

Diameter Operations Guide

Table of Contents

1. [Overview](#)
2. [Diameter in IMS Architecture](#)
3. [Diameter Interfaces](#)
4. [Peer Management via OmniWeb](#)
5. [Diameter Result Codes](#)
6. [Common Issues](#)

Overview

Diameter is the authentication, authorization, and accounting (AAA) protocol for the IMS architecture. OmniCSCF uses Diameter to communicate with critical network elements. These elements include the HSS, PCRF, and OCS.

What is Diameter?

Diameter (RFC 6733) is the successor to RADIUS. Diameter supports modern AAA scenarios:

- **Reliable transport** through TCP/SCTP. RADIUS uses UDP.
- **Extensible** through Application-Specific modules
- **Peer-to-peer** architecture. It is not only client-server.
- **Stateful** connections with watchdog monitoring
- **Standardized** error handling and result codes

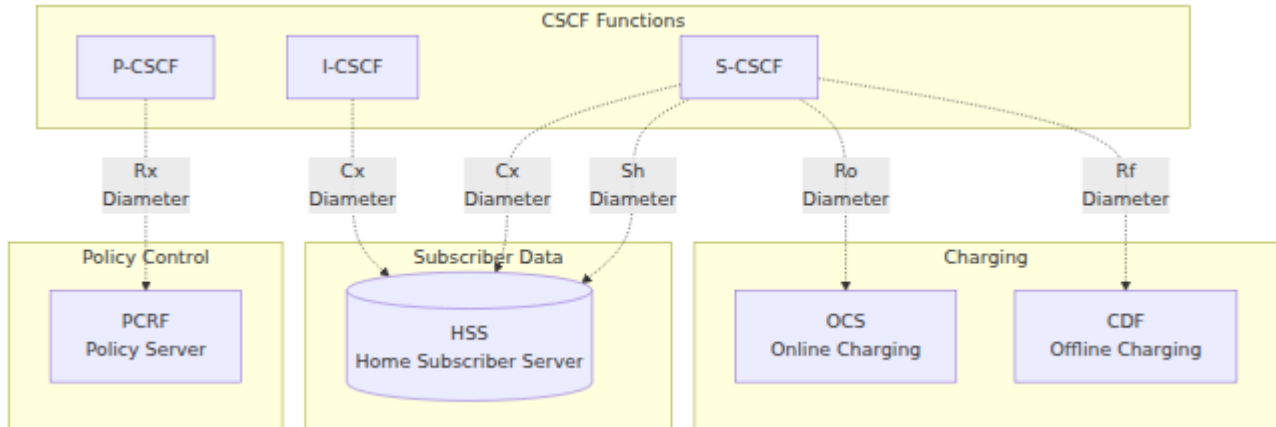
Diameter in CSCF

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 I-CSCF and S-CSCF use the Cx interface for user authentication and profile management.

3GPP Specification: TS 29.228

I-CSCF Operations

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

- **Purpose:** Query the HSS for S-CSCF assignment or capabilities
- **Trigger:** The I-CSCF receives a REGISTER from the user
- **Use Case:** The I-CSCF must route the registration to the correct S-CSCF

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

- **Purpose:** Query the HSS for the current S-CSCF of the user
- **Trigger:** The I-CSCF receives an INVITE or MESSAGE for the terminating user

- **Use Case:** The I-CSCF must route the session to the S-CSCF of the user

S-CSCF Operations

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

- **Purpose:** Retrieve authentication vectors from the HSS
- **Trigger:** The initial REGISTER, before the challenge
- **Use Case:** The S-CSCF must challenge the user for IMS AKA authentication

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

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

The **User-Data** AVP in the SAA contains the complete user profile. This profile includes:

- 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. The HSS pushes the request.
- **Trigger:** Administrative deregistration or subscription change
- **Use Case:** The HSS instructs the 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

Note on VoNR (5G NR): For VoNR sessions, the PCF authorizes media and QoS over the N5 AF interface (Npcf_PolicyAuthorization, HTTP/2 SBI). It does not use Diameter Rx. The Rx interface here therefore applies to 4G/LTE access.

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

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

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

- **Purpose:** PCRF-initiated policy update. The PCRF pushes the request.
- **Trigger:** A policy change or bearer modification
- **Use Case:** The PCRF instructs the P-CSCF to update the QoS policy

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

- **Purpose:** Release the Rx session and bearer resources
- **Trigger:** Call termination. The P-CSCF receives a BYE.
- **Use Case:** The P-CSCF informs the 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, or call termination
- **Use Case:** Prepaid charging and real-time credit checks

Types:

- **CCR-Initial:** Request credit at call start

- **CCR-Update:** Refresh the quota during the call
- **CCR-Terminate:** Report the final usage at call end

Peer Management via OmniWeb

View Diameter peer status, supported applications, and queue depths on the **Diameter** tab of each CSCF page in OmniWeb. OmniWeb is the unified management portal:

<<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>>.

The OmniWeb Diameter tab shows the following per CSCF:

- Realm and Diameter Origin-Host identity
- Configured peers and their connection state (I_Open, Closed, etc.)
- Supported Diameter applications per peer, mapped to 3GPP interface names (Cx/Dx, Sh/Dh, Rx, Ro, Gx, S6a/S6d, and others)
- Worker queue length and pending transactions
- Enable/disable operations for individual peers

Peer States

State	Description
I_Open	The connection is open and operational
Closed	No connection is established
Wait-Conn-Ack	The connection is initiated. It waits for a response.
Wait-I-CEA	The CER is sent. It waits for the CEA.

Diameter Result Codes

The following table lists 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 the destination	Check pe connecti
3003	DIAMETER_REALM_NOT_SERVED	The realm is not recognized	Verify the realm configura
3007	DIAMETER_APPLICATION_UNSUPPORTED	The application is not supported	Check th Applicati
4xxx	Transient Failures		
4001	DIAMETER_AUTHENTICATION_REJECTED	Authentication failed	Check th credentia
4010	DIAMETER_USER_UNKNOWN	The user is not provisioned	Verify the provision
5xxx	Permanent Failures		
5001	DIAMETER_AVP_UNSUPPORTED	The AVP is not recognized	Check th protocol version

Code	Name	Meaning	Action
5002	DIAMETER_UNKNOWN_SESSION_ID	The session is not found	The session expired or is invalid
5003	DIAMETER_AUTHORIZATION_REJECTED	Not authorized	Check the user permissions
5012	DIAMETER_UNABLE_TO_COMPLY	Cannot process the request	Check the HSS/PCRF logs

Common Issues

Critical Diameter Interfaces

When a Diameter peer goes down, the impact and the recovery urgency depend on the affected interface:

Interface	Impact if Down	Recovery Priority
Cx (HSS)	No new registrations. No IFC updates.	Critical. Recover immediately.
Rx (PCRF)	No QoS for new calls	High. Recover within minutes.
Ro (OCS)	No prepaid charging. Service can continue.	High. It depends on the policy.

Peer Connection Failures

Symptom: The peer is stuck in the "Closed" or "Wait-Conn-Ack" state

Diagnosis:

1. Verify the network connectivity:

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

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

Resolution:

- Fix the network and firewall issues
 - Verify the peer runs and listens on port 3868
 - Check that the peer has the correct configuration for the CSCF
 - Use **Enable Peer** on the OmniWeb Diameter tab to retry the connection
-

CER/CEA Exchange Failures

Symptom: The peer is stuck in the "Wait-I-CEA" state, or the CEA has an error code

Common Errors:

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

Resolution:

- Check the Diameter configuration for the Application-Id and realm
- Make sure that the peer configuration matches the CSCF expectations

- Review the CSCF backend logs for detailed error messages
-

HSS Cx Interface Issues

Symptom: Registration failures and MAR/MAA timeouts

Common Errors:

Result-Code	Meaning	Resolution
4010	USER_UNKNOWN	The user is not provisioned in the HSS
4001	AUTHENTICATION_REJECTED	The IMPI or credentials are incorrect
5012	UNABLE_TO_COMPLY	HSS internal error. Check the HSS logs.

Resolution:

- **USER_UNKNOWN:** Provision the user in the HSS
 - **AUTHENTICATION_REJECTED:** Verify the IMPI and shared secret in the HSS
 - **UNABLE_TO_COMPLY:** Check the HSS logs and the database connectivity
-

PCRF Rx Interface Issues

Symptom: Calls succeed but no QoS is applied. AAR/AAA timeouts occur.

Common Issues:

- **PCRF down:** Check the peer status on the OmniWeb Diameter tab

- **Framed-IP-Address not recognized:** The PCRF cannot map the UE IP to the subscriber
- **Policy not applied:** Check the PCRF policy rules. Verify the PCEF integration.

Resolution:

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

OCS Ro Interface Issues

Symptom: Prepaid calls fail. CCR/CCA timeouts occur. Calls are blocked.

Common Errors:

Result-Code	Meaning	Resolution
4012	CREDIT_LIMIT_REACHED	Insufficient credit
5003	AUTHORIZATION_REJECTED	The user is not authorized for prepaid

Resolution:

- **CREDIT_LIMIT_REACHED:** Normal for prepaid users without credit
 - **OCS timeout:** Check the OCS availability and the peer status
 - **AUTHORIZATION_REJECTED:** Verify that the user is provisioned for prepaid in the OCS
-

Performance Degradation

Symptom: Slow Diameter response times and high latency

Diagnosis:

1. Check the "Last Used" timestamp in the peer list. It must be recent.
2. Monitor the "Queue Length". High values indicate a backlog.
3. Review the CSCF backend logs for timeout warnings

Resolution:

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

Best Practices

Operational Guidelines

Peer Management:

- Monitor the peer status on the OmniWeb Diameter tab
- Set up external monitoring for peer-down events
- Test the peer connectivity during maintenance windows

Capacity Planning:

- Estimate the Diameter transaction rate from the registrations and the call volume
- Make sure that the HSS/PCRF/OCS can handle peak transaction rates
- For large deployments, consider Diameter routing agents (DRA)

Troubleshooting:

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

Security:

- Use TLS for Diameter connections in production, if TLS is supported
- Restrict Diameter peer access with the firewall. Allow only known peers.
- Review the peer enable/disable audit logs regularly

Limitations and Future Enhancements

Current Implementation

The OmniWeb Diameter tab provides:

- ☐ Real-time peer status viewing
- ☐ Enable/disable peer operations
- ☐ Application ID to interface name mapping

Not Yet Implemented

The following features are **not currently available**. Future versions can add them:

- **Diameter Message Inspector:** View recent Diameter transactions and AVP details
- **Peer Statistics:** Message counts, success rates, and average latency per peer
- **Watchdog Monitoring:** Real-time DWR/DWA status

Workarounds

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

For Detailed Statistics: Query the metrics from the Prometheus endpoint. See [Metrics Reference](#) for complete CDP/Diameter metric definitions and monitoring setup.

For Manual Reconnect: Use the OmniWeb Diameter tab 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
- **5G SBI Operations Guide** - N5/NRF service-based interfaces used for VoNR (the 5G counterpart to Rx)
- **Metrics Reference** - CDP/Diameter metrics and monitoring
- **OmniWeb** - Diameter peer management via the OmniWeb Diameter tab
- **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
- **Management Portal:** OmniWeb
(<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>)

Peer Configuration (Deployment)

Each CSCF node has a Diameter peer configuration file: `pcscf.xml`, `icscf.xml`, or `scscf.xml`. Ansible renders the file at deploy time. The file defines the Diameter identity of the node and the HSS/PCRF/DRA peers that it connects to. The structure is identical across all three files. Only the advertised application differs.

XML field	What it configures	Ansible source
DiameterPeer FQDN	The Diameter origin-host FQDN of this node	<inventory_hostname>.epc.mnc<mnc>.m
DiameterPeer Realm	The local Diameter realm	ims_realm if defined, else epc.mnc<mnc>.mcc<mcc>.3gppnetwork.o
Vendor_Id / Product_Name	The CER identity	10415 (3GPP) / OmniCSCF
Peer (direct mode)	Direct peer to each hss-group host over SCTP:3868	rendered per host in groups['hss'] wh false
Peer (DRA mode)	Peer to each dra-group host. Explicit IP when diameter_dra_ip is set.	rendered per host in groups['dra'] wh true
Acceptor	Local bind FQDN and port for inbound Diameter (3868)	node FQDN
DefaultRoute	Realm-routing default route to the HSS/PCRF peer (metric 1) or the DRA (metric 2)	rendered from groups['hss'] / groups[

Advertised application(s) per node:

Node (file)	Application(s)
P-CSCF (pcscf.xml)	Rx 16777236 (vendors 10415, 0)
I-CSCF (icscf.xml)	Cx 16777216 (vendors 10415, 13019, 0) + base accounting 4
S-CSCF (scscf.xml)	Cx 16777216 (vendors 10415, 13019, 0) + base accounting 4

The key Ansible variables are as follows. `plmn_id.mcc` and `plmn_id.mnc_longform` build all FQDNs and realms. `ims_realm` overrides the Diameter realm. `ims_dra_support` switches between direct-peer and DRA peering. `diameter_dra_ip` sets the static IP for the DRA peer. The `hss` and `dra` inventory groups provide the peer and default-route lists. When charging is enabled, `R0_DESTINATION` addresses the **Ro** peer (OCS) of the S-CSCF separately. The XML does not address this peer.

Edit these files through the deployment tooling, not through OmniWeb. OmniWeb provides monitoring and operational control (enable/disable) only.

I-CSCF Operations & Reference

The Interrogating-CSCF is the home network's inbound contact point for IMS signalling. A subscriber reaches this node when the subscriber registers. A session reaches this node when the session terminates toward a home subscriber. The I-CSCF holds no session state. The I-CSCF terminates no media. The I-CSCF consults the HSS over Cx. This consultation decides which Serving-CSCF handles a given request. On registration, the I-CSCF authorises the identity and the visited network. The I-CSCF then discovers the S-CSCF, or the S-CSCF capabilities to select one. On a terminating request, the I-CSCF locates the S-CSCF that already serves the user. After the I-CSCF chooses an S-CSCF, the I-CSCF forwards the request to that S-CSCF. The I-CSCF relays the responses back.

