Diameter Operations Guide

Table of Contents

Overview

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

What is Diameter?

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

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

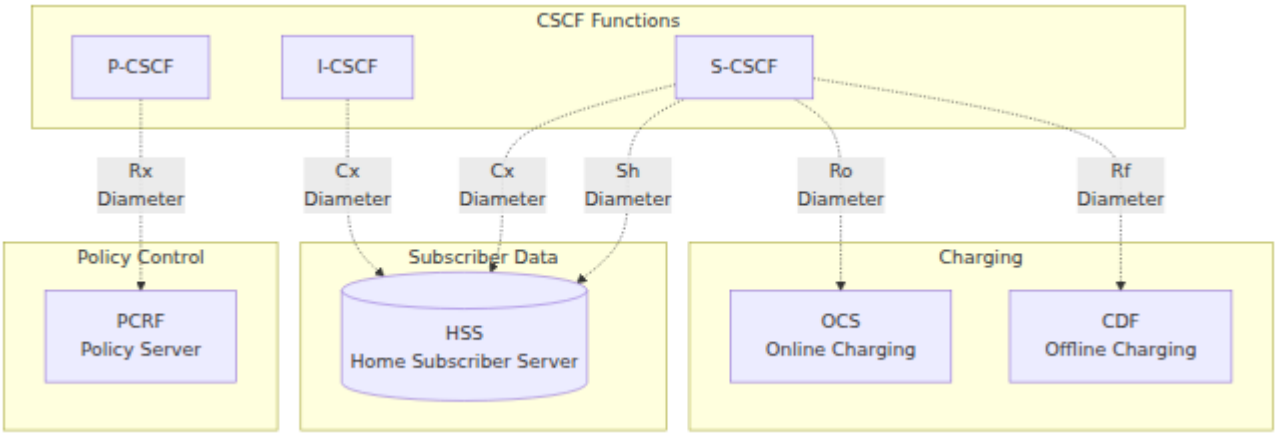
Diameter in CSCF

Each CSCF component uses specific Diameter application interfaces:

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

Diameter in IMS Architecture

Network Overview



Diameter Interfaces

Cx Interface (CSCF ↔ HSS)

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

3GPP Specification: TS 29.228

I-CSCF Operations

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

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

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

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

S-CSCF Operations

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

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

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

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

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

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

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

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

Rx Interface (P-CSCF ↔ PCRF)

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

3GPP Specification: TS 29.214

Note on VoNR (5G NR): For VoNR sessions, media and QoS are authorized over the N5 AF interface (Npcf_PolicyAuthorization, HTTP/2 SBI) to the PCF rather than Diameter Rx. The Rx interface described here therefore applies to 4G/LTE access.

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

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

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

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

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

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

Ro Interface (S-CSCF ↔ OCS)

The Ro interface provides online charging (credit control).

3GPP Specification: TS 32.299

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

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

Types:

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

Peer Management via OmniWeb

Diameter peer status, supported applications, and queue depths are now viewed on the **Diameter** tab of each CSCF page in OmniWeb, the unified management portal: <https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>.

From the OmniWeb Diameter tab you can see, 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	Connection open and operational
Closed	No connection established
Wait-Conn-Ack	Connection initiated, awaiting response
Wait-I-CEA	CER sent, awaiting CEA

Diameter Result Codes

Common result codes and their meanings:

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

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

Common Issues

Critical Diameter Interfaces

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

Interface	Impact if Down	Recovery Priority
Cx (HSS)	No new registrations, no IFC updates	Critical - immediate
Rx (PCRF)	No QoS for new calls	High - within minutes
Ro (OCS)	No prepaid charging, service may continue	High - depends on policy

---

Peer Connection Failures

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

Diagnosis:

1. Verify network connectivity:

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

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

Resolution:

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

---

CER/CEA Exchange Failures

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

Common Errors:

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

Resolution:

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

HSS Cx Interface Issues

Symptom: Registration failures, MAR/MAA timeouts

Common Errors:

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

Resolution:

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

---

PCRF Rx Interface Issues

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

Common Issues:

- **PCRF down**: Check peer status on the OmniWeb Diameter tab
- **Framed-IP-Address not recognized**: PCRF cannot map UE IP to subscriber
- **Policy not applied**: Check PCRF policy rules, verify PCEF integration

Resolution:

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

OCS Ro Interface Issues

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

Common Errors:

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

Resolution:

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

Performance Degradation

Symptom: Slow Diameter response times, high latency

Diagnosis:

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

Resolution:

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

Best Practices

Operational Guidelines

Peer Management:

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

Capacity Planning:

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

Troubleshooting:

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

Security:

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

Limitations and Future Enhancements

Current Implementation

The 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** but may be added in future versions:

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

Workarounds

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

For Detailed Statistics: Query metrics from Prometheus endpoint (see Metrics Reference for complete CDP/Diameter metric definitions and 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`, `scscf.xml` - rendered by Ansible at deploy time. It defines the node's Diameter identity and the HSS/PCRF/DRA peer(s) it connects to. The structure is identical across all three; only the advertised application differs.

XML field	What it configures	Ansible sourc
`DiameterPeerFQDN`	This node's Diameter origin-host FQDN	`<inventory_hostname>.epc.mnc<mnc>.m`
`DiameterPeerRealm`	Local Diameter realm	`ims_realm` if defined, else `epc.mnc<mnc>.mcc<mcc>.3gppnetwork.o`
`Vendor_Id` / `Product_Name`	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/port for inbound Diameter (3868)	node FQDN
`DefaultRoute`	Realm-routing default route to the HSS/PCRF peer (metric 1) or 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`

Key Ansible variables: `plmn_id.mcc` / `plmn_id.mnc_longform` (build all FQDNs/realms), `ims_realm` (override the Diameter realm), `ims_dra_support` (switch between direct-peer and DRA peering), `diameter_dra_ip` (static IP for the DRA peer), and the `hss` / `dra` inventory groups (peer and default-route lists). The S-CSCF's **Ro** peer (OCS) is addressed separately by `RO_DESTINATION` when charging is enabled, not via the XML.

These files are edited through the deployment tooling, not via 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 - the node reached when a subscriber registers and when a session terminates toward a home subscriber. It holds no session state and terminates no media. Its job is to consult the HSS over Cx to decide which Serving-CSCF should handle a given request: on registration it authorises the identity and visited network and discovers the S-CSCF (or the S-CSCF capabilities to select one); on a terminating request it locates the S-CSCF already serving the user. Having chosen an S-CSCF, it forwards the request to it and relays the responses back.

IMS Functions

Registration routing (Cx UAR)

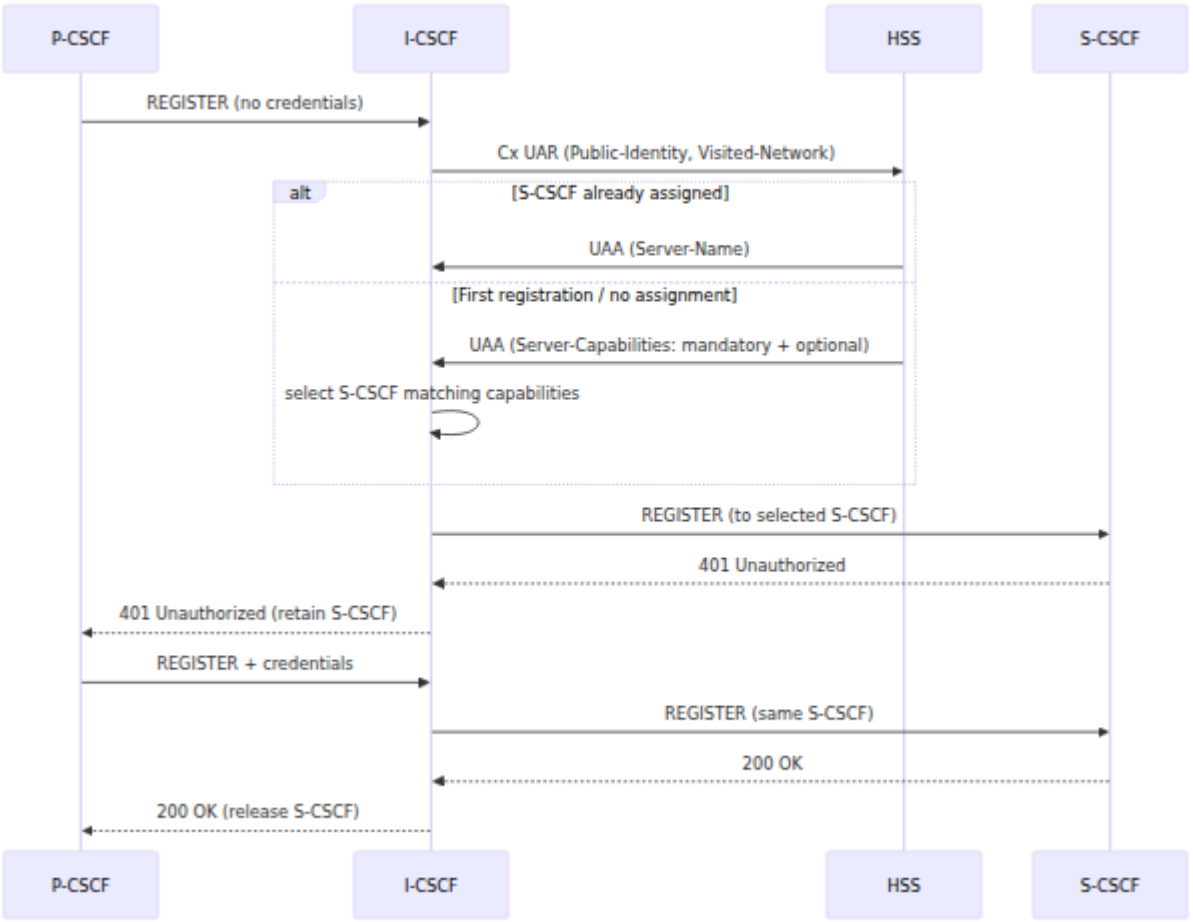
When a REGISTER arrives, the I-CSCF queries the HSS with a Cx **User-Authorization-Request (UAR)** before forwarding. The UAR carries the public identity and the visited-network identifier so the HSS can authorise the subscriber to register from that network. The answer (UAA) returns one of two things:

- **An already-assigned S-CSCF name** - used directly, so a re-registration returns to the same S-CSCF that holds the binding.
- **S-CSCF capabilities** - a set of mandatory and optional capability values that the selected S-CSCF must satisfy, returned on first registration or when no S-CSCF is currently assigned. The I-CSCF then performs capability-based selection (below).

