Guia de Operações Diameter

Índice

1. Visão Geral
2. Diameter na Arquitetura IMS
3. Interfaces Diameter
4. Gerenciamento de Pares via OmniWeb
5. Códigos de Resultado Diameter
6. Problemas Comuns

Visão Geral

Diameter é o protocolo de autenticação, autorização e contabilidade (AAA) para a arquitetura IMS. O OmniCSCF usa Diameter para se comunicar com elementos críticos da rede. Esses elementos incluem o HSS, PCRF e OCS.

O que é Diameter?

Diameter (RFC 6733) é o sucessor do RADIUS. Diameter suporta cenários AAA modernos:

- **Transporte confiável** através de TCP/SCTP. O RADIUS usa UDP.
- **Extensível** através de módulos específicos de aplicação
- **Arquitetura peer-to-peer**. Não é apenas cliente-servidor.
- Conexões **com estado** com monitoramento de watchdog
- Manipulação de erros e códigos de resultado **padronizados**

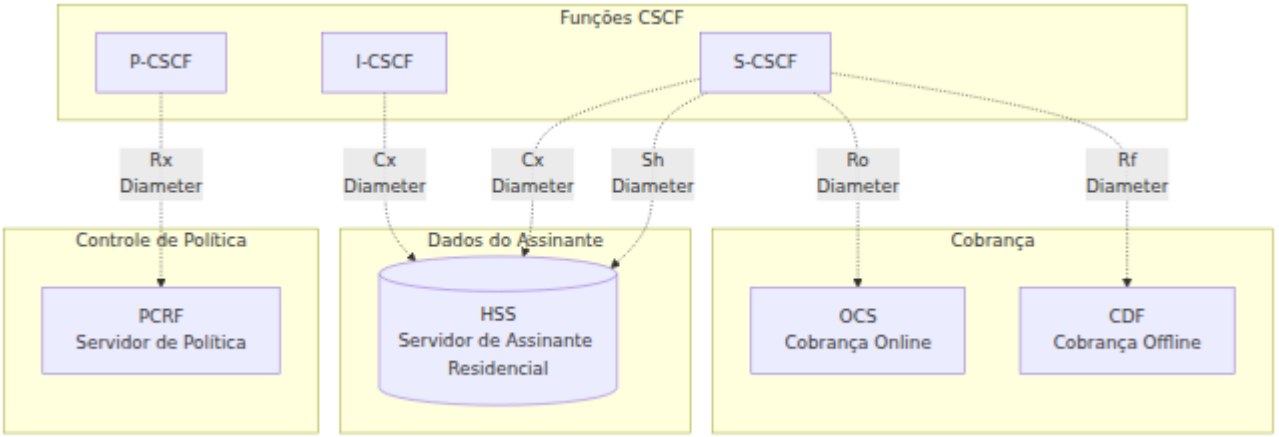
Diameter no CSCF

Cada componente CSCF usa interfaces de aplicação Diameter específicas:

CSCF	Interface	ID da Aplicação	Conectado a	Propósito
I-CSCF	Cx	16777216	HSS	Seleção do S-CSCF, localização do usuário
S-CSCF	Cx	16777216	HSS	Autenticação do usuário, download de perfil
S-CSCF	Sh	16777217	HSS	Acesso a dados do usuário (opcional)
P-CSCF	Rx	16777236	PCRF	Controle de política de QoS e bearer
S-CSCF	Ro	4	OCS	Cobrança online (controle de crédito)
S-CSCF	Rf	3	CDF	Cobrança offline (contabilidade)

Diameter na Arquitetura IMS

Visão Geral da Rede



Interfaces Diameter

Interface Cx (CSCF ↔ HSS)

O I-CSCF e o S-CSCF usam a interface Cx para autenticação de usuários e gerenciamento de perfil.

Especificação 3GPP: TS 29.228

Operações I-CSCF

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

- **Propósito**: Consultar o HSS para atribuição ou capacidades do S-CSCF
- **Gatilho**: O I-CSCF recebe um REGISTER do usuário
- **Caso de Uso**: O I-CSCF deve rotear o registro para o S-CSCF correto

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

- **Propósito**: Consultar o HSS para o S-CSCF atual do usuário
- **Gatilho**: O I-CSCF recebe um INVITE ou MESSAGE para o usuário que está terminando

- **Caso de Uso**: O I-CSCF deve rotear a sessão para o S-CSCF do usuário

Operações S-CSCF

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

- **Propósito**: Recuperar vetores de autenticação do HSS
- **Gatilho**: O REGISTER inicial, antes do desafio
- **Caso de Uso**: O S-CSCF deve desafiar o usuário para autenticação IMS AKA

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

- **Propósito**: Informar ao HSS sobre o estado de registro e baixar o perfil do usuário
- **Gatilho**: Autenticação bem-sucedida, após MAR/MAA
- **Caso de Uso**: O S-CSCF baixa o IFC e o perfil de serviço para o usuário

O AVP `User-Data` no SAA contém o perfil completo do usuário. Este perfil inclui:

- Identidades públicas
- Critérios de Filtro Inicial (IFC) para ativação de serviços
- Identificadores de perfil de mídia assinados
- Informações de cobrança

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

- **Propósito**: Desregistro iniciado pelo HSS. O HSS envia o pedido.
- **Gatilho**: Desregistro administrativo ou mudança de assinatura
- **Caso de Uso**: O HSS instrui o S-CSCF a desregistrar um usuário

Interface Rx (P-CSCF ↔ PCRF)

A interface Rx fornece controle de política e QoS para sessões IMS.

Especificação 3GPP: TS 29.214

Nota sobre VoNR (5G NR): Para sessões VoNR, o PCF autoriza mídia e QoS através da interface N5 AF (Npcf_PolicyAuthorization, HTTP/2 SBI). Não utiliza Diameter Rx. A interface Rx aqui, portanto, se aplica ao acesso 4G/LTE.

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

- **Propósito**: Solicitar autorização de QoS para uma sessão de mídia
- **Gatilho**: A troca de oferta/resposta SDP em um SIP INVITE
- **Caso de Uso**: O P-CSCF solicita ao PCRF a autorização de recursos de bearer

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

- **Propósito**: Atualização de política iniciada pelo PCRF. O PCRF envia o pedido.
- **Gatilho**: Uma mudança de política ou modificação de bearer
- **Caso de Uso**: O PCRF instrui o P-CSCF a atualizar a política de QoS

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

- **Propósito**: Liberar a sessão Rx e os recursos de bearer
- **Gatilho**: Término da chamada. O P-CSCF recebe um BYE.
- **Caso de Uso**: O P-CSCF informa ao PCRF para liberar recursos de QoS

Interface Ro (S-CSCF ↔ OCS)

A interface Ro fornece cobrança online (controle de crédito).

Especificação 3GPP: TS 32.299

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

- **Propósito**: Autorização e débito de crédito em tempo real
- **Gatilho**: Estabelecimento de chamada, durante a chamada ou término da chamada
- **Caso de Uso**: Cobrança pré-paga e verificações de crédito em tempo real

Tipos:

- **CCR-Initial**: Solicitar crédito no início da chamada
- **CCR-Update**: Atualizar a cota durante a chamada
- **CCR-Terminate**: Relatar o uso final ao término da chamada

Gerenciamento de Pares via OmniWeb

Visualize o status do par Diameter, aplicações suportadas e profundidades de fila na aba **Diameter** de cada página CSCF no OmniWeb. O OmniWeb é o portal de gerenciamento unificado: <https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>.

A aba Diameter do OmniWeb mostra o seguinte por CSCF:

- Identidade do Realm e Origin-Host Diameter
- Pares configurados e seu estado de conexão (I_Open, Closed, etc.)
- Aplicações Diameter suportadas por par, mapeadas para nomes de interface 3GPP (Cx/Dx, Sh/Dh, Rx, Ro, Gx, S6a/S6d, e outros)
- Comprimento da fila de trabalho e transações pendentes
- Operações de habilitar/desabilitar para pares individuais

Estados dos Pares

Estado	Descrição
I_Open	A conexão está aberta e operacional
Closed	Nenhuma conexão está estabelecida
Wait-Conn-Ack	A conexão foi iniciada. Aguarda uma resposta.
Wait-I-CEA	O CER foi enviado. Aguarda o CEA.

Códigos de Resultado Diameter

A tabela a seguir lista códigos de resultado comuns e seus significados:

Código	Nome	Significado	Aç
2xxx	**Sucesso**		
2001	DIAMETER_SUCCESS	Operação bem-sucedida	Nenhum
3xxx	**Erros de Protocolo**		
3002	DIAMETER_UNABLE_TO_DELIVER	Não é possível rotear para o destino	Verifique conectiv do par
3003	DIAMETER_REALM_NOT_SERVED	O realm não é reconhecido	Verifique configur realm
3007	DIAMETER_APPLICATION_UNSUPPORTED	A aplicação não é suportada	Verifique Applicat
4xxx	**Falhas Transitórias**		
4001	DIAMETER_AUTHENTICATION_REJECTED	Autenticação falhou	Verifique credenci
4010	DIAMETER_USER_UNKNOWN	O usuário não está provisionado	Verifique provisio do HSS
5xxx	**Falhas Permanentes**		
5001	DIAMETER_AVP_UNSUPPORTED	O AVP não é reconhecido	Verifique versão d protocol

Código	Nome	Significado	Aç
5002	DIAMETER_UNKNOWN_SESSION_ID	A sessão não foi encontrada	A sessão expirou inválida
5003	DIAMETER_AUTHORIZATION_REJECTED	Não autorizado	Verifique permiss usuário
5012	DIAMETER_UNABLE_TO_COMPLY	Não é possível processar o pedido	Verifique do HSS/PCR

Problemas Comuns

Interfaces Diameter Críticas

Quando um par Diameter fica fora do ar, o impacto e a urgência de recuperação dependem da interface afetada:

Interface	Impacto se Fora do Ar	Prioridade de Recuperação
Cx (HSS)	Nen novos registros. Nenhuma atualização de IFC.	Crítico. Recuperar imediatamente.
Rx (PCRF)	Sem QoS para novas chamadas	Alto. Recuperar em minutos.
Ro (OCS)	Sem cobrança pré-paga. O serviço pode continuar.	Alto. Depende da política.

Falhas de Conexão de Pares

Sintoma: O par está preso no estado "Closed" ou "Wait-Conn-Ack"

Diagnóstico:

1. Verifique a conectividade da rede:

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

2. Verifique as regras do firewall. A porta 3868 TCP deve estar aberta.
3. Verifique a configuração do par (endereço IP, porta)
4. Verifique os logs do par para tentativas de conexão

Resolução:

- Corrija os problemas de rede e firewall
- Verifique se o par está em execução e escutando na porta 3868
- Verifique se o par tem a configuração correta para o CSCF
- Use **Enable Peer** na aba Diameter do OmniWeb para tentar a conexão novamente

---

Falhas na Troca CER/CEA

Sintoma: O par está preso no estado "Wait-I-CEA", ou o CEA tem um código de erro

Erros Comuns:

- **5010 (NO_COMMON_APPLICATION)**: Verifique se ambos os pares suportam a mesma aplicação (por exemplo, Cx = 16777216)
- **3003 (REALM_NOT_SERVED)**: Verifique se o Origin-Realm corresponde ao realm esperado do par

Resolução:

- Verifique a configuração Diameter para o Application-Id e realm

- Certifique-se de que a configuração do par corresponda às expectativas do CSCF
- Revise os logs do backend do CSCF para mensagens de erro detalhadas

---

Problemas na Interface Cx do HSS

Sintoma: Falhas de registro e timeouts MAR/MAA

Erros Comuns:

Código de Resultado	Significado	Resolução
4010	USER_UNKNOWN	O usuário não está provisionado no HSS
4001	AUTHENTICATION_REJECTED	O IMPI ou credenciais estão incorretos
5012	UNABLE_TO_COMPLY	Erro interno do HSS. Verifique os logs do HSS.

Resolução:

- **USER_UNKNOWN**: Provisione o usuário no HSS
- **AUTHENTICATION_REJECTED**: Verifique o IMPI e a chave compartilhada no HSS
- **UNABLE_TO_COMPLY**: Verifique os logs do HSS e a conectividade do banco de dados

---

Problemas na Interface Rx do PCRF

Sintoma: Chamadas são bem-sucedidas, mas nenhuma QoS é aplicada. Ocorrem timeouts AAR/AAA.

Problemas Comuns:

- **PCRF fora do ar**: Verifique o status do par na aba Diameter do OmniWeb
- **Framed-IP-Address não reconhecido**: O PCRF não consegue mapear o IP do UE para o assinante
- **Política não aplicada**: Verifique as regras de política do PCRF. Verifique a integração do PCEF.

Resolução:

- Verifique se o par PCRF está no estado "I_Open"
- Verifique o provisionamento do endereço IP do UE no PCRF
- Verifique se a interface Gx (PCRF para PCEF) está funcional

---

Problemas na Interface Ro do OCS

Sintoma: Chamadas pré-pagas falham. Ocorrem timeouts CCR/CCA. Chamadas estão bloqueadas.

Erros Comuns:

Código de Resultado	Significado	Resolução
4012	CREDIT_LIMIT_REACHED	Crédito insuficiente
5003	AUTHORIZATION_REJECTED	O usuário não está autorizado para pré-pago

Resolução:

- **CREDIT_LIMIT_REACHED**: Normal para usuários pré-pagos sem crédito
- **Timeout do OCS**: Verifique a disponibilidade do OCS e o status do par
- **AUTHORIZATION_REJECTED**: Verifique se o usuário está provisionado para pré-pago no OCS

Degradação de Desempenho

Sintoma: Tempos de resposta Diameter lentos e alta latência

Diagnóstico:

1. Verifique o timestamp "Last Used" na lista de pares. Deve ser recente.
2. Monitore o "Queue Length". Valores altos indicam um backlog.
3. Revise os logs do backend do CSCF para avisos de timeout

Resolução:

- **Alta latência**: Investigue a rede entre o CSCF e o par
- **Alto comprimento da fila**: Verifique a carga do sistema do par (HSS/PCRF/OCS)
- **Timeouts**: Se a rede tiver alta latência, aumente o timeout da transação

Melhores Práticas

Diretrizes Operacionais

Gerenciamento de Pares:

- Monitore o status do par na aba Diameter do OmniWeb
- Configure monitoramento externo para eventos de queda de pares
- Teste a conectividade do par durante janelas de manutenção

Planejamento de Capacidade:

- Estime a taxa de transação Diameter a partir dos registros e do volume de chamadas
- Certifique-se de que o HSS/PCRF/OCS pode lidar com taxas de transação de pico
- Para grandes implantações, considere agentes de roteamento Diameter (DRA)

Resolução de Problemas:

- Verifique o status do par primeiro quando investigar falhas de registro ou chamada
- Correlacione falhas Diameter com falhas SIP (mesmo Call-ID ou usuário)
- Revise os logs do backend do CSCF para rastreamentos detalhados de transações Diameter

Segurança:

- Use TLS para conexões Diameter em produção, se TLS for suportado
- Restrinja o acesso ao par Diameter com o firewall. Permita apenas pares conhecidos.
- Revise regularmente os logs de auditoria de habilitação/desabilitação de pares

Limitações e Melhorias Futuras

Implementação Atual

A aba Diameter do OmniWeb fornece:

- □ Visualização em tempo real do status do par
- □ Habilitar/desabilitar operações de pares
- □ Mapeamento de ID de Aplicação para nome de interface

Ainda Não Implementado

Os seguintes recursos **não estão atualmente disponíveis**. Versões futuras podem adicioná-los:

- **Inspector de Mensagens Diameter**: Visualizar transações Diameter recentes e detalhes de AVP
- **Estatísticas de Pares**: Contagens de mensagens, taxas de sucesso e latência média por par
- **Monitoramento de Watchdog**: Status DWR/DWA em tempo real

Soluções Alternativas

Para Inspeção de Mensagens: Verifique os logs do backend do CSCF ou habilite o registro de depuração Diameter

Para Estatísticas Detalhadas: Consulte as métricas do endpoint Prometheus. Veja Referência de Métricas para definições completas de métricas CDP/Diameter e configuração de monitoramento.

Para Reconexão Manual: Use a aba Diameter do OmniWeb para desabilitar e, em seguida, reabilitar o par

Documentação Relacionada

- **Guia de Operações P-CSCF** - Operações da interface Rx do P-CSCF
- **Guia de Operações I-CSCF** - Operações da interface Cx do I-CSCF
- **Guia de Operações S-CSCF** - Interfaces Cx, Ro do S-CSCF
- **Guia de Operações 5G SBI** - Interfaces baseadas em serviços N5/NRF usadas para VoNR (o equivalente 5G ao Rx)
- **Referência de Métricas** - Métricas e monitoramento CDP/Diameter
- **OmniWeb** - Gerenciamento de pares Diameter através da aba Diameter do OmniWeb
- **Guia de Operações CSCF** - Operações gerais do CSCF

Especificações 3GPP

- **TS 29.228**: Interfaces Cx e Dx (CSCF-HSS)
- **TS 29.214**: Interface Rx (P-CSCF-PCRF)
- **TS 32.299**: Aplicações de cobrança Diameter (Ro, Rf)
- **RFC 6733**: Protocolo Base Diameter

Detalhes Técnicos

Implementação

- **Pilha Diameter**: Pilha de protocolo Diameter integrada
- **Interface de Gerenciamento**: Protocolo RPC para backend do CSCF
- **Portal de Gerenciamento**: OmniWeb (<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>)

Configuração de Pares (Implantação)

Cada nó CSCF tem um arquivo de configuração de par Diameter: `pcscf.xml`, `icscf.xml` ou `scscf.xml`. O Ansible renderiza o arquivo no momento da implantação. O arquivo define a identidade Diameter do nó e os pares HSS/PCRF/DRA aos quais se conecta. A estrutura é idêntica em todos os três arquivos. Apenas a aplicação anunciada difere.

Campo XML	O que configura	Fonte Ansible
`DiameterPeerFQDN`	O FQDN do origin-host Diameter deste nó	`<inventory_hostname>.epc.mnc<mnc>.m`
`DiameterPeerRealm`	O realm Diameter local	`ims_realm` se definido, caso contrário `epc.mnc<mnc>.mcc<mcc>.3gppnetwork.o`
`Vendor_Id` / `Product_Name`	A identidade CER	`10415` (3GPP) / `OmniCSCF`
`Peer` (modo direto)	Par direto para cada host do grupo `hss` via SCTP:3868	renderizado por host em `groups['hss']` `ims_dra_support` é falso
`Peer` (modo DRA)	Par para cada host do grupo `dra`. IP explícito quando `diameter_dra_ip` está definido.	renderizado por host em `groups['dra']` `ims_dra_support` é verdadeiro
`Acceptor`	FQDN local e porta para Diameter inbound (3868)	FQDN do nó
`DefaultRoute`	Rota padrão de roteamento de realm para o par HSS/PCRF (métrica 1) ou o DRA (métrica 2)	renderizado a partir de `groups['hss']` /

Aplicação(ões) anunciada(s) por nó:

Nó (arquivo)	Aplicação(ões)
P-CSCF (`pcscf.xml`)	**Rx** `16777236` (fornecedores 10415, 0)
I-CSCF (`icscf.xml`)	**Cx** `16777216` (fornecedores 10415, 13019, 0) + contabilidade base `4`
S-CSCF (`scscf.xml`)	**Cx** `16777216` (fornecedores 10415, 13019, 0) + contabilidade base `4`

As principais variáveis Ansible são as seguintes. `plmn_id.mcc` e `plmn_id.mnc_longform` constroem todos os FQDNs e realms. `ims_realm` substitui o realm Diameter. `ims_dra_support` alterna entre peering direto e DRA. `diameter_dra_ip` define o IP estático para o par DRA. Os grupos de inventário `hss` e `dra` fornecem as listas de pares e rotas padrão. Quando a cobrança está habilitada, `RO_DESTINATION` endereça o par **Ro** (OCS) do S-CSCF separadamente. O XML não aborda esse par.

Edite esses arquivos através da ferramenta de implantação, não através do OmniWeb. O OmniWeb fornece monitoramento e controle operacional (habilitar/desabilitar) apenas.

Operações e Referência do I-CSCF

O Interrogating-CSCF é o ponto de contato de entrada da rede doméstica para sinalização IMS. Um assinante alcança este nó quando se registra. Uma sessão chega a este nó quando a sessão termina em um assinante doméstico. O I-CSCF não mantém estado de sessão. O I-CSCF não termina mídia. O I-CSCF consulta o HSS sobre Cx. Esta consulta decide qual Serving-CSCF lida com um determinado pedido. Na inscrição, o I-CSCF autoriza a identidade e a rede visitada. O I-CSCF então descobre o S-CSCF ou as capacidades do S-CSCF para selecionar um. Em um pedido de término, o I-CSCF localiza o S-CSCF que já atende o usuário. Depois que o I-CSCF escolhe um S-CSCF, o I-CSCF encaminha o pedido para esse S-CSCF. O I-CSCF retransmite as respostas de volta.

Funções IMS

Roteamento de registro (Cx UAR)

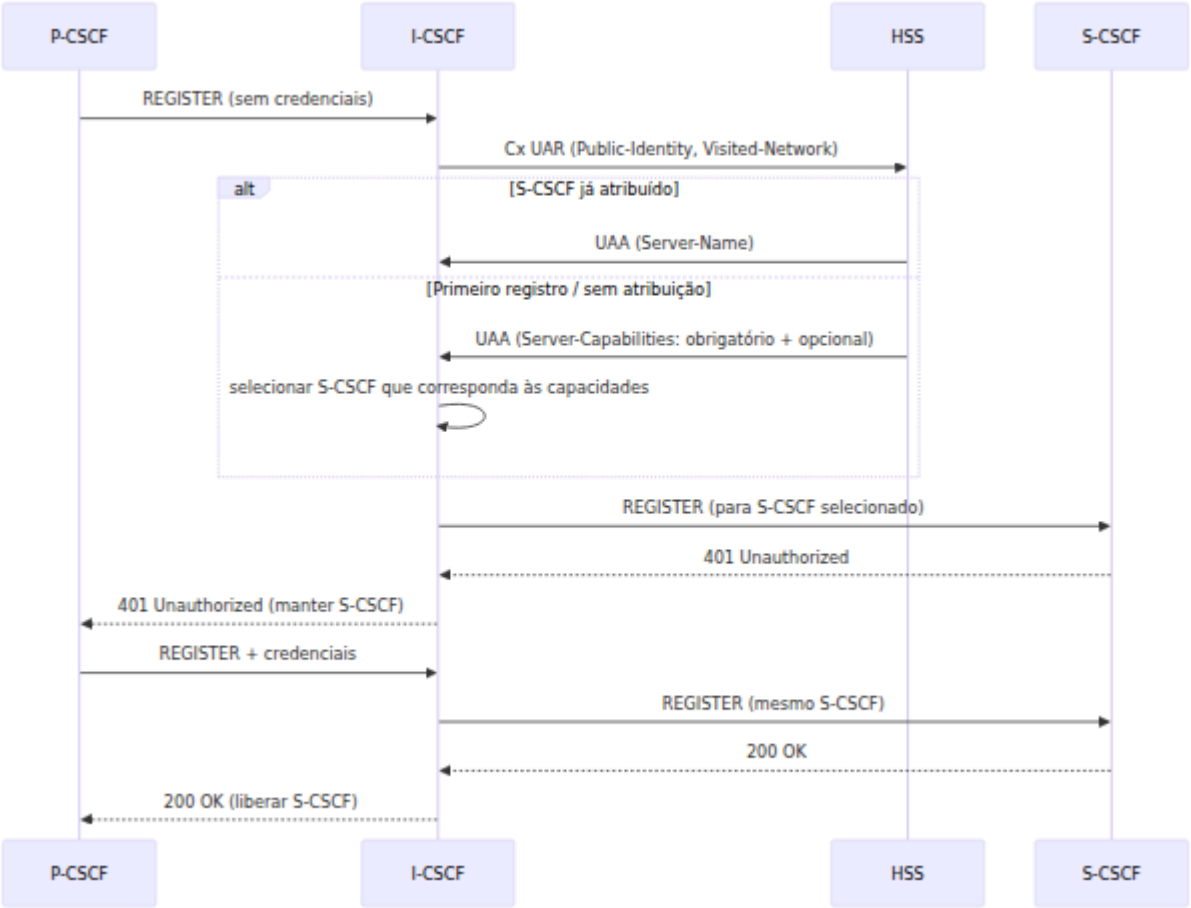
Quando um REGISTER chega, o I-CSCF consulta o HSS com um Cx **User-Authorization-Request (UAR)**. O I-CSCF envia essa consulta antes de encaminhar o REGISTER. O UAR carrega a identidade pública e o identificador da rede visitada. Esses valores permitem que o HSS autorize o assinante a se registrar a partir dessa rede. A resposta (UAA) retorna uma das duas coisas:

- **Um nome de S-CSCF já atribuído.** O I-CSCF usa esse nome diretamente. Um re-registro retorna para o mesmo S-CSCF que mantém a vinculação.
- **Capacidades do S-CSCF.** Estes são um conjunto de valores de capacidade obrigatórios e opcionais que o S-CSCF selecionado deve satisfazer. O HSS retorna esses valores no primeiro registro ou quando nenhum S-CSCF está atualmente atribuído. O I-CSCF então faz a seleção baseada em capacidades (abaixo).

