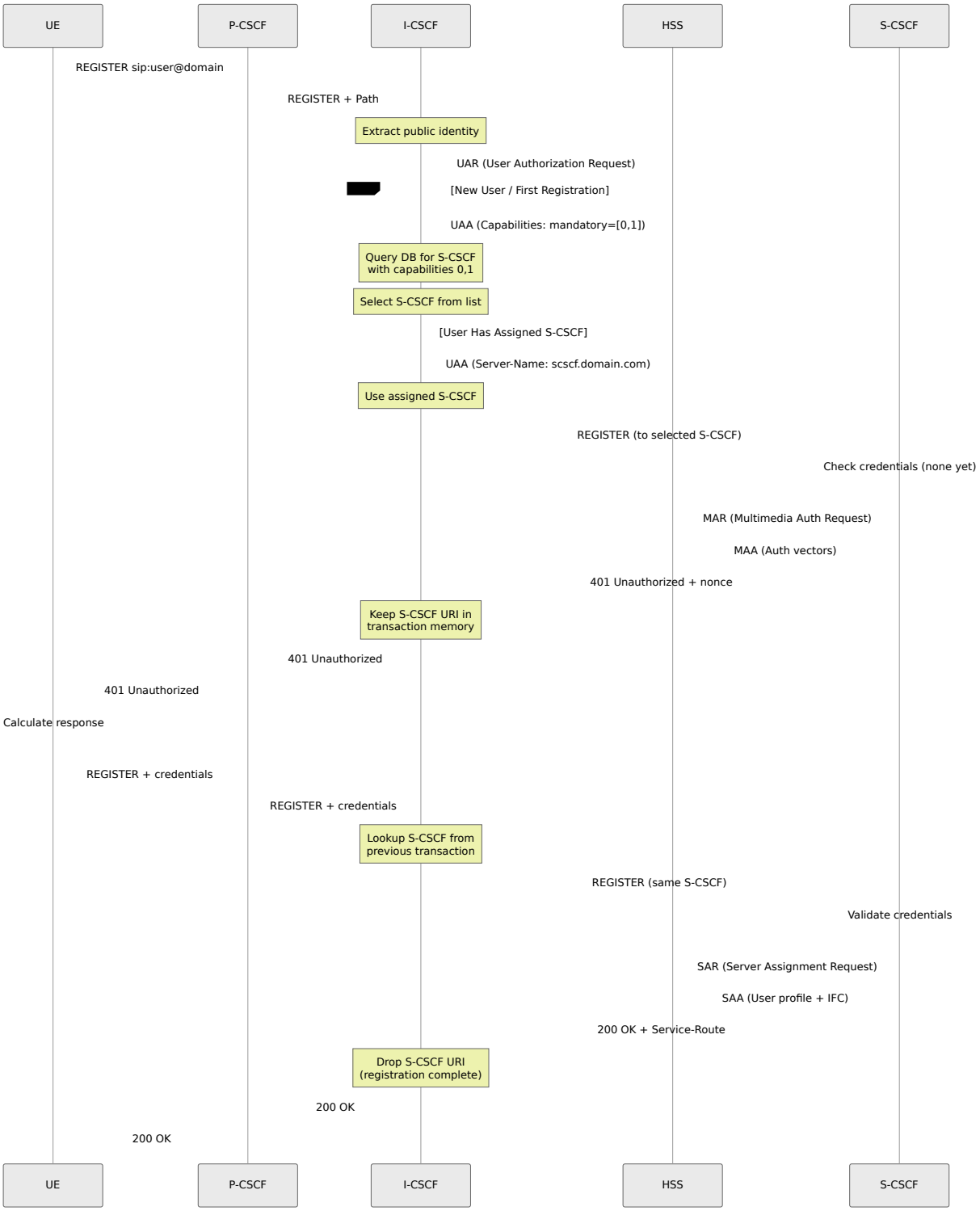
Common Use Cases:

- Cache UAR/LIR results (short TTL)
- Rate limiting per source IP
- Custom routing decisions

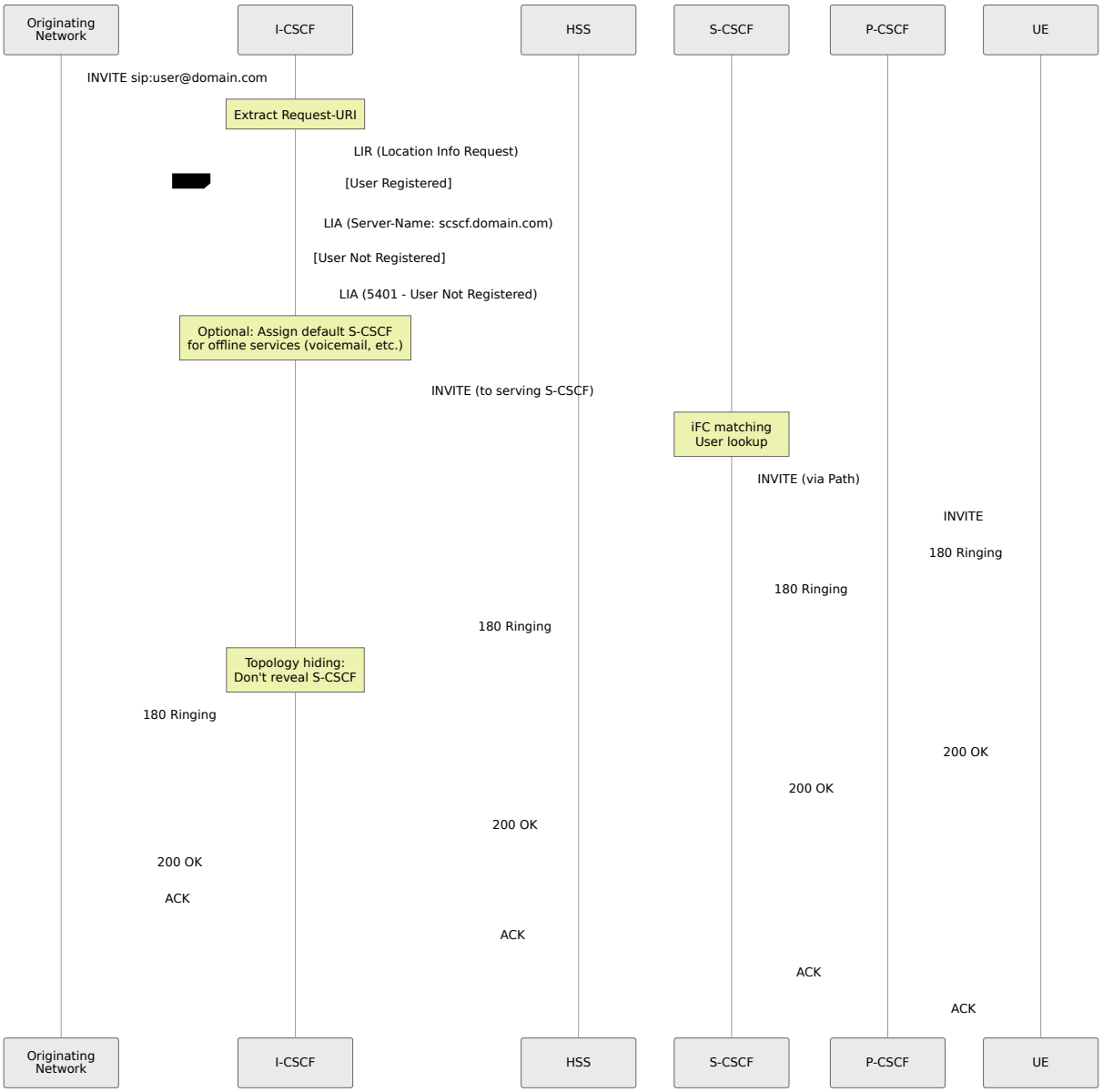
Operations: Same as P-CSCF (list, dump, delete, flush)

Call Flows

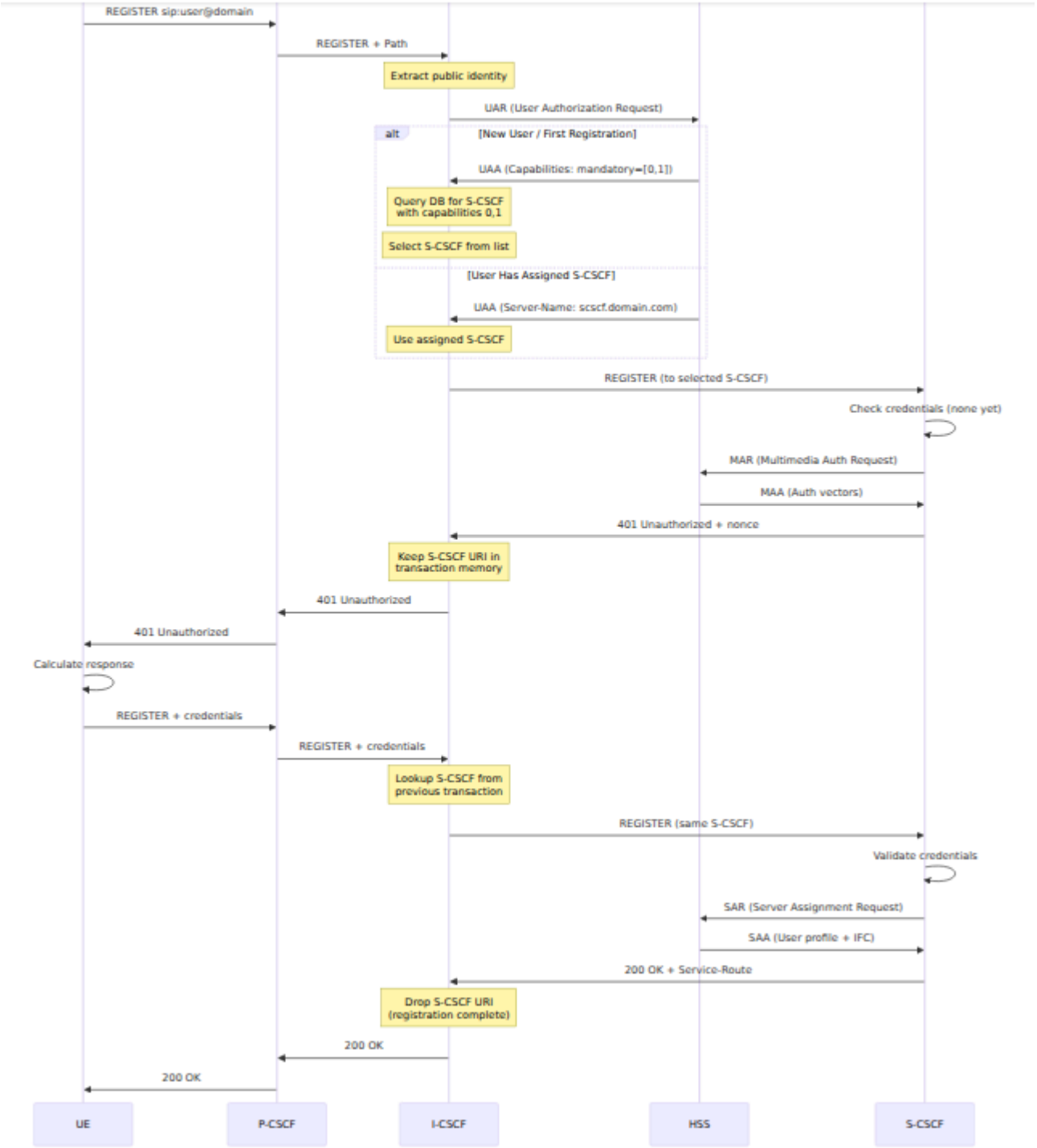
Registration Flow with I-CSCF



Terminating Call Flow via I-CSCF



S-CSCF Failover Flow



Troubleshooting

HSS Connectivity Issues

Diameter Peer Closed

Symptoms: Cannot query HSS, all registrations fail

Diagnostic Steps:

1. Check Diameter peer status in Web UI:
    - Navigate to Diameter page
    - Select I-CSCF node
    - Check HSS peer state
2. Verify network connectivity to HSS (coordinate with network team if needed)
3. Try to enable peer via the control panel:
    - Navigate to Diameter page
    - Find HSS peer
    - Click "Enable" button
4. Review system logs via the control panel Logs page for CER/CEA (Capabilities Exchange) messages and Diameter errors
5. Coordinate with system administrators to verify Diameter configuration if needed

UAR/LIR Timeout

Symptoms: Registrations/calls timeout, logs show Diameter timeout

Possible Causes:

- HSS overloaded
- Network latency

- Incorrect routing realm
- HSS not responding to this I-CSCF

Solutions:

1. Review system logs for Diameter timeout errors
2. Verify HSS peer is connected via the control panel (Diameter page)
3. Coordinate with system administrators to:
    - Increase Diameter transaction timeout if needed
    - Verify destination realm configuration
    - Check HSS logs if accessible
4. Monitor Diameter message flow via the control panel Logs page
5. Coordinate with network team to verify no network latency or routing issues to HSS

S-CSCF Selection Issues

No S-CSCF Selected

Symptoms: 503 Service Unavailable, logs show "No S-CSCF available"

Diagnostic Steps:

1. Check S-CSCF list via the control panel:
    - Navigate to I-CSCF → S-CSCF Servers tab
    - Verify S-CSCFs are configured with appropriate capabilities
2. Review system logs for HSS UAA (User Authorization Answer) capabilities
3. Verify capabilities matching between what HSS returns and what's configured in the I-CSCF database
4. Coordinate with system administrators to:

    - Verify database connectivity
    - Add missing S-CSCF entries if needed
    - Check capability configuration matches HSS expectations

Wrong S-CSCF Selected

Symptoms: Calls route to unexpected S-CSCF

Possible Causes:

- Capability mismatch
- Load balancing issue
- Database out of sync with HSS

Solutions:

1. Monitor session tracking via the control panel:
    - Navigate to I-CSCF → Sessions tab
    - Review S-CSCF selection decisions
2. Review system logs to check if HSS is assigning a specific S-CSCF name (which would override selection logic)
3. Verify I-CSCF database S-CSCF list and capabilities match HSS expectations
4. Coordinate with system administrators to review capability matching configuration

Routing Issues

Requests Not Forwarding to S-CSCF

Symptoms: I-CSCF receives request but doesn't forward

Diagnostic Steps:

1. Review system logs via the control panel Logs page for routing errors

2. Verify destination S-CSCF URI is being set correctly (check logs for routing decisions)

3. Verify network connectivity to S-CSCF (coordinate with network team)

4. Check that selected S-CSCF is actually reachable and responding

5. Coordinate with system administrators to enable debug logging if needed for deeper analysis

S-CSCF Responds But I-CSCF Doesn't Relay

Symptoms: Wireshark shows response to I-CSCF but not forwarded

Possible Causes:

- Transaction timeout
- Via header mismatch
- Record-Route loop

Solutions:

1. Review system logs for transaction matching errors or loop detection

2. Verify Via headers are being processed correctly (check logs)

3. Coordinate with system administrators to:

    - Increase transaction timeout if needed
    - Verify no SIP routing loops

Database Issues

Database Connection Lost

Symptoms: "Database connection error" in logs

Solutions:

1. Coordinate with system administrators to:

- Verify database service is running
- Test database connectivity
- Enable auto-reconnect if not already configured
- Restart I-CSCF service if needed

Database Schema Mismatch

Symptoms: SQL errors in logs about missing columns/tables

Solutions:

1. Coordinate with system administrators to:
   - Verify database schema matches expected structure
   - Check s_cscf, s_cscf_capabilities, and nds_trusted_domains tables exist and have correct columns
   - Re-create database schema if needed

Best Practices

High Availability

1. **Deploy multiple I-CSCF instances**:
   - Use DNS SRV for load balancing
   - Each instance connects to same HSS
   - Share database (read-only for S-CSCF list)
2. **DNS SRV Configuration**:

```
_sip._udp.ims.example.com. SRV 10 50 5060 icscf01.example.com.
_sip._udp.ims.example.com. SRV 10 50 5060 icscf02.example.com.
_sip._tcp.ims.example.com. SRV 10 50 5060 icscf01.example.com.
_sip._tcp.ims.example.com. SRV 10 50 5060 icscf02.example.com.
```

3. **Stateless operation**: I-CSCF doesn't maintain dialog state, making failover seamless

Performance Tuning

1. **Worker processes**: Set high worker count for optimal query throughput
    - children=64 (high value optimized for I-CSCF's query-heavy workload)
    - tcp_children=8 for handling TCP connections
2. **Database connection pooling**: Use persistent connections to reduce connection overhead
3. **Disable unnecessary features** to reduce processing overhead:
    - No RTP handling (I-CSCF is signaling-only)
    - No presence services
    - Minimal logging in production (set to info or warning level only)
4. **Optimize Diameter** for high-throughput Cx interface:
    - sessions_hash_size=4096 (larger hash table for better session lookup performance)
    - workers=4 (dedicated Diameter worker threads for concurrent Cx operations)

Security

1. **Validate trusted domains**: Check Via/P-Visited-Network-ID
2. **Rate limiting**: Prevent DoS attacks on HSS by limiting UAR/LIR queries per source IP
    - Use pike module to check request rate
    - If rate limit exceeded, respond with 503 Too Many Requests
    - Protects HSS from being overwhelmed by malicious query floods
3. **TLS to HSS**: Use Diameter over TLS (DTLS)
4. **Sanitize headers**: Remove untrusted P-headers from external networks

Monitoring

1. **Key Metrics**:
    - UAR success rate
    - LIR success rate
    - Average query latency
    - S-CSCF distribution (load balance)
    - Diameter peer uptime
2. **Prometheus Queries**:

```
# UAR success rate
rate(icscf_uar_success[5m]) / rate(icscf_uar_total[5m])

# Average Diameter latency
rate(diameter_request_duration_sum[5m]) /
rate(diameter_request_duration_count[5m])
```

3. **Alerting**:
    - HSS peer down
    - All S-CSCFs unavailable
    - High error rate (>5%)

Database Maintenance

Database maintenance is handled by system administrators. Key maintenance tasks include:

1. **Keep S-CSCF list updated**: Coordinate with administrators to ensure S-CSCF list in database matches actual deployments
    - Verify via web UI: Navigate to I-CSCF → S-CSCF List tab
    - Check that all active S-CSCF servers are listed with correct capabilities
2. **Prune old sessions**: If UAR/LIR results are cached, old entries should be cleaned periodically

Reference

3GPP Specifications

- **TS 23.228**: IMS Architecture
- **TS 29.228**: Cx Interface (I-CSCF to HSS)
- **TS 29.229**: Cx/Dx Protocol

Diameter RFCs

- **RFC 6733**: Diameter Base Protocol
- **RFC 7155**: Diameter NAT Traversal

IMS CSCF Metrics Reference

This document provides a comprehensive reference for all metrics exported by the P-CSCF, I-CSCF, and S-CSCF components.

Accessing Metrics

All CSCF components expose Prometheus metrics on port 9090:

```
http://<host>:9090/metrics
```

Each CSCF host (P-CSCF, I-CSCF, S-CSCF) exports its own metrics. Configure your Prometheus server to scrape all hosts for complete monitoring coverage.

Example Prometheus Configuration:

```yaml
scrape_configs:
  - job_name: 'cscf_pcscf'
    static_configs:
      - targets: ['pcscf1.example.com:9090',
'pcscf2.example.com:9090']

  - job_name: 'cscf_icscf'
    static_configs:
      - targets: ['icscf1.example.com:9090']

  - job_name: 'cscf_scscf'
    static_configs:
      - targets: ['scscf1.example.com:9090',
'scscf2.example.com:9090']
```

For operational guidance on monitoring and alerting, see:

- Web UI Operations Guide

- Capacity and Dimensioning Guide

Monitoring Through Control Panel

The OmniCall CSCF Control Panel provides real-time visibility into the operational state that generates these metrics. While metrics are exported via Prometheus for historical analysis and alerting, the control panel shows the current state of registrations, dialogs, and Diameter peers.

S-CSCF Management

View active registrations and user location data:

The registration count visible in the UI corresponds to metrics like `ims_usrloc_scscf_active_impus` and `ims_usrloc_scscf_active_contacts`.

Diameter Peer Monitoring

Monitor Diameter peer status and queue lengths:

The queue length shown here corresponds to the `cdp_queuelength` metric. Peer state "I_Open" indicates healthy connections.

Each peer shows supported Diameter applications. For example:

- **16777216:10415 (Cx/Dx)** - Used by I-CSCF and S-CSCF for HSS communication (UAR, LIR, MAR, SAR)
- **16777236:10415 (Rx)** - Used by P-CSCF for PCRF QoS policy
- **4 (Ro)** - Used by S-CSCF for online charging

These correspond to metrics like `ims_icscf_uar_*`, `ims_icscf_lir_*`, `ims_auth_mar_*`, `ims_registrar_scscf_sar_*`, and `ims_qos_*`.

P-CSCF Metrics

CDP (Diameter) Metrics

Metric Name	Meaning
`cdp_average_response_time`	Average response time for Diameter requests in milliseconds (calculated as replies_response_time / replies_received)
`cdp_queuelength`	Current length of the Diameter worker queue tasks
`cdp_replies_received`	Total number of Diameter replies received
`cdp_replies_response_time`	Total time spent waiting for Diameter replies in milliseconds
`cdp_timeout`	Number of timeout events on Diameter requests

Core SIP Statistics

Request Counters

Metric Name	Meaning
`core_rcv_requests`	Total number of SIP requests received
`core_rcv_requests_ack`	Number of ACK requests received
`core_rcv_requests_bye`	Number of BYE requests received
`core_rcv_requests_cancel`	Number of CANCEL requests received
`core_rcv_requests_info`	Number of INFO requests received
`core_rcv_requests_invite`	Number of INVITE requests received
`core_rcv_requests_message`	Number of MESSAGE requests received
`core_rcv_requests_notify`	Number of NOTIFY requests received
`core_rcv_requests_options`	Number of OPTIONS requests received
`core_rcv_requests_prack`	Number of PRACK requests received
`core_rcv_requests_publish`	Number of PUBLISH requests received
`core_rcv_requests_refer`	Number of REFER requests received
`core_rcv_requests_register`	Number of REGISTER requests received
`core_rcv_requests_subscribe`	Number of SUBSCRIBE requests received
`core_rcv_requests_update`	Number of UPDATE requests received

Reply Counters (General)

Metric Name	Meaning
`core_rcv_replies`	Total number of SIP replies received
`core_rcv_replies_18x`	Number of 180/181/183/186/187/189 provisional responses received
`core_rcv_replies_1xx`	Number of 1xx (provisional) responses received
`core_rcv_replies_2xx`	Number of 2xx (success) responses received
`core_rcv_replies_3xx`	Number of 3xx (redirection) responses received
`core_rcv_replies_4xx`	Number of 4xx (client error) responses received
`core_rcv_replies_5xx`	Number of 5xx (server error) responses received
`core_rcv_replies_6xx`	Number of 6xx (global failure) responses received

Reply Counters by Method (1xx)

Metric Name	Meaning
`core_rcv_replies_1xx_bye`	Number of 1xx responses to BYE requests
`core_rcv_replies_1xx_cancel`	Number of 1xx responses to CANCEL requests
`core_rcv_replies_1xx_invite`	Number of 1xx responses to INVITE requests
`core_rcv_replies_1xx_message`	Number of 1xx responses to MESSAGE requests
`core_rcv_replies_1xx_prack`	Number of 1xx responses to PRACK requests
`core_rcv_replies_1xx_refer`	Number of 1xx responses to REFER requests
`core_rcv_replies_1xx_reg`	Number of 1xx responses to REGISTER requests
`core_rcv_replies_1xx_update`	Number of 1xx responses to UPDATE requests

Reply Counters by Method (2xx)

Metric Name	Meaning
`core_rcv_replies_2xx_bye`	Number of 2xx (success) responses to BYE requests
`core_rcv_replies_2xx_cancel`	Number of 2xx (success) responses to CANCEL requests
`core_rcv_replies_2xx_invite`	Number of 2xx (success) responses to INVITE requests
`core_rcv_replies_2xx_message`	Number of 2xx (success) responses to MESSAGE requests
`core_rcv_replies_2xx_prack`	Number of 2xx (success) responses to PRACK requests
`core_rcv_replies_2xx_refer`	Number of 2xx (success) responses to REFER requests
`core_rcv_replies_2xx_reg`	Number of 2xx (success) responses to REGISTER requests
`core_rcv_replies_2xx_update`	Number of 2xx (success) responses to UPDATE requests

Reply Counters by Method (3xx)

Metric Name	Meaning
`core_rcv_replies_3xx_bye`	Number of 3xx (redirection) responses to BYE requests
`core_rcv_replies_3xx_cancel`	Number of 3xx (redirection) responses to CANCEL requests
`core_rcv_replies_3xx_invite`	Number of 3xx (redirection) responses to INVITE requests
`core_rcv_replies_3xx_message`	Number of 3xx (redirection) responses to MESSAGE requests
`core_rcv_replies_3xx_prack`	Number of 3xx (redirection) responses to PRACK requests
`core_rcv_replies_3xx_refer`	Number of 3xx (redirection) responses to REFER requests
`core_rcv_replies_3xx_reg`	Number of 3xx (redirection) responses to REGISTER requests
`core_rcv_replies_3xx_update`	Number of 3xx (redirection) responses to UPDATE requests

Reply Counters by Method (4xx)

Metric Name	Meaning
`core_rcv_replies_4xx_bye`	Number of 4xx (client error) responses to BYE requests
`core_rcv_replies_4xx_cancel`	Number of 4xx (client error) responses to CANCEL requests
`core_rcv_replies_4xx_invite`	Number of 4xx (client error) responses to INVITE requests
`core_rcv_replies_4xx_message`	Number of 4xx (client error) responses to MESSAGE requests
`core_rcv_replies_4xx_prack`	Number of 4xx (client error) responses to PRACK requests
`core_rcv_replies_4xx_refer`	Number of 4xx (client error) responses to REFER requests
`core_rcv_replies_4xx_reg`	Number of 4xx (client error) responses to REGISTER requests
`core_rcv_replies_4xx_update`	Number of 4xx (client error) responses to UPDATE requests

Reply Counters by Method (5xx)

Metric Name	Meaning
`core_rcv_replies_5xx_bye`	Number of 5xx (server error) responses to BYE requests
`core_rcv_replies_5xx_cancel`	Number of 5xx (server error) responses to CANCEL requests
`core_rcv_replies_5xx_invite`	Number of 5xx (server error) responses to INVITE requests
`core_rcv_replies_5xx_message`	Number of 5xx (server error) responses to MESSAGE requests
`core_rcv_replies_5xx_prack`	Number of 5xx (server error) responses to PRACK requests
`core_rcv_replies_5xx_refer`	Number of 5xx (server error) responses to REFER requests
`core_rcv_replies_5xx_reg`	Number of 5xx (server error) responses to REGISTER requests
`core_rcv_replies_5xx_update`	Number of 5xx (server error) responses to UPDATE requests

Reply Counters by Method (6xx)