IMS Functions

Registration routing (Cx UAR)

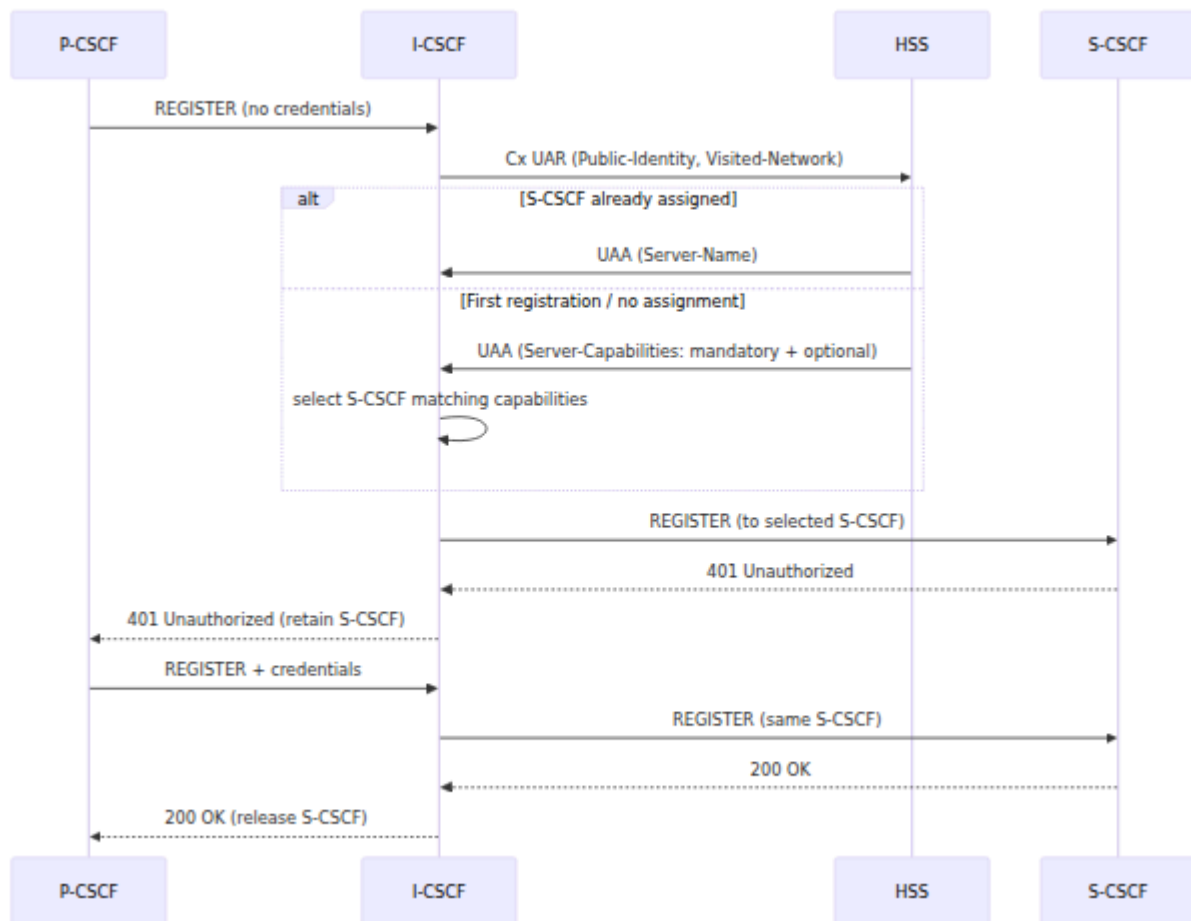
When a REGISTER arrives, the I-CSCF queries the HSS with a Cx **User-Authorization-Request (UAR)**. The I-CSCF sends this query before it forwards the REGISTER. The UAR carries the public identity and the visited-network identifier. These values let the HSS authorise the subscriber to register from that network. The answer (UAA) returns one of two things:

- **An already-assigned S-CSCF name.** The I-CSCF uses this name directly. A re-registration returns to the same S-CSCF that holds the binding.
- **S-CSCF capabilities.** These are a set of mandatory and optional capability values that the selected S-CSCF must satisfy. The HSS returns these values on first registration, or when no S-CSCF is currently assigned. The I-CSCF then does capability-based selection (below).

The I-CSCF forwards the REGISTER to the chosen S-CSCF. The I-CSCF remembers that S-CSCF for the duration of the registration handshake. The

authenticated re-REGISTER follows the 401 challenge. The I-CSCF routes this re-REGISTER to the **same** S-CSCF and does not query again. The I-CSCF retains the S-CSCF while a 401 is in flight. The I-CSCF discards the S-CSCF when registration completes (2xx) or finally fails.

An HSS that is unavailable or returns a malformed answer yields **503**. A UAR can authorise but yield no S-CSCF to select. In this case, the I-CSCF falls back to a configured default S-CSCF URI.



Terminating routing (Cx LIR)

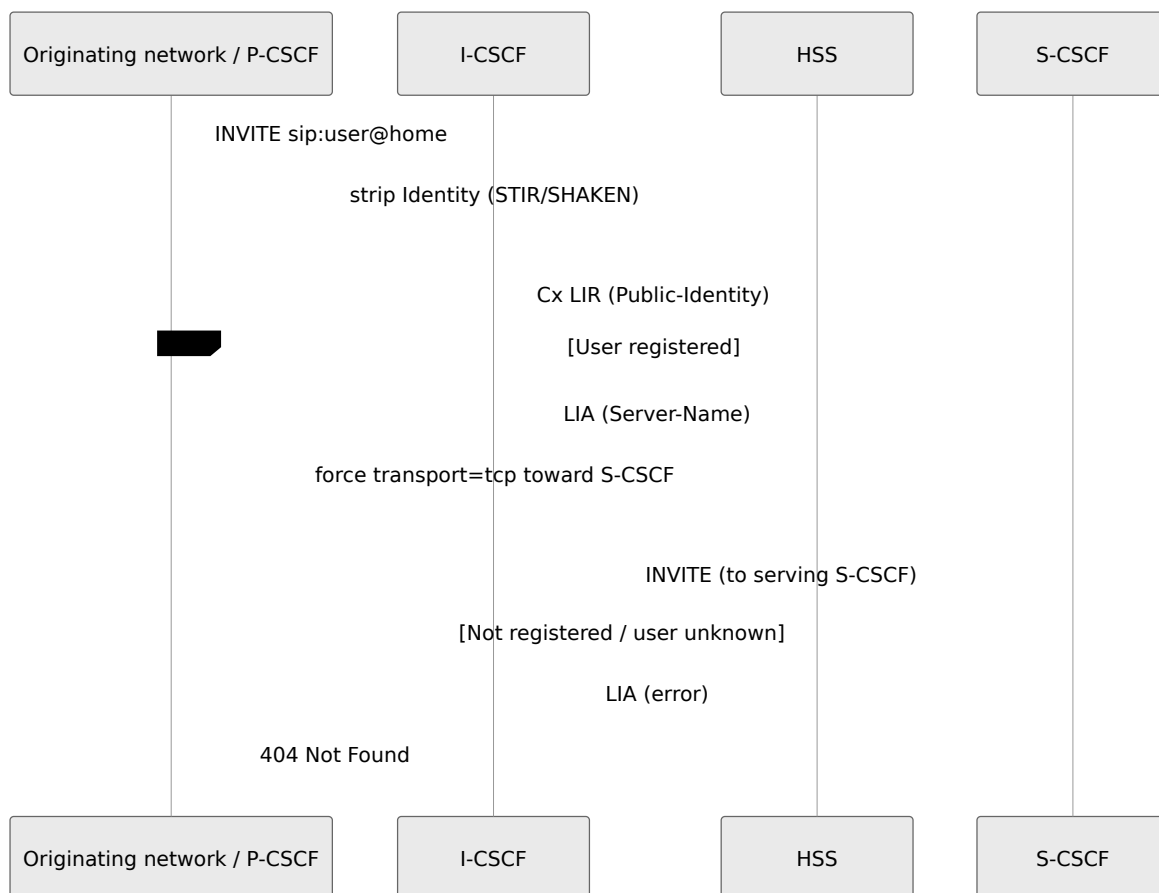
An initial terminating request is an INVITE, SUBSCRIBE, MESSAGE, INFO, or PUBLISH. On such a request, the I-CSCF queries the HSS with a Cx **Location-Info-Request (LIR)** for the Request-URI identity. The answer (LIA) returns the name of the S-CSCF that currently serves the user. For an unregistered user that has services provisioned, the LIA returns capabilities instead. The I-CSCF then selects an S-CSCF from these capabilities. The I-CSCF forwards the request to that S-CSCF. If the returned URI does not specify a transport, the I-CSCF

forces TCP transport toward the S-CSCF. The I-CSCF strips any inbound STIR/SHAKEN **Identity** header before it forwards the request.

Result handling:

- **Success.** The I-CSCF selects the S-CSCF and relays the request to it. A relay failure returns **500**.
- **User not found / not registered.** The I-CSCF returns **404 Not Found**.
- **HSS unavailable.** The I-CSCF returns **503**.

The I-CSCF does not interrogate CANCEL. The I-CSCF matches CANCEL to its existing transaction and relays it. The I-CSCF rejects any other non-initial, non-REGISTER method with **406** and an **Allow** list.

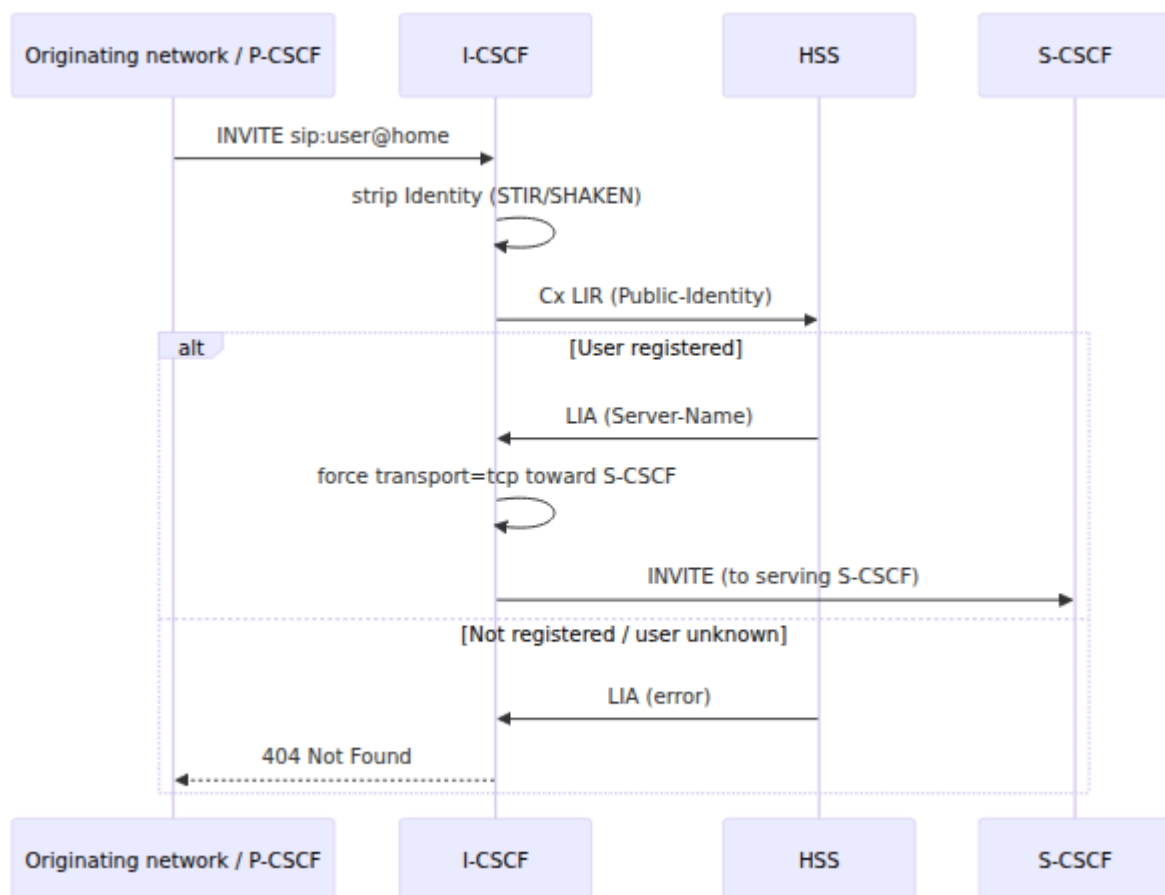


S-CSCF selection / capability matching

The HSS can return capabilities instead of an assigned S-CSCF name. In this case, the I-CSCF selects an S-CSCF from its **configured S-CSCF set**. Each candidate S-CSCF has a SIP URI and a set of capability values. Selection

requires that the S-CSCF satisfies **all mandatory** capabilities. Among the qualifying candidates, the I-CSCF prefers those that match more of the **optional** capabilities. Several candidates can be equally suitable. These candidates form an ordered candidate list. This list lets the I-CSCF try an alternate on failure.

The I-CSCF holds the candidate list in transaction memory for the life of the request. This preserves the list position across attempts. A forwarded REGISTER leg can time out or draw a 5xx/6xx. In this case, the I-CSCF advances to the next candidate S-CSCF and retries. When the list is exhausted, the I-CSCF stops. The I-CSCF retains the list across a 401 challenge, because the same S-CSCF must handle the authenticated retry. The I-CSCF drops the list on a successful or client-error final response. If selection yields nothing at all, the I-CSCF falls back to the configured default S-CSCF URI.



Deployment Configuration (Ansible-injected)

Ansible renders the I-CSCF's runtime configuration (`icscf.cfg`) and its Diameter peer table (`icscf.xml`) at deploy time. Values derive from the network's PLMN identity (MCC/MNC) and the node's inventory hostname. Feature toggles are `#!define` flags. A defined flag enables the feature. A commented-out flag disables the feature.