The I-CSCF forwards the REGISTER to the chosen S-CSCF and remembers that S-CSCF for the duration of the registration handshake, so the authenticated re-REGISTER (after the 401 challenge) is routed to the **same** S-CSCF rather than

re-querying. It retains the S-CSCF while a 401 is in flight and discards it once registration completes (2xx) or finally fails.

An HSS that is unavailable or returns a malformed answer yields **503**; a UAR that authorises but for which no S-CSCF can be selected falls back to a configured default S-CSCF URI.



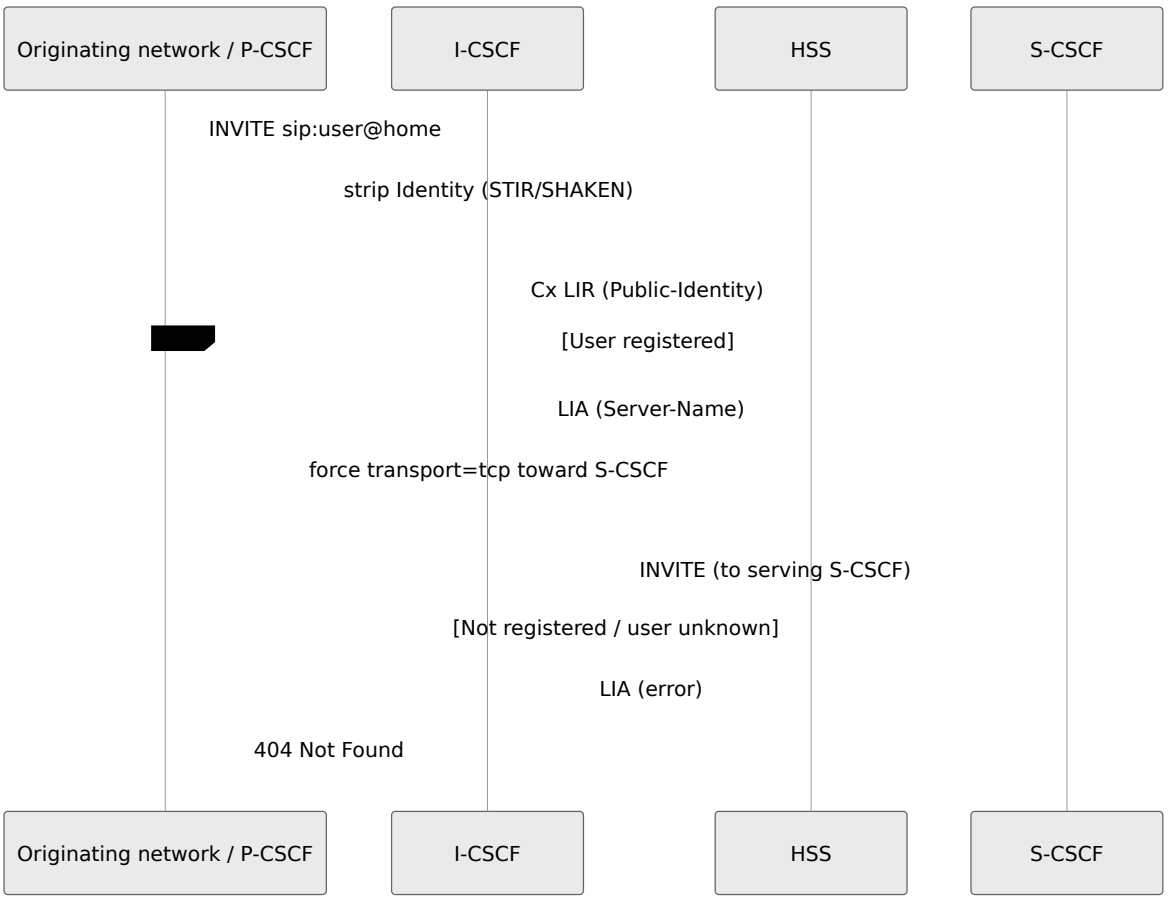
Terminating routing (Cx LIR)

On an initial terminating request (INVITE, SUBSCRIBE, MESSAGE, INFO, PUBLISH), 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 currently serving the user (or, for an unregistered user that has services provisioned, capabilities from which an S-CSCF is selected). The I-CSCF then forwards the request to that S-CSCF, forcing TCP transport toward it if the returned URI does not already specify a transport. Any inbound STIR/SHAKEN `Identity` header is stripped before forwarding.

Result handling:

- **Success** - the S-CSCF is selected and the request relayed to it; a relay failure returns **500**.
- **User not found / not registered** - returns **404 Not Found**.
- **HSS unavailable** - returns **503**.

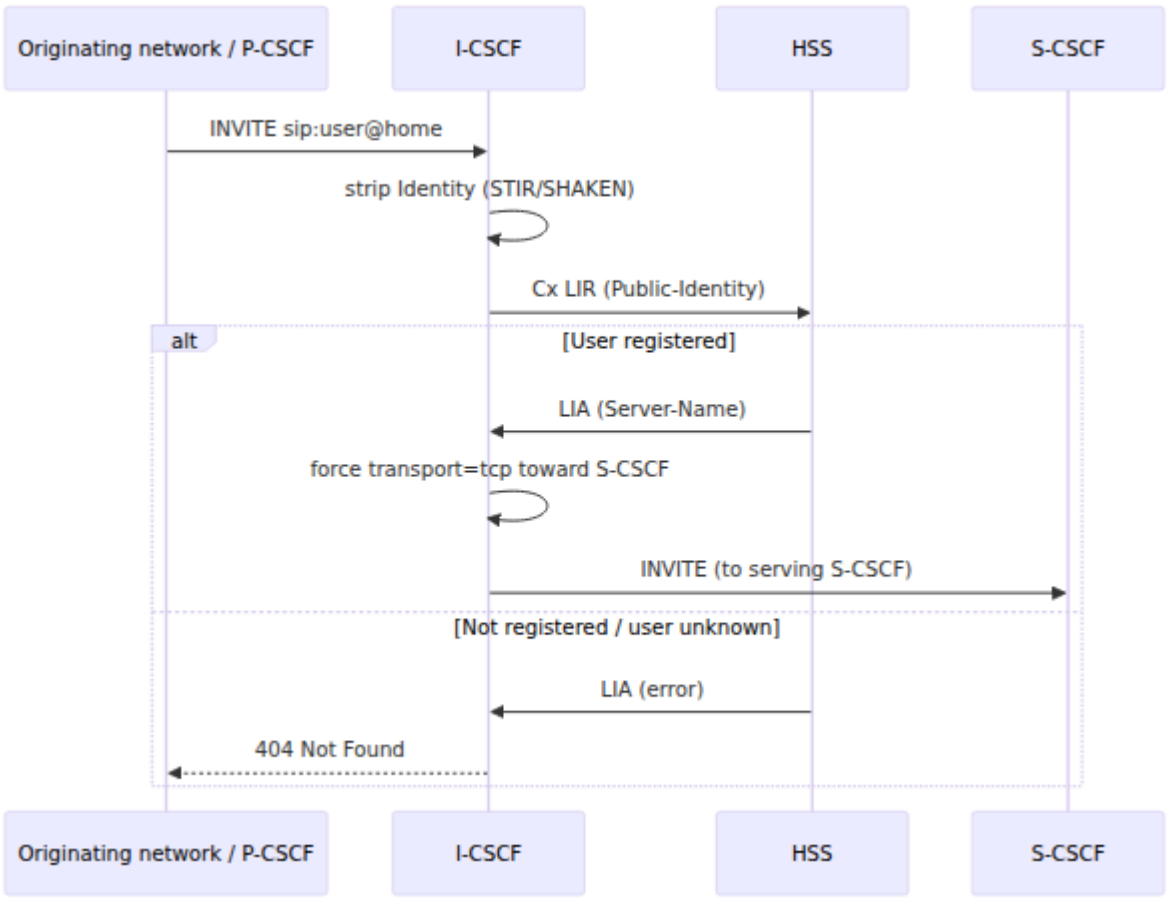
CANCEL is not interrogated; it is matched to its existing transaction and relayed. Any other (non-initial, non-REGISTER) method is rejected **406** with an `Allow` list.



S-CSCF selection / capability matching

When the HSS returns capabilities rather than an assigned S-CSCF name, 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 **all mandatory** capabilities are satisfied; among the qualifying candidates, those matching more of the **optional** capabilities are preferred. Where several candidates are equally suitable they form an ordered candidate list, which lets the I-CSCF try an alternate on failure.

The candidate list is held in transaction memory for the life of the request so its position is preserved across attempts. On a REGISTER whose forwarded leg times out or draws a 5xx/6xx, the I-CSCF advances to the next candidate S-CSCF and retries; when the list is exhausted it stops. The list is retained across a 401 challenge (the same S-CSCF must handle the authenticated retry) and dropped 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 - defined enables, commented out disables.

Identity / realm

Name	What it controls	Value / de
`NETWORKNAME`	Home IMS domain - the Cx destination realm (`cxdx_dest_realm`) and the domain checked when routing peered/unknown-user requests	`ims.mnc<mnc>.mcc<mcc>.3gppnetw`
`HOSTNAME`	This node's FQDN (host alias)	`<inventory_hostname>.ims.mnc<m`
`ICSCF_USER_AGENT`	`User-Agent` header the node emits	`User-Agent: Omnitouch I-CSCF <`
`ICSCF_SERVER`	`Server` header the node emits	`Server: Omnitouch I-CSCF <inve`
`SCSCF_URI`	Default / fallback S-CSCF URI, used when UAR-based selection yields no S-CSCF	`sip:scscf.ims.mnc<mnc>.mcc<mcc`

The SIP listen sockets (UDP/TCP 5060, TLS 9090) and host aliases (`ims.…`, `icscf.ims.…`, `<host>.ims.…`) are templated from the inventory host address and PLMN.

`CAPTURE_NODE` (the Homer capture target, `sip:<homer_host>:9060`) is templated only when Homer capture is enabled for the deployment

(`enable_homer` with a `homer` inventory group); it 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. The file structure and the Ansible variables that fill it are shared across all CSCFs - see Diameter → Peer Configuration (Deployment).