Metric Name	Meaning
`core_rcv_replies_6xx_bye`	Number of 6xx (global failure) responses to BYE requests
`core_rcv_replies_6xx_cancel`	Number of 6xx (global failure) responses to CANCEL requests
`core_rcv_replies_6xx_invite`	Number of 6xx (global failure) responses to INVITE requests
`core_rcv_replies_6xx_message`	Number of 6xx (global failure) responses to MESSAGE requests
`core_rcv_replies_6xx_prack`	Number of 6xx (global failure) responses to PRACK requests
`core_rcv_replies_6xx_refer`	Number of 6xx (global failure) responses to REFER requests
`core_rcv_replies_6xx_reg`	Number of 6xx (global failure) responses to REGISTER requests
`core_rcv_replies_6xx_update`	Number of 6xx (global failure) responses to UPDATE requests

Specific Status Code Counters

Metric Name	Meaning
`core_rcv_replies_400`	Number of 400 Bad Request responses received
`core_rcv_replies_401`	Number of 401 Unauthorized responses received
`core_rcv_replies_402`	Number of 402 Payment Required responses received
`core_rcv_replies_403`	Number of 403 Forbidden responses received
`core_rcv_replies_404`	Number of 404 Not Found responses received
`core_rcv_replies_405`	Number of 405 Method Not Allowed responses received
`core_rcv_replies_406`	Number of 406 Not Acceptable responses received
`core_rcv_replies_407`	Number of 407 Proxy Authentication Required responses received
`core_rcv_replies_408`	Number of 408 Request Timeout responses received
`core_rcv_replies_409`	Number of 409 Conflict responses received
`core_rcv_replies_410`	Number of 410 Gone responses received
`core_rcv_replies_411`	Number of 411 Length Required responses received
`core_rcv_replies_413`	Number of 413 Request Entity Too Large responses received
`core_rcv_replies_414`	Number of 414 Request-URI Too Long responses received

Metric Name	Meaning
`core_rcv_replies_415`	Number of 415 Unsupported Media Type responses received
`core_rcv_replies_420`	Number of 420 Bad Extension responses received
`core_rcv_replies_480`	Number of 480 Temporarily Unavailable responses received
`core_rcv_replies_481`	Number of 481 Call/Transaction Does Not Exist responses received
`core_rcv_replies_482`	Number of 482 Loop Detected responses received
`core_rcv_replies_483`	Number of 483 Too Many Hops responses received
`core_rcv_replies_484`	Number of 484 Address Incomplete responses received
`core_rcv_replies_485`	Number of 485 Ambiguous responses received
`core_rcv_replies_486`	Number of 486 Busy Here responses received
`core_rcv_replies_487`	Number of 487 Request Terminated responses received
`core_rcv_replies_488`	Number of 488 Not Acceptable Here responses received
`core_rcv_replies_489`	Number of 489 Bad Event responses received
`core_rcv_replies_491`	Number of 491 Request Pending responses received

Metric Name	Meaning
`core_rcv_replies_493`	Number of 493 Undecipherable responses received

Forwarding and Error Statistics

Metric Name	Meaning
`core_fwd_replies`	Number of SIP replies forwarded
`core_fwd_requests`	Number of SIP requests forwarded
`core_drop_replies`	Number of SIP replies dropped
`core_drop_requests`	Number of SIP requests dropped
`core_err_replies`	Number of error replies
`core_err_requests`	Number of error requests
`core_bad_URIs_rcvd`	Number of messages with malformed URIs received
`core_bad_msg_hdr`	Number of messages with bad/malformed headers
`core_unsupported_methods`	Number of requests with unsupported SIP methods

Dialog Tracking

Metric Name	Meaning
`dialog_ng_active`	Number of currently active (answered/confirmed) dialogs
`dialog_ng_early`	Number of early dialogs (ringing/provisional state)
`dialog_ng_expired`	Number of dialogs that have expired or been forcibly terminated
`dialog_ng_processed`	Total number of dialogs processed since startup

DNS Statistics

Metric Name	Meaning
`dns_failed_dns_request`	Number of failed DNS queries
`dns_slow_dns_request`	Number of slow DNS queries (exceeding threshold)

IMS IPSec P-CSCF

Metric Name	Meaning
`ims_ipsec_pcscf_spi_free`	Number of free SPI (Security Parameter Index) values available for allocation
`ims_ipsec_pcscf_spi_total`	Total SPI capacity configured for the system
`ims_ipsec_pcscf_spi_used`	Number of currently allocated/used SPI values
`ims_ipsec_pcscf_spi_utilization_pct`	Percentage of SPI pool utilization
`ims_ipsec_pcscf_worker_cache_size`	Size of the worker process IPSec cache

IMS QoS (Rx Interface)

Registration AAR Metrics

Metric Name	Meaning
`ims_qos_active_registration_rx_sessions`	Number of currently active registration Rx sessions
`ims_qos_registration_aars`	Total number of registration AAR (Authorization-Authentication Request) messages sent
`ims_qos_successful_registration_aars`	Number of successful registration AAR transactions
`ims_qos_failed_registration_aars`	Number of failed registration AAR transactions
`ims_qos_registration_aar_avg_response_time`	Average response time for registration AAR messages in milliseconds
`ims_qos_registration_aar_response_time`	Total response time for all registration AAR messages in milliseconds
`ims_qos_registration_aar_replies_received`	Total number of registration AAR replies received
`ims_qos_registration_aar_timeouts`	Number of registration AAR request timeouts

Media AAR Metrics

Metric Name	Meaning
`ims_qos_active_media_rx_sessions`	Number of currently active media Rx sessions
`ims_qos_media_rx_sessions`	Total number of media Rx sessions created
`ims_qos_media_aars`	Total number of media AAR messages sent
`ims_qos_successful_media_aars`	Number of successful media AAR transactions
`ims_qos_failed_media_aars`	Number of failed media AAR transactions
`ims_qos_media_aar_avg_response_time`	Average response time for media AAR messages in milliseconds
`ims_qos_media_aar_response_time`	Total response time for all media AAR messages in milliseconds
`ims_qos_media_aar_replies_received`	Total number of media AAR replies received
`ims_qos_media_aar_timeouts`	Number of media AAR request timeouts

ASR Metrics

Metric Name	Meaning
`ims_qos_asrs`	Total number of ASR (Abort-Session-Request) messages received from PCRF

IMS USRLOC P-CSCF

Metric Name	Meaning
`ims_usrloc_pcscf_expired_contacts`	Number of expired contact bindings
`ims_usrloc_pcscf_registered_contacts`	Number of currently registered contact bindings
`ims_usrloc_pcscf_registered_impus`	Number of currently registered IMPUs (IMS Public User Identities)

MySQL Database

Metric Name	Meaning
`mysql_driver_errors`	Number of MySQL driver/connection errors

Pike Module (IP Blocking)

Metric Name	Meaning
`pike_blocked_ips`	Number of currently blocked IP addresses (flood detection)

Registrar Module

Metric Name	Meaning
`registrar_accepted_regs`	Number of accepted REGISTER requests (legacy registrar module)
`registrar_rejected_regs`	Number of rejected REGISTER requests (legacy registrar module)
`registrar_default_expire`	Default expiration time for registrations in seconds
`registrar_default_expires_range`	Default expires range setting
`registrar_expires_range`	Configured expires range
`registrar_max_contacts`	Maximum number of contacts allowed per AOR
`registrar_max_expires`	Maximum expiration time allowed in seconds

Script Statistics

Metric Name	Meaning
`script_register_failed`	Number of registration attempts that failed in routing script logic
`script_register_success`	Number of successful registrations processed by routing script
`script_register_time`	Total time spent processing registrations in routing script (milliseconds)

SCTP Transport

Metric Name	Meaning
`sctp_assoc_shutdown`	Number of locally initiated SCTP association shutdowns
`sctp_comm_lost`	Number of SCTP associations lost due to communication failure
`sctp_connect_failed`	Number of failed outgoing SCTP association attempts
`sctp_current_opened_connections`	Number of currently opened SCTP associations
`sctp_current_tracked_connections`	Number of currently tracked SCTP associations
`sctp_established`	Total number of SCTP associations established
`sctp_local_reject`	Number of incoming SCTP associations rejected locally
`sctp_remote_shutdown`	Number of peer-initiated SCTP association shutdowns
`sctp_send_failed`	Number of SCTP send operations that failed
`sctp_send_force_retry`	Number of forced retries on failed SCTP sends
`sctp_sendq_full`	Number of send attempts that failed due to full send queue

Shared Memory

Metric Name	Meaning
`shmem_fragments`	Number of fragments in shared memory pool (indicates fragmentation)
`shmem_free_size`	Amount of free shared memory in bytes
`shmem_max_used_size`	Maximum shared memory used since startup in bytes
`shmem_real_used_size`	Real used shared memory including allocator overhead in bytes
`shmem_total_size`	Total shared memory pool size in bytes
`shmem_used_size`	Currently used shared memory (user data only) in bytes

SL (Stateless) Module

Stateless Reply Counters by Class

Metric Name	Meaning
`sl_1xx_replies`	Number of 1xx stateless replies sent
`sl_2xx_replies`	Number of 2xx stateless replies sent
`sl_3xx_replies`	Number of 3xx stateless replies sent
`sl_4xx_replies`	Number of 4xx stateless replies sent
`sl_5xx_replies`	Number of 5xx stateless replies sent
`sl_6xx_replies`	Number of 6xx stateless replies sent
`sl_xxx_replies`	Number of other stateless replies sent

Specific Stateless Reply Counters

Metric Name	Meaning
`sl_200_replies`	Number of 200 OK stateless replies sent
`sl_202_replies`	Number of 202 Accepted stateless replies sent
`sl_300_replies`	Number of 300 Multiple Choices stateless replies sent
`sl_301_replies`	Number of 301 Moved Permanently stateless replies sent
`sl_302_replies`	Number of 302 Moved Temporarily stateless replies sent
`sl_400_replies`	Number of 400 Bad Request stateless replies sent
`sl_401_replies`	Number of 401 Unauthorized stateless replies sent
`sl_403_replies`	Number of 403 Forbidden stateless replies sent
`sl_404_replies`	Number of 404 Not Found stateless replies sent
`sl_407_replies`	Number of 407 Proxy Authentication Required stateless replies sent
`sl_408_replies`	Number of 408 Request Timeout stateless replies sent
`sl_483_replies`	Number of 483 Too Many Hops stateless replies sent
`sl_500_replies`	Number of 500 Server Internal Error stateless replies sent

Stateless General Statistics

Metric Name	Meaning
`sl_sent_replies`	Total number of stateless replies sent
`sl_sent_err_replies`	Number of stateless error replies sent
`sl_received_ACKs`	Number of ACK messages received for stateless transactions
`sl_failures`	Number of stateless reply send failures

TCP Transport

Metric Name	Meaning
`tcp_con_reset`	Number of TCP connections reset (RST received on established connection)
`tcp_con_timeout`	Number of TCP connections closed due to idle timeout
`tcp_connect_failed`	Number of failed outgoing TCP connection attempts
`tcp_connect_success`	Number of successful outgoing TCP connections
`tcp_current_opened_connections`	Number of currently opened TCP connections
`tcp_current_write_queue_size`	Current total size of TCP write queues across all connections
`tcp_established`	Total number of TCP connections established (both incoming and outgoing)
`tcp_local_reject`	Number of incoming TCP connections rejected locally
`tcp_passive_open`	Number of accepted incoming TCP connections
`tcp_send_timeout`	Number of TCP send operations that timed out (async mode)
`tcp_sendq_full`	Number of send attempts that failed because the send queue was full

TM/TMX (Transaction) Module

Transaction Type Counters

Metric Name	Meaning
`tmx_UAC_transactions`	Number of UAC (client) transactions created
`tmx_UAS_transactions`	Number of UAS (server) transactions created
`tmx_active_transactions`	Number of currently active transactions
`tmx_inuse_transactions`	Number of transactions currently in use

Transaction Completion by Status

Metric Name	Meaning
`tmx_2xx_transactions`	Number of transactions completed with 2xx response
`tmx_3xx_transactions`	Number of transactions completed with 3xx response
`tmx_4xx_transactions`	Number of transactions completed with 4xx response
`tmx_5xx_transactions`	Number of transactions completed with 5xx response
`tmx_6xx_transactions`	Number of transactions completed with 6xx response

Transaction Reply Statistics

Metric Name	Meaning
`tmx_rpl_absorbed`	Number of replies absorbed by the transaction layer (duplicates)
`tmx_rpl_generated`	Number of replies generated locally by the transaction module
`tmx_rpl_received`	Number of replies received for transactions
`tmx_rpl_relayed`	Number of replies relayed by the transaction module
`tmx_rpl_sent`	Number of replies sent by the transaction module

USRLOC (User Location)

Metric Name	Meaning
`usrloc_location_contacts`	Number of contacts in the 'location' domain (standard usrloc module)
`usrloc_location_expires`	Number of expired contacts in the 'location' domain
`usrloc_registered_users`	Number of registered users/AORs (Address of Records)

I-CSCF Metrics

The I-CSCF shares most core SIP statistics with the P-CSCF (see P-CSCF Core SIP Statistics section above). The following metrics are specific to I-CSCF functionality.

I-CSCF Operational Context

The I-CSCF maintains a list of available S-CSCF instances for load balancing:

The I-CSCF queries the HSS to select appropriate S-CSCF instances for new registrations. The success of these operations is tracked in the UAR and LIR metrics below.

IMS I-CSCF (Cx Interface - HSS Communication)

The I-CSCF uses the Diameter Cx interface to communicate with the HSS (Home Subscriber Server) for user location and authorization queries.

UAR (User-Authorization-Request) Metrics

Metric Name	Meaning
`ims_icscf_uar_avg_response_time`	Average response time for UAR messages in milliseconds (calculated as uar_replies_response_time / uar_replies_received)
`ims_icscf_uar_replies_received`	Total number of UAA (User-Authorization-Answer) replies received from HSS
`ims_icscf_uar_replies_response_time`	Total response time for all UAR messages in milliseconds
`ims_icscf_uar_timeouts`	Number of UAR request timeouts

LIR (Location-Info-Request) Metrics

Metric Name	Meaning
`ims_icscf_lir_avg_response_time`	Average response time for LIR messages in milliseconds (calculated as lir_replies_response_time / lir_replies_received)
`ims_icscf_lir_replies_received`	Total number of LIA (Location-Info-Answer) replies received from HSS
`ims_icscf_lir_replies_response_time`	Total response time for all LIR messages in milliseconds
`ims_icscf_lir_timeouts`	Number of LIR request timeouts

Common Metrics

The I-CSCF also exports the following common metrics (documented in the P-CSCF section above):

- **CDP (Diameter) Metrics** - Diameter protocol statistics
- **Core SIP Statistics** - Request/reply counters by method and status code
- **DNS Statistics** - DNS query metrics
- **MySQL Database** - Database connection errors
- **Pike Module** - IP blocking statistics
- **Shared Memory** - Memory usage statistics
- **SL (Stateless) Module** - Stateless reply counters
- **TCP Transport** - TCP connection statistics
- **TM/TMX (Transaction) Module** - Transaction state tracking

---

S-CSCF Metrics

The S-CSCF shares most core SIP statistics with the P-CSCF and I-CSCF (see P-CSCF Core SIP Statistics section above). The following metrics are specific to S-CSCF functionality.

S-CSCF Operational Context

The S-CSCF provides detailed user location information and IFC (Initial Filter Criteria) management:

User location lookup shows registered IMPUs with contact bindings and service profiles. The number of active contacts and IMPUs is tracked by `ims_usrloc_scscf_active_contacts` and `ims_usrloc_scscf_active_impus` metrics.

IFC (Initial Filter Criteria) determines which Application Servers process SIP sessions. The control panel allows dumping and testing IFC rules. IFC evaluation performance can impact call setup times tracked in transaction metrics (`tmx_*`).

IMS ISC (IMS Service Control)

The IMS ISC module handles Initial Filter Criteria (iFC) evaluation to determine which Application Servers should process SIP sessions. These metrics track the performance and effectiveness of iFC matching operations.

Metric Name	Meaning
`ims_isc_ifc_match_attempts`	Total number of iFC matching attempts performed
`ims_isc_ifc_match_time_total`	Cumulative time spent performing iFC matching operations in milliseconds
`ims_isc_ifc_nomatch_count`	Number of iFC matching attempts where no trigger criteria matched

Performance Monitoring: Calculate average iFC match time as `ifc_match_time_total / ifc_match_attempts`. High average times may indicate complex filter criteria or performance bottlenecks in Application Server selection. A high ratio of `ifc_nomatch_count` to `ifc_match_attempts` may indicate misconfigured trigger points or unexpected traffic patterns.

IMS Authentication (Cx Interface - MAR)

The S-CSCF uses Diameter Cx interface to authenticate users with the HSS via MAR (Multimedia-Auth-Request).

Metric Name	Meaning
`ims_auth_mar_avg_response_time`	Average response time for MAR messages in milliseconds (calculated as mar_replies_response_time / mar_replies_received)
`ims_auth_mar_replies_received`	Total number of MAA (Multimedia-Auth-Answer) replies received from HSS
`ims_auth_mar_replies_response_time`	Total response time for all MAR messages in milliseconds
`ims_auth_mar_timeouts`	Number of MAR request timeouts

IMS Registrar S-CSCF

Registration Statistics

Metric Name	Meaning
`ims_registrar_scscf_accepted_regs`	Number of successfully accepted REGISTER requests
`ims_registrar_scscf_rejected_regs`	Number of rejected REGISTER requests
`ims_registrar_scscf_default_expire`	Default expiration time for registrations in seconds
`ims_registrar_scscf_default_expires_range`	Default expires range configuration
`ims_registrar_scscf_max_contacts`	Maximum number of contacts allowed per registration
`ims_registrar_scscf_max_expires`	Maximum expiration time allowed in seconds
`ims_registrar_scscf_notifies_in_q`	Number of pending NOTIFY messages in the queue

SAR (Server-Assignment-Request) Metrics

Metric Name	Meaning
`ims_registrar_scscf_sar_avg_response_time`	Average response time for SAR messages in milliseconds (calculated as sar_replies_response_tim / sar_replies_received)
`ims_registrar_scscf_sar_replies_received`	Total number of SAA (Server-Assignment-Answer) replies received from HSS
`ims_registrar_scscf_sar_replies_response_time`	Total response time for SAR messages in milliseconds
`ims_registrar_scscf_sar_timeouts`	Number of SAR request timeouts

IMS USRLOC S-CSCF

Metric Name	Meaning
`ims_usrloc_scscf_active_contacts`	Number of currently active registered contact bindings
`ims_usrloc_scscf_active_impus`	Number of currently active registered IMPUs (IMS Public User Identities)
`ims_usrloc_scscf_active_subscriptions`	Number of currently active subscriptions
`ims_usrloc_scscf_contact_collisions`	Number of hash collisions in the contact hash table
`ims_usrloc_scscf_impu_collisions`	Number of hash collisions in the IMPU hash table
`ims_usrloc_scscf_subscription_collisions`	Number of hash collisions in the subscription hash table

Dialog Tracking

The S-CSCF tracks dialog state for active calls:

Metric Name	Meaning
`dialog_ng_active`	Number of currently active (answered/confirmed) dialogs
`dialog_ng_early`	Number of early dialogs (ringing/provisional state)
`dialog_ng_expired`	Number of dialogs that have expired or been forcibly terminated
`dialog_ng_processed`	Total number of dialogs processed since startup

Common Metrics

The S-CSCF also exports the following common metrics (documented in the P-CSCF section above):

- **CDP (Diameter) Metrics** - Diameter protocol statistics
- **Core SIP Statistics** - Request/reply counters by method and status code (note: S-CSCF typically has higher fwd_requests and fwd_replies as it routes between endpoints)
- **DNS Statistics** - DNS query metrics
- **MySQL Database** - Database connection errors
- **Pike Module** - IP blocking statistics
- **Shared Memory** - Memory usage statistics
- **SL (Stateless) Module** - Stateless reply counters
- **TCP Transport** - TCP connection statistics
- **TM/TMX (Transaction) Module** - Transaction state tracking (note: S-CSCF typically has both UAC and UAS transactions as it acts as both client and server)

P-CSCF/E-CSCF Operations Guide

Table of Contents

1. Overview
2. Role in IMS Architecture
3. P-CSCF Functions
4. E-CSCF Functions
5. Web UI Operations
6. Call Flows
7. Troubleshooting

Overview

The **P-CSCF** (Proxy Call Session Control Function) is the first point of contact for User Equipment (UE) in the IMS network. It serves as an edge proxy that handles security, QoS enforcement, and emergency call routing. In this implementation, the P-CSCF also functions as the **E-CSCF** (Emergency CSCF) for emergency services.

Important: In our deployments, **P-CSCF does not relay media by default**. Media flows directly between the UE and **OmniTAS** (Telephony Application Server) or other media endpoints. The P-CSCF is purely a SIP signaling proxy.

3GPP Specifications

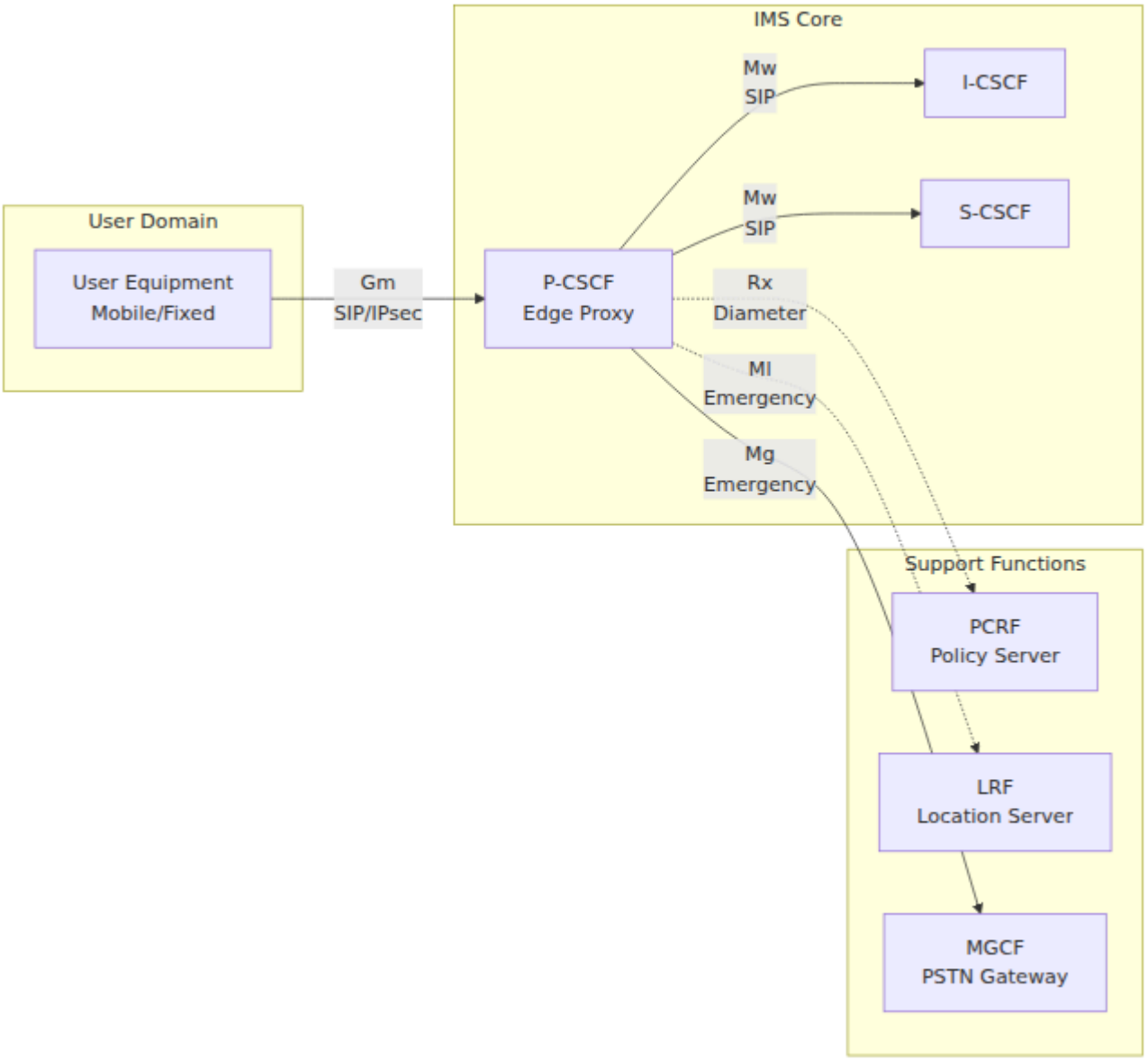
- **3GPP TS 23.228**: IP Multimedia Subsystem (IMS) Stage 2
- **3GPP TS 24.229**: IMS Call Control Protocol
- **3GPP TS 33.203**: Access security for IMS
- **3GPP TS 23.167**: IP Multimedia Subsystem (IMS) emergency sessions

Key Responsibilities

1. **First Contact Point**: UE's initial SIP proxy in IMS
2. **Security Enforcement**: IPsec tunnel establishment and management
3. **QoS Control**: Interfaces with PCRF via Rx for policy enforcement
4. **Emergency Services**: Routes emergency calls and provides IMEI-to-MSISDN lookup (E-CSCF function)
5. **Compression**: SigComp support for bandwidth optimization
6. **Transport Support**: Supports UDP and TCP

Role in IMS Architecture

Network Position



3GPP Reference Points

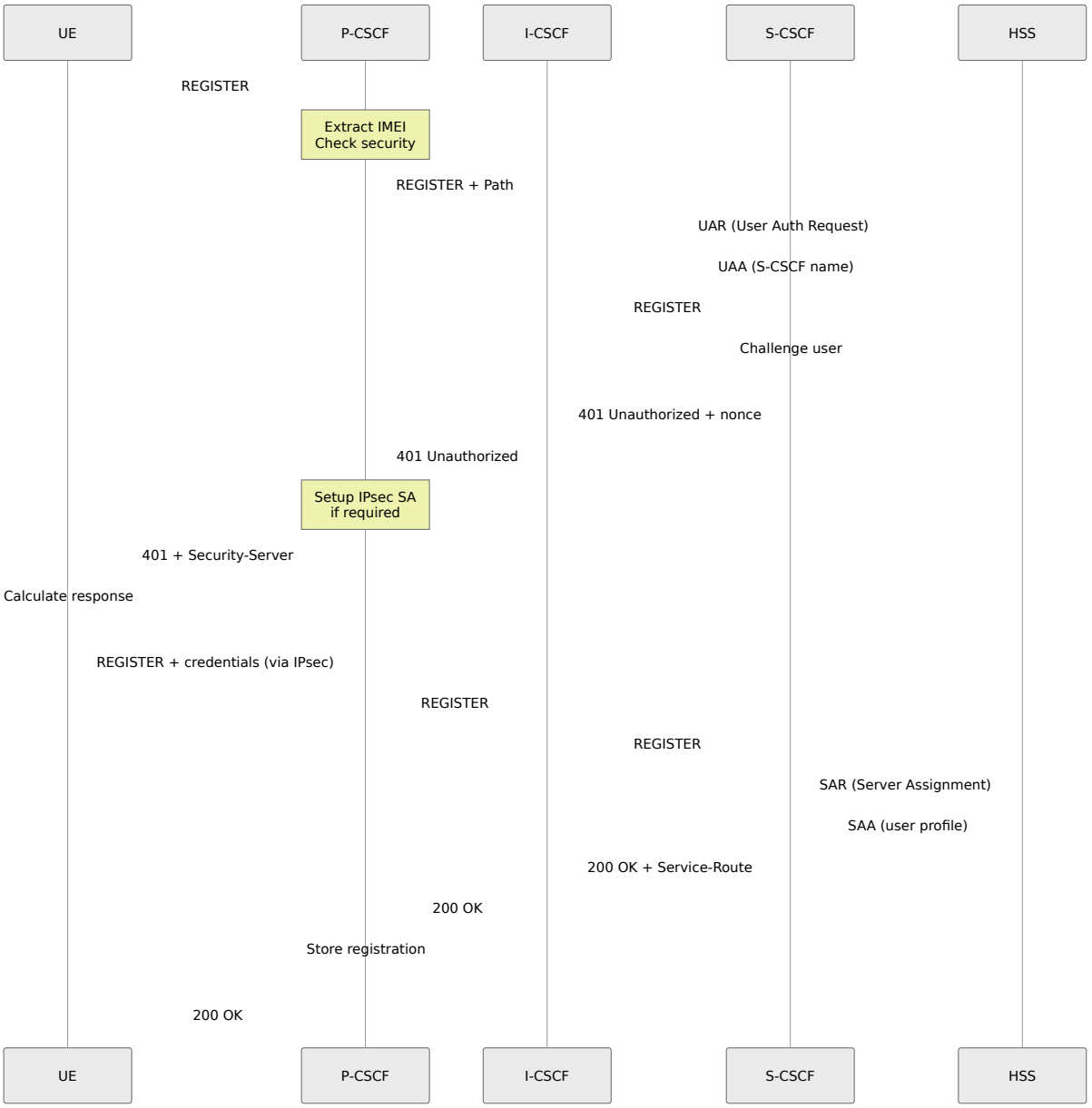
Interface	Protocol	Purpose	Connected To
Gm	SIP/IPsec	UE to P-CSCF	User Equipment
Mw	SIP	P-CSCF to I-CSCF/S-CSCF	Core IMS
Rx	Diameter	QoS/Policy control	PCRF
Ml	HTTP/HELD	Location retrieval	LRF (E-CSCF)
Mg	SIP	Emergency calls	MGCF/E-CSCF

P-CSCF Functions

1. Registration Handling

The P-CSCF is the first hop for SIP REGISTER messages from UEs.

