Guide des opérations Diameter

Table des matières

1. Aperçu
2. Diameter dans l'architecture IMS
3. Interfaces Diameter
4. Gestion des pairs via OmniWeb
5. Codes de résultat Diameter
6. Problèmes courants

Aperçu

Diameter est le protocole d'authentification, d'autorisation et de comptabilité (AAA) pour l'architecture IMS. OmniCSCF utilise Diameter pour communiquer avec des éléments de réseau critiques. Ces éléments incluent le HSS, le PCRF et l'OCS.

Qu'est-ce que Diameter ?

Diameter (RFC 6733) est le successeur de RADIUS. Diameter prend en charge des scénarios AAA modernes :

- **Transport fiable** via TCP/SCTP. RADIUS utilise UDP.
- **Extensible** via des modules spécifiques à l'application
- **Architecture pair à pair**. Ce n'est pas seulement client-serveur.
- **Connexions avec état** avec surveillance de garde
- **Gestion des erreurs** et codes de résultat **standardisés**

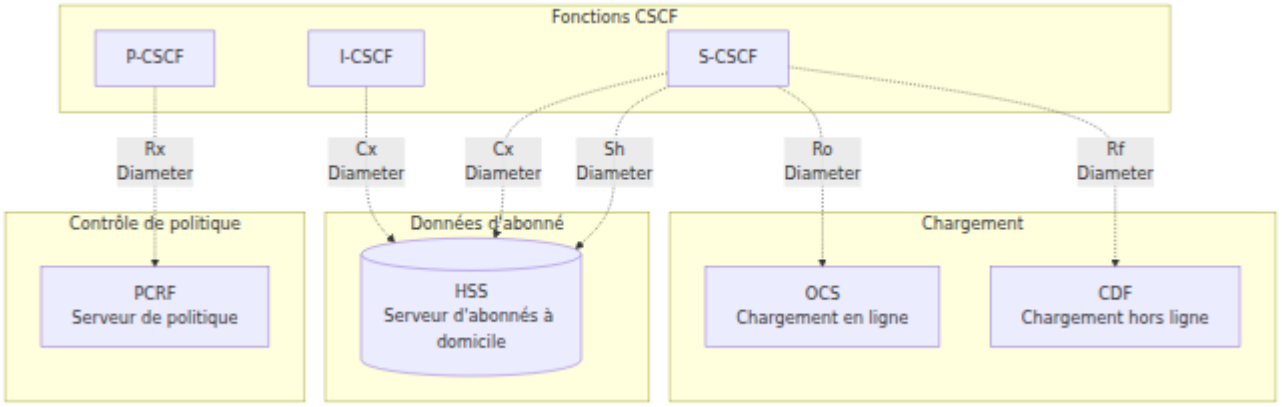
Diameter dans CSCF

Chaque composant CSCF utilise des interfaces d'application Diameter spécifiques :

CSCF	Interface	ID d'application	Connecté à	Objectif
I-CSCF	Cx	16777216	HSS	Sélection S-CSCF, localisation utilisateur
S-CSCF	Cx	16777216	HSS	Authentification utilisateur, téléchargement de profil
S-CSCF	Sh	16777217	HSS	Accès aux données utilisateur (optionnel)
P-CSCF	Rx	16777236	PCRF	Politique QoS et contrôle de porteur
S-CSCF	Ro	4	OCS	Chargement en ligne (contrôle de crédit)
S-CSCF	Rf	3	CDF	Chargement hors ligne (comptabilité)

Diameter dans l'architecture IMS

Aperçu du réseau



Interfaces Diameter

Interface Cx (CSCF ↔ HSS)

L'I-CSCF et le S-CSCF utilisent l'interface Cx pour l'authentification des utilisateurs et la gestion des profils.

Spécification 3GPP : TS 29.228

Opérations I-CSCF

Demande d'autorisation utilisateur (UAR) / Réponse d'autorisation utilisateur (UAA) :

- **Objectif** : Interroger le HSS pour l'attribution ou les capacités S-CSCF
- **Déclencheur** : L'I-CSCF reçoit un REGISTER de l'utilisateur
- **Cas d'utilisation** : L'I-CSCF doit acheminer l'enregistrement vers le S-CSCF correct

Demande d'informations de localisation (LIR) / Réponse d'informations de localisation (LIA) :

- **Objectif** : Interroger le HSS pour le S-CSCF actuel de l'utilisateur

- **Déclencheur** : L'I-CSCF reçoit un INVITE ou un MESSAGE pour l'utilisateur terminant
- **Cas d'utilisation** : L'I-CSCF doit acheminer la session vers le S-CSCF de l'utilisateur

Opérations S-CSCF

Demande d'authentification multimédia (MAR) / Réponse d'authentification multimédia (MAA) :

- **Objectif** : Récupérer les vecteurs d'authentification du HSS
- **Déclencheur** : Le REGISTER initial, avant le défi
- **Cas d'utilisation** : Le S-CSCF doit défier l'utilisateur pour l'authentification IMS AKA

Demande d'attribution de serveur (SAR) / Réponse d'attribution de serveur (SAA) :

- **Objectif** : Informer le HSS de l'état d'enregistrement et télécharger le profil utilisateur
- **Déclencheur** : Authentification réussie, après MAR/MAA
- **Cas d'utilisation** : Le S-CSCF télécharge l'IFC et le profil de service pour l'utilisateur

L'AVP `User-Data` dans la SAA contient le profil utilisateur complet. Ce profil inclut :

- Identités publiques
- Critères de filtrage initiaux (IFC) pour le déclenchement de services
- Identifiants de profil multimédia abonnés
- Informations de facturation

Demande de résiliation d'enregistrement (RTR) / Réponse de résiliation d'enregistrement (RTA) :

- **Objectif** : Désinscription initiée par le HSS. Le HSS pousse la demande.
- **Déclencheur** : Désinscription administrative ou changement d'abonnement

- **Cas d'utilisation** : Le HSS demande au S-CSCF de désinscrire un utilisateur

Interface Rx (P-CSCF ↔ PCRF)

L'interface Rx fournit un contrôle de politique et de QoS pour les sessions IMS.

Spécification 3GPP : TS 29.214

Remarque sur VoNR (5G NR) : Pour les sessions VoNR, le PCF autorise les médias et la QoS via l'interface N5 AF (Npcf_PolicyAuthorization, HTTP/2 SBI). Il n'utilise pas Diameter Rx. L'interface Rx ici s'applique donc à l'accès 4G/LTE.

Demande AA (AAR) / Réponse AA (AAA) :

- **Objectif** : Demander l'autorisation QoS pour une session multimédia
- **Déclencheur** : L'échange d'offre/réponse SDP dans un SIP INVITE
- **Cas d'utilisation** : Le P-CSCF demande au PCRF d'autoriser les ressources de porteur

Demande de ré-authentification (RAR) / Réponse de ré-authentification (RAA) :

- **Objectif** : Mise à jour de politique initiée par le PCRF. Le PCRF pousse la demande.
- **Déclencheur** : Un changement de politique ou une modification de porteur
- **Cas d'utilisation** : Le PCRF demande au P-CSCF de mettre à jour la politique QoS

Demande de résiliation de session (STR) / Réponse de résiliation de session (STA) :

- **Objectif** : Libérer la session Rx et les ressources de porteur
- **Déclencheur** : Résiliation d'appel. Le P-CSCF reçoit un BYE.
- **Cas d'utilisation** : Le P-CSCF informe le PCRF de libérer les ressources QoS

Interface Ro (S-CSCF ↔ OCS)

L'interface Ro fournit un chargement en ligne (contrôle de crédit).

Spécification 3GPP : TS 32.299

Demande de contrôle de crédit (CCR) / Réponse de contrôle de crédit (CCA) :

- **Objectif** : Autorisation de crédit en temps réel et débit
- **Déclencheur** : Établissement d'appel, en cours d'appel ou résiliation d'appel
- **Cas d'utilisation** : Chargement prépay►► et vérifications de crédit en temps réel

Types :

- **CCR-Initial** : Demander du crédit au début de l'appel
- **CCR-Update** : Rafraîchir le quota pendant l'appel
- **CCR-Terminate** : Signaler l'utilisation finale à la fin de l'appel

Gestion des pairs via OmniWeb

Consultez l'état des pairs Diameter, les applications prises en charge et les profondeurs de file d'attente dans l'onglet **Diameter** de chaque page CSCF dans OmniWeb. OmniWeb est le portail de gestion unifié : <https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>.

L'onglet Diameter d'OmniWeb affiche les éléments suivants par CSCF :

- Identité de domaine et d'origine Diameter
- Pairs configurés et leur état de connexion (I_Open, Closed, etc.)
- Applications Diameter prises en charge par pair, mappées aux noms d'interface 3GPP (Cx/Dx, Sh/Dh, Rx, Ro, Gx, S6a/S6d, et autres)
- Longueur de la file d'attente des travailleurs et transactions en attente
- Opérations d'activation/désactivation pour des pairs individuels

États des pairs

État	Description
I_Open	La connexion est ouverte et opérationnelle
Closed	Aucune connexion n'est établie
Wait-Conn-Ack	La connexion est initiée. Elle attend une réponse.
Wait-I-CEA	Le CER est envoyé. Il attend le CEA.

Codes de résultat Diameter

Le tableau suivant répertorie les codes de résultat courants et leurs significations :

Code	Nom	Signification	A
2xxx	**Succès**		
2001	DIAMETER_SUCCESS	Opération réussie	Aucun
3xxx	**Erreurs de protocole**		
3002	DIAMETER_UNABLE_TO_DELIVER	Impossible de router vers la destination	Vérifie connec pair
3003	DIAMETER_REALM_NOT_SERVED	Le domaine n'est pas reconnu	Vérifie configu domai
3007	DIAMETER_APPLICATION_UNSUPPORTED	L'application n'est pas prise en charge	Vérifie d'appli
4xxx	**Échecs transitoires**		
4001	DIAMETER_AUTHENTICATION_REJECTED	Échec de l'authentification	Vérifie identif
4010	DIAMETER_USER_UNKNOWN	L'utilisateur n'est pas provisionné	Vérifie provisi HSS
5xxx	**Échecs permanents**		
5001	DIAMETER_AVP_UNSUPPORTED	L'AVP n'est pas reconnu	Vérifie version protoc

Code	Nom	Signification	A
5002	DIAMETER_UNKNOWN_SESSION_ID	La session n'est pas trouvée	La ses expiré invalid
5003	DIAMETER_AUTHORIZATION_REJECTED	Non autorisé	Vérifie autoris l'utilisa
5012	DIAMETER_UNABLE_TO_COMPLY	Impossible de traiter la demande	Vérifie journa HSS/P

Problèmes courants

Interfaces Diameter critiques

Lorsqu'un pair Diameter tombe, l'impact et l'urgence de la récupération dépendent de l'interface affectée :

Interface	Impact si en panne	Priorité de récupération
Cx (HSS)	Pas de nouvelles inscriptions. Pas de mises à jour IFC.	Critique. Récupérer immédiatement.
Rx (PCRF)	Pas de QoS pour les nouveaux appels	Élevée. Récupérer dans les minutes.
Ro (OCS)	Pas de chargement prépayé. Le service peut continuer.	Élevée. Cela dépend de la politique.

Échecs de connexion des pairs

Symptôme : Le pair est bloqué dans l'état "Closed" ou "Wait-Conn-Ack"

Diagnostic :

1. Vérifiez la connectivité réseau :

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

2. Vérifiez les règles de pare-feu. Le port 3868 TCP doit être ouvert.
3. Vérifiez la configuration du pair (adresse IP, port)
4. Vérifiez les journaux du pair pour les tentatives de connexion

Résolution :

- Corrigez les problèmes de réseau et de pare-feu
- Vérifiez que le pair fonctionne et écoute sur le port 3868
- Vérifiez que le pair a la configuration correcte pour le CSCF
- Utilisez **Enable Peer** sur l'onglet Diameter d'OmniWeb pour réessayer la connexion

---

Échecs d'échange CER/CEA

Symptôme : Le pair est bloqué dans l'état "Wait-I-CEA", ou le CEA a un code d'erreur

Erreurs courantes :

- **5010 (NO_COMMON_APPLICATION)** : Vérifiez que les deux pairs prennent en charge la même application (par exemple, Cx = 16777216)
- **3003 (REALM_NOT_SERVED)** : Vérifiez que l'Origin-Realm correspond au domaine attendu du pair

Résolution :

- Vérifiez la configuration Diameter pour l'ID d'application et le domaine

- Assurez-vous que la configuration du pair correspond aux attentes du CSCF
- Consultez les journaux du backend CSCF pour des messages d'erreur détaillés

---

Problèmes d'interface Cx HSS

Symptôme : Échecs d'enregistrement et délais d'attente MAR/MAA

Erreurs courantes :

Code de résultat	Signification	Résolution
4010	USER_UNKNOWN	L'utilisateur n'est pas provisionné dans le HSS
4001	AUTHENTICATION_REJECTED	L'IMPI ou les identifiants sont incorrects
5012	UNABLE_TO_COMPLY	Erreur interne HSS. Vérifiez les journaux HSS.

Résolution :

- **USER_UNKNOWN** : Provisionnez l'utilisateur dans le HSS
- **AUTHENTICATION_REJECTED** : Vérifiez l'IMPI et le secret partagé dans le HSS
- **UNABLE_TO_COMPLY** : Vérifiez les journaux HSS et la connectivité de la base de données

---

Problèmes d'interface Rx PCRF

Symptôme : Les appels réussissent mais aucune QoS n'est appliquée. Des délais d'attente AAR/AAA se produisent.

Problèmes courants :

- **PCRF en panne** : Vérifiez l'état du pair sur l'onglet Diameter d'OmniWeb
- **Framed-IP-Address non reconnu** : Le PCRF ne peut pas mapper l'IP UE à l'abonné
- **Politique non appliquée** : Vérifiez les règles de politique PCRF. Vérifiez l'intégration PCEF.

Résolution :

- Vérifiez que le pair PCRF est dans l'état "I_Open"
- Vérifiez le provisionnement de l'adresse IP UE dans le PCRF
- Vérifiez que l'interface Gx (PCRF à PCEF) fonctionne

Problèmes d'interface Ro OCS

Symptôme : Les appels prépayés échouent. Des délais d'attente CCR/CCA se produisent. Les appels sont bloqués.

Erreurs courantes :

Code de résultat	Signification	Résolution
4012	CREDIT_LIMIT_REACHED	Crédit insuffisant
5003	AUTHORIZATION_REJECTED	L'utilisateur n'est pas autorisé pour le prépayé

Résolution :

- **CREDIT_LIMIT_REACHED** : Normal pour les utilisateurs prépayés sans crédit
- **Délai d'attente OCS** : Vérifiez la disponibilité de l'OCS et l'état du pair
- **AUTHORIZATION_REJECTED** : Vérifiez que l'utilisateur est provisionné pour le prépayé dans l'OCS

Dégradation des performances

Symptôme : Temps de réponse Diameter lents et forte latence

Diagnostic :

1. Vérifiez l'horodatage "Last Used" dans la liste des pairs. Il doit être récent.
2. Surveillez la "Longueur de la file d'attente". Des valeurs élevées indiquent un arriéré.
3. Consultez les journaux du backend CSCF pour des avertissements de délai d'attente

Résolution :

- **Haute latence** : Enquêtez sur le réseau entre le CSCF et le pair
- **Longueur de file d'attente élevée** : Vérifiez la charge système du pair (HSS/PCRF/OCS)
- **Délai d'attente** : Si le réseau a une haute latence, augmentez le délai d'attente des transactions

Meilleures pratiques

Directives opérationnelles

Gestion des pairs :

- Surveillez l'état des pairs sur l'onglet Diameter d'OmniWeb
- Mettez en place une surveillance externe pour les événements de panne de pair
- Testez la connectivité des pairs pendant les fenêtres de maintenance

Planification de la capacité :

- Estimez le taux de transaction Diameter à partir des enregistrements et du volume d'appels

- Assurez-vous que le HSS/PCRF/OCS peut gérer les taux de transaction de pointe
- Pour les grandes déploiements, envisagez des agents de routage Diameter (DRA)

Dépannage :

- Vérifiez d'abord l'état des pairs lorsque vous enquêtez sur des échecs d'enregistrement ou d'appel
- Corrélez les échecs Diameter avec les échecs SIP (même Call-ID ou utilisateur)
- Consultez les journaux du backend CSCF pour des traces de transactions Diameter détaillées

Sécurité :

- Utilisez TLS pour les connexions Diameter en production, si TLS est pris en charge
- Restreignez l'accès des pairs Diameter avec le pare-feu. Autorisez uniquement les pairs connus.
- Consultez régulièrement les journaux d'audit d'activation/désactivation des pairs

Limitations et améliorations futures

Mise en œuvre actuelle

L'onglet Diameter d'OmniWeb fournit :

- □ Visualisation en temps réel de l'état des pairs
- □ Opérations d'activation/désactivation des pairs
- □ Mappage de l'ID d'application aux noms d'interface

Pas encore implémenté

Les fonctionnalités suivantes ne sont **pas actuellement disponibles**. Les versions futures peuvent les ajouter :

- **Inspecteur de messages Diameter** : Voir les transactions Diameter récentes et les détails des AVP
- **Statistiques des pairs** : Comptes de messages, taux de réussite et latence moyenne par pair
- **Surveillance de garde** : État DWR/DWA en temps réel

Solutions de contournement

Pour l'inspection des messages : Consultez les journaux du backend CSCF, ou activez la journalisation de débogage Diameter

Pour des statistiques détaillées : Interrogez les métriques à partir du point de terminaison Prometheus. Voir Référence des métriques pour les définitions complètes des métriques CDP/Diameter et la configuration de surveillance.

Pour une reconnexion manuelle : Utilisez l'onglet Diameter d'OmniWeb pour désactiver puis réactiver le pair

Documentation connexe

- **Guide des opérations P-CSCF** - Opérations d'interface Rx P-CSCF
- **Guide des opérations I-CSCF** - Opérations d'interface Cx I-CSCF
- **Guide des opérations S-CSCF** - Interfaces Cx, Ro S-CSCF
- **Guide des opérations 5G SBI** - Interfaces basées sur les services N5/NRF utilisées pour VoNR (l'équivalent 5G de Rx)
- **Référence des métriques** - Métriques et surveillance CDP/Diameter
- **OmniWeb** - Gestion des pairs Diameter via l'onglet Diameter d'OmniWeb
- **Guide des opérations CSCF** - Opérations CSCF générales

Spécifications 3GPP

- **TS 29.228** : Interfaces Cx et Dx (CSCF-HSS)
- **TS 29.214** : Interface Rx (P-CSCF-PCRF)
- **TS 32.299** : Applications de facturation Diameter (Ro, Rf)
- **RFC 6733** : Protocole de base Diameter

Détails techniques

Mise en œuvre

- **Pile Diameter** : Pile de protocole Diameter intégrée
- **Interface de gestion** : Protocole RPC vers le backend CSCF
- **Portail de gestion** : OmniWeb (<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>)

Configuration des pairs (Déploiement)

Chaque nœud CSCF a un fichier de configuration de pair Diameter : `pcscf.xml`, `icscf.xml` ou `scscf.xml`. Ansible rend le fichier au moment du déploiement. Le fichier définit l'identité Diameter du nœud et les pairs HSS/PCRF/DRA auxquels il se connecte. La structure est identique dans les trois fichiers. Seule l'application annoncée diffère.

Champ XML	Ce qu'il configure	Source Ansibl
`DiameterPeerFQDN`	Le FQDN d'origine Diameter de ce nœud	`<inventory_hostname>.epc.mnc<mnc>.m`
`DiameterPeerRealm`	Le domaine Diameter local	`ims_realm` s'il est défini, sinon `epc.mnc<mnc>.mcc<mcc>.3gppnetwork.o`
`Vendor_Id` / `Product_Name`	L'identité CER	`10415` (3GPP) / `OmniCSCF`
`Peer` (mode direct)	Pair direct vers chaque hôte de groupe `hss` via SCTP:3868	rendu par hôte dans `groups['hss']` lors faux
`Peer` (mode DRA)	Pair vers chaque hôte de groupe `dra`. IP explicite lorsque `diameter_dra_ip` est défini.	rendu par hôte dans `groups['dra']` lors vrai
`Acceptor`	FQDN et port de liaison locaux pour Diameter entrant (3868)	FQDN du nœud
`DefaultRoute`	Route par défaut de routage de domaine vers le pair HSS/PCRF (métrique 1) ou	rendu à partir de `groups['hss']` / `group`

Champ XML	Ce qu'il configure	Source Ansibl
	le DRA (métrique 2)	

Applications annoncées par nœud :

Nœud (fichier)	Application(s)
P-CSCF (`pcscf.xml`)	**Rx** `16777236` (vendeurs 10415, 0)
I-CSCF (`icscf.xml`)	**Cx** `16777216` (vendeurs 10415, 13019, 0) + comptabilité de base `4`
S-CSCF (`scscf.xml`)	**Cx** `16777216` (vendeurs 10415, 13019, 0) + comptabilité de base `4`

Les principales variables Ansible sont les suivantes. `plmn_id.mcc` et `plmn_id.mnc_longform` construisent tous les FQDN et domaines. `ims_realm` remplace le domaine Diameter. `ims_dra_support` bascule entre le pair direct et le pair DRA. `diameter_dra_ip` définit l'IP statique pour le pair DRA. Les groupes d'inventaire `hss` et `dra` fournissent les listes de pairs et de routes par défaut. Lorsque la facturation est activée, `RO_DESTINATION` adresse le pair **Ro** (OCS) du S-CSCF séparément. Le XML ne traite pas ce pair.

Modifiez ces fichiers via les outils de déploiement, pas via OmniWeb. OmniWeb fournit uniquement une surveillance et un contrôle opérationnel (activation/désactivation).

Opérations et Référence de l'I-CSCF

Le Interrogating-CSCF est le point de contact entrant du réseau domestique pour le signalement IMS. Un abonné atteint ce nœud lorsque l'abonné s'enregistre. Une session atteint ce nœud lorsque la session se termine vers un abonné domestique. L'I-CSCF ne conserve aucun état de session. L'I-CSCF ne termine aucun média. L'I-CSCF consulte le HSS via Cx. Cette consultation décide quel Serving-CSCF gère une demande donnée. Lors de l'enregistrement, l'I-CSCF autorise l'identité et le réseau visité. L'I-CSCF découvre ensuite le S-CSCF, ou les capacités du S-CSCF pour en sélectionner un. Lors d'une demande de terminaison, l'I-CSCF localise le S-CSCF qui sert déjà l'utilisateur. Après que l'I-CSCF ait choisi un S-CSCF, l'I-CSCF transmet la demande à ce S-CSCF. L'I-CSCF relaie les réponses.