Identity / realm

Name	What it controls	Value / default
NETWORKNAME	Home IMS domain. This is the Cx destination realm (<code>cxdx_dest_realm</code>). The I-CSCF checks this domain when it routes peered or unknown-user requests.	<code>ims.mnc<mnc>.mcc<mcc>.3gppnet</code>
HOSTNAME	This node's FQDN (host alias)	<code><inventory_hostname>.ims.mnc<mnc>.mcc<mcc>.3gppnet</code>
ICSCF_USER_AGENT	The <code>User-Agent</code> header that the node emits	<code>User-Agent: Omnitouch I-CSCF <inventory_hostname></code>
ICSCF_SERVER	The <code>Server</code> header that the node emits	<code>Server: Omnitouch I-CSCF <inventory_hostname></code>
SCSCF_URI	Default or fallback S-CSCF URI. The I-CSCF uses this URI when UAR-based selection yields no S-CSCF.	<code>sip:scscf.ims.mnc<mnc>.mcc<mcc>.3gppnet</code>

Ansible templates the SIP listen sockets (UDP/TCP 5060, TLS 9090) from the inventory host address and PLMN. Ansible also templates the host aliases (`ims....`, `icscf.ims....`, `<host>.ims....`) from these values.

`CAPTURE_NODE` is the Homer capture target, `sip:<homer_host>:9060`. Ansible templates this value only when Homer capture is enabled for the deployment.

Homer capture needs `enable_homer` with a `homer` inventory group.
`CAPTURE_NODE` duplicates SIP signalling to Homer over HEP for tracing.

Diameter peer configuration

The I-CSCF's Diameter peer table (`icscf.xml`) advertises the **Cx** application (`16777216`) toward the HSS. All CSCFs share the file structure and the Ansible variables that fill it. See [Diameter → Peer Configuration \(Deployment\)](#).

Troubleshooting

Registration failures or terminating-session failures surface at the I-CSCF. These failures usually come from one of two causes:

- **S-CSCF selection / assignment.** The HSS can return capabilities instead of an assigned S-CSCF name. Selection then requires that the S-CSCF satisfies all mandatory capabilities. If no candidate qualifies, the I-CSCF falls back to the configured default S-CSCF URI. If a forwarded REGISTER draws a timeout or 5xx/6xx, the I-CSCF fails over to the next candidate until the list is exhausted. Confirm that the configured S-CSCF set and its capability values match what the HSS returns.
- **Cx connectivity to the HSS (UAR / LIR).** The I-CSCF cannot route without an answer to the Cx UAR (on REGISTER) or LIR (on a terminating request). An unavailable or malformed HSS answer yields **503**. A user that is unknown or not registered yields **404**. Verify that the Cx peer to the HSS is up. See [Diameter Operations](#).

Call Flows

The sequence diagrams appear with the functions that they document:

- Registration via I-CSCF → [Registration routing \(Cx UAR\)](#)
- Terminating session via I-CSCF → [Terminating routing \(Cx LIR\)](#)
- S-CSCF failover → [S-CSCF selection / capability matching](#)

Related Documentation

- [S-CSCF Operations & Reference](#)
- [Operations](#)
- [Diameter](#)
- [Metrics Reference](#)
- OmniWeb - S-CSCF list, active sessions, and Cx Diameter peer state:
<<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>>

P-CSCF Operations & Reference

The Proxy-CSCF is the SIP entry point of the IMS for User Equipment. Every REGISTER and every session from the UE arrives here first. The P-CSCF establishes and enforces the access-security association that protects the UE signalling. The P-CSCF inserts itself into the routing path. It adds a Path header on registration and a record-route on sessions. All subsequent traffic then traverses this node. This traffic includes terminating requests and in-dialog messages. The P-CSCF detects the UE access technology to drive media-bearer policy. The P-CSCF also provides the emergency-session entry point (E-CSCF) with a usable calling-line identity per TS 23.167. The P-CSCF is a signalling proxy only. Media flows directly between the UE and the terminating side. Media never flows through this node.

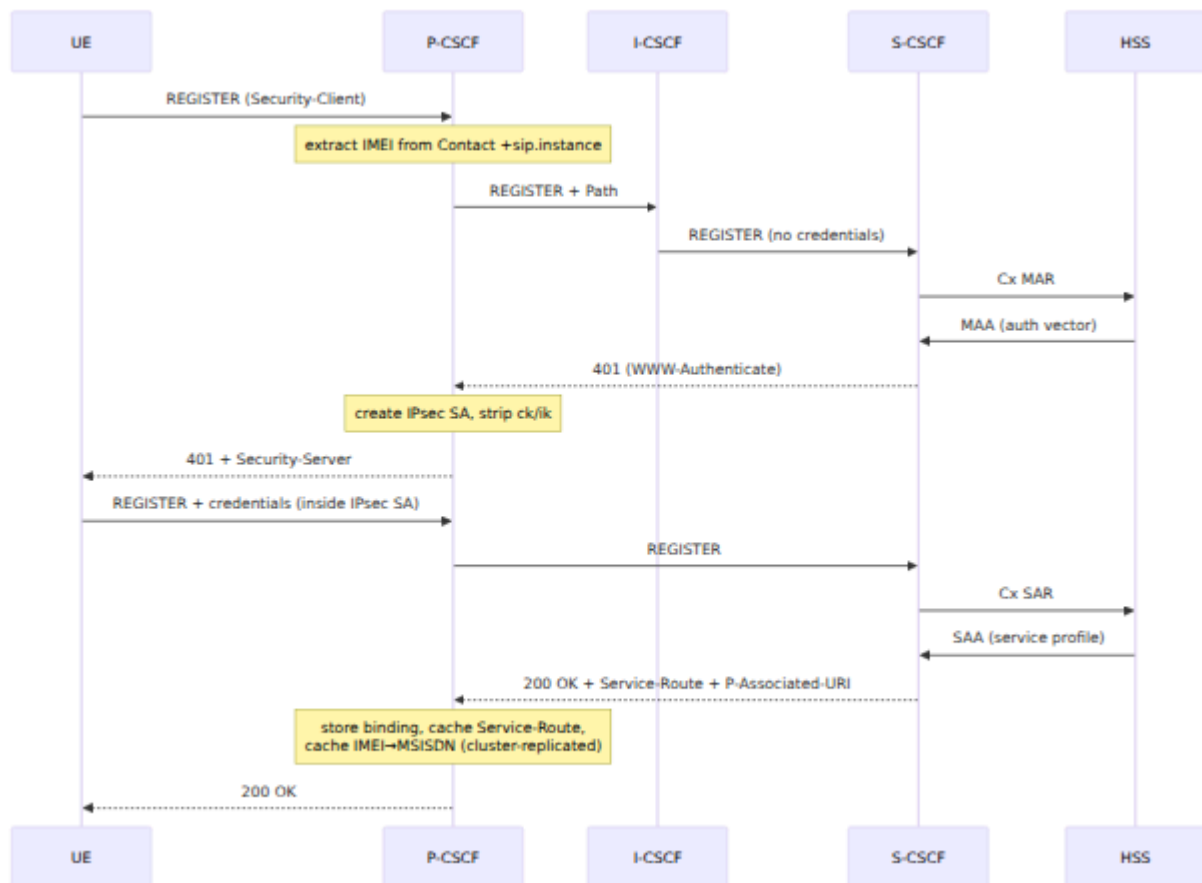
IMS Functions

Registration proxy & IPsec security association

The P-CSCF is the UE registrar-facing proxy. The P-CSCF relays the REGISTER toward the home network (I-CSCF/S-CSCF). On the challenge/response exchange the P-CSCF establishes an IPsec ESP security association with the UE. This is part of the IMS-AKA procedure. During registration the UE and the P-CSCF negotiate the SA parameters through the `Security-Client` / `Security-Server` headers. From the authenticated re-REGISTER onward, the SA carries all signalling for that UE.

On the forwarded REGISTER the P-CSCF inserts a **Path** header. This routes terminating requests back through this same node. The P-CSCF forces the registration expiry to a network-controlled value. The P-CSCF advertises `path` support. On the successful `200 OK` the P-CSCF stores the contact binding. The P-CSCF caches the returned `Service-Route` and `P-Associated-URI`. This steers subsequent requests through the correct home-network path.

Each registered UE uses **one** security association from a per-deployment resource pool. The P-CSCF releases the SA when the UE de-registers (expiry 0) or its registration lapses. The P-CSCF rejects a REGISTER whose Contact marks an emergency (`;sos`) registration. The P-CSCF handles emergency sessions directly on the INVITE, not through emergency registration.



Access detection & QoS / policy control

The P-CSCF never relays media. The P-CSCF still authorises the dedicated media bearer with the policy plane. The P-CSCF classifies the UE access from the `P-Access-Network-Info` header (per TS 24.229 §5.2.6.3). LTE reports `3GPP-E-UTRAN`. 5G NR reports `3GPP-NR`. WiFi access has no dedicated bearer. The P-CSCF excludes WiFi access from dynamic QoS.

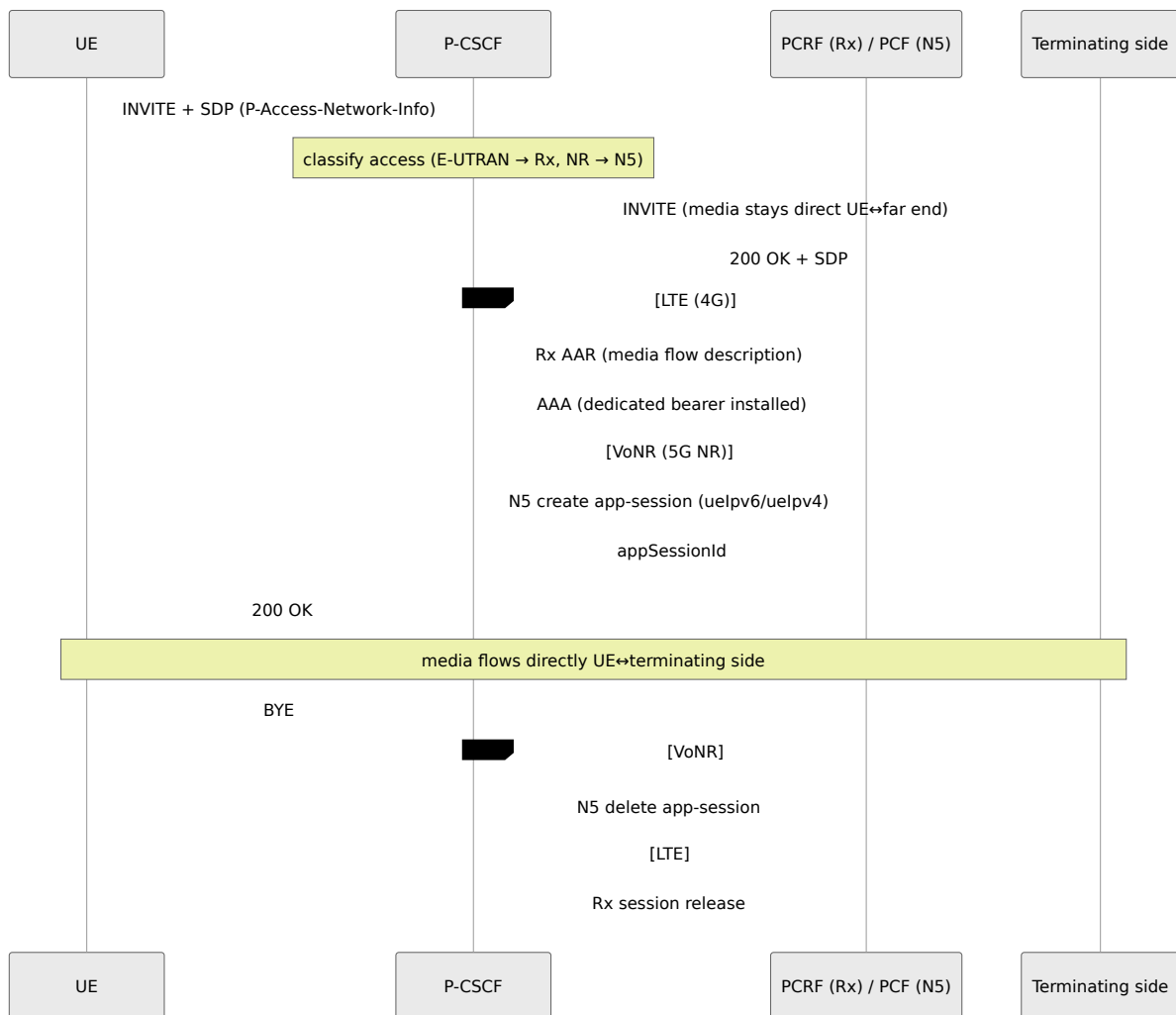
- **4G / LTE** - the P-CSCF authorises the media bearer QoS over **Diameter Rx** to the PCRF. On the answering leg (the `200 OK` carrying SDP) the P-CSCF issues an Authorization/Authentication Request (AAR). The AAR describes the audio media flow, and the video media flow where present. The PCRF then installs the corresponding dedicated bearer. The P-CSCF refreshes the

authorisation on in-dialog re-INVITEs. The P-CSCF releases the authorisation when the dialog ends.

- **VoNR (5G NR)** - the P-CSCF authorises the bearer QoS over the **N5** interface to the PCF. The P-CSCF uses the `Npcf_PolicyAuthorization` service. The P-CSCF acts as an Application Function. When the far end answers the media, the P-CSCF creates an application session on the PCF. This session uses afAppId `VoNR`, an `AUDIO` media component with `ENABLED` flow status, and a flow descriptor for the UE media. It also includes an AF notification URI for the PCF to call back on. The P-CSCF deletes that application session when the dialog ends.

The QoS authorisation runs on both the originating (MO) and terminating (MT) legs. It is keyed on the UE own IP address. **UE address binding:** the P-CSCF encodes the UE address to match the PDU-session/bearer binding the policy node holds. The P-CSCF signals an IPv6 UE as `ueIpv6` and an IPv4 UE as `ueIpv4`. A v6 address placed in the v4 field never matches the PCF binding. The PCF then installs no dedicated bearer.

For VoNR the P-CSCF locates the serving PCF via **NRF discovery**. The P-CSCF registers as an AF. For each session, the P-CSCF resolves the PCF bound to the UE PDU session through the NRF→BSF chain. This is the only PCF discovery path.



Emergency calls (E-CSCF) & calling-line identity - TS 23.167

The P-CSCF is the emergency entry point. The P-CSCF detects an emergency session by the emergency service URN (`urn:service:sos`) on the INVITE. The P-CSCF routes it directly to the emergency application server. This bypasses the normal registration check. An emergency INVITE frequently carries **no MSISDN**. The P-CSCF therefore supplies a usable calling-line identity for the PSAP. This applies even for callers that are unknown or anonymous. This complies with TS 23.167 Annex K and TS 29.214 §4.4.6a.

