

Université Versailles Saint-Quentin-en-Yvelines

Réseaux d'opérateurs

M2 IRS

Access and Mobility Management Function (AMF)

Réalisé par les étudiants :

- CHADOULI
- TIROUGNANASSAMMANDAM
- GUICHARD
- LAOUAR

2024/2025

Table des matières

1. Introduction	3
2. Le réseau 5G	4
2. 1. Cas d'utilisation de la 5G	5
2. 1. 1. Enhanced mobile broadband	5
2. 1. 2. Ultra-Reliable Low Latency Communication (uRLLC)	5
2. 1. 3. Massive Internet of Things (mIoT)	5
2. 2. Technologies habilitantes de la 5G	5
2. 2. 1. Software Defined Networking (SDN)	5
2. 2. 2. Network Functions Virtualization (NFV)	5
2. 3. L'architecture de la 5G	5
2. 3. 1. Perspective des composants	6
2. 3. 2. La perspective du flux de données	6
2. 4. Fonctions du cœur du réseau 5G	6
3. Access and Mobility Management Function (AMF) dans la 5G	8
3. 1. Comparaison entre l'AMF et le MME	8

3. 2. Fonctionnalités principales de l'AMF	9
3. 3. Interactions des interfaces AMF	10
3. 3. Comment sélectionner un AMF ?.....	11
3. 4. Procédure d'Enregistrement d'un Terminal dans un Réseau 5G	13
3. 5. Établissement de la Session PDU (Protocol Data Unit)	15
4. Les Services de l'AMF.....	15
4.1. Définition	15
4.2. Namf_Communication.....	16
4.2.1. Définition	16
4.2.2. Les opérations de service	16
4.3. Namf_EventExposure Service	26
4.3.1. Définition	26
4.3.2. Les opérations de service	26
4.4. Namf_MT Service	28
4.4.1. Définition	28
4.4.2. Les opérations de service	28
4.5. Namf_Location Service	30
4.5.1. Définition	30
4.5.2. Les opérations de service	30
5. APIs de l'AMF	34
5. 1. Format général des routes	34
5. 2. API du service Namf_Communication.....	35
5. 2. 1. Individual ueContext.....	36
5. 2. 2. N1N2 Subscriptions Collection for Individual UE Contexts	37
5. 2. 3. N1N2 Individual Subscription	37
5. 2. 4. N1N2 Messages Collection	37
5. 2. 5. Subscriptions collection	37
5. 2. 6. individual subscription.....	37
5. 2. 7. Non UE N2 Messages Collection.....	37
5. 3. API du service Namf_EventExposure.....	37
5. 3. 1. Subscriptions collection	38
5. 3. 2. Individual subscription	38

5. 4. API du service Namf_MT	38
5. 4. 1. ueReachInd	39
5. 4. 2. ueContext.....	39
5. 5. API du service Namf_Location.....	39
5. 5. 1 Individual UE context	40
6. Les interactions entre AMF et NF.....	40
6.1 AMF et AUSF (Authentication Server Function)	41
6.2 AMF et UDM (Unified Data Management)	42
6.3 AMF et NSSF (Network Slice Selection Function)	43
6.4 AMF et SMF (Session Management Function)	45
6.5 AMF et PCF (Policy Control Function)	47
6.6 AMF et NRF (Network Repository Function)	48
6.7 AMF et NEF (Network Exposure Function)	50
7. Etude de marché	50
7.1 Le marché en général de la 5G	50
7.2 Les acteurs du marché de la 5G	51
8. Conclusion	52
9. Bibliographie	53

1. Introduction

La 5G, ou nouvelle génération de réseaux mobiles, est en train d’être adoptée à grande échelle dans le monde entier. Depuis son introduction sur le marché en 2020, 1,7 milliard d'appareils dans le monde utilisent le réseau 5G. Ce chiffre devrait atteindre environ 5 milliards d'ici 2028.