Registration Flow



Key Features

Path Header Insertion:

```
Path: <sip:term@pcscf.ims.mnc001.mcc001.3gppnetwork.org:5060;lr>
```

- Ensures subsequent requests route back through P-CSCF
- Required per RFC 3327 for IMS

Registration Timer Enforcement:

- Forces registration expiry to 599 seconds

- Overrides UE-requested values for network control

IMEI Extraction:

- Extracts IMEI from Contact header: `+sip.instance="<urn:gsma:imei:...>"`
- Stores in hash table for emergency call mapping

Transport-Specific Handling:

- iOS devices: Extends TCP lifetime to prevent premature disconnection

2. Security Functions

IPsec Tunnel Management

The P-CSCF establishes IPsec ESP tunnels with UEs for secure SIP signaling.

IPsec Configuration:

The IPsec functionality is configured with the following parameters:

- **Listen address**: 10.4.12.165 (P-CSCF's IP address for IPsec endpoints)
- **Client port (base)**: 5100 (starting port for UE → P-CSCF traffic)
- **Server port (base)**: 6100 (starting port for P-CSCF → UE traffic)
- **Port range**: Configurable pool of ports (typically 1000-10000 ports)
- **SPI ID start**: 4096 (starting value for Security Parameter Index allocation)
- **SPI ID range**: 100000 (number of SPI pairs available for allocation)
- **Max connections**: 20 (maximum concurrent IPsec security associations per worker)

SPI and Port Management

Each IPsec tunnel between a UE and the P-CSCF requires unique identifiers to keep traffic separated and secure. The system manages two types of resources:

Security Parameter Indexes (SPIs):

Each IPsec tunnel uses TWO SPIs - one for each direction:

- **spi-c** (client SPI): Identifies packets sent from UE to P-CSCF
- **spi-s** (server SPI): Identifies packets sent from P-CSCF to UE

SPIs are allocated in pairs from a configured pool. The system is typically configured with:

- Starting SPI value: 4096
- Available range: 100,000 SPI values
- This provides capacity for 50,000 simultaneous tunnels (pairs are allocated as consecutive even/odd numbers)

Port Allocation:

Each tunnel also uses unique UDP ports on the P-CSCF:

- **client port**: P-CSCF port where it receives IPsec packets from the UE
- **server port**: P-CSCF port where it sends IPsec packets to the UE

Typical port configuration:

- Client port starting value: 5100
- Server port starting value: 6100
- Port range: 10,000 ports available
- Ports wrap around to the start when the range is exhausted

How Resource Allocation Works:

When a UE registers and requests IPsec protection:

1. **First Registration**: Gets spi-c=4096, spi-s=4097, client port=5100, server port=6100
2. **Second Registration**: Gets spi-c=4098, spi-s=4099, client port=5101, server port=6101
3. **Third Registration**: Gets spi-c=4100, spi-s=4101, client port=5102, server port=6102

And so on...

After 10,000 registrations, the ports wrap back to the beginning (5100, 6100), while SPIs continue incrementing. This allows for more tunnels than available ports, as long as UEs have different IP addresses.

Resource Limits:

The maximum number of simultaneous IPsec tunnels is determined by whichever limit is hit first:

- SPI range capacity (typically 50,000 pairs)
- Port range capacity (typically 10,000 ports)
- System memory and processing capacity

Monitoring via Web UI:

Navigate to P-CSCF page → IPsec Statistics (if available) to view:

- Number of active IPsec tunnels
- Number of available SPI/port pairs
- Utilization percentage

If you see registration failures with IPsec-related errors, it may indicate:

- SPI pool exhaustion (all 50,000 pairs in use)
- Port pool exhaustion (all 10,000 ports in use)
- Old tunnels not being cleaned up properly

When Resources Are Released:

SPIs and ports are returned to the available pool when:

- A UE de-registers (sends REGISTER with Expires: 0)
- A registration expires without being refreshed
- An IPsec tunnel is manually destroyed via the web interface
- System administrator cleans up stale tunnels

Capacity Planning:

For deployment planning:

- Each active tunnel uses approximately 1KB of memory
- Typical production deployment supports 10,000-50,000 simultaneous tunnels
- Monitor utilization trends to predict when capacity expansion is needed
- If regularly exceeding 80% utilization, coordinate with system administrators to increase SPI/port ranges

Security Association (SA) Setup:

1. UE sends REGISTER with `Security-Client` header:

```
Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; ealg=null;
                 spi-c=12345; spi-s=67890; port-c=5100; port-
s=6100
```

2. P-CSCF responds with `Security-Server`:

```
Security-Server: ipsec-3gpp; alg=hmac-sha-1-96; ealg=null;
                 spi-c=11111; spi-s=22222; port-c=5100; port-
s=6100
```

3. P-CSCF creates IPsec policies using `setkey`:

```
# Client to Server
spdadd <ue-ip>[5100] <pcscf-ip>[6100] any -P out ipsec
esp/transport//require;

# Server to Client
spdadd <pcscf-ip>[6100] <ue-ip>[5100] any -P in ipsec
esp/transport//require;
```

4. All subsequent SIP messages use IPsec tunnel

Supported Algorithms:

- **Authentication**: hmac-md5-96, hmac-sha-1-96
- **Encryption**: null, des-ede3-cbc, aes-cbc (preferred: null for LTE)

3. Media Handling

Important Note: In our deployments, **the P-CSCF does NOT relay media by default**. Media (RTP/SRTP) flows directly from the UE to **OmniTAS** (Telephony Application Server) or other media endpoints. The P-CSCF handles only SIP signaling.

Media flows directly between UEs and the OmniTAS (Telephony Application Server), bypassing the P-CSCF entirely for RTP/SRTP traffic:

```
UE <------ SIP ------> P-CSCF <------ SIP ------> S-CSCF <------
SIP ------> OmniTAS
    <----------------------- RTP/SRTP (direct to TAS) ------------
---------->
```

The P-CSCF handles only SIP signaling. All media (voice, video) is established directly between the UE and OmniTAS.

4. QoS and Policy Enforcement (Rx Interface)

Diameter Rx Integration

Purpose: Coordinate QoS with PCRF for bearer establishment

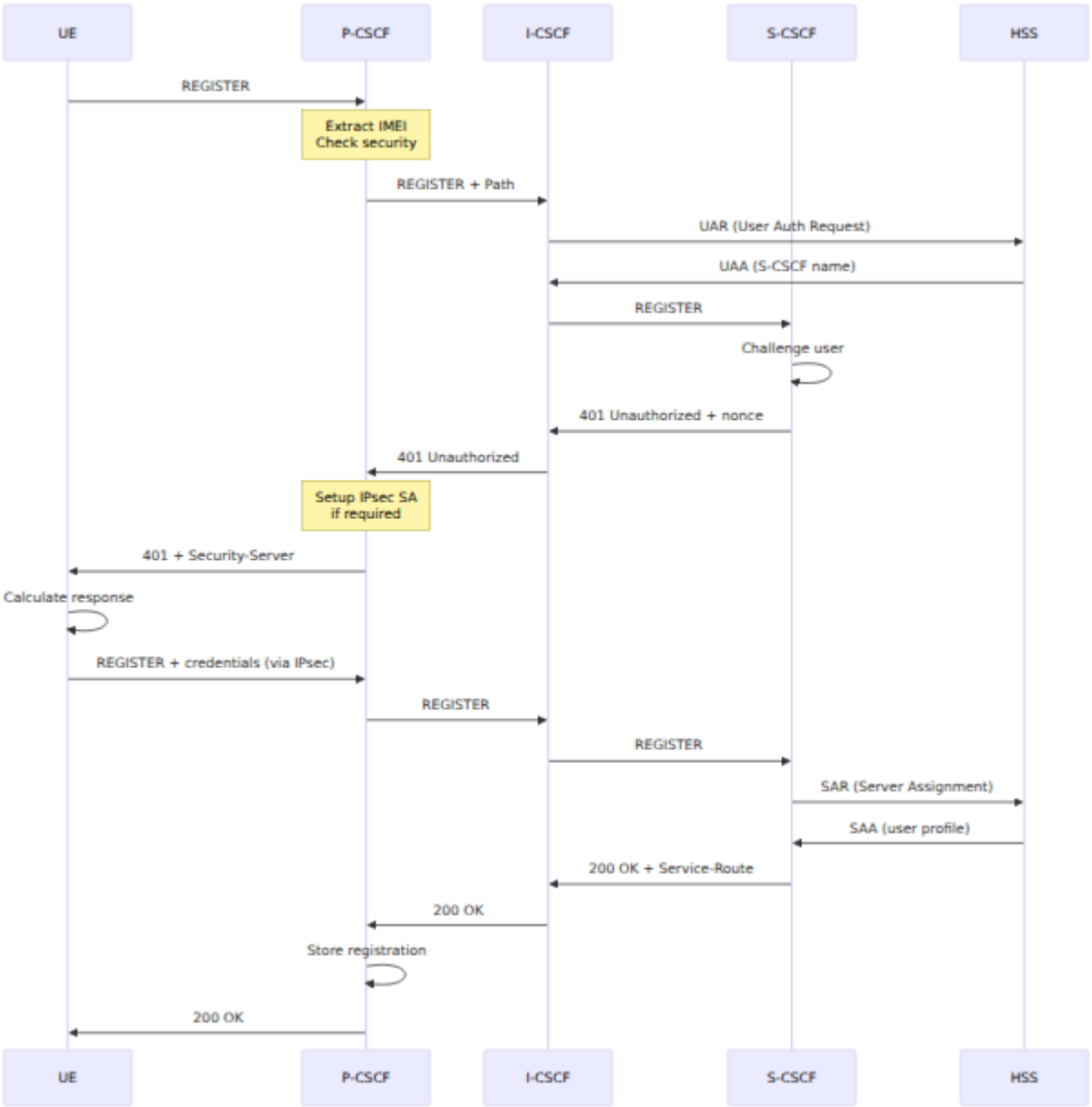
Diameter Configuration:

The P-CSCF connects to the PCRF via Diameter on port 3868 using the Rx application (Application ID 16777236, 3GPP Vendor ID 10415).

Rx Operations:

1. **AAR (Authorization Authentication Request)**: Request QoS for media flow
2. **AAA (Authorization Authentication Answer)**: PCRF grants/denies
3. **STR (Session Termination Request)**: Release QoS on call end

AAR Message Flow



Media Information Sent to PCRF:

- Flow description (IP, port, protocol)
- Bandwidth requirements (uplink/downlink)
- Media type (audio, video)
- Flow status (enabled, disabled)

5. Anti-Flood Protection

Pike Module Configuration (Rate Limiting): The pike module provides flood protection with these settings:

- **Sampling time unit**: 2 seconds - time window for measuring request rate

- **Requests density per unit**: 16 requests allowed per 2-second window from a single IP
- **Remove latency**: 300 seconds (5 minutes) - duration an IP is blocked after exceeding the limit

Failed Authentication Tracking: The P-CSCF tracks failed authentication attempts to prevent brute force attacks:

- Maintains a hash table counter for failed authentication attempts per source IP
- Increments counter on authentication failure with 120-second expiry
- If an IP exceeds 10 failed attempts within 120 seconds, blocks the IP with 403 Too Many Failed Attempts
- Prevents attackers from guessing user credentials

E-CSCF Functions

The P-CSCF includes E-CSCF functionality for emergency call handling.

Emergency Call Detection

SIP URIs Recognized:

- `urn:service:sos` (general emergency)
- `urn:service:sos.police`
- `urn:service:sos.ambulance`
- `urn:service:sos.fire`
- `urn:service:sos.marine`
- `urn:service:sos.mountain`

Detection Logic: Emergency calls are detected by examining the Request-URI:

- Checks if the method is INVITE (call setup request)
- Checks if the Request-URI matches emergency patterns:
  - URN format: urn:service:sos* (SOS URNs defined in RFC 5031)

    - North American emergency: 911
    - European/International emergency: 112
- If emergency call is detected, routes to EMERGENCY handling block for special processing

IMEI to MSISDN Mapping for Emergency Calls

Why This Is Needed: When users make emergency calls (e.g., 911, 112, urn:service:sos), the UE often **does not provide the MSISDN (phone number)** in the SIP message. Emergency services (PSAP - Public Safety Answering Point) need to know the caller's phone number for callback purposes. To solve this, the P-CSCF/E-CSCF maintains a mapping from IMEI (device identifier) to MSISDN.

How It Works:

1. **During Registration** (when MSISDN is known):
    - Extracts IMEI from Contact header's +sip.instance parameter (format: urn:gsma:imei:123456-78-901234-5)
    - Extracts MSISDN from the user's public identity (IMPU) in the From header username
    - Stores the IMEI → MSISDN mapping in a hash table with 24-hour TTL (86400 seconds)
    - Example: imei_msisdn["urn:gsma:imei:123456789012345"] = "12015551234"
    - **In clustered deployments**: Automatically replicates the mapping to all other P-CSCF nodes in the cluster
2. **During Emergency Call** (when MSISDN might be missing):
    - Extracts IMEI from the emergency call's Contact header +sip.instance parameter
    - Performs hash table lookup to retrieve the MSISDN associated with this IMEI
    - If MSISDN is found in the mapping:

    - Adds P-Asserted-Identity header with the full MSISDN (sip:+12015551234@domain)
    - This provides the PSAP with the callback number for the emergency caller

High Availability - Multi-Node Synchronization:

In production deployments with multiple P-CSCF nodes for redundancy, the IMEI→MSISDN mappings are automatically synchronized across all nodes:

Cluster Replication Behavior:

When a UE registers on **P-CSCF Node 1**:

1. Node 1 creates the IMEI→MSISDN mapping locally
2. Node 1 immediately broadcasts the mapping to all other P-CSCF nodes in the cluster
3. **P-CSCF Node 2**, **Node 3**, etc. receive the update and create identical local copies
4. All nodes now have the same IMEI→MSISDN mapping

Why This Matters:

If a UE registered through P-CSCF Node 1 but makes an emergency call that gets routed to P-CSCF Node 2 (due to load balancing or failover), Node 2 already has the IMEI→MSISDN mapping and can provide the callback number to the PSAP.

Synchronization Mechanism:

The synchronization happens via SIP-based messaging between P-CSCF nodes:

- Uses custom SIP messages to propagate hash table updates
- Messages are sent in JSON format containing the IMEI, MSISDN, and TTL
- Transmission is automatic and transparent - no operator intervention needed
- Updates are broadcast to all cluster members within milliseconds

Operations Impact:

- **Resilience**: Emergency calls work correctly regardless of which P-CSCF node handles the call
- **No Single Point of Failure**: Any P-CSCF node can provide callback number for any registered UE
- **Automatic**: Synchronization is built-in and requires no manual configuration or intervention
- **Monitoring**: Via web UI, navigate to P-CSCF → Hash Tables → imei_msisdn to see mappings on each node

Cluster Configuration Requirements:

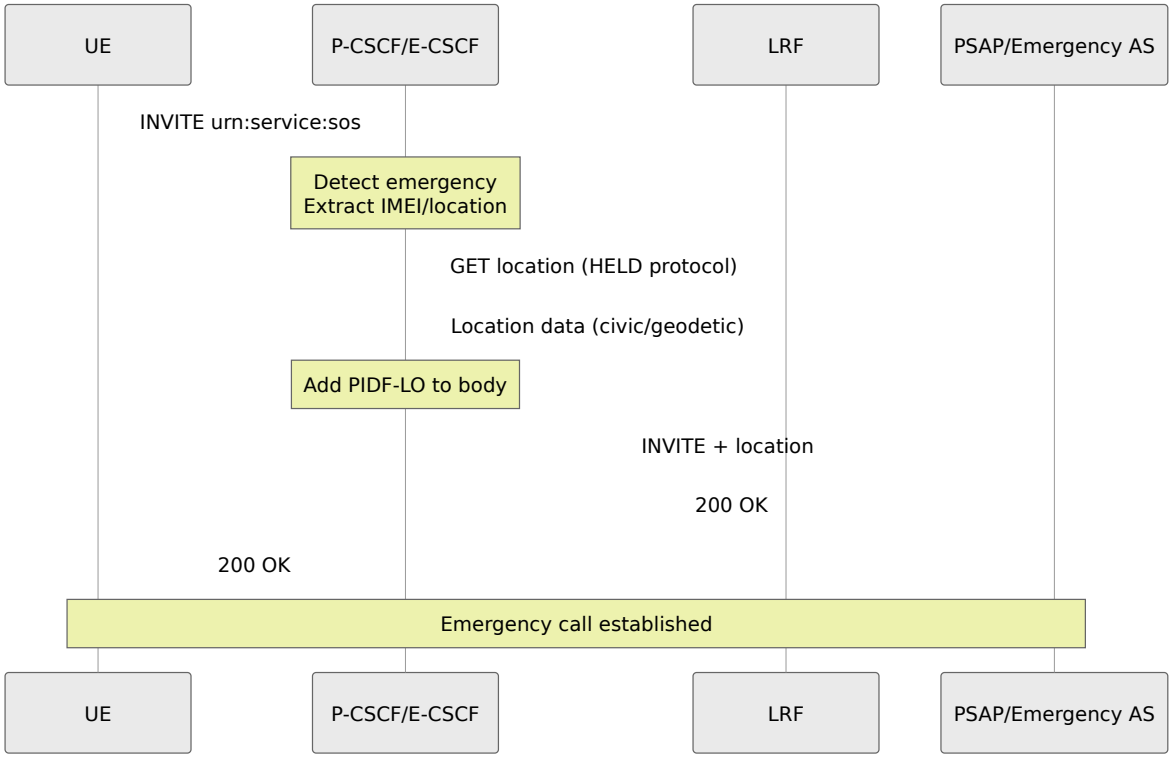
For hash table synchronization to work:

- All P-CSCF nodes must be configured with each other's addresses
- Nodes discover each other automatically through availability notifications
- Network connectivity must allow SIP traffic between all P-CSCF nodes
- If synchronization fails, check that firewall rules allow inter-node communication

Example Scenario:

```
1. User registers: IMEI=123456789012345, MSISDN=12015551234
   → Stored: imei_msisdn[123456789012345] = 12015551234

2. User dials 911: INVITE urn:service:sos (MSISDN not in From
header)
   → P-CSCF extracts IMEI from Contact: 123456789012345
   → P-CSCF looks up: imei_msisdn[123456789012345] → 12015551234
   → P-CSCF adds header: P-Asserted-Identity:
<sip:+12015551234@...>
   → PSAP receives call with callback number: +12015551234
```

Emergency Routing



Emergency Call Features:

- Bypasses registration check
- Adds PIDF-LO (Presence Information Data Format - Location Object)
- Routes to emergency application server or PSAP
- Priority handling (preempts normal calls)
- Location information from LRF or UE

Web UI Operations

Accessing P-CSCF Page

Navigate to: `https://<control-panel>/pcscf`

Page Layout

The P-CSCF page has three main tabs:

1. **Registered Contacts** - Active registrations

2. **User Location** - Search by IMSI/IP
3. **Hash Tables** - Shared memory tables

Viewing Registered Contacts

Display Columns:

- **AoR** (Address of Record): User's SIP identity
- **Contact**: Device contact URI
- **Expires**: Registration expiry timestamp
- **Public IP**: UE's public IP address
- **Received**: Actual received IP (if different from Contact)
- **Path**: Path header for routing
- **Rx Session ID**: Diameter Rx session (if QoS active)

Features:

- Auto-refresh every 5 seconds
- Search by partial AoR or Contact
- Sort by column (click header)
- Expandable rows for full details

Example Output:

```
AoR: sip:12015551234@ims.mnc001.mcc001.3gppnetwork.org
Contact: sip:12015551234@10.4.12.100:5060;transport=udp
Expires: 2025-11-29 14:30:15
Public IP: 10.4.12.100
Received: 10.4.12.100:52341
Path: <sip:term@pcscf.ims.mnc001.mcc001.3gppnetwork.org:5060;lr>
Rx Session: rx-pcscf-session-12345
```

Searching User Location

Search Options:

- By IMSI: `imsi:310150123456789`

- By IP: `10.4.12.100`

Use Cases:

1. Find which user is using a specific IP
2. Check if IMSI is registered
3. Verify IPsec tunnel status
4. Check service routes

Hash Table Management

Common Tables:

Table	Purpose	Typical Size
`imei_msisdn`	Emergency IMEI→MSISDN mapping	100-1000 entries
`service_routes`	Cached service routes	Per-registration
`dialog_out`	Outbound dialog tracking	Per-call

Operations:

- **List Tables**: Click "Hash Tables" tab
- **Dump Table**: Click table name to view contents
- **Delete Entry**: Click "Delete" next to entry
- **Flush Table**: Click "Flush" to clear entire table (use caution!)

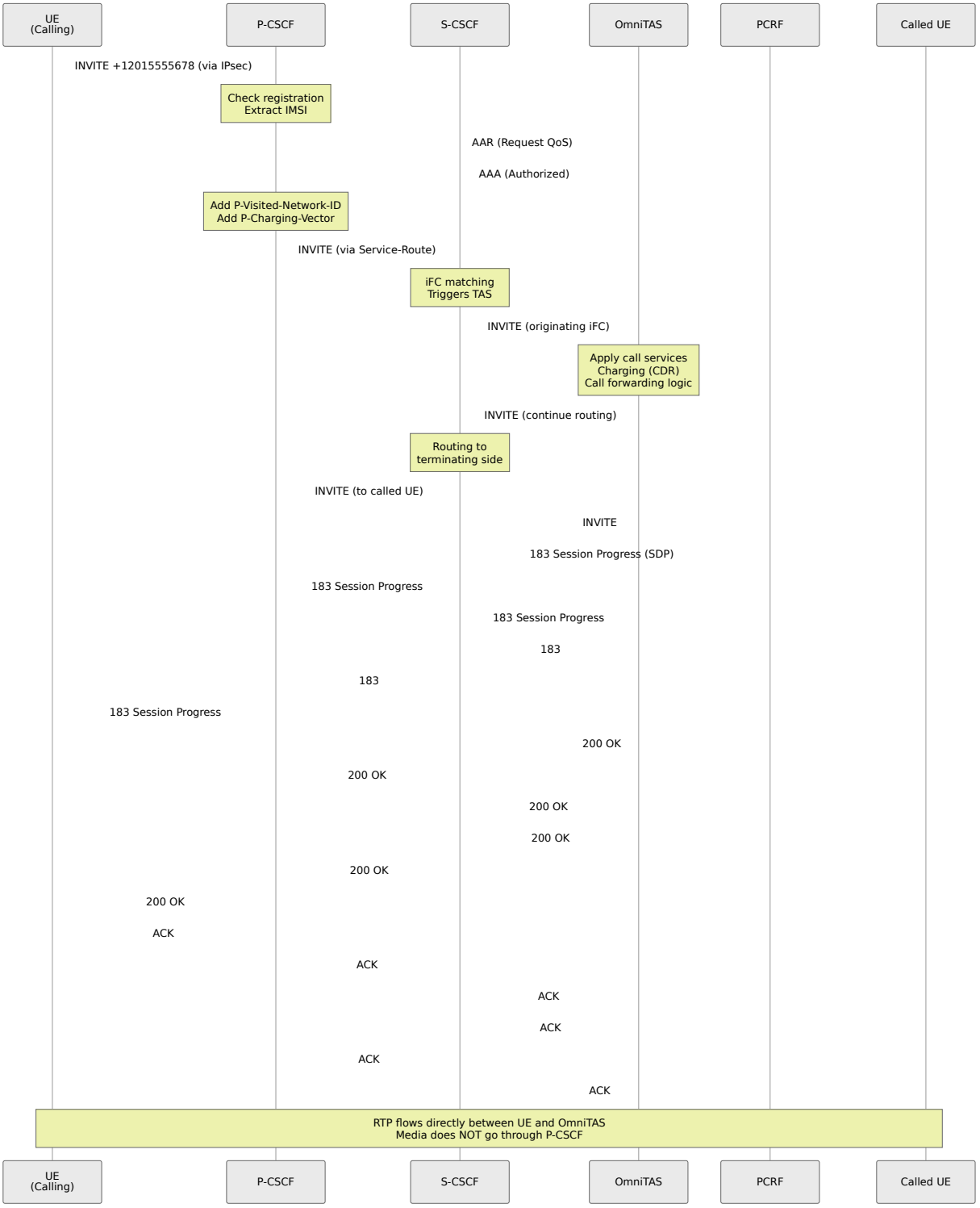
Example Entry:

```
Key:   urn:gsma:imei:123456-78-901234-5
Value: 310150123456789
TTL:   86400 seconds (24 hours)
```