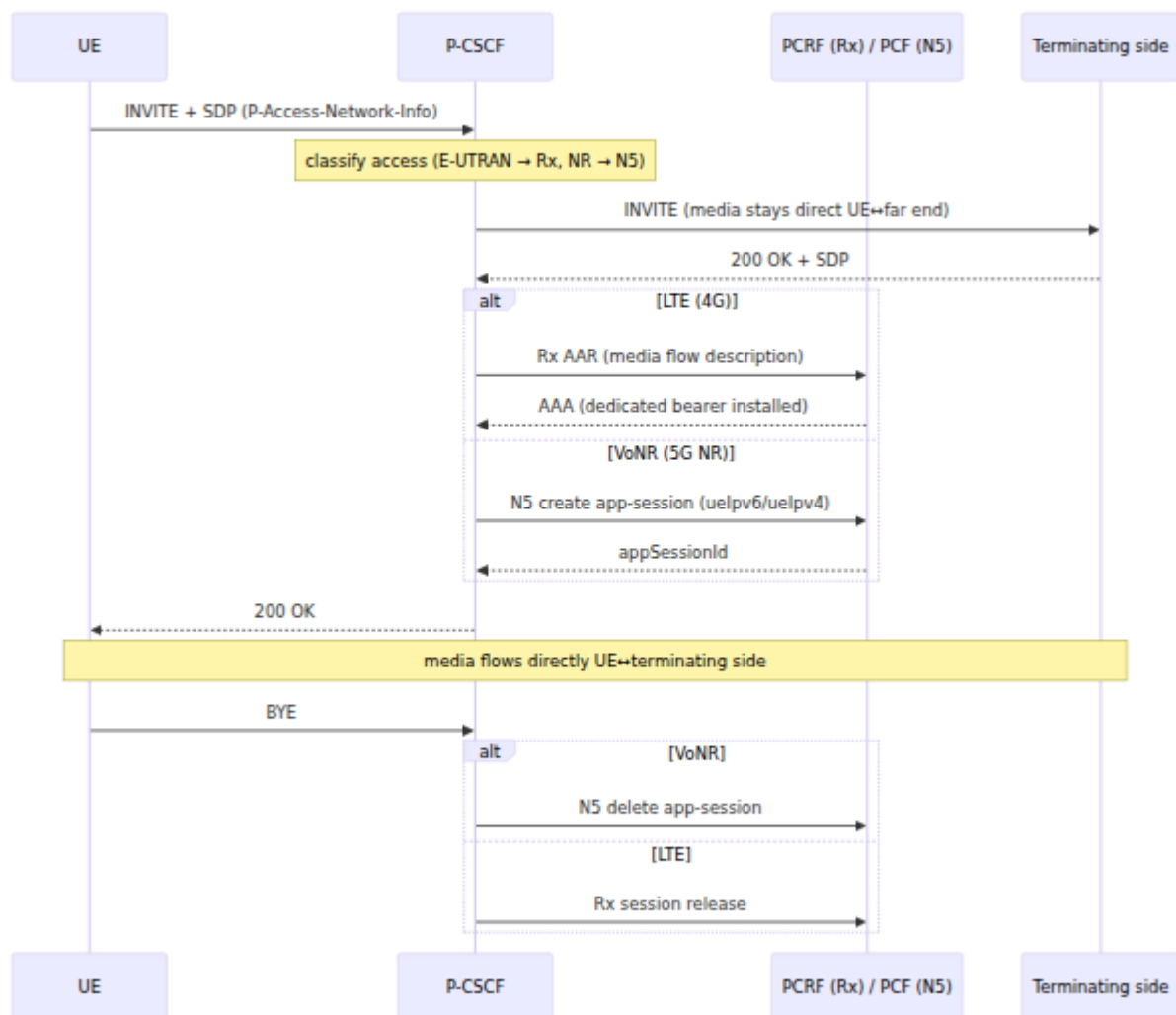
Two complementary mechanisms resolve the identity:

1. **Cached IMEI→MSISDN binding (fast path).** On each successful REGISTER the P-CSCF caches a binding. The binding maps the UE IMEI (from the Contact `+sip.instance`) to the MSISDN (from `P-Associated-`

URI). The P-CSCF **replicates the binding across all P-CSCF nodes**. Any node can then resolve the identity regardless of where the UE registered. On the emergency INVITE the P-CSCF extracts the IMEI and looks up the cached MSISDN.

2. **Asynchronous subscription query (unknown/anonymous callers)**. If no cached binding exists, the P-CSCF issues an asynchronous Rx subscription query to the PCRF. The query is keyed on the UE source IP address. The P-CSCF suspends the INVITE until the answer returns. The PCRF returns the EPC-level identities. The P-CSCF chooses one by precedence **MSISDN → IMSI → IMEISV**. The P-CSCF caches an IMEISV result back for reuse.

The P-CSCF asserts the resolved identity as the caller From URI and as a P-Asserted-Identity on the `sos.apn` domain. The P-CSCF restores the identity consistently on replies and in-dialog requests. The PSAP then sees a usable callback identity even for an originally anonymous caller. Whichever path resolves the identity, the emergency INVITE receives the same media/QoS and header treatment as any other originating request. The P-CSCF then forwards it to the emergency application server.



Security / anti-flood

The P-CSCF applies source-based flood protection. The P-CSCF rate-limits requests per source IP. The P-CSCF bans an IP that exceeds the sampling threshold for a hold-off period. The P-CSCF tracks failed registration authentication per source IP in a short-lived counter. The P-CSCF bans a source that exceeds the failed-attempt threshold within the window. This defeats credential-guessing. The P-CSCF drops requests that a UE addresses to the node itself. The P-CSCF also drops malformed messages. Under memory pressure the node sheds new requests with 503.

Cluster replication

The P-CSCF replicates registration-related and emergency state across P-CSCF nodes. In particular the P-CSCF synchronises the IMEI→MSISDN emergency binding between nodes. The P-CSCF does a full sync on start-up. Any node in

the cluster can then serve terminating traffic and resolve emergency-call identity. This works regardless of which node originally registered the UE. The P-CSCF needs no per-node provisioning.

Deployment Configuration (Ansible-injected)

Ansible renders the P-CSCF runtime configuration and its Diameter peer table (`pcscf.xml`) at deploy time. Most values derive from the network PLMN identity (MCC/MNC) and the node inventory hostname. Ansible emits the 5G SBI and PCF blocks only when the deployment inventory contains the relevant network functions.

Identity

Name	What it controls	Value / derivation
NETWORKNAME	Home IMS domain used in P-Visited-Network-ID and identity rewrites	ims.mnc<mnc>.mcc<mcc>.3gppnetwork
HOSTNAME	This node's FQDN (also its host alias)	<inventory_hostname>.ims.mnc<mnc>
URI	The P-CSCF's own SIP URI	sip:<hostname>:5060
PCSCF_URL	Source URI used for NAT-keepalive OPTIONS pings	sip:<hostname>:5060
PCSCF_USER_AGENT	User-Agent header the node emits	User-Agent: Omnitouch Proxy-CSCF

Name	What it controls	Value / derivation
PCSCF_SERVER	Server header the node emits	Server: Omnitouch Proxy-CSCF <ip>
DMQ_NOTIFICATION_ADDR	Cluster notification address for state replication between P-CSCF nodes	sip:pcscf.ims.mnc<mnc>.mcc<mcc>.

Ansible templates the SIP listen sockets (UDP/TCP 5060, plus IPv6 5060 where an IPv6 address is defined) and the Prometheus HTTP socket (TCP 9090) from the inventory host address. The P-CSCF fronts UEs on IPv6 where available. Peers behind it remain IPv4. Ansible also builds the `PATH_HEADER` and `P_VISITED_NETWORK_ID_HEADER` from the hostname and PLMN.

Rx / policy control (4G)

Name	What it controls	Value / derivation
<code>RX_DEST_REALM</code>	Diameter destination realm for Rx toward the PCRF	<code>{{ diameter_realm }}</code>
<code>PCRF_REALM</code>	PCRF realm	<code>epc.mnc<mnc>.mcc<mcc>.3gpp</code>
<code>RX_AF_SIGNALING_IP</code>	AF-signalling IP carried in the Rx AAR (this P-CSCF)	node <code>ansible_host</code> (override double-NAT)
<code>RX_IMS_REG_DIALOG_DIRECTION</code>	Dialog-direction mode for Rx registration	<code>3</code>

Fixed Rx media parameters include video authorisation on, a 64 kbit/s default/minimum audio bandwidth, RTCP flow inclusion, and a 24-hour maximum authorised session duration.

5G SBI / PCF (VoNR)

Emitted when the deployment inventory contains a PCF and an NRF.

Name	What it controls	Value / derivation
VONR_AF_NOTIF_URI	AF notification endpoint the PCF calls back on	http://<this host>: <pcscf_af_notif_port 9999>/
NRF_URI	NRF base URI for AF registration and discovery	http://<nrf host>: <nrf_sbi_port 7777>
IMS_NRF_NF_IPV4	This P-CSCF's NF IPv4 for its AF registration	node <code>ansible_host</code>
IMS_NRF_PLMN_MCC / IMS_NRF_PLMN_MNC	PLMN advertised in NRF registration/discovery	from <code>plmn_id</code>

PCF discovery: the P-CSCF registers with the NRF as an AF. For each VoNR session, the P-CSCF resolves the PCF bound to that UE PDU session via the NRF→BSF chain. App-sessions then always reach the correct per-subscriber PCF. This includes multi-PCF 5G cores. This is the only supported discovery path.

Sizing / transport

Name	What it controls	Value
CAPTURE_NODE	Homer SIP-capture target (templated only when Homer capture is enabled)	sip:<homer host>:9060

The base configuration tunes the number of SIP (UDP) worker processes and the registrar hash-table size for the deployment scale. iOS UEs get a shortened TCP connection lifetime to match their transport behaviour.

Diameter peer configuration

The P-CSCF Diameter peer table (`pcscf.xml`) advertises the **Rx** application (`16777236`) toward the PCRF. All CSCFs share the file structure and the Ansible variables that fill it. See [Diameter → Peer Configuration \(Deployment\)](#). Rx is only active when `WITH_RX` is defined.

Troubleshooting

Registration / IPsec connectivity

Users that cannot register, or registration timeouts, often point to the P-CSCF access-security or discovery layer rather than the home network:

- **IPsec SA establishment** - mobile devices must complete the IMS-AKA `Security-Client` / `Security-Server` negotiation. If the authenticated re-REGISTER never arrives inside the SA, check two things. Confirm that the UE and P-CSCF agreed on SA parameters. Confirm that no middlebox strips the security headers.
- **NAT traversal** - for devices behind NAT, verify the far-end NAT handling. Verify that keepalive OPTIONS pings reach the UE. The pinhole for terminating traffic then stays open.
- **P-CSCF discovery** - verify that the UE discovers the correct P-CSCF address (via DNS, DHCP, or static configuration). Verify that the SIP listen sockets are reachable on the access network.

Emergency call issues

Symptoms: Emergency calls not routing to the PSAP, or the PSAP receives no usable calling-line identity (CLI) / callback number.

- **Emergency detection** - the P-CSCF routes on the emergency service URN (`urn:service:sos`), plus the dialled emergency numbers. Confirm that the INVITE carries the expected emergency indication. Confirm that emergency routing bypasses the normal registration check.

- **CLI resolution for anonymous / unknown callers** - the P-CSCF supplies the caller identity from the cached IMEI→MSISDN binding (cluster-replicated, 4-hour TTL). For a caller with no cached binding, the P-CSCF falls back to an asynchronous Rx subscription query to the PCRF. The query is keyed on the UE source IP. The P-CSCF resolves an EPC identity by precedence **MSISDN → IMSI → IMEISV** (TS 23.167 Annex K). If the PSAP sees an anonymous caller, verify one of two things. Verify that the P-CSCF cached the binding at registration. Otherwise verify that the Rx subscription query returned an identity. OmniWeb shows the cached binding map.
- **Location availability** - verify that location information is available for E911/E112. Verify that the location retrieval leg (LRF) is reachable.
- **Test routing** - you can exercise emergency call routing without an actual PSAP connection. This confirms detection, identity assertion on the `sos.apn` domain, and routing to the emergency application server.

Emergency sessions succeed even for unregistered users, users with no SIM or invalid credentials, and roaming users. See [Emergency calls \(E-CSCF\) & calling-line identity - TS 23.167](#) for the underlying mechanism.

Call Flows

The sequence diagrams appear with the functions they document. The full session ladders appear below:

- Registration & IPsec SA → [Registration proxy & IPsec security association](#)
- Media QoS / policy (MO & MT) → [Access detection & QoS / policy control](#)
- Emergency session → [Emergency calls \(E-CSCF\) & calling-line identity - TS 23.167](#)

Mobile Originating call (MO)

The P-CSCF routes originating calls through the S-CSCF (via the cached Service-Route) to the TAS for service logic and charging. Media stays direct.