Fonctions IMS

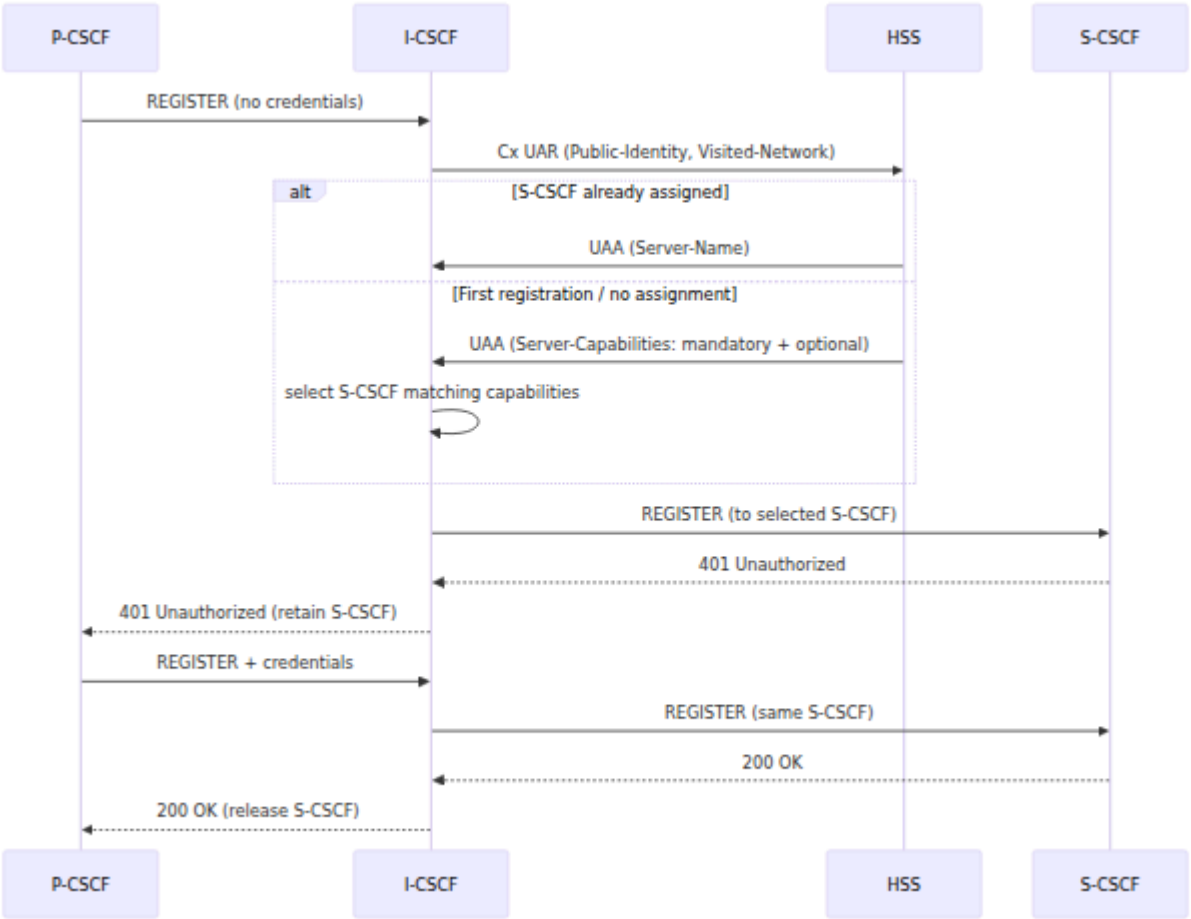
Routage d'enregistrement (Cx UAR)

Lorsqu'un REGISTER arrive, l'I-CSCF interroge le HSS avec un Cx **User-Authorization-Request (UAR)**. L'I-CSCF envoie cette requête avant de transmettre le REGISTER. L'UAR contient l'identité publique et l'identifiant du réseau visité. Ces valeurs permettent au HSS d'autoriser l'abonné à s'enregistrer depuis ce réseau. La réponse (UAA) retourne l'une des deux choses :

- **Un nom de S-CSCF déjà attribué.** L'I-CSCF utilise ce nom directement. Une réinscription retourne au même S-CSCF qui détient la liaison.
- **Capacités du S-CSCF.** Ce sont un ensemble de valeurs de capacité obligatoires et optionnelles que le S-CSCF sélectionné doit satisfaire. Le HSS retourne ces valeurs lors du premier enregistrement, ou lorsque aucun S-CSCF n'est actuellement attribué. L'I-CSCF effectue alors une sélection basée sur les capacités (ci-dessous).

L'I-CSCF transmet le REGISTER au S-CSCF choisi. L'I-CSCF se souvient de ce S-CSCF pendant la durée de la poignée de main d'enregistrement. Le re-REGISTER authentifié suit le défi 401. L'I-CSCF achemine ce re-REGISTER vers le **même** S-CSCF et ne questionne pas à nouveau. L'I-CSCF conserve le S-CSCF tant qu'un 401 est en cours. L'I-CSCF abandonne le S-CSCF lorsque l'enregistrement est terminé (2xx) ou échoue finalement.

Un HSS qui est indisponible ou retourne une réponse malformée produit **503**. Un UAR peut autoriser mais ne pas fournir de S-CSCF à sélectionner. Dans ce cas, l'I-CSCF revient à un URI S-CSCF par défaut configuré.



Routage de terminaison (Cx LIR)

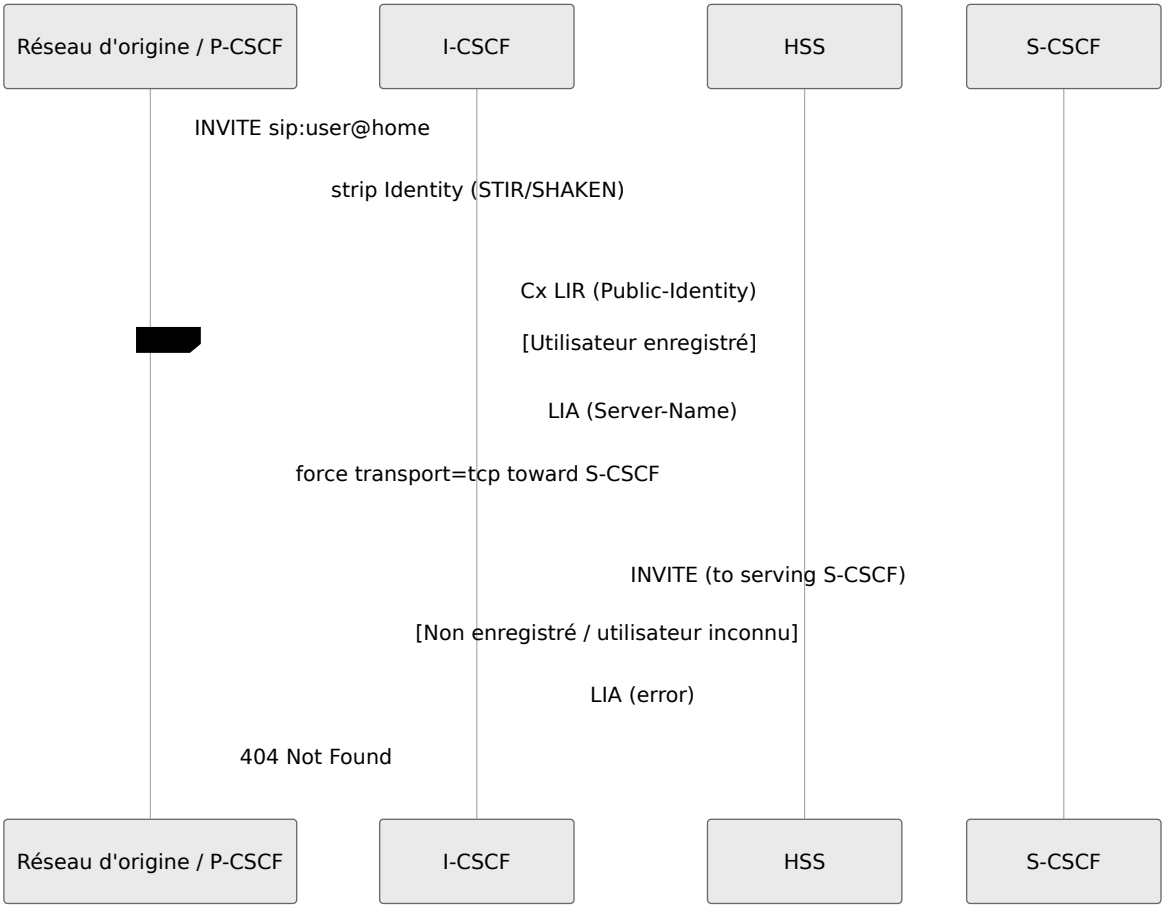
Une demande de terminaison initiale est un INVITE, SUBSCRIBE, MESSAGE, INFO ou PUBLISH. Lors d'une telle demande, l'I-CSCF interroge le HSS avec un Cx **Location-Info-Request (LIR)** pour l'identité Request-URI. La réponse (LIA) retourne le nom du S-CSCF qui sert actuellement l'utilisateur. Pour un utilisateur non enregistré qui a des services provisionnés, la LIA retourne des

capacités à la place. L'I-CSCF sélectionne ensuite un S-CSCF parmi ces capacités. L'I-CSCF transmet la demande à ce S-CSCF. Si l'URI retourné ne spécifie pas de transport, l'I-CSCF force le transport TCP vers le S-CSCF. L'I-CSCF supprime tout en-tête `Identity` STIR/SHAKEN entrant avant de transmettre la demande.

Gestion des résultats :

- **Succès.** L'I-CSCF sélectionne le S-CSCF et relaie la demande à celui-ci. Un échec de relais retourne **500**.
- **Utilisateur non trouvé / non enregistré.** L'I-CSCF retourne **404 Not Found**.
- **HSS indisponible.** L'I-CSCF retourne **503**.

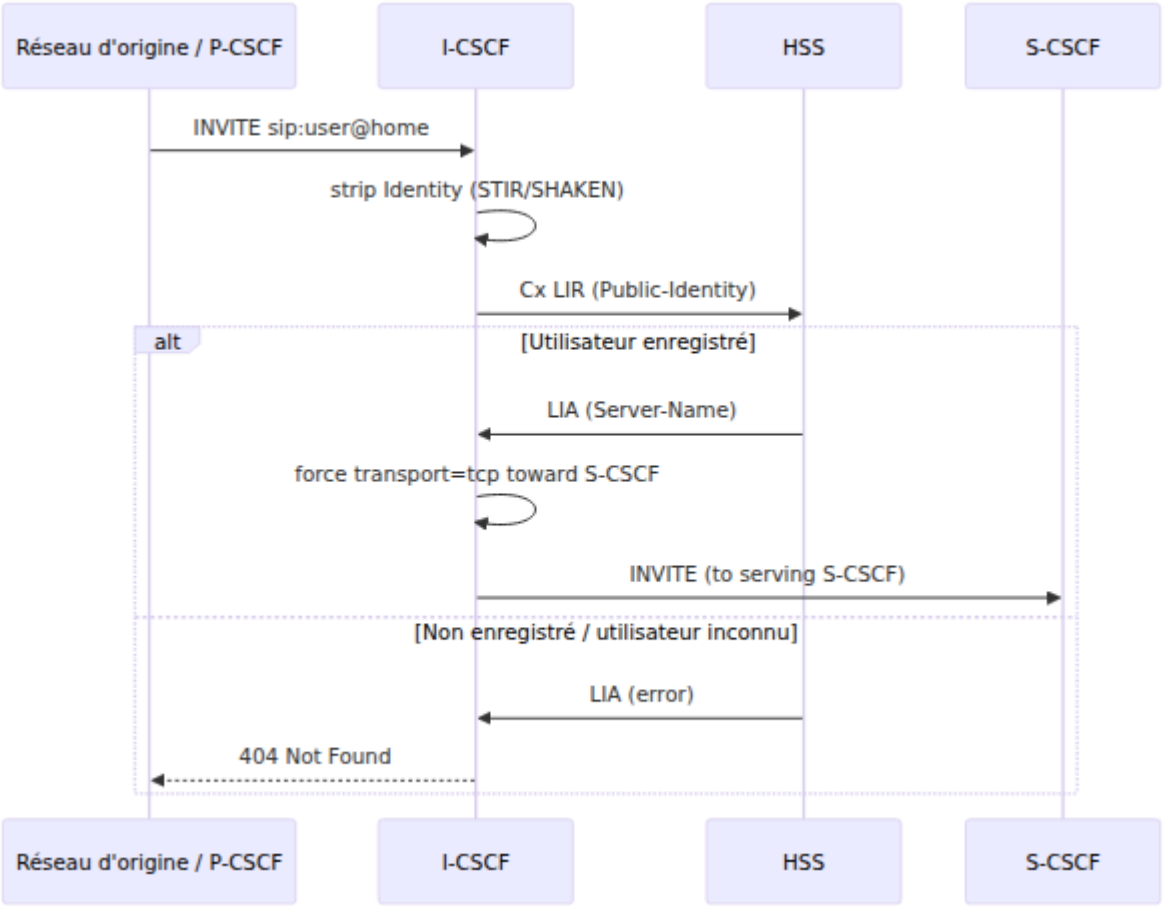
L'I-CSCF n'interroge pas CANCEL. L'I-CSCF associe CANCEL à sa transaction existante et le relaie. L'I-CSCF rejette toute autre méthode non initiale, non REGISTER avec **406** et une liste `Allow`.



Sélection du S-CSCF / correspondance des capacités

Le HSS peut retourner des capacités au lieu d'un nom de S-CSCF attribué. Dans ce cas, l'I-CSCF sélectionne un S-CSCF parmi son **ensemble S-CSCF configuré**. Chaque S-CSCF candidat a un URI SIP et un ensemble de valeurs de capacité. La sélection nécessite que le S-CSCF satisfasse **toutes les capacités obligatoires**. Parmi les candidats qualifiés, l'I-CSCF préfère ceux qui correspondent à plus de **capacités optionnelles**. Plusieurs candidats peuvent être également adaptés. Ces candidats forment une liste de candidats ordonnée. Cette liste permet à l'I-CSCF d'essayer un alternatif en cas d'échec.

L'I-CSCF conserve la liste des candidats en mémoire transactionnelle pendant la durée de la demande. Cela préserve la position de la liste à travers les tentatives. Un segment REGISTER transféré peut expirer ou recevoir un 5xx/6xx. Dans ce cas, l'I-CSCF passe au S-CSCF candidat suivant et réessaie. Lorsque la liste est épuisée, l'I-CSCF s'arrête. L'I-CSCF conserve la liste à travers un défi 401, car le même S-CSCF doit gérer la nouvelle tentative authentifiée. L'I-CSCF abandonne la liste lors d'une réponse finale réussie ou d'erreur client. Si la sélection ne donne rien du tout, l'I-CSCF revient à l'URI S-CSCF par défaut configuré.



Configuration de Déploiement (Injecté par Ansible)

Ansible génère la configuration d'exécution de l'I-CSCF (`icscf.cfg`) et sa table de pairs Diameter (`icscf.xml`) au moment du déploiement. Les valeurs dérivent de l'identité PLMN du réseau (MCC/MNC) et du nom d'hôte de l'inventaire du nœud. Les commutateurs de fonctionnalités sont des drapeaux `#!define`. Un drapeau défini active la fonctionnalité. Un drapeau commenté désactive la fonctionnalité.

Identité / domaine

Nom	Ce qu'il contrôle	Valeur / d
`NETWORKNAME`	Domaine IMS domestique. C'est le domaine de destination Cx (`cxdx_dest_realm`). L'I-CSCF vérifie ce domaine lorsqu'il achemine des demandes d'abonnés ou inconnues.	`ims.mnc<mnc>.mcc<mcc>.3gppnet`
`HOSTNAME`	FQDN (alias d'hôte) de ce nœud	`<inventory_hostname>.ims.mnc<`
`ICSCF_USER_AGENT`	L'en-tête `User-Agent` que le nœud émet	`User-Agent: Omnitouch I-CSCF`
`ICSCF_SERVER`	L'en-tête `Server` que le nœud émet	`Server: Omnitouch I-CSCF <inv`
`SCSCF_URI`	URI S-CSCF par défaut ou de secours. L'I-CSCF utilise cet URI lorsque la sélection basée sur UAR ne produit aucun S-CSCF.	`sip:scscf.ims.mnc<mnc>.mcc<mc`

Ansible modèle les sockets d'écoute SIP (UDP/TCP 5060, TLS 9090) à partir de l'adresse de l'hôte d'inventaire et du PLMN. Ansible modèle également les alias

d'hôte (`ims.…`, `icscf.ims.…`, `<host>.ims.…`) à partir de ces valeurs.

`CAPTURE_NODE` est la cible de capture Homer, `sip:<homer_host>:9060`. Ansible modèle cette valeur uniquement lorsque la capture Homer est activée pour le déploiement. La capture Homer nécessite `enable_homer` avec un groupe d'inventaire `homer`. `CAPTURE_NODE` duplique le signalement SIP vers Homer via HEP pour le traçage.

Configuration des pairs Diameter

La table des pairs Diameter de l'I-CSCF (`icscf.xml`) annonce l'application **Cx** (`16777216`) vers le HSS. Tous les CSCFs partagent la structure de fichier et les variables Ansible qui la remplissent. Voir Diameter → Configuration des Pairs (Déploiement).

Dépannage

Les échecs d'enregistrement ou d'échec de session de terminaison se manifestent à l'I-CSCF. Ces échecs proviennent généralement de l'une des deux causes :

- **Sélection / attribution du S-CSCF.** Le HSS peut retourner des capacités au lieu d'un nom de S-CSCF attribué. La sélection nécessite alors que le S-CSCF satisfasse toutes les capacités obligatoires. Si aucun candidat ne se qualifie, l'I-CSCF revient à l'URI S-CSCF par défaut configuré. Si un REGISTER transféré entraîne un délai d'attente ou un 5xx/6xx, l'I-CSCF passe au candidat suivant jusqu'à épuisement de la liste. Confirmez que l'ensemble S-CSCF configuré et ses valeurs de capacité correspondent à ce que retourne le HSS.
- **Connectivité Cx au HSS (UAR / LIR).** L'I-CSCF ne peut pas acheminer sans réponse au Cx UAR (sur REGISTER) ou LIR (sur une demande de terminaison). Une réponse HSS indisponible ou malformée produit **503**. Un utilisateur qui est inconnu ou non enregistré produit **404**. Vérifiez que le pair Cx vers le HSS est opérationnel. Voir Opérations Diameter.

Flux d'Appels

Les diagrammes de séquence apparaissent avec les fonctions qu'ils documentent :

- Enregistrement via I-CSCF → Routage d'enregistrement (Cx UAR)
- Session de terminaison via I-CSCF → Routage de terminaison (Cx LIR)
- Échec de S-CSCF → Sélection du S-CSCF / correspondance des capacités

Documentation Connexe

- Opérations et Référence du S-CSCF
- Opérations
- Diameter
- Référence des Métriques
- OmniWeb - liste S-CSCF, sessions actives et état des pairs Diameter Cx : <https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>

Opérations et Référence P-CSCF

Le Proxy-CSCF est le point d'entrée SIP de l'IMS pour l'équipement utilisateur. Chaque enregistrement et chaque session de l'UE arrive ici en premier. Le P-CSCF établit et applique l'association de sécurité d'accès qui protège la signalisation de l'UE. Le P-CSCF s'insère dans le chemin de routage. Il ajoute un en-tête Path lors de l'enregistrement et un enregistrement de route lors des sessions. Tout le trafic ultérieur traverse alors ce nœud. Ce trafic comprend les demandes de terminaison et les messages en dialogue. Le P-CSCF détecte la technologie d'accès de l'UE pour gérer la politique de support multimédia. Le P-CSCF fournit également au point d'entrée de session d'urgence (E-CSCF) une identité de ligne d'appel utilisable par rapport à la TS 23.167. Le P-CSCF est uniquement un proxy de signalisation. Les flux multimédias passent directement entre l'UE et le côté de terminaison. Les flux multimédias ne passent jamais par ce nœud.

Fonctions IMS

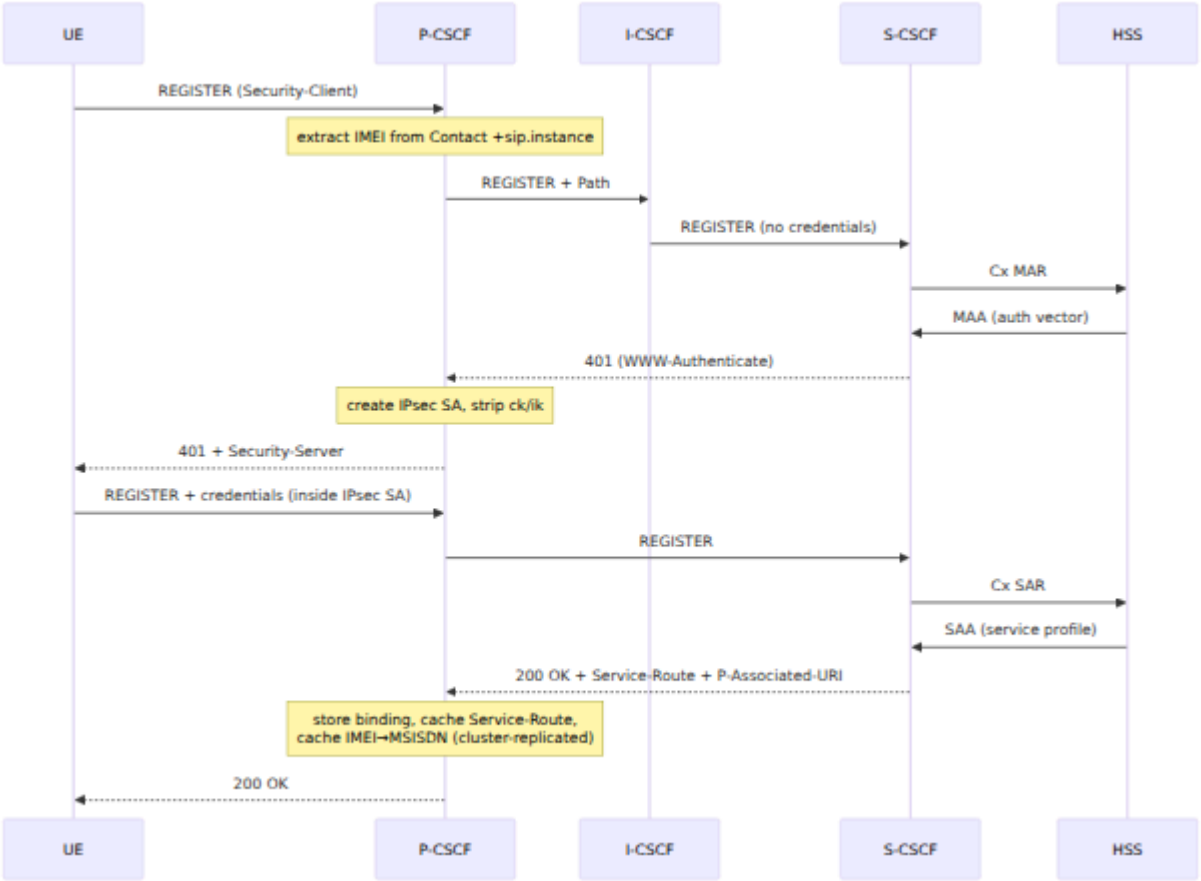
Proxy d'enregistrement & association de sécurité IPsec

Le P-CSCF est le proxy faisant face à l'enregistrement de l'UE. Le P-CSCF relaie l'enregistrement vers le réseau domestique (I-CSCF/S-CSCF). Lors de l'échange de défi/réponse, le P-CSCF établit une association de sécurité IPsec ESP avec l'UE. Cela fait partie de la procédure IMS-AKA. Pendant l'enregistrement, l'UE et le P-CSCF négocient les paramètres SA via les en-têtes `Security-Client` / `Security-Server`. À partir de l'enregistrement re-authentifié, la SA transporte toute la signalisation pour cet UE.

Sur l'enregistrement transféré, le P-CSCF insère un en-tête **Path**. Cela route les demandes de terminaison à travers ce même nœud. Le P-CSCF force l'expiration de l'enregistrement à une valeur contrôlée par le réseau. Le P-CSCF annonce le support `path`. Lors du `200 OK` réussi, le P-CSCF stocke le lien de

contact. Le P-CSCF met en cache le `Service-Route` et le `P-Associated-URI` retournés. Cela dirige les demandes ultérieures à travers le bon chemin du réseau domestique.

Chaque UE enregistré utilise **une** association de sécurité d'un pool de ressources par déploiement. Le P-CSCF libère la SA lorsque l'UE se désenregistre (expiration 0) ou que son enregistrement expire. Le P-CSCF rejette un enregistrement dont le Contact marque un enregistrement d'urgence (`;sos`). Le P-CSCF gère les sessions d'urgence directement sur l'INVITE, et non via l'enregistrement d'urgence.