Call Flows

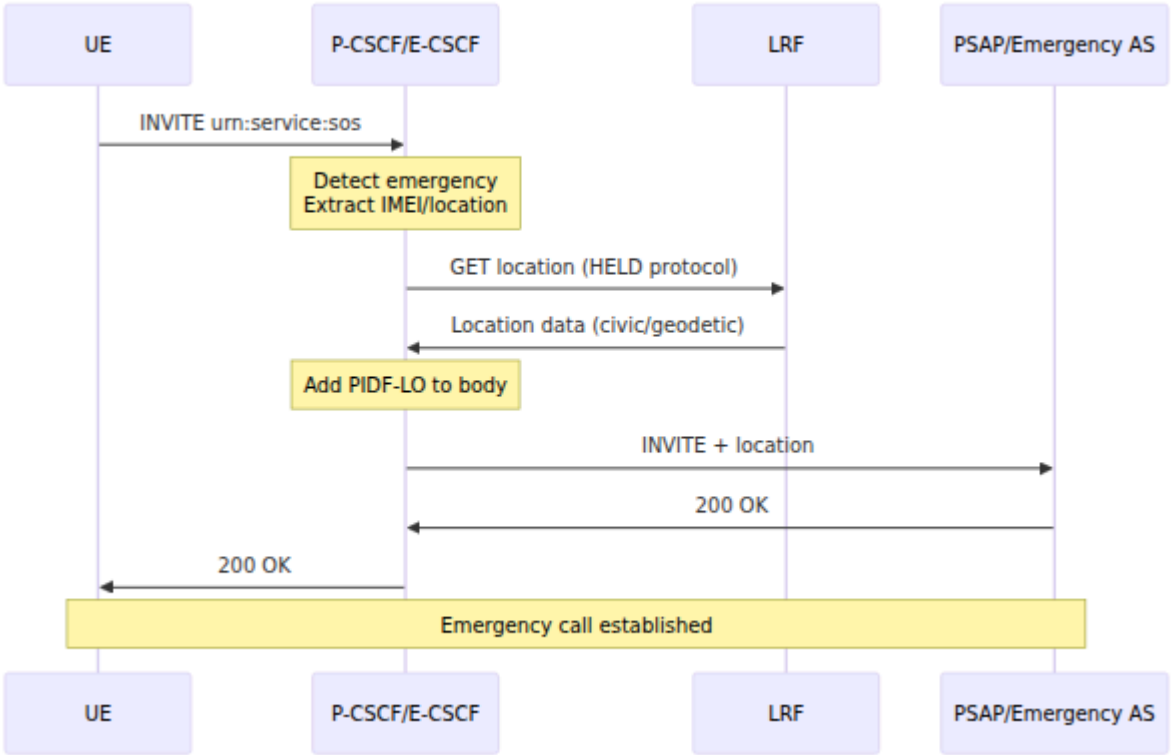
Mobile Originating Call (MO)

All originating calls are routed through the TAS (OmniTAS) for service logic and charging:

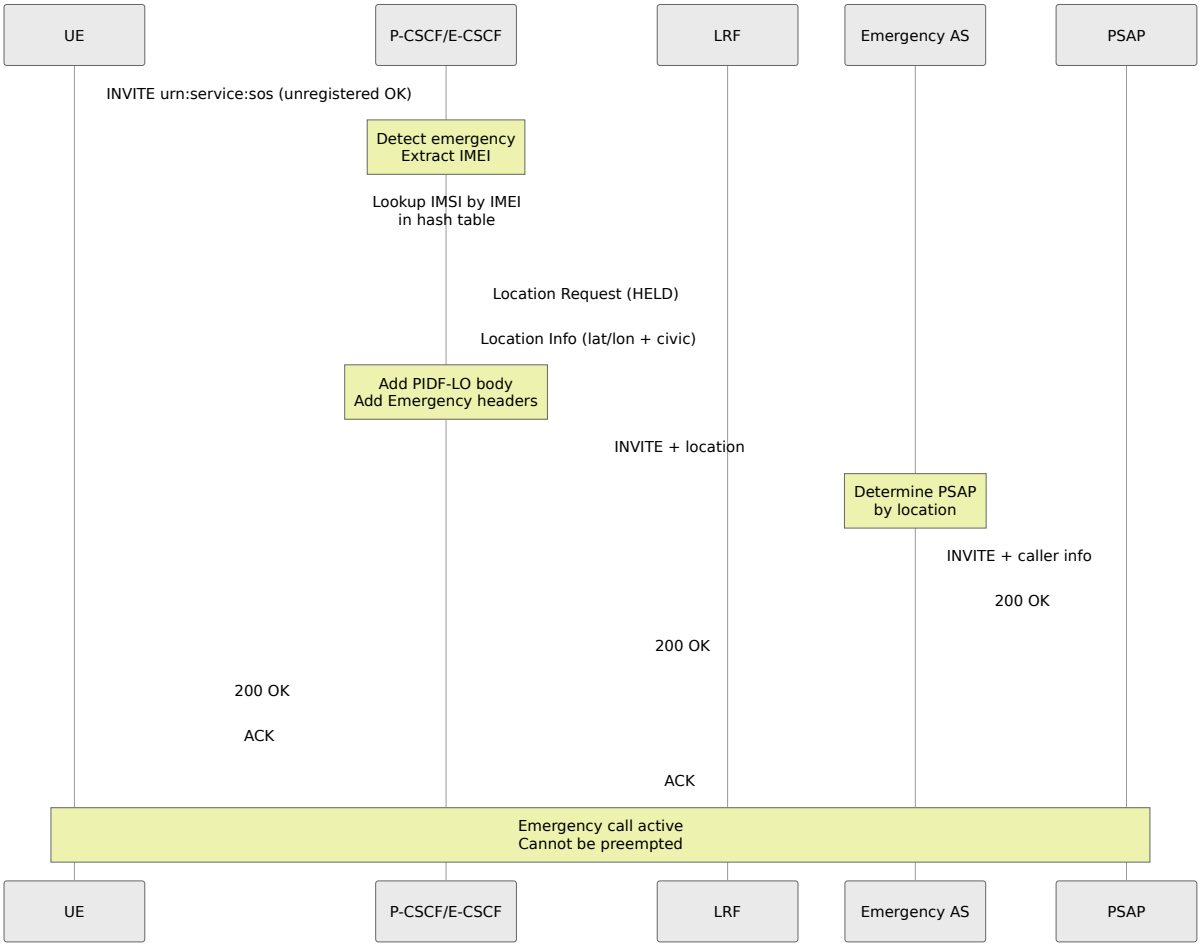


Mobile Terminating Call (MT)

Terminating calls also go through TAS for service logic:



Emergency Call Flow



Troubleshooting

Registration Issues

UE Cannot Register

Symptoms: UE gets 408 Timeout or no response

Diagnostic Steps:

1. Check registration status via the control panel:
    - Navigate to P-CSCF page
    - Check "Registered Contacts" tab
    - Verify user appears in the list

2. Review system logs via the control panel Logs page for errors
3. Verify network connectivity between UE and P-CSCF
4. Check firewall rules allow SIP traffic (port 5060 UDP/TCP)
5. Coordinate with system administrators if P-CSCF service appears to be down

IPsec Tunnel Not Established

Symptoms: 401 challenge sent but re-REGISTER fails

Diagnostic Steps:

1. Review system logs via the control panel Logs page for IPsec-related errors
2. Verify UE is sending Security-Client header in initial REGISTER
3. Check that UE is using IPsec ports (5100 client, 6100 server) in re-REGISTER
4. Verify received address matches expected IPsec tunnel endpoint
5. Coordinate with system administrators to verify IPsec kernel modules are loaded and no port conflicts exist

Call Issues

Calls Don't Route to UE

Symptoms: INVITE to P-CSCF but UE doesn't ring

Diagnostic Steps:

1. Verify registration exists via the control panel:
    - Navigate to P-CSCF page
    - Check "Registered Contacts" tab
    - Search for the user and verify registration is active

2. Verify Path header was stored in the registration
3. Check that calls are being sent to the correct contact address
4. Review system logs for routing errors
5. Verify network path from P-CSCF to UE is reachable

One-Way Audio

Symptoms: One party can't hear the other

Note: In our deployments, **P-CSCF does not relay media**. Media flows directly between UE and OmniTAS. If you're experiencing one-way audio, the issue is likely at the endpoints or in the network routing, not at the P-CSCF.

Diagnostic Steps:

1. Verify SDP in INVITE/200 OK contains correct IP addresses and ports (review via system logs or packet capture if available to administrators)
2. Verify firewall rules allow RTP/SRTP traffic between UE and OmniTAS
3. Check NAT configuration if UE is behind NAT
4. Verify OmniTAS media endpoint is reachable from UE (network connectivity)
5. Coordinate with system administrators for packet capture analysis if needed

Emergency Calls Fail

Symptoms: urn:service:sos calls rejected

Diagnostic Steps:

1. Verify IMEI→MSISDN hash table via the control panel:
    - Navigate to P-CSCF → Hash Tables tab
    - Check `imei_msisdn` table contains entries
    - Verify the caller's IMEI has a mapping

2. Test with a registered user making an emergency call first (to isolate registration vs. emergency routing issues)

3. Review system logs via the control panel Logs page for emergency routing errors

4. Verify emergency Application Server configuration

5. Coordinate with system administrators to review emergency route configuration if needed

Performance Issues

High CPU Usage

Possible Causes:

- Too many registrations
- Pike anti-flood triggering
- Database slow queries

Solutions:

1. Check registration count via the control panel:
    - Navigate to P-CSCF → Registered Contacts tab
    - Review total number of active registrations
2. Review system logs for Pike anti-flood blocks
3. Coordinate with system administrators to scale horizontally (add more P-CSCF instances) if needed

High Memory Usage

Possible Causes:

- Hash table growth
- Dialog table not being cleared
- Memory leak

Solutions:

1. Review hash tables via the control panel:
    - Navigate to P-CSCF → Hash Tables tab
    - Check table sizes and entry counts
2. Clear old entries via the control panel:
    - Select problematic hash table
    - Use "Flush" operation if needed (use with caution - clears entire table)
3. Coordinate with system administrators to restart the P-CSCF service if memory leak is suspected

Diameter/Rx Issues

PCRF Peer Closed

Symptoms: Diameter peer shows "Closed" state in Web UI

Diagnostic Steps:

1. Check Diameter peer status via the control panel:
    - Navigate to Diameter page
    - Select P-CSCF node
    - Verify PCRF peer state (should be "I_Open" when connected)
2. Verify network connectivity to PCRF (coordinate with network team if needed)
3. Try to enable peer via the control panel:
    - Navigate to Diameter page
    - Find PCRF peer
    - Click "Enable" button
4. Review system logs via the control panel Logs page for Diameter connection errors

5. Coordinate with system administrators to verify Diameter configuration if needed

QoS Not Working

Symptoms: Calls connect but no QoS bearer established

Diagnostic Steps:

1. Review system logs via the control panel for AAR (Authorization Authentication Request) and AAA (Authorization Authentication Answer) messages

2. Check PCRF response result code (should be 2001 for success)

3. Verify PCRF peer is connected (see previous section)

4. Verify media information in SDP is being correctly sent to PCRF

5. Coordinate with system administrators to verify QoS configuration if needed

Best Practices

Security

1. **Always use IPsec** for mobile devices (LTE/5G)
2. **Enable TLS** for fixed/enterprise clients
3. **Configure anti-flood** (Pike) for DoS protection
4. **Limit failed auth** attempts to prevent brute force
5. **Use strong ciphers** for TLS (disable SSLv2/v3)
6. **Regularly rotate** IPsec keys (via re-registration)

Performance

1. **Tune hash_size** based on expected registrations:

    - 1,000 users: hash_size=10 (creates 2^10 = 1,024 hash buckets)
    - 10,000 users: hash_size=13 (creates 2^13 = 8,192 hash buckets)
    - 100,000 users: hash_size=16 (creates 2^16 = 65,536 hash buckets)

2. **Adjust worker processes** based on CPU cores:
    - Set children to match number of CPU cores for SIP processing
    - Set tcp_children to 2× CPU cores for TCP connection handling
3. **Use mlock_pages** to prevent swapping:
    - Enable mlock_pages=yes to lock shared memory pages in RAM
    - Prevents performance degradation from memory swapping to disk
4. **Disable DNS cache** for IMS environments:
    - Set dns_cache_init=off to use fresh DNS lookups
    - Necessary for dynamic DNS SRV-based load balancing
5. **Enable SRV load balancing**:
    - Set dns_srv_lb=yes to distribute traffic across multiple servers
    - Uses DNS SRV records for automatic load distribution

Monitoring

1. **Enable Prometheus** metrics (port 9090 in config) - See Metrics Reference for all available P-CSCF metrics
2. **Monitor registration count** trends
3. **Track Diameter peer health** (Rx to PCRF)
4. **Alert on high error rates** in logs
5. **Monitor dialog count** (active sessions)
6. **Check memory usage** regularly

High Availability

1. **Deploy multiple P-CSCF** instances

2. **Use DNS SRV** for load balancing:

```
_sip._udp.pcscf.example.com. SRV 10 50 5060
pcscf01.example.com.
_sip._udp.pcscf.example.com. SRV 10 50 5060
pcscf02.example.com.
```

3. **Avoid state** where possible (stateless proxy)

4. **Use shared database** for persistent data (if needed)

5. **Monitor via web interface** using control panel health checks

Emergency Services

1. **Always allow** emergency calls even if unregistered
2. **Store IMEI→MSISDN** mapping during registration
3. **Set TTL** for emergency hash table (86400 = 24 hours)
4. **Test regularly** with test PSAP
5. **Ensure LRF** connectivity for location
6. **Priority handling** for emergency calls

Reference

Additional Technical Resources

For system administrators and developers, technical module documentation is available online for the underlying software components.

3GPP Specifications

- **TS 23.228**: IMS Architecture
- **TS 24.229**: IMS SIP Profile
- **TS 33.203**: Access Security
- **TS 23.167**: Emergency Services

- **TS 29.214**: Rx Interface (PCRF)

RFCs

- **RFC 3261**: SIP
- **RFC 3327**: Path Header
- **RFC 3608**: Service-Route Header
- **RFC 3GPP-IMS**: P-Headers (P-Asserted-Identity, etc.)
- **RFC 5626**: Outbound (connection management)

S-CSCF Operations Guide

Table of Contents

1. Overview
2. Role in IMS Architecture
3. S-CSCF Functions
4. Web UI Operations
5. Call Flows
6. Troubleshooting

Overview

The **S-CSCF** (Serving Call Session Control Function) is the central session control server in the IMS core. It performs registration, authentication, session routing, and service triggering. The S-CSCF is the authoritative registrar for users in its home network and maintains complete session state for all calls.

3GPP Specifications

- **3GPP TS 23.228**: IP Multimedia Subsystem (IMS) Stage 2
- **3GPP TS 24.229**: IMS Call Control Protocol
- **3GPP TS 29.228**: Cx Interface (S-CSCF to HSS)
- **3GPP TS 29.229**: Cx and Dx Protocols
- **3GPP TS 23.218**: ISC Interface (S-CSCF to AS)
- **3GPP TS 32.260**: IMS Charging

Key Responsibilities

1. **Registration Authority**: Authoritative SIP registrar for home network users
2. **Authentication**: Validates user credentials via HSS
3. **Session Routing**: Routes originating and terminating calls
4. **Service Triggering**: Invokes Application Servers based on iFC (initial Filter Criteria)
5. **User Profile Management**: Stores and applies service profiles from HSS
6. **Presence**: Handles SUBSCRIBE/PUBLISH/NOTIFY for presence services
7. **PSTN Interconnection**: Routes to/from legacy PSTN networks

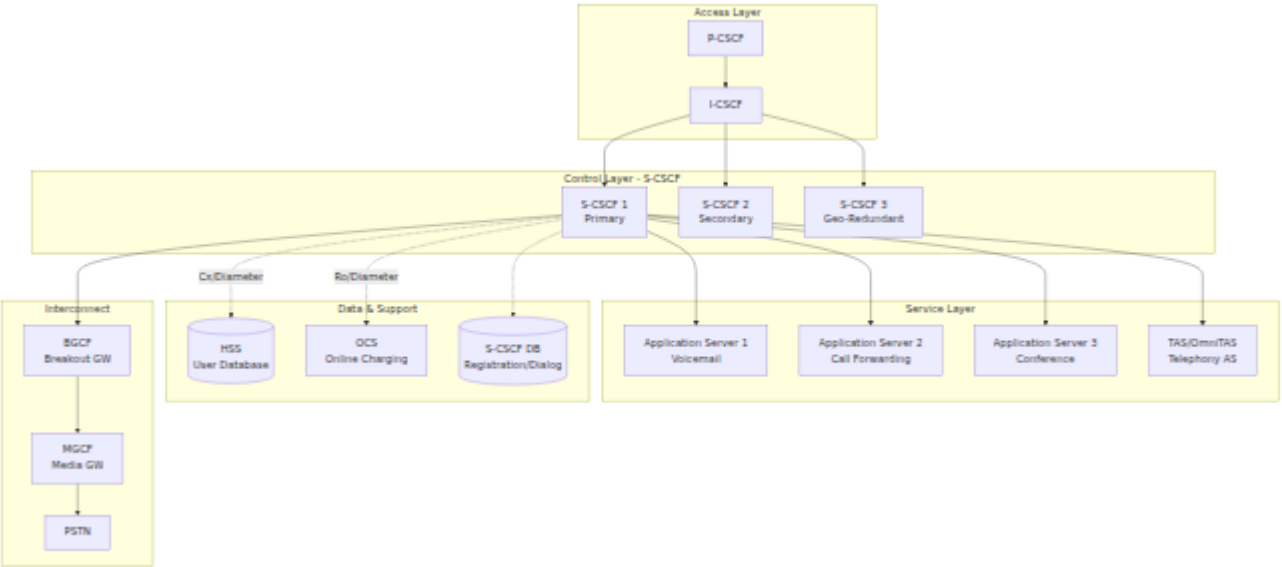
Note on Charging: While the S-CSCF has the capability to perform online charging via the Ro interface to an OCS (Online Charging System), **in our deployments this functionality is typically disabled**. Charging is instead handled by the **TAS (Telephony Application Server)** where it can properly account for complex scenarios such as call forwarding, call transfer, roaming on 2G/3G networks, and other supplementary services that the S-CSCF alone cannot accurately track.

Key Characteristics

- **Stateful**: Maintains full dialog state
- **Service Logic**: Executes complex routing rules and service triggers
- **HSS Integration**: Continuous sync with user database
- **Application Server Interface**: ISC (IMS Service Control)
- **Most Complex CSCF**: Largest configuration and most features

Role in IMS Architecture

Network Position



3GPP Reference Points

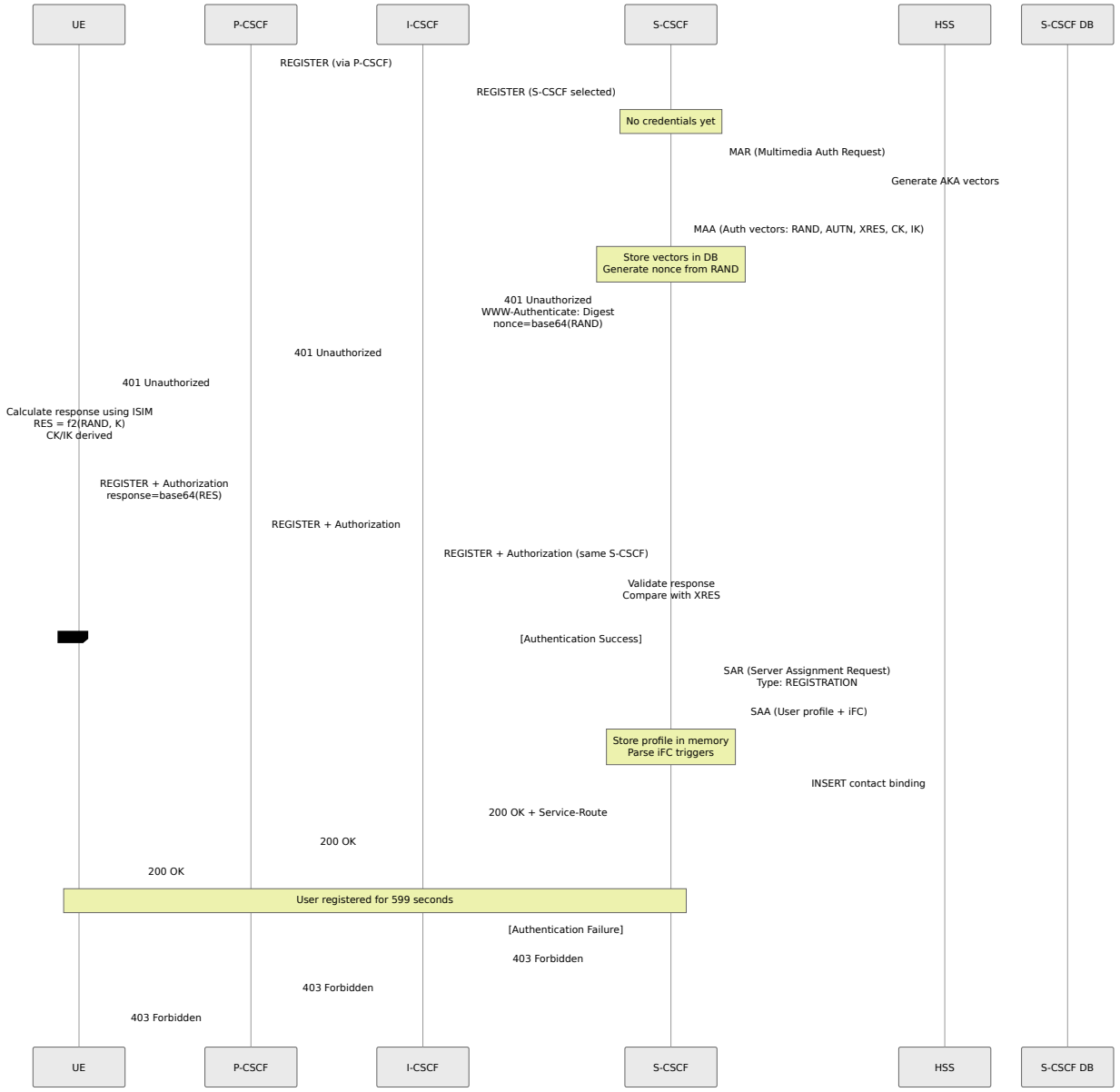
Interface	Protocol	Purpose	Connected To
Mw	SIP	I-CSCF/P-CSCF to S-CSCF	I-CSCF, P-CSCF
ISC	SIP	S-CSCF to Application Server	AS, TAS
Cx	Diameter	User data, authentication, registration	HSS
Ro	Diameter	Online charging (real-time)	OCS
Rf	Diameter	Offline charging (CDR)	CDF/CGF
Mi	SIP	S-CSCF to BGCF	BGCF (PSTN routing)

S-CSCF Functions

1. Registration and Authentication

The S-CSCF is the authoritative registrar that validates user credentials and stores registration bindings.

Registration Flow with Authentication



Authentication Algorithms Supported

Configuration: The S-CSCF is configured with the following authentication parameters:

- Authentication vector timeout: 599 seconds
- Authentication data hash size: 1024 buckets
- Checks only IMPU for authentication (not IMPI)

Supported Algorithms:

- **AKAv1-MD5**: 3GPP AKA with MD5 (most common for LTE/5G)
- **AKAv2-MD5**: Enhanced AKA
- **MD5**: HTTP Digest
- **CableLabs-Digest**: PacketCable/IMS for cable networks
- **3GPP-Digest**: Digest-MD5 variant
- **TISPAN-HTTP_DIGEST_MD5**: ETSI TISPAN
- **HSS-Selected**: Let HSS choose the algorithm

AKA Flow:

1. **RAND**: Random challenge (128 bits)
2. **AUTN**: Authentication token to prove HSS identity
3. **XRES**: Expected response from UE
4. **CK/IK**: Cipher Key / Integrity Key for IPsec

Nonce Generation:

```
nonce = base64(RAND) + ":" + algorithm_indicator
```

Response Validation:

```
UE_response = base64(RES)
Expected = base64(XRES)

if (UE_response == Expected) {
    # Authentication success
} else {
    # Authentication failure
}
```

AKA Re-Synchronization

If the UE's sequence number (SQN) is out of sync with the HSS:

Process:

1. UE sends AUTS (authentication sync token) in the Authorization header
2. S-CSCF extracts AUTS from the header
3. S-CSCF sends MAR (Multimedia-Auth-Request) with AUTS to HSS
4. HSS re-synchronizes its sequence number and sends new authentication vectors
5. S-CSCF receives new vectors and continues authentication flow

Registration Parameters

The S-CSCF is configured with the following registration parameters:

Registration Expiry Times:

- Default/Min/Max expires: 599 seconds (approximately 10 minutes)
- Subscription default/min/max expires: 599 seconds

Contact Management:

- Maximum contacts per IMPU: 1 (single device registration)
- Maximum contact behavior: Overwrite oldest (when limit exceeded, remove oldest contact)

2. User Location Database (USRLOC)

The S-CSCF maintains a database of registered users and their contact bindings.

Database Structure

The S-CSCF maintains several database tables to store registration and user information:

IMPU Table: Stores IP Multimedia Public Identities (the SIP URIs users register with). Each IMPU has attributes like:

- Public identity (sip:user@domain.com)
- Type (public user identity vs. public service identity)
- Barring status
- Registration state (registered/not registered)
- Charging function addresses (CCF1, CCF2, ECF1, ECF2)

IMPU Contact Table: Stores the actual contact bindings for each IMPU, including:

- Contact URI (where to reach the device)
- Expiration time
- Path header (route back through P-CSCF)
- User-Agent string
- Received address (actual IP where REGISTER came from)

Subscriber Table: Maps IMPIs (Private Identities) to their associated IMPUs. One private identity can have multiple public identities.

Service Profile Table: Stores the XML user profile received from the HSS during registration, including Initial Filter Criteria (iFC) for service triggering.

Hash Table Configuration

The S-CSCF uses an in-memory hash table for fast registration lookups. For deployments with 20,000+ users, the hash size should be tuned appropriately (e.g., 8,192 buckets for ~50,000 users) to maintain lookup performance.

Managing Registrations via Web UI

All user location operations can be performed through the **control panel web interface** at `/scscf`:

- **Registration List Tab**: View all registered users with pagination and search
- **User Location Tab**: Query specific IMPU details including all contact bindings
- **Quick Actions**: Lookup, deregister, dump IFC, and test IFC operations

The web interface provides a real-time view of registration status, contact bindings, and allows administrative actions like forced de-registration when needed for troubleshooting.