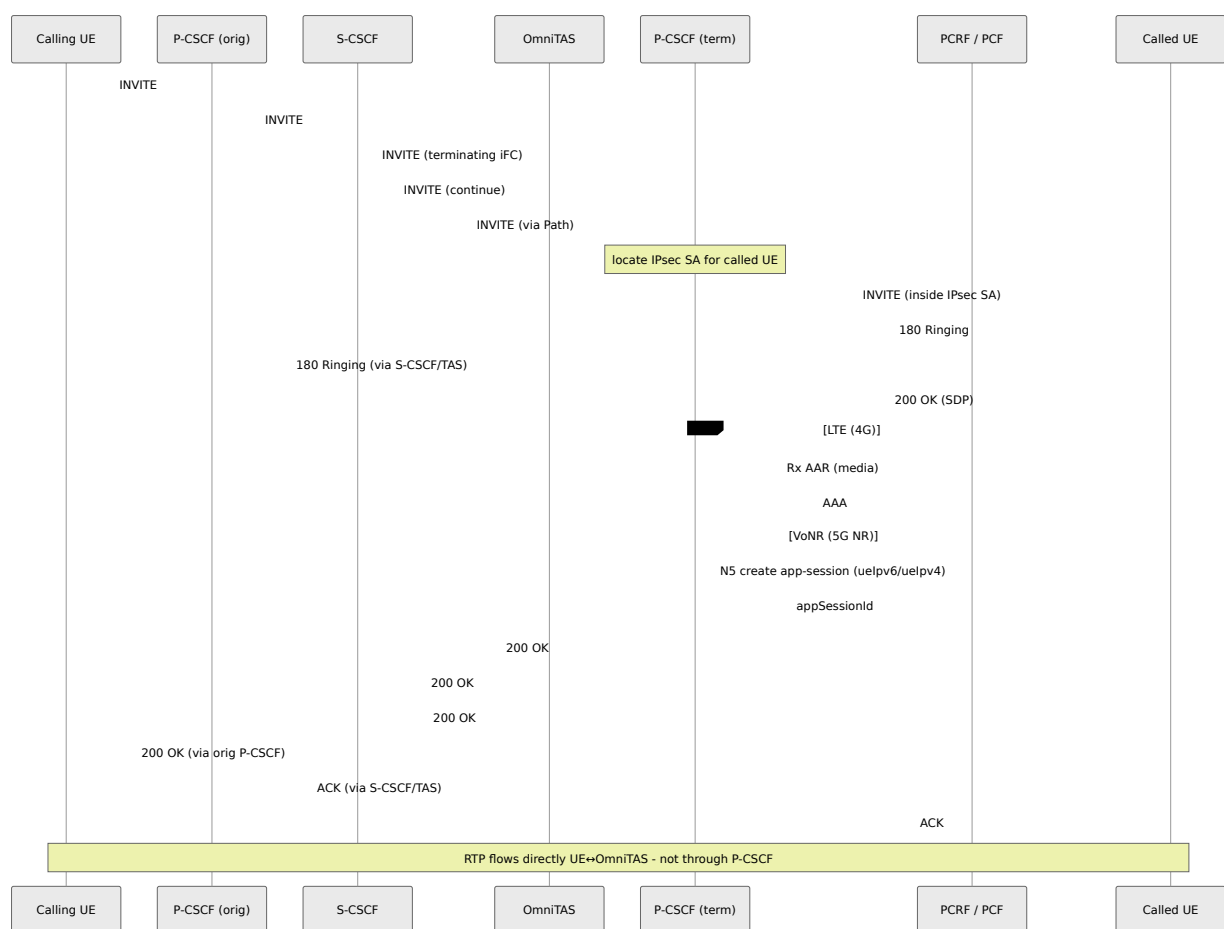
Parse error on line 10: ...-ID; classify access PCSCF->>SCSCF: -----
 --^ Expecting 'SOLID_OPEN_ARROW', 'DOTTED_OPEN_ARROW',

'SOLID_ARROW', 'BIDIRECTIONAL_SOLID_ARROW', 'DOTTED_ARROW',
'BIDIRECTIONAL_DOTTED_ARROW', 'SOLID_CROSS', 'DOTTED_CROSS',
'SOLID_POINT', 'DOTTED_POINT', got 'NEWLINE'

Try again

Mobile Terminating call (MT)

Terminating calls arrive back through the P-CSCF recorded in the Path at registration. The P-CSCF authorises QoS when the called UE answers.



Related Documentation

- [Operations](#)
- [Diameter](#)
- [Service-Based Interface \(SBI\)](#)
- [Metrics Reference](#)

- OmniWeb - registered contacts, hash tables (including the emergency IMEI→MSISDN map), NRF/PCF discovery, and Rx peer state:
<<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>>

5G SBI Operations Guide

Table of Contents

1. [Overview](#)
2. [SBI in the IMS Architecture](#)
3. [N5 - Npcf_PolicyAuthorization \(P-CSCF → PCF\)](#)
4. [Nnrf - NF Management and Discovery \(P-CSCF ↔ NRF\)](#)
5. [When SBI is Used vs Diameter](#)
6. [Configuration](#)
7. [Management via OmniWeb](#)
8. [Common Issues](#)
9. [Related Documentation](#)

Overview

The 5G core is **service-based**. Network functions expose HTTP/2 and JSON REST APIs to each other over the Service-Based Interface (SBI). The SBI replaces Diameter. For VoNR (Voice over New Radio), the P-CSCF acts as a 5G **Application Function (AF)**. The P-CSCF uses SBI to authorize media QoS. The P-CSCF also uses SBI to discover the network functions that it needs.

The SBI replaces the Diameter Rx path used for VoLTE. See [Diameter Operations](#) for the 4G/LTE side.

What is SBI?

The Service-Based Interface (3GPP TS 29.500) differs from Diameter in these ways:

- **Transport:** HTTP/2 over TCP. Diameter uses TCP or SCTP.

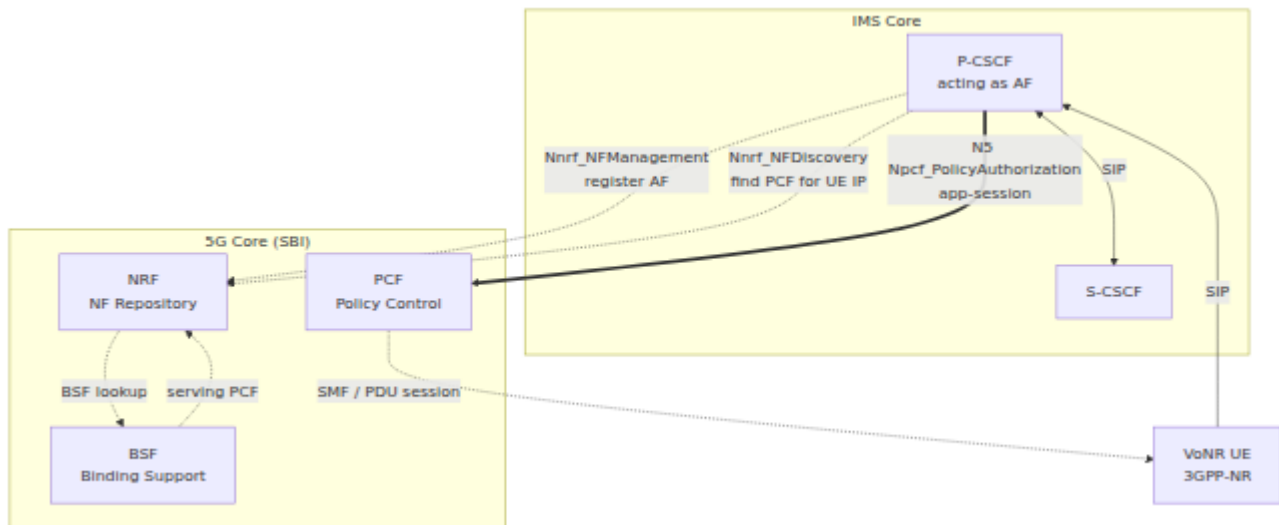
- **Encoding:** JSON payloads described by OpenAPI. Diameter uses AVPs.
- **Model:** RESTful resources. You create, modify, or delete an *app-session* resource. Diameter uses request and answer command pairs.
- **Discovery:** the **NRF** finds producers dynamically. Diameter uses statically configured peers.
- **Naming:** services use the name `Nxxx` (for example `Npcf_PolicyAuthorization`, `Nnrf_NFDiscovery`)

SBI in the CSCF

The P-CSCF is the only CSCF component that uses SBI. As a 5G Application Function (AF), the P-CSCF authorizes VoNR media QoS over N5 to the PCF. When NRF discovery is enabled, the P-CSCF registers with the NRF and queries the NRF.

Role	Service	Transport	Connected To	Purpose
AF	Npcf_PolicyAuthorization (N5)	HTTP/2	PCF	Authorize VoNR media and QoS. Create an app-session.
NF (AF)	Nnrf_NFManagement	HTTP/2	NRF	Register the P-CSCF as an AF instance (optional)
NF (AF)	Nnrf_NFDiscovery	HTTP/2	NRF → BSF	Discover the PCF bound to a UE PDU session (optional)

SBI in the IMS Architecture



For VoNR, the P-CSCF detects 5G access. The P-CSCF discovers the serving PCF through the NRF→BSF chain. The P-CSCF then POSTs a policy-authorization app-session to that PCF. This app-session reserves the voice bearer QoS.

N5 - Npcf_PolicyAuthorization (P-CSCF → PCF)

The **N5** reference point carries the `Npcf_PolicyAuthorization` service. On a VoNR call, the P-CSCF creates an *app-session* resource on the PCF. The app-session describes the media that the session needs. The PCF then installs the correct QoS on the UE 5G PDU session.

App-session request

The P-CSCF POSTs an `ascReqData` object to the PCF app-sessions collection. The default collection is `http://<pcf>/npcf-policyauthorization/v1/app-sessions`. The object contains these fields:

Field	Value	Notes
<code>notifUri</code>	AF notification URI	The address where the PCF sends app-session event notifications. This is the configured AF notification endpoint.
<code>suppFeat</code>	<code>3f</code>	Supported-features bitmap
<code>ueIpv4 / ueIpv6</code>	UE source IP	Must match the address family that the PCF bound to the SMF PDU session
<code>afAppId</code>	<code>VoNR</code>	Application identifier
<code>medComponents</code>	audio media component	<code>mediaType: AUDIO</code> , <code>fStatus: ENABLED</code> , with a flow description (<code>permit out 17 from <ue-ip> to any</code>)

Operational gotcha - address family. The PCF binds the app-session to the SMF PDU session by the UE IP address. You must encode a UE on an IPv6 PDU session as `ueIpv6`. A v6 address in `ueIpv4` never matches. A v4 address in `ueIpv6` never matches. In these cases the PCF rejects the authorization or drops the authorization silently. The P-CSCF selects `ueIpv6` or `ueIpv4` from the SIP source address automatically.

Lifecycle

- **Create** - the P-CSCF POSTs the app-session when it processes the VoNR INVITE or early media.
- **Notify** - the PCF calls back to `notifUri` for session events.
- **Delete** - the P-CSCF tears down the app-session when the dialog ends. This releases the reserved QoS.

Diameter Rx uses `Rx_AAR` and `Rx_STR`. N5 has no persistent peer connection. Each app-session is an independent HTTP/2 transaction to the PCF discovered for that UE.

Nnrf - NF Management and Discovery (P-CSCF ↔ NRF)

The P-CSCF uses NRF discovery to find the PCF for every VoNR session. NRF discovery is the only PCF discovery path.

NF registration (Nnrf_NFManagement)

The P-CSCF registers itself as an AF instance with the NRF. The P-CSCF uses a stable per-host instance identity. A restart reuses one registration. This prevents the NRF from accumulating stale AF registrations.

PCF discovery (Nnrf_NFDiscovery)

For a VoNR session, the P-CSCF queries the NRF with the UE source IP. This query discovers the PCF that serves that UE PDU session. The **NRF → BSF** chain resolves the query. The BSF holds the UE-IP to serving-PCF binding. The discovered endpoint becomes the N5 target. If the P-CSCF finds no binding, it skips dynamic QoS for that call. The session then proceeds without a dedicated bearer reservation.

When SBI is Used vs Diameter

The P-CSCF derives the access type from the `P-Access-Network-Info` header (per TS 24.229 §5.2.6.3). LTE reports `3GPP-E-UTRAN`. 5G NR reports `3GPP-NR`. The P-CSCF excludes WiFi (`3GPP-IEEE-802.11`) because WiFi has no dedicated bearers.

Access	P-Access- Network-Info	QoS path	Peer
5G NR (VoNR)	3GPP-NR	N5 SBI (Npcf_PolicyAuthorization)	PCF
LTE (VoLTE)	3GPP-E-UTRAN	Diameter Rx	PCRF
WiFi	3GPP-IEEE- 802.11	none (no dedicated bearer)	-

The P-CSCF discovers the PCF for the N5 path per session. It uses the NRF → BSF → serving-PCF chain.

Configuration

The deployment tooling provisions the SBI behaviour per deployment. Do not edit the SBI behaviour by hand. The relevant settings are:

Setting	Purpose
AF notification endpoint	The callback URL that the P-CSCF advertises to the PCF for app-session event notifications
NRF endpoint	The NRF address for AF registration and PCF discovery
Home PLMN identity (MCC / MNC)	The home-network identity that the P-CSCF presents to the NRF
AF instance identity	A stable per-host identity for NRF registration. A restart reuses a single registration.

OmniWeb shows the live NRF registration state. OmniWeb also shows the PCF bindings discovered per session. See below.

Management via OmniWeb

Omnitouch removed the built-in web control panel. The **NRF** tab of the OmniWeb P-CSCF page shows the NRF registration state, the discovered PCF bindings, and the 5G/N5 status. See the [OmniWeb documentation](#).

Common Issues

Symptom	Likely cause	Action
No PCF binding found for the UE (logged at call setup)	The NRF or BSF has no binding for the UE PDU session yet. Or the UE IP differs from the session anchor.	Confirm the UE PDU session is established. Confirm the BSF holds the binding. The call proceeds without dynamic QoS.
PCF rejects or ignores the app-session	The UE IP is encoded in the wrong family (ueIpv4 vs ueIpv6)	Verify the SIP source address family matches the PDU session. See the address-family gotcha above.
Stale AF registrations accumulate on the NRF	The AF instance identity is not stable across restarts	Make the per-host AF instance identity stable
No N5 traffic at all for a 5G call	The P-CSCF does not detect the access as 3GPP-NR. Or the NRF is unreachable, so the P-CSCF discovers no PCF.	Check P-Access-Network-Info. Verify the NRF endpoint is reachable.
VoNR call sets up but no dedicated bearer	The P-CSCF did not create the app-session because discovery failed. Or the P-CSCF tore down the app-session early.	Correlate the P-CSCF N5 POST with the PCF. Check HTTP/2 connectivity and timeouts.