Troubleshooting

Registration or terminating-session failures that surface at the I-CSCF usually stem from one of two causes:

- **S-CSCF selection / assignment** - when the HSS returns capabilities rather than an assigned S-CSCF name, selection requires all mandatory capabilities to be satisfied. 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 it fails over to the next candidate until the list is exhausted. Confirm 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 the Cx peer to the HSS is up. See Diameter Operations.

Call Flows

The sequence diagrams are embedded with the functions 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. It establishes and enforces the access-security association that protects the UE's signalling, inserts itself into the routing path (Path on registration, record-route on sessions) so that all subsequent traffic - including terminating requests and in-dialog messages - traverses this node, detects the UE's access technology to drive media-bearer policy, and provides the emergency-session entry point (E-CSCF) with a usable calling-line identity per TS 23.167. It is a signalling proxy only: media flows directly between the UE and the terminating side and never through this node.

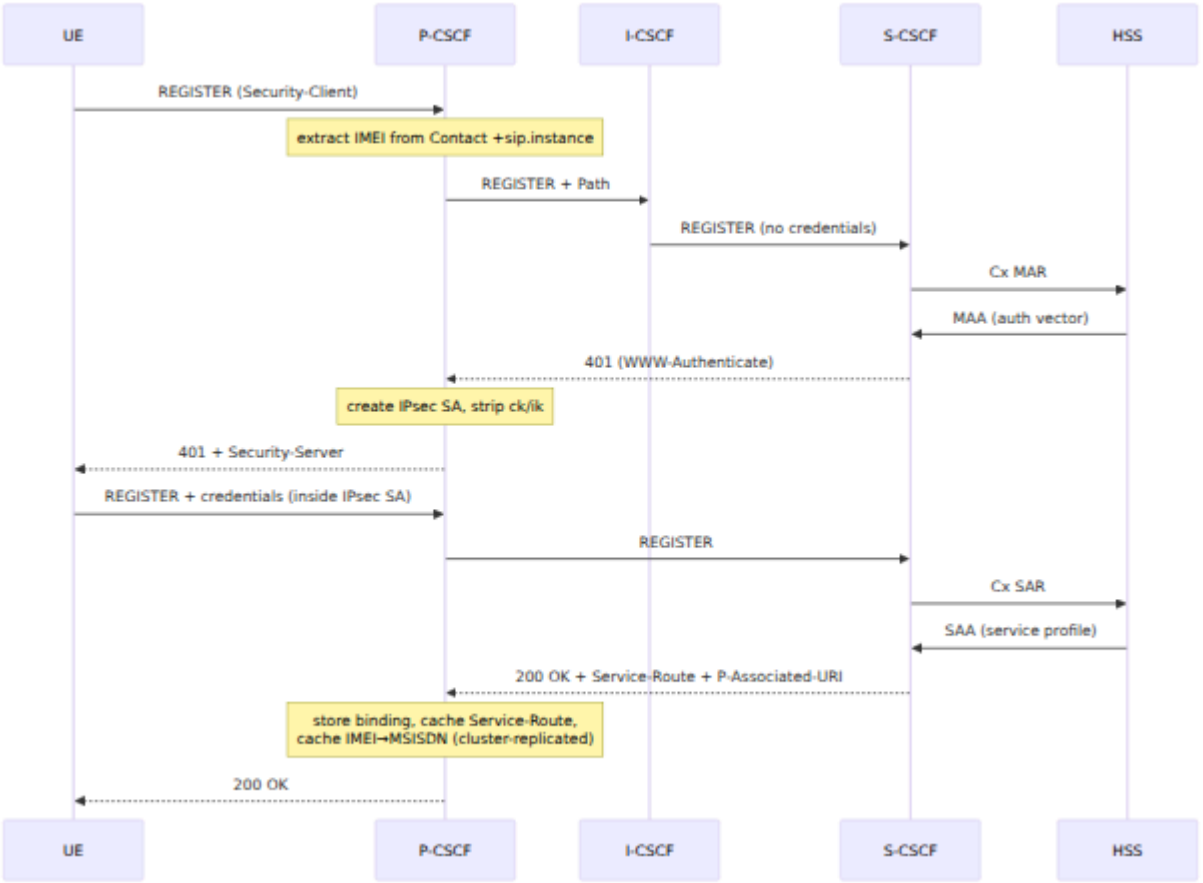
IMS Functions

Registration proxy & IPsec security association

The P-CSCF is the UE's registrar-facing proxy. It relays the REGISTER toward the home network (I-CSCF/S-CSCF), and on the challenge/response exchange it establishes an IPsec ESP security association with the UE as 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, all signalling for that UE is carried inside the SA.

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

Each registered UE consumes **one** security association drawn from a per-deployment resource pool; the SA is released when the UE de-registers (expiry 0) or its registration lapses. A REGISTER whose Contact marks an emergency (`;sos`) registration is rejected - emergency sessions are handled directly on the INVITE, not via emergency registration.



Access detection & QoS / policy control

Although it never relays media, the P-CSCF authorises the dedicated media bearer with the policy plane. It classifies the UE's 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 is excluded from dynamic QoS as it has no dedicated bearer.

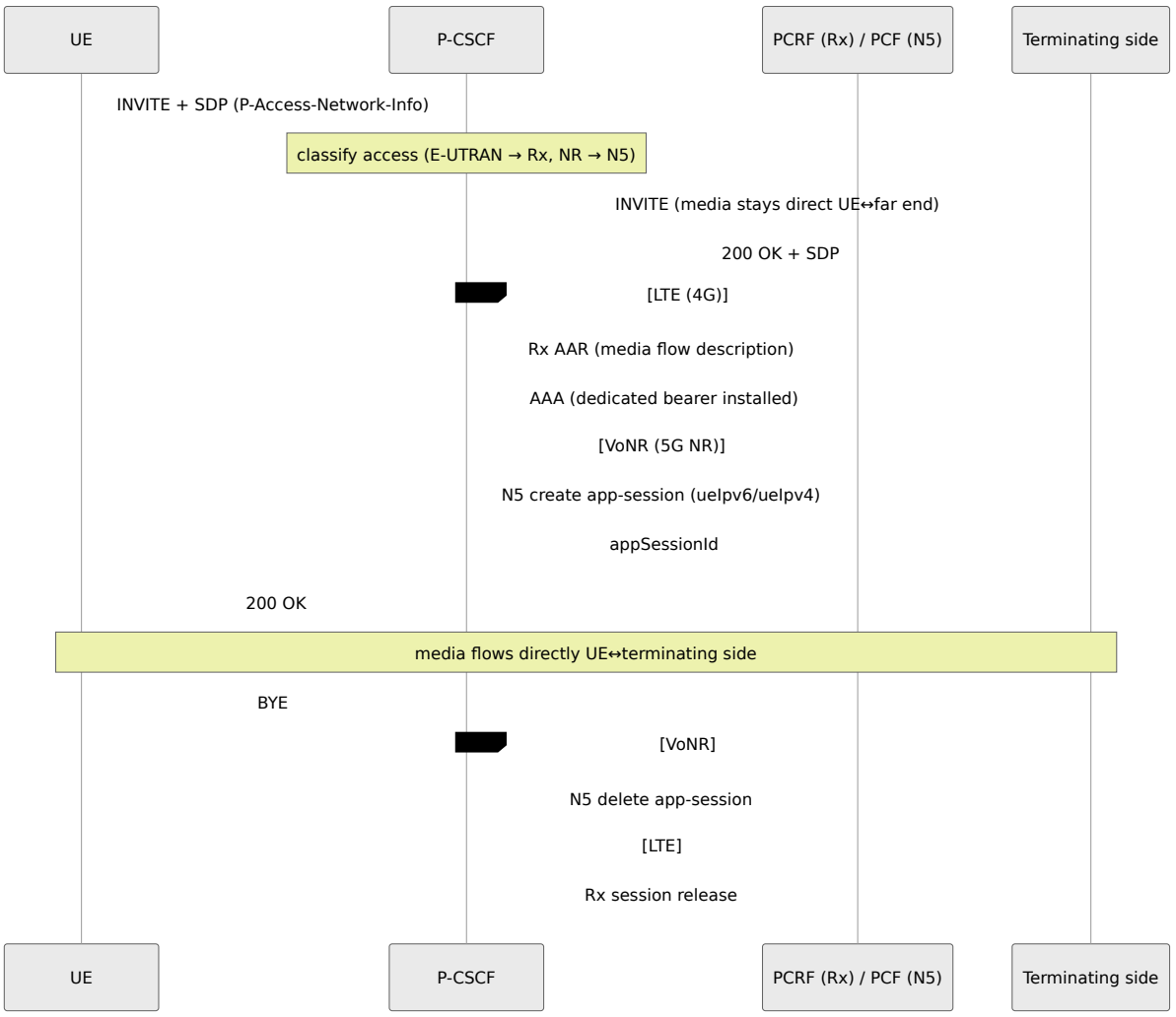
- **4G / LTE** - the media bearer QoS is authorised over **Diameter Rx** to the PCRF. On the answering leg (the `200 OK` carrying SDP) the P-CSCF issues an Authorization/Authentication Request (AAR) describing the audio (and, where present, video) media flow; the PCRF installs the corresponding

dedicated bearer. The authorisation is refreshed on in-dialog re-INVITEs and released when the dialog ends.

- **VoNR (5G NR)** - the bearer QoS is authorised over the **N5** interface to the PCF using the `Npcf_PolicyAuthorization` service. The P-CSCF acts as an Application Function: as the media is answered it creates an application session on the PCF (afAppId `VoNR`, an `AUDIO` media component with `ENABLED` flow status and a flow descriptor for the UE's media, plus an AF notification URI the PCF can call back on), and deletes that application session when the dialog ends.

The QoS authorisation runs on both the originating (MO) and terminating (MT) legs, keyed on the UE's own IP address. **UE address binding:** the UE address is encoded to match the PDU-session/bearer binding the policy node holds - an IPv6 UE is signalled as `ueIpv6` and an IPv4 UE as `ueIpv4`; a v6 address placed in the v4 field never matches the PCF's binding and no dedicated bearer is installed.

For VoNR the P-CSCF locates the serving PCF via **NRF discovery**: it registers as an AF and, for each session, resolves the PCF bound to the UE's 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. It detects an emergency session by the emergency service URN (`urn:service:sos`) on the INVITE, and routes it directly to the emergency application server (bypassing the normal registration check). Because an emergency INVITE frequently carries **no MSISDN**, the P-CSCF supplies a usable calling-line identity for the PSAP - even for callers that are unknown or anonymous - per TS 23.167 Annex K and TS 29.214 §4.4.6a.