O I-CSCF encaminha o REGISTER para o S-CSCF escolhido. O I-CSCF se lembra desse S-CSCF durante a duração do handshake de registro. O re-REGISTER

autenticado segue o desafio 401. O I-CSCF roteia este re-REGISTER para o **mesmo** S-CSCF e não consulta novamente. O I-CSCF retém o S-CSCF enquanto um 401 está em trânsito. O I-CSCF descarta o S-CSCF quando o registro é concluído (2xx) ou finalmente falha.

Um HSS que está indisponível ou retorna uma resposta malformada gera **503**. Um UAR pode autorizar, mas não fornecer um S-CSCF para selecionar. Nesse caso, o I-CSCF recua para um URI de S-CSCF padrão configurado.



Roteamento de término (Cx LIR)

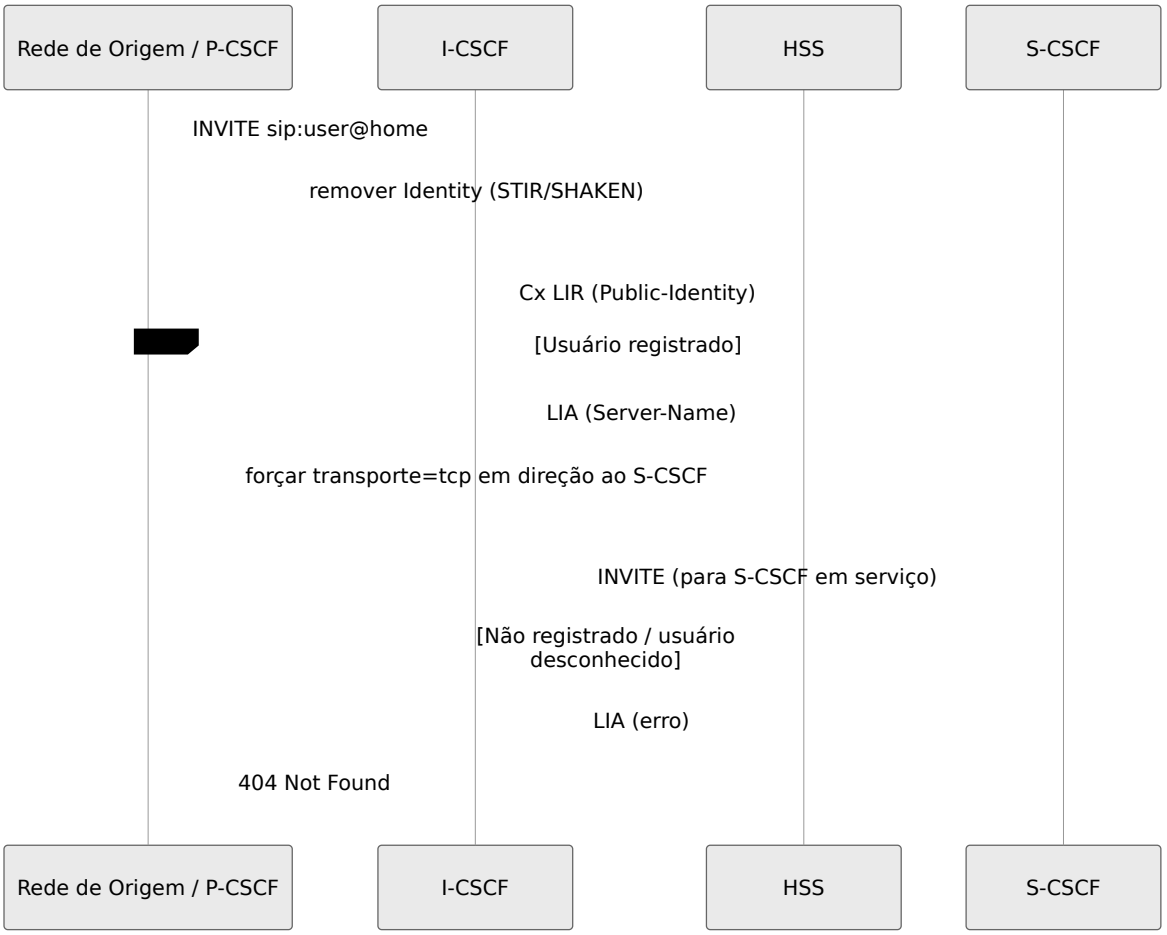
Um pedido de término inicial é um INVITE, SUBSCRIBE, MESSAGE, INFO ou PUBLISH. Em tal pedido, o I-CSCF consulta o HSS com um Cx **Location-Info-Request (LIR)** para a identidade do Request-URI. A resposta (LIA) retorna o nome do S-CSCF que atualmente atende o usuário. Para um usuário não registrado que tem serviços provisionados, a LIA retorna capacidades em vez disso. O I-CSCF então seleciona um S-CSCF a partir dessas capacidades. O I-CSCF encaminha o pedido para esse S-CSCF. Se o URI retornado não especificar um transporte, o I-CSCF força o transporte TCP em direção ao S-CSCF. O I-CSCF

remove qualquer cabeçalho `Identity` STIR/SHAKEN de entrada antes de encaminhar o pedido.

Tratamento de resultados:

- **Sucesso.** O I-CSCF seleciona o S-CSCF e retransmite o pedido para ele. Uma falha de retransmissão retorna **500**.
- **Usuário não encontrado / não registrado.** O I-CSCF retorna **404 Not Found**.
- **HSS indisponível.** O I-CSCF retorna **503**.

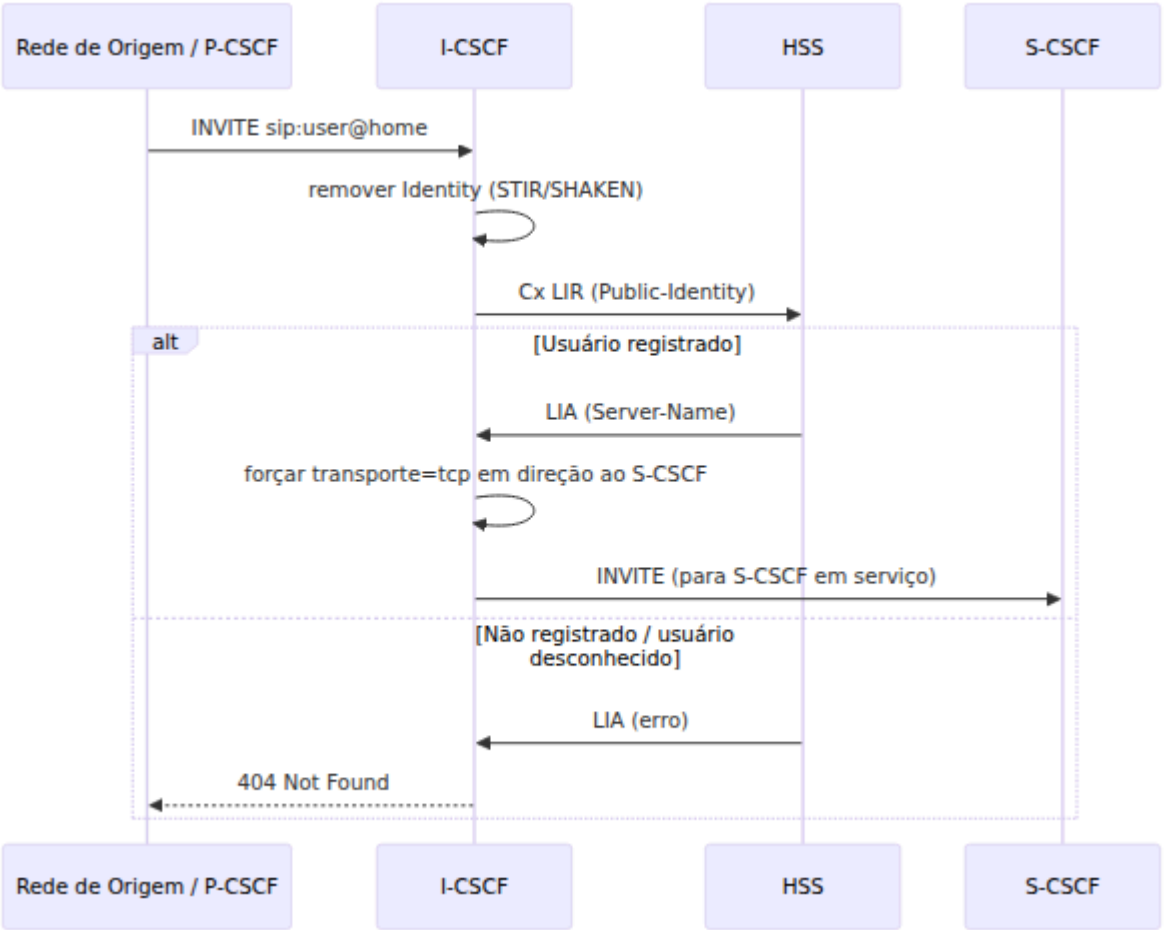
O I-CSCF não interroga CANCEL. O I-CSCF combina CANCEL com sua transação existente e a retransmite. O I-CSCF rejeita qualquer outro método não inicial, não REGISTER com **406** e uma lista `Allow`.



Seleção de S-CSCF / correspondência de capacidades

O HSS pode retornar capacidades em vez de um nome de S-CSCF atribuído. Nesse caso, o I-CSCF seleciona um S-CSCF de seu **conjunto de S-CSCF configurados**. Cada S-CSCF candidato tem um URI SIP e um conjunto de valores de capacidade. A seleção requer que o S-CSCF satisfaça **todas as capacidades obrigatórias**. Entre os candidatos qualificados, o I-CSCF prefere aqueles que correspondem a mais das capacidades **opcionais**. Vários candidatos podem ser igualmente adequados. Esses candidatos formam uma lista de candidatos ordenada. Esta lista permite que o I-CSCF tente um alternativo em caso de falha.

O I-CSCF mantém a lista de candidatos na memória da transação durante a vida do pedido. Isso preserva a posição da lista entre as tentativas. Um trecho de REGISTER encaminhado pode expirar ou gerar um 5xx/6xx. Nesse caso, o I-CSCF avança para o próximo S-CSCF candidato e tenta novamente. Quando a lista se esgota, o I-CSCF para. O I-CSCF retém a lista durante um desafio 401, porque o mesmo S-CSCF deve lidar com a nova tentativa autenticada. O I-CSCF descarta a lista em uma resposta final de sucesso ou erro do cliente. Se a seleção não gerar nada, o I-CSCF recua para o URI de S-CSCF padrão configurado.



Configuração de Implantação (Injetado pelo Ansible)

O Ansible renderiza a configuração em tempo de execução do I-CSCF (`icscf.cfg`) e sua tabela de pares Diameter (`icscf.xml`) no momento da implantação. Os valores derivam da identidade PLMN da rede (MCC/MNC) e do nome do host do inventário do nó. Os toggles de recursos são flags `#!define`. Uma flag definida habilita o recurso. Uma flag comentada desabilita o recurso.

Identidade / domínio

Nome	O que controla	Valor / d
`NETWORKNAME`	Domínio IMS doméstico. Este é o domínio de destino Cx (`cxdx_dest_realm`). O I-CSCF verifica este domínio quando roteia pedidos de usuários pareados ou desconhecidos.	`ims.mnc<mnc>.mcc<mcc>.3gppnet`
`HOSTNAME`	FQDN (alias do host) deste nó	`<inventory_hostname>.ims.mnc<`
`ICSCF_USER_AGENT`	O cabeçalho `User-Agent` que o nó emite	`User-Agent: Omnitouch I-CSCF`
`ICSCF_SERVER`	O cabeçalho `Server` que o nó emite	`Server: Omnitouch I-CSCF <inv`
`SCSCF_URI`	URI padrão ou de fallback do S-CSCF. O I-CSCF usa este URI quando a seleção baseada em UAR não gera S-CSCF.	`sip:scscf.ims.mnc<mnc>.mcc<mc`

O Ansible modela os sockets de escuta SIP (UDP/TCP 5060, TLS 9090) a partir do endereço do host do inventário e PLMN. O Ansible também modela os

aliases de host (`ims.…`, `icscf.ims.…`, `<host>.ims.…`) a partir desses valores.

`CAPTURE_NODE` é o alvo de captura do Homer, `sip:<homer_host>:9060`. O Ansible modela este valor apenas quando a captura do Homer está habilitada para a implantação. A captura do Homer precisa de `enable_homer` com um grupo de inventário `homer`. `CAPTURE_NODE` duplica a sinalização SIP para o Homer via HEP para rastreamento.

Configuração de pares Diameter

A tabela de pares Diameter do I-CSCF (`icscf.xml`) anuncia a aplicação **Cx** (`16777216`) em direção ao HSS. Todos os CSCFs compartilham a estrutura do arquivo e as variáveis do Ansible que a preenchem. Veja Diameter → Configuração de Pares (Implantação).

Solução de Problemas

Falhas de registro ou falhas de sessão de término surgem no I-CSCF. Essas falhas geralmente vêm de uma das duas causas:

- **Seleção / atribuição de S-CSCF.** O HSS pode retornar capacidades em vez de um nome de S-CSCF atribuído. A seleção então requer que o S-CSCF satisfaça todas as capacidades obrigatórias. Se nenhum candidato se qualificar, o I-CSCF recua para o URI de S-CSCF padrão configurado. Se um REGISTER encaminhado gerar um timeout ou 5xx/6xx, o I-CSCF falha para o próximo candidato até que a lista se esgote. Confirme que o conjunto de S-CSCF configurado e seus valores de capacidade correspondem ao que o HSS retorna.
- **Conectividade Cx com o HSS (UAR / LIR).** O I-CSCF não pode rotear sem uma resposta ao Cx UAR (no REGISTER) ou LIR (em um pedido de término). Uma resposta do HSS indisponível ou malformada gera **503**. Um usuário que é desconhecido ou não registrado gera **404**. Verifique se o par Cx para o HSS está ativo. Veja Operações Diameter.

Fluxos de Chamadas

Os diagramas de sequência aparecem com as funções que documentam:

- Registro via I-CSCF → Roteamento de registro (Cx UAR)
- Sessão de término via I-CSCF → Roteamento de término (Cx LIR)
- Failover do S-CSCF → Seleção de S-CSCF / correspondência de capacidades

Documentação Relacionada

- Operações e Referência do S-CSCF
- Operações
- Diameter
- Referência de Métricas
- OmniWeb - lista de S-CSCF, sessões ativas e estado do par Diameter Cx: <https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>

Operações e Referência do P-CSCF

O Proxy-CSCF é o ponto de entrada SIP do IMS para Equipamentos de Usuário. Cada REGISTER e cada sessão do UE chega aqui primeiro. O P-CSCF estabelece e aplica a associação de segurança de acesso que protege a sinalização do UE. O P-CSCF se insere no caminho de roteamento. Ele adiciona um cabeçalho Path na registro e um record-route nas sessões. Todo o tráfego subsequente então atravessa este nó. Esse tráfego inclui solicitações de terminação e mensagens em diálogo. O P-CSCF detecta a tecnologia de acesso do UE para direcionar a política de portadora de mídia. O P-CSCF também fornece ao ponto de entrada de sessão de emergência (E-CSCF) uma identidade de linha de chamada utilizável por meio da TS 23.167. O P-CSCF é um proxy de sinalização apenas. A mídia flui diretamente entre o UE e o lado de terminação. A mídia nunca flui através deste nó.

Funções do IMS

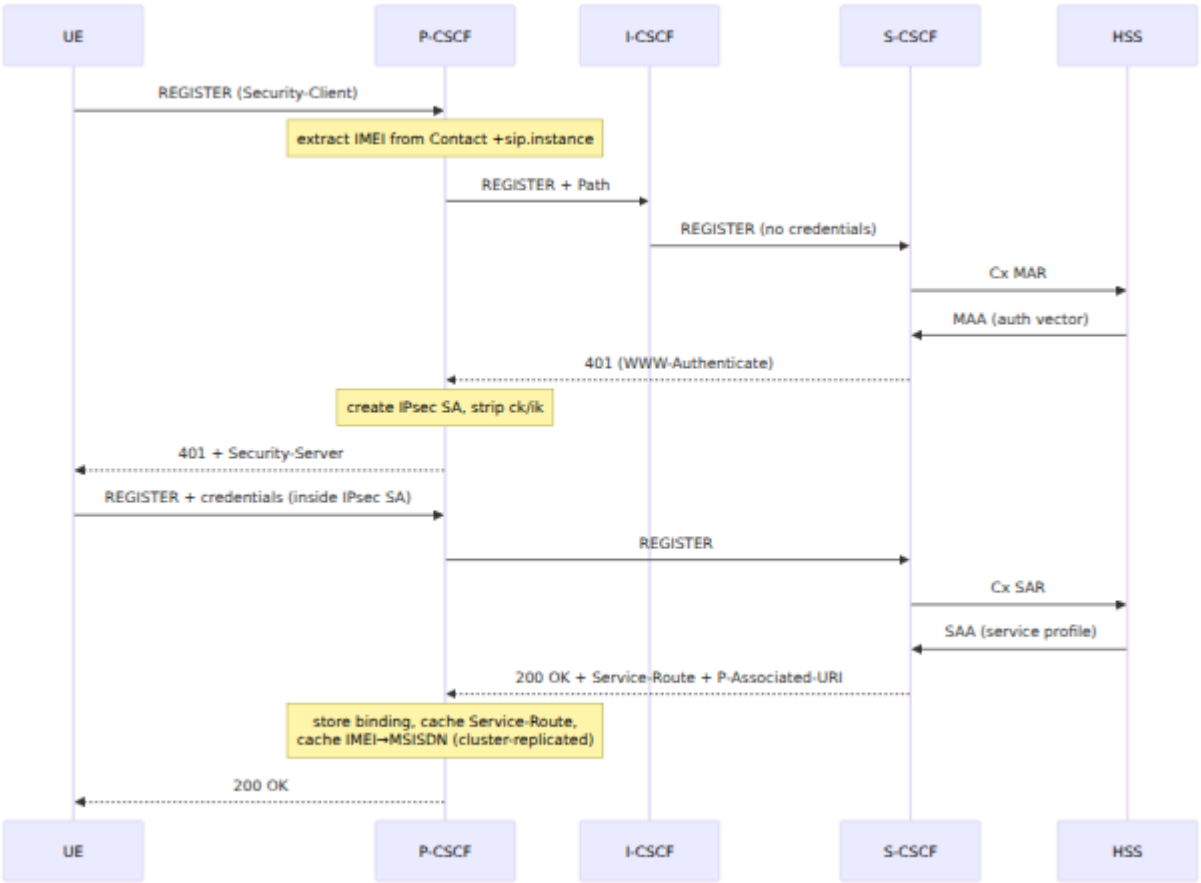
Proxy de Registro & Associação de Segurança IPsec

O P-CSCF é o proxy voltado para o registrador do UE. O P-CSCF retransmite o REGISTER em direção à rede doméstica (I-CSCF/S-CSCF). Na troca de desafio/resposta, o P-CSCF estabelece uma associação de segurança IPsec ESP com o UE. Isso faz parte do procedimento IMS-AKA. Durante o registro, o UE e o P-CSCF negociam os parâmetros da SA através dos cabeçalhos `Security-Client` / `Security-Server`. A partir do re-REGISTER autenticado, a SA transporta toda a sinalização para aquele UE.

No REGISTER encaminhado, o P-CSCF insere um cabeçalho **Path**. Isso roteia solicitações de terminação de volta através deste mesmo nó. O P-CSCF força a expiração do registro para um valor controlado pela rede. O P-CSCF anuncia suporte a `path`. No bem-sucedido `200 OK`, o P-CSCF armazena o vínculo de contato. O P-CSCF armazena em cache o `Service-Route` retornado e o `P-`

`Associated-URI`. Isso direciona solicitações subsequentes através do caminho correto da rede doméstica.

Cada UE registrado utiliza **uma** associação de segurança de um pool de recursos por implantação. O P-CSCF libera a SA quando o UE se desregistra (expiração 0) ou quando seu registro expira. O P-CSCF rejeita um REGISTER cujo Contato marca um registro de emergência (`;sos`). O P-CSCF lida com sessões de emergência diretamente no INVITE, não através do registro de emergência.