3. Initial Filter Criteria (iFC) and Service Triggering

The S-CSCF evaluates **iFC** (initial Filter Criteria) from the user's service profile to determine when to invoke Application Servers.

iFC Structure (XML)

Example from HSS User Profile:

```
<IMSSubscription>
  <PrivateID>user@ims.mnc001.mcc001.3gppnetwork.org</PrivateID>
  <ServiceProfile>
    <PublicIdentity>

<Identity>sip:user@ims.mnc001.mcc001.3gppnetwork.org</Identity>
      <IdentityType>0</IdentityType>  <!-- 0=public user identity
-->
    </PublicIdentity>

    <InitialFilterCriteria>
      <Priority>0</Priority>  <!-- Lower = higher priority -->
      <TriggerPoint>
        <ConditionTypeCNF>1</ConditionTypeCNF>  <!-- 0=DNF, 1=CNF
-->
        <SPT>
          <ConditionNegated>0</ConditionNegated>
          <Group>0</Group>
          <Method>INVITE</Method>
        </SPT>
        <SPT>
          <ConditionNegated>0</ConditionNegated>
          <Group>0</Group>
          <SessionCase>0</SessionCase>  <!-- 0=originating -->
        </SPT>
      </TriggerPoint>
      <ApplicationServer>

<ServerName>sip:tas.ims.mnc001.mcc001.3gppnetwork.org</ServerName>
        <DefaultHandling>0</DefaultHandling>  <!--
0=SESSION_CONTINUED, 1=SESSION_TERMINATED -->
      </ApplicationServer>
    </InitialFilterCriteria>

    <InitialFilterCriteria>
      <Priority>1</Priority>
      <TriggerPoint>
        <ConditionTypeCNF>0</ConditionTypeCNF>  <!-- DNF -->
        <SPT>
          <ConditionNegated>0</ConditionNegated>
          <Group>0</Group>
          <RequestURI>^sip:\+1800.*</RequestURI>  <!-- Toll-free -
->
```

```
        </SPT>
      </TriggerPoint>
      <ApplicationServer>
        <ServerName>sip:tollfree-as.example.com</ServerName>
        <DefaultHandling>0</DefaultHandling>
      </ApplicationServer>
    </InitialFilterCriteria>
  </ServiceProfile>
</IMSSubscription>
```

Service Point Triggers (SPT)

SPT Types:

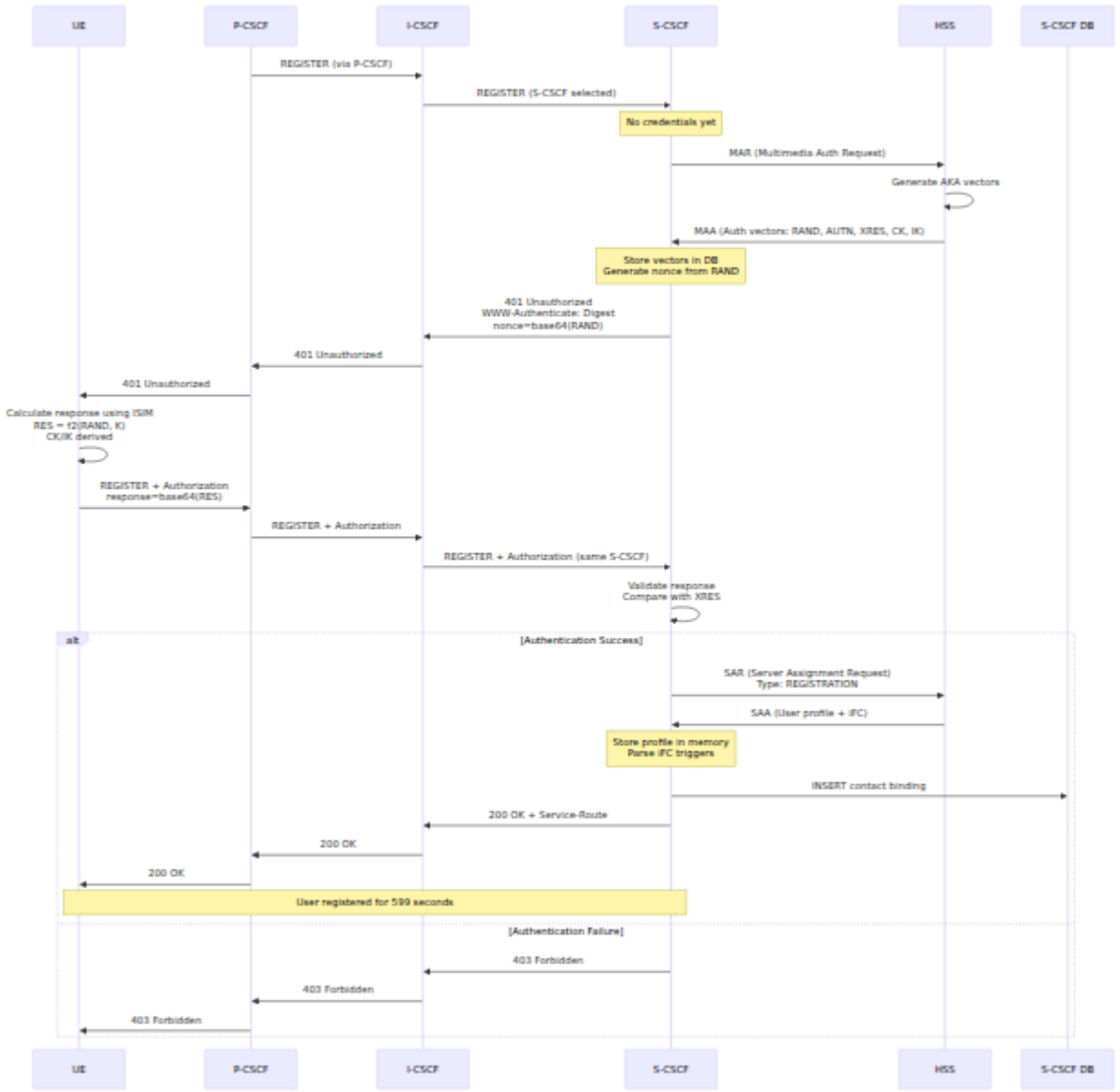
1. **Method**: SIP method (INVITE, MESSAGE, SUBSCRIBE, etc.)
2. **RequestURI**: Regex on Request-URI
3. **SIPHeader**: Check for presence/value of SIP header
4. **SessionCase**: Originating (0), Terminating (1), Terminating Unregistered (2)
5. **SessionDescription**: SDP content (media type, codec, etc.)

Logic:

- **CNF** (Conjunctive Normal Form): AND of ORs - `(A OR B) AND (C OR D)`
- **DNF** (Disjunctive Normal Form): OR of ANDs - `(A AND B) OR (C AND D)`

Group: SPTs with same group number are OR'd together, then groups are AND'd (for CNF).

iFC Matching Flow



iFC Testing via Web UI

The control panel provides two operations through the web interface:

1. **Dump iFC**: Show all iFC for a user - displays the complete XML structure of trigger points and Application Server routing

2. **Test iFC**: Simulate a call to see which AS would be triggered - tests a hypothetical call scenario with specified IMPU, originating URI, and destination URI to determine which iFC would match

Web UI Workflow:

1. Navigate to S-CSCF page

2. Click "IFC" tab
3. Enter IMPU
4. Choose "Dump IFC" or "Test IFC"
5. View detailed iFC structure with trigger points and AS routing

4. Dialog Management

The S-CSCF maintains full SIP dialog state for all active calls.

Dialog Database

The S-CSCF maintains a dialog table that tracks active calls with the following information:

- Call-ID (unique identifier for the SIP dialog)
- From/To URIs and tags
- Caller and callee sequence numbers (CSeq)
- Route sets for both parties
- Contact addresses
- Socket information
- Dialog state and timestamps
- Timeout values

Dialog States

Dialogs transition through three states:

- **Early**: Provisional response received (e.g., 180 Ringing)
- **Confirmed**: 200 OK received and ACK sent/received (call active)
- **Deleted**: BYE sent/received (call ended)

Dialog Configuration

The dialog module is configured to:

- Detect spiral routing (same request passing through multiple times)
- Maintain separate profiles for originating and terminating sides

- Persist dialogs to database (write-through mode with periodic updates)
- Set dialog-specific timeouts
- Track route sets for proper in-dialog routing

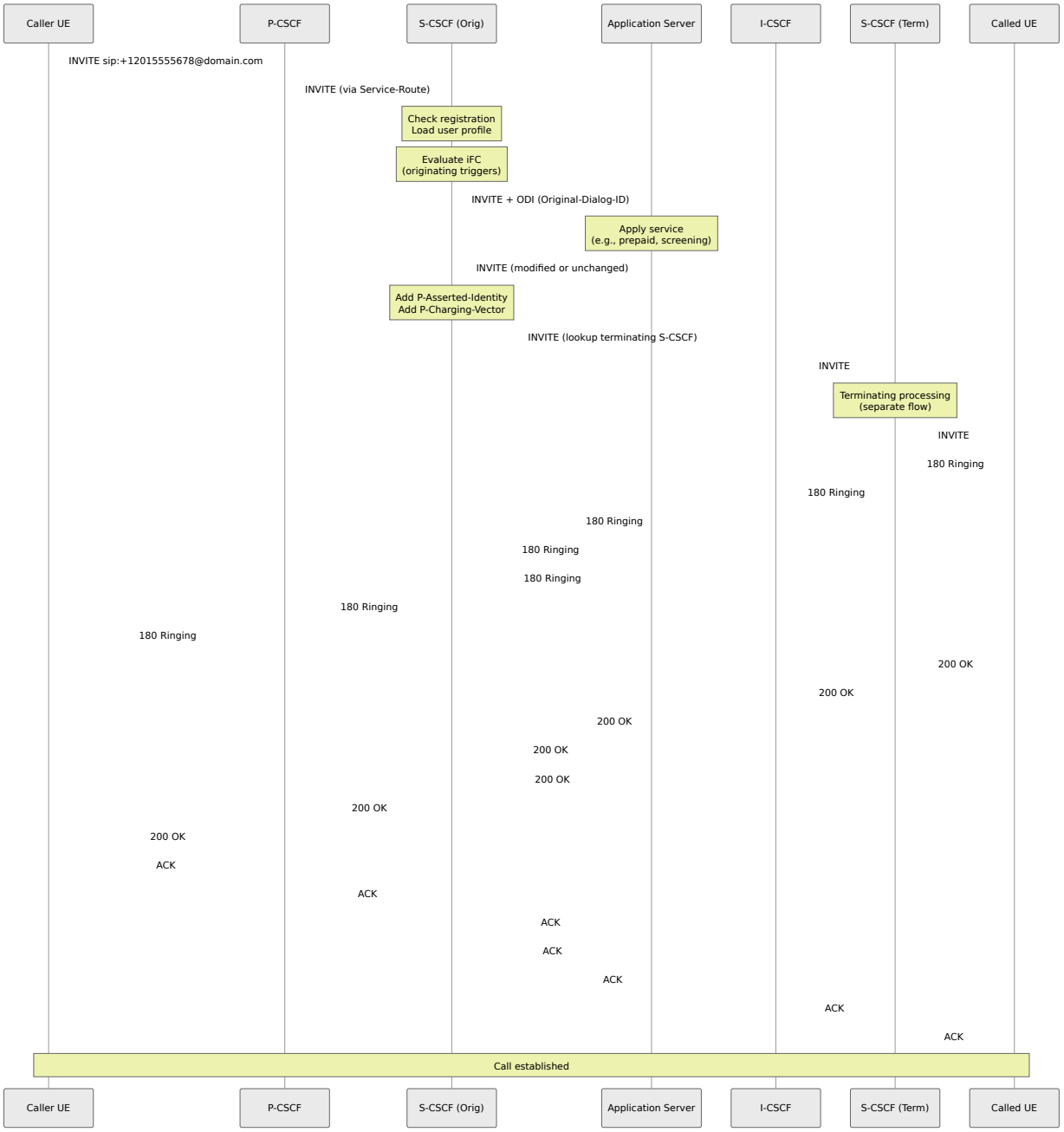
Web UI Operations:

1. Navigate to S-CSCF → Dialogs tab
2. View active calls with:
    - Call-ID
    - From/To URIs
    - State (Early/Confirmed)
    - Start time
    - Timeout
3. Click "End Dialog" to terminate specific call
4. Click "End All Active Dialogs" for emergency mass termination

5. Originating Call Handling

When a registered user initiates a call, the S-CSCF processes it as an **originating** session.

Originating Call Flow



Originating Route Configuration

Originating Call Processing: The S-CSCF performs several validation and routing steps when processing originating calls:

1. **Registration Check**: Verifies that the calling user is currently registered. If not, the call is rejected with a 403 Forbidden response.

2. **Identity Header Management**:

    - Removes any existing P-Asserted-Identity headers from the request

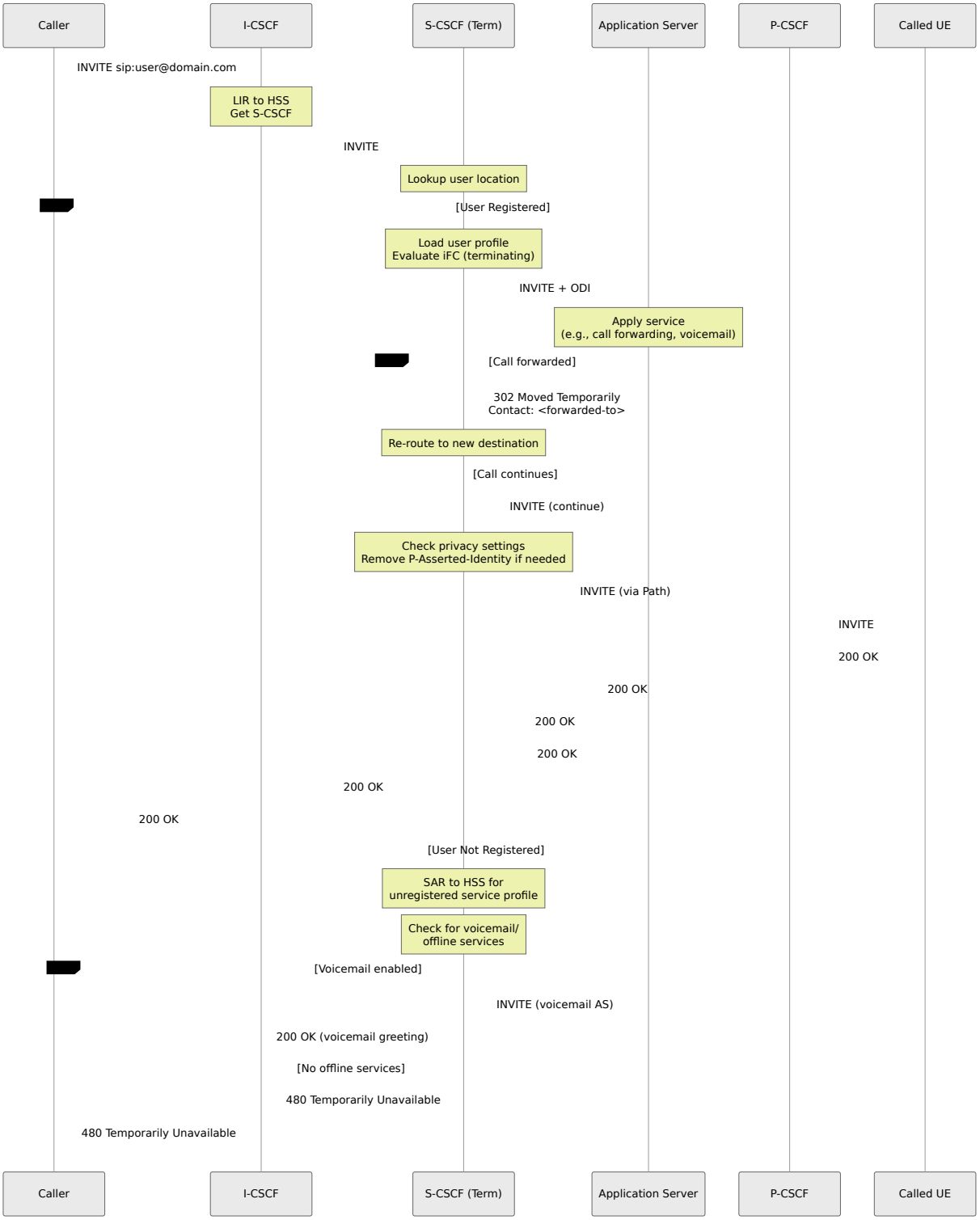
    - Adds a new P-Asserted-Identity header containing the authenticated caller's identity

3. **Charging Correlation**: Creates and adds a P-Charging-Vector header containing:
    - IMS Charging Identifier (icid) generated from the Call-ID and timestamp
    - Originating Inter-Operator Identifier (orig-ioi) for multi-operator charging
4. **Service Triggering**: Evaluates Initial Filter Criteria (iFC) for originating session triggers to determine if any Application Servers should be invoked
5. **Online Charging** (if enabled): Initiates a Diameter Ro Credit Control Request (CCR) with event type "0" (initial request) for originating calls
6. **Dialog Tracking**: Assigns the call to the "orig" (originating) dialog profile for tracking purposes
7. **Routing Decision**: Routes the call either to PSTN handling (if destination is a phone number) or to the terminating I-CSCF for IMS routing

6. Terminating Call Handling

When a call is destined for a registered user, the S-CSCF processes it as **terminating**.

Terminating Call Flow



Terminating Route Configuration

Terminating Call Processing: The S-CSCF handles terminating calls by first attempting to locate the called user and then applying appropriate service logic:

1. **User Location Lookup**: Queries the registration database to determine if the called user is currently registered
    - Uses the Request-URI username and domain to construct the IMPU
    - Retrieves contact bindings and routing information if registered
2. **If User is NOT Registered**:
    - Attempts to retrieve unregistered service profile from HSS via Server Assignment Request (SAR)
    - If successful, evaluates iFC for "unregistered terminating" session triggers (e.g., voicemail, offline services)
    - If no unregistered services are available, responds with 480 Temporarily Unavailable
3. **If User IS Registered**:
    - Evaluates iFC for "terminating" session triggers to determine Application Server invocation
    - Initiates online charging (if enabled) by sending Diameter Ro CCR with event type "0" for terminating calls
    - Assigns call to "term" (terminating) dialog profile for tracking
    - Forwards the INVITE to the registered P-CSCF using the Path header stored during registration

7. PSTN Interconnection via OmniTAS

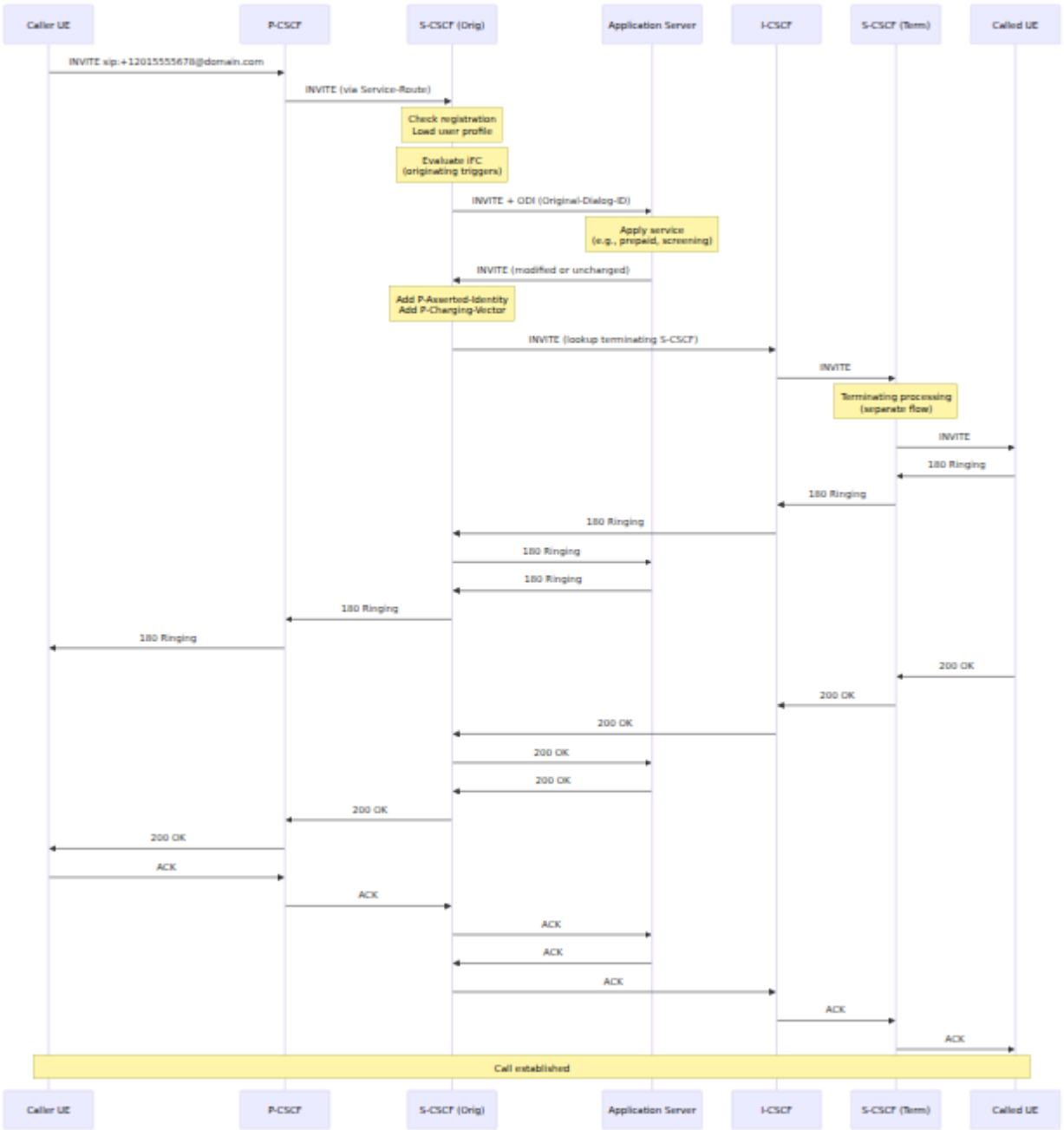
The S-CSCF routes calls to/from PSTN via the **Mi interface** to the **BGCF (Breakout Gateway Control Function)**, which is integrated within OmniTAS in our deployment.

Mi Interface - S-CSCF to BGCF

3GPP Reference Point: Mi (SIP interface between S-CSCF and BGCF)

The Mi interface is used when the S-CSCF determines that a call needs to break out to the PSTN. In our architecture, the BGCF functionality is built directly into OmniTAS, so all mobile-originated (MO) calls destined for PSTN numbers are routed to OmniTAS.

PSTN Routing Flow



How PSTN Routing Works:

1. **Destination Number Detection**: The S-CSCF examines the Request-URI to determine if the destination is a phone number (E.164 format like +12015551234)

2. **Route to OmniTAS**: For PSTN destinations, the S-CSCF routes the call via the Mi interface to OmniTAS, which includes integrated BGCF functionality

3. **BGCF Processing at OmniTAS**: OmniTAS determines the appropriate PSTN breakout point based on:

    - Destination number analysis (country code, area code)
    - Least-cost routing rules
    - Available trunk groups
    - Carrier selection

4. **PSTN Breakout**: OmniTAS handles the actual media gateway interaction to complete the call to the PSTN network

Mi Interface Details:

- **Protocol**: SIP
- **Purpose**: Route PSTN-destined calls from S-CSCF to BGCF
- **Direction**: S-CSCF → OmniTAS (with BGCF)
- **Call Types**: Mobile originated (MO) calls to PSTN numbers

Configuration: The S-CSCF is configured to recognize PSTN destinations (phone numbers) and route them to OmniTAS. When OmniTAS is used as the TAS (Telephony Application Server), it inherently includes BGCF capabilities, eliminating the need for a separate BGCF component.

8. Charging Architecture

The S-CSCF has built-in capability to interface with an OCS (Online Charging System) via the Diameter Ro interface for real-time credit control. However, **in our deployments, S-CSCF charging is typically disabled** in favor of performing charging at the **TAS (Telephony Application Server)** level.

Why Charging is Done at the TAS Instead of S-CSCF

TAS-Based Charging Advantages:

1. **Call Forwarding Scenarios**: When a call is forwarded, the S-CSCF only sees the initial INVITE to the original destination. It doesn't have visibility into the forwarding logic or final destination. The TAS, however, handles the forwarding service and knows:

    - Who initiated the call
    - Who the call was originally for

    - Where the call was forwarded to
    - Duration of the forwarded call
    - Proper party to charge (caller, forwardee, or both)

2. **2G/3G Roaming**: When subscribers roam on legacy 2G/3G networks, calls may bypass the IMS core entirely and route through circuit-switched infrastructure. The TAS integrates with both IMS and CS (Circuit Switched) domains and can:

    - Detect when a subscriber is roaming on 2G/3G
    - Apply appropriate roaming charges
    - Track call duration across network types
    - Handle handoffs between IMS and CS domains

3. **Call Transfer**: Similar to call forwarding, call transfers involve mid-call changes that the S-CSCF doesn't track:

    - Blind transfers (immediate handoff)
    - Attended transfers (consultation then handoff)
    - Transfer to voicemail
    - Multi-party transfers

4. **Conference Calls**: Multi-party conferences require special charging logic:

    - Who initiated the conference
    - How many participants
    - Duration each participant was on the call
    - Different rates for conference initiator vs. participants

5. **Supplementary Services**: Services like call waiting, call hold, and three-way calling require the TAS to understand service state:

    - Multiple simultaneous calls per user
    - Hold/resume events
    - Merged calls

6. **Prepaid vs. Postpaid Logic**: The TAS can apply different charging strategies:

    - Prepaid: Real-time credit checks and call cutoff
    - Postpaid: CDR generation for monthly billing
    - Hybrid: Different rates for different service features

7. **Rating Flexibility**: The TAS has full context to apply complex rating rules:
    - Time-of-day pricing
    - Destination-based pricing (local, long distance, international)
    - Volume discounts
    - Promotional rates
    - Bundle minutes vs. overage charges

S-CSCF Charging Limitations:

- Only sees basic SIP dialog (INVITE → 200 OK → BYE)
- No knowledge of supplementary services
- Cannot track call state changes mid-call
- Limited context for rating decisions
- Doesn't understand CS domain activity

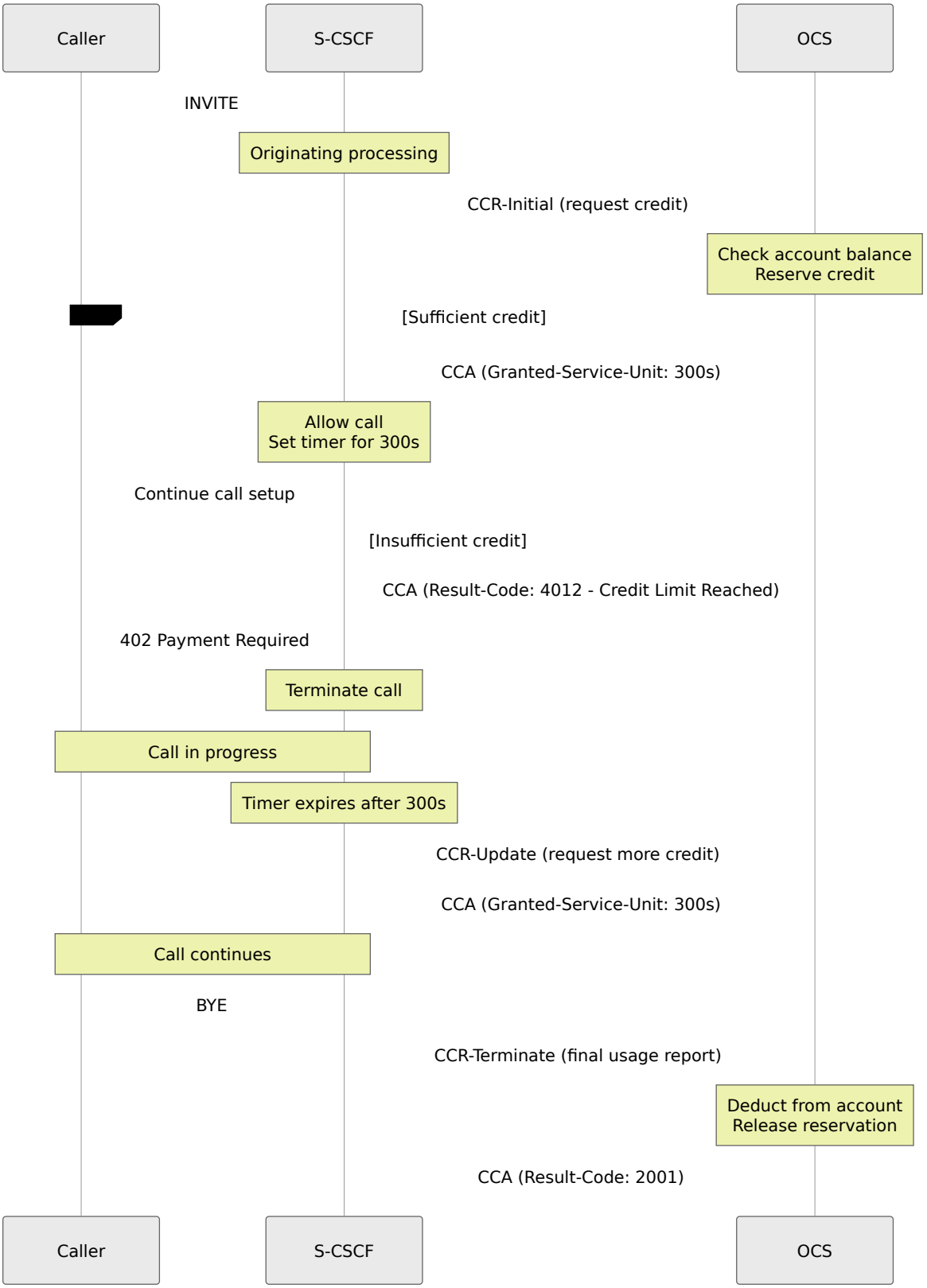
S-CSCF Ro Interface (Available but Disabled by Default)

While not used in production, the S-CSCF does support online charging via Diameter Ro. This capability remains in the configuration but is deactivated.