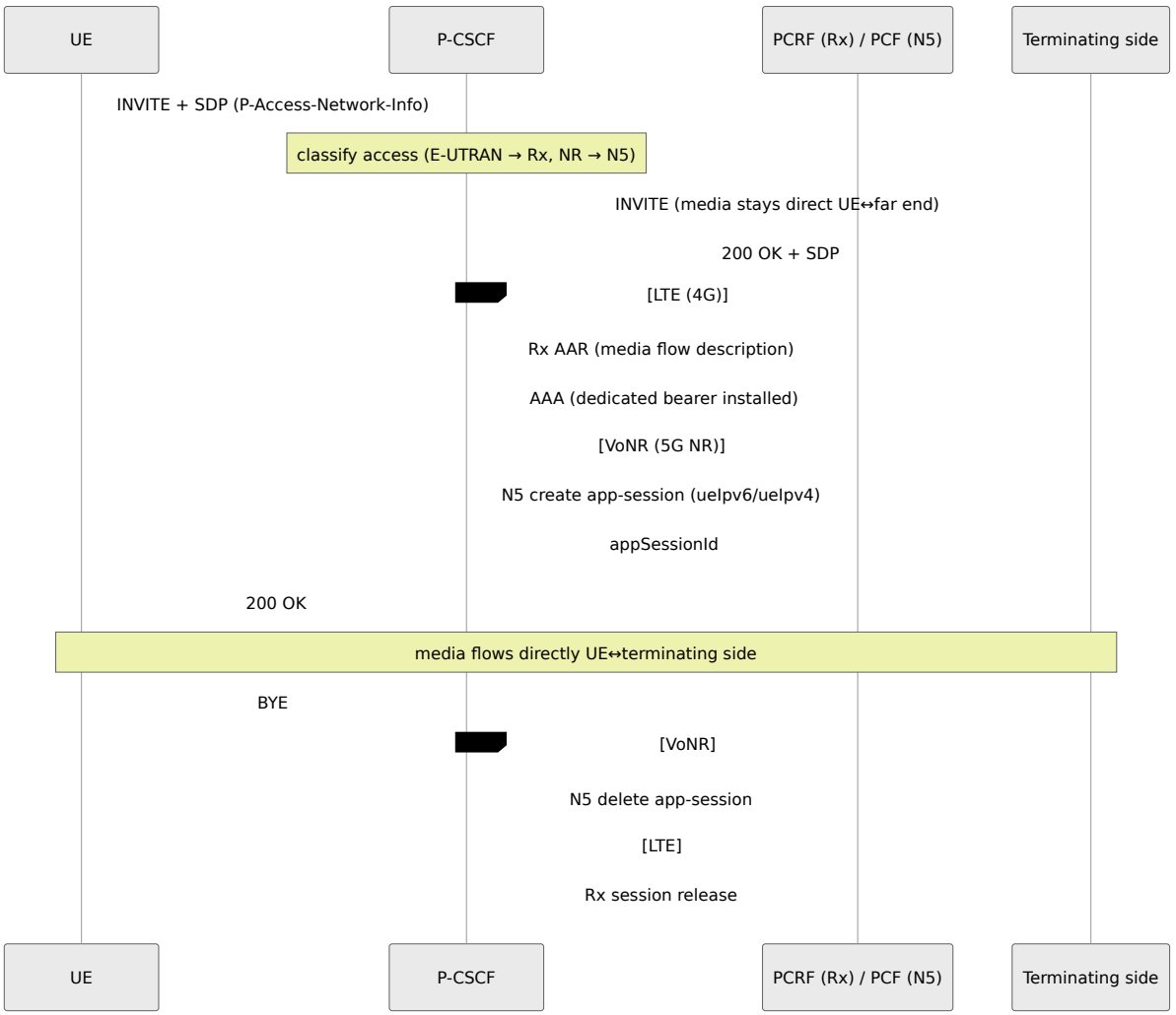
Détection d'accès & contrôle de QoS / politique

Le P-CSCF ne relaie jamais les médias. Le P-CSCF autorise néanmoins le support multimédia dédié avec le plan de politique. Le P-CSCF classe l'accès de l'UE à partir de l'en-tête `P-Access-Network-Info` (selon la TS 24.229 §5.2.6.3). LTE rapporte `3GPP-E-UTRAN`. 5G NR rapporte `3GPP-NR`. L'accès WiFi n'a pas de porteur dédié. Le P-CSCF exclut l'accès WiFi du QoS dynamique.

- **4G / LTE** - le P-CSCF autorise le QoS du porteur multimédia via **Diameter Rx** vers le PCRF. Sur la branche de réponse (le `200 OK` portant SDP), le P-CSCF émet une demande d'autorisation/authentification (AAR). L'AAR décrit le flux multimédia audio, et le flux multimédia vidéo le cas échéant. Le PCRF installe alors le porteur dédié correspondant. Le P-CSCF rafraîchit l'autorisation lors des re-INVITES en dialogue. Le P-CSCF libère l'autorisation lorsque le dialogue se termine.
- **VoNR (5G NR)** - le P-CSCF autorise le QoS du porteur via l'interface **N5** vers le PCF. Le P-CSCF utilise le service `Npcf_PolicyAuthorization`. Le P-CSCF agit en tant que fonction d'application. Lorsque l'autre extrémité répond au média, le P-CSCF crée une session d'application sur le PCF. Cette session utilise afAppId `VoNR`, un composant multimédia `AUDIO` avec un statut de flux `ENABLED`, et un descripteur de flux pour le média de l'UE. Elle inclut également une URI de notification AF pour que le PCF rappelle. Le P-CSCF supprime cette session d'application lorsque le dialogue se termine.

L'autorisation QoS s'exécute sur les deux branches, d'origine (MO) et de terminaison (MT). Elle est basée sur l'adresse IP propre de l'UE. **Liaison d'adresse UE :** le P-CSCF encode l'adresse de l'UE pour correspondre à la liaison de session PDU/porteur que le nœud de politique détient. Le P-CSCF signale un UE IPv6 comme `ueIpv6` et un UE IPv4 comme `ueIpv4`. Une adresse v6 placée dans le champ v4 ne correspond jamais à la liaison PCF. Le PCF n'installe alors aucun porteur dédié.

Pour VoNR, le P-CSCF localise le PCF de service via la **découverte NRF**. Le P-CSCF s'enregistre en tant qu'AF. Pour chaque session, le P-CSCF résout le PCF lié à la session PDU de l'UE via la chaîne NRF→BSF. C'est le seul chemin de découverte PCF.



Appels d'urgence (E-CSCF) & identité de ligne d'appel - TS 23.167

Le P-CSCF est le point d'entrée d'urgence. Le P-CSCF détecte une session d'urgence par l'URN de service d'urgence (`urn:service:sos`) sur l'INVITE. Le P-CSCF le route directement vers le serveur d'application d'urgence. Cela contourne la vérification d'enregistrement normale. Un INVITE d'urgence porte souvent **aucun MSISDN**. Le P-CSCF fournit donc une identité de ligne d'appel utilisable pour le PSAP. Cela s'applique même aux appelants qui sont inconnus ou anonymes. Cela est conforme à l'annexe K de la TS 23.167 et à la §4.4.6a de la TS 29.214.

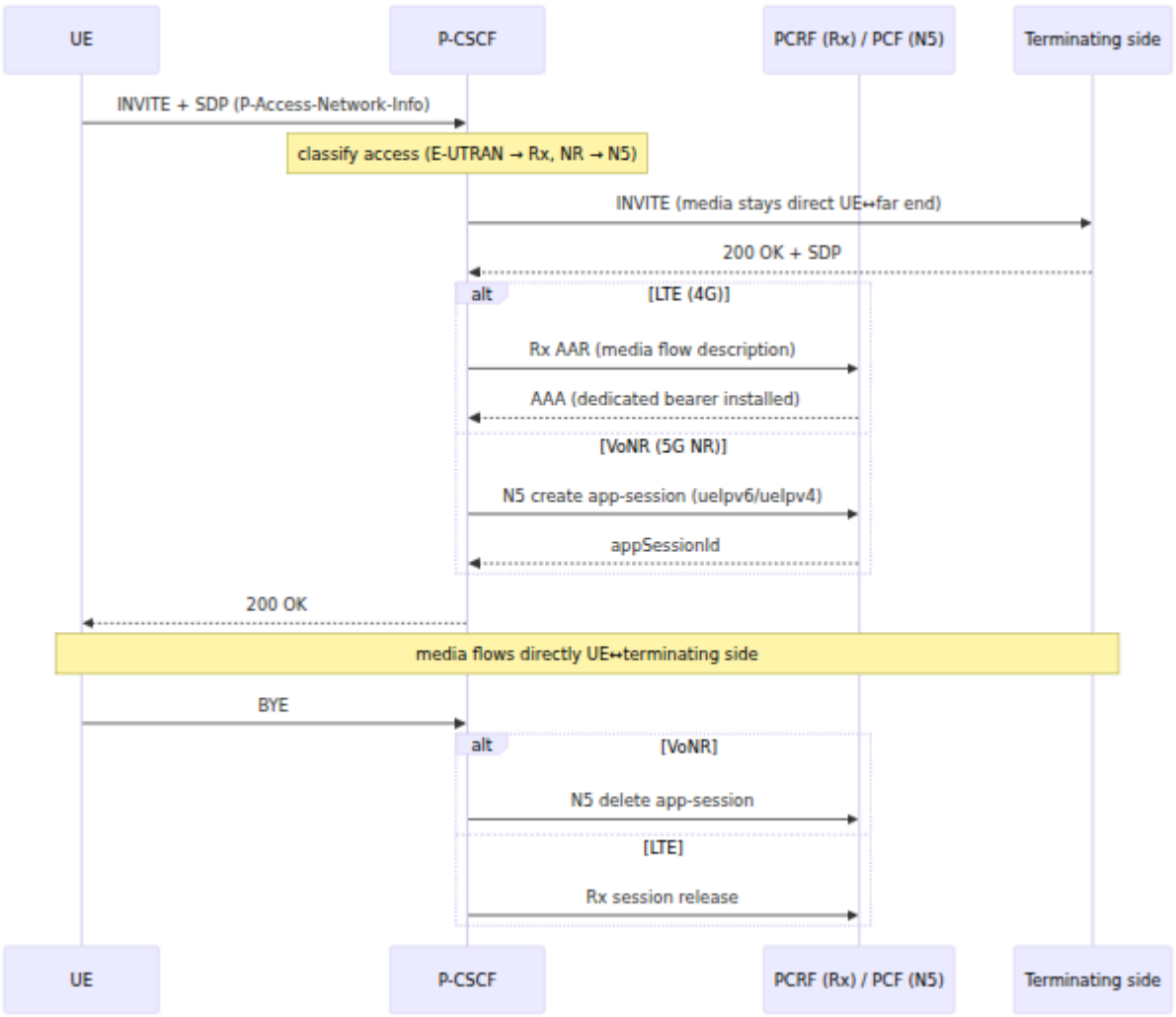
Deux mécanismes complémentaires résolvent l'identité :

1. **Liaison IMEI→MSISDN mise en cache (chemin rapide).** À chaque enregistrement réussi, le P-CSCF met en cache une liaison. La liaison

associe l'IMEI de l'UE (à partir du Contact `+sip.instance`) au MSISDN (à partir de `P-Associated-URI`). Le P-CSCF **réplique la liaison à travers tous les nœuds P-CSCF**. Tout nœud peut alors résoudre l'identité peu importe où l'UE s'est enregistré. Sur l'INVITE d'urgence, le P-CSCF extrait l'IMEI et cherche le MSISDN mis en cache.

2. **Requête d'abonnement asynchrone (appelants inconnus/anonymes).** Si aucune liaison mise en cache n'existe, le P-CSCF émet une requête d'abonnement Rx asynchrone au PCRF. La requête est basée sur l'adresse IP source de l'UE. Le P-CSCF suspend l'INVITE jusqu'à ce que la réponse revienne. Le PCRF retourne les identités au niveau EPC. Le P-CSCF en choisit une par priorité **MSISDN → IMSI → IMEISV**. Le P-CSCF met en cache un résultat IMEISV pour réutilisation.

Le P-CSCF affirme l'identité résolue comme l'URI From de l'appelant et comme un `P-Asserted-Identity` sur le domaine `sos.apn`. Le P-CSCF restaure l'identité de manière cohérente sur les réponses et dans les demandes en dialogue. Le PSAP voit alors une identité de rappel utilisable même pour un appelant à l'origine anonyme. Quel que soit le chemin qui résout l'identité, l'INVITE d'urgence reçoit le même traitement multimédia/QoS et en-tête que toute autre demande d'origine. Le P-CSCF le transmet alors au serveur d'application d'urgence.



Sécurité / anti-inondation

Le P-CSCF applique une protection contre les inondations basée sur la source. Le P-CSCF limite le taux de demandes par adresse IP source. Le P-CSCF interdit une IP qui dépasse le seuil d'échantillonnage pour une période de maintien. Le P-CSCF suit les échecs d'authentification d'enregistrement par adresse IP source dans un compteur à courte durée de vie. Le P-CSCF interdit une source qui dépasse le seuil de tentatives échouées dans la fenêtre. Cela empêche les devinettes de crédentiels. Le P-CSCF rejette les demandes qu'un UE adresse au nœud lui-même. Le P-CSCF rejette également les messages malformés. Sous pression mémoire, le nœud abandonne les nouvelles demandes avec `503`.

Réplication de cluster

Le P-CSCF réplique l'état lié à l'enregistrement et d'urgence à travers les nœuds P-CSCF. En particulier, le P-CSCF synchronise la liaison d'urgence

IMEI→MSISDN entre les nœuds. Le P-CSCF effectue une synchronisation complète au démarrage. Tout nœud du cluster peut alors servir le trafic de terminaison et résoudre l'identité d'appel d'urgence. Cela fonctionne indépendamment du nœud qui a initialement enregistré l'UE. Le P-CSCF n'a pas besoin de provisionnement par nœud.

Configuration de Déploiement (Injecté par Ansible)

Ansible génère la configuration d'exécution du P-CSCF et sa table de pairs Diameter (`pcscf.xml`) au moment du déploiement. La plupart des valeurs dérivent de l'identité PLMN du réseau (MCC/MNC) et du nom d'hôte de l'inventaire du nœud. Ansible émet les blocs 5G SBI et PCF uniquement lorsque l'inventaire de déploiement contient les fonctions réseau pertinentes.

Identité

Nom	Ce qu'il contrôle	Valeur / dér
`NETWORKNAME`	Domaine IMS domestique utilisé dans `P-Visited-Network-ID` et réécritures d'identité	`ims.mnc<mnc>.mcc<mcc>.3gppnetwo`
`HOSTNAME`	FQDN de ce nœud (également son alias d'hôte)	`<inventory_hostname>.ims.mnc<mn`
`URI`	Le propre URI SIP du P-CSCF	`sip:<hostname>:5060`
`PCSCF_URL`	URI source utilisée pour les pings OPTIONS de maintien de NAT	`sip:<hostname>:5060`
`PCSCF_USER_AGENT`	En-tête `User-Agent` émis	`User-Agent: Omnitouch Proxy-CSC`

Nom	Ce qu'il contrôle	Valeur / dér
	par le nœud	
`PCSCF_SERVER`	En-tête `Server` émis par le nœud	`Server: Omnitouch Proxy-CSCF <i`
`DMQ_NOTIFICATION_ADDR`	Adresse de notification de cluster pour la réplication d'état entre les nœuds P-CSCF	`sip:pcscf.ims.mnc<mnc>.mcc<mcc>`

Ansible modèle les sockets d'écoute SIP (UDP/TCP 5060, plus IPv6 5060 où une adresse IPv6 est définie) et le socket HTTP Prometheus (TCP 9090) à partir de l'adresse hôte de l'inventaire. Le P-CSCF fait face aux UEs sur IPv6 lorsque disponible. Les pairs derrière lui restent en IPv4. Ansible construit également le `PATH_HEADER` et le `P_VISITED_NETWORK_ID_HEADER` à partir du nom d'hôte et du PLMN.

Contrôle Rx / politique (4G)

Nom	Ce qu'il contrôle	Valeur / déri
`RX_DEST_REALM`	Domaine de destination Diameter pour Rx vers le PCRF	`{{ diameter_realm }}`
`PCRF_REALM`	Domaine PCRF	`epc.mnc<mnc>.mcc<mcc>`
`RX_AF_SIGNALING_IP`	IP de signalisation AF portée dans le Rx AAR (ce P-CSCF)	nœud `ansible_host` (re uniquement pour double
`RX_IMS_REG_DIALOG_DIRECTION`	Mode de direction de dialogue pour l'enregistrement Rx	`3`

Les paramètres multimédias Rx fixes incluent l'autorisation vidéo activée, une bande passante audio par défaut/minimum de 64 kbit/s, l'inclusion de flux RTCP, et une durée de session maximale autorisée de 24 heures.

5G SBI / PCF (VoNR)

Émis lorsque l'inventaire de déploiement contient un PCF et un NRF.

Nom	Ce qu'il contrôle	Valeur / dérivati
`VONR_AF_NOTIF_URI`	Point de terminaison de notification AF sur lequel le PCF rappelle	`http://<this host>:<pcscf_af_notif_port|`
`NRF_URI`	URI de base NRF pour l'enregistrement et la découverte AF	`http://<nrf host>:<nrf_sbi_port|7777>`
`IMS_NRF_NF_IPV4`	NF IPv4 de ce P-CSCF pour son enregistrement AF	nœud `ansible_host`
`IMS_NRF_PLMN_MCC` / `IMS_NRF_PLMN_MNC`	PLMN annoncé dans l'enregistrement/découverte NRF	à partir de `plmn_id`

Découverte PCF : le P-CSCF s'enregistre auprès du NRF en tant qu'AF. Pour chaque session VoNR, le P-CSCF résout le PCF lié à cette session PDU de l'UE via la chaîne NRF→BSF. Les sessions d'application atteignent alors toujours le PCF correct par abonné. Cela inclut les cœurs 5G multi-PCF. C'est le seul chemin de découverte pris en charge.

Dimensionnement / transport

Nom	Ce qu'il contrôle	Valeur
`CAPTURE_NODE`	Cible de capture SIP Homer (modélisé uniquement lorsque la capture Homer est activée)	`sip:<homer host>:9060`

La configuration de base ajuste le nombre de processus de travail SIP (UDP) et la taille de la table de hachage de l'enregistreur pour l'échelle de déploiement. Les UEs iOS obtiennent une durée de vie de connexion TCP raccourcie pour correspondre à leur comportement de transport.

Configuration des pairs Diameter

La table des pairs Diameter du P-CSCF (`pcscf.xml`) annonce l'application **Rx** (`16777236`) vers le PCRF. Tous les CSCFs partagent la structure de fichier et les variables Ansible qui la remplissent. Voir Diameter → Configuration des pairs (Déploiement). Rx n'est actif que lorsque `WITH_RX` est défini.

Dépannage

Enregistrement / connectivité IPsec

Les utilisateurs qui ne peuvent pas s'enregistrer, ou qui rencontrent des délais d'enregistrement, pointent souvent vers la sécurité d'accès P-CSCF ou la couche de découverte plutôt que vers le réseau domestique :

- **Établissement de la SA IPsec** - les appareils mobiles doivent compl►►ter la négociation `Security-Client` / `Security-Server` IMS-AKA. Si le re-REGISTER authentifié n'arrive jamais à l'intérieur de la SA, vérifiez deux choses. Confirmez que l'UE et le P-CSCF se sont mis d'accord sur les paramètres SA. Confirmez qu'aucun dispositif intermédiaire ne supprime les en-têtes de sécurité.
- **Traversée NAT** - pour les appareils derrière un NAT, vérifiez le traitement NAT de l'autre extrémité. Vérifiez que les pings OPTIONS de maintien atteignent l'UE. Le trou pour le trafic de terminaison reste alors ouvert.
- **Découverte P-CSCF** - vérifiez que l'UE découvre la bonne adresse P-CSCF (via DNS, DHCP ou configuration statique). Vérifiez que les sockets d'écoute SIP sont accessibles sur le réseau d'accès.

Problèmes d'appel d'urgence

Symptômes : Les appels d'urgence ne sont pas routés vers le PSAP, ou le PSAP ne reçoit aucune identité de ligne d'appel (CLI) / numéro de rappel utilisable.

- **Détection d'urgence** - le P-CSCF route sur l'URN de service d'urgence (`urn:service:sos`), plus les numéros d'urgence composés. Confirmez que

l'INVITE porte l'indication d'urgence attendue. Confirmez que le routage d'urgence contourne la vérification d'enregistrement normale.

- **Résolution CLI pour les appelants anonymes / inconnus** - le P-CSCF fournit l'identité de l'appelant à partir de la liaison IMEI→MSISDN mise en cache (répliquée en cluster, TTL de 4 heures). Pour un appelant sans liaison mise en cache, le P-CSCF revient à une requête d'abonnement Rx asynchrone au PCRF. La requête est basée sur l'adresse IP source de l'UE. Le P-CSCF résout une identité EPC par priorité **MSISDN → IMSI → IMEISV** (annexe K de la TS 23.167). Si le PSAP voit un appelant anonyme, vérifiez l'une des deux choses. Vérifiez que le P-CSCF a mis en cache la liaison à l'enregistrement. Sinon, vérifiez que la requête d'abonnement Rx a retourné une identité. OmniWeb affiche la carte de liaison mise en cache.
- **Disponibilité de localisation** - vérifiez que les informations de localisation sont disponibles pour E911/E112. Vérifiez que la branche de récupération de localisation (LRF) est accessible.
- **Test de routage** - vous pouvez exercer le routage des appels d'urgence sans connexion réelle au PSAP. Cela confirme la détection, l'affirmation d'identité sur le domaine `sos.apn`, et le routage vers le serveur d'application d'urgence.

Les sessions d'urgence réussissent même pour les utilisateurs non enregistrés, les utilisateurs sans SIM ou avec des identifiants invalides, et les utilisateurs en itinérance. Voir Appels d'urgence (E-CSCF) & identité de ligne d'appel - TS 23.167 pour le mécanisme sous-jacent.