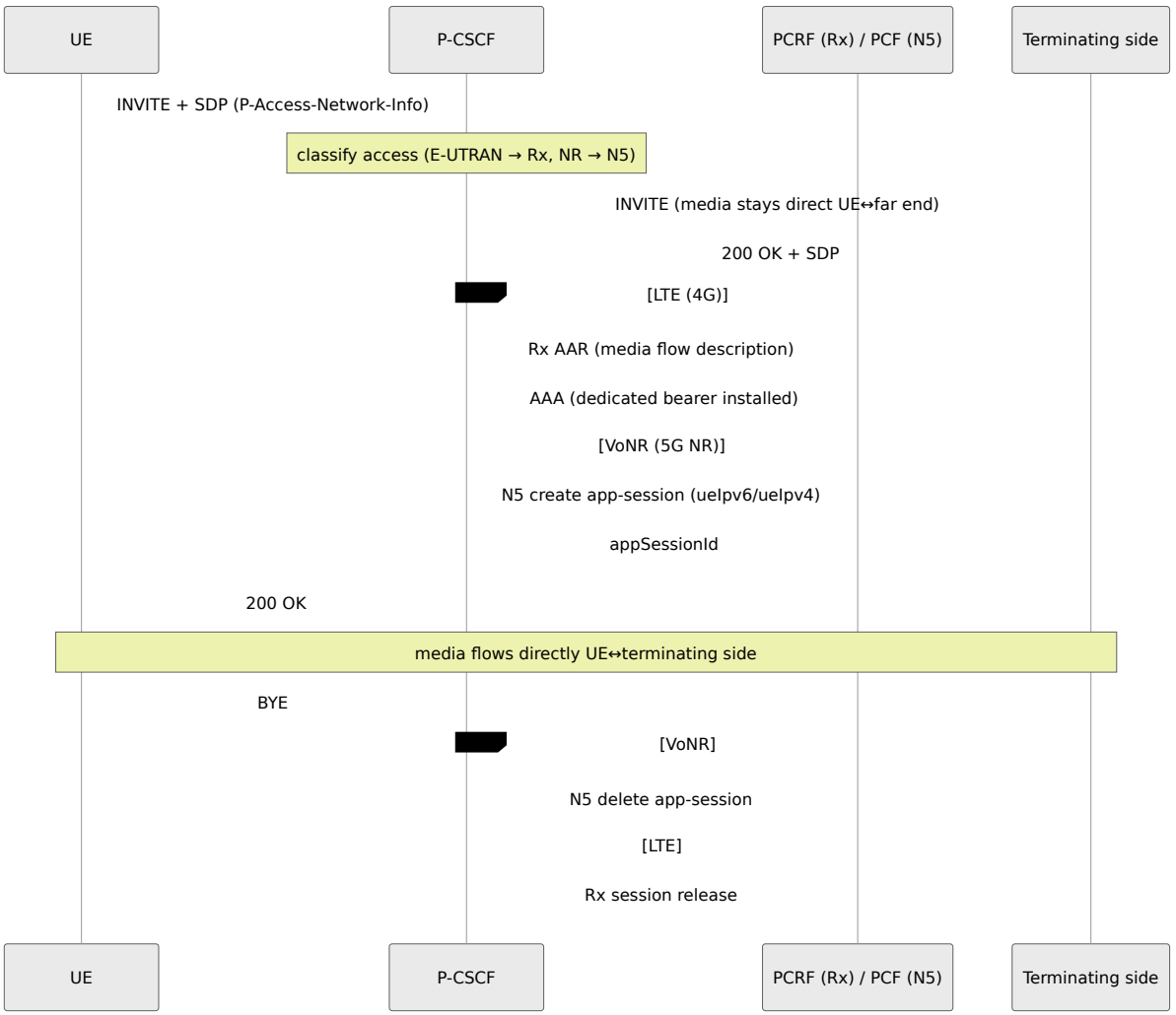
Detecção de Acesso & Controle de QoS / Política

O P-CSCF nunca retransmite mídia. O P-CSCF ainda autoriza a portadora de mídia dedicada com o plano de política. O P-CSCF classifica o acesso do UE a partir do cabeçalho `P-Access-Network-Info` (por TS 24.229 §5.2.6.3). LTE reporta `3GPP-E-UTRAN`. 5G NR reporta `3GPP-NR`. O acesso WiFi não tem portadora dedicada. O P-CSCF exclui o acesso WiFi do QoS dinâmico.

- **4G / LTE** - o P-CSCF autoriza o QoS da portadora de mídia sobre **Diameter Rx** para o PCRF. No lado da resposta (o `200 OK` carregando SDP), o P-CSCF emite uma Solicitação de Autorização/Autenticação (AAR). A AAR descreve o fluxo de mídia de áudio e o fluxo de mídia de vídeo, quando presente. O PCRF então instala a portadora dedicada correspondente. O P-CSCF atualiza a autorização em re-INVITEs em diálogo. O P-CSCF libera a autorização quando o diálogo termina.
- **VoNR (5G NR)** - o P-CSCF autoriza o QoS da portadora sobre a interface **N5** para o PCF. O P-CSCF utiliza o serviço `Npcf_PolicyAuthorization`. O P-CSCF atua como uma Função de Aplicação. Quando o lado remoto responde à mídia, o P-CSCF cria uma sessão de aplicação no PCF. Esta sessão utiliza afAppId `VoNR`, um componente de mídia `AUDIO` com status de fluxo `ENABLED`, e um descritor de fluxo para a mídia do UE. Também inclui um URI de notificação AF para o PCF retornar. O P-CSCF exclui essa sessão de aplicação quando o diálogo termina.

A autorização de QoS ocorre tanto nos lados de origem (MO) quanto de terminação (MT). Ela é baseada no próprio endereço IP do UE. **Vinculação de endereço do UE:** o P-CSCF codifica o endereço do UE para corresponder à vinculação de sessão PDU/portadora que o nó de política possui. O P-CSCF sinaliza um UE IPv6 como `ueIpv6` e um UE IPv4 como `ueIpv4`. Um endereço v6 colocado no campo v4 nunca corresponde à vinculação do PCF. O PCF então não instala nenhuma portadora dedicada.

Para VoNR, o P-CSCF localiza o PCF de serviço via **descoberta NRF**. O P-CSCF se registra como um AF. Para cada sessão, o P-CSCF resolve o PCF vinculado à sessão PDU do UE através da cadeia NRF→BSF. Este é o único caminho de descoberta do PCF.



Chamadas de Emergência (E-CSCF) & Identidade de Linha de Chamada - TS 23.167

O P-CSCF é o ponto de entrada de emergência. O P-CSCF detecta uma sessão de emergência pelo URN do serviço de emergência (`urn:service:sos`) no INVITE. O P-CSCF a roteia diretamente para o servidor de aplicação de emergência. Isso contorna a verificação normal de registro. Um INVITE de emergência frequentemente não carrega **MSISDN**. O P-CSCF, portanto, fornece uma identidade de linha de chamada utilizável para o PSAP. Isso se aplica mesmo para chamadores que são desconhecidos ou anônimos. Isso está em conformidade com o Anexo K da TS 23.167 e §4.4.6a da TS 29.214.

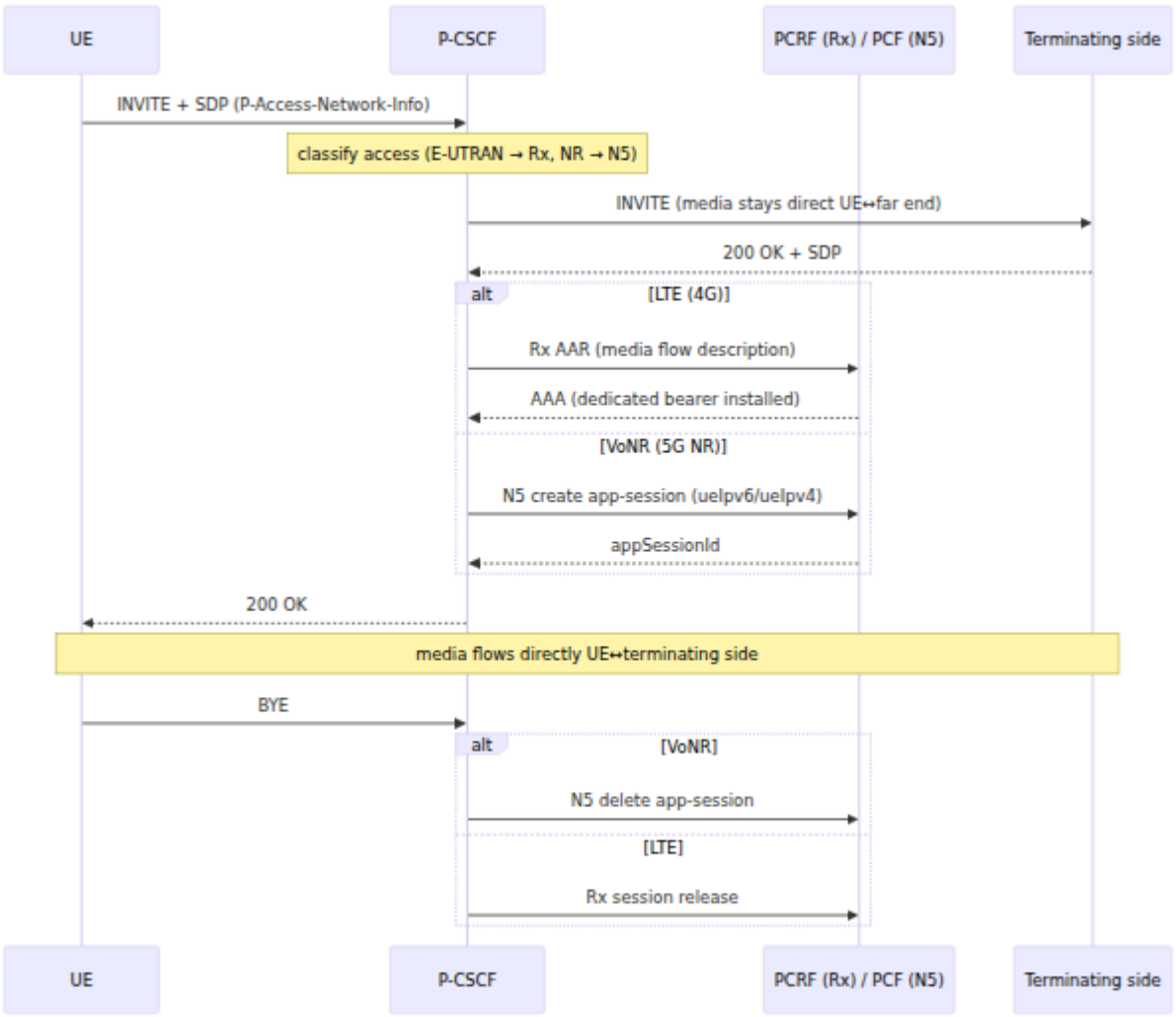
Dois mecanismos complementares resolvem a identidade:

1. **Vinculação IMEI→MSISDN em cache (caminho rápido).** Em cada REGISTER bem-sucedido, o P-CSCF armazena em cache uma vinculação. A

vinculação mapeia o IMEI do UE (do Contato `+sip.instance`) para o MSISDN (do `P-Associated-URI`). O P-CSCF **replica a vinculação entre todos os nós P-CSCF**. Qualquer nó pode então resolver a identidade, independentemente de onde o UE se registrou. No INVITE de emergência, o P-CSCF extrai o IMEI e procura o MSISDN em cache.

2. **Consulta de assinatura assíncrona (chamadores desconhecidos/anônimos).** Se nenhuma vinculação em cache existir, o P-CSCF emite uma consulta de assinatura assíncrona Rx para o PCRF. A consulta é baseada no endereço IP de origem do UE. O P-CSCF suspende o INVITE até que a resposta retorne. O PCRF retorna as identidades em nível EPC. O P-CSCF escolhe uma por precedência **MSISDN → IMSI → IMEISV**. O P-CSCF armazena em cache um resultado IMEISV para reutilização.

O P-CSCF afirma a identidade resolvida como o URI From do chamador e como um `P-Asserted-Identity` no domínio `sos.apn`. O P-CSCF restaura a identidade de forma consistente em respostas e solicitações em diálogo. O PSAP então vê uma identidade de retorno utilizável mesmo para um chamador originalmente anônimo. Qualquer que seja o caminho que resolva a identidade, o INVITE de emergência recebe o mesmo tratamento de mídia/QoS e cabeçalho que qualquer outra solicitação de origem. O P-CSCF então o encaminha para o servidor de aplicação de emergência.



Segurança / Anti-flood

O P-CSCF aplica proteção contra inundação baseada em origem. O P-CSCF limita a taxa de solicitações por IP de origem. O P-CSCF proíbe um IP que excede o limite de amostragem por um período de espera. O P-CSCF rastreia falhas de autenticação de registro por IP de origem em um contador de curta duração. O P-CSCF proíbe uma origem que excede o limite de tentativas falhadas dentro da janela. Isso derrota tentativas de adivinhação de credenciais. O P-CSCF descarta solicitações que um UE endereça ao próprio nó. O P-CSCF também descarta mensagens malformadas. Sob pressão de memória, o nó descarta novas solicitações com `503`.

Replicação de Cluster

O P-CSCF replica o estado relacionado ao registro e de emergência entre os nós P-CSCF. Em particular, o P-CSCF sincroniza a vinculação de emergência

IMEI→MSISDN entre os nós. O P-CSCF faz uma sincronização completa na inicialização. Qualquer nó no cluster pode então atender ao tráfego de terminação e resolver a identidade da chamada de emergência. Isso funciona independentemente de qual nó registrou originalmente o UE. O P-CSCF não precisa de provisionamento por nó.

Configuração de Implantação (Injetado pelo Ansible)

O Ansible renderiza a configuração de tempo de execução do P-CSCF e sua tabela de pares Diameter (`pcscf.xml`) no momento da implantação. A maioria dos valores deriva da identidade PLMN da rede (MCC/MNC) e do nome do host do inventário do nó. O Ansible emite os blocos 5G SBI e PCF apenas quando o inventário de implantação contém as funções de rede relevantes.

Identidade

Nome	O que controla	Valor / deriv
`NETWORKNAME`	Domínio IMS doméstico usado em `P-Visited-Network-ID` e reescritas de identidade	`ims.mnc<mnc>.mcc<mcc>.3gppnetwor`
`HOSTNAME`	FQDN deste nó (também seu alias de host)	`<inventory_hostname>.ims.mnc<mnc`
`URI`	O próprio URI SIP do P-CSCF	`sip:<hostname>:5060`
`PCSCF_URL`	URI de origem usado para pings de keepalive NAT	`sip:<hostname>:5060`
`PCSCF_USER_AGENT`	Cabeçalho `User-`	`User-Agent: Omnitouch Proxy-CSCF`

Nome	O que controla	Valor / deriv
	`Agent` que o nó emite	
`PCSCF_SERVER`	Cabeçalho `Server` que o nó emite	`Server: Omnitouch Proxy-CSCF <in`
`DMQ_NOTIFICATION_ADDR`	Endereço de notificação do cluster para replicação de estado entre nós P-CSCF	`sip:pcscf.ims.mnc<mnc>.mcc<mcc>.`

O Ansible modela os sockets de escuta SIP (UDP/TCP 5060, além de IPv6 5060 onde um endereço IPv6 é definido) e o socket HTTP do Prometheus (TCP 9090) a partir do endereço do host do inventário. O P-CSCF atende UEs em IPv6 onde disponível. Pares atrás dele permanecem IPv4. O Ansible também constrói o `PATH_HEADER` e o `P_VISITED_NETWORK_ID_HEADER` a partir do nome do host e do PLMN.

Controle de Política / Rx (4G)

Nome	O que controla	Valor / derivaçã
`RX_DEST_REALM`	Reino de destino Diameter para Rx em direção ao PCRF	`{{ diameter_realm }}`
`PCRF_REALM`	Reino do PCRF	`epc.mnc<mnc>.mcc<mcc>.3gpp`
`RX_AF_SIGNALING_IP`	IP de sinalização AF carregado na AAR Rx (este P-CSCF)	nó `ansible_host` (sobrescrev para double-NAT)
`RX_IMS_REG_DIALOG_DIRECTION`	Modo de direção de diálogo para registro Rx	`3`

Os parâmetros de mídia Rx fixos incluem autorização de vídeo ativada, uma largura de banda de áudio padrão/mínima de 64 kbit/s, inclusão de fluxo RTCP e uma duração máxima de sessão autorizada de 24 horas.

5G SBI / PCF (VoNR)

Emitido quando o inventário de implantação contém um PCF e um NRF.

Nome	O que controla	Valor / derivação
`VONR_AF_NOTIF_URI`	Endpoint de notificação AF que o PCF chama de volta	`http://<this host>:<pcscf_af_notif_port|9999>/af`
`NRF_URI`	URI base do NRF para registro e descoberta de AF	`http://<nrf host>:<nrf_sbi_port|7777>`
`IMS_NRF_NF_IPV4`	Este IPv4 NF do P-CSCF para seu registro AF	nó `ansible_host`
`IMS_NRF_PLMN_MCC` / `IMS_NRF_PLMN_MNC`	PLMN anunciado no registro/descoberta do NRF	a partir de `plmn_id`

Descoberta do PCF: o P-CSCF se registra no NRF como um AF. Para cada sessão VoNR, o P-CSCF resolve o PCF vinculado àquela sessão PDU do UE através da cadeia NRF→BSF. As sessões de aplicação sempre alcançam o PCF correto por assinante. Isso inclui núcleos 5G multi-PCF. Este é o único caminho de descoberta suportado.

Dimensionamento / Transporte

Nome	O que controla	Valor
`CAPTURE_NODE`	Alvo de captura SIP Homer (modelado apenas quando a captura Homer está habilitada)	`sip:<homer host>:9060`

A configuração base ajusta o número de processos de trabalho SIP (UDP) e o tamanho da tabela hash do registrador para a escala de implantação. UEs iOS

recebem um tempo de vida de conexão TCP encurtado para corresponder ao seu comportamento de transporte.

Configuração de pares Diameter

A tabela de pares Diameter do P-CSCF (`pcscf.xml`) anuncia a aplicação **Rx** (`16777236`) em direção ao PCRF. Todos os CSCFs compartilham a estrutura do arquivo e as variáveis do Ansible que a preenchem. Veja Diameter → Configuração de Pares (Implantação). Rx só está ativo quando `WITH_RX` é definido.

Solução de Problemas

Registro / Conectividade IPsec

Usuários que não conseguem se registrar ou que enfrentam timeouts de registro frequentemente apontam para a segurança de acesso do P-CSCF ou camada de descoberta, em vez da rede doméstica:

- **Estabelecimento de SA IPsec** - dispositivos móveis devem concluir a negociação `Security-Client` / `Security-Server` do IMS-AKA. Se o re-REGISTER autenticado nunca chegar dentro da SA, verifique duas coisas. Confirme que o UE e o P-CSCF concordaram sobre os parâmetros da SA. Confirme que nenhum middlebox remove os cabeçalhos de segurança.
- **Travessia NAT** - para dispositivos atrás de NAT, verifique o tratamento de NAT do lado remoto. Verifique se os pings de keepalive OPTIONS alcançam o UE. O furo para tráfego de terminação então permanece aberto.
- **Descoberta do P-CSCF** - verifique se o UE descobre o endereço correto do P-CSCF (via DNS, DHCP ou configuração estática). Verifique se os sockets de escuta SIP são acessíveis na rede de acesso.

Problemas de chamada de emergência

Sintomas: Chamadas de emergência não roteando para o PSAP, ou o PSAP não recebe uma identidade de linha de chamada (CLI) / número de retorno utilizável.

- **Detecção de emergência** - o P-CSCF roteia com base no URN do serviço de emergência (`urn:service:sos`), além dos números de emergência discados. Confirme que o INVITE carrega a indicação de emergência esperada. Confirme que o roteamento de emergência contorna a verificação normal de registro.
- **Resolução de CLI para chamadores anônimos/desconhecidos** - o P-CSCF fornece a identidade do chamador a partir da vinculação IMEI→MSISDN em cache (replicada em cluster, TTL de 4 horas). Para um chamador sem vinculação em cache, o P-CSCF recorre a uma consulta de assinatura assíncrona Rx para o PCRF. A consulta é baseada no endereço IP de origem do UE. O P-CSCF resolve uma identidade EPC por precedência **MSISDN → IMSI → IMEISV** (Anexo K da TS 23.167). Se o PSAP vê um chamador anônimo, verifique uma das duas coisas. Verifique se o P-CSCF armazenou em cache a vinculação no registro. Caso contrário, verifique se a consulta de assinatura Rx retornou uma identidade. O OmniWeb mostra o mapa de vinculação em cache.
- **Disponibilidade de localização** - verifique se as informações de localização estão disponíveis para E911/E112. Verifique se o lado de recuperação de localização (LRF) é acessível.
- **Teste de roteamento** - você pode exercitar o roteamento de chamadas de emergência sem uma conexão real com o PSAP. Isso confirma a detecção, a afirmação de identidade no domínio `sos.apn` e o roteamento para o servidor de aplicação de emergência.

As sessões de emergência têm sucesso mesmo para usuários não registrados, usuários sem SIM ou credenciais inválidas, e usuários em roaming. Veja Chamadas de Emergência (E-CSCF) & Identidade de Linha de Chamada - TS 23.167 para o mecanismo subjacente.

Fluxos de Chamadas

Os diagramas de sequência aparecem com as funções que documentam. As escadas de sessão completas aparecem abaixo:

- Registro & SA IPsec → Proxy de Registro & Associação de Segurança IPsec

- QoS de Mídia / Política (MO & MT) → Detecção de Acesso & Controle de QoS / Política
- Sessão de Emergência → Chamadas de Emergência (E-CSCF) & Identidade de Linha de Chamada - TS 23.167

Chamada de Origem Móvel (MO)

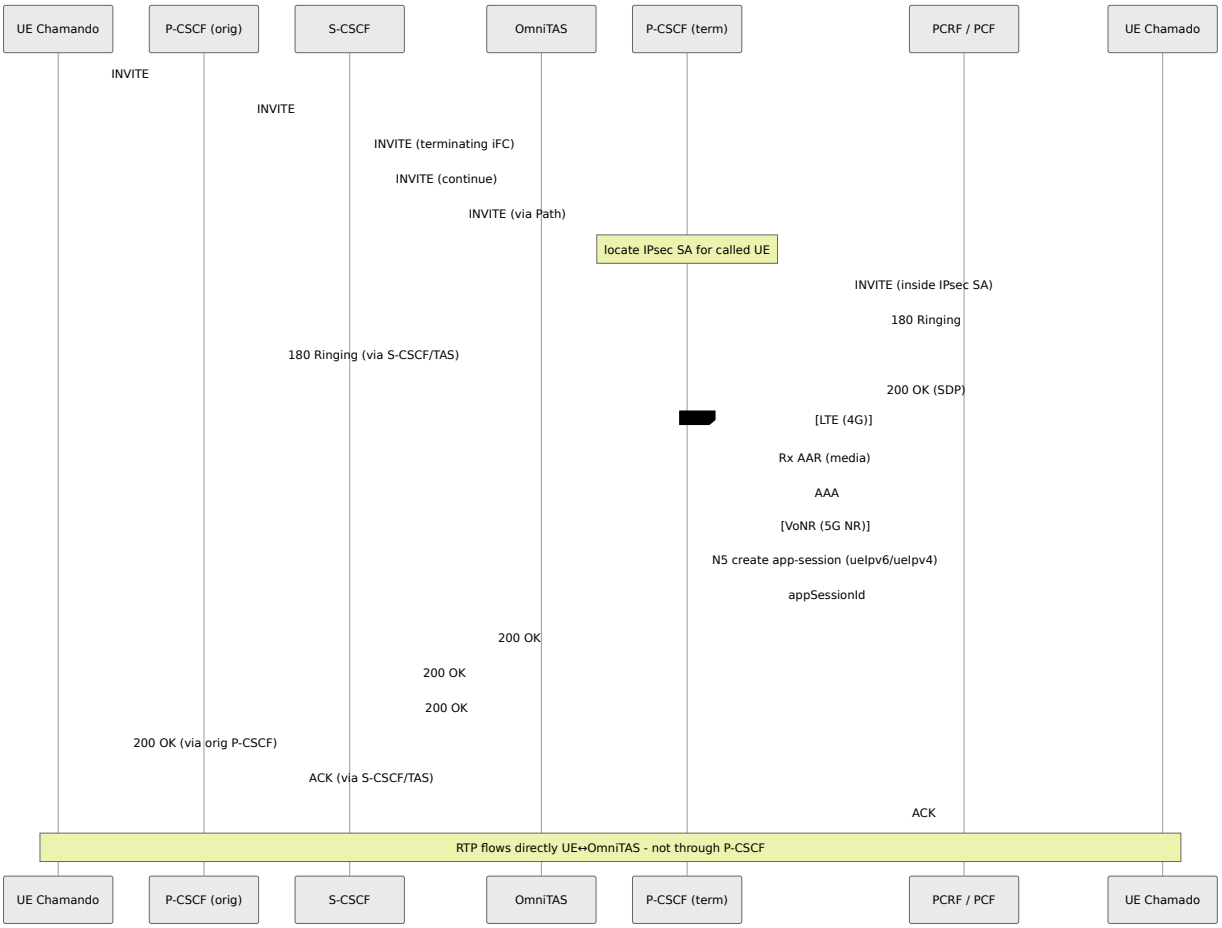
O P-CSCF roteia chamadas de origem através do S-CSCF (via o Service-Route em cache) para o TAS para lógica de serviço e cobrança. A mídia permanece direta.