How S-CSCF Charging Would Work (If Enabled)

If S-CSCF charging were enabled, the system would use the Diameter Ro interface (Application ID 4) to communicate with an OCS. The S-CSCF would be configured with the OCS peer information (FQDN, realm, port 3868) and would send Credit Control Requests (CCR) at three key points in the call lifecycle:

CCR Flow (If Enabled):



When Charging Would Trigger:

1. **CCR-Initial**: Sent when the INVITE is received, before allowing the call to proceed. The OCS checks the account balance and either grants credit (allowing the call) or denies it (call rejected with 402 Payment Required).

2. **CCR-Update**: Sent periodically during the call based on the Granted-Service-Unit time from the OCS (e.g., every 300 seconds). This ensures long calls don't exceed available credit.

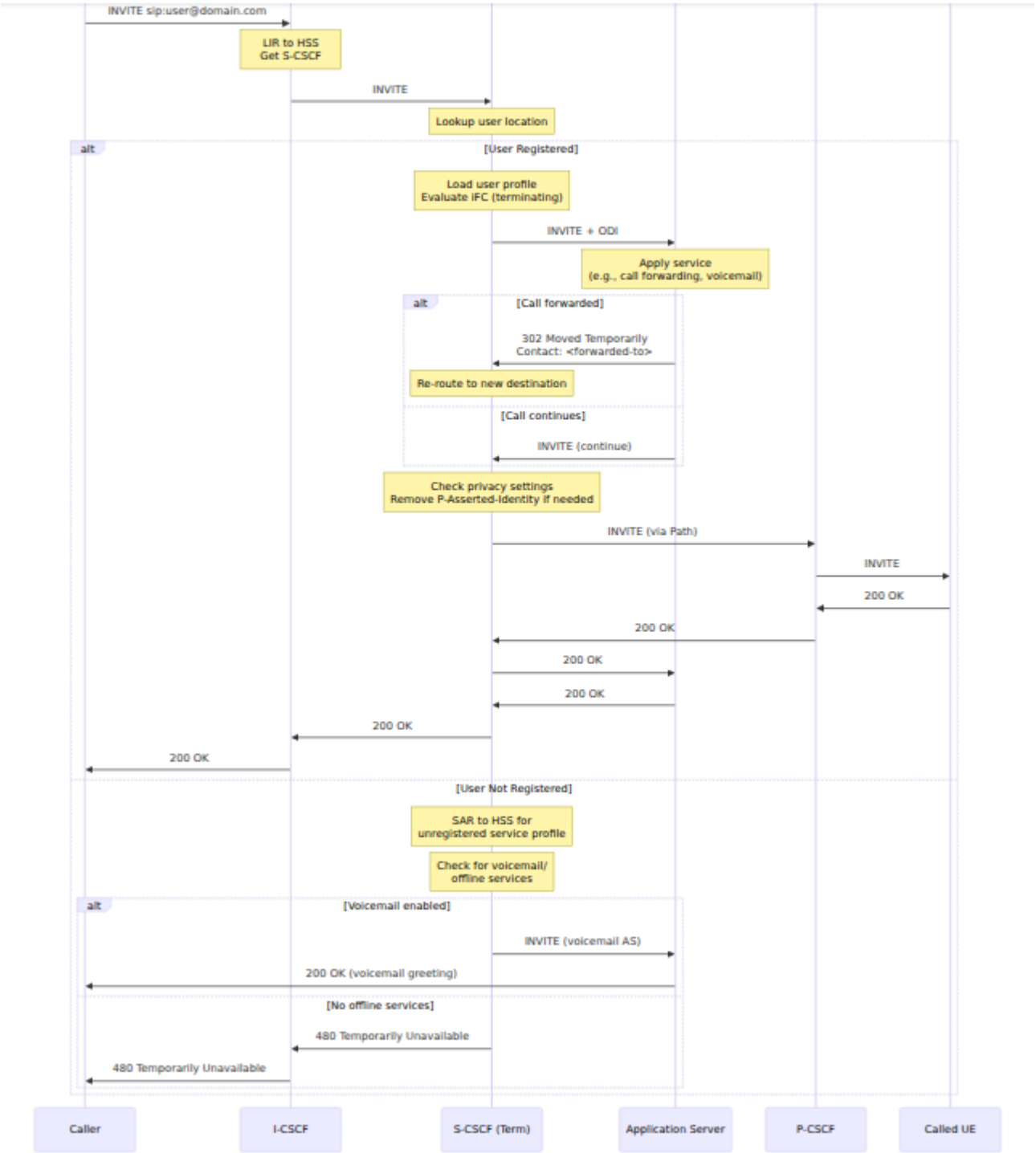
3. **CCR-Terminate**: Sent when the call ends (BYE received or dialog timeout), reporting final usage to the OCS for account deduction.

Actual Deployment: Since this charging functionality is disabled in our deployments, the S-CSCF simply routes calls without any credit control checks. All charging logic is handled downstream by the TAS, which has full visibility into the complete call flow and service context.

9. Presence and SUBSCRIBE/PUBLISH

The S-CSCF handles SIP presence for user availability status.

Presence Architecture



Presence Configuration

The S-CSCF presence functionality is configured with:

- **Maximum expires**: 3600 seconds (1 hour) - maximum subscription duration
- **Default state**: "active" - presence state defaults to active

- **PIDF support**: Enabled - allows modification of PIDF (Presence Information Data Format) documents

PUBLISH Handling

Presence Publication Processing: When the S-CSCF receives a PUBLISH request (used to update presence status):

1. **Method Detection**: Checks if the incoming request is a PUBLISH method
2. **Authorization Check**: Verifies the user is currently registered in the location database. If not registered, responds with 403 Forbidden
3. **Presence Update**: Processes the PUBLISH request to update the user's presence information in the presence database
4. **Error Handling**: If presence handling fails (e.g., database error, malformed presence document), responds with 500 Server Error

SUBSCRIBE Handling

Presence Subscription Processing: When the S-CSCF receives a SUBSCRIBE request (used to watch another user's presence):

1. **Method Detection**: Checks if the incoming request is a SUBSCRIBE method
2. **Event Type Check**: Examines the Event header to determine subscription type
   - If Event is "reg" (registration event package), this is a subscription to registration state changes
   - For reg event subscriptions, performs Server Assignment Request (SAR) to HSS if user is not registered, to get service profile
   - Evaluates iFC for "subscribe" triggers to determine if any Application Servers should handle the subscription
3. **Presence Subscription Processing**: Handles the SUBSCRIBE request to create or refresh a presence watcher subscription
4. **Error Handling**: If subscription processing fails, responds with 500 Server Error

Web UI Operations

Accessing S-CSCF Page

Navigate to: `https://<control-panel>/scscf`

Page Layout

The S-CSCF page has five main tabs:

1. **Registration List** - Paginated list of registered users
2. **User Location** - Query specific IMPU details
3. **Dialogs** - Active call sessions
4. **IFC** - Initial Filter Criteria management and testing
5. **Hash Tables** - Shared memory tables

Registration List Tab

Purpose: View all registered users with pagination

Display Columns:

- **IMPU**: IP Multimedia Public Identity (SIP URI)
- **Contacts**: Number of registered contact bindings
- **State**: Registration state (Registered/Not Registered)
- **Expires**: Registration expiry timestamp

Features:

- Pagination (50 users per page)
- Search by IMPU or contact
- Sort by column
- Click row to expand and see contact details

Example:

```
IMPU: sip:12015551234@ims.mnc001.mcc001.3gppnetwork.org
Contacts: 1
State: Registered
Expires: 2025-11-29 15:45:30

[Expand to see:]
  Contact: sip:12015551234@10.4.12.100:5060;transport=tcp
  Path: <sip:term@pcscf.ims.mnc001.mcc001.3gppnetwork.org:5060;lr>
  User-Agent: Android IMS Client v1.0
  Received: 10.4.12.100:52341
```

Quick Actions:

- **Lookup**: Quick search for specific IMPU
- **Dump IFC**: View Initial Filter Criteria for user
- **Test IFC**: Simulate call to test AS triggering
- **Deregister**: Force de-registration (use with caution!)

User Location Tab

Purpose: Detailed query of specific IMPU

Operations:

1. Enter IMPU (e.g., `sip:user@domain.com`)
2. Click "Lookup"
3. View detailed information:
    - All registered contacts
    - Service-Route header
    - Registration timestamps
    - Path headers
    - Associated IMPIs (Private Identities)

Use Cases:

- Troubleshoot why user can't receive calls
- Verify registration details
- Check contact bindings
- Verify service routes

Dialogs Tab

Purpose: Monitor and manage active call sessions

Display Columns:

- **Call-ID**: SIP Call-ID
- **From URI**: Caller identity
- **To URI**: Called identity
- **State**: Early (ringing) or Confirmed (answered)
- **Start Time**: When dialog was created
- **Timeout**: Dialog timeout value

Operations:

- **Refresh**: Manual refresh (auto-refresh every 5s)
- **End Dialog**: Terminate specific call (sends BYE)
- **End All Active Dialogs**: Emergency mass termination

Example:

```
Call-ID: 3c26700857a87f84@10.4.12.165
From: sip:12015551234@ims.mnc001.mcc001.3gppnetwork.org
To: sip:+12015555678@ims.mnc001.mcc001.3gppnetwork.org
State: Confirmed
Start Time: 2025-11-29 15:30:15
Timeout: 360000 seconds

[End Dialog] button
```

Warning: Ending dialogs will immediately terminate active calls. Use for troubleshooting or emergency situations only.

IFC Tab

Purpose: View and test Initial Filter Criteria for service triggering

The IFC tab provides two main operations: Dump IFC (retrieve and display a user's IFC from HSS) and Test IFC (simulate a call scenario to see which Application Servers would be triggered).

Dump IFC Operation

1. Enter IMPU: `sip:user@domain.com`
2. Click "Dump IFC"
3. View detailed iFC structure:
    - Priority order
    - Trigger points (SPT conditions)
    - Application Server URIs
    - Default handling

Example Output:

```
<InitialFilterCriteria>
  <Priority>0</Priority>
  <TriggerPoint>
    <ConditionTypeCNF>1</ConditionTypeCNF>
    <SPT>
      <Group>0</Group>
      <Method>INVITE</Method>
    </SPT>
    <SPT>
      <Group>0</Group>
      <SessionCase>0</SessionCase>  <!-- Originating -->
    </SPT>
  </TriggerPoint>
  <ApplicationServer>

<ServerName>sip:tas.ims.mnc001.mcc001.3gppnetwork.org</ServerName>
    <DefaultHandling>0</DefaultHandling>
  </ApplicationServer>
</InitialFilterCriteria>
```

Test IFC Operation

1. Enter IMPU: `sip:user@domain.com`
2. Enter Originating URI: `sip:user@domain.com` (calling party)
3. Enter Destination URI: `sip:+12015555678@domain.com` (called party)
4. Click "Test IFC"
5. View results:
   - Which iFC matched
   - Which Application Servers would be invoked
   - In what order (priority)

Use Cases:

- Verify service triggering configuration
- Troubleshoot why AS is not being invoked
- Test new iFC before deploying to production
- Understand call flow for specific scenarios

Hash Tables Tab

Similar to P-CSCF and I-CSCF, manage shared memory hash tables.

Common S-CSCF Hash Tables:

- `auth`: Authentication vectors cache
- `profile`: Cached user profiles (if using)
- Custom tables for service logic

Call Flows

Complete Registration Flow

See "1. Registration and Authentication" section above for detailed sequence diagram.

Complete Originating Call Flow

See "5. Originating Call Handling" section above for detailed sequence diagram.

Complete Terminating Call Flow

See "6. Terminating Call Handling" section above for detailed sequence diagram.

Troubleshooting

Registration Issues

User Cannot Register - 403 Forbidden

Possible Causes:

- User not provisioned in HSS
- HSS unreachable
- Authentication failure
- Barring applied

Diagnostic Steps:

1. Check HSS connectivity via the control panel:
    - Navigate to Diameter page
    - Select S-CSCF node
    - Verify HSS peer shows as "I_Open" (connected)
2. Review S-CSCF logs for MAR/MAA (Multimedia Auth Request/Answer) message flow
3. Verify user exists in HSS (if accessible)
4. Check S-CSCF logs for authentication vectors received from HSS
5. Test with different authentication algorithm if supported

User Cannot Register - 500 Server Error

Possible Causes:

- Database connection lost
- SAR/SAA failure
- Module error

Solutions:

1. Check database connectivity from the S-CSCF server (verify database is reachable and credentials are correct)
2. Review S-CSCF logs for SAR/SAA (Server Assignment Request/Answer) Diameter message flow
3. Restart S-CSCF service if needed to recover from module errors

Call Routing Issues

Calls Not Routing to User

Symptoms: INVITE reaches S-CSCF but doesn't forward to P-CSCF

Diagnostic Steps:

1. Check user is registered via the control panel web interface:
    - Navigate to S-CSCF → User Location tab
    - Enter the IMPU and click "Lookup"
    - Verify user shows as registered with contact bindings
2. Verify contact bindings exist and Path header is present
3. Review S-CSCF logs for terminating route processing
4. Test with different destination to isolate issue

Application Server Not Triggered

Symptoms: iFC should match but AS not invoked

Diagnostic Steps:

1. Dump iFC via the control panel web interface:
    - Navigate to S-CSCF → IFC tab
    - Enter the IMPU
    - Click "Dump IFC"
    - Review the trigger points and Application Server URIs
2. Test iFC matching via the web interface:
    - Navigate to S-CSCF → IFC tab
    - Enter IMPU, originating URI, and destination URI
    - Click "Test IFC"
    - Verify which iFC should have matched

3. Check if user profile was loaded from HSS by reviewing logs
4. Verify SAA (Server Assignment Answer) from HSS contained user profile XML
5. Review S-CSCF logs for iFC parsing errors

Dialog Issues

Dialogs Not Terminating After BYE

Symptoms: Dialog remains in database after call ends

Solutions:

1. Check active dialogs via the control panel:
    - Navigate to S-CSCF → Dialogs tab
    - Review dialog count and states
2. Verify BYE detection in dialog module logs
3. Check dialog timeout settings in configuration
4. Manually end dialog via the control panel:
    - Navigate to S-CSCF → Dialogs tab
    - Find the stuck dialog
    - Click "End Dialog"
5. Review database for orphaned dialog entries and clean up if needed

Charging Issues

CCR Timeout

Note: In our deployments, S-CSCF charging is typically disabled. Charging is handled by the TAS. If you're seeing charging-related errors, verify that S-CSCF Ro charging wasn't accidentally enabled.

Symptoms: Calls fail with charging errors (if charging is enabled)

Possible Causes:

- OCS unreachable
- Diameter Ro peer down
- Transaction timeout too short

Solutions:

1. Check OCS peer status via the control panel:
    - Navigate to Diameter page
    - Select S-CSCF node
    - Check if OCS peer shows as "I_Open" (connected)
2. Test OCS network connectivity from the S-CSCF server
3. Review Diameter transaction timeout configuration
4. Check S-CSCF logs for CCR/CCA message flow and errors

Insufficient Credit - All Calls Fail

Note: This issue only applies if S-CSCF charging is enabled (which it typically isn't in our deployments).

Symptoms: Users get 402 Payment Required for all calls

Solutions:

1. Verify S-CSCF charging should actually be enabled (usually it should be disabled)
2. Check OCS balance for test accounts if charging is intentionally enabled
3. Review CCA (Credit Control Answer) result codes in S-CSCF logs
4. Consider disabling S-CSCF charging and using TAS-based charging instead

PSTN Issues

Calls to PSTN Fail - 503 No Gateway Available

Possible Causes:

- No MGCF/gateway configured
- All gateways down
- Dispatcher not loaded

Solutions:

1. Coordinate with system administrators to verify PSTN gateways are configured
2. Test gateway connectivity from the S-CSCF server (network reachability, SIP response)
3. Review gateway configuration with system administrators
4. Add missing gateways if needed via system administrators

Performance Issues

High CPU Usage

Possible Causes:

- Too many dialogs
- Database slow queries
- iFC evaluation overhead

Solutions:

1. Check dialog count via the control panel:
    - Navigate to S-CSCF → Dialogs tab
    - Review number of active dialogs

2. Optimize database tables (dialog, impu, impu_contact) if database queries are slow

3. Add database indexes if needed (on impu.impu, dialog.callid, etc.)

4. Tune worker process count in configuration if needed (increase from default 4 to 8 for high load)

Best Practices

High Availability

1. **Deploy multiple S-CSCFs** with shared database
2. **Use capabilities** for S-CSCF selection at I-CSCF
3. **Database replication**: Master-master or master-slave
4. **Session persistence**: Write-through dialog mode
5. **Health checks**: Monitor registration and dialog counts

Security

1. **Always authenticate** users via HSS
2. **Validate P-Asserted-Identity** from trusted sources only
3. **Rate limit** registrations and calls per user
4. **Sanitize headers** from untrusted networks
5. **Use TLS** for Diameter (Cx, Ro)

Performance

1. **Tune hash_size for user location**: The hash size should be set based on expected user count. For example, hash_size=13 (which equals 2^13 = 8192 buckets) is appropriate for approximately 50,000 users

2. **Cache user profiles**: If the HSS supports it, enable profile caching to reduce Diameter SAR requests

3. **Optimize iFC**: Keep Service Point Trigger (SPT) conditions simple and minimize the number of iFC rules per user to reduce evaluation overhead

4. **Use async operations for Diameter**: Configure asynchronous processing for MAR (authentication), SAR (registration), and CCR (charging) to prevent blocking worker processes

5. **Monitor database performance regularly**: Track query execution times, optimize indexes, and ensure connection pooling is working efficiently

Monitoring

For a complete list of all S-CSCF metrics, see the **Metrics Reference**.

Key metrics to track:

- Registration success rate
- MAR/SAR/LIR success rate
- Dialog count (active calls)
- iFC evaluation time
- Database query latency
- Diameter peer uptime
- Call setup time

Reference

3GPP Specifications

- **TS 23.228**: IMS Architecture
- **TS 24.229**: IMS SIP Protocol
- **TS 29.228**: Cx Interface
- **TS 23.218**: ISC Interface
- **TS 32.260**: IMS Charging

Web UI Operations Guide

Table of Contents

1. Overview
2. Accessing the Control Panel
3. P-CSCF Management
4. I-CSCF Management
5. S-CSCF Management
6. Diameter Peer Management
7. Hash Table Operations
8. Logs Viewing
9. Monitoring and Metrics

Overview

The OmniCall CSCF Web UI provides a comprehensive control panel for real-time monitoring and management of all CSCF components (P-CSCF, I-CSCF, S-CSCF). The interface is built on Phoenix LiveView and provides:

- **Real-time visibility** into registrations, active calls, and system state
- **Hash table management** for performance-critical in-memory data structures
- **Diameter peer monitoring** and control
- **Prometheus metrics** for system monitoring
- **Live log viewing** for troubleshooting

Architecture

The control panel communicates with CSCF backend instances to:

- Query user registrations and location data
- Inspect active dialogs (calls)
- Manage Diameter peers
- View and manipulate hash tables
- Access Initial Filter Criteria (IFC) configuration

Accessing the Control Panel

Default Access

The control panel is accessible via HTTP on the CSCF server:

```
http://<cscf-server>:4000/
```

Default Port: 4000 (configurable in `ControlPanel.Supervisor`)

Configuration

The control panel requires CSCF host configuration in `config/config.exs` or `config/runtime.exs`:

```
config :cscf, :cscf_hosts,
  pcscf: [
    {host: "10.4.12.165", port: 9060, label: "P-CSCF 1"}
  ],
  icscf: [
    {host: "10.4.12.166", port: 9060, label: "I-CSCF 1"}
  ],
  scscf: [
    {host: "10.4.12.167", port: 9060, label: "S-CSCF 1"}
  ]
```

Navigation

The control panel provides navigation tabs for each CSCF component:

- **P-CSCF** - `/pcscf` - Registration contacts and hash tables
- **I-CSCF** - `/icscf` - S-CSCF list, NDS domains, sessions
- **S-CSCF** - `/scscf` - Registrations, dialogs, IFC management
- **Diameter** - `/diameter` - Diameter peer status and control
- **Logs** - `/logs` - Live log viewing

P-CSCF Management

URL: `/pcscf`

Features

The P-CSCF panel displays registered contacts and hash table information from P-CSCF instances.

Registered Contacts Tab

Displays all current IMS registrations visible to the P-CSCF:

Column	Description
IMSI	Subscriber IMSI or Contact identifier
State	Registration state (registered, unregistered)
Expires	Time until registration expires
Path	SIP Path header for routing

Operations:

- **Click on row** to expand and view detailed contact information including:
  - Full AoR (Address of Record)
  - UE IP address
  - Path details
  - Statistics (max slots, records)

Hash Tables Tab

Manage P-CSCF hash tables. See Hash Table Operations below.

Real-time Updates

The P-CSCF view automatically refreshes every 5 seconds to show current registration status.

I-CSCF Management

URL: `/icscf`

Features

The I-CSCF panel provides monitoring of I-CSCF operations including S-CSCF selection and session tracking.

S-CSCF List Tab

Displays all configured S-CSCF servers known to the I-CSCF:

- **ID**: S-CSCF identifier
- **Name**: S-CSCF FQDN
- **Capabilities**: Number of supported capabilities

NDS Domains Tab

Shows trusted NDS (Network Domain Security) domains configured on the I-CSCF.

Sessions Tab

Displays active I-CSCF sessions including:

- **Call-ID**: SIP Call-ID
- **S-CSCF Candidates**: List of S-CSCF servers considered for assignment
  - S-CSCF name

    - Selection score
    - Age (time since candidate was added)

Hash Tables Tab

Manage I-CSCF hash tables. See Hash Table Operations below.

S-CSCF Management

URL: `/scscf`

The S-CSCF panel is the most feature-rich, providing comprehensive registration, dialog, and IFC management.

List Registrations Tab

Browse all active registrations with pagination:

Features:

- **Pagination controls**: Offset and limit for large registration databases
- **Registration details** for each IMPU:
    - Public user identity (IMPU)
    - Registration state
    - Slot number
    - Contact details with User-Agent and expiry
    - Call-ID

Quick Actions for each registration:

- **Lookup**: View detailed IMPU information
- **Dump IFC**: View Initial Filter Criteria for the user
- **Test IFC**: Test IFC matching for simulated calls
- **Deregister**: Administratively remove registration

User Location Tab

Query and inspect user location data:

- View raw user location status from S-CSCF
- **IMPU Lookup form**: Query specific public user identity
- Displays complete registration details including contacts, state, and metadata

Dialogs Tab

Manage active call sessions (dialogs):

Column	Description
Dialog ID	h_entry:h_id identifier
Call-ID	SIP Call-ID
From	Calling party URI
To	Called party URI
State	Dialog state

Operations:

- **End Dialog**: Terminate specific call (sends BYE)
- **End All**: Terminate all active calls (with confirmation)

IFC Tab

Initial Filter Criteria tools for service triggering management:

Dump IFC

Retrieve and display all IFC rules for a given IMPU:

- Public identity
- Private identity
- Service profile count
- **Filter Criteria** for each service profile:
  - Priority (execution order)
  - Default handling (SESSION_CONTINUED vs SESSION_TERMINATED)
  - Application Server name
  - REGISTER inclusion flags
  - **Trigger Point** details:
    - Condition type (DNF or CNF)
    - Service Point Triggers (SPTs):
      - METHOD, HEADER, SESSION_CASE, REQUEST_URI, etc.
      - Negation flags

The IFC display includes:

- Color-coded priority badges
- Expandable trigger point logic explanations
- DNF (Disjunctive Normal Form) = OR of ANDs
- CNF (Conjunctive Normal Form) = AND of ORs

Test IFC

Test which Application Servers would be triggered for a simulated session:

Input:

- URI (subscriber public identity)
- Direction (originating or terminating)
- Method (INVITE, REGISTER, MESSAGE, SUBSCRIBE)
- Request URI (destination)

Output:

- Registration status
- Matching IFC count
- List of triggered Application Servers with IFC index

Hash Tables Tab

Manage S-CSCF hash tables. See Hash Table Operations below.

Diameter Peer Management

URL: `/diameter`

Features

Monitor and control Diameter peer connections (Cx, Rx, Ro interfaces).

Summary Information

Dashboard displays:

- **Realm**: Diameter realm
- **Identity**: Diameter Origin-Host
- **Peer Count**: Number of configured peers
- **Workers**: CDP worker count
- **Queue Length**: Pending transactions
- **Connect Timeout**: Connection timeout (seconds)
- **Transaction Timeout**: Transaction timeout (seconds)
- **Accept Unknown Peers**: Policy flag

Peer List

Table of all Diameter peers:

Column	Description
FQDN	Peer fully-qualified domain name
State	Connection state (I_Open, Closed, etc.)
Status	Enabled or Disabled
Last Used	Time since last transaction
Applications	Number of supported Diameter applications

Operations:

- **Enable Peer**: Activate disabled peer
- **Disable Peer**: Deactivate peer (with confirmation)
- **Click on row**: Expand to view supported applications

Application Mapping

The control panel automatically maps Diameter Application IDs to 3GPP interface names:

- **Cx/Dx** (16777216:10415) - IMS Subscription/Authorization
- **Sh/Dh** (16777217:10415) - User Data Access
- **Rx** (16777236:10415) - IMS Media Plane Control
- **Ro** (16777238:10415/0) - Online Charging
- **Gx** (16777224:10415) - Policy Control
- **S6a/S6d** (16777251:10415) - LTE/EPC MME-HSS
- And many more (see source: `diameter_live.ex`)

Real-time Updates

Diameter peer status automatically refreshes every 5 seconds.