Related Documentation

- [Diameter Operations](#) - the Rx, Cx, and Ro Diameter interfaces used for VoLTE (4G/LTE)
- [P-CSCF Operations](#) - VoNR access detection, N5 QoS, and NRF discovery in context
- [Metrics Reference](#) - P-CSCF metrics
- [OmniWeb documentation](#) - NRF and 5G status in the management portal

S-CSCF Operations & Reference

The Serving-CSCF is the home-network SIP registrar and session-control point of the IMS. It authenticates subscribers against the HSS over Cx (MAR/SAR). It stores the registration binding. It downloads the subscriber's service profile (Initial Filter Criteria). It sits in the signalling path for every originating and terminating session. From this position it triggers Application Servers over the ISC interface, asserts the caller's identity, and routes the session toward the terminating side, an Application Server, or the PSTN. The HSS records this S-CSCF's name for the subscriber. Therefore, all subsequent traffic for that user traverses this node.

IMS Functions

Registration & authentication

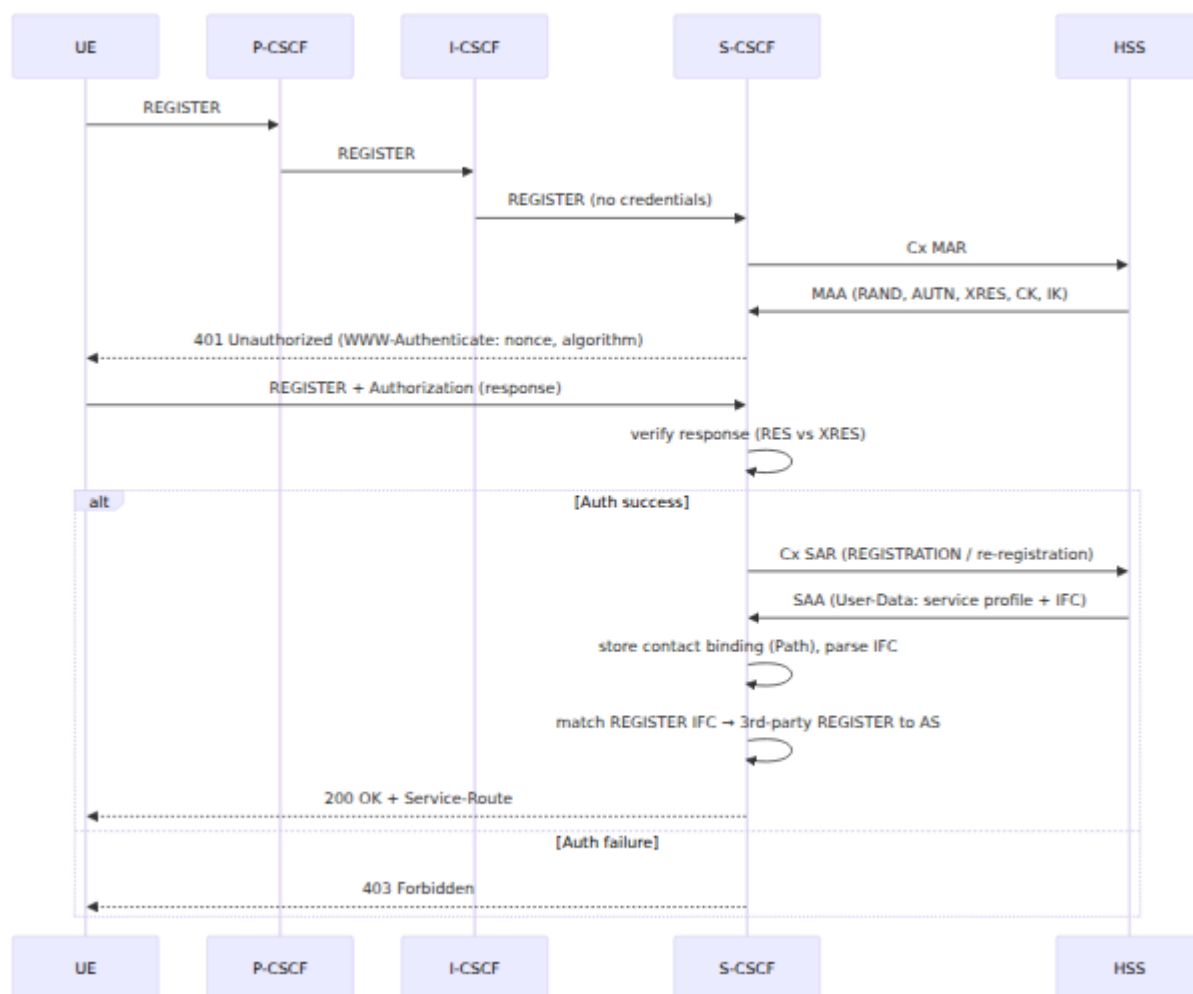
The S-CSCF is the authoritative registrar. It challenges the UE. It validates the response against a Cx authentication vector from the HSS. On success it records the contact binding and downloads the subscriber's service profile.

Registration proceeds as:

1. **Algorithm selection.** The S-CSCF challenges with the algorithm the UE offers in its Authorization header. If the UE offers no algorithm, the S-CSCF defaults to SIP Digest (MD5). SIP Digest accommodates non-IMS softphones. By default the S-CSCF authenticates every REGISTER.
2. **Challenge (MAR).** The S-CSCF receives an un-credentialed REGISTER. It requests an authentication vector from the HSS with a Cx Multimedia-Auth-Request. The HSS returns the vector in the answer (for AKA: RAND, AUTN, XRES, CK, IK). The S-CSCF replies **401 Unauthorized** with a `WWW-Authenticate` header. This header carries the nonce (derived from RAND) and the selected algorithm. If the HSS rejects the identity, the registration

fails **403**. If the HSS is unavailable or returns a malformed answer, the registration fails **503**.

3. **Verification.** The UE re-sends REGISTER with its computed response. The S-CSCF checks the response against the stored vector. It matches on the public identity.
4. **Re-sync.** If the UE reports a sequence-number (SQN) mismatch, the S-CSCF forwards the AUTS token to the HSS to resynchronise. Then the S-CSCF re-challenges with fresh vectors.
5. **Server assignment (SAR).** After successful authentication the S-CSCF sends a Cx Server-Assignment-Request. The assignment type is REGISTRATION on first registration, or re-registration on a refresh. The answer returns the subscriber's User-Data (service profile and IFC). The S-CSCF holds the User-Data in memory. A rejected assignment, or a subscriber with no IMS service profile, fails **403**. An HSS timeout fails **503**.
6. **Binding & Service-Route.** The S-CSCF stores the contact binding together with the P-CSCF Path. The Path lets terminating requests route back through the same P-CSCF. The 200 OK carries a Service-Route, so the UE sends subsequent requests through this S-CSCF. The S-CSCF keeps one contact per public identity. A new binding replaces the previous one. The expiry is a fixed 599 seconds.
7. **Third-party register / reg-event.** The S-CSCF also evaluates registration against the REGISTER-triggered Initial Filter Criteria. This evaluation fires third-party REGISTERs to any matching Application Servers. The registration-event package notifies subscribed entities of the registration state. The S-CSCF tears down the subscription on de-registration.



Service triggering via IFC (ISC)

The S-CSCF evaluates every initial request against the subscriber's downloaded **Initial Filter Criteria**. Each IFC has a prioritised Trigger Point, an Application Server address, and a Default Handling value. The Trigger Point is a boolean combination of Service Point Triggers (method, Request-URI, SIP header, Session Case, SDP). The Default Handling value is session-continued, or session-terminated on AS failure. The Trigger Point uses conjunctive or disjunctive normal form. You can group and negate the individual triggers.

The S-CSCF walks the profile in priority order for the relevant session case. On a match it forwards the request to the Application Server over ISC. The S-CSCF marks the request with an **Original Dialog Identifier (ODI)**. It also inserts a **P-Served-User** header (RFC 5502) that identifies the served subscriber and session case. These marks let the AS return the request to the point in the chain it left. When the AS routes the request back, the S-CSCF recognises the

ODI. Then it resumes IFC evaluation after the last-matched criterion instead of restarting.

Default Handling governs AS-failure behaviour. The Application Server returns a 408 or 5xx. The S-CSCF then continues to the next criterion (session-continued) or abandons the leg, as the IFC specifies.

Originating call handling

A request is **originating** when it arrives with the originating indicator in its top Route header, or when it returns from an originating Application Server. The S-CSCF then:

- Assigns the originating dialog context and record-routes, so it recognises in-dialog requests as the originating leg.
- **Asserts identity.** The request does not return from an AS. The S-CSCF removes any client-supplied `P-Asserted-Identity`. It replaces the identity with the identity that it authenticated at registration. This is the authenticated calling-line identity for the leg.
- Evaluates the originating IFC and forwards matches to the Application Server over ISC.
- **Number normalisation.** A Request-URI carries a `phone-context`. The S-CSCF rewrites the Request-URI to a `tel:` URI in the home network's phone-context before routing.
- **PSTN / ENUM.** For E.164 destinations the S-CSCF resolves the number by ENUM. On an ENUM miss the S-CSCF sends the call to the PSTN breakout gateways, with failover across the gateway set. If the request carries a roaming Transit-and-Roaming Function indication (`Feature-Caps: +g.3gpp.trf`), the S-CSCF routes it to that TRF instead.
- **Charging vector.** Originating calls carry a `P-Charging-Vector` for inter-operator charging correlation.
- If online charging is enabled, the S-CSCF sends a credit-control request before the call proceeds (see Charging).

The S-CSCF relays non-PSTN destinations toward the terminating side. If this same S-CSCF serves the terminating user, terminating handling continues locally.

Parse error on line 15: ...eturned; resume IFC) end opt On -----^
Expecting 'SOLID_OPEN_ARROW', 'DOTTED_OPEN_ARROW', 'SOLID_ARROW',
'BIDIRECTIONAL_SOLID_ARROW', 'DOTTED_ARROW',
'BIDIRECTIONAL_DOTTED_ARROW', 'SOLID_CROSS', 'DOTTED_CROSS',
'SOLID_POINT', 'DOTTED_POINT', got 'NEWLINE'

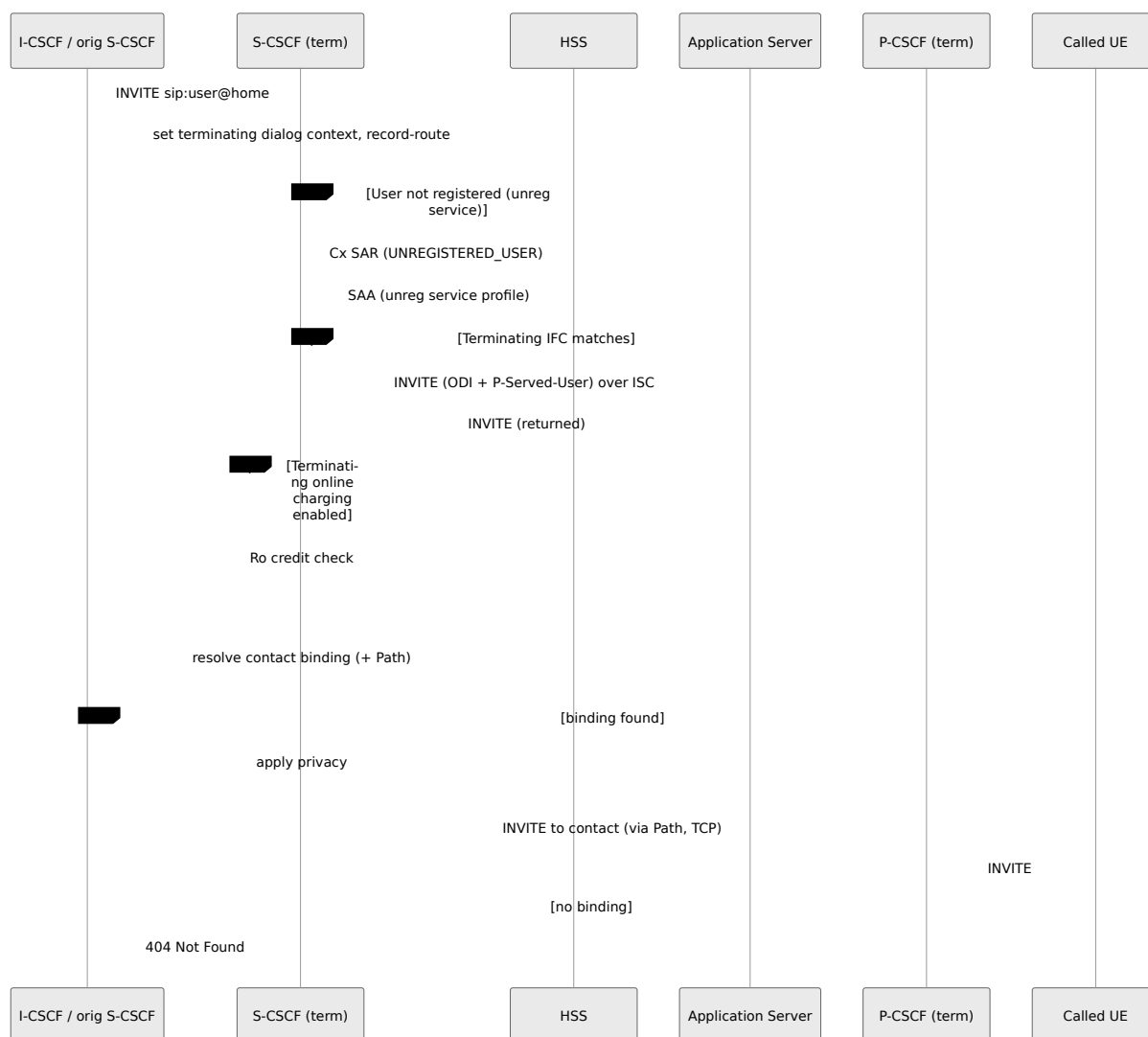
Try again

Terminating call handling

A request is **terminating** when its Request-URI is a locally-served identity. The S-CSCF then:

1. Assigns the terminating dialog context and record-routes, so it recognises in-dialog requests as the terminating leg.
2. Restores the original Request-URI. For non-INVITE methods it evaluates the terminating IFC and forwards matches to the Application Server over ISC. For INVITEs, IFC forwarding follows the AS return cycle.
3. If terminating online charging is enabled, the S-CSCF sends a terminating-side credit-control request before it proceeds.
4. **Location resolution.** The S-CSCF retrieves the served user's contact binding. It relays the request to that contact via the P-CSCF recorded in the Path at registration. If the user has no binding, the S-CSCF returns a **404 Not Found**.
5. The S-CSCF receives an INVITE to an identity that is **not currently registered**. First it fetches the unregistered service profile from the HSS with a Cx Server-Assignment-Request of type UNREGISTERED_USER. This lets terminating-unregistered services run (for example, voicemail). An HSS timeout fails **503**. A missing profile fails **403**.