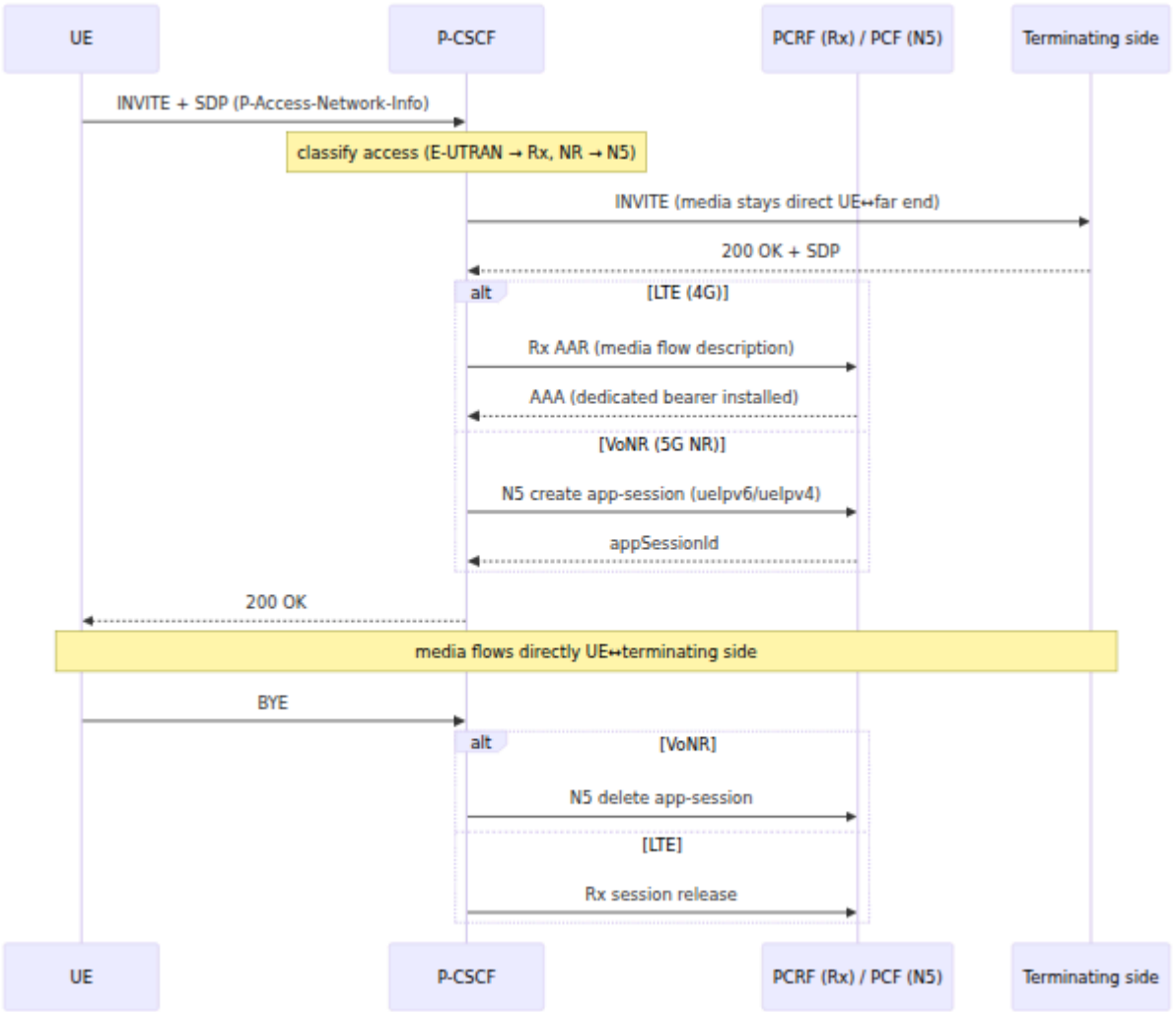
The identity is resolved by two complementary mechanisms:

1. **Cached IMEI→MSISDN binding (fast path).** On each successful REGISTER the P-CSCF caches a binding of the UE's IMEI (from the Contact `+sip.instance`) to the MSISDN (from `P-Associated-URI`). The binding is **replicated across all P-CSCF nodes**, so any node can 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 there is no cached binding, the P-CSCF issues an asynchronous Rx subscription query to the PCRF keyed on the UE's source IP address, suspending the INVITE until the answer returns. The PCRF returns the EPC-level identities, from which one is chosen by precedence **MSISDN → IMSI → IMEISV** (an IMEISV result is cached back for reuse).

The resolved identity is asserted as the caller's From URI and as a `P-Asserted-Identity` on the `sos.apn` domain, and is restored consistently on replies and in-dialog requests, so the PSAP sees a usable callback identity even for an originally anonymous caller. Whichever path resolves the identity, the emergency INVITE then receives the same media/QoS and header treatment as any other originating request before being forwarded to the emergency application server.



Security / anti-flood

The P-CSCF applies source-based flood protection: requests are rate-limited per source IP, and an IP that exceeds the sampling threshold is banned for a hold-off period. Failed registration authentication is tracked per source IP in a short-lived counter; a source that exceeds the failed-attempt threshold within the window is banned, frustrating credential-guessing. Requests that a UE addresses to the node itself, and malformed messages, are dropped. Under memory pressure the node sheds new requests with `503`.

Cluster replication

Registration-related and emergency state is replicated across P-CSCF nodes. In particular the IMEI→MSISDN emergency binding is synchronised between nodes (with a full sync on start-up), so any node in the cluster can serve terminating traffic and resolve emergency-call identity regardless of which node originally registered the UE - no per-node provisioning is required.

Deployment Configuration (Ansible-injected)

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

Identity

Name	What it controls	Value / deri
`NETWORKNAME`	Home IMS domain used in `P-Visited-Network-ID` and identity rewrites	`ims.mnc<mnc>.mcc<mcc>.3gppnetwor`
`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 / deri
`PCSCF_SERVER`	`Server` header the node emits	`Server: Omnitouch Proxy-CSCF <in`
`DMQ_NOTIFICATION_ADDR`	Cluster notification address for state replication between P-CSCF nodes	`sip:pcscf.ims.mnc<mnc>.mcc<mcc>.`

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

Rx / policy control (4G)

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

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.

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 `ansible_host`
`IMS_NRF_PLMN_MCC` / `IMS_NRF_PLMN_MNC`	PLMN advertised in NRF registration/discovery	from `plmn_id`

PCF discovery: the P-CSCF registers with the NRF as an AF and, for each VoNR session, resolves the PCF bound to that UE's PDU session via the NRF→BSF chain - so app-sessions always reach the correct per-subscriber PCF, including in 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 number of SIP (UDP) worker processes and the registrar hash-table size are tuned in the base configuration for the deployment scale; iOS UEs get a shortened TCP connection lifetime to accommodate their transport behaviour.

Diameter peer configuration

The P-CSCF's Diameter peer table (`pcscf.xml`) advertises the **Rx** application (`16777236`) toward the PCRF. The file structure and the Ansible variables that fill it are shared across all CSCFs - see Diameter → Peer Configuration (Deployment). Rx is only active when `WITH_RX` is defined.

Troubleshooting

Registration / IPsec connectivity

Users unable to register, or registration timeouts, often point to the P-CSCF's 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 that the UE and P-CSCF agreed on SA parameters and that no middlebox is stripping the security headers.
- **NAT traversal** - for devices behind NAT, verify the far-end NAT handling and that keepalive OPTIONS pings are reaching the UE, so the pinhole for terminating traffic stays open.
- **P-CSCF discovery** - verify the UE is discovering the correct P-CSCF address (via DNS, DHCP, or static configuration) and 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 the INVITE carries the expected emergency indication and that emergency routing bypasses the normal registration check.

- **CLI resolution for anonymous / unknown callers** - the caller's identity is supplied 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, keyed on the UE source IP, resolving an EPC identity by precedence **MSISDN → IMSI → IMEISV** (TS 23.167 Annex K). If the PSAP sees an anonymous caller, verify the binding was cached at registration, or that the Rx subscription query returned an identity. The cached binding map is viewable in OmniWeb.
- **Location availability** - verify location information is available for E911/E112 and that the location retrieval leg (LRF) is reachable.
- **Test routing** - emergency call routing can be exercised without an actual PSAP connection to confirm 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 / 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 are embedded with the functions they document, plus the full session ladders 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)

Originating calls are routed through the S-CSCF (via the cached Service-Route) to the TAS for service logic and charging; media stays direct.