Flux d'Appels

Les diagrammes de séquence apparaissent avec les fonctions qu'ils documentent. Les échelles de session complètes apparaissent ci-dessous :

- Enregistrement & SA IPsec → Proxy d'enregistrement & association de sécurité IPsec
- QoS multimédia / politique (MO & MT) → Détection d'accès & contrôle de QoS / politique
- Session d'urgence → Appels d'urgence (E-CSCF) & identité de ligne d'appel - TS 23.167

Appel d'origine mobile (MO)

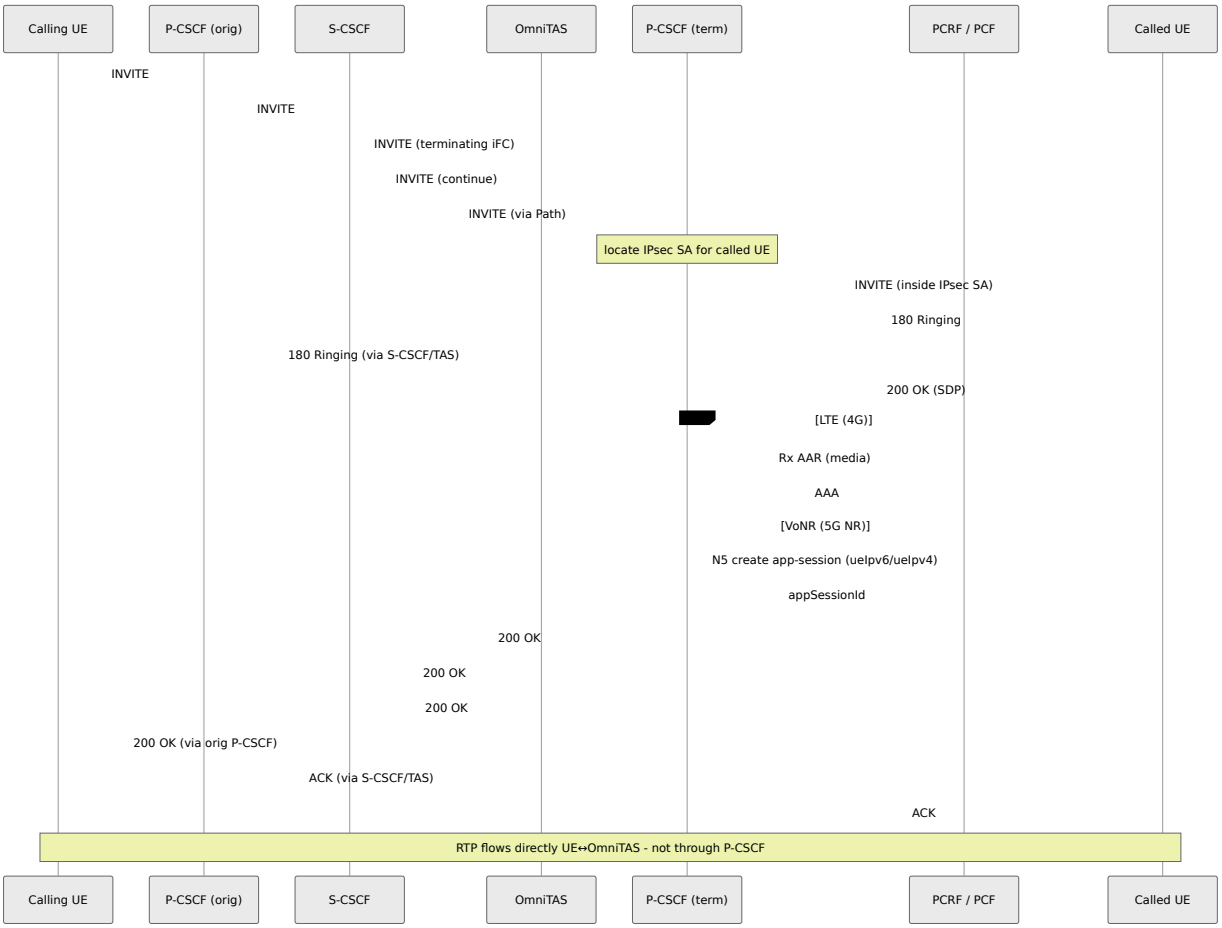
Le P-CSCF route les appels d'origine à travers le S-CSCF (via le Service-Route mis en cache) vers le TAS pour la logique de service et la facturation. Les médias restent directs.

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'

Réessayer

Appel de terminaison mobile (MT)

Les appels de terminaison arrivent à nouveau via le P-CSCF enregistré dans le Path lors de l'enregistrement. Le P-CSCF autorise le QoS lorsque l'UE appelé répond.



Documentation Connexe

- Opérations
- Diameter
- Interface Basée sur le Service (SBI)
- Référence des Métriques
- OmniWeb - contacts enregistrés, tables de hachage (y compris la carte d'urgence IMEI→MSISDN), découverte NRF/PCF, et état des pairs Rx : <https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>

Guide des opérations SBI 5G

Table des matières

1. Aperçu
2. SBI dans l'architecture IMS
3. N5 - Npcf_PolicyAuthorization (P-CSCF → PCF)
4. Nnrf - Gestion et découverte des NF (P-CSCF ↔ NRF)
5. Quand SBI est utilisé vs Diameter
6. Configuration
7. Gestion via OmniWeb
8. Problèmes courants
9. Documentation connexe

Aperçu

Le cœur 5G est **basé sur les services**. Les fonctions réseau exposent des API REST JSON et HTTP/2 les unes aux autres via l'Interface Basée sur les Services (SBI). Le SBI remplace Diameter. Pour VoNR (Voix sur Nouvelle Radio), le P-CSCF agit en tant que **Fonction d'Application (AF)** 5G. Le P-CSCF utilise le SBI pour autoriser la QoS des médias. Le P-CSCF utilise également le SBI pour découvrir les fonctions réseau dont il a besoin.

Le SBI remplace le chemin Diameter Rx utilisé pour VoLTE. Voir Opérations Diameter pour le côté 4G/LTE.

Qu'est-ce que le SBI ?

L'Interface Basée sur les Services (3GPP TS 29.500) diffère de Diameter de ces manières :

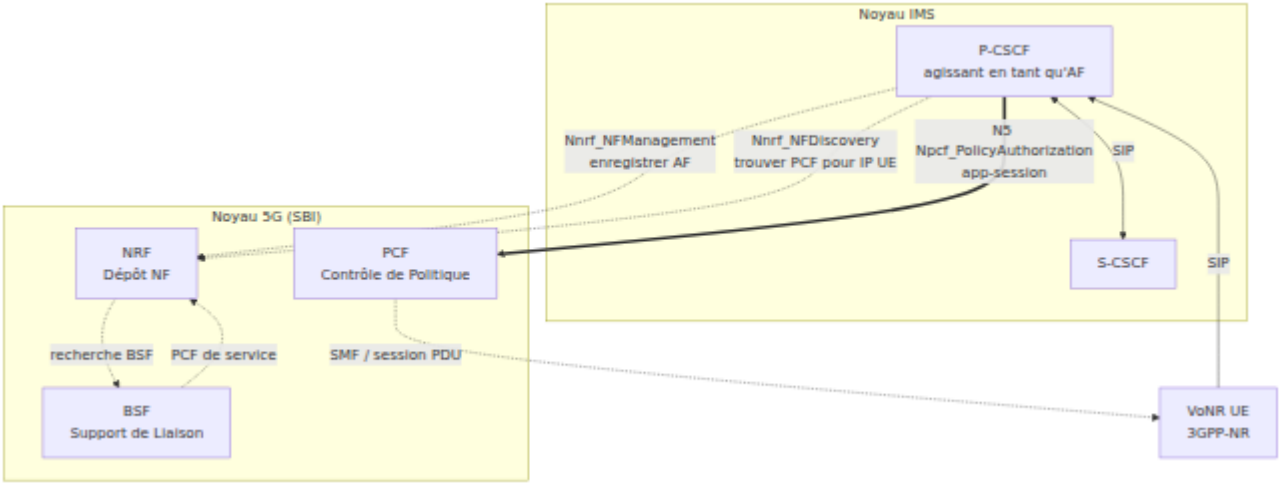
- **Transport** : HTTP/2 sur TCP. Diameter utilise TCP ou SCTP.
- **Encodage** : charges utiles JSON décrites par OpenAPI. Diameter utilise des AVP.
- **Modèle** : ressources RESTful. Vous créez, modifiez ou supprimez une ressource *app-session*. Diameter utilise des paires de commandes de demande et de réponse.
- **Découverte** : le **NRF** trouve les producteurs dynamiquement. Diameter utilise des pairs configurés statiquement.
- **Nommage** : les services utilisent le nom `Nxxx` (par exemple `Npcf_PolicyAuthorization`, `Nnrf_NFDiscovery`)

SBI dans le CSCF

Le P-CSCF est le seul composant CSCF qui utilise le SBI. En tant que Fonction d'Application (AF) 5G, le P-CSCF autorise la QoS des médias VoNR via N5 vers le PCF. Lorsque la découverte NRF est activée, le P-CSCF s'enregistre auprès du NRF et interroge le NRF.

Rôle	Service	Transport	Connecté à	But
AF	Npcf_PolicyAuthorization (N5)	HTTP/2	PCF	Autoriser les médias VoNR et la QoS. Créer une app-session.
NF (AF)	Nnrf_NFManagement	HTTP/2	NRF	Enregistrer le P-CSCF en tant qu'instance AF (optionnel)
NF (AF)	Nnrf_NFDiscovery	HTTP/2	NRF → BSF	Découvrir le PCF lié à une session PDU UE (optionnel)

SBI dans l'architecture IMS



Pour VoNR, le P-CSCF détecte l'accès 5G. Le P-CSCF découvre le PCF de service via la chaîne NRF→BSF. Le P-CSCF envoie ensuite une app-session d'autorisation de politique à ce PCF. Cette app-session réserve la QoS du porteur vocal.

N5 - Npcf_PolicyAuthorization (P-CSCF → PCF)

Le point de référence **N5** transporte le service `Npcf_PolicyAuthorization`. Lors d'un appel VoNR, le P-CSCF crée une ressource *app-session* sur le PCF. L'app-session décrit les médias dont la session a besoin. Le PCF installe ensuite la QoS correcte sur la session PDU 5G de l'UE.

Demande d'app-session

Le P-CSCF envoie un objet `ascReqData` à la collection d'app-sessions du PCF. La collection par défaut est `http://<pcf>/npcf-policyauthorization/v1/app-sessions`. L'objet contient ces champs :

Champ	Valeur	Remarques
`notifUri`	URI de notification AF	L'adresse où le PCF envoie les notifications d'événements d'app-session. C'est le point de terminaison de notification AF configuré.
`suppFeat`	`3f`	Bitmap des fonctionnalités prises en charge
`ueIpv4` / `ueIpv6`	IP source de l'UE	**Doit correspondre à la famille d'adresses** que le PCF a liée à la session PDU SMF
`afAppId`	`VoNR`	Identifiant d'application
`medComponents`	composant média audio	`mediaType: AUDIO`, `fStatus: ENABLED`, avec une description de flux (`permit out 17 from <ue-ip> to any`)

> **Problème opérationnel - famille d'adresses.** Le PCF lie l'app-session à la session PDU SMF par l'adresse IP de l'UE. Vous devez encoder un UE sur une session PDU IPv6 en tant que `ueIpv6`. Une adresse v6 dans `ueIpv4` ne correspond jamais. Une adresse v4 dans `ueIpv6` ne correspond jamais. Dans ces cas, le PCF rejette l'autorisation ou abandonne l'autorisation silencieusement. Le P-CSCF sélectionne `ueIpv6` ou `ueIpv4` à partir de l'adresse source SIP automatiquement.

Cycle de vie

- **Créer** - le P-CSCF envoie l'app-session lorsqu'il traite l'INVITE VoNR ou les médias précoces.
- **Notifier** - le PCF rappelle à `notifUri` pour les événements de session.
- **Supprimer** - le P-CSCF détruit l'app-session lorsque le dialogue se termine. Cela libère la QoS réservée.

Diameter Rx utilise `Rx_AAR` et `Rx_STR`. N5 n'a pas de connexion de pair persistante. Chaque app-session est une transaction HTTP/2 indépendante vers le PCF découvert pour cet UE.

Nnrf - Gestion et découverte des NF (P-CSCF ↔ NRF)

Le P-CSCF utilise la découverte NRF pour trouver le PCF pour chaque session VoNR. La découverte NRF est le seul chemin de découverte du PCF.

Enregistrement NF (Nnrf_NFManagement)

Le P-CSCF s'enregistre en tant qu'instance AF auprès du NRF. Le P-CSCF utilise une identité d'instance stable par hôte. Un redémarrage réutilise un enregistrement. Cela empêche le NRF d'accumuler des enregistrements AF obsolètes.

Découverte du PCF (Nnrf_NFDiscovery)

Pour une session VoNR, le P-CSCF interroge le NRF avec l'IP source de l'UE. Cette requête découvre le PCF qui sert cette session PDU UE. La chaîne **NRF → BSF** résout la requête. Le BSF détient la liaison UE-IP vers le PCF de service. Le point de terminaison découvert devient la cible N5. Si le P-CSCF ne trouve aucune liaison, il saute la QoS dynamique pour cet appel. La session se poursuit alors sans réservation de porteur dédiée.

Quand SBI est utilisé vs Diameter

Le P-CSCF dérive le type d'accès à partir de l'en-tête `P-Access-Network-Info` (selon TS 24.229 §5.2.6.3). LTE rapporte `3GPP-E-UTRAN`. 5G NR rapporte `3GPP-NR`. Le P-CSCF exclut le WiFi (`3GPP-IEEE-802.11`) car le WiFi n'a pas de porteurs dédiés.

Accès	`P-Access-Network-Info`	Chemin QoS	Pair
5G NR (VoNR)	`3GPP-NR`	**N5 SBI** (`Npcf_PolicyAuthorization`)	PCF
LTE (VoLTE)	`3GPP-E-UTRAN`	**Diameter Rx**	PCRF
WiFi	`3GPP-IEEE-802.11`	aucun (pas de porteur dédié)	-

Le P-CSCF découvre le PCF pour le chemin N5 par session. Il utilise la chaîne NRF → BSF → PCF de service.

Configuration

L'outil de déploiement provisionne le comportement du SBI par déploiement. Ne modifiez pas le comportement du SBI manuellement. Les paramètres pertinents sont :

Paramètre	But
Point de terminaison de notification AF	L'URL de rappel que le P-CSCF annonce au PCF pour les notifications d'événements d'app-session
Point de terminaison NRF	L'adresse NRF pour l'enregistrement AF et la découverte du PCF
Identité du PLMN domicile (MCC / MNC)	L'identité du réseau domestique que le P-CSCF présente au NRF
Identité d'instance AF	Une identité stable par hôte pour l'enregistrement NRF. Un redémarrage réutilise un seul enregistrement.

OmniWeb montre l'état d'enregistrement NRF en direct. OmniWeb montre également les liaisons PCF découvertes par session. Voir ci-dessous.

Gestion via OmniWeb

Omnitouch a supprimé le panneau de contrôle web intégré. L'onglet **NRF** de la page P-CSCF d'OmniWeb montre l'état d'enregistrement NRF, les liaisons PCF découvertes et l'état 5G/N5. Voir la documentation OmniWeb.

Problèmes courants

Symptôme	Cause probable	Action
Aucune liaison PCF trouvée pour l'UE (journalisée lors de la configuration de l'appel)	Le NRF ou le BSF n'a pas encore de liaison pour la session PDU UE. Ou l'IP de l'UE diffère de l'ancre de session.	Confirmer que la session PDU de l'UE est établie. Confirmer que le BSF détient la liaison. L'appel se poursuit sans QoS dynamique.
Le PCF rejette ou ignore l'app-session	L'IP de l'UE est encodée dans la mauvaise famille (`ueIpv4` vs `ueIpv6`)	Vérifier que la famille d'adresses de l'adresse source SIP correspond à la session PDU. Voir le problème de famille d'adresses ci-dessus.
Des enregistrements AF obsolètes s'accumulent sur le NRF	L'identité d'instance AF n'est pas stable entre les redémarrages	Rendre l'identité d'instance AF par hôte stable
Aucun trafic N5 du tout pour un appel 5G	Le P-CSCF ne détecte pas l'accès comme `3GPP-NR`. Ou le NRF est injoignable, donc le P-CSCF ne découvre aucun PCF.	Vérifier `P-Access-Network-Info`. Vérifier que le point de terminaison NRF est joignable.
L'appel VoNR se met en place mais pas de porteur dédié	Le P-CSCF n'a pas créé l'app-session car la découverte a échoué. Ou le P-CSCF a détruit l'app-session trop tôt.	Corréler le POST N5 du P-CSCF avec le PCF. Vérifier la connectivité HTTP/2 et les délais d'attente.

Documentation connexe

- Opérations Diameter - les interfaces Diameter Rx, Cx et Ro utilisées pour VoLTE (4G/LTE)
- Opérations P-CSCF - Détection d'accès VoNR, QoS N5 et découverte NRF dans le contexte
- Référence des métriques - métriques P-CSCF
- Documentation OmniWeb - état NRF et 5G dans le portail de gestion

Opérations et Référence S-CSCF

Le Serving-CSCF est le registraire SIP du réseau domestique et le point de contrôle de session de l'IMS. Il authentifie les abonnés auprès du HSS via Cx (MAR/SAR). Il stocke le lien d'enregistrement. Il télécharge le profil de service de l'abonné (Critères de Filtrage Initiaux). Il se trouve dans le chemin de signalisation pour chaque session d'origine et de terminaison. De cette position, il déclenche des serveurs d'applications via l'interface ISC, affirme l'identité de l'appelant et achemine la session vers le côté de terminaison, un serveur d'application ou le PSTN. Le HSS enregistre le nom de ce S-CSCF pour l'abonné. Par conséquent, tout le trafic ultérieur pour cet utilisateur passe par ce nœud.

Fonctions IMS

Enregistrement et authentification

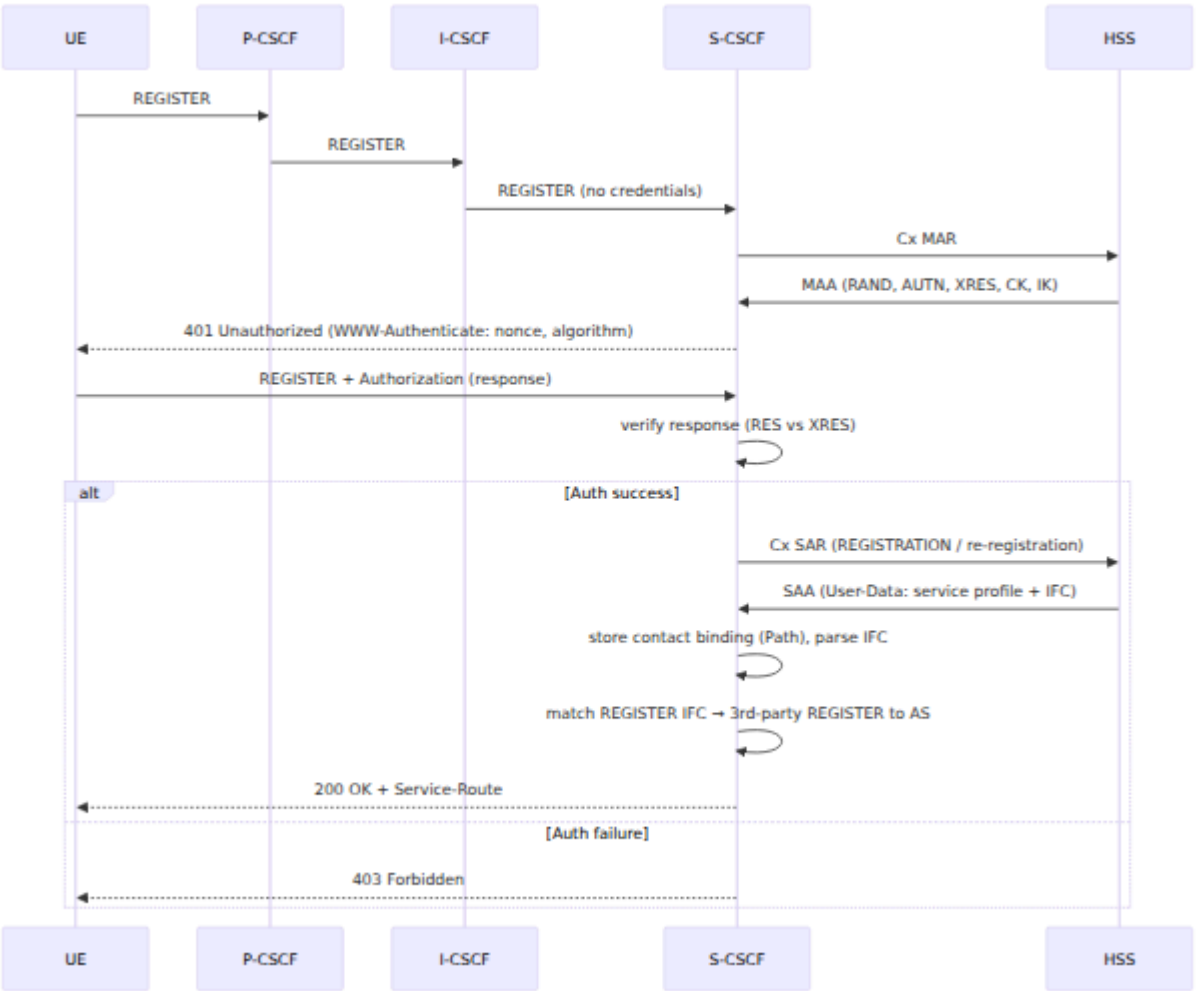
Le S-CSCF est le registraire autoritaire. Il défie l'UE. Il valide la réponse contre un vecteur d'authentification Cx du HSS. En cas de succès, il enregistre le lien de contact et télécharge le profil de service de l'abonné.

L'enregistrement se déroule comme suit :

1. **Sélection de l'algorithme.** Le S-CSCF défie avec l'algorithme que l'UE propose dans son en-tête Authorization. Si l'UE ne propose aucun algorithme, le S-CSCF utilise par défaut SIP Digest (MD5). SIP Digest s'adapte aux softphones non-IMS. Par défaut, le S-CSCF authentifie chaque REGISTER.
2. **Défi (MAR).** Le S-CSCF reçoit un REGISTER sans identifiants. Il demande un vecteur d'authentification au HSS avec une Cx Multimedia-Auth-Request. Le HSS renvoie le vecteur dans la réponse (pour AKA : RAND, AUTN, XRES, CK, IK). Le S-CSCF répond **401 Unauthorized** avec un en-tête `WWW-Authenticate`. Cet en-tête contient le nonce (dérivé de RAND) et

l'algorithme sélectionné. Si le HSS rejette l'identité, l'enregistrement échoue **403**. Si le HSS est indisponible ou renvoie une réponse mal formée, l'enregistrement échoue **503**.

3. **Vérification.** L'UE renvoie le REGISTER avec sa réponse calculée. Le S-CSCF vérifie la réponse par rapport au vecteur stocké. Il correspond à l'identité publique.
4. **Re-synchronisation.** Si l'UE signale un décalage de numéro de séquence (SQN), le S-CSCF transmet le jeton AUTS au HSS pour se resynchroniser. Ensuite, le S-CSCF relance avec de nouveaux vecteurs.
5. **Attribution de serveur (SAR).** Après une authentification réussie, le S-CSCF envoie une Cx Server-Assignment-Request. Le type d'attribution est REGISTRATION lors du premier enregistrement, ou re-registration lors d'un rafraîchissement. La réponse renvoie les User-Data de l'abonné (profil de service et IFC). Le S-CSCF conserve les User-Data en mémoire. Une attribution rejetée, ou un abonné sans profil de service IMS, échoue **403**. Un délai d'attente du HSS échoue **503**.
6. **Liaison et Service-Route.** Le S-CSCF stocke le lien de contact avec le chemin P-CSCF. Le chemin permet aux demandes de terminaison de revenir par le même P-CSCF. Le 200 OK contient un Service-Route, de sorte que l'UE envoie les demandes suivantes via ce S-CSCF. Le S-CSCF conserve un contact par identité publique. Une nouvelle liaison remplace la précédente. L'expiration est fixée à 599 secondes.
7. **Enregistrement tiers / reg-event.** Le S-CSCF évalue également l'enregistrement par rapport aux Critères de Filtrage Initiaux déclenchés par le REGISTER. Cette évaluation déclenche des REGISTER tiers vers tous les serveurs d'applications correspondants. Le paquet d'événements d'enregistrement notifie les entités abonnées de l'état de l'enregistrement. Le S-CSCF met fin à l'abonnement lors de la désinscription.



Déclenchement de service via IFC (ISC)

Le S-CSCF évalue chaque demande initiale par rapport aux **Critères de Filtrage Initiaux** téléchargés de l'abonné. Chaque IFC a un Point de Déclenchement priorisé, une adresse de Serveur d'Application et une valeur de Gestion par Défaut. Le Point de Déclenchement est une combinaison booléenne de Déclencheurs de Point de Service (méthode, Request-URI, en-tête SIP, Cas de Session, SDP). La valeur de Gestion par Défaut est session-continue, ou session-terminée en cas d'échec de l'AS. Le Point de Déclenchement utilise une forme normale conjonctive ou disjonctive. Vous pouvez regrouper et nier les déclencheurs individuels.

Le S-CSCF parcourt le profil par ordre de priorité pour le cas de session pertinent. En cas de correspondance, il transmet la demande au Serveur d'Application via ISC. Le S-CSCF marque la demande avec un **Identifiant de Dialogue Original (ODI)**. Il insère également un en-tête **P-Served-User** (RFC 5502) qui identifie l'abonné servi et le cas de session. Ces marques permettent

à l'AS de renvoyer la demande au point de la chaîne où elle a été laissée. Lorsque l'AS achemine la demande de retour, le S-CSCF reconnaît l'ODI. Ensuite, il reprend l'évaluation de l'IFC après le dernier critère correspondant au lieu de redémarrer.