The S-CSCF applies privacy on egress. If the request asserts `Privacy: id`, the S-CSCF removes the `P-Asserted-Identity` before the message leaves the S-CSCF.



Charging (optional)

Online charging over Diameter **Ro** to an OCS is optional. You enable it per deployment (see the charging flags below). When enabled, the S-CSCF sends a credit-control request before it allows an INVITE. The S-CSCF maps the answer to SIP responses (for example, insufficient funds → 402, credit-limit reached → 486, unknown charging subscriber → 403). The Service-Context-Id identifies the charged service. The S-CSCF assembles this identifier from the charging parameters listed in the configuration reference.

In production this is normally **disabled**. The TAS performs charging instead. The TAS correctly accounts for supplementary services (forwarding, transfer, roaming legs) that the S-CSCF cannot observe end-to-end. Treat S-CSCF Ro charging as an optional capability, not a default.

Presence / reg-event

The S-CSCF does not act as a general presence server. The S-CSCF accepts registration-event (Event: reg) SUBSCRIBE requests (200 OK). The S-CSCF does not serve general presence subscriptions. The S-CSCF accepts a registration-event PUBLISH only from a registered user. Such a PUBLISH updates the published registration state. Otherwise the S-CSCF rejects it **403**. This configuration has no user-availability (PIDF) presence handling.

Deployment Configuration (Ansible-injected)

Ansible renders the S-CSCF's runtime configuration and its Diameter peer table (scscf.xml) at deploy time. The values below derive from the network's PLMN identity (MCC/MNC) and the node's inventory hostname.

Identity / realm

Name	What it controls	Value / derivation
NETWORKNAME	Home IMS domain. It is the Cx destination realm and the phone-context used in number normalisation	ims.mnc<mnc>.mcc<mcc>.3gppnetwork.
HOSTNAME	This node's FQDN (host alias, and Diameter origin-host when Ro is enabled)	<inventory_hostname>.ims.mnc<mnc>.
URI	The S-CSCF's own SIP URI. It is the registrar and authentication identity	sip:<hostname>:5060
SCSCF_USER_AGENT	The User-Agent header that the node emits	User-Agent: Omnitouch S-CSCF <inventory_hostname>
ISC_MY_URI	Host token that identifies	<inventory_hostname>

Name	What it controls	Value / derivation
	this S-CSCF's own ODI routes when an AS returns a request	
ENUM_SUFFIX	ENUM domain suffix for E.164→URI resolution of originating PSTN-bound numbers	mnc<mnc>.mcc<mcc>.3gppnetwork.org.

Ansible templates the SIP listen sockets (UDP/TCP 5060, TLS 9090) and host aliases from the inventory host address and PLMN.

Authentication - REG_AUTH_DEFAULT_ALG

The default authentication algorithm that the S-CSCF applies when it must choose one, rather than echo the algorithm the UE requests. Options:

Value	Meaning / when to use
AKAv1-MD5	3GPP IMS-AKA (TS 33.203). Standard for USIM/ISIM VoLTE/VoNR with IPsec SAs. Use for normal mobile subscribers.
AKAv2-MD5	Enhanced IMS-AKA variant. Use only where UEs and HSS specifically negotiate AKAv2.
MD5	Plain SIP HTTP Digest (no AKA, no IPsec). Use for non-IMS / softphone clients that cannot do AKA.
CableLabs-Digest	PacketCable/CableLabs digest profile. Cable-network deployments.
3GPP-Digest	3GPP SIP Digest (TS 33.203 Annex N). Password-based, no ISIM. Fixed-line / non-UICC subscribers.
TISPAN-HTTP_DIGEST_MD5	ETSI TISPAN NASS/HTTP-Digest profile. TISPAN fixed-broadband subscribers.
HSS-Selected	Default. The S-CSCF imposes no algorithm. The HSS returns the per-subscriber scheme in the auth answer. Use this so the S-CSCF challenges each subscriber with whatever the HSS provisioned (AKA for mobiles, Digest for fixed, etc.).

The algorithm does not change the following defaults. The S-CSCF authenticates every REGISTER by default (see `WITH_AUTH`). The Cx destination realm is the home network domain (`NETWORKNAME`). The S-CSCF matches auth vectors on the public identity. Vectors expire after 599 s.

Charging (Ro) - flags and peer

Name	What it controls	Values
WITH_RO	Enable originating Diameter Ro credit-control before an outgoing INVITE	define / undef (default: undef)
WITH_RO_TERM	Enable terminating-side Diameter Ro credit-control	define / undef (default: undef)
RO_DESTINATION	OCS Diameter destination host (destination realm is the home network domain)	OCS FQDN, e.g. <code>hssocs.voiceblue.com</code>
RO_FORCED_PEER	Pin credit-control routing to a specific Diameter peer. This bypasses realm routing	peer id (e.g. <code>32260@3gpp.org</code>); off by default
RO_ROOT	Service-Context-Id root	<code>32260@3gpp.org</code>
RO_EXT	Service-Context-Id extension	<code>ext</code>
RO_MNC	MNC component of Service-Context-Id	e.g. <code>07</code>
RO_MCC	MCC component of Service-Context-Id	e.g. <code>262</code>
RO_RELEASE	3GPP release for Service-Context-Id	e.g. <code>8</code>

Feature flags (`WITH_*`)

Flag	Effect when defined
<code>WITH_AUTH</code>	Authenticate every REGISTER (not just Digest/MD5 clients). Enabled by default in the template.
<code>WITH_RO</code>	Enable originating online charging via Diameter Ro.
<code>WITH_RO_TERM</code>	Enable terminating online charging via Diameter Ro.

Ansible templates `CAPTURE_NODE` (the Homer capture target) only when Homer capture is enabled for the deployment. `CAPTURE_NODE` duplicates SIP signalling to Homer for tracing.

Diameter peer configuration

The S-CSCF's Diameter peer table (`scscf.xml`) advertises the **Cx** application (`16777216`) toward the HSS plus base accounting. The file structure and the Ansible variables that fill it are shared across all CSCFs. See [Diameter → Peer Configuration \(Deployment\)](#). When Ro charging is enabled, `RO_DESTINATION` addresses the OCS peer rather than the XML.

Troubleshooting

Registration failures

Symptoms: Users unable to register, registration timeouts, 4xx/5xx on REGISTER.

- **HSS connectivity (Cx)** - the S-CSCF depends on the HSS to answer the Cx MAR (auth vector) and SAR (service profile). If MAR/SAR time out or return malformed answers, the registration fails **503**. Verify that the Cx peer to the HSS is up and responds. See [Diameter Operations](#).
- **Authentication failures** - confirm that the subscriber's credentials are provisioned in the HSS and that the HSS generated the auth vector

(MAR/MAA). Verify that the challenge algorithm is one the UE supports (AKA/Milenage for USIM/ISIM, Digest for non-IMS clients). A rejected identity fails **403**.

- **S-CSCF assignment / capacity** - a subscriber with no IMS service profile, or a rejected server assignment (SAR), fails **403**. Confirm that the S-CSCF's capabilities match what the I-CSCF selected on. Also confirm that the node has registration capacity.

Call setup failures

Symptoms: Calls fail to establish, 4xx/5xx SIP errors.

- **User not registered** - verify that both the originating and terminating identities are IMS-registered. A terminating INVITE to an identity with no contact binding returns **404**. For an unregistered terminating identity with provisioned services, the S-CSCF fetches the unregistered profile (Cx SAR UNREGISTERED_USER). An HSS timeout here fails **503**.
- **IFC / service triggering** - verify that the S-CSCF downloaded the IFC from the HSS (SAR/SAA) and that the trigger points match the session case. Check that any Application Server invoked over ISC (OmniTAS, OmniMessage) is reachable. Default Handling governs whether an AS failure continues the leg or abandons it.
- **QoS** - the P-CSCF authorises media QoS for the call (Rx to the PCRF for VoLTE, N5 to the PCF for VoNR). If calls connect but have no media path, check the policy leg on the P-CSCF.
- **Routing** - for E.164 destinations verify ENUM resolution and PSTN-gateway failover. Verify roaming/off-net routing for calls that leave the home network.

SMS delivery issues

Symptoms: SMS not delivered over IMS, or falling back to the legacy SMSC.

- **IFC triggering of OmniMessage** - verify that the subscriber's IFC triggers OmniMessage on the SIP MESSAGE method and that its priority is high enough to fire. Test IFC matching with a simulated SMS.

- **SMSC integration** - verify OmniMessage's connectivity to the SMSC (MAP/SMPP) and that the SIP MESSAGE ↔ SMS PDU conversion is intact.
- **Content type** - verify that the SIP MESSAGE carries `Content-Type: application/vnd.3gpp.sms` and the correct character-set encoding (GSM-7, UCS-2).

Call Flows

The sequence diagrams are embedded with the functions they document:

- Registration & authentication → [Registration & authentication](#)
- Originating session → [Originating call handling](#)
- Terminating session → [Terminating call handling](#)

Related Documentation

- [Operations](#)
- [Diameter](#)
- [Service-Based Interface \(SBI\)](#)
- [Metrics Reference](#)
- OmniWeb - registrations, dialogs, and Diameter peer state:
<<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>>

ANSSI R226 Interception Compliance Documentation

Document Purpose: This document gives the technical specifications required for ANSSI R226 authorization. These specifications apply under Articles R226-3 and R226-7 of the French Penal Code. They cover 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 sections below describe the interception capabilities and encryption characteristics.

1.2 Interception Capabilities

1.2.1 Registration and Session Acquisition

SIP Registration Capture:

The CSCF system processes all SIP registrations. It keeps 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 keeps 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 emergency calls and routes them:

- 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)

Calling-Identity Determination (per 3GPP TS 23.167):

The system establishes the authenticated calling-line identity presented on the emergency leg as follows:

- **Known caller (registered):** The system takes the identity from the registered IMPU. Where applicable, it also uses the cached IMEI→MSISDN binding held by the P-CSCF.
- **Unknown / anonymous caller (unauthenticated emergency, no registered identity):** The P-CSCF resolves the EPC-level identity from the PCRF over the Diameter Rx interface. It uses an asynchronous `Rx_AAR_Subscription`, bound by the UE source IP address. The system selects the identity by precedence **MSISDN → IMSI → IMEISV**. It asserts the resolved value as the **P-Asserted-Identity** on the `sos.apn` domain.

In both cases, the resulting P-Asserted-Identity is the authenticated calling-line identity presented to the PSAP and on the LI interfaces. It is a network-asserted identity, not a mere approximation.

1.2.2 Data Storage and Processing

IMPORTANT: In-Memory State Only

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

Active Registration Data (In-Memory):

The CSCF system keeps 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 keeps 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: The **TAS (Telephony Application Server - OmniTAS)** handles all call detail records, charging data, and historical call tracking. The CSCF components do not handle them.

SIP/Diameter Message Logging:

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

- **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. You can configure the log retention. The retention is typically short-term (hours to days) for debugging only.

1.2.3 Analysis Capabilities

Real-Time Monitoring:

The OmniWeb management portal

(<<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>>) 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 keep historical data. **OmniTAS (Telephony Application Server)** handles all CDR generation and long-term call tracking. For historical call records, CDRs, and communication pattern analysis, lawful interception authorities must coordinate with OmniTAS.

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:

- OmniWeb authentication and role-based access control
- BINRPC management interface (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 OmniWeb
- 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:

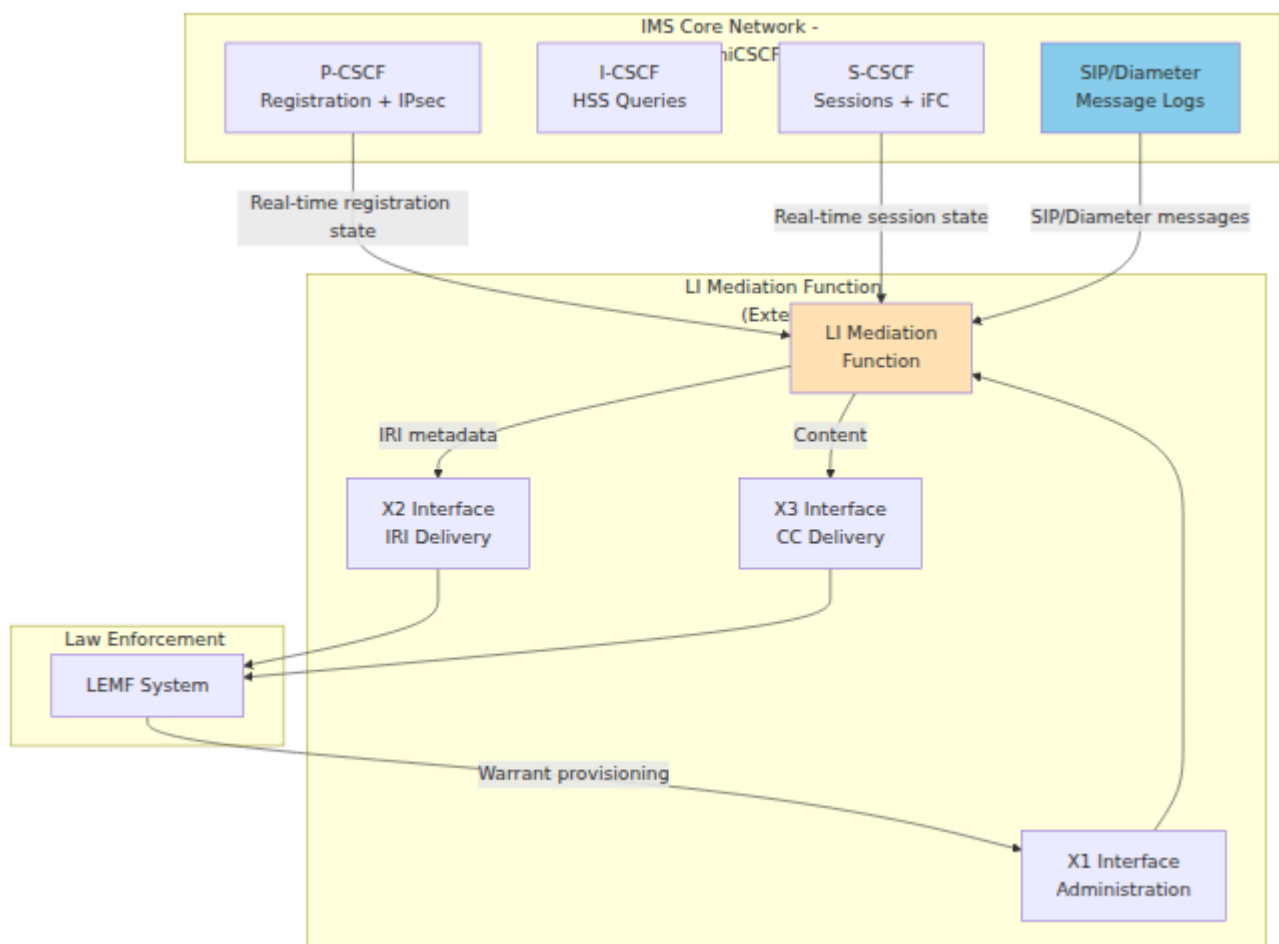
- Minimal exposed network ports (5060 SIP, 3868 Diameter, 2046 BINRPC management)
- SIP message sanity checking
- Max-Forwards loop prevention
- Rate limiting and anti-flood protection
- Message size limits
- Worker process isolation