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'

Tentar novamente

Chamada de Terminação Móvel (MT)

Chamadas de terminação chegam de volta através do P-CSCF registrado no Path durante o registro. O P-CSCF autoriza o QoS quando o UE chamado responde.



Documentação Relacionada

- Operações
- Diameter
- Interface Baseada em Serviço (SBI)
- Referência de Métricas
- OmniWeb - contatos registrados, tabelas hash (incluindo o mapa de emergência IMEI→MSISDN), descoberta NRF/PCF e estado de pares Rx: <https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>

Guia de Operações do 5G SBI

Índice

1. Visão Geral
2. SBI na Arquitetura IMS
3. N5 - Npcf_PolicyAuthorization (P-CSCF → PCF)
4. Nnrf - Gerenciamento e Descoberta de NF (P-CSCF ↔ NRF)
5. Quando o SBI é Usado vs Diameter
6. Configuração
7. Gerenciamento via OmniWeb
8. Problemas Comuns
9. Documentação Relacionada

Visão Geral

O núcleo 5G é **baseado em serviços**. As funções de rede expõem APIs REST HTTP/2 e JSON umas às outras através da Interface Baseada em Serviços (SBI). O SBI substitui o Diameter. Para VoNR (Voz sobre Nova Rádio), o P-CSCF atua como uma **Função de Aplicação (AF)** 5G. O P-CSCF usa o SBI para autorizar a QoS de mídia. O P-CSCF também usa o SBI para descobrir as funções de rede que precisa.

O SBI substitui o caminho Diameter Rx usado para VoLTE. Veja Operações Diameter para o lado 4G/LTE.

O que é SBI?

A Interface Baseada em Serviços (3GPP TS 29.500) difere do Diameter das seguintes maneiras:

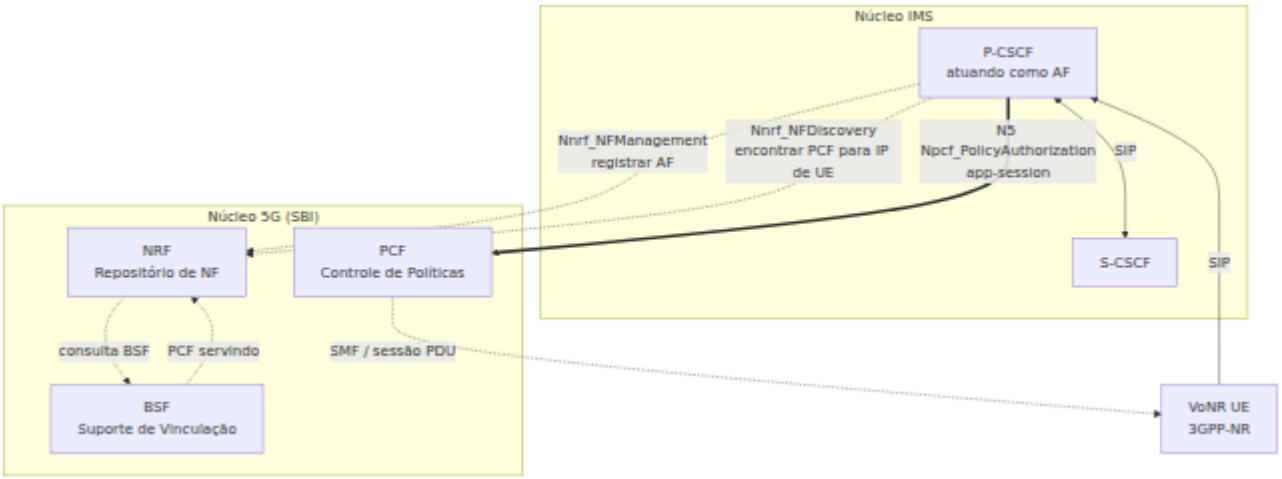
- **Transporte**: HTTP/2 sobre TCP. O Diameter usa TCP ou SCTP.
- **Codificação**: cargas JSON descritas pelo OpenAPI. O Diameter usa AVPs.
- **Modelo**: recursos RESTful. Você cria, modifica ou exclui um recurso *app-session*. O Diameter usa pares de comandos de solicitação e resposta.
- **Descoberta**: o **NRF** encontra produtores dinamicamente. O Diameter usa pares configurados estaticamente.
- **Nomeação**: os serviços usam o nome `Nxxx` (por exemplo `Npcf_PolicyAuthorization`, `Nnrf_NFDiscovery`)

SBI no CSCF

O P-CSCF é o único componente CSCF que usa o SBI. Como uma Função de Aplicação (AF) 5G, o P-CSCF autoriza a QoS de mídia VoNR sobre N5 para o PCF. Quando a descoberta NRF está habilitada, o P-CSCF se registra no NRF e consulta o NRF.

Função	Serviço	Transporte	Conectado a	Propósit
AF	Npcf_PolicyAuthorization (N5)	HTTP/2	PCF	Autorizar mídia VoNR e QoS. Cria uma app-session.
NF (AF)	Nnrf_NFManagement	HTTP/2	NRF	Registrar o P-CSCF como um instância AF (opcional
NF (AF)	Nnrf_NFDiscovery	HTTP/2	NRF → BSF	Descobrir o PCF vinculado a uma sessão PDU de U (opcional

SBI na Arquitetura IMS



Para VoNR, o P-CSCF detecta o acesso 5G. O P-CSCF descobre o PCF servindo através da cadeia NRF→BSF. O P-CSCF então POSTa uma app-session de autorização de política para esse PCF. Esta app-session reserva a QoS do portador de voz.

N5 - Npcf_PolicyAuthorization (P-CSCF → PCF)

O ponto de referência **N5** transporta o serviço `Npcf_PolicyAuthorization`. Em uma chamada VoNR, o P-CSCF cria um recurso *app-session* no PCF. A app-session descreve a mídia que a sessão precisa. O PCF então instala a QoS correta na sessão PDU 5G do UE.

Solicitação de app-session

O P-CSCF POSTa um objeto `ascReqData` para a coleção de app-sessions do PCF. A coleção padrão é `http://<pcf>/npcf-policyauthorization/v1/app-sessions`. O objeto contém os seguintes campos:

Campo	Valor	Notas
`notifUri`	URI de notificação AF	O endereço onde o PCF envia notificações de eventos de app-session. Este é o endpoint de notificação AF configurado.
`suppFeat`	`3f`	Bitmap de recursos suportados
`ueIpv4` / `ueIpv6`	IP de origem do UE	**Deve corresponder à família de endereços** que o PCF vinculou à sessão PDU do SMF
`afAppId`	`VoNR`	Identificador da aplicação
`medComponents`	componente de mídia de áudio	`mediaType: AUDIO`, `fStatus: ENABLED`, com uma descrição de fluxo (`permit out 17 from <ue-ip> to any`)

> **Dica operacional - família de endereços.** O PCF vincula a app-session à sessão PDU do SMF pelo endereço IP do UE. Você deve codificar um UE em uma sessão PDU IPv6 como `ueIpv6`. Um endereço v6 em `ueIpv4` nunca corresponde. Um endereço v4 em `ueIpv6` nunca corresponde. Nesses casos, o PCF rejeita a autorização ou descarta a autorização silenciosamente. O P-CSCF seleciona `ueIpv6` ou `ueIpv4` automaticamente a partir do endereço de origem SIP.

Ciclo de Vida

- **Criar** - o P-CSCF POSTa a app-session quando processa o INVITE VoNR ou mídia inicial.
- **Notificar** - o PCF chama de volta para `notifUri` para eventos de sessão.
- **Excluir** - o P-CSCF encerra a app-session quando o diálogo termina. Isso libera a QoS reservada.

O Diameter Rx usa `Rx_AAR` e `Rx_STR`. O N5 não possui conexão de par persistente. Cada app-session é uma transação HTTP/2 independente para o PCF descoberto para aquele UE.

Nnrf - Gerenciamento e Descoberta de NF (P-CSCF ↔ NRF)

O P-CSCF usa a descoberta NRF para encontrar o PCF para cada sessão VoNR. A descoberta NRF é o único caminho de descoberta do PCF.

Registro de NF (Nnrf_NFManagement)

O P-CSCF se registra como uma instância AF no NRF. O P-CSCF usa uma identidade de instância estável por host. Uma reinicialização reutiliza um registro. Isso impede que o NRF acumule registros AF obsoletos.

Descoberta do PCF (Nnrf_NFDiscovery)

Para uma sessão VoNR, o P-CSCF consulta o NRF com o IP de origem do UE. Esta consulta descobre o PCF que atende aquela sessão PDU do UE. A cadeia **NRF → BSF** resolve a consulta. O BSF mantém a vinculação de UE-IP ao PCF servindo. O endpoint descoberto se torna o alvo N5. Se o P-CSCF não encontrar uma vinculação, ele pula a QoS dinâmica para aquela chamada. A sessão então prossegue sem uma reserva de portador dedicada.

Quando o SBI é Usado vs Diameter

O P-CSCF deriva o tipo de acesso do cabeçalho `P-Access-Network-Info` (conforme TS 24.229 §5.2.6.3). O LTE relata `3GPP-E-UTRAN`. O 5G NR relata `3GPP-NR`. O P-CSCF exclui WiFi (`3GPP-IEEE-802.11`) porque o WiFi não possui portadores dedicados.

Acesso	`P-Access-Network-Info`	Caminho QoS	Par
5G NR (VoNR)	`3GPP-NR`	**N5 SBI** (`Npcf_PolicyAuthorization`)	PCF
LTE (VoLTE)	`3GPP-E-UTRAN`	**Diameter Rx**	PCRF
WiFi	`3GPP-IEEE-802.11`	nenhum (sem portador dedicado)	-

O P-CSCF descobre o PCF para o caminho N5 por sessão. Ele usa a cadeia NRF → BSF → PCF servindo.

Configuração

A ferramenta de implantação provisiona o comportamento do SBI por implantação. Não edite o comportamento do SBI manualmente. As configurações relevantes são:

Configuração	Propósito
Endpoint de notificação AF	A URL de callback que o P-CSCF anuncia ao PCF para notificações de eventos de app-session
Endpoint NRF	O endereço NRF para registro de AF e descoberta de PCF
Identidade do PLMN doméstico (MCC / MNC)	A identidade da rede doméstica que o P-CSCF apresenta ao NRF
Identidade da instância AF	Uma identidade estável por host para registro no NRF. Uma reinicialização reutiliza um único registro.

OmniWeb mostra o estado de registro NRF ao vivo. OmniWeb também mostra as vinculações de PCF descobertas por sessão. Veja abaixo.

Gerenciamento via OmniWeb

Omnitouch removeu o painel de controle web embutido. A aba **NRF** da página OmniWeb P-CSCF mostra o estado de registro do NRF, as vinculações de PCF descobertas e o status 5G/N5. Veja a documentação do OmniWeb.

Problemas Comuns

Sintoma	Causa provável	Ação
Nenhuma vinculação de PCF encontrada para o UE (registrado na configuração da chamada)	O NRF ou BSF ainda não tem vinculação para a sessão PDU do UE. Ou o IP do UE difere do âncora da sessão.	Confirme que a sessão PDU do UE está estabelecida. Confirme que o BSF mantém a vinculação. A chamada prossegue sem QoS dinâmica.
PCF rejeita ou ignora a app-session	O IP do UE está codificado na família errada (`ueIpv4` vs `ueIpv6`)	Verifique se a família de endereço de origem SIP corresponde à sessão PDU. Veja a dica sobre família de endereços acima.
Registros AF obsoletos se acumulam no NRF	A identidade da instância AF não é estável entre reinicializações	Torne a identidade da instância AF por host estável
Nenhum tráfego N5 para uma chamada 5G	O P-CSCF não detecta o acesso como `3GPP-NR`. Ou o NRF está inacessível, então o P-CSCF não descobre nenhum PCF.	Verifique `P-Access-Network-Info`. Verifique se o endpoint NRF é acessível.
Chamada VoNR é configurada, mas sem portador dedicado	O P-CSCF não criou a app-session porque a descoberta falhou. Ou o P-CSCF encerrou a app-session precocemente.	Correlacione o POST N5 do P-CSCF com o PCF. Verifique a conectividade HTTP/2 e os timeouts.

Documentação Relacionada

- Operações Diameter - as interfaces Diameter Rx, Cx e Ro usadas para VoLTE (4G/LTE)
- Operações do P-CSCF - Detecção de acesso VoNR, QoS N5 e descoberta NRF em contexto
- Referência de Métricas - métricas do P-CSCF
- Documentação do OmniWeb - status do NRF e 5G no portal de gerenciamento

Operações e Referência do S-CSCF

O Serving-CSCF é o registrador SIP da rede doméstica e o ponto de controle de sessão do IMS. Ele autentica assinantes contra o HSS via Cx (MAR/SAR). Ele armazena o vínculo de registro. Ele baixa o perfil de serviço do assinante (Critérios de Filtro Iniciais). Ele está na rota de sinalização para cada sessão de origem e término. A partir dessa posição, ele aciona Servidores de Aplicação através da interface ISC, afirma a identidade do chamador e roteia a sessão em direção ao lado de término, a um Servidor de Aplicação ou à PSTN. O HSS registra o nome deste S-CSCF para o assinante. Portanto, todo o tráfego subsequente para esse usuário passa por este nó.

Funções do IMS

Registro e autenticação

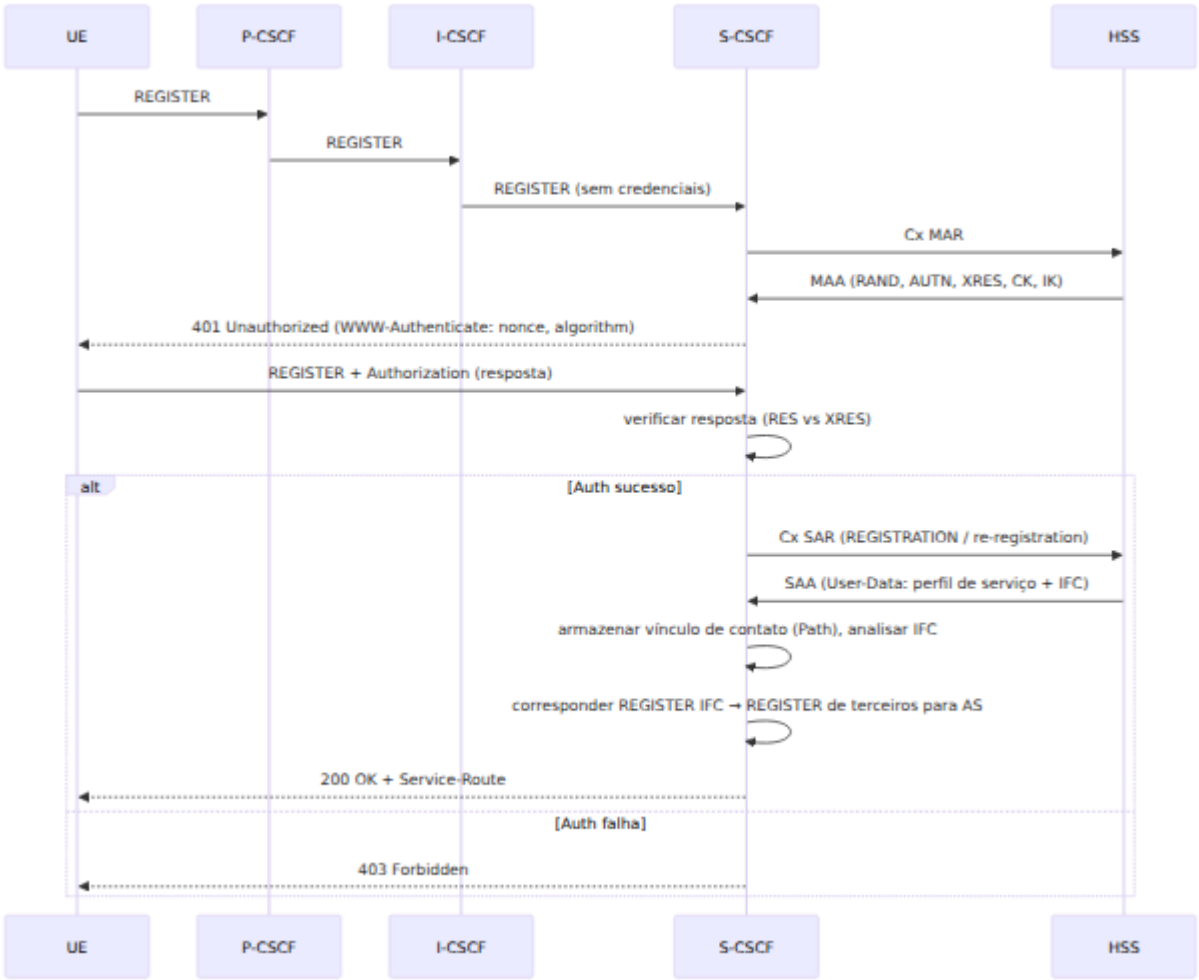
O S-CSCF é o registrador autoritativo. Ele desafia o UE. Ele valida a resposta contra um vetor de autenticação Cx do HSS. Em caso de sucesso, ele registra o vínculo de contato e baixa o perfil de serviço do assinante.

O registro procede da seguinte forma:

1. **Seleção do algoritmo.** O S-CSCF desafia com o algoritmo que o UE oferece em seu cabeçalho Authorization. Se o UE não oferecer nenhum algoritmo, o S-CSCF usa o SIP Digest (MD5) por padrão. O SIP Digest acomoda softphones não-IMS. Por padrão, o S-CSCF autentica cada REGISTER.
2. **Desafio (MAR).** O S-CSCF recebe um REGISTER sem credenciais. Ele solicita um vetor de autenticação ao HSS com um Cx Multimedia-Auth-Request. O HSS retorna o vetor na resposta (para AKA: RAND, AUTN, XRES, CK, IK). O S-CSCF responde **401 Unauthorized** com um cabeçalho `WWW-Authenticate`. Este cabeçalho carrega o nonce (derivado de RAND) e o algoritmo selecionado. Se o HSS rejeitar a identidade, o registro falha **403**.

Se o HSS estiver indisponível ou retornar uma resposta malformada, o registro falha **503**.

3. **Verificação.** O UE reenvia o REGISTER com sua resposta calculada. O S-CSCF verifica a resposta em relação ao vetor armazenado. Ele corresponde à identidade pública.
4. **Re-sincronização.** Se o UE relatar uma discrepância no número de sequência (SQN), o S-CSCF encaminha o token AUTS ao HSS para re-sincronizar. Então, o S-CSCF re-desafia com vetores novos.
5. **Atribuição de servidor (SAR).** Após a autenticação bem-sucedida, o S-CSCF envia um Cx Server-Assignment-Request. O tipo de atribuição é REGISTRATION na primeira inscrição, ou re-inscrição em um refresh. A resposta retorna os Dados do Usuário do assinante (perfil de serviço e IFC). O S-CSCF mantém os Dados do Usuário na memória. Uma atribuição rejeitada, ou um assinante sem perfil de serviço IMS, falha **403**. Um timeout do HSS falha **503**.
6. **Vínculo e Service-Route.** O S-CSCF armazena o vínculo de contato juntamente com o caminho P-CSCF. O caminho permite que as solicitações de término sejam roteadas de volta através do mesmo P-CSCF. O 200 OK carrega um Service-Route, então o UE envia solicitações subsequentes através deste S-CSCF. O S-CSCF mantém um contato por identidade pública. Um novo vínculo substitui o anterior. O prazo de expiração é fixo em 599 segundos.
7. **Registro de terceiros / reg-event.** O S-CSCF também avalia o registro contra os Critérios de Filtro Iniciais acionados pelo REGISTER. Essa avaliação dispara REGISTERs de terceiros para qualquer Servidor de Aplicação correspondente. O pacote de evento de registro notifica entidades inscritas sobre o estado do registro. O S-CSCF encerra a assinatura na desinscrição.



Acionamento de serviço via IFC (ISC)

O S-CSCF avalia cada solicitação inicial contra os **Critérios de Filtro Iniciais** baixados do assinante. Cada IFC tem um Ponto de Acionamento priorizado, um endereço de Servidor de Aplicação e um valor de Tratamento Padrão. O Ponto de Acionamento é uma combinação booleana de Gatilhos de Ponto de Serviço (método, Request-URI, cabeçalho SIP, Caso de Sessão, SDP). O valor de Tratamento Padrão é sessão-continuada ou sessão-terminada em caso de falha do AS. O Ponto de Acionamento usa forma normal conjuntiva ou disjuntiva. Você pode agrupar e negar os gatilhos individuais.

O S-CSCF percorre o perfil em ordem de prioridade para o caso de sessão relevante. Ao encontrar uma correspondência, ele encaminha a solicitação para o Servidor de Aplicação via ISC. O S-CSCF marca a solicitação com um **Identificador de Diálogo Original (ODI)**. Ele também insere um cabeçalho **P-Served-User** (RFC 5502) que identifica o assinante atendido e o caso de sessão. Essas marcas permitem que o AS retorne a solicitação ao ponto na

cadeia de onde saiu. Quando o AS roteia a solicitação de volta, o S-CSCF reconhece o ODI. Então, ele retoma a avaliação do IFC após o último critério correspondente, em vez de reiniciar.

O Tratamento Padrão governa o comportamento em caso de falha do AS. O Servidor de Aplicação retorna um 408 ou 5xx. O S-CSCF então continua para o próximo critério (sessão-continuada) ou abandona o trecho, conforme especificado pelo IFC.