La Gestion par Défaut régit le comportement en cas d'échec de l'AS. Le Serveur d'Application renvoie un 408 ou un 5xx. Le S-CSCF continue alors vers le critère suivant (session-continue) ou abandonne la branche, comme spécifié par l'IFC.

Gestion des appels d'origine

Une demande est **d'origine** lorsqu'elle arrive avec l'indicateur d'origine dans son en-tête Route supérieur, ou lorsqu'elle revient d'un Serveur d'Application d'origine. Le S-CSCF alors :

- Attribue le contexte de dialogue d'origine et enregistre les routes, afin de reconnaître les demandes en dialogue comme la branche d'origine.
- **Affirme l'identité.** La demande ne revient pas d'un AS. Le S-CSCF supprime tout `P-Asserted-Identity` fourni par le client. Il remplace l'identité par l'identité qu'il a authentifiée lors de l'enregistrement. C'est l'identité de ligne d'appel authentifiée pour la branche.
- Évalue l'IFC d'origine et transmet les correspondances au Serveur d'Application via ISC.
- **Normalisation des numéros.** Un Request-URI porte un `phone-context`. Le S-CSCF réécrit le Request-URI en un URI `tel:` dans le contexte téléphonique du réseau domestique avant l'acheminement.
- **PSTN / ENUM.** Pour les destinations E.164, le S-CSCF résout le numéro par ENUM. En cas d'échec de l'ENUM, le S-CSCF envoie l'appel aux passerelles de sortie PSTN, avec un basculement à travers l'ensemble des passerelles. Si la demande porte une indication de Transit-and-Roaming Function en itinérance (`Feature-Caps: +g.3gpp.trf`), le S-CSCF l'achemine vers ce TRF à la place.
- **Vecteur de facturation.** Les appels d'origine portent un `P-Charging-Vector` pour la corrélation de facturation inter-opérateurs.
- Si la facturation en ligne est activée, le S-CSCF envoie une demande de contrôle de crédit avant que l'appel ne se poursuive (voir Facturation).

Le S-CSCF relaye les destinations non-PSTN vers le côté de terminaison. Si ce même S-CSCF sert l'utilisateur de terminaison, la gestion de terminaison se poursuit localement.

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

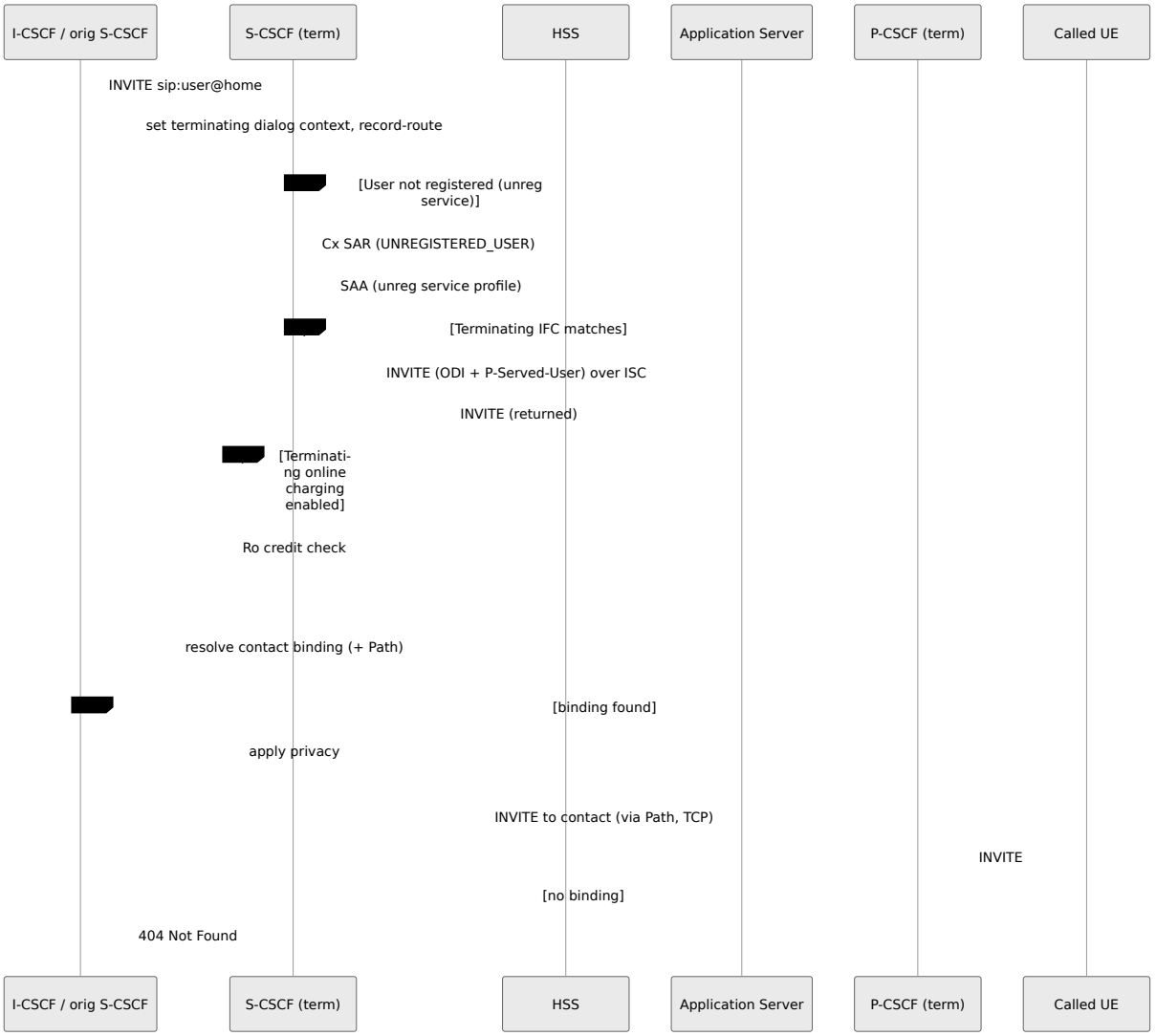
Réessayer

Gestion des appels de terminaison

Une demande est **de terminaison** lorsque son Request-URI est une identité servie localement. Le S-CSCF alors :

1. Attribue le contexte de dialogue de terminaison et enregistre les routes, afin de reconnaître les demandes en dialogue comme la branche de terminaison.
2. Restaure le Request-URI original. Pour les méthodes non-INVITE, il évalue l'IFC de terminaison et transmet les correspondances au Serveur d'Application via ISC. Pour les INVITE, le transfert de l'IFC suit le cycle de retour de l'AS.
3. Si la facturation en ligne de terminaison est activée, le S-CSCF envoie une demande de contrôle de crédit du côté de terminaison avant de procéder.
4. **Résolution de localisation.** Le S-CSCF récupère le lien de contact de l'utilisateur servi. Il relaye la demande à ce contact via le P-CSCF enregistré dans le chemin lors de l'enregistrement. Si l'utilisateur n'a pas de liaison, le S-CSCF renvoie un **404 Not Found**.
5. Le S-CSCF reçoit un INVITE pour une identité qui **n'est pas actuellement enregistrée**. D'abord, il récupère le profil de service non enregistré du HSS avec une Cx Server-Assignment-Request de type UNREGISTERED_USER. Cela permet aux services non enregistrés de terminaison de fonctionner (par exemple, la messagerie vocale). Un délai d'attente du HSS échoue **503**. Un profil manquant échoue **403**.

Le S-CSCF applique la confidentialité à la sortie. Si la demande affirme `Privacy: id`, le S-CSCF supprime le `P-Asserted-Identity` avant que le message ne quitte le S-CSCF.



Facturation (optionnelle)

La facturation en ligne via Diameter **Ro** vers un OCS est optionnelle. Vous l'activez par déploiement (voir les indicateurs de facturation ci-dessous). Lorsqu'elle est activée, le S-CSCF envoie une demande de contrôle de crédit avant de permettre un INVITE. Le S-CSCF associe la réponse aux réponses SIP (par exemple, fonds insuffisants → 402, limite de crédit atteinte → 486, abonné de facturation inconnu → 403). Le Service-Context-Id identifie le service facturé. Le S-CSCF assemble cet identifiant à partir des paramètres de facturation énumérés dans la référence de configuration.

En production, cela est normalement **désactivé**. Le TAS effectue la facturation à la place. Le TAS prend correctement en compte les services supplémentaires (transfert, transfert, branches en itinérance) que le S-CSCF ne peut pas observer de bout en bout. Traitez la facturation Ro du S-CSCF comme une capacité optionnelle, et non comme un défaut.

Présence / reg-event

Le S-CSCF ne fonctionne pas comme un serveur de présence général. Le S-CSCF accepte les demandes `SUBSCRIBE` d'événements d'enregistrement (`Event: reg`) (200 OK). Le S-CSCF ne sert pas les abonnements de présence générale. Le S-CSCF accepte un `PUBLISH` d'événements d'enregistrement uniquement d'un utilisateur enregistré. Un tel PUBLISH met à jour l'état d'enregistrement publié. Sinon, le S-CSCF le rejette **403**. Cette configuration n'a pas de gestion de présence de disponibilité utilisateur (PIDF).

Configuration de Déploiement (Injecté par Ansible)

Ansible rend la configuration d'exécution du S-CSCF et sa table de pairs Diameter (`scscf.xml`) au moment du déploiement. Les valeurs ci-dessous dérivent de l'identité PLMN du réseau (MCC/MNC) et du nom d'hôte de l'inventaire du nœud.

Identité / domaine

Nom	Ce qu'il contrôle	Valeur / dér
`NETWORKNAME`	Domaine IMS domestique. C'est le domaine de destination Cx et le `phone-context` utilisé dans la normalisation des numéros	`ims.mnc<mnc>.mcc<mcc>.3gppnetwo`
`HOSTNAME`	Le FQDN de ce nœud (alias d'hôte, et origin-host Diameter lorsque Ro est activé)	`<inventory_hostname>.ims.mnc<mn`
`URI`	Le propre URI SIP du S-CSCF. C'est l'identité de registraire et d'authentification	`sip:<hostname>:5060`
`SCSCF_USER_AGENT`	L'en-tête `User-Agent` que le nœud émet	`User-Agent: Omnitouch S-CSCF <i`
`ISC_MY_URI`	Jeton d'hôte qui identifie les propres routes ODI de ce S-CSCF lorsque	`<inventory_hostname>`

Nom	Ce qu'il contrôle	Valeur / dér
	l'AS renvoie une demande	
`ENUM_SUFFIX`	Suffixe de domaine ENUM pour la résolution E.164→URI des numéros liés au PSTN d'origine	`mnc<mnc>.mcc<mcc>.3gppnetwork.o`

Ansible modèle les sockets d'écoute SIP (UDP/TCP 5060, TLS 9090) et les alias d'hôte à partir de l'adresse de l'hôte de l'inventaire et du PLMN.

Authentification - `REG_AUTH_DEFAULT_ALG`

L'algorithme d'authentification par défaut que le S-CSCF applique lorsqu'il doit en choisir un, plutôt que de renvoyer l'algorithme demandé par l'UE. Options :

Valeur	Signification / quand l'utiliser
`AKAv1-MD5`	3GPP IMS-AKA (TS 33.203). Standard pour USIM/ISIM VoLTE/VoNR avec SAs IPsec. Utiliser pour les abonnés mobiles normaux.
`AKAv2-MD5`	Variante améliorée de l'IMS-AKA. Utiliser uniquement lorsque les UE et le HSS négocient spécifiquement AKAv2.
`MD5`	SIP HTTP Digest simple (pas d'AKA, pas d'IPsec). Utiliser pour les clients non-IMS / softphone qui ne peuvent pas faire d'AKA.
`CableLabs-Digest`	Profil de digest PacketCable/CableLabs. Déploiements de réseaux câblés.
`3GPP-Digest`	3GPP SIP Digest (TS 33.203 Annexe N). Basé sur mot de passe, pas d'ISIM. Abonnés fixes / non-UICC.
`TISPAN-HTTP_DIGEST_MD5`	Profil ETSI TISPAN NASS/HTTP-Digest. Abonnés fixes à large bande TISPAN.
`HSS-Selected`	**Par défaut.** Le S-CSCF n'impose aucun algorithme. Le HSS renvoie le schéma par abonné dans la réponse d'authentification. Utilisez ceci pour que le S-CSCF défie chaque abonné avec ce que le HSS a provisionné (AKA pour mobiles, Digest pour fixes, etc.).

L'algorithme ne change pas les défauts suivants. Le S-CSCF authentifie chaque REGISTER par défaut (voir `WITH_AUTH`). Le domaine de destination Cx est le domaine du réseau domestique (`NETWORKNAME`). Le S-CSCF correspond aux vecteurs d'authentification sur l'identité publique. Les vecteurs expirent après 599 s.

Facturation (Ro) - indicateurs et pairs

Nom	Ce qu'il contrôle	Valeurs
`WITH_RO`	Activer le contrôle de crédit Diameter Ro d'origine avant un INVITE sortant	define / undef (par défaut : undef)
`WITH_RO_TERM`	Activer le contrôle de crédit Diameter Ro du côté de terminaison	define / undef (par défaut : undef)
`RO_DESTINATION`	Hôte de destination Diameter OCS (le domaine de destination est le domaine du réseau domestique)	FQDN OCS, par exemple `hssocs.voiceblue.com`
`RO_FORCED_PEER`	Fixer le routage de contrôle de crédit à un pair Diameter spécifique. Cela contourne le routage de domaine	id de pair (par exemple `32260@3gpp.org`); désactivé par défaut
`RO_ROOT`	Racine de Service-Context-Id	`32260@3gpp.org`
`RO_EXT`	Extension de Service-Context-Id	`ext`
`RO_MNC`	Composant MNC de Service-Context-Id	par exemple `07`
`RO_MCC`	Composant MCC de Service-Context-Id	par exemple `262`

Nom	Ce qu'il contrôle	Valeurs
`RO_RELEASE`	version 3GPP pour Service-Context-Id	par exemple `8`

Indicateurs de fonctionnalités (`WITH_*`)

Indicateur	Effet lorsqu'il est défini
`WITH_AUTH`	Authentifier chaque REGISTER (pas seulement les clients Digest/MD5). Activé par défaut dans le modèle.
`WITH_RO`	Activer la facturation en ligne d'origine via Diameter Ro.
`WITH_RO_TERM`	Activer la facturation en ligne de terminaison via Diameter Ro.

Ansible modèle `CAPTURE_NODE` (la cible de capture Homer) uniquement lorsque la capture Homer est activée pour le déploiement. `CAPTURE_NODE` duplique le signalement SIP vers Homer pour le traçage.

Configuration des pairs Diameter

La table des pairs Diameter du S-CSCF (`scscf.xml`) annonce l'application **Cx** (`16777216`) vers le HSS ainsi que la comptabilité de base. La structure du fichier et les variables Ansible qui la remplissent sont partagées entre tous les CSCFs. Voir Diameter → Configuration des Pairs (Déploiement). Lorsque la facturation Ro est activée, `RO_DESTINATION` adresse le pair OCS plutôt que le XML.

Dépannage

Échecs d'enregistrement

Symptômes : Utilisateurs incapables de s'enregistrer, délais d'enregistrement, 4xx/5xx sur REGISTER.

- **Connectivité HSS (Cx)** - le S-CSCF dépend du HSS pour répondre au Cx MAR (vecteur d'authentification) et SAR (profil de service). Si MAR/SAR expirent ou renvoient des réponses mal formées, l'enregistrement échoue **503**. Vérifiez que le pair Cx vers le HSS est opérationnel et répond. Voir Opérations Diameter.
- **Échecs d'authentification** - confirmez que les identifiants de l'abonné sont provisionnés dans le HSS et que le HSS a généré le vecteur d'authentification (MAR/MAA). Vérifiez que l'algorithme de défi est un que l'UE prend en charge (AKA/Milenage pour USIM/ISIM, Digest pour les clients non-IMS). Une identité rejetée échoue **403**.
- **Attribution S-CSCF / capacité** - un abonné sans profil de service IMS, ou une attribution de serveur rejetée (SAR), échoue **403**. Confirmez que les capacités du S-CSCF correspondent à ce sur quoi l'I-CSCF a sélectionné. Confirmez également que le nœud a la capacité d'enregistrement.

Échecs de configuration d'appel

Symptômes : Les appels échouent à établir, erreurs SIP 4xx/5xx.

- **Utilisateur non enregistré** - vérifiez que les identités d'origine et de terminaison sont toutes deux enregistrées IMS. Un INVITE de terminaison vers une identité sans liaison de contact renvoie **404**. Pour une identité de terminaison non enregistrée avec des services provisionnés, le S-CSCF récupère le profil non enregistré (Cx SAR UNREGISTERED_USER). Un délai d'attente du HSS ici échoue **503**.
- **IFC / déclenchement de service** - vérifiez que le S-CSCF a téléchargé l'IFC du HSS (SAR/SAA) et que les points de déclenchement correspondent au cas de session. Vérifiez que tout Serveur d'Application invoqué via ISC (OmniTAS, OmniMessage) est accessible. La Gestion par Défaut régit si un échec de l'AS continue la branche ou l'abandonne.

- **QoS** - le P-CSCF autorise la QoS média pour l'appel (Rx vers le PCRF pour VoLTE, N5 vers le PCF pour VoNR). Si les appels se connectent mais n'ont pas de chemin média, vérifiez la branche de politique sur le P-CSCF.
- **Routage** - pour les destinations E.164, vérifiez la résolution ENUM et le basculement de passerelle PSTN. Vérifiez le routage en itinérance/hors réseau pour les appels qui quittent le réseau domestique.

Problèmes de livraison de SMS

Symptômes : SMS non livrés via IMS, ou revenant à l'ancien SMSC.

- **Déclenchement IFC d'OmniMessage** - vérifiez que l'IFC de l'abonné déclenche OmniMessage sur la méthode SIP MESSAGE et que sa priorité est suffisamment élevée pour être déclenchée. Testez la correspondance de l'IFC avec un SMS simulé.
- **Intégration SMSC** - vérifiez la connectivité d'OmniMessage au SMSC (MAP/SMPP) et que la conversion SIP MESSAGE ↔ PDU SMS est intacte.
- **Type de contenu** - vérifiez que le SIP MESSAGE porte `Content-Type: application/vnd.3gpp.sms` et le bon encodage de jeu de caractères (GSM-7, UCS-2).

Flux d'appels

Les diagrammes de séquence sont intégrés avec les fonctions qu'ils documentent :

- Enregistrement et authentification → Enregistrement et authentification
- Session d'origine → Gestion des appels d'origine
- Session de terminaison → Gestion des appels de terminaison

Documentation Connexe

- Opérations
- Diameter
- Interface Basée sur le Service (SBI)

- Référence des Métriques
- OmniWeb - enregistrements, dialogues et état des pairs Diameter : <https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>

Documentation de conformité à l'interception ANSSI R226

Objectif du document : Ce document fournit les spécifications techniques requises pour l'autorisation ANSSI R226. Ces spécifications s'appliquent en vertu des articles R226-3 et R226-7 du Code pénal français. Elles couvrent le réseau de cœur IMS OmniCSCF (Fonctions de contrôle de session d'appel).

Classification : Documentation de conformité réglementaire

Autorité cible : Agence nationale de la sécurité des systèmes d'information (ANSSI)

Réglementation : R226 - Protection de la vie privée des correspondances et interception légale

---

1. SPÉCIFICATIONS TECHNIQUES DÉTAILLÉES

1.1 Identification du système

Nom du produit : Réseau de cœur IMS OmniCSCF
Type de produit : Système multimédia IP (IMS) Réseau de cœur
Fonction principale : Contrôle de session d'appel VoIP/VoLTE et livraison de services multimédias
Modèle de déploiement : Infrastructure de télécommunications sur site

Composants du réseau :

- P-CSCF (Fonction de contrôle de session d'appel proxy)
- E-CSCF (Fonction de contrôle de session d'appel d'urgence)
- I-CSCF (Fonction de contrôle de session d'appel interrogateur)
- S-CSCF (Fonction de contrôle de session d'appel de service)

Ce système gère l'enregistrement, l'authentification, le routage de session et le contrôle des appels pour les réseaux de système multimédia IP (IMS). Les sections ci-dessous décrivent les capacités d'interception et les caractéristiques de cryptage.

1.2 Capacités d'interception

1.2.1 Enregistrement et acquisition de session

Capture d'enregistrement SIP :

Le système CSCF traite tous les enregistrements SIP. Il conserve l'état complet de l'enregistrement :

- **Identifiants utilisateur :**
  - IMPU (Identité publique multimédia IP) - URI SIP (par exemple, sip:+33612345678@ims.mnc001.mcc001.3gppnetwork.org)
  - IMPI (Identité privée multimédia IP) - Nom d'utilisateur d'authentification (par exemple, user@ims.mnc001.mcc001.3gppnetwork.org)
  - IMSI (Identité d'abonné mobile international) - À partir des en-têtes P ou HSS
  - MSISDN (Numéro de téléphone mobile) - À partir de l'IMPU ou du profil utilisateur HSS
- **Métadonnées d'enregistrement :**
  - URI de contact (adresse réseau actuelle de l'UE)
  - En-tête de chemin (route de retour via P-CSCF)
  - En-tête Service-Route (route vers S-CSCF)
  - Chaîne User-Agent (identification du type d'appareil)
  - Horodatage d'expiration de l'enregistrement

    - Adresse IP source et port
    - Protocole de transport (TCP/UDP/TLS)
    - Vecteurs d'authentification (RAND, AUTN, XRES, CK, IK du HSS)

- **Informations de localisation du réseau :**

    - En-tête P-Access-Network-Info (tour de téléphonie mobile, zone de localisation)
    - P-Visited-Network-ID (identification du réseau en itinérance)
    - Adresse IP reçue (source réelle)
    - Adresse P-CSCF (point d'entrée du réseau)

Capture de session d'appel :

Le S-CSCF conserve l'état complet du dialogue SIP pour tous les appels actifs :

- **Identifiants de session :**

    - Call-ID (identifiant de session unique)
    - URIs et tags From/To
    - Ensembles de route pour les deux parties
    - Original-Dialog-ID (pour le suivi des interactions avec le serveur d'application)

- **Métadonnées de session :**

    - Identité de l'appelant (en-tête From, P-Asserted-Identity)
    - Partie appelée (en-tête To, Request-URI)
    - Horodatage d'établissement de session
    - Horodatage de terminaison de session
    - État du dialogue (Précoce/Confirmé/Supprimé)
    - Numéros CSeq (séquençage des transactions)

- **Informations multimédia :**

    - SDP (Protocole de description de session) dans les corps de message SIP
    - Adresses des serveurs multimédias (OmniTAS)

    - Informations sur les codecs (formats audio/vidéo)
    - Points de terminaison de flux multimédia
    - Allocations de ports RTP/RTCP

Identification des appels d'urgence :

Le composant E-CSCF identifie les appels d'urgence et les route :

- Détection de numéro d'urgence (112, 911, etc.)
- Capture de l'IMEI (Identité internationale d'équipement mobile)
- Cartographie IMEI vers MSISDN (pour rappel)
- Informations de localisation de l'UE ou du réseau
- Support du protocole HELD (HTTP-Enabled Location Delivery)
- Destination de routage d'urgence (PSAP/AS d'urgence)

Détermination de l'identité de l'appelant (selon 3GPP TS 23.167) :

Le système établit l'identité de ligne d'appel authentifiée présentée sur la branche d'urgence comme suit :

- **Appelant connu (enregistré) :** Le système prend l'identité de l'IMPU enregistré. Le cas échéant, il utilise également le lien IMEI→MSISDN mis en cache détenu par le P-CSCF.
- **Appelant inconnu/anonyme (urgence non authentifiée, pas d'identité enregistrée) :** Le P-CSCF résout l'identité au niveau EPC à partir du PCRF via l'interface Diameter Rx. Il utilise un `Rx_AAR_Subscription` asynchrone, lié par l'adresse IP source de l'UE. Le système sélectionne l'identité par ordre de priorité **MSISDN → IMSI → IMEISV**. Il affirme la valeur résolue comme **P-Asserted-Identity** sur le domaine `sos.apn`.