1.4 Lawful Interception Integration Points

1.5.1 ETSI Lawful Interception Architecture

The CSCF system provides a foundation for ETSI-compliant lawful interception. The system does not build in native X1/X2/X3 interfaces. 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 keeps the warrant database (target list, external to CSCF)
 - LIMF monitors CSCF real-time state and message logs for matching sessions
 - LIMF filters on the 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). This integration captures the actual media content. The CSCF provides session setup information (SDP). This information shows 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
- OmniWeb 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:

- The P-CSCF creates the mapping when a UE registers with an IMEI (htable `emergency_imei_msisdn_map`)
- 4-hour TTL (14400s autoexpire)
- Used for emergency callback
- Replicated across P-CSCF cluster nodes

Data Retention:

- IMEI to MSISDN mappings retained for 4 hours (14400s)
- 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 several 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

The 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.

Note on emergency calling identity (Party A): For a normal (registered) call, the system derives Party A from the registered IMPU / P-Asserted-Identity. For an **unknown/anonymous emergency call**, the P-CSCF resolves Party A from the PCRF over Diameter Rx (Rx_AAR_Subscription, bound by UE source IP, precedence MSISDN → IMSI → IMEISV). The P-CSCF asserts this identity as P-Asserted-Identity on the `sos.apn` domain, per 3GPP TS 23.167. This is the authenticated calling-line identity carried on the X2/IRI interface for such calls.

1.5 Web-Based Monitoring Interface

OmniWeb provides monitoring and administrative access. OmniWeb is the unified management portal

(<<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>>). It delivers real-time monitoring and administrative access to the CSCF components:

Monitoring Capabilities:

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

Security:

- HTTPS/TLS encrypted access
 - Authentication required
 - Role-based access control (RBAC), including read-only access modes for monitoring personnel
 - Audit logging of all administrative actions
-

2. ENCRYPTION AND CRYPTANALYSIS CAPABILITIES

2.1 Cryptographic Capabilities Overview

The OmniCSCF implements several 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:

The system derives IPsec keys (CK - Cipher Key, IK - Integrity Key) 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:

You can configure the P-CSCF 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 the following:

- **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 $MAC-A = f_1(K, RAND, SQN, AMF)$
3. HSS computes $AUTN = (SQN \oplus AK) || AMF || MAC-A$
4. HSS computes $XRES = f_2(K, RAND)$
5. HSS computes $CK = f_3(K, RAND)$
6. HSS computes $IK = f_4(K, RAND)$
7. HSS sends $\{RAND, AUTN, XRES, CK, IK\}$ to S-CSCF
8. S-CSCF challenges UE with RAND and AUTN
9. UE computes $RES = f_2(K, RAND)$ 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 the following hash functions (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 the following:

- **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=0mnitouch/CN=scscf.ims.mnc001.mcc001.3gppnetv

# 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)

IMS CSCF Metrics Reference

This document is the reference for all metrics that the P-CSCF, I-CSCF, and S-CSCF components export.

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. To get full monitoring coverage, configure your Prometheus server to scrape all hosts.

Example Prometheus Configuration:

```
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 guidance on monitoring and alerting, see:

- [Monitoring via OmniWeb and Grafana](#)

Monitoring via OmniWeb and Grafana

View operational state in **OmniWeb**, the unified management portal:

<<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>>. Operational state includes registrations, dialogs, and Diameter peer status. OmniWeb embeds Grafana dashboards for real-time and historical visibility. These dashboards include S-CSCF registration and user-location views. The metrics `ims_usrloc_scscf_active_impus` and `ims_usrloc_scscf_active_contacts` back these views. The dashboards also show Diameter peer status and queue depth. The metric `cdp_queuelength` and the interface metrics `ims_icscf_uar_*`, `ims_icscf_lir_*`, `ims_auth_mar_*`, `ims_registrar_scscf_sar_*`, and `ims_qos_*` back these views.

The Prometheus metrics in this reference back those Grafana dashboards. They also back any custom alerting that you configure.

P-CSCF Metrics

CDP (Diameter) Metrics

Metric Name	Meaning
<code>cdp_average_response_time</code>	Average response time for Diameter requests in milliseconds (calculated as $\text{replies_response_time} / \text{replies_received}$)
<code>cdp_queuelength</code>	Current length of the Diameter worker queue tasks
<code>cdp_replies_received</code>	Total number of Diameter replies received
<code>cdp_replies_response_time</code>	Total time spent waiting for Diameter replies in milliseconds
<code>cdp_timeout</code>	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
<code>core_rcv_replies_3xx_bye</code>	Number of 3xx (redirection) responses to BYE requests
<code>core_rcv_replies_3xx_cancel</code>	Number of 3xx (redirection) responses to CANCEL requests
<code>core_rcv_replies_3xx_invite</code>	Number of 3xx (redirection) responses to INVITE requests
<code>core_rcv_replies_3xx_message</code>	Number of 3xx (redirection) responses to MESSAGE requests
<code>core_rcv_replies_3xx_prack</code>	Number of 3xx (redirection) responses to PRACK requests
<code>core_rcv_replies_3xx_refer</code>	Number of 3xx (redirection) responses to REFER requests
<code>core_rcv_replies_3xx_reg</code>	Number of 3xx (redirection) responses to REGISTER requests
<code>core_rcv_replies_3xx_update</code>	Number of 3xx (redirection) responses to UPDATE requests

Reply Counters by Method (4xx)

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

Reply Counters by Method (5xx)

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

Reply Counters by Method (6xx)

Metric Name	Meaning
<code>core_rcv_replies_6xx_bye</code>	Number of 6xx (global failure) responses to BYE requests
<code>core_rcv_replies_6xx_cancel</code>	Number of 6xx (global failure) responses to CANCEL requests
<code>core_rcv_replies_6xx_invite</code>	Number of 6xx (global failure) responses to INVITE requests
<code>core_rcv_replies_6xx_message</code>	Number of 6xx (global failure) responses to MESSAGE requests
<code>core_rcv_replies_6xx_prack</code>	Number of 6xx (global failure) responses to PRACK requests
<code>core_rcv_replies_6xx_refer</code>	Number of 6xx (global failure) responses to REFER requests
<code>core_rcv_replies_6xx_reg</code>	Number of 6xx (global failure) responses to REGISTER requests
<code>core_rcv_replies_6xx_update</code>	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
<code>dialog_ng_active</code>	Number of currently active (answered/confirmed) dialogs
<code>dialog_ng_early</code>	Number of early dialogs (ringing/provisional state)
<code>dialog_ng_expired</code>	Number of dialogs that have expired or been forcibly terminated
<code>dialog_ng_processed</code>	Total number of dialogs processed since startup

DNS Statistics

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

Media AAR Metrics

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

ASR Metrics

Metric Name	Meaning
<code>ims_qos_asrs</code>	Total number of ASR (Abort-Session-Request) messages received from PCRF

P-CSCF User Location

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

MySQL Database

Metric Name	Meaning
<code>mysql_driver_errors</code>	Number of MySQL driver/connection errors

Anti-Flood (IP Blocking)

Metric Name	Meaning
<code>pike_blocked_ips</code>	Number of currently blocked IP addresses (flood detection)

Registrar Module

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

Script Statistics

Metric Name	Meaning
<code>script_register_failed</code>	Number of registration attempts that failed in routing script logic
<code>script_register_success</code>	Number of successful registrations processed by routing script
<code>script_register_time</code>	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
<code>shmem_fragments</code>	Number of fragments in shared memory pool (indicates fragmentation)
<code>shmem_free_size</code>	Amount of free shared memory in bytes
<code>shmem_max_used_size</code>	Maximum shared memory used since startup in bytes
<code>shmem_real_used_size</code>	Real used shared memory including allocator overhead in bytes
<code>shmem_total_size</code>	Total shared memory pool size in bytes
<code>shmem_used_size</code>	Currently used shared memory (user data only) in bytes

SL (Stateless) Module

Stateless Reply Counters by Class

Metric Name	Meaning
<code>sl_1xx_replies</code>	Number of 1xx stateless replies sent
<code>sl_2xx_replies</code>	Number of 2xx stateless replies sent
<code>sl_3xx_replies</code>	Number of 3xx stateless replies sent
<code>sl_4xx_replies</code>	Number of 4xx stateless replies sent
<code>sl_5xx_replies</code>	Number of 5xx stateless replies sent
<code>sl_6xx_replies</code>	Number of 6xx stateless replies sent
<code>sl_xxx_replies</code>	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
<code>tcp_con_reset</code>	Number of TCP connections reset (RST received on established connection)
<code>tcp_con_timeout</code>	Number of TCP connections closed due to idle timeout
<code>tcp_connect_failed</code>	Number of failed outgoing TCP connection attempts
<code>tcp_connect_success</code>	Number of successful outgoing TCP connections
<code>tcp_current_opened_connections</code>	Number of currently opened TCP connections
<code>tcp_current_write_queue_size</code>	Current total size of TCP write queues across all connections
<code>tcp_established</code>	Total number of TCP connections established (both incoming and outgoing)
<code>tcp_local_reject</code>	Number of incoming TCP connections rejected locally
<code>tcp_passive_open</code>	Number of accepted incoming TCP connections
<code>tcp_send_timeout</code>	Number of TCP send operations that timed out (async mode)
<code>tcp_sendq_full</code>	Number of send attempts that failed because the send queue was full

TM/TMX (Transaction) Module

Transaction Type Counters

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

Transaction Completion by Status

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

Transaction Reply Statistics

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

User Location

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

I-CSCF Metrics

The I-CSCF shares most core SIP statistics with the P-CSCF. See the P-CSCF Core SIP Statistics section above. The metrics below are specific to the I-CSCF.

I-CSCF Operational Context

The I-CSCF keeps a list of available S-CSCF instances for load balancing. For a new registration, the I-CSCF queries the HSS to select the correct S-CSCF instance. The UAR and LIR metrics below track the success of these operations.

IMS I-CSCF (Cx Interface - HSS Communication)

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

UAR (User-Authorization-Request) Metrics

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

LIR (Location-Info-Request) Metrics

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

Common Metrics

The I-CSCF also exports the common metrics below. The P-CSCF section above documents these metrics.

- **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
 - **Anti-Flood** - 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 the P-CSCF Core SIP Statistics section above. The metrics below are specific to the S-CSCF.

S-CSCF Operational Context

The S-CSCF gives detailed user location information. It also manages IFC (Initial Filter Criteria).

A user location lookup shows registered IMPUs with contact bindings and service profiles. The metrics `ims_usrloc_scscf_active_contacts` and `ims_usrloc_scscf_active_impus` track the number of active contacts and IMPUs.

IFC (Initial Filter Criteria) determines which Application Servers process SIP sessions. IFC evaluation performance can change call setup times. The transaction metrics (`tmx_*`) track these times.

IMS ISC (IMS Service Control)

The IMS ISC module evaluates Initial Filter Criteria (iFC). It determines which Application Servers must process SIP sessions. These metrics track the performance and effect of iFC matching operations.

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

Performance Monitoring: Calculate the average iFC match time as $\text{ifc_match_time_total} / \text{ifc_match_attempts}$. A high average time can show complex filter criteria. It can also show a performance limit in Application Server selection. A high ratio of ifc_nomatch_count to $\text{ifc_match_attempts}$ can show incorrect trigger points. It can also show unexpected traffic patterns.

IMS Authentication (Cx Interface - MAR)

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

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

IMS Registrar S-CSCF

Registration Statistics

Metric Name	Meaning
<code>ims_registrar_scscf_accepted_regs</code>	Number of successfully accepted REGISTER requests
<code>ims_registrar_scscf_rejected_regs</code>	Number of rejected REGISTER requests
<code>ims_registrar_scscf_default_expire</code>	Default expiration time for registrations in seconds
<code>ims_registrar_scscf_default_expires_range</code>	Default expires range configuration
<code>ims_registrar_scscf_max_contacts</code>	Maximum number of contacts allowed per registration
<code>ims_registrar_scscf_max_expires</code>	Maximum expiration time allowed in seconds
<code>ims_registrar_scscf_notifies_in_q</code>	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 $\text{sar_replies_response_time} / \text{sar_replies_received}$)
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

S-CSCF User Location

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

Dialog Tracking

The S-CSCF tracks the dialog state for active calls:

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

Common Metrics

The S-CSCF also exports the common metrics below. The P-CSCF section above documents these metrics.

- **CDP (Diameter) Metrics** - Diameter protocol statistics
- **Core SIP Statistics** - Request/reply counters by method and status code (note: the S-CSCF routes between endpoints. It usually has higher fwd_requests and fwd_replies.)
- **DNS Statistics** - DNS query metrics
- **MySQL Database** - Database connection errors
- **Anti-Flood** - 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: the S-CSCF acts as both a client and a server. It usually has both UAC and UAS transactions.)