Manipulação de chamadas de origem

Uma solicitação é **de origem** quando chega com o indicador de origem em seu cabeçalho Route superior, ou quando retorna de um Servidor de Aplicação de origem. O S-CSCF então:

- Atribui o contexto de diálogo de origem e registra rotas, para que reconheça solicitações em diálogo como o trecho de origem.
- **Afirma a identidade.** A solicitação não retorna de um AS. O S-CSCF remove qualquer `P-Asserted-Identity` fornecido pelo cliente. Ele substitui a identidade pela identidade que autenticou no registro. Esta é a identidade de linha de chamada autenticada para o trecho.
- Avalia o IFC de origem e encaminha correspondências para o Servidor de Aplicação via ISC.
- **Normalização de número.** Um Request-URI carrega um `phone-context`. O S-CSCF reescreve o Request-URI para um URI `tel:` no phone-context da rede doméstica antes de roteá-lo.
- **PSTN / ENUM.** Para destinos E.164, o S-CSCF resolve o número via ENUM. Em um erro de ENUM, o S-CSCF envia a chamada para os gateways de saída da PSTN, com failover através do conjunto de gateways. Se a solicitação carregar uma indicação de Função de Trânsito e Roaming (`Feature-Caps: +g.3gpp.trf`), o S-CSCF a roteia para esse TRF em vez disso.
- **Vetor de cobrança.** Chamadas de origem carregam um `P-Charging-Vector` para correlação de cobrança entre operadores.
- Se a cobrança online estiver habilitada, o S-CSCF envia uma solicitação de controle de crédito antes que a chamada prossiga (veja Cobrança).

O S-CSCF encaminha destinos não-PSTN em direção ao lado de término. Se este mesmo S-CSCF atender o usuário de término, o manuseio de término continua localmente.

Parse error on line 15: ...ornado; retomar IFC) end opt Co ----------^
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'

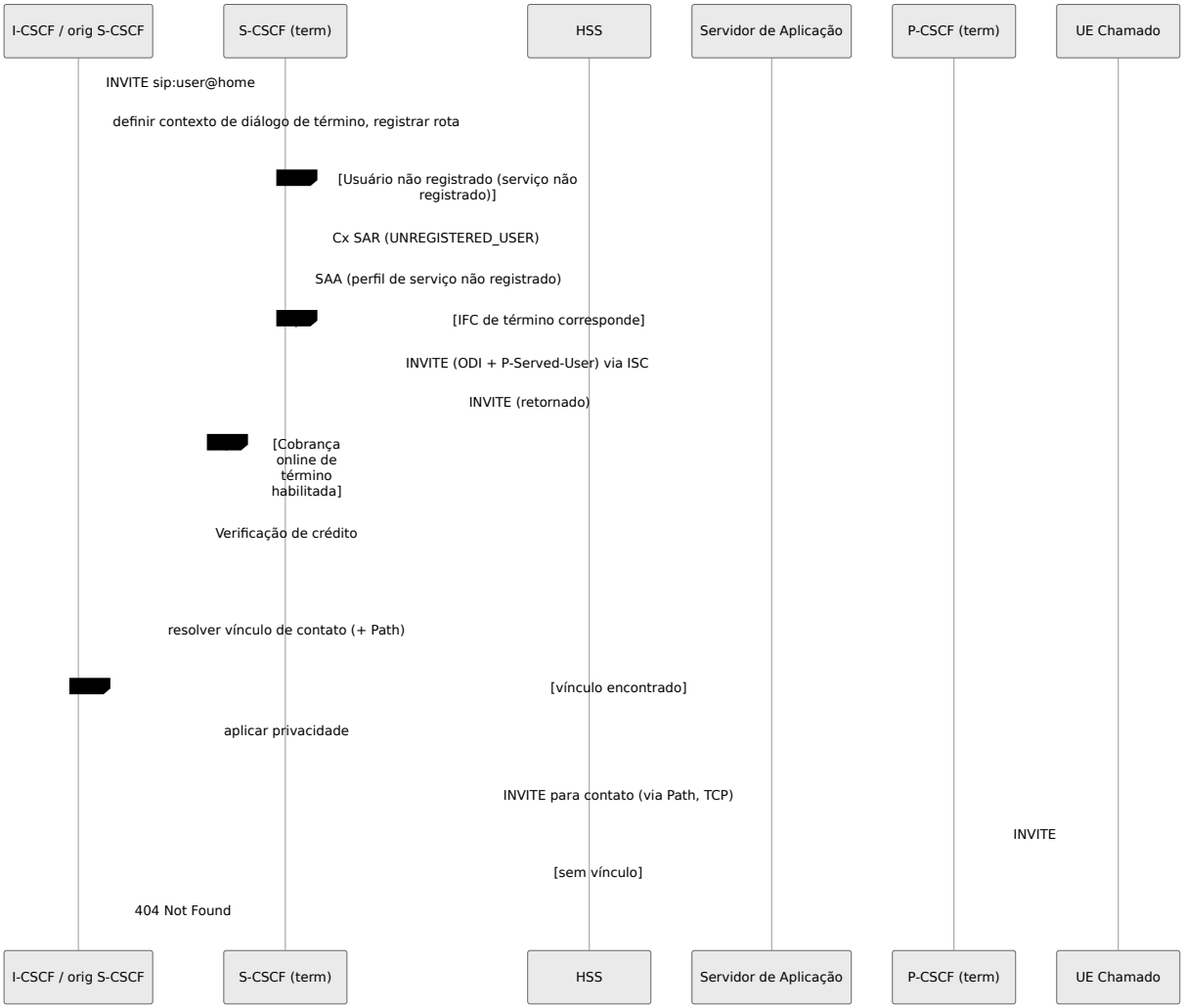
Tentar novamente

Manipulação de chamadas de término

Uma solicitação é **de término** quando seu Request-URI é uma identidade atendida localmente. O S-CSCF então:

1. Atribui o contexto de diálogo de término e registra rotas, para que reconheça solicitações em diálogo como o trecho de término.
2. Restaura o Request-URI original. Para métodos não-INVITE, ele avalia o IFC de término e encaminha correspondências para o Servidor de Aplicação via ISC. Para INVITEs, o encaminhamento do IFC segue o ciclo de retorno do AS.
3. Se a cobrança online de término estiver habilitada, o S-CSCF envia uma solicitação de controle de crédito do lado de término antes de prosseguir.
4. **Resolução de localização.** O S-CSCF recupera o vínculo de contato do usuário atendido. Ele encaminha a solicitação para esse contato via o P-CSCF registrado no Path durante o registro. Se o usuário não tiver vínculo, o S-CSCF retorna um **404 Not Found**.
5. O S-CSCF recebe um INVITE para uma identidade que **não está atualmente registrada**. Primeiro, ele busca o perfil de serviço não registrado no HSS com um Cx Server-Assignment-Request do tipo UNREGISTERED_USER. Isso permite que serviços não registrados de término sejam executados (por exemplo, correio de voz). Um timeout do HSS falha **503**. Um perfil ausente falha **403**.

O S-CSCF aplica privacidade na saída. Se a solicitação afirmar `Privacy: id`, o S-CSCF remove o `P-Asserted-Identity` antes que a mensagem deixe o S-CSCF.



Cobrança (opcional)

A cobrança online via Diameter **Ro** para um OCS é opcional. Você a habilita por implantação (veja as flags de cobrança abaixo). Quando habilitada, o S-CSCF envia uma solicitação de controle de crédito antes de permitir um INVITE. O S-CSCF mapeia a resposta para respostas SIP (por exemplo, fundos insuficientes → 402, limite de crédito atingido → 486, assinante de cobrança desconhecido → 403). O Service-Context-Id identifica o serviço cobrado. O S-CSCF monta esse identificador a partir dos parâmetros de cobrança listados na referência de configuração.

Na produção, isso é normalmente **desabilitado**. O TAS realiza a cobrança em vez disso. O TAS contabiliza corretamente os serviços suplementares (encaminhamento, transferência, trechos de roaming) que o S-CSCF não pode observar de ponta a ponta. Trate a cobrança Ro do S-CSCF como uma capacidade opcional, não como um padrão.

Presença / reg-event

O S-CSCF não atua como um servidor de presença geral. O S-CSCF aceita solicitações `SUBSCRIBE` de evento de registro (`Event: reg`) (200 OK). O S-CSCF não serve assinaturas de presença geral. O S-CSCF aceita um `PUBLISH` de evento de registro apenas de um usuário registrado. Tal PUBLISH atualiza o estado de registro publicado. Caso contrário, o S-CSCF o rejeita **403**. Esta configuração não possui manipulação de presença de disponibilidade do usuário (PIDF).

Configuração de Implantação (Injetada pelo Ansible)

O Ansible renderiza a configuração de tempo de execução do S-CSCF e sua tabela de pares Diameter (`scscf.xml`) no momento da implantação. Os valores abaixo derivam da identidade PLMN da rede (MCC/MNC) e do nome do host do inventário do nó.

Identidade / domínio

Nome	O que controla	Valor / derivaç
`NETWORKNAME`	Domínio IMS doméstico. É o domínio de destino Cx e o `phone-context` usado na normalização de números	`ims.mnc<mnc>.mcc<mcc>.3gppnetwork.o`
`HOSTNAME`	O FQDN deste nó (alias do host, e origin-host Diameter quando Ro está habilitado)	`<inventory_hostname>.ims.mnc<mnc>.m`
`URI`	O próprio URI SIP do S-CSCF. É a identidade de registrador e autenticação	`sip:<hostname>:5060`
`SCSCF_USER_AGENT`	O cabeçalho `User-Agent` que o nó emite	`User-Agent: Omnitouch S-CSCF <inven`

Nome	O que controla	Valor / derivaç
`ISC_MY_URI`	Token do host que identifica as próprias rotas ODI deste S-CSCF quando um AS retorna uma solicitação	`<inventory_hostname>`
`ENUM_SUFFIX`	Sufixo de domínio ENUM para resolução de E.164→URI de números destinados à PSTN	`mnc<mnc>.mcc<mcc>.3gppnetwork.org.`

O Ansible template os sockets de escuta SIP (UDP/TCP 5060, TLS 9090) e aliases de host a partir do endereço do host do inventário e PLMN.

Autenticação - `REG_AUTH_DEFAULT_ALG`

O algoritmo de autenticação padrão que o S-CSCF aplica quando deve escolher um, em vez de ecoar o algoritmo que o UE solicita. Opções:

Valor	Significado / quando usar
`AKAv1-MD5`	3GPP IMS-AKA (TS 33.203). Padrão para USIM/ISIM VoLTE/VoNR com SAs IPsec. Use para assinantes móveis normais.
`AKAv2-MD5`	Variante aprimorada do IMS-AKA. Use apenas onde UEs e HSS negociam especificamente AKAv2.
`MD5`	SIP HTTP Digest simples (sem AKA, sem IPsec). Use para clientes não-IMS / softphone que não podem fazer AKA.
`CableLabs-Digest`	Perfil de digestão PacketCable/CableLabs. Implantações de rede a cabo.
`3GPP-Digest`	3GPP SIP Digest (TS 33.203 Anexo N). Baseado em senha, sem ISIM. Assinantes de linha fixa / não-UICC.
`TISPAN-HTTP_DIGEST_MD5`	Perfil ETSI TISPAN NASS/HTTP-Digest. Assinantes de banda larga fixa TISPAN.
`HSS-Selected`	**Padrão.** O S-CSCF não impõe nenhum algoritmo. O HSS retorna o esquema por assinante na resposta de autenticação. Use isso para que o S-CSCF desafie cada assinante com o que o HSS provisionou (AKA para móveis, Digest para fixos, etc.).

O algoritmo não altera os seguintes padrões. O S-CSCF autentica cada REGISTER por padrão (veja `WITH_AUTH`). O domínio de destino Cx é o domínio da rede doméstica (`NETWORKNAME`). O S-CSCF corresponde vetores de autenticação na identidade pública. Os vetores expiram após 599 s.

Cobrança (Ro) - flags e par

Nome	O que controla	Valores
`WITH_RO`	Habilitar controle de crédito Diameter Ro de origem antes de um INVITE de saída	definir / undef (padrão: undef)
`WITH_RO_TERM`	Habilitar controle de crédito Diameter Ro do lado de término	definir / undef (padrão: undef)
`RO_DESTINATION`	Host de destino Diameter OCS (o domínio de destino é o domínio da rede doméstica)	FQDN do OCS, por exemplo, `hssocs.voiceblue.com`
`RO_FORCED_PEER`	Fixar o roteamento de controle de crédito a um par Diameter específico. Isso ignora o roteamento de domínio	id do par (por exemplo, `32260@3gpp.org`); desativado por padrão
`RO_ROOT`	Raiz do Service-Context-Id	`32260@3gpp.org`
`RO_EXT`	Extensão do Service-Context-Id	`ext`
`RO_MNC`	Componente MNC do Service-Context-Id	por exemplo, `07`
`RO_MCC`	Componente MCC do Service-Context-Id	por exemplo, `262`

Nome	O que controla	Valores
`RO_RELEASE`	Lançamento 3GPP para Service-Context-Id	por exemplo, `8`

Flags de recurso (`WITH_*`)

Flag	Efeito quando definido
`WITH_AUTH`	Autenticar cada REGISTER (não apenas clientes Digest/MD5). Habilitado por padrão no template.
`WITH_RO`	Habilitar cobrança online de origem via Diameter Ro.
`WITH_RO_TERM`	Habilitar cobrança online de término via Diameter Ro.

O Ansible template `CAPTURE_NODE` (o alvo de captura do Homer) apenas quando a captura do Homer está habilitada para a implantação. `CAPTURE_NODE` duplica a sinalização SIP para o Homer para rastreamento.

Configuração de pares Diameter

A tabela de pares Diameter do S-CSCF (`scscf.xml`) anuncia a aplicação **Cx** (`16777216`) em direção ao HSS, além da contabilidade básica. A estrutura do arquivo e as variáveis do Ansible que a preenchem são compartilhadas entre todos os CSCFs. Veja Diameter → Configuração de Par (Implantação). Quando a cobrança Ro está habilitada, `RO_DESTINATION` endereça o par OCS em vez do XML.

Solução de Problemas

Falhas de registro

Sintomas: Usuários incapazes de registrar, timeouts de registro, 4xx/5xx no REGISTER.

- **Conectividade HSS (Cx)** - o S-CSCF depende do HSS para responder ao Cx MAR (vetor de autenticação) e SAR (perfil de serviço). Se MAR/SAR expirarem ou retornarem respostas malformadas, o registro falha **503**. Verifique se o par Cx para o HSS está ativo e responde. Veja Operações Diameter.
- **Falhas de autenticação** - confirme se as credenciais do assinante estão provisionadas no HSS e se o HSS gerou o vetor de autenticação (MAR/MAA). Verifique se o algoritmo de desafio é um que o UE suporta (AKA/Milenage para USIM/ISIM, Digest para clientes não-IMS). Uma identidade rejeitada falha **403**.
- **Atribuição / capacidade do S-CSCF** - um assinante sem perfil de serviço IMS, ou uma atribuição de servidor rejeitada (SAR), falha **403**. Confirme se as capacidades do S-CSCF correspondem ao que o I-CSCF selecionou. Também confirme se o nó tem capacidade de registro.

Falhas na configuração de chamadas

Sintomas: Chamadas falham ao estabelecer, erros SIP 4xx/5xx.

- **Usuário não registrado** - verifique se tanto as identidades de origem quanto de término estão registradas no IMS. Um INVITE de término para uma identidade sem vínculo de contato retorna **404**. Para uma identidade de término não registrada com serviços provisionados, o S-CSCF busca o perfil não registrado (Cx SAR UNREGISTERED_USER). Um timeout do HSS aqui falha **503**.
- **IFC / acionamento de serviço** - verifique se o S-CSCF baixou o IFC do HSS (SAR/SAA) e se os pontos de acionamento correspondem ao caso de sessão. Verifique se qualquer Servidor de Aplicação invocado via ISC (OmniTAS, OmniMessage) é acessível. O Tratamento Padrão governa se uma falha do AS continua o trecho ou o abandona.

- **QoS** - o P-CSCF autoriza QoS de mídia para a chamada (Rx para o PCRF para VoLTE, N5 para o PCF para VoNR). Se as chamadas se conectam, mas não têm caminho de mídia, verifique o trecho de política no P-CSCF.
- **Roteamento** - para destinos E.164, verifique a resolução ENUM e o failover do gateway PSTN. Verifique o roteamento de roaming/off-net para chamadas que saem da rede doméstica.

Problemas de entrega de SMS

Sintomas: SMS não entregues via IMS, ou voltando para o SMSC legado.

- **Acionamento de IFC do OmniMessage** - verifique se os IFC do assinante acionam o OmniMessage no método SIP MESSAGE e se sua prioridade é alta o suficiente para disparar. Teste a correspondência do IFC com um SMS simulado.
- **Integração do SMSC** - verifique a conectividade do OmniMessage com o SMSC (MAP/SMPP) e se a conversão SIP MESSAGE ↔ SMS PDU está intacta.
- **Tipo de conteúdo** - verifique se o SIP MESSAGE carrega `Content-Type: application/vnd.3gpp.sms` e a codificação de conjunto de caracteres correta (GSM-7, UCS-2).

Fluxos de Chamadas

Os diagramas de sequência estão incorporados com as funções que documentam:

- Registro e autenticação → Registro e autenticação
- Sessão de origem → Manipulação de chamadas de origem
- Sessão de término → Manipulação de chamadas de término

Documentação Relacionada

- Operações
- Diameter
- Interface Baseada em Serviço (SBI)

- Referência de Métricas
- OmniWeb - registros, diálogos e estado do par Diameter: <https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>

Documentação de Conformidade de Interceptação ANSSI R226

Objetivo do Documento: Este documento fornece as especificações técnicas necessárias para a autorização ANSSI R226. Essas especificações se aplicam sob os Artigos R226-3 e R226-7 do Código Penal Francês. Elas cobrem a Rede Central IMS OmniCSCF (Funções de Controle de Sessão de Chamada).

Classificação: Documentação de Conformidade Regulamentar

Autoridade Alvo: Agence nationale de la sécurité des systèmes d'information (ANSSI)

Regulamentação: R226 - Proteção da Privacidade da Correspondência e Interceptação Legal

---

1. ESPECIFICAÇÕES TÉCNICAS DETALHADAS

1.1 Identificação do Sistema

Nome do Produto: OmniCSCF IMS Core Network
Tipo de Produto: Rede Central do Subsistema Multimídia IP (IMS)
Função Primária: Controle de sessão de chamada VoIP/VoLTE e entrega de serviços multimídia
Modelo de Implantação: Infraestrutura de telecomunicações local

Componentes da Rede:

- P-CSCF (Função de Controle de Sessão de Chamada Proxy)
- E-CSCF (Função de Controle de Sessão de Chamada de Emergência)
- I-CSCF (Função de Controle de Sessão de Chamada de Interrogatório)
- S-CSCF (Função de Controle de Sessão de Chamada Servidora)

Este sistema gerencia registro, autenticação, roteamento de sessão e controle de chamada para redes do Subsistema Multimídia IP (IMS). As seções abaixo descrevem as capacidades de interceptação e características de criptografia.

1.2 Capacidades de Interceptação

1.2.1 Registro e Aquisição de Sessão

Captura de Registro SIP:

O sistema CSCF processa todos os registros SIP. Ele mantém o estado de registro completo:

- **Identificadores de Usuário:**
  - IMPU (Identidade Pública Multimídia IP) - URI SIP (ex: sip:+33612345678@ims.mnc001.mcc001.3gppnetwork.org)
  - IMPI (Identidade Privada Multimídia IP) - Nome de usuário de autenticação (ex: user@ims.mnc001.mcc001.3gppnetwork.org)
  - IMSI (Identidade Internacional do Assinante Móvel) - A partir de cabeçalhos P ou HSS
  - MSISDN (Número de telefone móvel) - A partir de IMPU ou perfil de usuário HSS
- **Metadados de Registro:**
  - URI de contato (endereço de rede UE atual)
  - Cabeçalho de caminho (rota de volta através do P-CSCF)
  - Cabeçalho Service-Route (rota para S-CSCF)
  - String User-Agent (identificação do tipo de dispositivo)
  - Timestamp de expiração do registro
  - Endereço IP de origem e porta

    - Protocolo de transporte (TCP/UDP/TLS)
    - Vetores de autenticação (RAND, AUTN, XRES, CK, IK do HSS)

- **Informações de Localização da Rede:**
    - Cabeçalho P-Access-Network-Info (torre de celular, área de localização)
    - P-Visited-Network-ID (identificação da rede de roaming)
    - Endereço IP recebido (fonte real)
    - Endereço P-CSCF (ponto de entrada da rede)

Captura de Sessão de Chamada:

O S-CSCF mantém o estado de diálogo SIP completo para todas as chamadas ativas:

- **Identificadores de Sessão:**
    - Call-ID (identificador único da sessão)
    - URIs e tags From/To
    - Conjuntos de rota para ambas as partes
    - Original-Dialog-ID (para rastreamento de interação com o Servidor de Aplicação)

- **Metadados da Sessão:**
    - Identidade do chamador (cabeçalho From, P-Asserted-Identity)
    - Parte chamada (cabeçalho To, Request-URI)
    - Timestamp de estabelecimento da sessão
    - Timestamp de término da sessão
    - Estado do diálogo (Early/Confirmed/Deleted)
    - Números CSeq (sequenciamento de transações)

- **Informações de Mídia:**
    - SDP (Protocolo de Descrição de Sessão) nos corpos das mensagens SIP
    - Endereços do servidor de mídia (OmniTAS)
    - Informações de codec (formatos de áudio/vídeo)
    - Pontos finais de fluxo de mídia

    - Alocações de porta RTP/RTCP

Identificação de Chamada de Emergência:

O componente E-CSCF identifica chamadas de emergência e as roteia:

- Detecção de número de emergência (112, 911, etc.)
- Captura de IMEI (Identidade Internacional de Equipamento Móvel)
- Mapeamento de IMEI para MSISDN (para retorno de chamada)
- Informações de localização da UE ou da rede
- Suporte ao protocolo HELD (HTTP-Enabled Location Delivery)
- Destino de roteamento de emergência (PSAP/AS de emergência)

Determinação da Identidade do Chamador (conforme 3GPP TS 23.167):

O sistema estabelece a identidade da linha de chamada autenticada apresentada na perna de emergência da seguinte forma:

- **Chamador conhecido (registrado):** O sistema pega a identidade do IMPU registrado. Onde aplicável, ele também usa o mapeamento IMEI→MSISDN em cache mantido pelo P-CSCF.
- **Chamador desconhecido/anônimo (emergência não autenticada, sem identidade registrada):** O P-CSCF resolve a identidade no nível EPC a partir do PCRF através da interface Diameter Rx. Ele usa um `Rx_AAR_Subscription` assíncrono, vinculado pelo endereço IP de origem da UE. O sistema seleciona a identidade por precedência **MSISDN → IMSI → IMEISV**. Ele afirma o valor resolvido como **P-Asserted-Identity** no domínio `sos.apn`.

Em ambos os casos, o resultado P-Asserted-Identity é a identidade da linha de chamada autenticada apresentada ao PSAP e nas interfaces LI. É uma identidade afirmada pela rede, não uma mera aproximação.

1.2.2 Armazenamento e Processamento de Dados

IMPORTANTE: Somente Estado em Memória

Os componentes CSCF (P-CSCF, E-CSCF, I-CSCF, S-CSCF) mantêm **todos os dados de estado apenas na memória**. Não há **armazenamento de banco**

de dados persistente de dados de registro ou sessão de chamada. O sistema armazena todos os mapeamentos de registro, estado de diálogo e associações de segurança IPsec na memória. O sistema perde esses dados na reinicialização.