Dans les deux cas, le P-Asserted-Identity résultant est l'identité de ligne d'appel authentifiée présentée au PSAP et sur les interfaces LI. C'est une identité affirmée par le réseau, pas une simple approximation.

1.2.2 Stockage et traitement des données

IMPORTANT : État en mémoire uniquement

Les composants CSCF (P-CSCF, E-CSCF, I-CSCF, S-CSCF) conservent **toutes les données d'état en mémoire uniquement**. Il n'y a **aucun stockage de base de données persistant** des données d'enregistrement ou de session d'appel. Le système stocke tous les liens d'enregistrement, l'état du dialogue et les associations de sécurité IPsec en mémoire. Le système perd ces données lors du redémarrage.

Données d'enregistrement actives (en mémoire) :

Le système CSCF conserve uniquement l'état en temps réel :

État d'enregistrement P-CSCF :

- Données d'association de sécurité IPsec (paires SPI, ports, paramètres de cryptage)
- Liens de contact de l'UE et adresses réseau
- Points de terminaison et statut de tunnel IPsec
- Périodes de validité d'enregistrement

État d'enregistrement S-CSCF :

- Identités publiques (IMPU) et état d'enregistrement actuel
- Liens de contact avec en-têtes de chemin, User-Agent, adresses reçues
- Mappages d'identité privée (IMPI) vers identités publiques
- Profils utilisateurs du HSS (mis en cache lors de l'enregistrement)

État de session active (en mémoire) :

Le S-CSCF conserve uniquement l'état des appels actifs :

- Identifiants d'appel (Call-ID), identités des participants (tags From/To)
- Ensembles de route et adresses de contact
- État de session (Précoce/Confirmé/Terminé)
- Informations temporelles de session

Pas de CDR ni de suivi historique :

Les composants CSCF ne génèrent ni ne stockent :

- Enregistrements de détails d'appel (CDRs)
- Enregistrements d'appels historiques
- Enregistrements d'enregistrements historiques
- Suivi d'événements à long terme

Génération de CDR et suivi historique : Le **TAS (Serveur d'application de téléphonie - OmniTAS)** gère tous les enregistrements de détails d'appel, les données de facturation et le suivi des appels historiques. Les composants CSCF ne les gèrent pas.

Journalisation des messages SIP/Diameter :

Les CSCF peuvent générer des journaux d'événements en temps réel pour un usage opérationnel :

- **Journalisation des messages SIP :** Journalisation optionnelle des messages SIP (INVITE, REGISTER, etc.)
- **Journalisation des messages Diameter :** Journalisation optionnelle des transactions Diameter (Cx, Rx, Ro)
- **Événements système :** Changements de configuration, erreurs, pannes

Ces journaux sont des journaux opérationnels transitoires, pas des enregistrements d'appels persistants. Vous pouvez configurer la rétention des journaux. La rétention est généralement à court terme (heures à jours) uniquement pour le débogage.

1.2.3 Capacités d'analyse

Surveillance en temps réel :

Le portail de gestion OmniWeb (<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>) fournit :

- **Surveillance des enregistrements :**
  - Voir tous les utilisateurs enregistrés avec pagination
  - Recherche par IMPU, contact, IMPI
  - Détails d'enregistrement (contact, chemin, user-agent, expiration)
  - Capacité de désenregistrement forcé

- **Surveillance des dialogues :**
  - Vue des sessions d'appel actives
  - Call-ID, URIs From/To, état, durée
  - Capacité de terminaison d'appel (envoyer BYE)
  - Actualisation automatique toutes les 5 secondes
- **État du système :**
  - État des pairs Diameter (HSS, PCRF, connectivité OCS)
  - État de la passerelle frontend
  - Métriques de capacité du système
  - Capacité de tunnel IPsec (P-CSCF)

Remarque sur les données historiques :

Les composants CSCF ne conservent pas de données historiques. **OmniTAS (Serveur d'application de téléphonie)** gère toute la génération de CDR et le suivi des appels à long terme. Pour les enregistrements d'appels historiques, les CDR et l'analyse des modèles de communication, les autorités d'interception légale doivent coordonner avec OmniTAS.

Visibilité de déclenchement de service en temps réel :

Le S-CSCF traite les critères de filtre initiaux (iFC) en temps réel :

- L'évaluation des iFC détermine quels serveurs d'application sont déclenchés pour chaque appel
- Visibilité en temps réel sur les services invoqués
- Décisions de routage du serveur d'application visibles dans le flux de messages SIP

État du réseau :

- État de connectivité HSS (interface Diameter Cx)
- Distribution de sélection S-CSCF (I-CSCF)
- Modèles de routage des appels
- Temps de réponse du serveur d'application

- Performance des transactions Diameter

1.3 Capacités de contre-mesures

1.3.1 Mécanismes de protection de la vie privée

Confidentialité des communications :

- **Tunnels IPsec :** Tunnels ESP (Encapsulating Security Payload) entre l'UE et le P-CSCF
  - Cryptage : AES-CBC, AES-GCM
  - Authentification : HMAC-SHA1, HMAC-SHA256
  - Dérivation de clé à partir de l'IMS AKA (CK/IK du HSS)
  - Associations de sécurité par UE
- **Support TLS/TLS :**
  - Support SIP sur TLS (SIPS)
  - Diameter sur TLS (HSS, PCRF, connexions OCS)
  - Authentification basée sur des certificats
  - Confidentialité parfaite des échanges (PFS) via ECDHE/DHE
- **En-têtes de confidentialité SIP :**
  - P-Asserted-Identity (ID d'appelant authentifié)
  - En-tête de confidentialité (demande de suppression de l'ID d'appelant)
  - Support de session anonyme

Contrôle d'accès :

- Authentification OmniWeb et contrôle d'accès basé sur les rôles
- Interface de gestion BINRPC (port 2046)
- Contrôles d'accès au registre et séparation des rôles
- Authentification SIP (AKA via HSS)
- Authentification des pairs Diameter

Journalisation d'audit :

- Journalisation complète des messages SIP et Diameter
- Événements d'enregistrement/désenregistrement
- Événements d'établissement et de terminaison d'appel
- Actions administratives via OmniWeb
- Changements de configuration
- Succès/échec de l'authentification

1.3.2 Fonctionnalités de protection des données

Sécurité d'accès :

- Contrôle d'accès basé sur les rôles (RBAC)
- Comptes de surveillance en lecture seule
- Contrôles d'authentification et d'autorisation

Renforcement du système :

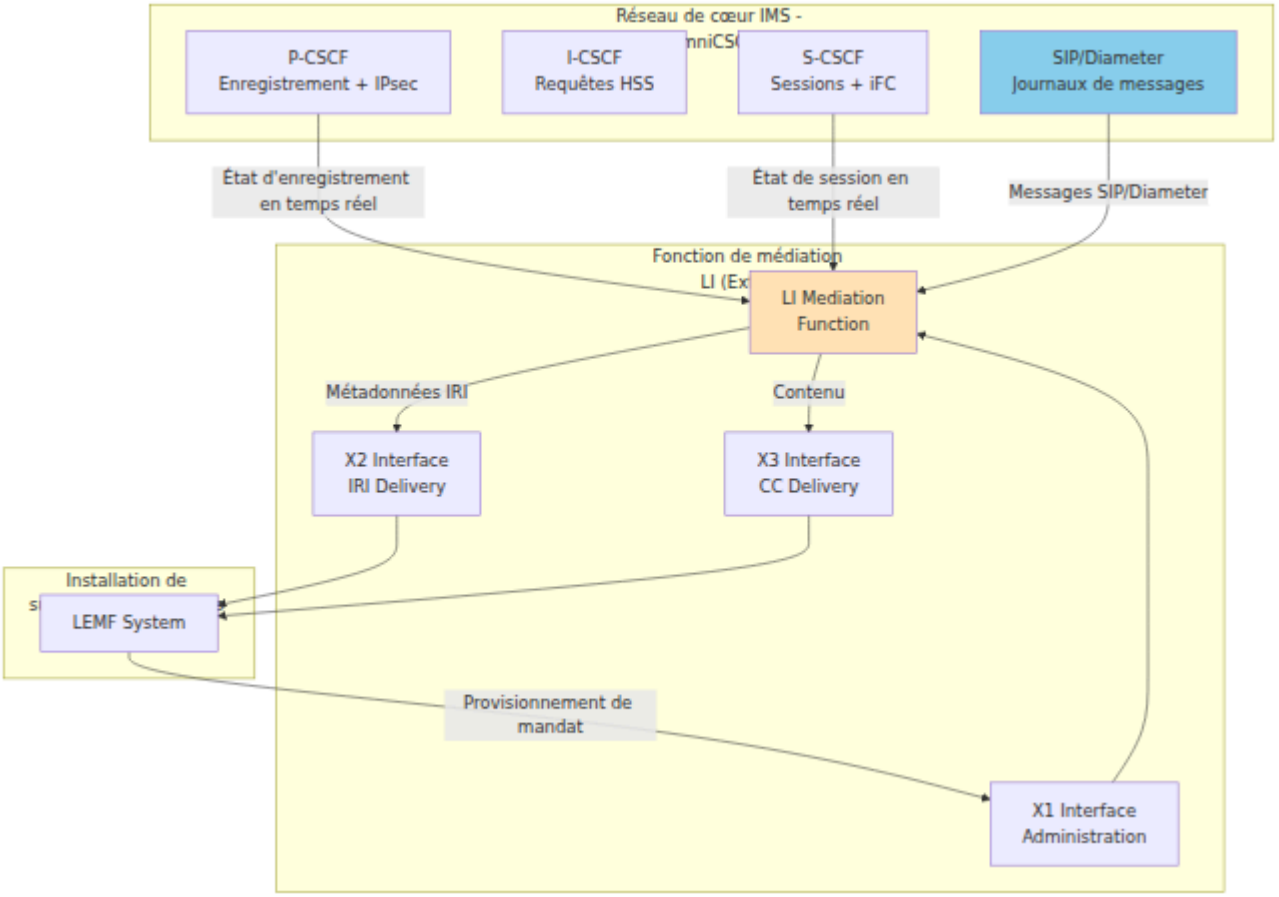
- Ports réseau exposés minimaux (5060 SIP, 3868 Diameter, 2046 gestion BINRPC)
- Vérification de la validité des messages SIP
- Prévention des boucles Max-Forwards
- Limitation de débit et protection contre les inondations
- Limites de taille des messages
- Isolation des processus de travail

1.4 Points d'intégration pour l'interception légale

1.5.1 Architecture d'interception légale ETSI

Le système CSCF fournit une base pour l'interception légale conforme à l'ETSI. Le système ne construit pas d'interfaces X1/X2/X3 natives. Tous les points d'accès aux données nécessaires existent pour l'intégration avec des systèmes externes de fonction de médiation d'interception légale (LIMF).

Interfaces LI standard ETSI :



Interface X1 - Fonction d'administration :

- **Objectif :** Provisionnement de mandat et de cible par les forces de l'ordre
- **Direction :** LEMF → LIMF (bidirectionnelle)
- **Fonctions :**
  - Activer/désactiver l'interception pour les cibles (IMPUs, IMSIs, MSISDNs)
  - Définir la durée et la période de validité de l'interception
  - Configurer les critères de filtrage (identités, fenêtres temporelles)
  - Récupérer l'état de l'interception
- **Intégration avec CSCF :**
  - LIMF conserve la base de données des mandats (liste de cibles, externe au CSCF)
  - LIMF surveille l'état en temps réel du CSCF et les journaux de messages pour les sessions correspondantes
  - LIMF filtre sur les critères provisionnés par X1

Interface X2 - Livraison d'IRI (Informations liées à l'interception) :

- **Objectif :** Livrer des métadonnées de session aux forces de l'ordre

- **Direction :** LIMF → LEMF (unidirectionnelle)
- **Format de données :** Conformité ETSI TS 102 232 XML/ASN.1
- **Contenu du CSCF :**
  - Identifiants de session (Call-ID, tags de dialogue)
  - Partie appelante (URI From, P-Asserted-Identity, IMPU, IMSI, MSISDN)
  - Partie appelée (URI To, Request-URI, IMPU, IMSI, MSISDN)
  - Horodatages d'enregistrement
  - Horodatages de mise en place/teardown de session
  - Localisation réseau (P-Access-Network-Info, tour de téléphonie mobile, zone de localisation)
  - Adresses P-CSCF/S-CSCF (identification des éléments du réseau)
  - User-Agent (type d'appareil)
  - Informations sur l'itinérance (P-Visited-Network-ID)

Interface X3 - Livraison CC (Contenu de la communication) :

- **Objectif :** Livrer le contenu de communication réel
- **Direction :** LIMF → LEMF (unidirectionnelle)
- **Format de données :** Conformité ETSI TS 102 232
- **Contenu du CSCF :**
  - Corps de messages SIP (descriptions de session SDP)
  - Adresses des serveurs multimédias (pour l'interception RTP)
  - Informations sur les codecs
  - Messages instantanés SIP MESSAGE (contenu du corps)
  - Données d'application (si routées via CSCF)

Remarque : Pour les flux RTP de voix/vidéo, le LIMF doit également s'intégrer avec les serveurs multimédias (OmniTAS). Cette intégration capture le contenu multimédia réel. Le CSCF fournit des informations de configuration de session (SDP). Ces informations montrent où les flux multimédias circulent.

1.5.2 Sources de données CSCF pour l'interception légale

1. Accès aux données d'enregistrement :

Données d'enregistrement P-CSCF :

- IMPU (identité publique)
- URI de contact (adresse réseau de l'UE)
- IP et port reçus
- En-tête de chemin
- Expiration de l'enregistrement
- Informations SPI et port IPsec
- Chaîne User-Agent

Données d'enregistrement S-CSCF :

- Identités publiques (IMPU), statut de barring, état d'enregistrement
- Liens de contact avec en-têtes de chemin, User-Agent, adresses reçues
- Mappages d'identité privée (IMPI) vers identités publiques
- Profils utilisateurs du HSS (format XML incluant les détails de l'abonné)

Méthodes d'accès :

- Interfaces d'accès aux données en lecture seule
- Interface de surveillance OmniWeb
- Journalisation d'événements en temps réel

2. Données de session active :

Données de dialogue S-CSCF :

- Call-ID (identifiant de session unique)
- URIs et tags From/To
- Numéros CSeq de l'appelant et du destinataire
- Ensembles de route pour les deux parties
- Adresses de contact
- État du dialogue (Précoce, Confirmé, Supprimé)
- Horodatage de début
- Valeurs de timeout

Méthodes d'accès :

- Surveillance de l'état du dialogue en temps réel

- Requête par identifiants de session ou identifiants de partie
- Capacités d'exportation pour analyse judiciaire

3. Journalisation des messages SIP :

Capture de journal :

- Tous les messages SIP peuvent être journalisés (REGISTER, INVITE, MESSAGE, etc.)
- Niveaux de journalisation configurables
- Journalisation structurée avec horodatages
- Journalisation basée sur Syslog ou fichier

Analyse des journaux :

- Analyse des en-têtes SIP pour extraction d'identité
- Extraction de SDP pour informations multimédias
- Suivi des séquences de messages (CSeq)
- Corrélation des requêtes et des réponses

Exemple d'entrée de journal :

```
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. Journalisation des messages Diameter :

Messages Cx (Communication HSS) :

- UAR/UAA : Autorisation utilisateur (contient IMPU, IMPI)
- LIR/LIA : Informations de localisation (contient IMPU, S-CSCF de service)
- MAR/MAA : Authentification (contient IMPI, vecteurs d'authentification)
- SAR/SAA : Attribution de serveur (contient IMPU, IMPI, XML de profil utilisateur)

Données Diameter disponibles :

- IMSI (à partir du profil utilisateur)
- MSISDN (à partir du profil utilisateur)
- IMPUs associés (plusieurs identités par abonné)
- Profil utilisateur (services, barring, statut d'itinérance)

Exemple de journal :