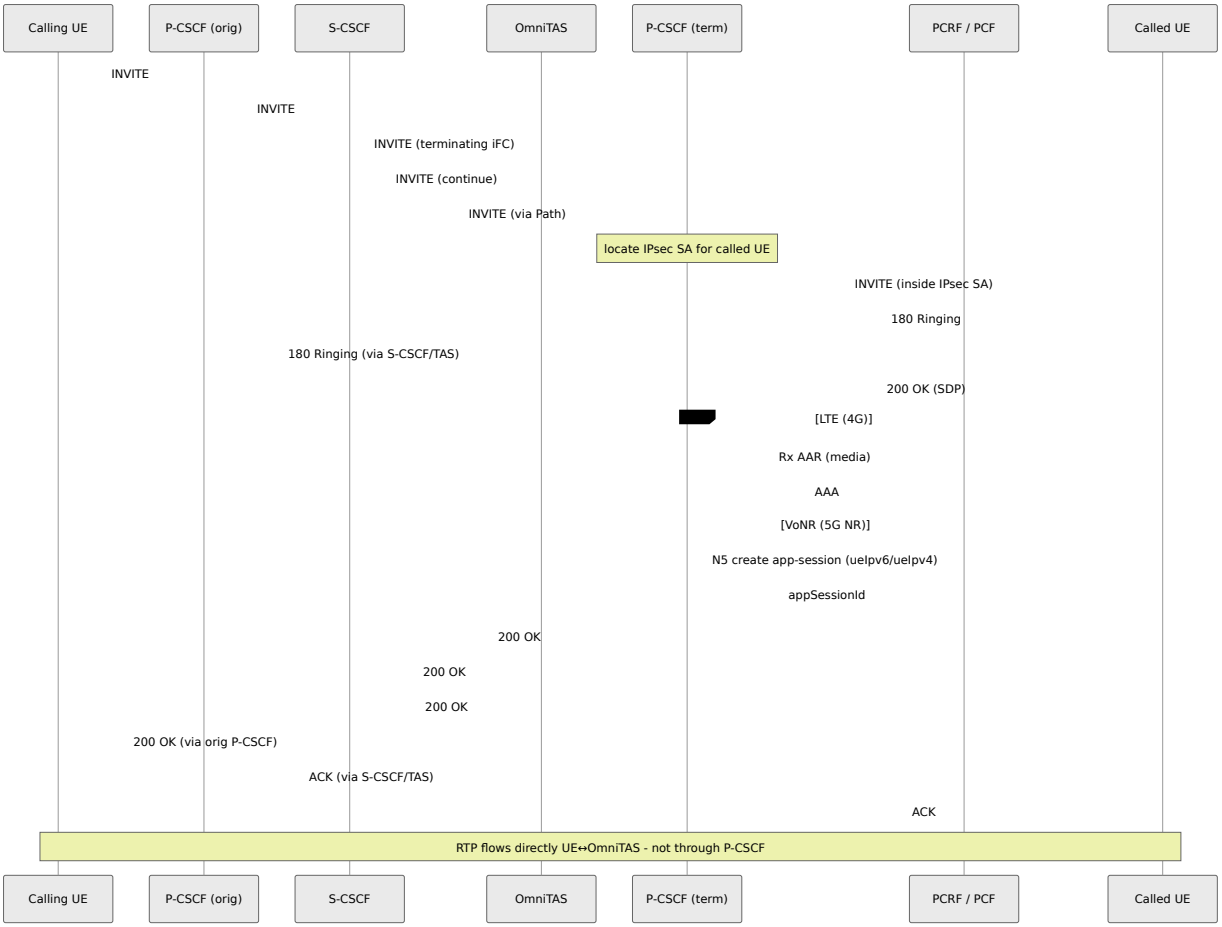
Parse error on line 10: ...-ID; classify access PCSCF->>SCSCF: ----------
--^ Expecting 'SOLID_OPEN_ARROW', 'DOTTED_OPEN_ARROW',
'SOLID_ARROW', 'BIDIRECTIONAL_SOLID_ARROW', 'DOTTED_ARROW',

'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; QoS is authorised as 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

Overview

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

This 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 several ways:

- **Transport**: HTTP/2 over TCP (vs. Diameter over TCP/SCTP)

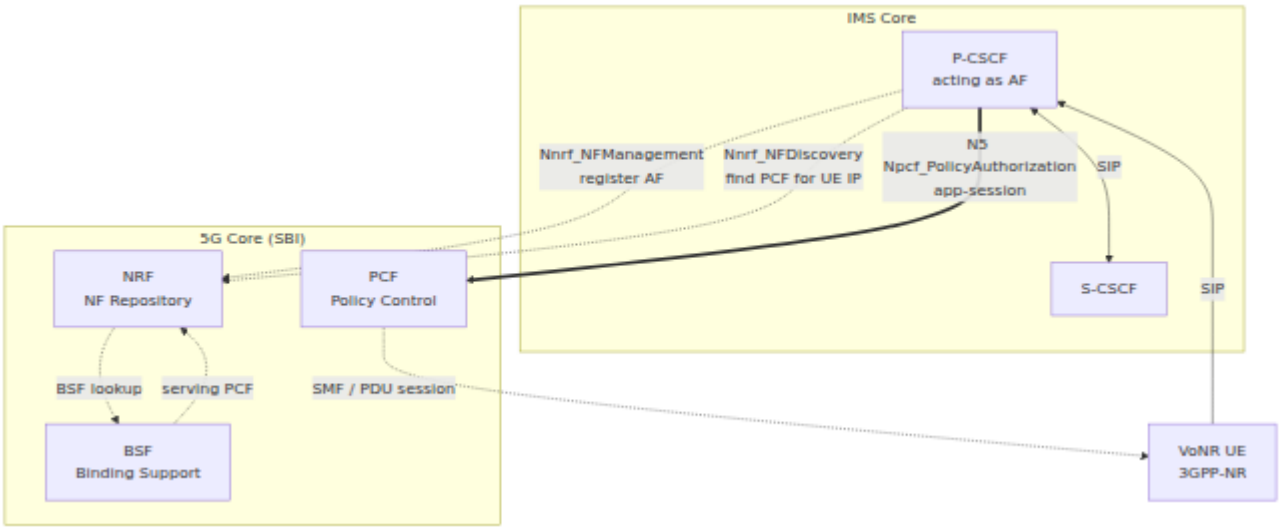
- **Encoding**: JSON payloads described by OpenAPI (vs. Diameter AVPs)
- **Model**: RESTful resources - create/modify/delete an *app-session* resource (vs. request/answer command pairs)
- **Discovery**: producers are found dynamically through the **NRF** (vs. statically configured Diameter peers)
- **Naming**: services are named `Nxxx` (e.g. `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) it authorizes VoNR media QoS over N5 to the PCF and, when NRF discovery is enabled, registers with and queries the NRF.

Role	Service	Transport	Connected To	Purpose
AF	Npcf_PolicyAuthorization (N5)	HTTP/2	PCF	Authorize VoNR media/QoS by creating 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's PDU session (optional)

SBI in the IMS Architecture



For VoNR, the P-CSCF detects 5G access, discovers the serving PCF via the NRF→BSF chain, and POSTs a policy-authorization app-session to that PCF to reserve 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, describing the media the session needs so the PCF can install the corresponding QoS on the UE's 5G PDU session.

App-session request

The P-CSCF POSTs to the PCF's app-sessions collection (default `http://<pcf>/npcf-policyauthorization/v1/app-sessions`) an `ascReqData` object containing:

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

> **Operational gotcha - address family.** The PCF binds the app-session to the SMF's PDU session by the UE IP address. A UE on an IPv6 PDU session must be encoded as `ueIpv6`; putting a v6 address in `ueIpv4` (or vice-versa) never matches, and the PCF rejects or silently drops the authorization. The P-CSCF selects `ueIpv6` vs `ueIpv4` from the SIP source address automatically.

Lifecycle

- **Create** - app-session POSTed when the VoNR INVITE / early media is processed.
- **Notify** - the PCF calls back to `notifUri` for session events.
- **Delete** - the app-session is torn down when the dialog ends, releasing the reserved QoS.

Unlike Diameter Rx (which uses `Rx_AAR`/`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)

NRF discovery is how the P-CSCF finds the PCF for every VoNR session - it is the only PCF discovery path.

NF registration (Nnrf_NFManagement)

The P-CSCF registers itself as an AF instance with the NRF, using a stable per-host instance identity so that restarts reuse one registration and the NRF does not accumulate stale AF registrations.

PCF discovery (Nnrf_NFDiscovery)

For a given VoNR session the P-CSCF queries the NRF with the UE's source IP to discover the PCF serving that UE's PDU session, resolved through the **NRF → BSF** chain (the BSF holds the UE-IP → serving-PCF binding). The discovered endpoint becomes the N5 target. If no binding is found, dynamic QoS is skipped for that call and the session proceeds without a dedicated bearer reservation.

When SBI is Used vs Diameter

Access type is derived from the `P-Access-Network-Info` header (per TS 24.229 §5.2.6.3): LTE reports `3GPP-E-UTRAN` and 5G NR reports `3GPP-NR`. WiFi (`3GPP-IEEE-802.11`) is excluded because it 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 PCF for the N5 path is discovered per session via the NRF → BSF → serving-PCF chain.

Configuration

The SBI behaviour is provisioned per deployment (through the deployment tooling, not edited by hand). The relevant settings are:

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

Live NRF registration state and the PCF bindings discovered per session are shown in OmniWeb (see below).

Management via OmniWeb

The built-in web control panel has been removed. NRF registration state, discovered PCF bindings, and 5G/N5 status are shown on the **NRF** tab of the OmniWeb P-CSCF page. See the OmniWeb documentation.

Common Issues

Symptom	Likely cause	Action
No PCF binding found for the UE (logged at call setup)	NRF/BSF has no binding for the UE's PDU session yet, or the UE IP differs from the session anchor	Confirm the UE's PDU session is established and the BSF holds the binding; the call proceeds without dynamic QoS
PCF rejects/ignores the app-session	UE IP 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	AF instance identity not stable across restarts	Ensure the per-host AF instance identity is stable
No N5 traffic at all for a 5G call	Access not detected as `3GPP-NR`, or the NRF is unreachable so no PCF is discovered	Check `P-Access-Network-Info`; verify NRF endpoint reachability
VoNR call sets up but no dedicated bearer	app-session not created (discovery failed) or torn down early	Correlate the P-CSCF N5 POST with the PCF; check HTTP/2 connectivity and timeouts

Related Documentation

- Diameter Operations - the Rx/Cx/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/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), stores the registration binding, downloads the subscriber's service profile (Initial Filter Criteria), and sits in the signalling path for every originating and terminating session so it can trigger Application Servers over the ISC interface, assert the caller's identity, and route the session toward the terminating side, an Application Server, or the PSTN. The HSS records this S-CSCF's name for the subscriber, so all subsequent traffic for that user traverses this node.