Dados de Registro Ativo (Em Memória):

O sistema CSCF mantém o estado em tempo real apenas:

Estado de Registro P-CSCF:

- Dados de Associação de Segurança IPsec (pares SPI, portas, parâmetros de criptografia)
- Mapeamentos de contato da UE e endereços de rede
- Pontos finais e status do túnel IPsec
- Períodos de validade do registro

Estado de Registro S-CSCF:

- Identidades públicas (IMPU) e estado de registro atual
- Mapeamentos de contato com cabeçalhos de caminho, User-Agent, endereços recebidos
- Mapeamentos de identidade privada (IMPI) para identidade pública
- Perfis de usuário do HSS (em cache durante o registro)

Estado de Sessão Ativa (Em Memória):

O S-CSCF mantém o estado de chamada ativa apenas:

- Identificadores de chamada (Call-ID), identidades de participantes (tags From/To)
- Conjuntos de rota e endereços de contato
- Estado da sessão (Early/Confirmed/Terminated)
- Informações de tempo da sessão

Sem CDR ou Rastreio Histórico:

Os componentes CSCF **não** geram ou armazenam:

- Registros de Detalhes de Chamada (CDRs)
- Registros de chamadas históricas
- Registros de registro históricos
- Rastreio de eventos de longo prazo

Geração de CDR e Rastreio Histórico: O **TAS (Servidor de Aplicação de Telefonia - OmniTAS)** gerencia todos os registros de detalhes de chamadas, dados de cobrança e rastreamento de chamadas históricas. Os componentes CSCF não lidam com eles.

Registro de Mensagens SIP/Diameter:

Os CSCFs podem gerar logs de eventos em tempo real para uso operacional:

- **Registro de Mensagens SIP:** Registro opcional de mensagens SIP (INVITE, REGISTER, etc.)
- **Registro de Mensagens Diameter:** Registro opcional de transações Diameter (Cx, Rx, Ro)
- **Eventos do Sistema:** Mudanças de configuração, erros, falhas

Esses logs são logs operacionais transitórios, não registros de chamadas persistentes. Você pode configurar a retenção do log. A retenção é tipicamente de curto prazo (horas a dias) apenas para depuração.

1.2.3 Capacidades de Análise

Monitoramento em Tempo Real:

O portal de gerenciamento OmniWeb (<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>) fornece:

- **Monitoramento de Registro:**
  - Visualizar todos os usuários registrados com paginação
  - Pesquisar por IMPU, contato, IMPI
  - Detalhes do registro (contato, caminho, user-agent, expiração)
  - Capacidade de desregistro forçado
- **Monitoramento de Diálogo:**

    - Visualizar sessões de chamada ativas
    - Call-ID, URIs From/To, estado, duração
    - Capacidade de término de chamada (enviar BYE)
    - Atualização automática a cada 5 segundos

- **Status do Sistema:**

    - Status do par Diameter (HSS, PCRF, conectividade OCS)
    - Status do gateway frontend
    - Métricas de capacidade do sistema
    - Capacidade do túnel IPsec (P-CSCF)

Nota sobre Dados Históricos:

Os componentes CSCF não mantêm dados históricos. **OmniTAS (Servidor de Aplicação de Telefonia)** gerencia toda a geração de CDR e rastreamento de chamadas de longo prazo. Para registros de chamadas históricos, CDRs e análise de padrões de comunicação, as autoridades de interceptação legal devem coordenar com o OmniTAS.

Visibilidade de Acionamento de Serviço em Tempo Real:

O S-CSCF processa Critérios de Filtro Iniciais (iFC) em tempo real:

- A avaliação de iFC determina quais Servidores de Aplicação são acionados para cada chamada
- Visibilidade em tempo real sobre quais serviços são invocados
- Decisões de roteamento do Servidor de Aplicação visíveis no fluxo de mensagens SIP

Status da Rede:

- Status de conectividade HSS (interface Diameter Cx)
- Distribuição de seleção S-CSCF (I-CSCF)
- Padrões de roteamento de chamadas
- Tempos de resposta do Servidor de Aplicação
- Desempenho de transações Diameter

1.3 Capacidades de Contramedidas

1.3.1 Mecanismos de Proteção à Privacidade

Confidencialidade da Comunicação:

- **Túneis IPsec:** Túneis ESP (Encapsulating Security Payload) entre UE e P-CSCF
  - Criptografia: AES-CBC, AES-GCM
  - Autenticação: HMAC-SHA1, HMAC-SHA256
  - Derivação de chave a partir do IMS AKA (CK/IK do HSS)
  - Associações de segurança por UE
- **Suporte a TLS/TLS:**
  - Suporte a SIP sobre TLS (SIPS)
  - Diameter sobre TLS (conexões HSS, PCRF, OCS)
  - Autenticação baseada em certificado
  - Perfeita Segurança de Encaminhamento (PFS) via ECDHE/DHE
- **Cabeçalhos de Privacidade SIP:**
  - P-Asserted-Identity (ID do chamador autenticado)
  - Cabeçalho de privacidade (solicitar supressão do ID do chamador)
  - Suporte a sessão anônima

Controle de Acesso:

- Autenticação OmniWeb e controle de acesso baseado em função
- Interface de gerenciamento BINRPC (porta 2046)
- Controles de acesso ao registro e separação de funções
- Autenticação SIP (AKA via HSS)
- Autenticação de pares Diameter

Registro de Auditoria:

- Registro abrangente de mensagens SIP e Diameter

- Eventos de registro/desregistro
- Eventos de estabelecimento e término de chamadas
- Ações administrativas via OmniWeb
- Mudanças de configuração
- Sucesso/falha de autenticação

1.3.2 Recursos de Proteção de Dados

Segurança de Acesso:

- Controle de acesso baseado em função (RBAC)
- Contas de monitoramento somente leitura
- Controles de autenticação e autorização

Fortalecimento do Sistema:

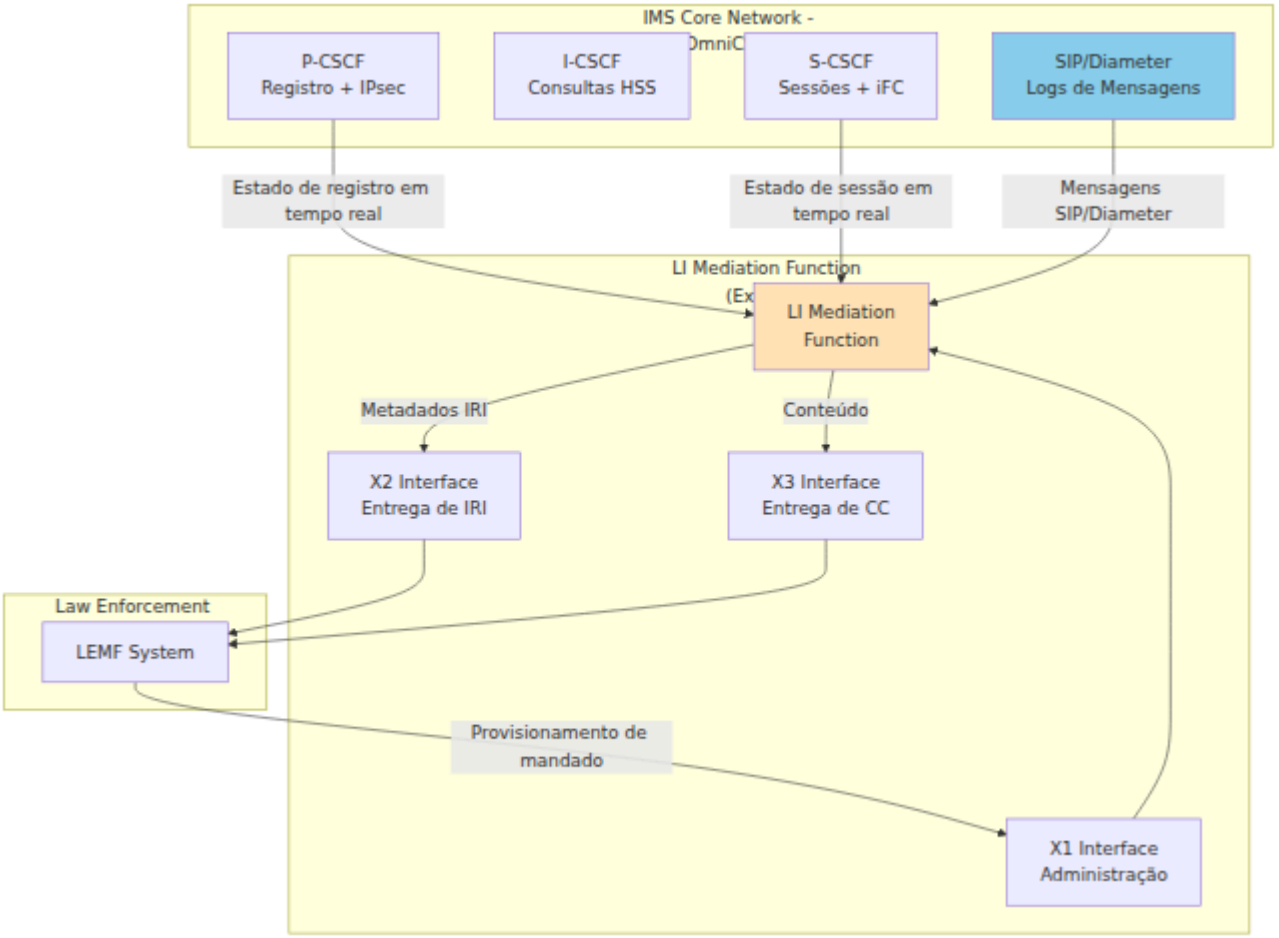
- Mínimos ports de rede expostos (5060 SIP, 3868 Diameter, 2046 gerenciamento BINRPC)
- Verificação de sanidade de mensagens SIP
- Prevenção de loops Max-Forwards
- Limitação de taxa e proteção contra inundação
- Limites de tamanho de mensagem
- Isolamento de processos de trabalho

1.4 Pontos de Integração de Interceptação Legal

1.5.1 Arquitetura de Interceptação Legal ETSI

O sistema CSCF fornece uma base para interceptação legal em conformidade com a ETSI. O sistema não constrói interfaces nativas X1/X2/X3. Todos os pontos de acesso de dados necessários existem para integração com sistemas externos de Função de Mediação de Interceptação Legal (LIMF).

Interfaces LI Padrão ETSI:



Interface X1 - Função de Administração:

- **Propósito:** Provisionamento de mandados e alvos a partir da aplicação da lei
- **Direção:** LEMF → LIMF (bidirecional)
- **Funções:**
  - Ativar/desativar interceptação para alvos (IMPUs, IMSIs, MSISDNs)
  - Definir duração e período de validade da interceptação
  - Configurar critérios de filtragem (identidades, janelas de tempo)
  - Recuperar status de interceptação
- **Integração com CSCF:**
  - LIMF mantém o banco de dados de mandados (lista de alvos, externa ao CSCF)
  - LIMF monitora o estado em tempo real do CSCF e logs de mensagens para sessões correspondentes
  - LIMF filtra com base nos critérios provisionados pelo X1

Interface X2 - Entrega de IRI (Informações Relacionadas à Interceptação):

- **Propósito:** Entregar metadados de sessão à aplicação da lei
- **Direção:** LIMF → LEMF (unidirecional)
- **Formato de Dados:** XML/ASN.1 compatível com ETSI TS 102 232
- **Conteúdo do CSCF:**
  - Identificadores de sessão (Call-ID, tags de diálogo)
  - Parte chamadora (URI From, P-Asserted-Identity, IMPU, IMSI, MSISDN)
  - Parte chamada (URI To, Request-URI, IMPU, IMSI, MSISDN)
  - Timestamps de registro
  - Timestamps de configuração/desmontagem da sessão
  - Localização da rede (P-Access-Network-Info, torre de celular, área de localização)
  - Endereços P-CSCF/S-CSCF (identificação do elemento da rede)
  - User-Agent (tipo de dispositivo)
  - Informações de roaming (P-Visited-Network-ID)

Interface X3 - Entrega de CC (Conteúdo da Comunicação):

- **Propósito:** Entregar o conteúdo real da comunicação
- **Direção:** LIMF → LEMF (unidirecional)
- **Formato de Dados:** Compatível com ETSI TS 102 232
- **Conteúdo do CSCF:**
  - Corpos de mensagens SIP (descrições de sessão SDP)
  - Endereços do servidor de mídia (para interceptação RTP)
  - Informações de codec
  - Mensagens instantâneas SIP MESSAGE (conteúdo do corpo)
  - Dados de aplicação (se roteados através do CSCF)

Nota: Para fluxos RTP de voz/vídeo, o LIMF também deve se integrar com servidores de mídia (OmniTAS). Esta integração captura o conteúdo real da mídia. O CSCF fornece informações de configuração da sessão (SDP). Essas informações mostram onde a mídia flui.

1.5.2 Fontes de Dados do CSCF para Interceptação Legal

1. Acesso a Dados de Registro:

Dados de Registro P-CSCF:

- IMPU (identidade pública)
- URI de contato (endereço de rede UE)
- IP e porta recebidos
- Cabeçalho de caminho
- Expiração do registro
- Informações de SPI e porta IPsec
- String User-Agent

Dados de Registro S-CSCF:

- Identidades públicas (IMPU), status de bloqueio, estado de registro
- Mapeamentos de contato com cabeçalhos de caminho, User-Agent, endereços recebidos
- Mapeamentos de identidade privada (IMPI) para identidade pública
- Perfis de usuário do HSS (formato XML incluindo detalhes do assinante)

Métodos de Acesso:

- Interfaces de acesso a dados somente leitura
- Interface de monitoramento OmniWeb
- Capacidade de consulta em tempo real

2. Dados de Sessão Ativa:

Dados de Diálogo S-CSCF:

- Call-ID (identificador único da sessão)
- URIs From/To e tags
- Números CSeq do chamador e chamado
- Conjuntos de rota para ambas as partes
- Endereços de contato
- Estado do diálogo (Early, Confirmed, Deleted)
- Timestamp de início

- Valores de timeout

Métodos de Acesso:

- Monitoramento do estado do diálogo em tempo real
- Consulta por identificadores de sessão ou identificadores de partes
- Capacidades de exportação para análise forense

3. Registro de Mensagens SIP:

Captura de Log:

- Todas as mensagens SIP podem ser registradas (REGISTER, INVITE, MESSAGE, etc.)
- Níveis de log configuráveis
- Registro estruturado com timestamps
- Registro baseado em Syslog ou arquivo

Análise de Log:

- Analisar cabeçalhos SIP para extração de identidade
- Extrair SDP para informações de mídia
- Rastrear sequências de mensagens (CSeq)
- Correlacionar solicitações e respostas

Exemplo de Entrada de Log:

```
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. Registro de Mensagens Diameter:

Mensagens Cx (Comunicação HSS):

- UAR/UAA: Autorização de usuário (contém IMPU, IMPI)
- LIR/LIA: Informações de localização (contém IMPU, S-CSCF em serviço)
- MAR/MAA: Autenticação (contém IMPI, vetores de autenticação)
- SAR/SAA: Atribuição de servidor (contém IMPU, IMPI, perfil de usuário XML)

Dados Diameter Disponíveis:

- IMSI (do perfil de usuário)
- MSISDN (do perfil de usuário)
- IMPUs associados (múltiplas identidades por assinante)
- Perfil de usuário (serviços, status de bloqueio, status de roaming)

Exemplo de Log:

```
Diameter Cx SAA recebido do 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 (Sucesso)
User-Data: <XML perfil de usuário com IMSI, MSISDN, iFC>
```

5. Dados de Chamada de Emergência (E-CSCF):

Mapeamento de IMEI para MSISDN:

- O P-CSCF cria o mapeamento quando uma UE se registra com um IMEI (tabela `emergency_imei_msisdn_map`)
- TTL de 4 horas (14400s autoexpiração)
- Usado para retorno de chamada de emergência
- Replicado entre os nós do cluster P-CSCF

Retenção de Dados:

- Mapeamentos de IMEI para MSISDN retidos por 4 horas (14400s)
- Disponíveis para correlação de retorno de chamada de emergência
- Acessíveis via interfaces de monitoramento

Logs de Chamada de Emergência:

- Detecção de número de emergência (112, 911, etc.)
- Extração de IMEI de cabeçalhos de contato ou P
- Informações de localização (do HELD ou P-Access-Network-Info)
- Roteamento PSAP (Ponto de Resposta de Segurança Pública)
- Roteamento E-CSCF para AS de emergência

1.5.3 Capacidades de Integração para LIMF

O sistema fornece vários métodos de integração para sistemas de Função de Mediação de Interceptação Legal (LIMF):

1. **Acesso a Dados de Registro e Sessão:**

    - Acesso em tempo real a dados de registro (identidades, localizações, informações do dispositivo)
    - Monitoramento de sessão ativa (estado da chamada, participantes, tempo)
    - Capacidades de consulta histórica

2. **Registro de Eventos:**

    - Registro de mensagens SIP com níveis de detalhe configuráveis
    - Registro de mensagens Diameter para interações HSS
    - Logs de eventos estruturados com timestamps

3. **Monitoramento em Tempo Real:**

    - Monitoramento do status de registro ao vivo
    - Rastreamento de sessão de chamada ativa
    - Detecção de chamadas de emergência e informações de roteamento

Os métodos de integração suportam arquiteturas baseadas em polling e acionadas por eventos para conectividade LIMF.

1.5.4 Mapeamento de Dados do CSCF para Interfaces LI

Mapeamento de Dados CSCF para IRI (X2):

Fonte de Dados CSCF	Campo IRI	Exemplo de Dados
IMPU (cabeçalhos SIP/estado em memória)	Parte A	sip:+33612345678@ims.mnc001.mcc001.3gp
IMPI (cabeçalhos SIP/estado em memória)	ID de Autenticação	user@ims.mnc001.mcc001.3gppnetwork.org
IMSI (perfil de usuário HSS)	ID do Assinante	208011234567890
MSISDN (perfil de usuário HSS)	Número de Telefone	+33612345678
Call-ID (cabeçalhos SIP/estado de diálogo)	ID da Sessão	f81d4fae-7dec-11d0-a765-00a0c91e6bf6@...
From/To (cabeçalhos SIP)	Parte A/Parte B	sip:+33612345678@... / sip:+33687654321@.
Timestamp de registro	Hora do Evento	2025-11-29T10:30:00Z

Fonte de Dados CSCF	Campo IRI	Exemplo de Dados
(em memória)		
P-Access-Network-Info (cabeçalho SIP)	Localização	3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=208011
IP Recebido (contato SIP)	Endereço IP da UE	10.20.30.40:5060
Endereço P-CSCF (roteamento SIP)	Elemento da Rede	10.4.12.165:5060
Endereço S-CSCF (roteamento SIP)	Elemento da Rede	10.4.11.45:5060

Mapeamento de Dados CSCF para CC (X3):

Fonte de Dados CSCF	Campo CC	Exemplo de Dados
Corpo da mensagem SIP MESSAGE	Conteúdo da Mensagem Instantânea	"Olá, como você está?"
SDP no INVITE	Informações da Sessão de Mídia	Pontos finais RTP, codecs
Endereço do servidor de mídia	Alvo de Interceptação RTP	10.50.60.70:49170

Nota: Para conteúdo real de voz/vídeo (RTP), o LIMF deve coordenar com servidores de mídia (OmniTAS) para capturar fluxos RTP. O CSCF fornece apenas informações de configuração da sessão.

Nota sobre a identidade de chamada de emergência (Parte A): Para uma chamada normal (registrada), o sistema deriva a Parte A do IMPU registrado / P-Asserted-Identity. Para uma **chamada de emergência desconhecida/anônima**, o P-CSCF resolve a Parte A a partir do PCRF sobre Diameter Rx (`Rx_AAR_Subscription`, vinculado pelo IP de origem da UE, precedência MSISDN → IMSI → IMEISV). O P-CSCF afirma essa identidade como P-Asserted-Identity no domínio `sos.apn`, conforme 3GPP TS 23.167. Esta é a identidade da linha de chamada autenticada transportada na interface X2/IRI para tais chamadas.

1.5 Interface de Monitoramento Baseada na Web

OmniWeb fornece acesso de monitoramento e administrativo. OmniWeb é o portal de gerenciamento unificado (<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>). Ele oferece monitoramento em tempo real e acesso administrativo aos componentes CSCF:

Capacidades de Monitoramento:

- Monitoramento em tempo real de registro e sessão (assinantes ativos, localizações, informações do dispositivo, estado da chamada, tempo)
- Pesquisa de identidade por IMPU, IMPI, IMSI ou MSISDN
- Status do túnel IPsec e monitoramento de capacidade
- Capacidades de exportação para análise forense

Segurança:

- Acesso criptografado por HTTPS/TLS
- Autenticação necessária
- Controle de acesso baseado em função (RBAC), incluindo modos de acesso somente leitura para pessoal de monitoramento
- Registro de auditoria de todas as ações administrativas

---

2. CAPACIDADES DE CRIPTOGRAFIA E CRIPTOANÁLISE

2.1 Visão Geral das Capacidades Criptográficas

O OmniCSCF implementa várias camadas de proteção criptográfica para sinalização e dados de assinantes. Esta seção documenta todas as capacidades criptográficas, conforme exigido pela ANSSI.

2.2 Criptografia de Túneis IPsec ESP (UE para P-CSCF)

2.2.1 Implementação do Protocolo IPsec

Modo IPsec Suportado:

- ESP (Encapsulating Security Payload) - Protocolo IP 50
- Modo de transporte (não modo túnel)
- Protege a sinalização SIP entre UE e P-CSCF

Algoritmos de Criptografia Suportados:

O sistema com IPsec do kernel suporta:

- **AES-CBC (Padrão de Criptografia Avançada - Cadeia de Blocos de Cifras):**
  - AES-128-CBC (chave de 128 bits)
  - AES-192-CBC (chave de 192 bits)
  - AES-256-CBC (chave de 256 bits) - Recomendado
- **AES-GCM (Padrão de Criptografia Avançada - Modo Galois/Contador):**
  - AES-128-GCM (chave de 128 bits com AEAD)
  - AES-256-GCM (chave de 256 bits com AEAD) - Recomendado
- **3DES-CBC (Triple DES - Cadeia de Blocos de Cifras):**
  - Chave efetiva de 168 bits (obsoleto, compatibilidade legada)
- **Criptografia NULL:**
  - Sem confidencialidade (somente autenticação)
  - Usado apenas para depuração ou cenários de conformidade específicos

Algoritmos de Autenticação Suportados:

- **HMAC-SHA1 (Código de Autenticação de Mensagem Baseado em Hash - SHA-1):**
  - Saída de 160 bits
  - Compatibilidade legada
- **HMAC-SHA256 (HMAC - SHA-256):**
  - Saída de 256 bits
  - Recomendado
- **HMAC-SHA384 (HMAC - SHA-384):**

    - Saída de 384 bits

- **HMAC-SHA512 (HMAC - SHA-512):**
    - Saída de 512 bits

- **HMAC-MD5:**
    - Saída de 128 bits
    - Obsoleto, apenas compatibilidade legada

Derivação de Chave:

O sistema deriva chaves IPsec (CK - Chave de Cifração, IK - Chave de Integridade) a partir da autenticação IMS AKA:

1. UE realiza autenticação AKA com S-CSCF/HSS
2. HSS gera CK (128 bits) e IK (128 bits)
3. S-CSCF entrega CK/IK ao P-CSCF via interface interna
4. P-CSCF usa CK/IK para estabelecer associações de segurança IPsec com a UE
5. CK usado para criptografia ESP
6. IK usado para autenticação ESP

Parâmetros de Associação de Segurança:

- **Vida Útil:** Vinculada à expiração do registro SIP (tipicamente 599 segundos)
- **Proteção contra Repetição:** Habilitada (janela anti-repetição)
- **Números de Sequência:** 32 bits ou 64 bits (ESN - Números de Sequência Estendidos)
- **Perfeita Segurança de Encaminhamento:** Não aplicável (chaves do AKA, não Diffie-Hellman)

Implementação:

A capacidade IPsec do P-CSCF:

- Interage com a pilha IPsec do kernel Linux (framework XFRM)

- Configura políticas e associações de segurança via API do kernel
- Alocação e gerenciamento de SPI (Índice de Parâmetro de Segurança)
- Alocação de porta para tráfego protegido

2.2.2 Capacidades de Configuração IPsec

Seleção de Conjunto de Cifras:

Você pode configurar o P-CSCF para preferir conjuntos de cifras específicos:

Preferidos (segurança forte):

- ESP com AES-256-GCM e HMAC-SHA256
- ESP com AES-256-CBC e HMAC-SHA256

Suportados (compatibilidade):

- ESP com AES-128-CBC e HMAC-SHA1
- ESP com 3DES-CBC e HMAC-SHA1 (legado)

Gerenciamento de Chaves:

- IKE (Internet Key Exchange) NÃO é usado
- Chaves fornecidas via IMS AKA (CK/IK do HSS)
- Configuração manual de associações de segurança via kernel XFRM
- Destruição automática de SA na expiração do registro

Ciclo de Vida do Túnel:

1. UE se registra → autenticação AKA → CK/IK gerados
2. P-CSCF recebe CK/IK do S-CSCF
3. P-CSCF aloca par de SPI (SPI do cliente, SPI do servidor)
4. P-CSCF aloca par de portas (porta do cliente, porta do servidor)
5. P-CSCF configura SAs IPsec do kernel usando CK/IK
6. P-CSCF envia parâmetros IPsec para a UE no 200 OK (cabeçalho Security-Server)
7. UE configura SAs IPsec com os mesmos parâmetros
8. Todo o tráfego SIP subsequente flui através de túneis ESP

9. Na expiração do registro ou desregistro: SAs deletadas, recursos liberados

2.3 Criptografia TLS (SIP e Diameter)

2.3.1 TLS para SIP (SIPS)

Versões TLS Suportadas:

- **TLS 1.2** (RFC 5246) - Suportado
- **TLS 1.3** (RFC 8446) - Suportado (se suporte do kernel/biblioteca)
- **TLS 1.0/1.1** - Obsoleto (desativado por padrão)
- **SSL 2.0/3.0** - NÃO SUPORTADO (vulnerabilidades conhecidas)

Implementação TLS:

O sistema usa OpenSSL ou LibreSSL:

- Bibliotecas TLS padrão da indústria
- Implementações validadas criptograficamente
- Atualizações de segurança regulares

Conjuntos de Cifras Suportados:

TLS 1.3 (Preferido):

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256

TLS 1.2 (Suportado):

- ECDHE-RSA-AES256-GCM-SHA384 (Perfeita Segurança de Encaminhamento)
- ECDHE-RSA-AES128-GCM-SHA256 (Perfeita Segurança de Encaminhamento)
- ECDHE-ECDSA-AES256-GCM-SHA384 (Perfeita Segurança de Encaminhamento)
- DHE-RSA-AES256-GCM-SHA384 (Perfeita Segurança de Encaminhamento)

- DHE-RSA-AES128-GCM-SHA256 (Perfeita Segurança de Encaminhamento)

Cifras fracas desativadas:

- Sem RC4
- Sem MD5
- Sem criptografia NULL
- Sem cifras de grau EXPORT
- Sem DES/3DES (obsoleto)

Suporte a Certificados:

- **Certificados X.509** (formato padrão)
- **Chaves RSA:** mínimo de 2048 bits, recomendado 4096 bits
- **Chaves ECDSA:** curvas P-256, P-384, P-521 suportadas
- **Validação de cadeia de certificados**
- **Verificação de CRL (Lista de Revogação de Certificados)** (opcional)
- **OCSP (Protocolo de Status de Certificado Online)** (opcional)

Recursos TLS:

- **Perfeita Segurança de Encaminhamento (PFS):** Via troca de chaves ECDHE/DHE
- **Indicação de Nome do Servidor (SNI):** Suportado
- **Retomada de Sessão TLS:** Suportada (otimização de desempenho)
- **Autenticação de Certificado do Cliente:** Suportada (mutual TLS)

SIP sobre TLS (SIPS):

- Transporte: TCP com criptografia TLS
- Porta: 5061 (porta padrão SIPS)
- Usado para comunicação inter-CSCF (opcional)
- Usado para conexões de rede confiáveis

2.3.2 TLS para Diameter

Capacidades Diameter:

O sistema suporta o seguinte:

- **Diameter sobre SCTP** (preferido para confiabilidade)
- **Diameter sobre TCP com TLS**
- **Porta:** 3868 (porta padrão Diameter)

Casos de Uso:

- **Interface Cx:** S-CSCF/I-CSCF para HSS (dados do assinante, autenticação)
- **Interface Rx:** P-CSCF para PCRF (política de QoS)
- **Interface Ro:** S-CSCF para OCS (cobrança online - se habilitado)

Configuração TLS para Diameter:

Mesmos conjuntos de cifras que SIP

- TLS 1.2/1.3
- Troca de chaves ECDHE/DHE (PFS)
- Criptografia AES-GCM
- Autenticação SHA256/SHA384

Autenticação Baseada em Certificado:

- Pares Diameter se autenticam via certificados TLS
- Mutual TLS (certificados de cliente e servidor)
- Validação de FQDN (Nome de Domínio Totalmente Qualificado) em certificados
- Validação de cadeia CA confiável

2.4 Criptografia de Autenticação

2.4.1 Funções Criptográficas IMS AKA

Algoritmo 3GPP AKA (MILENAGE):

Usado para gerar vetores de autenticação (RAND, AUTN, XRES, CK, IK):

Funções Criptográficas:

- **f1:** Função de autenticação de mensagem (calcular MAC-A e MAC-S)
- **f2:** Função de resposta (calcular RES a partir de RAND e K)
- **f3:** Derivação de chave de cifração (calcular CK)
- **f4:** Derivação de chave de integridade (calcular IK)
- **f5:** Função de chave de anonimato (calcular AK para privacidade de IMSI)

Material de Chave:

- **K:** Chave permanente de assinante de 128 bits (armazenada em ISIM e HSS)
- **OPc:** Chave variante do operador (derivada de K e OP)
- **RAND:** Desafio aleatório de 128 bits
- **SQN:** Número de sequência de 48 bits (proteção contra repetição)

Sequência AKA:

1. HSS gera RAND (aleatório criptograficamente)
2. HSS calcula MAC-A = f1(K, RAND, SQN, AMF)
3. HSS calcula AUTN = (SQN ⊕ AK) || AMF || MAC-A
4. HSS calcula XRES = f2(K, RAND)
5. HSS calcula CK = f3(K, RAND)
6. HSS calcula IK = f4(K, RAND)
7. HSS envia {RAND, AUTN, XRES, CK, IK} para S-CSCF
8. S-CSCF desafia UE com RAND e AUTN
9. UE calcula RES = f2(K, RAND) usando ISIM
10. UE envia RES para S-CSCF
11. S-CSCF compara RES com XRES (validação de autenticação)

Propriedades de Segurança:

- **Autenticação Mútua:** UE verifica HSS via AUTN, HSS verifica UE via RES
- **Frescura da Chave:** RAND é aleatório, SQN previne repetição
- **Derivação de Chave:** CK e IK derivadas do segredo compartilhado K

2.4.2 Autenticação Digest HTTP

Para autenticação não-IMS (se utilizada):

Algoritmo: MD5 (RFC 2617)

- **Função de Hash:** MD5 (saída de 128 bits)
- **Desafio-Resposta:** Baseado em nonce
- **Proteção contra Repetição:** Nonce com timestamp

Nota: HTTP Digest com MD5 é considerado fraco. IMS AKA é fortemente preferido.

2.5 Hashing e Integridade

2.5.1 Funções de Hash Disponíveis

O sistema pode usar as seguintes funções de hash (via OpenSSL/crypto do kernel):

- **SHA-256:** saída de 256 bits, recomendado
- **SHA-384:** saída de 384 bits
- **SHA-512:** saída de 512 bits
- **SHA-1:** saída de 160 bits, obsoleto para uso em segurança
- **MD5:** saída de 128 bits, obsoleto para uso em segurança

Uso:

- Construções HMAC para IPsec/TLS
- Verificação de integridade de dados
- Geração de nonce
- Detecção de duplicatas (hashing de Call-ID)

2.5.2 Integridade da Mensagem

Integridade da Mensagem SIP:

- **IPsec ESP:** HMAC-SHA256 para SIP autenticado sobre IPsec
- **TLS:** Autenticação de mensagem via MAC TLS
- **Digest SIP:** Integridade do cabeçalho de autenticação

Integridade da Mensagem Diameter:

- **TLS:** Diameter sobre TLS fornece autenticação de mensagem
- **HMAC:** Mensagens Diameter podem incluir AVPs HMAC para integridade

2.6 Geração de Números Aleatórios

Geração de Números Aleatórios Criptograficamente Segura:

O sistema depende do seguinte:

- **Linux kernel /dev/urandom:** PRNG (Gerador de Números Aleatórios Criptograficamente Seguro)
- **OpenSSL RAND_bytes():** CSPRNG (Gerador de Números Aleatórios Pseudo-Criptograficamente Seguro)

Uso:

- Alocação de SPI (valor inicial aleatório)
- Geração de Call-ID
- Geração de parâmetro de ramificação
- Geração de nonce para autenticação
- Geração de ID de sessão

2.7 Gerenciamento de Chaves

2.7.1 Gerenciamento de Certificados TLS

Armazenamento de Certificados:

- Armazenamento em sistema de arquivos com permissões restritas (0600)
- Localizado em: `/etc/system/tls/`
- Formato PEM para certificados e chaves

Geração de Certificados:

```
# Gerar chave privada RSA de 4096 bits
openssl genrsa -out system-key.pem 4096

# Gerar CSR (Solicitação de Assinatura de Certificado)
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

# Certificado autoassinado (desenvolvimento/teste)
openssl x509 -req -days 365 -in system.csr \
  -signkey system-key.pem -out system-cert.pem