Hash Table Operations

Overview

CSCF components use in-memory hash tables for performance-critical data. The control panel provides visibility and management of these tables.

Available Hash Tables

Tables vary by CSCF type. Common examples:

Hash Table	CSCF	Purpose
`imei_msisdn`	P-CSCF	Emergency callback mapping
`service_routes`	P-CSCF	Cached service routes
`auth`	S-CSCF	Authentication vectors
Various	All	Component-specific caching

Hash tables are in-memory data structures used for performance-critical operations.

Viewing Hash Tables

Access: Navigate to any CSCF panel → Hash Tables tab

1. View list of all hash tables with statistics:
    - Table name
    - Item count
    - Size
2. **Select table** to view entries
3. **Sort** by name, items, or size

Viewing Hash Table Contents

Click on a table to inspect all entries:

- **Key**: Hash table key
- **Value**: Stored value
- **Actions**: Delete button

Managing Hash Entries

Delete Single Entry

1. Select hash table
2. Locate the entry
3. Click **Delete** button (trash icon)
4. Confirm action

Result: Entry removed from hash table

Flush Entire Table

1. Select hash table
2. Click **Clear Table** button
3. **WARNING**: Confirms before clearing ALL entries
4. Confirm action

Result: All entries removed from table

Caution: Flushing tables can cause temporary service disruption:

- `imei_msisdn` flush: Emergency callbacks may fail until re-registration
- `auth` flush: In-progress authentication challenges will fail
- `service_routes` flush: Next request will route via I-CSCF discovery

Logs Viewing

URL: `/logs`

Features

View application logs in real-time from the control panel.

Features (implementation in ControlPanel dependency):

- Live log streaming
- Log level filtering
- Search and filtering capabilities

Monitoring and Metrics

Prometheus Integration

OmniCall CSCF exposes Prometheus metrics for monitoring and alerting.

Metrics Endpoint:

```
http://<host>:9090/metrics
```

Each CSCF host (P-CSCF, I-CSCF, S-CSCF) exposes metrics on port 9090. Configure Prometheus to scrape all hosts for complete visibility.

For a complete reference of all P-CSCF, I-CSCF, and S-CSCF metrics see the **Metrics Reference**.

Available Metrics

The following metrics are exposed by the OmniCall CSCF control panel application. For CSCF component metrics (SIP, Diameter, IMS, etc.), see the **Metrics Reference**.

VM Metrics

- `vm_memory_total` - Total Erlang VM memory (bytes)
- `vm_memory_processes_used` - Memory used by processes (bytes)

- `vm_memory_binary` - Binary memory (bytes)
- `vm_memory_ets` - ETS table memory (bytes)
- `vm_total_run_queue_lengths_total` - Total run queue length
- `vm_system_counts_process_count` - Process count
- `vm_system_counts_atom_count` - Atom count
- `vm_system_counts_port_count` - Port count

Phoenix HTTP Metrics

- `phoenix_endpoint_stop_duration` - HTTP request duration (milliseconds)
- `phoenix_router_dispatch_stop_duration` - Router dispatch duration (milliseconds)

LiveView Metrics

- `phoenix_live_view_mount_stop_duration` - LiveView mount duration (milliseconds)

CSCF Backend Integration Metrics

- `cscf_backend_request_count` - Backend RPC request count
  - Tags: `host`, `command`, `result`
- `cscf_backend_request_duration` - Backend RPC duration (milliseconds)
  - Tags: `host`, `command`
- `cscf_backend_error_count` - Backend RPC error count
  - Tags: `host`, `error_type`

Grafana Dashboards

Current Status: Metrics are exposed via Prometheus endpoint. Pre-built Grafana dashboards are not currently included but can be created using the available metrics.

Recommended Dashboard Panels:

- Backend RPC latency by command
- Registration count trends
- Dialog count trends

- Backend error rates
- Erlang VM memory usage
- LiveView mount performance

Integration

Configure Prometheus to scrape metrics from all CSCF hosts:

```
scrape_configs:
  - job_name: 'cscf_pcscf'
    static_configs:
      - targets: ['pcscf1.example.com:9090',
'pcscf2.example.com:9090']

  - job_name: 'cscf_icscf'
    static_configs:
      - targets: ['icscf1.example.com:9090',
'icscf2.example.com:9090']

  - job_name: 'cscf_scscf'
    static_configs:
      - targets: ['scscf1.example.com:9090',
'scscf2.example.com:9090']
```

Best Practices

Operational Guidelines

Monitoring:

- Monitor Prometheus metrics for system health
- Watch for backend RPC errors
- Track Erlang VM memory growth

Hash Table Management:

- Avoid flushing tables in production unless absolutely necessary

- Monitor table size growth for potential memory issues
- Use selective deletion instead of full table flush

Troubleshooting:

- Use Live Logs for real-time debugging
- Check Diameter peer status before investigating registration failures
- Verify CSCF backend connectivity if control panel shows errors

Performance:

- Control panel auto-refresh is 5 seconds by default
- Large registration lists use pagination to avoid performance issues
- Hash table operations are read-heavy; minimize write operations during peak hours

Related Documentation

- **P-CSCF Operations Guide** - P-CSCF specific operations
- **I-CSCF Operations Guide** - I-CSCF specific operations
- **S-CSCF Operations Guide** - S-CSCF specific operations
- **Diameter Operations Guide** - Diameter peer management
- **CSCF Operations Guide** - General CSCF operations and troubleshooting

OmniCall CSCF Operations Guide

Table of Contents

1. Overview
2. Understanding IMS Architecture
3. Call Session Flows
4. CSCF Components
5. Common Operations
6. Troubleshooting
7. Additional Documentation
8. Glossary

Overview

OmniCall CSCF is a comprehensive IMS (IP Multimedia Subsystem) solution that provides carrier-grade Call Session Control Functions for mobile and **fixed-line service providers**. Built on proven open-source technology and enhanced with enterprise-grade management capabilities, OmniCall CSCF delivers the core session control infrastructure required for VoLTE, VoWiFi, RCS, and traditional fixed-line VoIP services.

What is IMS?

The IP Multimedia Subsystem (IMS) is the 3GPP-standardized architecture for delivering IP-based multimedia services. It provides:

- **Session control** for voice, video, and messaging services
- **Quality of Service (QoS)** management for real-time communications
- **Service convergence** across mobile, fixed, and WiFi networks
- **Standards-based interoperability** with other carriers and networks

- **Rich Communication Services (RCS)** capabilities
- **Fixed-Mobile Convergence (FMC)** for unified service delivery

OmniCall CSCF implements all core CSCF functions defined in 3GPP TS 23.228, providing a complete, production-ready IMS core network solution.

OmniCall CSCF Components

OmniCall CSCF provides complete management of all CSCF network elements:

- **P-CSCF** (Proxy-CSCF) - User-facing edge proxy and security anchor
- **E-CSCF** (Emergency-CSCF) - Emergency services routing (integrated with P-CSCF)
- **I-CSCF** (Interrogating-CSCF) - Network entry point and topology hiding
- **S-CSCF** (Serving-CSCF) - Core session control, registration, and service triggering

Key Capabilities

Network Functions:

- Full 3GPP-compliant IMS session control
- **GSMA IR.92/IR.94 compliant** - Works with any standards-compliant device, no custom carrier bundles required
- VoLTE, VoWiFi, and RCS support
- Fixed-line SIP service integration
- Emergency services (E911/E112) support with location services
- Topology hiding and network security
- IPsec-based security associations
- Diameter-based AAA and policy integration

Service Features:

- Real-time call session management
- Service triggering via Initial Filter Criteria (IFC)
- Application Server (AS) integration via ISC interface

- Charging integration (online and offline)
- QoS policy enforcement via PCRF integration
- Multi-tenancy support for MVNO scenarios

Management & Operations:

- Real-time monitoring via web-based control panel
- Prometheus metrics integration (see Metrics Reference)
- RESTful API for automation
- Distributed clustering for high availability
- Live troubleshooting and diagnostics

Integrated Components:

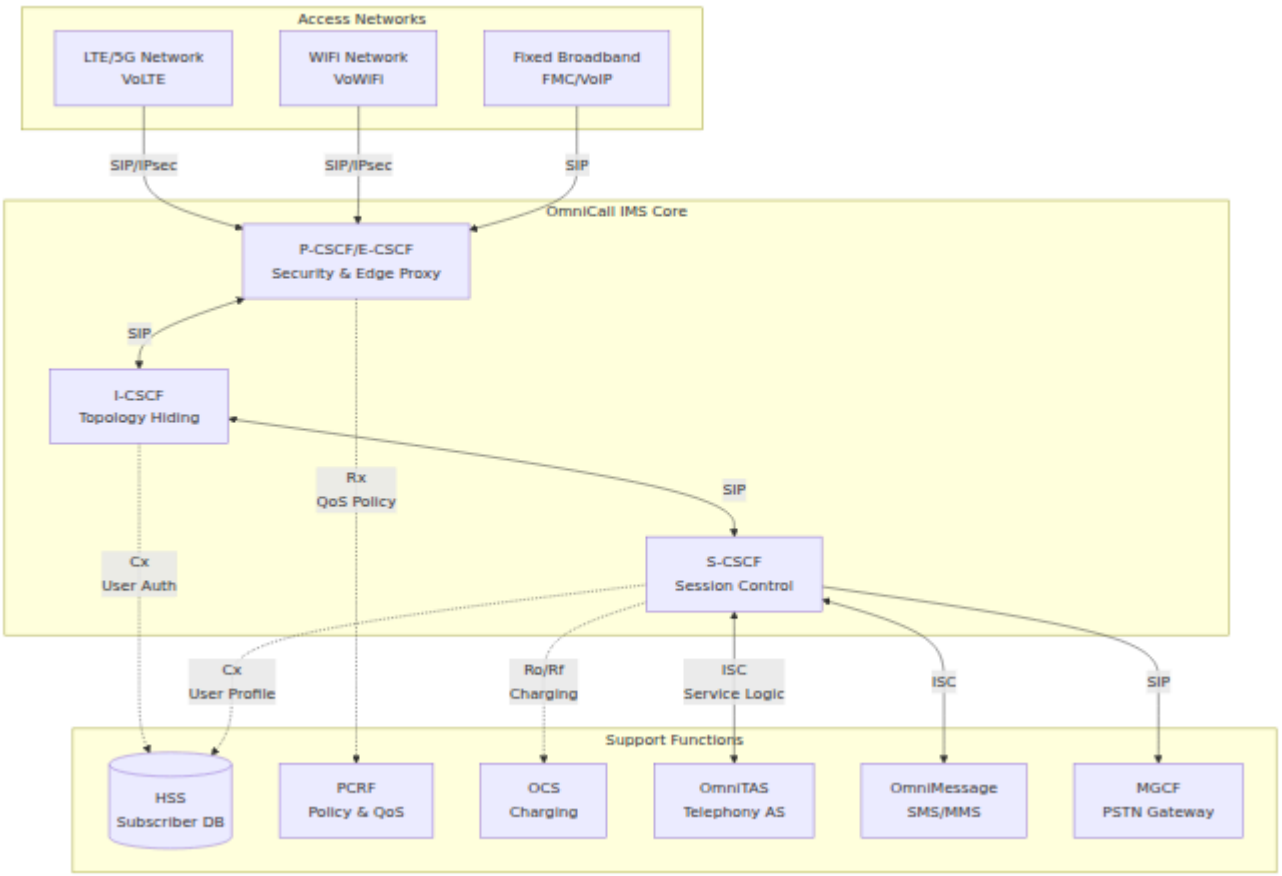
- **OmniePDG**: Evolved Packet Data Gateway for VoWiFi (IR.94 compliant)
- **OmniTAS**: Telephony Application Server for supplementary services
- **OmniMessage**: SMS/MMS Application Server (3GPP TS 24.341)

For detailed control panel usage, see Web UI Operations.

Understanding IMS Architecture

IMS Network Architecture

The OmniCall CSCF solution sits at the heart of the IMS architecture, providing the session control layer that connects user equipment to services and manages all call sessions.



How CSCFs Work Together

The CSCF functions work as a coordinated system to handle IMS sessions:

1. **P-CSCF** - First Point of Contact
    - User equipment (mobile, WiFi, or fixed-line devices) establish secure connections to P-CSCF
    - Provides IPsec security associations for mobile devices
    - Acts as the QoS policy enforcement point via PCRF integration
    - Handles NAT traversal and media anchoring
    - Routes emergency calls to E-CSCF functionality
    - Maintains user location information
2. **I-CSCF** - Network Gateway & Load Balancer
    - Hides internal network topology from external networks
    - Queries HSS to select appropriate S-CSCF for users
    - Performs S-CSCF load balancing based on capabilities

    - Acts as the entry/exit point for roaming scenarios
    - Enforces Network Domain Security (NDS/TLS)

3. **S-CSCF** - Core Session Controller

    - Performs user registration and authentication
    - Maintains session state for all active calls
    - Enforces routing policies and service logic
    - Triggers Application Servers based on IFC (Initial Filter Criteria)
    - Integrates with charging systems (online and offline)
    - Manages supplementary services

Integration with Supporting Systems

OmniCall CSCF integrates with IMS support functions via standard 3GPP Diameter interfaces:

Interface	From → To	Purpose	3GPP Spec
Cx	I-CSCF/S-CSCF ↔ HSS	User authentication, profile retrieval, S-CSCF assignment	TS 29.228
Dx	I-CSCF ↔ SLF	Subscription locator for multi-HSS environments	TS 29.229
Rx	P-CSCF ↔ PCRF	QoS policy authorization, media flow control	TS 29.214
Ro	S-CSCF → OCS	Online charging (credit control)	TS 32.299
Rf	S-CSCF → CDF	Offline charging (CDR generation)	TS 32.299
ISC	S-CSCF ↔ AS	Service triggering and application server invocation	TS 23.228
Sh	AS ↔ HSS	Application server access to user data	TS 29.328

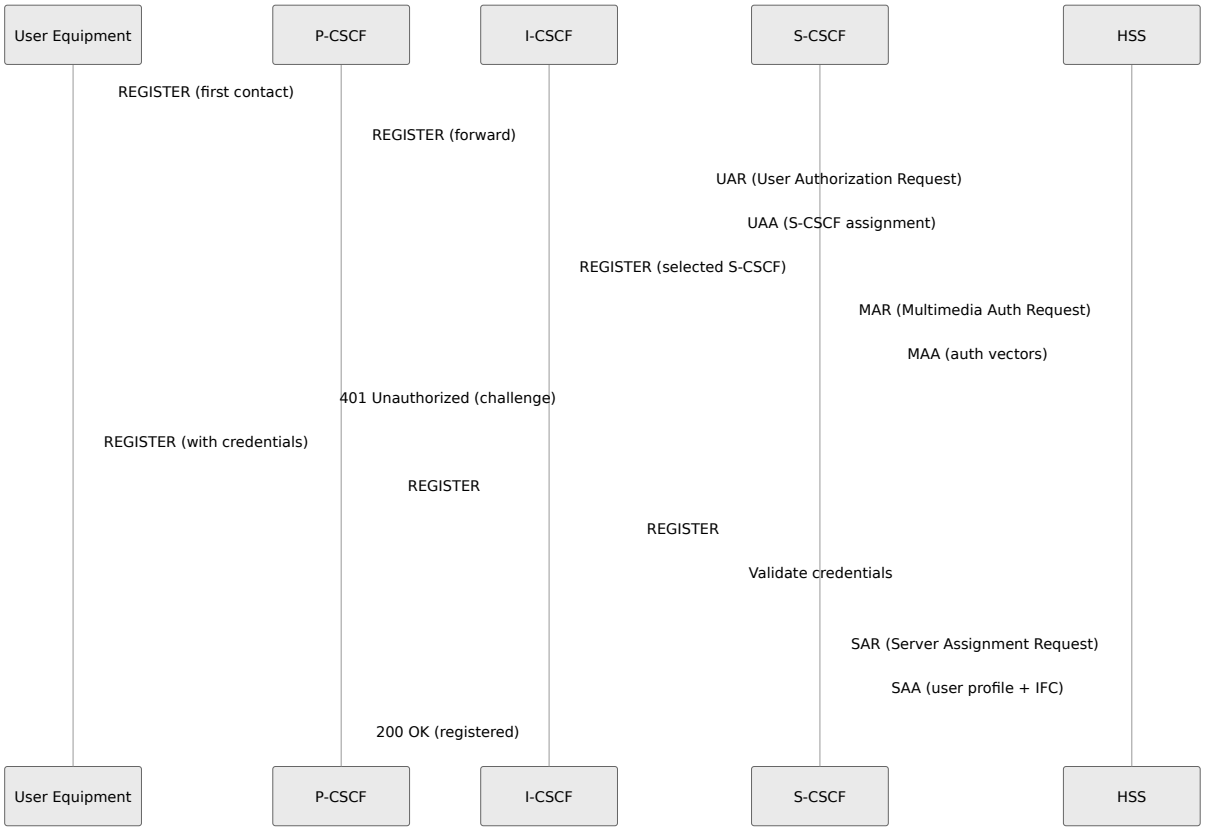
For Diameter peer management, see Diameter Operations.

Call Session Flows

Understanding how CSCFs process different types of sessions is essential for operations and troubleshooting.

IMS Registration Flow

When a device registers to the IMS network, the CSCFs coordinate to authenticate and authorize the user:

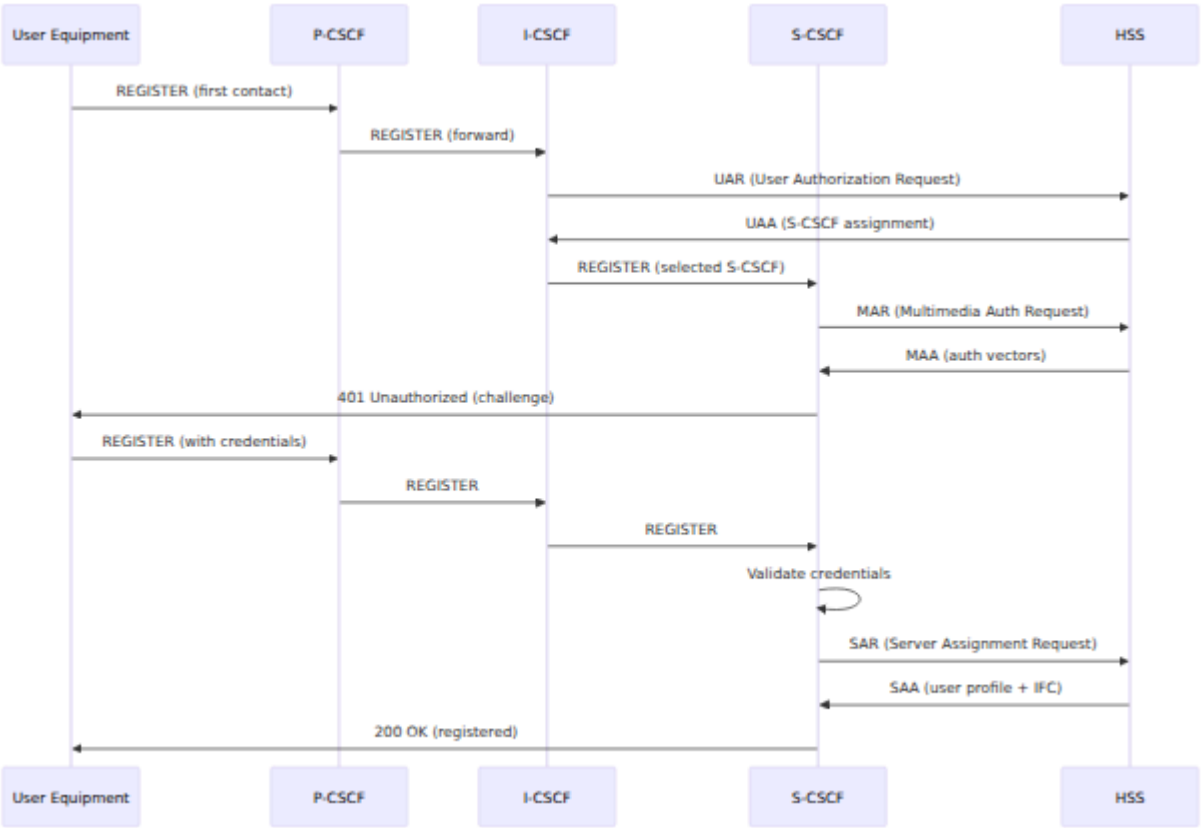


Key Points:

- P-CSCF maintains IPsec security association with UE
- I-CSCF queries HSS to find/assign S-CSCF
- S-CSCF performs authentication and stores user profile
- User's service profile (IFC) determines which Application Servers will be triggered

Mobile Originated Call Flow

When a registered user initiates a call:

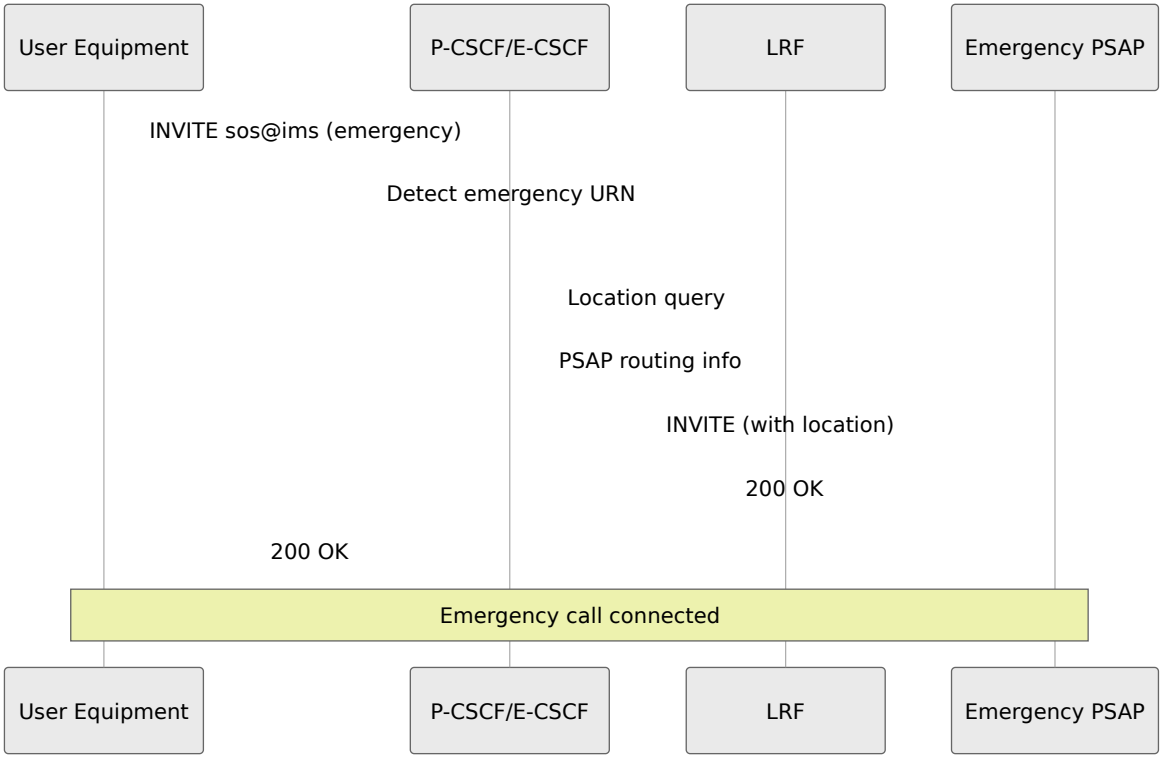


Key Points:

- P-CSCF coordinates with PCRF for QoS bearer establishment
- S-CSCF evaluates IFC to determine service triggering
- **OmniTAS** provides telephony application services (call forwarding, screening, etc.)
- **OmniMessage** handles SMS/MMS traffic when triggered by IFC
- For monitoring active calls, see S-CSCF Dialog Management

Emergency Call Flow (E-CSCF)

Emergency calls receive special handling to ensure connectivity even without full IMS registration:

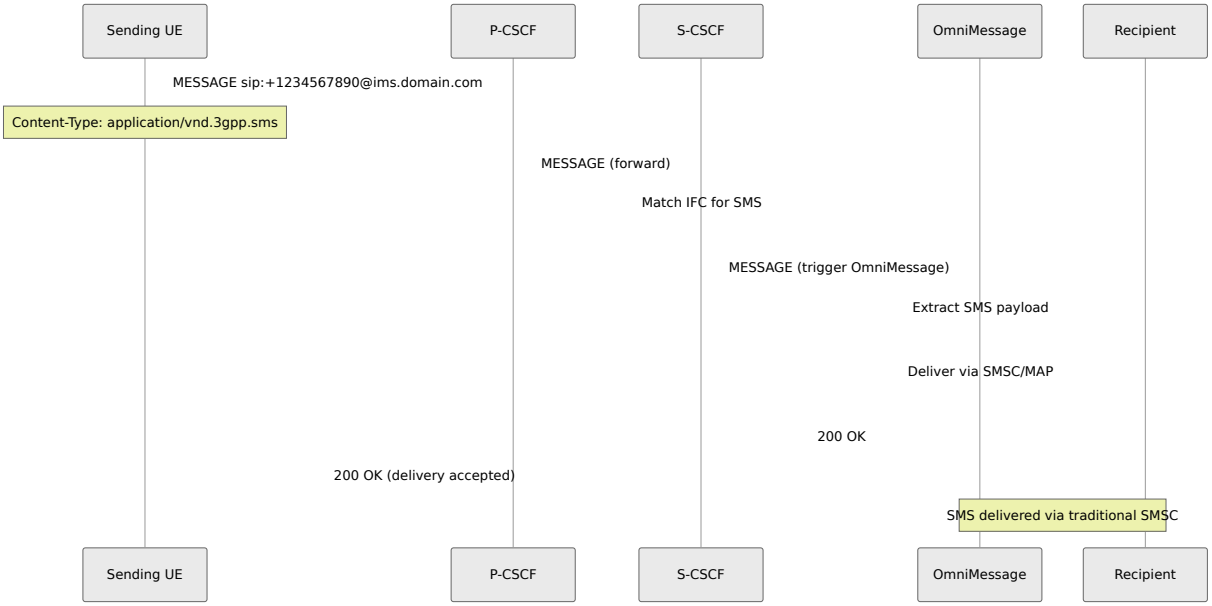


Key Points:

- E-CSCF functionality is integrated into P-CSCF
- Works even for unregistered or roaming users
- Includes callback number storage for emergency services
- For emergency operations, see P-CSCF Emergency Services

SMS over IMS - Mobile Originated (3GPP TS 24.341)

When a user sends an SMS via IMS, OmniMessage handles the message delivery:



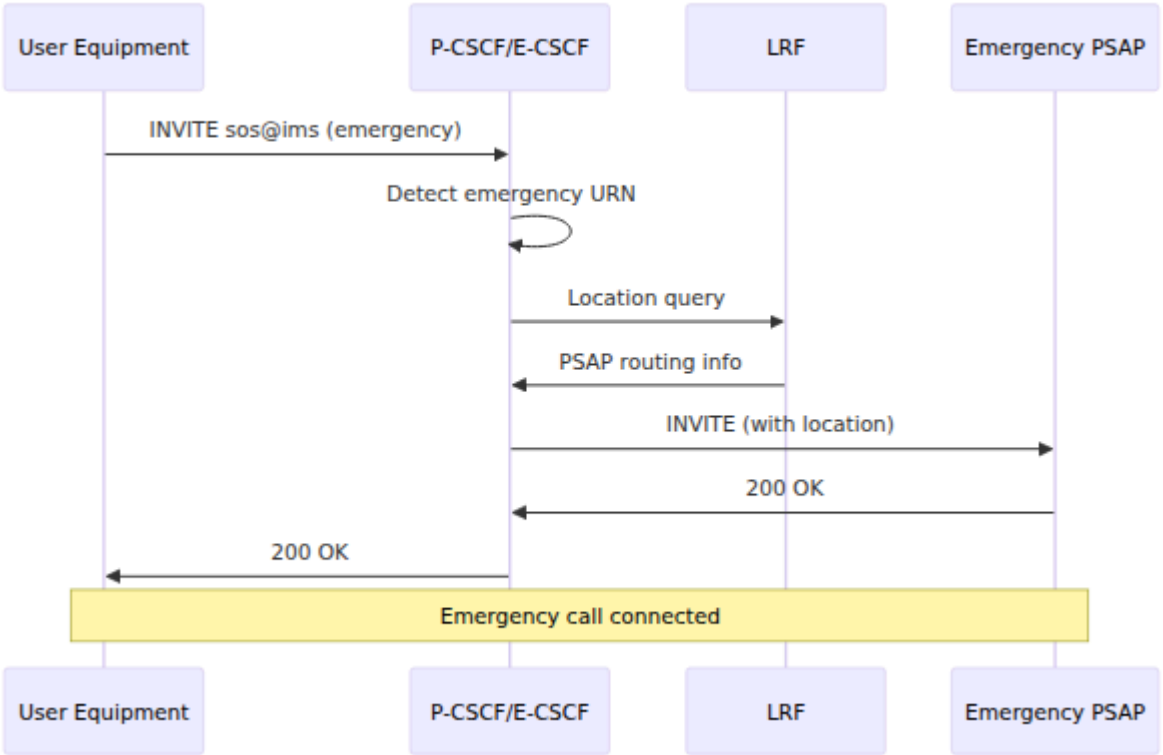
Key Points:

- SMS encoded in SIP MESSAGE method per 3GPP TS 24.341
- Content-Type: `application/vnd.3gpp.sms` identifies SMS payload
- S-CSCF IFC triggers **OmniMessage** for SMS traffic
- OmniMessage interfaces with traditional SMSC infrastructure
- Supports both GSM-7, UCS-2 character sets and concatenated messages

---

SMS over IMS - Mobile Terminated (3GPP TS 24.341)

When an SMS arrives for an IMS-registered user, OmniMessage routes it via IMS:



Key Points:

- SMSC forwards SMS to **OmniMessage** via traditional protocols (MAP/SMPP)
- OmniMessage converts to SIP MESSAGE method
- S-CSCF routes based on registered IMPU
- Supports delivery reports and status notifications
- Fallback to traditional SMS if user not IMS-registered

For SMS operations and monitoring, see S-CSCF IFC Management.