IMS Functions

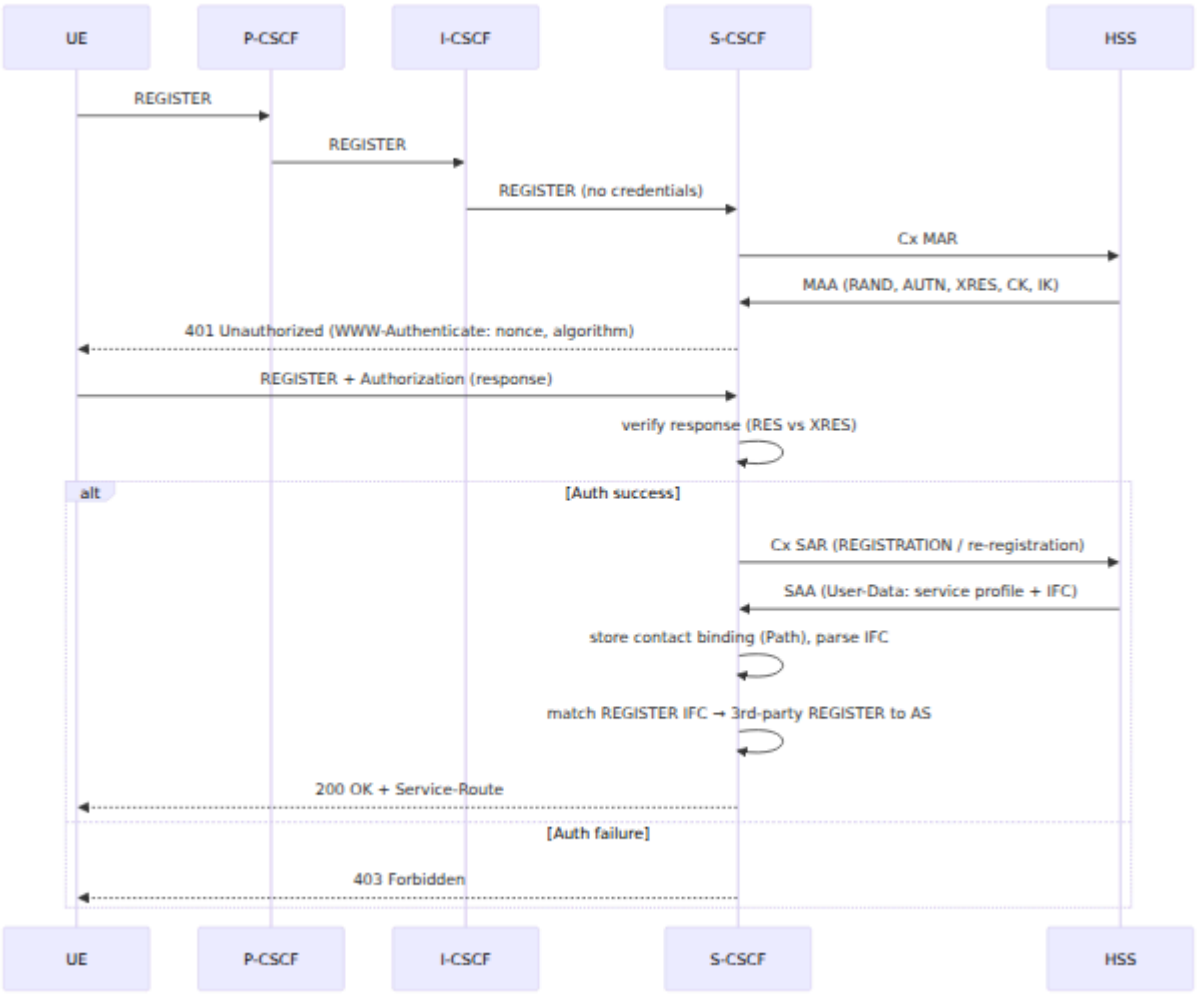
Registration & authentication

The S-CSCF is the authoritative registrar. It challenges the UE, validates the response against a Cx authentication vector obtained from the HSS, and - on success - 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 none is offered it defaults to SIP Digest (MD5), which accommodates non-IMS softphones. By default every REGISTER is authenticated.
2. **Challenge (MAR).** On an un-credentialed REGISTER the S-CSCF requests an authentication vector from the HSS with a Cx Multimedia-Auth-Request. The HSS returns the vector (for AKA: RAND, AUTN, XRES, CK, IK) in the answer, and the S-CSCF replies **401 Unauthorized** with a `WWW-Authenticate` header carrying 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, **503**.

3. **Verification.** The UE re-sends REGISTER with its computed response, which the S-CSCF checks against the stored vector (matched 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, and re-challenges with fresh vectors.
5. **Server assignment (SAR).** After successful authentication the S-CSCF sends a Cx Server-Assignment-Request - assignment type REGISTRATION on first registration, re-registration on a refresh. The answer returns the subscriber's User-Data (service profile and IFC), which is held 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 contact binding is stored together with the P-CSCF Path (so terminating requests can be routed back through the same P-CSCF), and the 200 OK carries a Service-Route so the UE sends subsequent requests through this S-CSCF. One contact is kept per public identity - a new binding replaces the previous one - with a fixed 599-second expiry.
7. **Third-party register / reg-event.** Registration is also evaluated against the REGISTER-triggered Initial Filter Criteria, firing third-party REGISTERs to any matching Application Servers, and the registration-event package notifies subscribed entities of the registration state (the subscription is torn down on de-registration).



Service triggering via IFC (ISC)

Every initial request is evaluated against the subscriber's downloaded **Initial Filter Criteria**. Each IFC is a prioritised Trigger Point (a boolean combination of Service Point Triggers - method, Request-URI, SIP header, Session Case, SDP) plus an Application Server address and a Default Handling value (session-continued, or session-terminated on AS failure). The Trigger Point is expressed in conjunctive or disjunctive normal form, with the individual triggers groupable and negatable.

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. So the AS can return the request to the point in the chain it left off, the S-CSCF marks it with an **Original Dialog Identifier (ODI)** and inserts a **P-Served-User** header (RFC 5502) identifying the served subscriber and session case. When the AS routes the request back, the S-CSCF recognises the ODI and resumes IFC evaluation after the last-matched criterion instead of restarting.

Default Handling governs AS-failure behaviour: a 408 or 5xx from the Application Server either 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 in-dialog requests are recognised as the originating leg.
- **Asserts identity.** Unless the request is returning from an AS, any client-supplied `P-Asserted-Identity` is removed and replaced with the identity the S-CSCF authenticated at registration - 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 carrying a `phone-context` is rewritten to a `tel:` URI in the home network's phone-context before routing.
- **PSTN / ENUM.** For E.164 destinations the number is resolved by ENUM; on an ENUM miss the call is sent 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`), it is routed to that TRF instead.
- **Charging vector.** Originating calls carry a `P-Charging-Vector` for inter-operator charging correlation.
- If online charging is enabled, a credit-control request is sent before the call proceeds (see Charging).

Non-PSTN destinations are relayed toward the terminating side; where the terminating user is served by this same S-CSCF, 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'

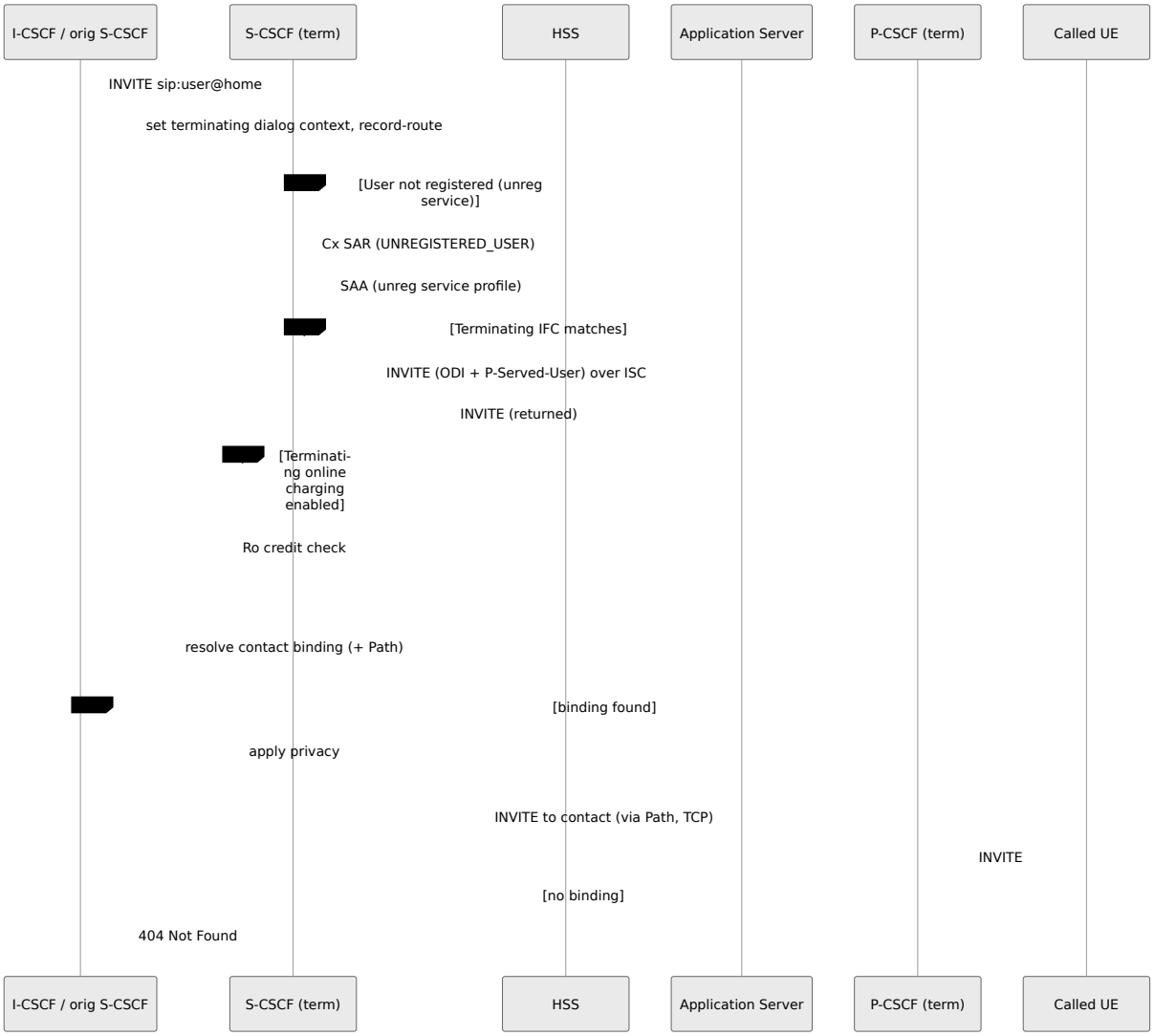
Try again

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 in-dialog requests are recognised as the terminating leg.
2. Restores the original Request-URI and evaluates the terminating IFC for non-INVITE methods, forwarding matches to the Application Server over ISC; for INVITEs, IFC forwarding follows the AS return cycle.
3. If terminating online charging is enabled, a terminating-side credit-control request is sent before proceeding.
4. **Location resolution.** The S-CSCF retrieves the served user's contact binding and relays the request to that contact via the P-CSCF recorded in the Path at registration. If the user has no binding, a **404 Not Found** is returned.
5. For an INVITE to an identity that is **not currently registered**, the S-CSCF first fetches the unregistered service profile from the HSS with a Cx Server-Assignment-Request of type UNREGISTERED_USER, so terminating-unregistered services (e.g. voicemail) can run; an HSS timeout fails **503** and a missing profile fails **403**.

Privacy is applied on egress: if the request asserts `Privacy: id`, the `P-Asserted-Identity` is removed before the message leaves the S-CSCF.