# Produção: Enviar CSR para CA confiável
```

Rotação de Certificados:

- Renovação anual de certificados recomendada
- Reinicialização suave do serviço para carregar novos certificados
- Sem tempo de inatividade necessário

2.7.2 Gerenciamento de Chaves IPsec

Derivação de Chave:

- CK (Chave de Cifração) e IK (Chave de Integridade) do IMS AKA
- Chaves de 128 bits do HSS
- Entregues de forma segura via Diameter Cx (sobre TLS)

Vida Útil da Chave:

- Vinculada à expiração do registro SIP (tipicamente 599 segundos)
- Re-keying na atualização do registro
- Destruição automática da chave no desregistro

Armazenamento de Chave:

- Efêmera (somente em memória durante o registro ativo)
- Instaladas na pilha IPsec do kernel
- Sem armazenamento persistente de chaves

- Chaves descartadas quando SA deletada

2.8 Resistência à Criptoanálise

2.8.1 Seleção de Algoritmo

Defesa Contra Criptoanálise:

- **Sem algoritmos personalizados:** Apenas algoritmos padrão da indústria, revisados por pares
- **Tamanhos de chave fortes:** AES-256, RSA-4096, SHA-256
- **Criptografia autenticada:** AES-GCM (AEAD - Criptografia Autenticada com Dados Associados)
- **Perfeita Segurança de Encaminhamento:** ECDHE/DHE em TLS
- **Atualizações regulares:** Aplicações de patches de segurança OpenSSL/LibreSSL

Algoritmos Obsoletos Desativados:

- MD5 (colisões de hash)
- RC4 (fraquezas do cifrador de fluxo)
- DES/3DES (tamanho de bloco pequeno, comprimento da chave)
- SSL 2.0/3.0 (vulnerabilidades de protocolo)
- TLS 1.0/1.1 (ataques BEAST, POODLE)

2.8.2 Mitigação de Ataques de Canal Lateral

Resistência a Ataques de Tempo:

- Comparação em tempo constante para respostas de autenticação
- Sem vazamentos de tempo em operações criptográficas (via OpenSSL)

Proteção de Memória:

- Isolamento da pilha IPsec do kernel
- Isolamento de memória do processo
- Sem swap para dados sensíveis (se configurado)

2.9 Conformidade e Padrões

Conformidade com Padrões Criptográficos:

- **NIST SP 800-52:** Diretrizes TLS
- **NIST SP 800-131A:** Transições de algoritmo criptográfico
- **RFC 7525:** Recomendações TLS
- **ETSI TS 133 203:** Segurança de acesso 3GPP (IMS AKA)
- **ETSI TS 133 210:** Segurança da camada de rede IP (IPsec)
- **3GPP TS 33.203:** Segurança de acesso para IMS
- **3GPP TS 33.210:** Segurança do domínio da rede

Regulamentações Francesas sobre Criptografia:

- Nenhuma criptografia restrita à exportação (todos os algoritmos padrão)
- Meios criptográficos padrão (sem portas traseiras governamentais)
- Certificação de produtos criptográficos ANSSI (se necessário)

Referência de Métricas do IMS CSCF

Este documento é a referência para todas as métricas que os componentes P-CSCF, I-CSCF e S-CSCF exportam.

Acessando Métricas

Todos os componentes CSCF expõem métricas Prometheus na porta 9090:

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

Cada host CSCF (P-CSCF, I-CSCF, S-CSCF) exporta suas próprias métricas. Para obter cobertura total de monitoramento, configure seu servidor Prometheus para coletar dados de todos os hosts.

Exemplo de Configuração do Prometheus:

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

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

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

Para orientações sobre monitoramento e alertas, consulte:

- Monitoramento via OmniWeb e Grafana

Monitoramento via OmniWeb e Grafana

Visualize o estado operacional no **OmniWeb**, o portal de gerenciamento unificado: <https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>. O estado operacional inclui registros, diálogos e status de pares Diameter. O OmniWeb incorpora painéis Grafana para visibilidade em tempo real e histórica. Esses painéis incluem visualizações de registro S-CSCF e localização de usuários. As métricas `ims_usrloc_scscf_active_impus` e `ims_usrloc_scscf_active_contacts` sustentam essas visualizações. Os painéis também mostram o status de pares Diameter e a profundidade da fila. A métrica `cdp_queuelength` e as métricas de interface `ims_icscf_uar_*`, `ims_icscf_lir_*`, `ims_auth_mar_*`, `ims_registrar_scscf_sar_*` e `ims_qos_*` sustentam essas visualizações.

As métricas Prometheus nesta referência sustentam esses painéis Grafana. Elas também sustentam qualquer alerta personalizado que você configurar.

Métricas P-CSCF

Métricas CDP (Diameter)

Nome da Métrica	Significado
`cdp_average_response_time`	Tempo médio de resposta para solicitações Diameter em milissegundos (calculado como replies_response_time / replies_received)
`cdp_queuelength`	Comprimento atual da fila de tarefas do trabalhador Diameter
`cdp_replies_received`	Número total de respostas Diameter recebidas
`cdp_replies_response_time`	Tempo total gasto aguardando respostas Diameter em milissegundos
`cdp_timeout`	Número de eventos de timeout em solicitações Diameter

Estatísticas SIP Core

Contadores de Solicitações

Nome da Métrica	Significado
`core_rcv_requests`	Número total de solicitações SIP recebidas
`core_rcv_requests_ack`	Número de solicitações ACK recebidas
`core_rcv_requests_bye`	Número de solicitações BYE recebidas
`core_rcv_requests_cancel`	Número de solicitações CANCEL recebidas
`core_rcv_requests_info`	Número de solicitações INFO recebidas
`core_rcv_requests_invite`	Número de solicitações INVITE recebidas
`core_rcv_requests_message`	Número de solicitações MESSAGE recebidas
`core_rcv_requests_notify`	Número de solicitações NOTIFY recebidas
`core_rcv_requests_options`	Número de solicitações OPTIONS recebidas
`core_rcv_requests_prack`	Número de solicitações PRACK recebidas
`core_rcv_requests_publish`	Número de solicitações PUBLISH recebidas
`core_rcv_requests_refer`	Número de solicitações REFER recebidas
`core_rcv_requests_register`	Número de solicitações REGISTER recebidas
`core_rcv_requests_subscribe`	Número de solicitações SUBSCRIBE recebidas
`core_rcv_requests_update`	Número de solicitações UPDATE recebidas

Contadores de Respostas (Geral)

Nome da Métrica	Significado
`core_rcv_replies`	Número total de respostas SIP recebidas
`core_rcv_replies_18x`	Número de respostas provisórias 180/181/183/186/187/189 recebidas
`core_rcv_replies_1xx`	Número de respostas 1xx (provisórias) recebidas
`core_rcv_replies_2xx`	Número de respostas 2xx (sucesso) recebidas
`core_rcv_replies_3xx`	Número de respostas 3xx (redirecionamento) recebidas
`core_rcv_replies_4xx`	Número de respostas 4xx (erro do cliente) recebidas
`core_rcv_replies_5xx`	Número de respostas 5xx (erro do servidor) recebidas
`core_rcv_replies_6xx`	Número de respostas 6xx (falha global) recebidas

Contadores de Respostas por Método (1xx)

Nome da Métrica	Significado
`core_rcv_replies_1xx_bye`	Número de respostas 1xx para solicitações BYE
`core_rcv_replies_1xx_cancel`	Número de respostas 1xx para solicitações CANCEL
`core_rcv_replies_1xx_invite`	Número de respostas 1xx para solicitações INVITE
`core_rcv_replies_1xx_message`	Número de respostas 1xx para solicitações MESSAGE
`core_rcv_replies_1xx_prack`	Número de respostas 1xx para solicitações PRACK
`core_rcv_replies_1xx_refer`	Número de respostas 1xx para solicitações REFER
`core_rcv_replies_1xx_reg`	Número de respostas 1xx para solicitações REGISTER
`core_rcv_replies_1xx_update`	Número de respostas 1xx para solicitações UPDATE

Contadores de Respostas por Método (2xx)

Nome da Métrica	Significado
`core_rcv_replies_2xx_bye`	Número de respostas 2xx (sucesso) para solicitações BYE
`core_rcv_replies_2xx_cancel`	Número de respostas 2xx (sucesso) para solicitações CANCEL
`core_rcv_replies_2xx_invite`	Número de respostas 2xx (sucesso) para solicitações INVITE
`core_rcv_replies_2xx_message`	Número de respostas 2xx (sucesso) para solicitações MESSAGE
`core_rcv_replies_2xx_prack`	Número de respostas 2xx (sucesso) para solicitações PRACK
`core_rcv_replies_2xx_refer`	Número de respostas 2xx (sucesso) para solicitações REFER
`core_rcv_replies_2xx_reg`	Número de respostas 2xx (sucesso) para solicitações REGISTER
`core_rcv_replies_2xx_update`	Número de respostas 2xx (sucesso) para solicitações UPDATE

Contadores de Respostas por Método (3xx)

Nome da Métrica	Significado
`core_rcv_replies_3xx_bye`	Número de respostas 3xx (redirecionamento) para solicitações BYE
`core_rcv_replies_3xx_cancel`	Número de respostas 3xx (redirecionamento) para solicitações CANCEL
`core_rcv_replies_3xx_invite`	Número de respostas 3xx (redirecionamento) para solicitações INVITE
`core_rcv_replies_3xx_message`	Número de respostas 3xx (redirecionamento) para solicitações MESSAGE
`core_rcv_replies_3xx_prack`	Número de respostas 3xx (redirecionamento) para solicitações PRACK
`core_rcv_replies_3xx_refer`	Número de respostas 3xx (redirecionamento) para solicitações REFER
`core_rcv_replies_3xx_reg`	Número de respostas 3xx (redirecionamento) para solicitações REGISTER
`core_rcv_replies_3xx_update`	Número de respostas 3xx (redirecionamento) para solicitações UPDATE

Contadores de Respostas por Método (4xx)

Nome da Métrica	Significado
`core_rcv_replies_4xx_bye`	Número de respostas 4xx (erro do cliente) para solicitações BYE
`core_rcv_replies_4xx_cancel`	Número de respostas 4xx (erro do cliente) para solicitações CANCEL
`core_rcv_replies_4xx_invite`	Número de respostas 4xx (erro do cliente) para solicitações INVITE
`core_rcv_replies_4xx_message`	Número de respostas 4xx (erro do cliente) para solicitações MESSAGE
`core_rcv_replies_4xx_prack`	Número de respostas 4xx (erro do cliente) para solicitações PRACK
`core_rcv_replies_4xx_refer`	Número de respostas 4xx (erro do cliente) para solicitações REFER
`core_rcv_replies_4xx_reg`	Número de respostas 4xx (erro do cliente) para solicitações REGISTER
`core_rcv_replies_4xx_update`	Número de respostas 4xx (erro do cliente) para solicitações UPDATE

Contadores de Respostas por Método (5xx)

Nome da Métrica	Significado
`core_rcv_replies_5xx_bye`	Número de respostas 5xx (erro do servidor) para solicitações BYE
`core_rcv_replies_5xx_cancel`	Número de respostas 5xx (erro do servidor) para solicitações CANCEL
`core_rcv_replies_5xx_invite`	Número de respostas 5xx (erro do servidor) para solicitações INVITE
`core_rcv_replies_5xx_message`	Número de respostas 5xx (erro do servidor) para solicitações MESSAGE
`core_rcv_replies_5xx_prack`	Número de respostas 5xx (erro do servidor) para solicitações PRACK
`core_rcv_replies_5xx_refer`	Número de respostas 5xx (erro do servidor) para solicitações REFER
`core_rcv_replies_5xx_reg`	Número de respostas 5xx (erro do servidor) para solicitações REGISTER
`core_rcv_replies_5xx_update`	Número de respostas 5xx (erro do servidor) para solicitações UPDATE

Contadores de Respostas por Método (6xx)

Nome da Métrica	Significado
`core_rcv_replies_6xx_bye`	Número de respostas 6xx (falha global) para solicitações BYE
`core_rcv_replies_6xx_cancel`	Número de respostas 6xx (falha global) para solicitações CANCEL
`core_rcv_replies_6xx_invite`	Número de respostas 6xx (falha global) para solicitações INVITE
`core_rcv_replies_6xx_message`	Número de respostas 6xx (falha global) para solicitações MESSAGE
`core_rcv_replies_6xx_prack`	Número de respostas 6xx (falha global) para solicitações PRACK
`core_rcv_replies_6xx_refer`	Número de respostas 6xx (falha global) para solicitações REFER
`core_rcv_replies_6xx_reg`	Número de respostas 6xx (falha global) para solicitações REGISTER
`core_rcv_replies_6xx_update`	Número de respostas 6xx (falha global) para solicitações UPDATE

Contadores de Códigos de Status Específicos

Nome da Métrica	Significado
`core_rcv_replies_400`	Número de respostas 400 Bad Request recebidas
`core_rcv_replies_401`	Número de respostas 401 Unauthorized recebidas
`core_rcv_replies_402`	Número de respostas 402 Payment Required recebidas
`core_rcv_replies_403`	Número de respostas 403 Forbidden recebidas
`core_rcv_replies_404`	Número de respostas 404 Not Found recebidas
`core_rcv_replies_405`	Número de respostas 405 Method Not Allowed recebidas
`core_rcv_replies_406`	Número de respostas 406 Not Acceptable recebidas
`core_rcv_replies_407`	Número de respostas 407 Proxy Authentication Required recebidas
`core_rcv_replies_408`	Número de respostas 408 Request Timeout recebidas
`core_rcv_replies_409`	Número de respostas 409 Conflict recebidas
`core_rcv_replies_410`	Número de respostas 410 Gone recebidas
`core_rcv_replies_411`	Número de respostas 411 Length Required recebidas
`core_rcv_replies_413`	Número de respostas 413 Request Entity Too Large recebidas
`core_rcv_replies_414`	Número de respostas 414 Request-URI Too Long recebidas

Nome da Métrica	Significado
`core_rcv_replies_415`	Número de respostas 415 Unsupported Media Type recebidas
`core_rcv_replies_420`	Número de respostas 420 Bad Extension recebidas
`core_rcv_replies_480`	Número de respostas 480 Temporarily Unavailable recebidas
`core_rcv_replies_481`	Número de respostas 481 Call/Transaction Does Not Exist recebidas
`core_rcv_replies_482`	Número de respostas 482 Loop Detected recebidas
`core_rcv_replies_483`	Número de respostas 483 Too Many Hops recebidas
`core_rcv_replies_484`	Número de respostas 484 Address Incomplete recebidas
`core_rcv_replies_485`	Número de respostas 485 Ambiguous recebidas
`core_rcv_replies_486`	Número de respostas 486 Busy Here recebidas
`core_rcv_replies_487`	Número de respostas 487 Request Terminated recebidas
`core_rcv_replies_488`	Número de respostas 488 Not Acceptable Here recebidas
`core_rcv_replies_489`	Número de respostas 489 Bad Event recebidas
`core_rcv_replies_491`	Número de respostas 491 Request Pending recebidas

Nome da Métrica	Significado
`core_rcv_replies_493`	Número de respostas 493 Undecipherable recebidas

Estatísticas de Encaminhamento e Erro

Nome da Métrica	Significado
`core_fwd_replies`	Número de respostas SIP encaminhadas
`core_fwd_requests`	Número de solicitações SIP encaminhadas
`core_drop_replies`	Número de respostas SIP descartadas
`core_drop_requests`	Número de solicitações SIP descartadas
`core_err_replies`	Número de respostas de erro
`core_err_requests`	Número de solicitações de erro
`core_bad_URIs_rcvd`	Número de mensagens com URIs malformadas recebidas
`core_bad_msg_hdr`	Número de mensagens com cabeçalhos ruins/malformados
`core_unsupported_methods`	Número de solicitações com métodos SIP não suportados

Rastreamento de Diálogos

Nome da Métrica	Significado
`dialog_ng_active`	Número de diálogos atualmente ativos (respondidos/confirmados)
`dialog_ng_early`	Número de diálogos iniciais (tocando/estado provisório)
`dialog_ng_expired`	Número de diálogos que expiraram ou foram encerrados à força
`dialog_ng_processed`	Número total de diálogos processados desde o início

Estatísticas DNS

Nome da Métrica	Significado
`dns_failed_dns_request`	Número de consultas DNS falhadas
`dns_slow_dns_request`	Número de consultas DNS lentas (excedendo o limite)

IMS IPSec P-CSCF

Nome da Métrica	Significado
`ims_ipsec_pcscf_spi_free`	Número de valores SPI (Security Parameter Index) livres disponíveis para alocação
`ims_ipsec_pcscf_spi_total`	Capacidade total de SPI configurada para o sistema
`ims_ipsec_pcscf_spi_used`	Número de valores SPI atualmente alocados/usados
`ims_ipsec_pcscf_spi_utilization_pct`	Porcentagem de utilização do pool de SPI
`ims_ipsec_pcscf_worker_cache_size`	Tamanho do cache IPSec do processo trabalhador

IMS QoS (Interface Rx)

Métricas de Registro AAR

Nome da Métrica	Significado
`ims_qos_active_registration_rx_sessions`	Número de sessões de registro Rx atualmente ativas
`ims_qos_registration_aars`	Número total de mensagens AAR (Authorization-Authentication Request) de registro enviadas
`ims_qos_successful_registration_aars`	Número de transações AAR de registro bem-sucedidas
`ims_qos_failed_registration_aars`	Número de transações AAR de registro falhadas
`ims_qos_registration_aar_avg_response_time`	Tempo médio de resposta para mensagens AAR de registro em milissegundos
`ims_qos_registration_aar_response_time`	Tempo total de resposta para todas as mensagens AAR de registro em milissegundos
`ims_qos_registration_aar_replies_received`	Número total de respostas AAR de registro recebidas
`ims_qos_registration_aar_timeouts`	Número de timeouts de solicitações AAR de

Nome da Métrica	Significado
	registro

Métricas de AAR de Mídia

Nome da Métrica	Significado
`ims_qos_active_media_rx_sessions`	Número de sessões de mídia Rx atualmente ativas
`ims_qos_media_rx_sessions`	Número total de sessões de mídia Rx criadas
`ims_qos_media_aars`	Número total de mensagens AAR de mídia enviadas
`ims_qos_successful_media_aars`	Número de transações AAR de mídia bem-sucedidas
`ims_qos_failed_media_aars`	Número de transações AAR de mídia falhadas
`ims_qos_media_aar_avg_response_time`	Tempo médio de resposta para mensagens AAR de mídia em milissegundos
`ims_qos_media_aar_response_time`	Tempo total de resposta para todas as mensagens AAR de mídia em milissegundos
`ims_qos_media_aar_replies_received`	Número total de respostas AAR de mídia recebidas
`ims_qos_media_aar_timeouts`	Número de timeouts de solicitações AAR de mídia

Métricas ASR

Nome da Métrica	Significado
`ims_qos_asrs`	Número total de mensagens ASR (Abort-Session-Request) recebidas do PCRF

Localização de Usuários P-CSCF

Nome da Métrica	Significado
`ims_usrloc_pcscf_expired_contacts`	Número de associações de contato expiradas
`ims_usrloc_pcscf_registered_contacts`	Número de associações de contato atualmente registradas
`ims_usrloc_pcscf_registered_impus`	Número de IMPUs (Identidades Públicas IMS) atualmente registradas

Banco de Dados MySQL

Nome da Métrica	Significado
`mysql_driver_errors`	Número de erros de driver/conexão MySQL

Anti-Flood (Bloqueio de IP)

Nome da Métrica	Significado
`pike_blocked_ips`	Número de endereços IP atualmente bloqueados (detecção de inundação)

Módulo Registrar

Nome da Métrica	Significado
`registrar_accepted_regs`	Número de solicitações REGISTER aceitas (módulo registrar legado)
`registrar_rejected_regs`	Número de solicitações REGISTER rejeitadas (módulo registrar legado)
`registrar_default_expire`	Tempo de expiração padrão para registros em segundos
`registrar_default_expires_range`	Configuração de intervalo de expiração padrão
`registrar_expires_range`	Intervalo de expiração configurado
`registrar_max_contacts`	Número máximo de contatos permitidos por AOR
`registrar_max_expires`	Tempo máximo de expiração permitido em segundos

Estatísticas de Script

Nome da Métrica	Significado
`script_register_failed`	Número de tentativas de registro que falharam na lógica do script de roteamento
`script_register_success`	Número de registros bem-sucedidos processados pelo script de roteamento
`script_register_time`	Tempo total gasto processando registros no script de roteamento (milissegundos)

Transporte SCTP

Nome da Métrica	Significado
`sctp_assoc_shutdown`	Número de encerramentos de associação SCTP iniciados localmente
`sctp_comm_lost`	Número de associações SCTP perdidas devido a falha de comunicação
`sctp_connect_failed`	Número de tentativas de associação SCTP de saída que falharam
`sctp_current_opened_connections`	Número de associações SCTP atualmente abertas
`sctp_current_tracked_connections`	Número de associações SCTP atualmente rastreadas
`sctp_established`	Número total de associações SCTP estabelecidas
`sctp_local_reject`	Número de associações SCTP de entrada rejeitadas localmente
`sctp_remote_shutdown`	Número de encerramentos de associação SCTP iniciados pelo par
`sctp_send_failed`	Número de operações de envio SCTP que falharam
`sctp_send_force_retry`	Número de tentativas forçadas em envios SCTP que falharam

Nome da Métrica	Significado
`sctp_sendq_full`	Número de tentativas de envio que falharam devido à fila de envio cheia

Memória Compartilhada

Nome da Métrica	Significado
`shmem_fragments`	Número de fragmentos no pool de memória compartilhada (indica fragmentação)
`shmem_free_size`	Quantidade de memória compartilhada livre em bytes
`shmem_max_used_size`	Máximo de memória compartilhada usada desde o início em bytes
`shmem_real_used_size`	Memória compartilhada realmente usada incluindo sobrecarga do alocador em bytes
`shmem_total_size`	Tamanho total do pool de memória compartilhada em bytes
`shmem_used_size`	Memória compartilhada atualmente usada (somente dados do usuário) em bytes

Módulo SL (Sem Estado)

Contadores de Respostas Sem Estado por Classe

Nome da Métrica	Significado
`sl_1xx_replies`	Número de respostas 1xx sem estado enviadas
`sl_2xx_replies`	Número de respostas 2xx sem estado enviadas
`sl_3xx_replies`	Número de respostas 3xx sem estado enviadas
`sl_4xx_replies`	Número de respostas 4xx sem estado enviadas
`sl_5xx_replies`	Número de respostas 5xx sem estado enviadas
`sl_6xx_replies`	Número de respostas 6xx sem estado enviadas
`sl_xxx_replies`	Número de outras respostas sem estado enviadas

Contadores de Respostas Sem Estado Específicos

Nome da Métrica	Significado
`sl_200_replies`	Número de respostas 200 OK sem estado enviadas
`sl_202_replies`	Número de respostas 202 Accepted sem estado enviadas
`sl_300_replies`	Número de respostas 300 Multiple Choices sem estado enviadas
`sl_301_replies`	Número de respostas 301 Moved Permanently sem estado enviadas
`sl_302_replies`	Número de respostas 302 Moved Temporarily sem estado enviadas
`sl_400_replies`	Número de respostas 400 Bad Request sem estado enviadas
`sl_401_replies`	Número de respostas 401 Unauthorized sem estado enviadas
`sl_403_replies`	Número de respostas 403 Forbidden sem estado enviadas
`sl_404_replies`	Número de respostas 404 Not Found sem estado enviadas
`sl_407_replies`	Número de respostas 407 Proxy Authentication Required sem estado enviadas
`sl_408_replies`	Número de respostas 408 Request Timeout sem estado enviadas
`sl_483_replies`	Número de respostas 483 Too Many Hops sem estado enviadas

Nome da Métrica	Significado
`sl_500_replies`	Número de respostas 500 Server Internal Error sem estado enviadas

Estatísticas Gerais Sem Estado

Nome da Métrica	Significado
`sl_sent_replies`	Número total de respostas sem estado enviadas
`sl_sent_err_replies`	Número de respostas de erro sem estado enviadas
`sl_received_ACKs`	Número de mensagens ACK recebidas para transações sem estado
`sl_failures`	Número de falhas no envio de respostas sem estado

Transporte TCP

Nome da Métrica	Significado
`tcp_con_reset`	Número de conexões TCP redefinidas (RST recebido em conexão estabelecida)
`tcp_con_timeout`	Número de conexões TCP fechadas devido a timeout ocioso
`tcp_connect_failed`	Número de tentativas de conexão TCP de saída que falharam
`tcp_connect_success`	Número de conexões TCP de saída bem-sucedidas
`tcp_current_opened_connections`	Número de conexões TCP atualmente abertas
`tcp_current_write_queue_size`	Tamanho total atual das filas de escrita TCP em todas as conexões
`tcp_established`	Número total de conexões TCP estabelecidas (tanto de entrada quanto de saída)
`tcp_local_reject`	Número de conexões TCP de entrada rejeitadas localmente
`tcp_passive_open`	Número de conexões TCP de entrada aceitas
`tcp_send_timeout`	Número de operações de envio TCP que expiraram (modo assíncrono)

Nome da Métrica	Significado
`tcp_sendq_full`	Número de tentativas de envio que falharam porque a fila de envio estava cheia

Módulo TM/TMX (Transação)

Contadores de Tipo de Transação

Nome da Métrica	Significado
`tmx_UAC_transactions`	Número de transações UAC (cliente) criadas
`tmx_UAS_transactions`	Número de transações UAS (servidor) criadas
`tmx_active_transactions`	Número de transações atualmente ativas
`tmx_inuse_transactions`	Número de transações atualmente em uso

Conclusão de Transação por Status

Nome da Métrica	Significado
`tmx_2xx_transactions`	Número de transações concluídas com resposta 2xx
`tmx_3xx_transactions`	Número de transações concluídas com resposta 3xx
`tmx_4xx_transactions`	Número de transações concluídas com resposta 4xx
`tmx_5xx_transactions`	Número de transações concluídas com resposta 5xx
`tmx_6xx_transactions`	Número de transações concluídas com resposta 6xx

Estatísticas de Resposta de Transação

Nome da Métrica	Significado
`tmx_rpl_absorbed`	Número de respostas absorvidas pela camada de transação (duplicatas)
`tmx_rpl_generated`	Número de respostas geradas localmente pelo módulo de transação
`tmx_rpl_received`	Número de respostas recebidas para transações
`tmx_rpl_relayed`	Número de respostas retransmitidas pelo módulo de transação
`tmx_rpl_sent`	Número de respostas enviadas pelo módulo de transação

Localização de Usuários

Nome da Métrica	Significado
`usrloc_location_contacts`	Número de contatos no domínio 'location' (módulo usrloc padrão)
`usrloc_location_expires`	Número de contatos expirados no domínio 'location'
`usrloc_registered_users`	Número de usuários/AORs (Address of Records) registrados

---

Métricas I-CSCF

O I-CSCF compartilha a maioria das estatísticas SIP core com o P-CSCF. Consulte a seção Estatísticas SIP Core do P-CSCF acima. As métricas abaixo são específicas do I-CSCF.

Contexto Operacional do I-CSCF

O I-CSCF mantém uma lista de instâncias S-CSCF disponíveis para balanceamento de carga. Para um novo registro, o I-CSCF consulta o HSS para selecionar a instância S-CSCF correta. As métricas UAR e LIR abaixo rastreiam o sucesso dessas operações.

IMS I-CSCF (Interface Cx - Comunicação HSS)

O I-CSCF utiliza a interface Diameter Cx para se comunicar com o HSS (Home Subscriber Server). Ele envia consultas de localização de usuário e autorização.

Métricas UAR (User-Authorization-Request)

Nome da Métrica	Significado
`ims_icscf_uar_avg_response_time`	Tempo médio de resposta para mensagens UAR em milissegundos (calculado como uar_replies_response_time / uar_replies_received)
`ims_icscf_uar_replies_received`	Número total de respostas UAA (User-Authorization-Answer) recebidas do HSS
`ims_icscf_uar_replies_response_time`	Tempo total de resposta para todas as mensagens UAR em milissegundos
`ims_icscf_uar_timeouts`	Número de timeouts de solicitações UAR

Métricas LIR (Location-Info-Request)

Nome da Métrica	Significado
`ims_icscf_lir_avg_response_time`	Tempo médio de resposta para mensagens LIR em milissegundos (calculado como lir_replies_response_time / lir_replies_received)
`ims_icscf_lir_replies_received`	Número total de respostas LIA (Location-Info-Answer) recebidas do HSS
`ims_icscf_lir_replies_response_time`	Tempo total de resposta para todas as mensagens LIR em milissegundos
`ims_icscf_lir_timeouts`	Número de timeouts de solicitações LIR

Métricas Comuns

O I-CSCF também exporta as métricas comuns abaixo. A seção P-CSCF acima documenta essas métricas.

- **Métricas CDP (Diameter)** - Estatísticas do protocolo Diameter
- **Estatísticas SIP Core** - Contadores de solicitações/respostas por método e código de status
- **Estatísticas DNS** - Métricas de consultas DNS
- **Banco de Dados MySQL** - Erros de conexão com o banco de dados
- **Anti-Flood** - Estatísticas de bloqueio de IP
- **Memória Compartilhada** - Estatísticas de uso de memória
- **Módulo SL (Sem Estado)** - Contadores de respostas sem estado
- **Transporte TCP** - Estatísticas de conexão TCP
- **Módulo TM/TMX (Transação)** - Rastreamento de estado de transação

---

Métricas S-CSCF

O S-CSCF compartilha a maioria das estatísticas SIP core com o P-CSCF e I-CSCF. Consulte a seção Estatísticas SIP Core do P-CSCF acima. As métricas abaixo são específicas do S-CSCF.

Contexto Operacional do S-CSCF

O S-CSCF fornece informações detalhadas de localização do usuário. Ele também gerencia IFC (Critérios de Filtragem Inicial).

Uma pesquisa de localização do usuário mostra IMPUs registrados com associações de contato e perfis de serviço. As métricas `ims_usrloc_scscf_active_contacts` e `ims_usrloc_scscf_active_impus` rastreiam o número de contatos e IMPUs ativos.

IFC (Critérios de Filtragem Inicial) determina quais Servidores de Aplicação processam sessões SIP. O desempenho da avaliação de IFC pode alterar os tempos de configuração de chamadas. As métricas de transação (`tmx_*`) rastreiam esses tempos.

IMS ISC (Controle de Serviço IMS)

O módulo IMS ISC avalia os Critérios de Filtragem Inicial (iFC). Ele determina quais Servidores de Aplicação devem processar sessões SIP. Essas métricas rastreiam o desempenho e o efeito das operações de correspondência de iFC.

Nome da Métrica	Significado
`ims_isc_ifc_match_attempts`	Número total de tentativas de correspondência de iFC realizadas
`ims_isc_ifc_match_time_total`	Tempo acumulado gasto realizando operações de correspondência de iFC em milissegundos
`ims_isc_ifc_nomatch_count`	Número de tentativas de correspondência de iFC em que nenhum critério de disparo correspondeu

Monitoramento de Desempenho: Calcule o tempo médio de correspondência de iFC como `ifc_match_time_total / ifc_match_attempts`. Um tempo médio alto pode indicar critérios de filtragem complexos. Também pode mostrar um limite de desempenho na seleção do Servidor de Aplicação. Uma alta proporção de `ifc_nomatch_count` para `ifc_match_attempts` pode indicar pontos de disparo incorretos. Também pode mostrar padrões de tráfego inesperados.

IMS Autenticação (Interface Cx - MAR)

O S-CSCF utiliza a interface Diameter Cx para autenticar usuários com o HSS. Ele envia um MAR (Multimedia-Auth-Request).

Nome da Métrica	Significado
`ims_auth_mar_avg_response_time`	Tempo médio de resposta para mensagens MAR em milissegundos (calculado como mar_replies_response_time / mar_replies_received)
`ims_auth_mar_replies_received`	Número total de respostas MAA (Multimedia-Auth-Answer) recebidas do HSS
`ims_auth_mar_replies_response_time`	Tempo total de resposta para todas as mensagens MAR em milissegundos
`ims_auth_mar_timeouts`	Número de timeouts de solicitações MAR

IMS Registrar S-CSCF

Estatísticas de Registro

Nome da Métrica	Significado
`ims_registrar_scscf_accepted_regs`	Número de solicitações REGISTER aceitas com sucesso
`ims_registrar_scscf_rejected_regs`	Número de solicitações REGISTER rejeitadas
`ims_registrar_scscf_default_expire`	Tempo de expiração padrão para registros em segundos
`ims_registrar_scscf_default_expires_range`	Configuração de intervalo de expiração padrão
`ims_registrar_scscf_max_contacts`	Número máximo de contatos permitidos por registro
`ims_registrar_scscf_max_expires`	Tempo máximo de expiração permitido em segundos
`ims_registrar_scscf_notifies_in_q`	Número de mensagens NOTIFY pendentes na fila

Métricas SAR (Server-Assignment-Request)

Nome da Métrica	Significado
`ims_registrar_scscf_sar_avg_response_time`	Tempo médio de respos para mensagens SAR e milissegundos (calculad como sar_replies_response_ti / sar_replies_received)
`ims_registrar_scscf_sar_replies_received`	Número total de respostas SAA (Server-Assignment-Answer) recebidas do HSS
`ims_registrar_scscf_sar_replies_response_time`	Tempo total de resposta para todas as mensage SAR em milissegundos
`ims_registrar_scscf_sar_timeouts`	Número de timeouts de solicitações SAR

Localização de Usuários S-CSCF

Nome da Métrica	Significado
`ims_usrloc_scscf_active_contacts`	Número de associações de contato registradas ativas atualmente
`ims_usrloc_scscf_active_impus`	Número de IMPUs (Identidades Públicas IMS) registradas ativas atualmente
`ims_usrloc_scscf_active_subscriptions`	Número de assinaturas ativas atualmente
`ims_usrloc_scscf_contact_collisions`	Número de colisões de hash na tabela de hash de contatos
`ims_usrloc_scscf_impu_collisions`	Número de colisões de hash na tabela de hash de IMPU
`ims_usrloc_scscf_subscription_collisions`	Número de colisões de hash na tabela de hash de assinaturas

Rastreamento de Diálogos

O S-CSCF rastreia o estado do diálogo para chamadas ativas:

Nome da Métrica	Significado
`dialog_ng_active`	Número de diálogos atualmente ativos (respondidos/confirmados)
`dialog_ng_early`	Número de diálogos iniciais (tocando/estado provisório)
`dialog_ng_expired`	Número de diálogos que expiraram ou foram encerrados à força
`dialog_ng_processed`	Número total de diálogos processados desde o início

Métricas Comuns

O S-CSCF também exporta as métricas comuns abaixo. A seção P-CSCF acima documenta essas métricas.

- **Métricas CDP (Diameter)** - Estatísticas do protocolo Diameter
- **Estatísticas SIP Core** - Contadores de solicitações/respostas por método e código de status (observação: o S-CSCF roteia entre pontos finais. Geralmente, possui mais fwd_requests e fwd_replies.)
- **Estatísticas DNS** - Métricas de consultas DNS
- **Banco de Dados MySQL** - Erros de conexão com o banco de dados
- **Anti-Flood** - Estatísticas de bloqueio de IP
- **Memória Compartilhada** - Estatísticas de uso de memória
- **Módulo SL (Sem Estado)** - Contadores de respostas sem estado
- **Transporte TCP** - Estatísticas de conexão TCP
- **Módulo TM/TMX (Transação)** - Rastreamento de estado de transação (observação: o S-CSCF atua como cliente e servidor. Geralmente, possui transações UAC e UAS.)