```
Diameter Cx SAA reçu du 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 (Succès)
User-Data: <XML profil utilisateur avec IMSI, MSISDN, iFC>
```

5. Données d'appel d'urgence (E-CSCF) :

Cartographie IMEI vers MSISDN :

- Le P-CSCF crée la cartographie lorsqu'un UE s'enregistre avec un IMEI (table `emergency_imei_msisdn_map`)
- TTL de 4 heures (14400s auto-expiration)
- Utilisé pour le rappel d'urgence
- Répliqué à travers les nœuds de cluster P-CSCF

Conservation des données :

- Les mappages IMEI vers MSISDN sont conservés pendant 4 heures (14400s)
- Disponibles pour la corrélation de rappel d'urgence
- Accessibles via les interfaces de surveillance

Journaux d'appels d'urgence :

- Détection de numéro d'urgence (112, 911, etc.)
- Extraction de l'IMEI à partir du contact ou des en-têtes P
- Informations de localisation (à partir de HELD ou P-Access-Network-Info)
- Routage PSAP (Point de réponse de sécurité publique)
- Routage E-CSCF vers AS d'urgence

1.5.3 Capacités d'intégration pour LIMF

Le système fournit plusieurs méthodes d'intégration pour les systèmes de fonction de médiation d'interception légale (LIMF) :

1. **Accès aux données d'enregistrement et de session :**

    - Accès en temps réel aux données d'enregistrement (identités, emplacements, informations sur les appareils)
    - Surveillance des sessions actives (état d'appel, participants, timing)
    - Capacités de requête historique

2. **Journalisation des événements :**

    - Journalisation des messages SIP avec niveaux de détail configurables
    - Journalisation des messages Diameter pour les interactions HSS
    - Journaux d'événements structurés avec horodatages

3. **Surveillance en temps réel :**

    - Surveillance en direct de l'état d'enregistrement
    - Suivi des sessions d'appel actives
    - Détection des appels d'urgence et informations de routage

Les méthodes d'intégration prennent en charge à la fois les architectures basées sur le polling et celles basées sur les événements pour la connectivité LIMF.

1.5.4 Mappage des données CSCF vers les interfaces LI

Mappage des données CSCF vers IRI (X2) :

Source de données CSCF	Champ IRI	Exemple de donn
IMPU (en-têtes SIP/état en mémoire)	Partie A	sip:+33612345678@ims.mnc001.mcc
IMPI (en-têtes SIP/état en mémoire)	ID d'authentification	user@ims.mnc001.mcc001.3gppnetw
IMSI (profil utilisateur HSS)	ID d'abonné	208011234567890
MSISDN (profil utilisateur HSS)	Numéro de téléphone	+33612345678
Call-ID (en-têtes SIP/état de dialogue)	ID de session	f81d4fae-7dec-11d0-a765-00a0c91e6
From/To (en-têtes SIP)	Partie A/Partie B	sip:+33612345678@... / sip:+336876
Horodatage d'enregistrement (en mémoire)	Heure de l'événement	2025-11-29T10:30:00Z
P-Access-Network-Info (en-tête SIP)	Localisation	3GPP-E-UTRAN-FDD;utran-cell-id-3gpp
IP reçue (contact SIP)	Adresse IP de l'UE	10.20.30.40:5060
Adresse P-CSCF (routage SIP)	Élément de réseau	10.4.12.165:5060

Source de données CSCF	Champ IRI	Exemple de donn
Adresse S-CSCF (routage SIP)	Élément de réseau	10.4.11.45:5060

Mappage des données CSCF vers CC (X3) :

Source de données CSCF	Champ CC	Exemple de données
Corps de MESSAGE SIP	Contenu du message instantané	"Bonjour, comment ça va ?"
SDP dans INVITE	Informations de session multimédia	Points de terminaison RTP, codecs
Adresse du serveur multimédia	Cible d'interception RTP	10.50.60.70:49170

Remarque : Pour le contenu réel de la voix/vidéo (RTP), le LIMF doit coordonner avec les serveurs multimédias (OmniTAS) pour capturer les flux RTP. Le CSCF fournit uniquement des informations de configuration de session.

Remarque sur l'identité d'appel d'urgence (Partie A) : Pour un appel normal (enregistré), le système dérive la Partie A de l'IMPU enregistré / P-Asserted-Identity. Pour un **appel d'urgence inconnu/anonyme**, le P-CSCF résout la Partie A à partir du PCRF via Diameter Rx (`Rx_AAR_Subscription`, lié par l'adresse IP source de l'UE, priorité MSISDN → IMSI → IMEISV). Le P-CSCF affirme cette identité comme P-Asserted-Identity sur le domaine `sos.apn`, conformément à la 3GPP TS 23.167. C'est l'identité de ligne d'appel authentifiée portée sur l'interface X2/IRI pour de tels appels.

1.5 Interface de surveillance basée sur le web

OmniWeb fournit un accès de surveillance et administratif. OmniWeb est le portail de gestion unifié

(<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>). Il offre une surveillance en temps réel et un accès administratif aux composants CSCF :

Capacités de surveillance :

- Surveillance en temps réel des enregistrements et des sessions (abonnés actifs, emplacements, informations sur les appareils, état des appels, timing)
- Recherche d'identité par IMPU, IMPI, IMSI ou MSISDN
- État et capacité des tunnels IPsec
- Capacités d'exportation pour analyse judiciaire

Sécurité :

- Accès chiffré HTTPS/TLS
- Authentification requise
- Contrôle d'accès basé sur les rôles (RBAC), y compris des modes d'accès en lecture seule pour le personnel de surveillance
- Journalisation d'audit de toutes les actions administratives

---

2. CAPACITÉS DE CRYPTAGE ET DE CRYPTANALYSE

2.1 Aperçu des capacités cryptographiques

L'OmniCSCF met en œuvre plusieurs couches de protection cryptographique pour le signalement et les données des abonnés. Cette section documente toutes les capacités cryptographiques, comme l'exige l'ANSSI.

2.2 Cryptage du tunnel IPsec ESP (UE vers P-CSCF)

2.2.1 Mise en œuvre du protocole IPsec

Mode IPsec pris en charge :

- ESP (Encapsulating Security Payload) - Protocole IP 50
- Mode transport (pas de mode tunnel)
- Protège le signalement SIP entre l'UE et le P-CSCF

Algorithmes de cryptage pris en charge :

Le système avec IPsec du noyau prend en charge :

- **AES-CBC (Advanced Encryption Standard - Cipher Block Chaining) :**
  - AES-128-CBC (clé de 128 bits)
  - AES-192-CBC (clé de 192 bits)
  - AES-256-CBC (clé de 256 bits) - Recommandé
- **AES-GCM (Advanced Encryption Standard - Galois/Counter Mode) :**
  - AES-128-GCM (clé de 128 bits avec AEAD)
  - AES-256-GCM (clé de 256 bits avec AEAD) - Recommandé
- **3DES-CBC (Triple DES - Cipher Block Chaining) :**
  - Clé effective de 168 bits (déprécié, compatibilité héritée)
- **Cryptage NULL :**
  - Pas de confidentialité (authentification uniquement)
  - Utilisé uniquement pour le débogage ou des scénarios de conformité spécifiques

Algorithmes d'authentification pris en charge :

- **HMAC-SHA1 (Hash-based Message Authentication Code - SHA-1) :**
  - Sortie de 160 bits
  - Compatibilité héritée
- **HMAC-SHA256 (HMAC - SHA-256) :**
  - Sortie de 256 bits
  - Recommandé

- **HMAC-SHA384 (HMAC - SHA-384) :**
  - Sortie de 384 bits
- **HMAC-SHA512 (HMAC - SHA-512) :**
  - Sortie de 512 bits
- **HMAC-MD5 :**
  - Sortie de 128 bits
  - Déprécié, compatibilité héritée uniquement

Dérivation de clé :

Le système dérive les clés IPsec (CK - Cipher Key, IK - Integrity Key) à partir de l'authentification IMS AKA :

1. L'UE effectue l'authentification AKA avec S-CSCF/HSS
2. HSS génère CK (128 bits) et IK (128 bits)
3. S-CSCF délivre CK/IK au P-CSCF via une interface interne
4. P-CSCF utilise CK/IK pour établir des associations de sécurité IPsec avec l'UE
5. CK utilisé pour le cryptage ESP
6. IK utilisé pour l'authentification ESP

Paramètres d'association de sécurité :

- **Durée de vie :** Liée à l'expiration de l'enregistrement SIP (typiquement 599 secondes)
- **Protection contre la répétition :** Activée (fenêtre anti-répétition)
- **Numéros de séquence :** 32 bits ou 64 bits (ESN - Numéros de séquence étendus)
- **Confidentialité parfaite des échanges :** Non applicable (clés provenant d'AKA, pas de Diffie-Hellman)

Mise en œuvre :

La capacité IPsec du P-CSCF :

- Interagit avec la pile IPsec du noyau Linux (framework XFRM)
- Configure les politiques de sécurité et les associations via l'API du noyau
- Allocation et gestion des SPI (Security Parameter Index)
- Allocation de port pour le trafic protégé

2.2.2 Capacités de configuration IPsec

Sélection de suite de chiffrement :

Vous pouvez configurer le P-CSCF pour privilégier des suites de chiffrement spécifiques :

Préférées (sécurité forte) :

- ESP avec AES-256-GCM et HMAC-SHA256
- ESP avec AES-256-CBC et HMAC-SHA256

Supportées (compatibilité) :

- ESP avec AES-128-CBC et HMAC-SHA1
- ESP avec 3DES-CBC et HMAC-SHA1 (héritage)

Gestion des clés :

- IKE (Internet Key Exchange) n'est PAS utilisé
- Clés fournies via IMS AKA (CK/IK du HSS)
- Configuration manuelle des associations de sécurité via le XFRM du noyau
- Destruction automatique des SA à l'expiration de l'enregistrement

Cycle de vie du tunnel :

1. L'UE s'enregistre → Authentification AKA → CK/IK générés
2. P-CSCF reçoit CK/IK de S-CSCF
3. P-CSCF alloue une paire de SPI (SPI client, SPI serveur)
4. P-CSCF alloue une paire de ports (port client, port serveur)
5. P-CSCF configure les SA IPsec du noyau en utilisant CK/IK
6. P-CSCF envoie les paramètres IPsec à l'UE dans 200 OK (en-tête Security-Server)

7. L'UE configure les SA IPsec avec les mêmes paramètres
8. Tout le trafic SIP ultérieur passe par les tunnels ESP
9. À l'expiration de l'enregistrement ou au désenregistrement : SA supprimées, ressources libérées

2.3 Cryptage TLS (SIP et Diameter)

2.3.1 TLS pour SIP (SIPS)

Versions TLS prises en charge :

- **TLS 1.2** (RFC 5246) - Pris en charge
- **TLS 1.3** (RFC 8446) - Pris en charge (si support du noyau/bibliothèque)
- **TLS 1.0/1.1** - Déprécié (désactivé par défaut)
- **SSL 2.0/3.0** - NON SUPPORTE (vulnérabilités connues)

Mise en œuvre de TLS :

Le système utilise OpenSSL ou LibreSSL :

- Bibliothèques TLS standard de l'industrie
- Implémentations validées cryptographiquement
- Mises à jour de sécurité régulières

Suites de chiffrement prises en charge :

TLS 1.3 (Préféré) :

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256

TLS 1.2 (Pris en charge) :

- ECDHE-RSA-AES256-GCM-SHA384 (Confidentialité parfaite des échanges)
- ECDHE-RSA-AES128-GCM-SHA256 (Confidentialité parfaite des échanges)
- ECDHE-ECDSA-AES256-GCM-SHA384 (Confidentialité parfaite des échanges)

- DHE-RSA-AES256-GCM-SHA384 (Confidentialité parfaite des échanges)
- DHE-RSA-AES128-GCM-SHA256 (Confidentialité parfaite des échanges)

Chiffres faibles désactivés :

- Pas de RC4
- Pas de MD5
- Pas de cryptage NULL
- Pas de chiffres de grade EXPORT
- Pas de DES/3DES (déprécié)

Support des certificats :

- **Certificats X.509** (format standard)
- **Clés RSA :** minimum 2048 bits, recommandé 4096 bits
- **Clés ECDSA :** courbes P-256, P-384, P-521 prises en charge
- **Validation de la chaîne de certificats**
- **Vérification CRL (Liste de révocation de certificats)** (optionnel)
- **OCSP (Protocole de statut de certificat en ligne)** (optionnel)

Fonctionnalités TLS :

- **Confidentialité parfaite des échanges (PFS) :** Via échange de clés ECDHE/DHE
- **Indication de nom de serveur (SNI) :** Prise en charge
- **Reprise de session TLS :** Prise en charge (optimisation des performances)
- **Authentification par certificat client :** Prise en charge (TLS mutuel)

SIP sur TLS (SIPS) :

- Transport : TCP avec cryptage TLS
- Port : 5061 (port standard SIPS)
- Utilisé pour la communication inter-CSCF (optionnel)
- Utilisé pour les connexions réseau de confiance

2.3.2 TLS pour Diameter

Capacités Diameter :

Le système prend en charge les éléments suivants :

- **Diameter sur SCTP** (préféré pour la fiabilité)
- **Diameter sur TCP avec TLS**
- **Port :** 3868 (port Diameter standard)

Cas d'utilisation :

- **Interface Cx :** S-CSCF/I-CSCF vers HSS (données d'abonné, authentification)
- **Interface Rx :** P-CSCF vers PCRF (politique QoS)
- **Interface Ro :** S-CSCF vers OCS (facturation en ligne - si activé)

Configuration TLS pour Diameter :

Les mêmes suites de chiffrement que pour SIP

- TLS 1.2/1.3
- Échange de clés ECDHE/DHE (PFS)
- Cryptage AES-GCM
- Authentification SHA256/SHA384

Authentification basée sur des certificats :

- Les pairs Diameter s'authentifient via des certificats TLS
- TLS mutuel (certificats client et serveur)
- Validation FQDN (Nom de domaine entièrement qualifié) dans les certificats
- Validation de la chaîne CA de confiance

2.4 Cryptographie d'authentification

2.4.1 Fonctions cryptographiques IMS AKA

Algorithme 3GPP AKA (MILENAGE) :

Utilisé pour générer des vecteurs d'authentification (RAND, AUTN, XRES, CK, IK) :

Fonctions cryptographiques :

- **f1 :** Fonction d'authentification de message (calculer MAC-A et MAC-S)
- **f2 :** Fonction de réponse (calculer RES à partir de RAND et K)
- **f3 :** Dérivation de clé de chiffrement (calculer CK)
- **f4 :** Dérivation de clé d'intégrité (calculer IK)
- **f5 :** Fonction de clé d'anonymat (calculer AK pour la confidentialité de l'IMSI)

Matériel de clé :

- **K :** Clé d'abonné permanente de 128 bits (stockée dans ISIM et HSS)
- **OPc :** Clé variante d'opérateur (dérivée de K et OP)
- **RAND :** Défi aléatoire de 128 bits
- **SQN :** Numéro de séquence de 48 bits (protection contre la répétition)

Séquence AKA :

1. HSS génère RAND (aléatoire cryptographiquement)
2. HSS calcule MAC-A = f1(K, RAND, SQN, AMF)
3. HSS calcule AUTN = (SQN ⊕ AK) || AMF || MAC-A
4. HSS calcule XRES = f2(K, RAND)
5. HSS calcule CK = f3(K, RAND)
6. HSS calcule IK = f4(K, RAND)
7. HSS envoie {RAND, AUTN, XRES, CK, IK} à S-CSCF
8. S-CSCF défie l'UE avec RAND et AUTN
9. L'UE calcule RES = f2(K, RAND) en utilisant ISIM
10. L'UE envoie RES à S-CSCF
11. S-CSCF compare RES avec XRES (validation d'authentification)

Propriétés de sécurité :

- **Authentification mutuelle :** L'UE vérifie HSS via AUTN, HSS vérifie l'UE via RES

- **Fraîcheur des clés :** RAND est aléatoire, SQN empêche la répétition
- **Dérivation de clé :** CK et IK dérivés du secret partagé K

2.4.2 Authentification Digest HTTP

Pour l'authentification non-IMS (si utilisée) :

Algorithme : MD5 (RFC 2617)

- **Fonction de hachage :** MD5 (sortie de 128 bits)
- **Défi-réponse :** Basé sur nonce
- **Protection contre la répétition :** Nonce avec horodatage

Remarque : L'authentification Digest HTTP avec MD5 est considérée comme faible. L'IMS AKA est fortement préférée.

2.5 Hachage et intégrité

2.5.1 Fonctions de hachage disponibles

Le système peut utiliser les fonctions de hachage suivantes (via OpenSSL/crypto du noyau) :

- **SHA-256 :** Sortie de 256 bits, recommandé
- **SHA-384 :** Sortie de 384 bits
- **SHA-512 :** Sortie de 512 bits
- **SHA-1 :** Sortie de 160 bits, déprécié pour une utilisation en sécurité
- **MD5 :** Sortie de 128 bits, déprécié pour une utilisation en sécurité

Utilisation :

- Constructions HMAC pour IPsec/TLS
- Vérification de l'intégrité des données
- Génération de nonce
- Détection de doublons (hachage Call-ID)

2.5.2 Intégrité des messages

Intégrité des messages SIP :

- **IPsec ESP :** HMAC-SHA256 pour SIP authentifié sur IPsec
- **TLS :** Authentification des messages via TLS MAC
- **Digest SIP :** Intégrité de l'en-tête d'authentification

Intégrité des messages Diameter :

- **TLS :** Diameter sur TLS fournit une authentification des messages
- **HMAC :** Les messages Diameter peuvent inclure des AVPs HMAC pour l'intégrité

2.6 Génération de nombres aléatoires

Génération de nombres aléatoires cryptographiquement sécurisés :

Le système repose sur les éléments suivants :

- **Linux kernel /dev/urandom :** PRNG (Générateur de nombres pseudo-aléatoires cryptographiquement sécurisé)
- **OpenSSL RAND_bytes() :** CSPRNG (Générateur de nombres pseudo-aléatoires cryptographiquement sécurisé)

Utilisation :

- Allocation de SPI (valeur de départ aléatoire)
- Génération de Call-ID
- Génération de paramètres de branche
- Génération de nonce pour l'authentification
- Génération d'ID de session

2.7 Gestion des clés

2.7.1 Gestion des certificats TLS

Stockage des certificats :

- Stockage dans le système de fichiers avec des permissions restreintes (0600)
- Situé dans : `/etc/system/tls/`
- Format PEM pour les certificats et les clés

Génération de certificats :

```
# Générer une clé privée RSA de 4096 bits
openssl genrsa -out system-key.pem 4096

# Générer une CSR (demande de signature de certificat)
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

# Certificat auto-signé (développement/test)
openssl x509 -req -days 365 -in system.csr \
  -signkey system-key.pem -out system-cert.pem

# Production : Soumettre CSR à une CA de confiance
```

Rotation des certificats :

- Renouvellement annuel des certificats recommandé
- Redémarrage en douceur du service pour charger de nouveaux certificats
- Aucun temps d'arrêt requis

2.7.2 Gestion des clés IPsec

Dérivation de clé :

- CK (Clé de chiffrement) et IK (Clé d'intégrité) à partir de l'IMS AKA
- Clés de 128 bits du HSS
- Livrées en toute sécurité via Diameter Cx (sur TLS)

Durée de vie des clés :

- Liée à l'expiration de l'enregistrement SIP (typiquement 599 secondes)
- Renouvellement de clé lors du rafraîchissement de l'enregistrement

- Destruction automatique des clés lors du désenregistrement

Stockage des clés :

- Éphémère (en mémoire uniquement pendant l'enregistrement actif)
- Installé dans la pile IPsec du noyau
- Aucun stockage de clé persistant
- Clés supprimées lorsque SA supprimée

2.8 Résistance à la cryptanalyse

2.8.1 Sélection d'algorithme

Défense contre la cryptanalyse :

- **Aucun algorithme personnalisé :** Uniquement des algorithmes standard de l'industrie, examinés par des pairs
- **Tailles de clés fortes :** AES-256, RSA-4096, SHA-256
- **Chiffrement authentifié :** AES-GCM (AEAD - Chiffrement authentifié avec données associées)
- **Confidentialité parfaite des échanges :** ECDHE/DHE dans TLS
- **Mises à jour régulières :** Patches de sécurité OpenSSL/LibreSSL appliqués

Algorithmes dépréciés désactivés :

- MD5 (collisions de hachage)
- RC4 (faiblesses du chiffrement par flux)
- DES/3DES (petit taille de bloc, longueur de clé)
- SSL 2.0/3.0 (vulnérabilités de protocole)
- TLS 1.0/1.1 (attaques BEAST, POODLE)

2.8.2 Atténuation des attaques par canaux auxiliaires

Résistance aux attaques par temporisation :

- Comparaison en temps constant pour les réponses d'authentification

- Pas de fuites de temporisation dans les opérations cryptographiques (via OpenSSL)

Protection de la mémoire :

- Isolation de la pile IPsec du noyau
- Isolation de la mémoire des processus
- Pas de swap pour les données sensibles (si configuré)

2.9 Conformité et normes

Conformité aux normes cryptographiques :

- **NIST SP 800-52 :** Directives TLS
- **NIST SP 800-131A :** Transitions d'algorithmes cryptographiques
- **RFC 7525 :** Recommandations TLS
- **ETSI TS 133 203 :** Sécurité d'accès 3GPP (IMS AKA)
- **ETSI TS 133 210 :** Sécurité de couche réseau IP (IPsec)
- **3GPP TS 33.203 :** Sécurité d'accès pour IMS
- **3GPP TS 33.210 :** Sécurité de domaine réseau

Réglementations françaises en matière de cryptographie :

- Pas de cryptographie restreinte à l'exportation (tous les algorithmes standard)
- Moyens cryptographiques standard (pas de portes dérobées gouvernementales)
- Certification de produit cryptographique ANSSI (si nécessaire)

Référence des métriques IMS CSCF

Ce document est la référence pour toutes les métriques que les composants P-CSCF, I-CSCF et S-CSCF exportent.

Accès aux métriques

Tous les composants CSCF exposent des métriques Prometheus sur le port 9090 :

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

Chaque hôte CSCF (P-CSCF, I-CSCF, S-CSCF) exporte ses propres métriques. Pour obtenir une couverture de surveillance complète, configurez votre serveur Prometheus pour interroger tous les hôtes.

Exemple de configuration 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']
```

Pour des conseils sur la surveillance et l'alerte, voir :

- Surveillance via OmniWeb et Grafana

Surveillance via OmniWeb et Grafana

Visualisez l'état opérationnel dans **OmniWeb**, le portail de gestion unifié : <https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>. L'état opérationnel comprend les enregistrements, les dialogues et l'état des pairs Diameter. OmniWeb intègre des tableaux de bord Grafana pour une visibilité en temps réel et historique. Ces tableaux de bord incluent des vues d'enregistrement S-CSCF et de localisation d'utilisateur. Les métriques `ims_usrloc_scscf_active_impus` et `ims_usrloc_scscf_active_contacts` soutiennent ces vues. Les tableaux de bord affichent également l'état des pairs Diameter et la profondeur de la file d'attente. La métrique `cdp_queuelength` et les métriques d'interface `ims_icscf_uar_*`, `ims_icscf_lir_*`, `ims_auth_mar_*`, `ims_registrar_scscf_sar_*`, et `ims_qos_*` soutiennent ces vues.

Les métriques Prometheus dans cette référence soutiennent ces tableaux de bord Grafana. Elles soutiennent également toute alerte personnalisée que vous configurez.

Métriques P-CSCF

Métriques CDP (Diameter)

Nom de la métrique	Signification
`cdp_average_response_time`	Temps de réponse moyen pour les requêtes Diameter en millisecondes (calculé comme replies_response_time / replies_received)
`cdp_queuelength`	Longueur actuelle de la file d'attente des tâches du travailleur Diameter
`cdp_replies_received`	Nombre total de réponses Diameter reçues
`cdp_replies_response_time`	Temps total passé à attendre les réponses Diameter en millisecondes
`cdp_timeout`	Nombre d'événements de délai d'attente sur les requêtes Diameter

Statistiques SIP de base

Compteurs de requêtes

Nom de la métrique	Signification
`core_rcv_requests`	Nombre total de requêtes SIP reçues
`core_rcv_requests_ack`	Nombre de requêtes ACK reçues
`core_rcv_requests_bye`	Nombre de requêtes BYE reçues
`core_rcv_requests_cancel`	Nombre de requêtes CANCEL reçues
`core_rcv_requests_info`	Nombre de requêtes INFO reçues
`core_rcv_requests_invite`	Nombre de requêtes INVITE reçues
`core_rcv_requests_message`	Nombre de requêtes MESSAGE reçues
`core_rcv_requests_notify`	Nombre de requêtes NOTIFY reçues
`core_rcv_requests_options`	Nombre de requêtes OPTIONS reçues
`core_rcv_requests_prack`	Nombre de requêtes PRACK reçues
`core_rcv_requests_publish`	Nombre de requêtes PUBLISH reçues
`core_rcv_requests_refer`	Nombre de requêtes REFER reçues
`core_rcv_requests_register`	Nombre de requêtes REGISTER reçues
`core_rcv_requests_subscribe`	Nombre de requêtes SUBSCRIBE reçues
`core_rcv_requests_update`	Nombre de requêtes UPDATE reçues

Compteurs de réponses (Général)

Nom de la métrique	Signification
`core_rcv_replies`	Nombre total de réponses SIP reçues
`core_rcv_replies_18x`	Nombre de réponses provisoires 180/181/183/186/187/189 reçues
`core_rcv_replies_1xx`	Nombre de réponses 1xx (provisoires) reçues
`core_rcv_replies_2xx`	Nombre de réponses 2xx (succès) reçues
`core_rcv_replies_3xx`	Nombre de réponses 3xx (redirection) reçues
`core_rcv_replies_4xx`	Nombre de réponses 4xx (erreur client) reçues
`core_rcv_replies_5xx`	Nombre de réponses 5xx (erreur serveur) reçues
`core_rcv_replies_6xx`	Nombre de réponses 6xx (échec global) reçues

Compteurs de réponses par méthode (1xx)

Nom de la métrique	Signification
`core_rcv_replies_1xx_bye`	Nombre de réponses 1xx aux requêtes BYE
`core_rcv_replies_1xx_cancel`	Nombre de réponses 1xx aux requêtes CANCEL
`core_rcv_replies_1xx_invite`	Nombre de réponses 1xx aux requêtes INVITE
`core_rcv_replies_1xx_message`	Nombre de réponses 1xx aux requêtes MESSAGE
`core_rcv_replies_1xx_prack`	Nombre de réponses 1xx aux requêtes PRACK
`core_rcv_replies_1xx_refer`	Nombre de réponses 1xx aux requêtes REFER
`core_rcv_replies_1xx_reg`	Nombre de réponses 1xx aux requêtes REGISTER
`core_rcv_replies_1xx_update`	Nombre de réponses 1xx aux requêtes UPDATE

Compteurs de réponses par méthode (2xx)

Nom de la métrique	Signification
`core_rcv_replies_2xx_bye`	Nombre de réponses 2xx (succès) aux requêtes BYE
`core_rcv_replies_2xx_cancel`	Nombre de réponses 2xx (succès) aux requêtes CANCEL
`core_rcv_replies_2xx_invite`	Nombre de réponses 2xx (succès) aux requêtes INVITE
`core_rcv_replies_2xx_message`	Nombre de réponses 2xx (succès) aux requêtes MESSAGE
`core_rcv_replies_2xx_prack`	Nombre de réponses 2xx (succès) aux requêtes PRACK
`core_rcv_replies_2xx_refer`	Nombre de réponses 2xx (succès) aux requêtes REFER
`core_rcv_replies_2xx_reg`	Nombre de réponses 2xx (succès) aux requêtes REGISTER
`core_rcv_replies_2xx_update`	Nombre de réponses 2xx (succès) aux requêtes UPDATE

Compteurs de réponses par méthode (3xx)

Nom de la métrique	Signification
`core_rcv_replies_3xx_bye`	Nombre de réponses 3xx (redirection) aux requêtes BYE
`core_rcv_replies_3xx_cancel`	Nombre de réponses 3xx (redirection) aux requêtes CANCEL
`core_rcv_replies_3xx_invite`	Nombre de réponses 3xx (redirection) aux requêtes INVITE
`core_rcv_replies_3xx_message`	Nombre de réponses 3xx (redirection) aux requêtes MESSAGE
`core_rcv_replies_3xx_prack`	Nombre de réponses 3xx (redirection) aux requêtes PRACK
`core_rcv_replies_3xx_refer`	Nombre de réponses 3xx (redirection) aux requêtes REFER
`core_rcv_replies_3xx_reg`	Nombre de réponses 3xx (redirection) aux requêtes REGISTER
`core_rcv_replies_3xx_update`	Nombre de réponses 3xx (redirection) aux requêtes UPDATE

Compteurs de réponses par méthode (4xx)

Nom de la métrique	Signification
`core_rcv_replies_4xx_bye`	Nombre de réponses 4xx (erreur client) aux requêtes BYE
`core_rcv_replies_4xx_cancel`	Nombre de réponses 4xx (erreur client) aux requêtes CANCEL
`core_rcv_replies_4xx_invite`	Nombre de réponses 4xx (erreur client) aux requêtes INVITE
`core_rcv_replies_4xx_message`	Nombre de réponses 4xx (erreur client) aux requêtes MESSAGE
`core_rcv_replies_4xx_prack`	Nombre de réponses 4xx (erreur client) aux requêtes PRACK
`core_rcv_replies_4xx_refer`	Nombre de réponses 4xx (erreur client) aux requêtes REFER
`core_rcv_replies_4xx_reg`	Nombre de réponses 4xx (erreur client) aux requêtes REGISTER
`core_rcv_replies_4xx_update`	Nombre de réponses 4xx (erreur client) aux requêtes UPDATE

Compteurs de réponses par méthode (5xx)

Nom de la métrique	Signification
`core_rcv_replies_5xx_bye`	Nombre de réponses 5xx (erreur serveur) aux requêtes BYE
`core_rcv_replies_5xx_cancel`	Nombre de réponses 5xx (erreur serveur) aux requêtes CANCEL
`core_rcv_replies_5xx_invite`	Nombre de réponses 5xx (erreur serveur) aux requêtes INVITE
`core_rcv_replies_5xx_message`	Nombre de réponses 5xx (erreur serveur) aux requêtes MESSAGE
`core_rcv_replies_5xx_prack`	Nombre de réponses 5xx (erreur serveur) aux requêtes PRACK
`core_rcv_replies_5xx_refer`	Nombre de réponses 5xx (erreur serveur) aux requêtes REFER
`core_rcv_replies_5xx_reg`	Nombre de réponses 5xx (erreur serveur) aux requêtes REGISTER
`core_rcv_replies_5xx_update`	Nombre de réponses 5xx (erreur serveur) aux requêtes UPDATE

Compteurs de réponses par méthode (6xx)

Nom de la métrique	Signification
`core_rcv_replies_6xx_bye`	Nombre de réponses 6xx (échec global) aux requêtes BYE
`core_rcv_replies_6xx_cancel`	Nombre de réponses 6xx (échec global) aux requêtes CANCEL
`core_rcv_replies_6xx_invite`	Nombre de réponses 6xx (échec global) aux requêtes INVITE
`core_rcv_replies_6xx_message`	Nombre de réponses 6xx (échec global) aux requêtes MESSAGE
`core_rcv_replies_6xx_prack`	Nombre de réponses 6xx (échec global) aux requêtes PRACK
`core_rcv_replies_6xx_refer`	Nombre de réponses 6xx (échec global) aux requêtes REFER
`core_rcv_replies_6xx_reg`	Nombre de réponses 6xx (échec global) aux requêtes REGISTER
`core_rcv_replies_6xx_update`	Nombre de réponses 6xx (échec global) aux requêtes UPDATE