Charging (optional)

Online charging over Diameter **Ro** to an OCS is optional and enabled per deployment (see the charging flags below). When enabled, the S-CSCF sends a credit-control request before allowing an INVITE and maps the answer to SIP responses (e.g. insufficient funds → 402, credit-limit reached → 486, unknown charging subscriber → 403). The Service-Context-Id identifying the charged service is assembled from the charging parameters listed in the configuration reference.

In production this is normally **disabled**: charging is performed at the TAS, which can correctly account 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. Registration-event (`Event: reg`) `SUBSCRIBE` requests are accepted (200 OK); general presence subscriptions are not served. A registration-event `PUBLISH` is accepted only from a registered user and updates the published registration state, otherwise it is rejected **403**. There is no user-availability (PIDF) presence handling in this configuration.

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 / deriva
`NETWORKNAME`	Home IMS domain - 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 - its registrar and authentication identity	`sip:<hostname>:5060`
`SCSCF_USER_AGENT`	`User-Agent` header the node emits	`User-Agent: Omnitouch S-CSCF <inve`
`ISC_MY_URI`	Host token used to recognise this S-CSCF's own	`<inventory_hostname>`

Name	What it controls	Value / deriva
	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.`

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

Authentication - `REG_AUTH_DEFAULT_ALG`

The default authentication algorithm the S-CSCF applies when it must choose one (rather than echoing 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 each subscriber is challenged with whatever the HSS provisioned (AKA for mobiles, Digest for fixed, etc.).

Regardless of algorithm, every REGISTER is authenticated by default (see `WITH_AUTH`), the Cx destination realm is the home network domain (`NETWORKNAME`), auth vectors are matched on the public identity, and 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. `hssocs.voiceblue.com`
`RO_FORCED_PEER`	Pin credit-control routing to a specific Diameter peer, bypassing realm routing	peer id (e.g. `32260@3gpp.org`); off by default
`RO_ROOT`	Service-Context-Id root	`32260@3gpp.org`
`RO_EXT`	Service-Context-Id extension	`ext`
`RO_MNC`	MNC component of Service-Context-Id	e.g. `07`
`RO_MCC`	MCC component of Service-Context-Id	e.g. `262`
`RO_RELEASE`	3GPP release for Service-Context-Id	e.g. `8`

Feature flags (`WITH_*`)

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

`CAPTURE_NODE` (the Homer capture target) is templated only when Homer capture is enabled for the deployment; it 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, the OCS peer is addressed by `RO_DESTINATION` 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 answering the Cx MAR (auth vector) and SAR (service profile). If MAR/SAR time out or return malformed answers the registration fails **503**; verify the Cx peer to the HSS is up and responding. See Diameter Operations.
- **Authentication failures** - confirm the subscriber's credentials are provisioned in the HSS and that the auth vector was generated (MAR/MAA).

Verify 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 the S-CSCF's capabilities match what the I-CSCF selected on, and that the node has registration capacity.

Call setup failures

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

- **User not registered** - verify 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 the IFC was downloaded 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** - media QoS for the call is authorised by the P-CSCF (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 the subscriber's IFC is configured to trigger 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 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 provides technical specifications required for ANSSI R226 authorization under Articles R226-3 and R226-7 of the French Penal Code for the OmniCSCF IMS Core Network (Call Session Control Functions).

Classification: Regulatory Compliance Documentation

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

Regulation: R226 - Protection of Correspondence Privacy and Lawful Interception

---

1. DETAILED TECHNICAL SPECIFICATIONS

1.1 System Identification

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

Network Components:

- P-CSCF (Proxy Call Session Control Function)

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

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

1.2 Interception Capabilities

1.2.1 Registration and Session Acquisition

SIP Registration Capture:

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

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

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

Call Session Capture:

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

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

Emergency Call Identification:

The E-CSCF component identifies and routes emergency calls:

- Emergency number detection (112, 911, etc.)

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

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

The authenticated calling-line identity presented on the emergency leg is established as follows:

- **Known caller (registered):** the identity is taken from the registered IMPU and, where applicable, 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 via an asynchronous `Rx_AAR_Subscription`, bound by the UE source IP address. Identity is selected by precedence **MSISDN → IMSI → IMEISV**, and the resolved value is asserted 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) maintain **all state data in memory only**. There is **no persistent database storage** of registration or call session data. All registration bindings, dialog state, and IPsec security associations are stored in-memory and are lost on system restart.

Active Registration Data (In-Memory):

The CSCF system maintains real-time state only:

P-CSCF Registration State:

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

S-CSCF Registration State:

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

Active Session State (In-Memory):

The S-CSCF maintains active call state only:

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

No CDR or Historical Tracking:

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

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

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

SIP/Diameter Message Logging:

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

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

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

1.2.3 Analysis Capabilities

Real-Time Monitoring:

The 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 maintain historical data. For historical call records, CDRs, and communication pattern analysis, lawful interception authorities must coordinate with **OmniTAS (Telephony Application Server)**, which handles all CDR generation and long-term call tracking.

Real-Time Service Triggering Visibility:

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

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

Network Status:

- HSS connectivity status (Diameter Cx interface)
- S-CSCF selection distribution (I-CSCF)
- Call routing patterns
- Application Server response times
- Diameter transaction performance

1.3 Countermeasure Capabilities

1.3.1 Privacy Protection Mechanisms

Communication Confidentiality:

- **IPsec Tunnels:** ESP (Encapsulating Security Payload) tunnels between UE and P-CSCF
    - Encryption: AES-CBC, AES-GCM
    - Authentication: HMAC-SHA1, HMAC-SHA256
    - Key derivation from IMS AKA (CK/IK from HSS)
    - Per-UE security associations

- **TLS/TLS Support:**
  - SIP over TLS (SIPS) support
  - Diameter over TLS (HSS, PCRF, OCS connections)
  - Certificate-based authentication
  - Perfect Forward Secrecy (PFS) via ECDHE/DHE
- **SIP Privacy Headers:**
  - P-Asserted-Identity (authenticated caller ID)
  - Privacy header (request caller ID suppression)
  - Anonymous session support

Access Control:

- 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:

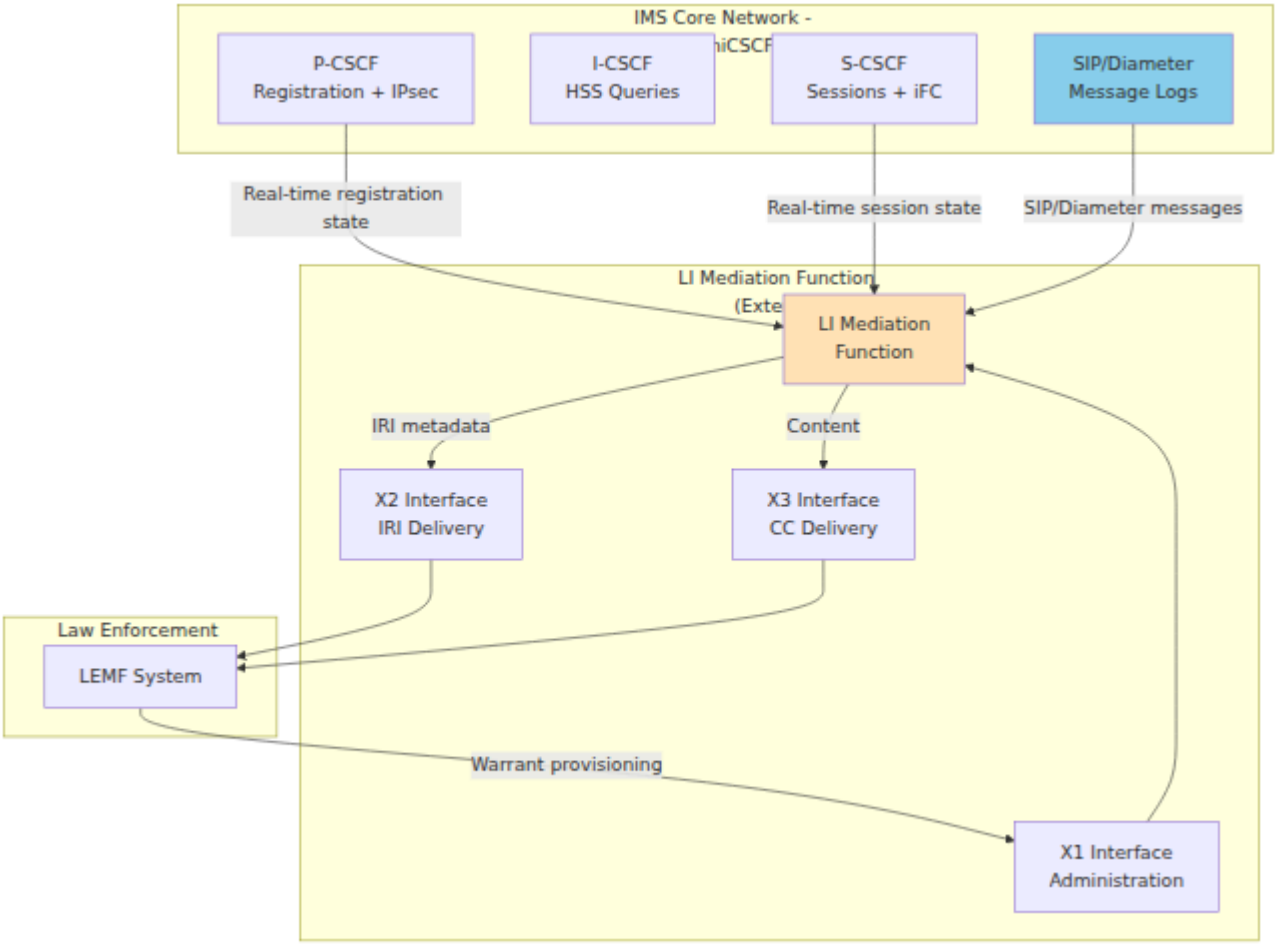
- Minimal exposed network ports (5060 SIP, 3868 Diameter, 2046 BINRPC management)
- SIP message sanity checking
- Max-Forwards loop prevention
- Rate limiting and anti-flood protection
- Message size limits
- Worker process isolation

1.4 Lawful Interception Integration Points

1.5.1 ETSI Lawful Interception Architecture

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

Standard ETSI LI Interfaces:



X1 Interface - Administration Function:

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

X2 Interface - IRI (Intercept Related Information) Delivery:

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

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

X3 Interface - CC (Content of Communication) Delivery:

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

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

1.5.2 CSCF Data Sources for Lawful Interception

1. Registration Data Access:

P-CSCF Registration Data:

- IMPU (public identity)

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

S-CSCF Registration Data:

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

Access Methods:

- Read-only data access interfaces
- 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:

- 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 multiple integration methods for Lawful Interception Mediation Function (LIMF) systems:

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

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

2. **Event Logging:**

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

3. **Real-Time Monitoring:**

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

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

1.5.4 CSCF Data Mapping to LI Interfaces

CSCF Data to IRI (X2) Mapping:

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

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

CSCF Data to CC (X3) Mapping:

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

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

Note on emergency calling identity (Party A): For a normal (registered) call, Party A is derived from the registered IMPU / P-Asserted-Identity. For an **unknown/anonymous emergency call**, Party A is the identity the P-CSCF resolves from the PCRF over Diameter Rx (`Rx_AAR_Subscription`, bound by UE source IP, precedence MSISDN → IMSI → IMEISV) and asserts 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

Monitoring and administrative access is provided by **OmniWeb**, the unified management portal (<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>), which

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

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

2.2.1 IPsec Protocol Implementation

Supported IPsec Mode:

- ESP (Encapsulating Security Payload) - IP Protocol 50

- Transport mode (not tunnel mode)
- Protects SIP signaling between UE and P-CSCF

Encryption Algorithms Supported:

The system with kernel IPsec supports:

- **AES-CBC (Advanced Encryption Standard - Cipher Block Chaining):**
  - AES-128-CBC (128-bit key)
  - AES-192-CBC (192-bit key)
  - AES-256-CBC (256-bit key) - Recommended
- **AES-GCM (Advanced Encryption Standard - Galois/Counter Mode):**
  - AES-128-GCM (128-bit key with AEAD)
  - AES-256-GCM (256-bit key with AEAD) - Recommended
- **3DES-CBC (Triple DES - Cipher Block Chaining):**
  - 168-bit effective key (deprecated, legacy compatibility)
- **NULL Encryption:**
  - No confidentiality (authentication only)
  - Used only for debugging or specific compliance scenarios

Authentication Algorithms Supported:

- **HMAC-SHA1 (Hash-based Message Authentication Code - SHA-1):**
  - 160-bit output
  - Legacy compatibility
- **HMAC-SHA256 (HMAC - SHA-256):**
  - 256-bit output
  - Recommended
- **HMAC-SHA384 (HMAC - SHA-384):**

    - 384-bit output
- **HMAC-SHA512 (HMAC - SHA-512):**
    - 512-bit output
- **HMAC-MD5:**
    - 128-bit output
    - Deprecated, legacy compatibility only

Key Derivation:

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

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

Security Association Parameters:

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

Implementation:

The P-CSCF IPsec capability:

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

2.2.2 IPsec Configuration Capabilities

Cipher Suite Selection:

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

Preferred (strong security):

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

Supported (compatibility):

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

Key Management:

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

Tunnel Lifecycle:

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

2.3 TLS Encryption (SIP and Diameter)

2.3.1 TLS for SIP (SIPS)

Supported TLS Versions:

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

TLS Implementation:

the system uses OpenSSL or LibreSSL:

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

Cipher Suites Supported:

TLS 1.3 (Preferred):

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256

TLS 1.2 (Supported):

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

Weak ciphers disabled:

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

Certificate Support:

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

TLS Features:

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

SIP over TLS (SIPS):

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

2.3.2 TLS for Diameter

Diameter Capabilities:

The system supports:

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

Use Cases:

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

TLS Configuration for Diameter:

Same cipher suites as SIP

- TLS 1.2/1.3
- ECDHE/DHE key exchange (PFS)
- AES-GCM encryption
- SHA256/SHA384 authentication

Certificate-Based Authentication:

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

2.4 Authentication Cryptography

2.4.1 IMS AKA Cryptographic Functions

3GPP AKA Algorithm (MILENAGE):

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

Cryptographic Functions:

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

Key Material:

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

AKA Sequence:

1. HSS generates RAND (cryptographically random)
2. HSS computes MAC-A = f1(K, RAND, SQN, AMF)
3. HSS computes AUTN = (SQN ⊕ AK) || AMF || MAC-A
4. HSS computes XRES = f2(K, RAND)
5. HSS computes CK = f3(K, RAND)
6. HSS computes IK = f4(K, RAND)
7. HSS sends {RAND, AUTN, XRES, CK, IK} to S-CSCF
8. S-CSCF challenges UE with RAND and AUTN
9. UE computes RES = f2(K, RAND) using ISIM
10. UE sends RES to S-CSCF
11. S-CSCF compares RES with XRES (authentication validation)

Security Properties:

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

2.4.2 HTTP Digest Authentication

For non-IMS authentication (if used):

Algorithm: MD5 (RFC 2617)

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

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

2.5 Hashing and Integrity

2.5.1 Hash Functions Available

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

- **SHA-256:** 256-bit output, recommended
- **SHA-384:** 384-bit output
- **SHA-512:** 512-bit output
- **SHA-1:** 160-bit output, deprecated for security use
- **MD5:** 128-bit output, deprecated for security use

Usage:

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

2.5.2 Message Integrity

SIP Message Integrity:

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

Diameter Message Integrity:

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

2.6 Random Number Generation

Cryptographically Secure Random Number Generation:

the system relies on:

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

Usage:

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

2.7 Key Management

2.7.1 TLS Certificate Management

Certificate Storage:

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

Certificate Generation:

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

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

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

# Production: Submit CSR to trusted CA
```

Certificate Rotation:

- Annual certificate renewal recommended
- Graceful service restart to load new certificates

- No downtime required

2.7.2 IPsec Key Management

Key Derivation:

- CK (Cipher Key) and IK (Integrity Key) from IMS AKA
- 128-bit keys from HSS
- Delivered securely via Diameter Cx (over TLS)

Key Lifetime:

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

Key Storage:

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

2.8 Cryptanalysis Resistance

2.8.1 Algorithm Selection

Defense Against Cryptanalysis:

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

Deprecated Algorithms Disabled:

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

2.8.2 Side-Channel Attack Mitigation

Timing Attack Resistance:

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

Memory Protection:

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

2.9 Compliance and Standards

Cryptographic Standards Compliance:

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

French Cryptography Regulations:

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

IMS CSCF Metrics Reference

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

Accessing Metrics

All CSCF components expose Prometheus metrics on port 9090:

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

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

Example Prometheus Configuration:

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

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

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

For operational guidance on monitoring and alerting, see:

- Monitoring via OmniWeb and Grafana

Monitoring via OmniWeb and Grafana

Operational state - registrations, dialogs, and Diameter peer status - is viewed in **OmniWeb**, the unified management portal: <https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>. OmniWeb embeds Grafana dashboards for real-time and historical visibility, including S-CSCF registration and user-location views (backed by metrics such as `ims_usrloc_scscf_active_impus` and `ims_usrloc_scscf_active_contacts`) and Diameter peer status and queue depth (backed by `cdp_queuelength`, and interface metrics such as `ims_icscf_uar_*`, `ims_icscf_lir_*`, `ims_auth_mar_*`, `ims_registrar_scscf_sar_*`, and `ims_qos_*`).

The Prometheus metrics documented in this reference back those Grafana dashboards as well as any custom alerting you configure.

P-CSCF Metrics

CDP (Diameter) Metrics

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

Core SIP Statistics

Request Counters

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

Reply Counters (General)

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

Reply Counters by Method (1xx)

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

Reply Counters by Method (2xx)

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

Reply Counters by Method (3xx)

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

Reply Counters by Method (4xx)

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

Reply Counters by Method (5xx)

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

Reply Counters by Method (6xx)

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

Specific Status Code Counters

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

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

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

Forwarding and Error Statistics

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

Dialog Tracking

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

DNS Statistics

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

IMS IPSec P-CSCF

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

IMS QoS (Rx Interface)

Registration AAR Metrics

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

Media AAR Metrics

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

ASR Metrics

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

P-CSCF User Location

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

MySQL Database

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

Anti-Flood (IP Blocking)

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

Registrar Module

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

Script Statistics

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

SCTP Transport

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

Shared Memory

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

SL (Stateless) Module

Stateless Reply Counters by Class

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

Specific Stateless Reply Counters

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

Stateless General Statistics

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

TCP Transport

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

TM/TMX (Transaction) Module

Transaction Type Counters

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

Transaction Completion by Status

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

Transaction Reply Statistics

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

User Location

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

I-CSCF Metrics

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

I-CSCF Operational Context

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

IMS I-CSCF (Cx Interface - HSS Communication)

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

UAR (User-Authorization-Request) Metrics

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

LIR (Location-Info-Request) Metrics

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

Common Metrics

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

- **CDP (Diameter) Metrics** - Diameter protocol statistics
- **Core SIP Statistics** - Request/reply counters by method and status code
- **DNS Statistics** - DNS query metrics
- **MySQL Database** - Database connection errors
- **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 P-CSCF Core SIP Statistics section above). The following metrics are specific to S-CSCF functionality.

S-CSCF Operational Context

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

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

IFC (Initial Filter Criteria) determines which Application Servers process SIP sessions. IFC evaluation performance can impact call setup times tracked in transaction metrics (`tmx_*`).

IMS ISC (IMS Service Control)

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

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

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

IMS Authentication (Cx Interface - MAR)

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

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

IMS Registrar S-CSCF

Registration Statistics

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

SAR (Server-Assignment-Request) Metrics

Metric Name	Meaning
`ims_registrar_scscf_sar_avg_response_time`	Average response time for SAR messages in milliseconds (calculated as sar_replies_response_ti / sar_replies_received)
`ims_registrar_scscf_sar_replies_received`	Total number of SAA (Server-Assignment-Answer) replies receive 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
`ims_usrloc_scscf_active_contacts`	Number of currently active registered contact bindings
`ims_usrloc_scscf_active_impus`	Number of currently active registered IMPUs (IMS Public User Identities)
`ims_usrloc_scscf_active_subscriptions`	Number of currently active subscriptions
`ims_usrloc_scscf_contact_collisions`	Number of hash collisions in the contact hash table
`ims_usrloc_scscf_impu_collisions`	Number of hash collisions in the IMPU hash table
`ims_usrloc_scscf_subscription_collisions`	Number of hash collisions in the subscription hash table

Dialog Tracking

The S-CSCF tracks dialog state for active calls:

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

Common Metrics

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

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