Roaming Scenarios

OmniCall CSCF supports **home-routed** roaming as mandated by 3GPP/GSMA standards:

Home-Routed Roaming: When users roam to a visited network, all IMS sessions are routed back through the home network's S-CSCF. This ensures:

- Consistent service experience regardless of location
- Home network control over service triggering and charging
- Simplified roaming agreements between operators

- Compliance with GSMA PRD IR.92 and IR.94 standards

The visited network's I-CSCF queries the home HSS and routes registration/session requests to the home S-CSCF, which then invokes home network application servers (OmniTAS, OmniMessage, etc.).

For roaming configuration details, see I-CSCF Network Domain Security.

CSCF Components

P-CSCF/E-CSCF - Edge Proxy and Security Anchor

The **Proxy-CSCF** is the first IMS element that user equipment contacts. It serves as the security boundary and policy enforcement point.

Core Functions:

- **Security Association Management**: Establishes and maintains IPsec tunnels with mobile devices for signaling and media protection
- **QoS Policy Enforcement**: Coordinates with PCRF via Rx interface to authorize and enforce QoS bearers
- **NAT Traversal**: Handles far-end NAT traversal for devices behind NAT/firewalls
- **Compression**: SigComp support for bandwidth-constrained networks
- **Service Route**: Maintains service route for subsequent requests

Emergency Services (E-CSCF):

- Integrated emergency call routing without requiring full IMS registration
- Location information handling for E911/E112
- IMEI-to-callback number mapping for emergency callbacks
- Integration with LRF (Location Retrieval Function)

Supported Access Types:

- LTE/5G (VoLTE) via IPsec

- WiFi (VoWiFi) via IPsec
- Fixed broadband via SIP
- Cable/DSL residential gateways

For detailed operations, see **P-CSCF Documentation**.

I-CSCF - Topology Hiding and Load Balancing

The **Interrogating-CSCF** acts as the contact point within an operator's network for connections from other networks or from the same network.

Core Functions:

- **Topology Hiding**: Shields internal network structure from external networks
- **S-CSCF Assignment**: Queries HSS via Cx interface to assign S-CSCF to new users
- **S-CSCF Selection**: Selects appropriate S-CSCF based on capabilities and load
- **Routing Proxy**: Routes incoming requests to the assigned S-CSCF
- **Network Domain Security**: Enforces NDS/TLS for inter-operator security

Key Features:

- **Multi-S-CSCF Support**: Distributes users across multiple S-CSCF instances
- **Capability Matching**: Matches user requirements to S-CSCF capabilities
- **Roaming Support**: Handles both home-routed and local breakout scenarios
- **Subscription Locator**: Dx interface support for multi-HSS environments

Use Cases:

- Interconnection point for roaming partners
- Load distribution across S-CSCF cluster
- Geographic routing for disaster recovery

- MVNO traffic segregation

For detailed operations, see **I-CSCF Documentation**.

S-CSCF - Core Session Controller

The **Serving-CSCF** is the central component of the IMS network, providing session control and service intelligence.

Core Functions:

- **Registration**: Authenticates users and maintains registration bindings
- **Session Control**: Manages all call states (dialog establishment, modification, termination)
- **Service Triggering**: Evaluates Initial Filter Criteria (IFC) to invoke Application Servers
- **Routing**: Routes SIP requests based on service logic and user preferences
- **Charging Integration**: Coordinates with online (OCS) and offline (CDF) charging systems

Service Triggering via IFC: The S-CSCF uses XML-based Initial Filter Criteria downloaded from HSS to determine when to route calls through Application Servers (such as **OmniTAS** for telephony services and **OmniMessage** for SMS/MMS):

- **Trigger Points**: Match on SIP method, Request-URI, Session-Case (originating/terminating)
- **Priority-based**: IFC processed in priority order
- **Service Chaining**: Multiple AS can be invoked in sequence (e.g., OmniTAS → OmniMessage)
- **Default Handling**: Configurable behavior when AS is unreachable

Supported Services:

- Call forwarding (busy, no answer, unconditional)
- Call barring (outgoing, incoming, roaming)
- Call screening and filtering

- Number translation and routing
- Prepaid/postpaid charging
- Usage tracking and quota enforcement
- Supplementary services (call waiting, hold, transfer)

Scalability Features:

- Distributed dialog storage
- Stateful session handling
- Database-backed user profiles
- Horizontal scaling via I-CSCF distribution

For detailed operations, see **S-CSCF Documentation**.

Diameter Interface Management

OmniCall CSCF provides comprehensive Diameter peer management across all CSCF components.

Supported Diameter Applications:

Application	Interface	App ID	Used By	Purpose
3GPP Cx	Cx	16777216	I-CSCF, S-CSCF	User authentication, profile retrieval
3GPP Dx	Dx	16777216	I-CSCF	Subscription location in multi-HSS
3GPP Rx	Rx	16777236	P-CSCF	Policy authorization, QoS control
3GPP Ro	Ro	4 (CC)	S-CSCF	Online charging (credit control)
3GPP Rf	Rf	3 (Accounting)	S-CSCF	Offline charging (CDR)
3GPP Sh	Sh	16777217	AS	User data access from AS

Diameter Capabilities:

- Automatic peer discovery via DNS
- Failover and redundancy support
- Watchdog and connection management
- Per-peer statistics and monitoring
- Dynamic peer enable/disable

For Diameter operations and troubleshooting, see **Diameter Management Guide**.

Common Operations

OmniCall CSCF provides comprehensive operational capabilities through its web-based control panel. This section covers common operational tasks and their significance.

Registration Management

Understanding IMS Registrations:

IMS registration is a two-tier process:

- **P-CSCF Contact**: User equipment establishes IPsec/SIP connection to P-CSCF
- **S-CSCF Registration**: Full IMS registration with authentication via HSS

Key Registration Operations:

- **View active registrations** across P-CSCF and S-CSCF
- **Query specific users** by IMPU, IMSI, or IP address
- **Monitor registration state** (authenticated, active, expired)
- **Force deregistration** for troubleshooting or administrative purposes
- **Track registration expiry** to identify re-registration issues

For detailed registration procedures, see:

- P-CSCF Contact Management
- S-CSCF Registration Operations

Call Session Monitoring

Dialog (Session) Management:

The S-CSCF maintains state for all active IMS sessions (calls). Operators can:

- **Monitor active dialogs** including Call-ID, participants, and session state

- **View dialog details** such as SDP (media parameters), route sets, and timers
- **Terminate dialogs** for troubleshooting or emergency situations
- **Track session duration** and detect long-running or stuck sessions

Session States:

- **Early**: Call is ringing, not yet answered
- **Confirmed**: Active call with media flowing
- **Terminated**: Call ended normally

For call monitoring procedures, see S-CSCF Dialog Management.

Service Triggering and IFC Management

Initial Filter Criteria (IFC) determines when and how the S-CSCF routes sessions to application servers like **OmniTAS** and **OmniMessage**.

IFC Operations:

- **Dump user's IFC** to view configured service profile from HSS
- **Test IFC matching** with simulated call scenarios
- **Verify AS routing** to ensure proper service invocation
- **Debug service failures** by examining trigger point evaluation

Example IFC Structure:

```
<InitialFilterCriteria>
  <Priority>10</Priority>
  <TriggerPoint>
    <SPT><Method>INVITE</Method></SPT>
    <SPT><SessionCase>0</SessionCase><!-- Originating --></SPT>
  </TriggerPoint>
  <ApplicationServer>
    <ServerName>sip:omnitas.ims.example.com</ServerName>
    <DefaultHandling>0</DefaultHandling><!-- Must invoke -->
  </ApplicationServer>
</InitialFilterCriteria>
```

For IFC testing and troubleshooting, see S-CSCF IFC Operations.

Diameter Peer Management

Monitoring Diameter Connectivity:

OmniCall CSCF relies on Diameter interfaces for HSS, PCRF, and charging integration. Operators can:

- **Monitor peer status** (I_Open = connected, Closed = disconnected)
- **View peer capabilities** (supported Diameter applications)
- **Enable/disable peers** for maintenance or failover testing
- **Track peer statistics** (requests, failures, timeouts)

Critical Diameter Connections:

- **Cx to HSS** (I-CSCF, S-CSCF): User authentication and profiles
- **Rx to PCRF** (P-CSCF): QoS policy and bearer control
- **Ro to OCS** (S-CSCF): Online charging and credit control

For Diameter troubleshooting, see Diameter Operations Guide.

Emergency Services Management

E-CSCF Operations:

Emergency call handling requires special operational attention:

- **Monitor IMEI-to-callback mappings** for emergency callbacks
- **Verify location information** availability for E911/E112
- **Test emergency call routing** without actual PSAP connection
- **Manage emergency registration** for unprovisioned devices

Emergency services work even for:

- Unregistered users
- Users with no SIM/invalid credentials
- Roaming users from other networks

For emergency operations, see P-CSCF Emergency Services.

Hash Table Management

Shared Memory Data Structures:

CSCF nodes use in-memory hash tables for performance-critical data:

Hash Table	CSCF	Purpose	TTL
`imei_msisdn`	P-CSCF	Emergency callback mapping	24 hours
`service_routes`	P-CSCF	Cached service routes	Registration expiry
`auth`	S-CSCF	Authentication vectors	Challenge timeout

Operations:

- **View table contents** for troubleshooting
- **Delete specific entries** to clear stale data
- **Flush entire tables** for emergency recovery (use with caution)

For detailed UI operations, see the Web UI Operations Guide.

Troubleshooting

This section covers common operational issues and their resolution strategies.

Registration Failures

Symptoms: Users unable to register to IMS network, registration timeouts

Common Root Causes:

1. **HSS Connectivity Issues**
   - Check Diameter Cx peer status on I-CSCF and S-CSCF
   - Verify HSS is reachable and responding to UAR/MAR requests
   - Check for Diameter routing issues
2. **Authentication Failures**
   - Verify user credentials provisioned in HSS
   - Check authentication vector generation (MAR/MAA)
   - Verify AKA algorithm compatibility (Milenage)
3. **P-CSCF Connectivity**
   - Verify IPsec SA establishment for mobile devices
   - Check NAT traversal for devices behind NAT
   - Verify P-CSCF discovery (DNS, DHCP, or static configuration)
4. **S-CSCF Assignment**
   - Check I-CSCF S-CSCF selection logic
   - Verify S-CSCF capabilities match user requirements

    - Check S-CSCF capacity (registration limits)

For detailed troubleshooting, see component-specific guides:

- P-CSCF Troubleshooting
- I-CSCF Troubleshooting
- S-CSCF Troubleshooting

Call Setup Failures

Symptoms: Calls fail to establish, receive 4xx/5xx SIP errors

Common Root Causes:

1. **User Not Registered**
    - Verify both originating and terminating users are IMS-registered
    - Check registration status via S-CSCF
2. **IFC/Service Triggering Issues**
    - Verify IFC downloaded from HSS (check SAR/SAA)
    - Test IFC matching for call scenario
    - Check OmniTAS/OmniMessage availability if triggered
3. **QoS/PCRF Issues**
    - Verify Rx Diameter peer status on P-CSCF
    - Check PCRF QoS policy authorization
    - Verify bearer resources available in access network
4. **Routing Failures**
    - Verify destination routing (ENUM, number translation)
    - Check interconnect/MGCF configuration for PSTN calls
    - Verify roaming routing for off-net calls

Diameter Connectivity Issues

Symptoms: Diameter peer shows "Closed" state, operations timing out

Diagnosis Steps:

1. **Check Peer Status**: Use control panel to view Diameter peer state
2. **Verify Network Connectivity**: Test IP reachability to Diameter peer (port 3868)
3. **Check Capabilities**: Verify Application IDs match between peers
4. **Review Watchdog**: Check Diameter watchdog (DWR/DWA) exchanges

Critical Diameter Interfaces:

Interface	Impact if Down	Recovery Priority
Cx (HSS)	No new registrations, no IFC updates	Critical - immediate
Rx (PCRF)	No QoS for new calls	High - within minutes
Ro (OCS)	No prepaid charging, service may continue	High - depends on policy

For Diameter troubleshooting, see Diameter Operations Guide.

SMS Delivery Issues

Symptoms: SMS not delivered via IMS, fallback to legacy SMSC

Common Root Causes:

1. **OmniMessage Not Triggered**
    - Verify IFC configured to trigger OmniMessage for MESSAGE requests
    - Check IFC priority (should be higher than other AS)
    - Test IFC matching with simulated SMS

2. **SMSC Integration**
    - Verify OmniMessage to SMSC connectivity (MAP/SMPP)
    - Check message format conversion (SIP MESSAGE ↔ SMS PDU)
    - Verify subscriber routing in SMSC
3. **Content Type Issues**
    - Verify `Content-Type: application/vnd.3gpp.sms` in SIP MESSAGE
    - Check character set encoding (GSM-7, UCS-2)

For SMS troubleshooting, see S-CSCF IFC Management.

Emergency Call Issues

Symptoms: Emergency calls not routing to PSAP, location not included

Common Root Causes:

1. **E-CSCF Detection**
    - Verify emergency URN detection (urn:service:sos)
    - Check emergency routing rules on P-CSCF
    - Verify LRF connectivity
2. **Location Information**
    - Check location header in SIP INVITE
    - Verify IMEI-to-callback mapping for callbacks
    - Test location retrieval from LRF
3. **PSAP Routing**
    - Verify PSAP routing table configuration
    - Check ESQK (Emergency Service Query Key) generation
    - Verify trunk/interconnect to PSAP

For emergency services operations, see P-CSCF Emergency Services.

Performance Degradation

Symptoms: Slow call setup, registration delays, high latency

Diagnosis:

1. **Monitor Prometheus Metrics**: Check CSCF performance metrics (see Metrics Reference for complete metric definitions)
2. **Database Performance**: Verify S-CSCF database query times
3. **Network Latency**: Check latency between CSCF nodes
4. **Resource Utilization**: Monitor CPU, memory, and network on CSCF servers

Scalability Considerations:

- **P-CSCF**: ~50,000 IPsec SAs per instance (VoLTE); 100,000+ via OmniePDG (VoWiFi)
- **I-CSCF**: Stateless, scales horizontally (1,000-5,000 registrations/sec per instance)
- **S-CSCF**: 100,000-500,000 registrations per instance; 20,000-100,000 concurrent dialogs

For detailed capacity planning and deployment sizing, see the **Capacity and Dimensioning Guide**.

For performance monitoring and metrics, see the Web UI Operations Guide.

Additional Documentation

Component-Specific Operations Guides

For detailed operations and troubleshooting for each CSCF component:

- **P-CSCF/E-CSCF Operations Guide** - Edge proxy, security associations, emergency services
- **I-CSCF Operations Guide** - S-CSCF selection, topology hiding, roaming

- **S-CSCF Operations Guide** - Registration, dialog management, IFC operations
- **Diameter Operations Guide** - Diameter peer management and troubleshooting
- **Web UI Operations Guide** - Control panel usage, monitoring, and administration
- **Metrics Reference** - Complete reference of all P-CSCF, I-CSCF, and S-CSCF Prometheus metrics
- **Capacity and Dimensioning Guide** - Deployment sizing, capacity planning, performance tuning

Regulatory Compliance

- **ANSSI R226 Interception Compliance** - Lawful interception capabilities as required by French regulatory authorities

3GPP Standards Reference

OmniCall CSCF implements the following 3GPP specifications:

Specification	Title	Relevance
TS 23.228	IP Multimedia Subsystem (IMS) - Stage 2	Core IMS architecture
TS 24.229	IP multimedia call control protocol (SIP)	IMS SIP profile
TS 29.228	Cx and Dx interfaces (CSCF-HSS)	User data and authentication
TS 29.214	Rx interface (P-CSCF-PCRF)	QoS policy control
TS 32.299	Charging - Diameter applications	Online/offline charging
TS 24.341	SMS over IP networks	SMS over IMS
TS 23.167	Emergency services	E-CSCF and emergency calls

GSMA Standards Compliance

OmniCall CSCF is fully compliant with GSMA IMS profiles, ensuring interoperability with off-the-shelf devices:

IR.92 - IMS Profile for Voice and SMS (VoLTE)

GSMA PRD IR.92 defines the mandatory IMS profile for VoLTE services, ensuring that commercial devices work seamlessly without carrier-specific configuration or custom device bundles.

Key IR.92 Benefits for OmniCall CSCF:

✓ **Open Market Device Support**: Any IR.92-compliant smartphone works immediately—no custom carrier bundles, proprietary APNs, or special provisioning required

✓ **Standardized SIP Profile**: Devices use standard SIP headers, authentication, and registration flows as defined in 3GPP TS 24.229

✓ **Codec Interoperability**: Mandatory codec support (AMR-WB for HD Voice) ensures consistent voice quality across all devices

✓ **SMS over IMS**: Integration with **OmniMessage** provides standards-based SMS delivery (TS 24.341) to any IR.92 device

✓ **Emergency Services**: E.164 emergency number handling (911, 112, etc.) works on all compliant devices without special configuration

✓ **Roaming Consistency**: Home-routed roaming ensures users get the same VoLTE experience when visiting other IR.92-compliant networks

What This Means: Operators can launch VoLTE services immediately with existing consumer devices (iPhone, Samsung, Google Pixel, etc.) without waiting for custom device certification or carrier bundle updates.

IR.94 - IMS Profile for Voice, Video and SMS (VoWiFi)

GSMA PRD IR.94 extends IR.92 to include Voice over WiFi, enabling VoLTE services over untrusted WiFi networks.

VoWiFi Architecture with OmniCall:

VoWiFi Components:

- **OmniePDG**: Evolved Packet Data Gateway - Provides IPsec tunnel termination for untrusted WiFi access
- **OmniCall P-CSCF**: Handles VoWiFi registrations identically to VoLTE (same service routes, same IFC triggering)
- **Seamless Handover**: Devices can move between LTE and WiFi without call interruption

IR.94 Benefits:

- Same IR.92 benefits apply to VoWiFi

- Devices automatically discover ePDG via DNS (no manual configuration)
- Single IMS registration covers both VoLTE and VoWiFi
- Indoor coverage extension without femtocells or DAS

For ePDG operations and VoWiFi troubleshooting, see **OmniePDG Documentation**.

Other GSMA Standards

- **IR.51** - GSMA Roaming Database Structure
- **IR.88** - LTE Roaming Guidelines
- **AA.80** - IMS/RCS Device Configuration and Supporting Services

Product Differentiation

Why Choose OmniCall CSCF?

✓ **Plug-and-Play Device Support**: GSMA IR.92/IR.94 compliant - works with off-the-shelf iPhones, Android phones, and fixed-line devices without custom carrier bundles or device certification delays

✓ **Complete IMS Solution**: All CSCF components (P/I/S/E) plus OmniePDG for VoWiFi in a unified platform

✓ **Fixed-Mobile Convergence**: Unified IMS core for mobile (VoLTE/VoWiFi), fixed broadband, and cable telephony services

✓ **Zero Touch Provisioning**: Standards-based device discovery (DNS, DHCP) means users can swap SIM cards between devices without IT support

✓ **Enterprise Management**: Web-based control panel with real-time monitoring, diagnostics, and troubleshooting

✓ **Carrier-Grade Scalability**: Horizontal scaling to support millions of subscribers with sub-second call setup times

✓ **Application Server Ecosystem**: Seamless integration with OmniTAS (telephony services) and OmniMessage (SMS/MMS)

✓ **Emergency Services**: Built-in E-CSCF with E911/E112 support, location services, and callback handling

✓ **Interoperability First**: Full 3GPP and GSMA compliance ensures roaming agreements and interconnection work out-of-the-box

✓ **Production Proven**: Deployed in tier-1, tier-2, and MVNO networks worldwide serving millions of subscribers

Glossary

IMS Architecture Terms

- **3GPP**: 3rd Generation Partnership Project - Standards body for mobile telecommunications
- **AKA**: Authentication and Key Agreement - Security mechanism for IMS
- **AoR**: Address of Record - SIP identity (e.g., sip:user@domain.com)
- **CSCF**: Call Session Control Function - IMS session control entity
- **DAS**: Distributed Antenna System - Indoor coverage solution
- **E-CSCF**: Emergency CSCF - Emergency call routing function
- **ePDG**: Evolved Packet Data Gateway - IPsec tunnel endpoint for untrusted WiFi access
- **ENUM**: E.164 Number Mapping - DNS-based number translation
- **ESQK**: Emergency Service Query Key - Emergency call identifier
- **FMC**: Fixed-Mobile Convergence - Unified services across access types
- **GSMA**: GSM Association - Mobile industry standards organization
- **HD Voice**: High Definition Voice - Wideband audio using AMR-WB codec
- **HSS**: Home Subscriber Server - Subscriber database and authentication
- **I-CSCF**: Interrogating CSCF - Network entry point and topology hiding
- **IFC**: Initial Filter Criteria - XML-based service triggering rules
- **IMS**: IP Multimedia Subsystem - 3GPP architecture for IP-based services
- **IMPU**: IP Multimedia Public Identity - User's public identity (SIP URI or tel URI)
- **IMSI**: International Mobile Subscriber Identity - Subscriber identifier

- **IR.92**: GSMA IMS Profile for Voice and SMS - VoLTE interoperability standard
- **IR.94**: GSMA IMS Profile for Conversational Video - VoWiFi interoperability standard
- **ISC**: IMS Service Control - Interface between S-CSCF and Application Servers
- **LRF**: Location Retrieval Function - Emergency location services
- **MGCF**: Media Gateway Control Function - PSTN interconnection
- **MVNO**: Mobile Virtual Network Operator - Operator without own radio infrastructure
- **NDS**: Network Domain Security - Inter-operator security (TLS/IPsec)
- **P-CSCF**: Proxy CSCF - Edge proxy and first point of contact
- **PSAP**: Public Safety Answering Point - Emergency services call center
- **RCS**: Rich Communication Services - Enhanced messaging services
- **S-CSCF**: Serving CSCF - Core session control and registration
- **SPT**: Service Point Trigger - Matching condition in IFC (Method, Request-URI, etc.)
- **SWu**: 3GPP interface between UE and ePDG (IPsec/IKEv2)
- **UE**: User Equipment - End-user device (phone, tablet, fixed terminal)
- **VoLTE**: Voice over LTE - Voice services via LTE data network
- **VoWiFi**: Voice over WiFi - Voice services via untrusted WiFi networks

Diameter Protocol Terms

- **AAA**: Authentication, Authorization, Accounting
- **AVP**: Attribute-Value Pair - Diameter message data element
- **CCR/CCA**: Credit-Control-Request/Answer - Online charging messages
- **CDF**: Charging Data Function - Offline charging collector
- **Cx**: Diameter interface between I-CSCF/S-CSCF and HSS
- **Diameter**: AAA protocol used in IMS (evolution of RADIUS)
- **Dx**: Diameter interface between I-CSCF and SLF (subscription locator)
- **DWR/DWA**: Device-Watchdog-Request/Answer - Peer health check
- **MAR/MAA**: Multimedia-Auth-Request/Answer - Authentication vector request
- **OCS**: Online Charging System - Real-time charging and credit control

- **PCRF**: Policy and Charging Rules Function - QoS policy server
- **Rf**: Diameter interface for offline charging (accounting)
- **Ro**: Diameter interface for online charging (credit control)
- **Rx**: Diameter interface between P-CSCF and PCRF (QoS authorization)
- **SAR/SAA**: Server-Assignment-Request/Answer - User profile download
- **Sh**: Diameter interface between AS and HSS (user data access)
- **SLF**: Subscription Locator Function - HSS location in multi-HSS environment
- **UAR/UAA**: User-Authorization-Request/Answer - S-CSCF selection

OmniCall Product Terms

- **OmniCall CSCF**: Complete IMS CSCF solution (this product)
- **OmniePDG**: Evolved Packet Data Gateway - IPsec tunnel termination for VoWiFi (IR.94 compliant)
- **OmniTAS**: Telephony Application Server - Provides supplementary voice services
- **OmniMessage**: Messaging Application Server - SMS/MMS over IMS (TS 24.341)

SIP Protocol Terms

- **Dialog**: SIP session state between two endpoints
- **INVITE**: SIP method for session establishment (calls)
- **MESSAGE**: SIP method for instant messaging (including SMS over IMS)
- **REGISTER**: SIP method for user registration
- **SDP**: Session Description Protocol - Media parameters (codecs, ports)
- **SIP**: Session Initiation Protocol - Signaling protocol for IMS