Compteurs de codes d'état spécifiques

Nom de la métrique	Signification
`core_rcv_replies_400`	Nombre de réponses 400 Bad Request reçues
`core_rcv_replies_401`	Nombre de réponses 401 Unauthorized reçues
`core_rcv_replies_402`	Nombre de réponses 402 Payment Required reçues
`core_rcv_replies_403`	Nombre de réponses 403 Forbidden reçues
`core_rcv_replies_404`	Nombre de réponses 404 Not Found reçues
`core_rcv_replies_405`	Nombre de réponses 405 Method Not Allowed reçues
`core_rcv_replies_406`	Nombre de réponses 406 Not Acceptable reçues
`core_rcv_replies_407`	Nombre de réponses 407 Proxy Authentication Required reçues
`core_rcv_replies_408`	Nombre de réponses 408 Request Timeout reçues
`core_rcv_replies_409`	Nombre de réponses 409 Conflict reçues
`core_rcv_replies_410`	Nombre de réponses 410 Gone reçues
`core_rcv_replies_411`	Nombre de réponses 411 Length Required reçues
`core_rcv_replies_413`	Nombre de réponses 413 Request Entity Too Large reçues
`core_rcv_replies_414`	Nombre de réponses 414 Request-URI Too Long reçues
`core_rcv_replies_415`	Nombre de réponses 415 Unsupported Media Type reçues

Nom de la métrique	Signification
`core_rcv_replies_420`	Nombre de réponses 420 Bad Extension reçues
`core_rcv_replies_480`	Nombre de réponses 480 Temporarily Unavailable reçues
`core_rcv_replies_481`	Nombre de réponses 481 Call/Transaction Does Not Exist reçues
`core_rcv_replies_482`	Nombre de réponses 482 Loop Detected reçues
`core_rcv_replies_483`	Nombre de réponses 483 Too Many Hops reçues
`core_rcv_replies_484`	Nombre de réponses 484 Address Incomplete reçues
`core_rcv_replies_485`	Nombre de réponses 485 Ambiguous reçues
`core_rcv_replies_486`	Nombre de réponses 486 Busy Here reçues
`core_rcv_replies_487`	Nombre de réponses 487 Request Terminated reçues
`core_rcv_replies_488`	Nombre de réponses 488 Not Acceptable Here reçues
`core_rcv_replies_489`	Nombre de réponses 489 Bad Event reçues
`core_rcv_replies_491`	Nombre de réponses 491 Request Pending reçues
`core_rcv_replies_493`	Nombre de réponses 493 Undecipherable reçues

Statistiques de transfert et d'erreur

Nom de la métrique	Signification
`core_fwd_replies`	Nombre de réponses SIP transférées
`core_fwd_requests`	Nombre de requêtes SIP transférées
`core_drop_replies`	Nombre de réponses SIP abandonnées
`core_drop_requests`	Nombre de requêtes SIP abandonnées
`core_err_replies`	Nombre de réponses d'erreur
`core_err_requests`	Nombre de requêtes d'erreur
`core_bad_URIs_rcvd`	Nombre de messages avec des URI malformées reçues
`core_bad_msg_hdr`	Nombre de messages avec des en-têtes incorrects/malformés
`core_unsupported_methods`	Nombre de requêtes avec des méthodes SIP non prises en charge

Suivi des dialogues

Nom de la métrique	Signification
`dialog_ng_active`	Nombre de dialogues actuellement actifs (répondu/confirmé)
`dialog_ng_early`	Nombre de dialogues précoces (sonnant/état provisoire)
`dialog_ng_expired`	Nombre de dialogues qui ont expiré ou ont été terminés de force
`dialog_ng_processed`	Nombre total de dialogues traités depuis le démarrage

Statistiques DNS

Nom de la métrique	Signification
`dns_failed_dns_request`	Nombre de requêtes DNS échouées
`dns_slow_dns_request`	Nombre de requêtes DNS lentes (dépassant le seuil)

P-CSCF IPSec IMS

Nom de la métrique	Signification
`ims_ipsec_pcscf_spi_free`	Nombre de valeurs SPI (Security Parameter Index) libres disponibles pour allocation
`ims_ipsec_pcscf_spi_total`	Capacité totale SPI configurée pour le système
`ims_ipsec_pcscf_spi_used`	Nombre de valeurs SPI actuellement allouées/utilisées
`ims_ipsec_pcscf_spi_utilization_pct`	Pourcentage d'utilisation du pool SPI
`ims_ipsec_pcscf_worker_cache_size`	Taille du cache IPSec du processus de travail

QoS IMS (Interface Rx)

Métriques d'enregistrement AAR

Nom de la métrique	Signification
`ims_qos_active_registration_rx_sessions`	Nombre de sessions d'enregistrement Rx actuellement actives
`ims_qos_registration_aars`	Nombre total de messages AAR (Authorization-Authentication Request) d'enregistrement envoyés
`ims_qos_successful_registration_aars`	Nombre de transactions AAR d'enregistrement réussies
`ims_qos_failed_registration_aars`	Nombre de transactions AAR d'enregistrement échouées
`ims_qos_registration_aar_avg_response_time`	Temps de réponse moyen pour les messages AAR d'enregistrement en millisecondes
`ims_qos_registration_aar_response_time`	Temps total de réponse pour tous les messages AAR d'enregistrement en millisecondes
`ims_qos_registration_aar_replies_received`	Nombre total de réponses AAR d'enregistrement reçues

Nom de la métrique	Signification
`ims_qos_registration_aar_timeouts`	Nombre de délais d'attente de requêtes AAR d'enregistrement

Métriques AAR de média

Nom de la métrique	Signification
`ims_qos_active_media_rx_sessions`	Nombre de sessions Rx de média actuellement actives
`ims_qos_media_rx_sessions`	Nombre total de sessions Rx de média créées
`ims_qos_media_aars`	Nombre total de messages AAR de média envoyés
`ims_qos_successful_media_aars`	Nombre de transactions AAR de média réussies
`ims_qos_failed_media_aars`	Nombre de transactions AAR de média échouées
`ims_qos_media_aar_avg_response_time`	Temps de réponse moyen pour les messages AAR de média en millisecondes
`ims_qos_media_aar_response_time`	Temps total de réponse pour tous les messages AAR de média en millisecondes
`ims_qos_media_aar_replies_received`	Nombre total de réponses AAR de média reçues
`ims_qos_media_aar_timeouts`	Nombre de délais d'attente de requêtes AAR de média

Métriques ASR

Nom de la métrique	Signification
`ims_qos_asrs`	Nombre total de messages ASR (Abort-Session-Request) reçus du PCRF

Localisation d'utilisateur P-CSCF

Nom de la métrique	Signification
`ims_usrloc_pcscf_expired_contacts`	Nombre de liaisons de contact expirées
`ims_usrloc_pcscf_registered_contacts`	Nombre de liaisons de contact actuellement enregistrées
`ims_usrloc_pcscf_registered_impus`	Nombre d'IMPUs (Identités Publiques IMS) actuellement enregistrées

Base de données MySQL

Nom de la métrique	Signification
`mysql_driver_errors`	Nombre d'erreurs de pilote/connexion MySQL

Anti-Flood (Blocage IP)

Nom de la métrique	Signification
`pike_blocked_ips`	Nombre d'adresses IP actuellement bloquées (détection de flood)

Module Registrar

Nom de la métrique	Signification
`registrar_accepted_regs`	Nombre de requêtes REGISTER acceptées (module registrar hérité)
`registrar_rejected_regs`	Nombre de requêtes REGISTER rejetées (module registrar hérité)
`registrar_default_expire`	Temps d'expiration par défaut pour les enregistrements en secondes
`registrar_default_expires_range`	Paramètre de plage d'expiration par défaut
`registrar_expires_range`	Plage d'expiration configurée
`registrar_max_contacts`	Nombre maximum de contacts autorisés par AOR
`registrar_max_expires`	Temps d'expiration maximum autorisé en secondes

Statistiques de script

Nom de la métrique	Signification
`script_register_failed`	Nombre de tentatives d'enregistrement échouées dans la logique de script de routage
`script_register_success`	Nombre d'enregistrements réussis traités par le script de routage
`script_register_time`	Temps total passé à traiter les enregistrements dans le script de routage (millisecondes)

Transport SCTP

Nom de la métrique	Signification
`sctp_assoc_shutdown`	Nombre d'arrêts d'association SCTP initiés localement
`sctp_comm_lost`	Nombre d'associations SCTP perdues en raison d'une défaillance de communication
`sctp_connect_failed`	Nombre de tentatives d'association SCTP sortantes échouées
`sctp_current_opened_connections`	Nombre d'associations SCTP actuellement ouvertes
`sctp_current_tracked_connections`	Nombre d'associations SCTP actuellement suivies
`sctp_established`	Nombre total d'associations SCTP établies
`sctp_local_reject`	Nombre d'associations SCTP entrantes rejetées localement
`sctp_remote_shutdown`	Nombre d'arrêts d'association SCTP initiés par le pair
`sctp_send_failed`	Nombre d'opérations d'envoi SCTP échouées
`sctp_send_force_retry`	Nombre de nouvelles tentatives forcées sur des envois SCTP échoués

Nom de la métrique	Signification
`sctp_sendq_full`	Nombre de tentatives d'envoi échouées en raison d'une file d'attente d'envoi pleine

Mémoire partagée

Nom de la métrique	Signification
`shmem_fragments`	Nombre de fragments dans le pool de mémoire partagée (indique la fragmentation)
`shmem_free_size`	Montant de mémoire partagée libre en octets
`shmem_max_used_size`	Taille maximale de mémoire partagée utilisée depuis le démarrage en octets
`shmem_real_used_size`	Taille réelle de la mémoire partagée utilisée, y compris la surcharge de l'allocateur en octets
`shmem_total_size`	Taille totale du pool de mémoire partagée en octets
`shmem_used_size`	Mémoire partagée actuellement utilisée (données utilisateur uniquement) en octets

Module SL (Sans état)

Compteurs de réponses sans état par classe

Nom de la métrique	Signification
`sl_1xx_replies`	Nombre de réponses sans état 1xx envoyées
`sl_2xx_replies`	Nombre de réponses sans état 2xx envoyées
`sl_3xx_replies`	Nombre de réponses sans état 3xx envoyées
`sl_4xx_replies`	Nombre de réponses sans état 4xx envoyées
`sl_5xx_replies`	Nombre de réponses sans état 5xx envoyées
`sl_6xx_replies`	Nombre de réponses sans état 6xx envoyées
`sl_xxx_replies`	Nombre d'autres réponses sans état envoyées

Compteurs de réponses sans état spécifiques

Nom de la métrique	Signification
`sl_200_replies`	Nombre de réponses sans état 200 OK envoyées
`sl_202_replies`	Nombre de réponses sans état 202 Accepted envoyées
`sl_300_replies`	Nombre de réponses sans état 300 Multiple Choices envoyées
`sl_301_replies`	Nombre de réponses sans état 301 Moved Permanently envoyées
`sl_302_replies`	Nombre de réponses sans état 302 Moved Temporarily envoyées
`sl_400_replies`	Nombre de réponses sans état 400 Bad Request envoyées
`sl_401_replies`	Nombre de réponses sans état 401 Unauthorized envoyées
`sl_403_replies`	Nombre de réponses sans état 403 Forbidden envoyées
`sl_404_replies`	Nombre de réponses sans état 404 Not Found envoyées
`sl_407_replies`	Nombre de réponses sans état 407 Proxy Authentication Required envoyées
`sl_408_replies`	Nombre de réponses sans état 408 Request Timeout envoyées
`sl_483_replies`	Nombre de réponses sans état 483 Too Many Hops envoyées

Nom de la métrique	Signification
`sl_500_replies`	Nombre de réponses sans état 500 Server Internal Error envoyées

Statistiques générales sans état

Nom de la métrique	Signification
`sl_sent_replies`	Nombre total de réponses sans état envoyées
`sl_sent_err_replies`	Nombre de réponses d'erreur sans état envoyées
`sl_received_ACKs`	Nombre de messages ACK reçus pour des transactions sans état
`sl_failures`	Nombre d'échecs d'envoi de réponses sans état

Transport TCP

Nom de la métrique	Signification
`tcp_con_reset`	Nombre de connexions TCP réinitialisées (RST reçu sur une connexion établie)
`tcp_con_timeout`	Nombre de connexions TCP fermées en raison d'un délai d'attente d'inactivité
`tcp_connect_failed`	Nombre de tentatives de connexion TCP sortantes échouées
`tcp_connect_success`	Nombre de connexions TCP sortantes réussies
`tcp_current_opened_connections`	Nombre de connexions TCP actuellement ouvertes
`tcp_current_write_queue_size`	Taille totale actuelle des files d'écriture TCP sur toutes les connexions
`tcp_established`	Nombre total de connexions TCP établies (entrantes et sortantes)
`tcp_local_reject`	Nombre de connexions TCP entrantes rejetées localement
`tcp_passive_open`	Nombre de connexions TCP entrantes acceptées
`tcp_send_timeout`	Nombre d'opérations d'envoi TCP qui ont expiré (mode asynchrone)

Nom de la métrique	Signification
`tcp_sendq_full`	Nombre de tentatives d'envoi échouées parce que la file d'attente d'envoi était pleine

Module TM/TMX (Transaction)

Compteurs de types de transaction

Nom de la métrique	Signification
`tmx_UAC_transactions`	Nombre de transactions UAC (client) créées
`tmx_UAS_transactions`	Nombre de transactions UAS (serveur) créées
`tmx_active_transactions`	Nombre de transactions actuellement actives
`tmx_inuse_transactions`	Nombre de transactions actuellement en cours d'utilisation

Achèvement de transaction par statut

Nom de la métrique	Signification
`tmx_2xx_transactions`	Nombre de transactions complétées avec une réponse 2xx
`tmx_3xx_transactions`	Nombre de transactions complétées avec une réponse 3xx
`tmx_4xx_transactions`	Nombre de transactions complétées avec une réponse 4xx
`tmx_5xx_transactions`	Nombre de transactions complétées avec une réponse 5xx
`tmx_6xx_transactions`	Nombre de transactions complétées avec une réponse 6xx

Statistiques de réponse de transaction

Nom de la métrique	Signification
`tmx_rpl_absorbed`	Nombre de réponses absorbées par la couche de transaction (doublons)
`tmx_rpl_generated`	Nombre de réponses générées localement par le module de transaction
`tmx_rpl_received`	Nombre de réponses reçues pour des transactions
`tmx_rpl_relayed`	Nombre de réponses relayées par le module de transaction
`tmx_rpl_sent`	Nombre de réponses envoyées par le module de transaction

Localisation d'utilisateur

Nom de la métrique	Signification
`usrloc_location_contacts`	Nombre de contacts dans le domaine 'location' (module usrloc standard)
`usrloc_location_expires`	Nombre de contacts expirés dans le domaine 'location'
`usrloc_registered_users`	Nombre d'utilisateurs/AORs (Address of Records) enregistrés

---

Métriques I-CSCF

L'I-CSCF partage la plupart des statistiques SIP de base avec le P-CSCF. Voir la section Statistiques SIP de base P-CSCF ci-dessus. Les métriques ci-dessous sont spécifiques à l'I-CSCF.

Contexte opérationnel I-CSCF

L'I-CSCF maintient une liste d'instances S-CSCF disponibles pour l'équilibrage de charge. Pour un nouvel enregistrement, l'I-CSCF interroge le HSS pour sélectionner l'instance S-CSCF correcte. Les métriques UAR et LIR ci-dessous suivent le succès de ces opérations.

IMS I-CSCF (Interface Cx - Communication HSS)

L'I-CSCF utilise l'interface Diameter Cx pour communiquer avec le HSS (Home Subscriber Server). Il envoie des requêtes de localisation d'utilisateur et d'autorisation.

Métriques UAR (User-Authorization-Request)

Nom de la métrique	Signification
`ims_icscf_uar_avg_response_time`	Temps de réponse moyen pour les messages UAR en millisecondes (calculé comme uar_replies_response_time / uar_replies_received)
`ims_icscf_uar_replies_received`	Nombre total de réponses UAA (User-Authorization-Answer) reçues du HSS
`ims_icscf_uar_replies_response_time`	Temps total de réponse pour tous les messages UAR en millisecondes
`ims_icscf_uar_timeouts`	Nombre de délais d'attente de requêtes UAR

Métriques LIR (Location-Info-Request)

Nom de la métrique	Signification
`ims_icscf_lir_avg_response_time`	Temps de réponse moyen pour les messages LIR en millisecondes (calculé comme lir_replies_response_time / lir_replies_received)
`ims_icscf_lir_replies_received`	Nombre total de réponses LIA (Location-Info-Answer) reçues du HSS
`ims_icscf_lir_replies_response_time`	Temps total de réponse pour tous les messages LIR en millisecondes
`ims_icscf_lir_timeouts`	Nombre de délais d'attente de requêtes LIR

Métriques communes

L'I-CSCF exporte également les métriques communes ci-dessous. La section P-CSCF ci-dessus documente ces métriques.

- **Métriques CDP (Diameter)** - Statistiques du protocole Diameter
- **Statistiques SIP de base** - Compteurs de requêtes/réponses par méthode et code d'état
- **Statistiques DNS** - Métriques de requêtes DNS
- **Base de données MySQL** - Erreurs de connexion à la base de données
- **Anti-Flood** - Statistiques de blocage IP
- **Mémoire partagée** - Statistiques d'utilisation de la mémoire
- **Module SL (Sans état)** - Compteurs de réponses sans état
- **Transport TCP** - Statistiques de connexion TCP
- **Module TM/TMX (Transaction)** - Suivi de l'état des transactions

---

Métriques S-CSCF

Le S-CSCF partage la plupart des statistiques SIP de base avec le P-CSCF et l'I-CSCF. Voir la section Statistiques SIP de base P-CSCF ci-dessus. Les métriques ci-dessous sont spécifiques au S-CSCF.

Contexte opérationnel S-CSCF

Le S-CSCF fournit des informations détaillées sur la localisation des utilisateurs. Il gère également les IFC (Critères de Filtrage Initiaux).

Une recherche de localisation d'utilisateur montre les IMPUs enregistrés avec des liaisons de contact et des profils de service. Les métriques `ims_usrloc_scscf_active_contacts` et `ims_usrloc_scscf_active_impus` suivent le nombre de contacts et d'IMPUs actifs.

L'IFC (Critères de Filtrage Initiaux) détermine quels serveurs d'application traitent les sessions SIP. Les performances d'évaluation de l'IFC peuvent changer les temps de mise en place des appels. Les métriques de transaction (`tmx_*`) suivent ces temps.

IMS ISC (Contrôle de Service IMS)

Le module IMS ISC évalue les Critères de Filtrage Initiaux (iFC). Il détermine quels serveurs d'application doivent traiter les sessions SIP. Ces métriques suivent la performance et l'effet des opérations de correspondance d'iFC.

Nom de la métrique	Signification
`ims_isc_ifc_match_attempts`	Nombre total de tentatives de correspondance d'iFC effectuées
`ims_isc_ifc_match_time_total`	Temps cumulé passé à effectuer des opérations de correspondance d'iFC en millisecondes
`ims_isc_ifc_nomatch_count`	Nombre de tentatives de correspondance d'iFC où aucun critère de déclenchement n'a correspondu

Surveillance de la performance : Calculez le temps moyen de correspondance d'iFC comme `ifc_match_time_total / ifc_match_attempts`. Un temps moyen élevé peut montrer des critères de filtrage complexes. Cela peut également montrer une limite de performance dans la sélection des serveurs d'application. Un ratio élevé de `ifc_nomatch_count` par rapport à `ifc_match_attempts` peut montrer des points de déclenchement incorrects. Cela peut également montrer des modèles de trafic inattendus.

Authentification IMS (Interface Cx - MAR)

Le S-CSCF utilise l'interface Diameter Cx pour authentifier les utilisateurs avec le HSS. Il envoie un MAR (Multimedia-Auth-Request).

Nom de la métrique	Signification
`ims_auth_mar_avg_response_time`	Temps de réponse moyen pour les messages MAR en millisecondes (calculé comme mar_replies_response_time / mar_replies_received)
`ims_auth_mar_replies_received`	Nombre total de réponses MAA (Multimedia-Auth-Answer) reçues du HSS
`ims_auth_mar_replies_response_time`	Temps total de réponse pour tous les messages MAR en millisecondes
`ims_auth_mar_timeouts`	Nombre de délais d'attente de requêtes MAR

IMS Registrar S-CSCF

Statistiques d'enregistrement

Nom de la métrique	Signification
`ims_registrar_scscf_accepted_regs`	Nombre de requêtes REGISTER acceptées avec succès
`ims_registrar_scscf_rejected_regs`	Nombre de requêtes REGISTER rejetées
`ims_registrar_scscf_default_expire`	Temps d'expiration par défaut pour les enregistrements en secondes
`ims_registrar_scscf_default_expires_range`	Configuration de la plage d'expiration par défaut
`ims_registrar_scscf_max_contacts`	Nombre maximum de contacts autorisés par enregistrement
`ims_registrar_scscf_max_expires`	Temps d'expiration maximum autorisé en secondes
`ims_registrar_scscf_notifies_in_q`	Nombre de messages NOTIFY en attente dans la file d'attente

Métriques SAR (Server-Assignment-Request)

Nom de la métrique	Signification
`ims_registrar_scscf_sar_avg_response_time`	Temps de réponse moye pour les messages SAR en millisecondes (calcu comme sar_replies_response_ti / sar_replies_received)
`ims_registrar_scscf_sar_replies_received`	Nombre total de répons SAA (Server-Assignmen Answer) reçues du HSS
`ims_registrar_scscf_sar_replies_response_time`	Temps total de réponse pour tous les messages SAR en millisecondes
`ims_registrar_scscf_sar_timeouts`	Nombre de délais d'attente de requêtes SAR

Localisation d'utilisateur S-CSCF

Nom de la métrique	Signification
`ims_usrloc_scscf_active_contacts`	Nombre de liaisons de contact enregistrées actuellement actives
`ims_usrloc_scscf_active_impus`	Nombre d'IMPUs (Identités Publiques IMS) enregistrées actuellement actives
`ims_usrloc_scscf_active_subscriptions`	Nombre d'abonnements actuellement actifs
`ims_usrloc_scscf_contact_collisions`	Nombre de collisions de hachage dans la table de hachage des contacts
`ims_usrloc_scscf_impu_collisions`	Nombre de collisions de hachage dans la table de hachage des IMPU
`ims_usrloc_scscf_subscription_collisions`	Nombre de collisions de hachage dans la table de hachage des abonnements

Suivi des dialogues

Le S-CSCF suit l'état du dialogue pour les appels actifs :

Nom de la métrique	Signification
`dialog_ng_active`	Nombre de dialogues actuellement actifs (répondu/confirmé)
`dialog_ng_early`	Nombre de dialogues précoces (sonnant/état provisoire)
`dialog_ng_expired`	Nombre de dialogues qui ont expiré ou ont été terminés de force
`dialog_ng_processed`	Nombre total de dialogues traités depuis le démarrage

Métriques communes

Le S-CSCF exporte également les métriques communes ci-dessous. La section P-CSCF ci-dessus documente ces métriques.

- **Métriques CDP (Diameter)** - Statistiques du protocole Diameter
- **Statistiques SIP de base** - Compteurs de requêtes/réponses par méthode et code d'état (remarque : le S-CSCF achemine entre les points de terminaison. Il a généralement plus de fwd_requests et fwd_replies.)
- **Statistiques DNS** - Métriques de requêtes DNS
- **Base de données MySQL** - Erreurs de connexion à la base de données
- **Anti-Flood** - Statistiques de blocage IP
- **Mémoire partagée** - Statistiques d'utilisation de la mémoire
- **Module SL (Sans état)** - Compteurs de réponses sans état
- **Transport TCP** - Statistiques de connexion TCP
- **Module TM/TMX (Transaction)** - Suivi de l'état des transactions (remarque : le S-CSCF agit à la fois comme client et serveur. Il a généralement à la fois des transactions UAC et UAS.)