La 5G apporte des améliorations significatives par rapport à ses prédécesseurs, promettant un monde entièrement connecté et offrant une variété de nouveaux services et cas d'utilisation qui révolutionneront notre vie de tous les jours tels que la technologie des véhicules autonomes et la chirurgie à distance.

Au cœur de cette infrastructure complexe se trouve le réseau cœur 5G, qui est composé de plusieurs fonctions réseau, dont l'une des plus importantes, la fonction

AMF ou Access and Mobility Management Function. Cette fonction joue un rôle crucial dans la gestion des connexions des utilisateurs, assurant l'enregistrement, l'authentification, et le suivi des équipements utilisateur connectés au réseau.

Dans ce rapport, nous exposons tout d'abord la 5G, puis nous explorons en détail le rôle et les responsabilités de la fonction AMF, ses différents services, APIs et interactions avec les autres fonctions réseau.

2. Le réseau 5G

La 5G débarque avec des exigences strictes en latence et en bande passante, promettant d'ambitieux cas d'utilisation.

2. 1. Cas d'utilisation de la 5G

2. 1. 1. Enhanced mobile broadband

Concerne les applications où une connexion rapide est cruciale pour des performances optimales telles que le streaming, et les procédures médicales de précision comme la chirurgie.

2. 1. 2. Ultra-Reliable Low Latency Communication (uRLLC)

Pour les applications nécessitant une communication quasi-instantanée, telles que les véhicules autonomes.

2. 1. 3. Massive Internet of Things (mIoT)

La 5G permettra une connectivité transparente pour un grand nombre de capteurs intégrés comme les bracelets de fitness connectés et les appareils de domotique.

2. 2. Technologies habilitantes de la 5G

Pour répondre aux exigences strictes de la 5G, des technologies telles que le Software Defined Networking (SDN) et la Network Function Virtualization (NFV) ont été définies comme des technologies clés pour la 5G.

2. 2. 1. Software Defined Networking (SDN)

Le réseau défini par logiciel (SDN) sépare les plans de contrôle et de données au sein d'un réseau, ce qui simplifie la gestion, améliore la programabilité et facilite la mise à niveau des services. Il centralise les fonctions du plan de contrôle, ce qui permet une modification et une mise à niveau aisées à partir d'un contrôleur centralisé.

2. 2. 2. Network Functions Virtualization (NFV)

La virtualisation des fonctions de réseau (NFV) élimine le matériel spécialisé pour les services de réseau, ce qui améliore l'évolutivité et la souplesse. L'architecture de l'ETSI garantit la stabilité et l'interopérabilité de l'ensemble du système.

2. 3. L'architecture de la 5G

L'architecture du réseau 5G peut être envisagée sous deux angles différents :

2. 3. 1. Perspective des composants

L'architecture générale des réseaux mobiles ne change pas beaucoup d'une génération à une autre. Elle contient toujours les mêmes éléments : le réseau cœur, le réseau d'accès radio et l'équipement de l'utilisateur.

- **Réseaux cœur** : Responsable de la gestion des fonctionnalités du réseau telles que l'accès, l'authentification, la sécurité et la mobilité. Il supervise la qualité de service (QoS) et assure une interopérabilité transparente avec d'autres réseaux, il joue un rôle crucial pour le fonctionnement du réseau et l'expérience de l'utilisateur.
- **Le réseau d'accès radio** : Le réseau d'accès radio est la partie du réseau responsable de l'établissement des connexions sans fil entre l'équipement de l'utilisateur et le réseau central. Cette liaison sans fil est faite via des antennes appelées stations de base (BS).
- **Équipement de l'utilisateur** : Il s'agit de l'appareil mobile de l'utilisateur.

2. 3. 2. La perspective du flux de données

L'architecture est divisée en deux plans : le plan de contrôle, qui contient les fonctions administratives du réseau telles que l'authentification de l'utilisateur, et le plan utilisateur, qui comprend des composants tels que l'équipement de l'utilisateur, le RAN et l'UPF.

La communication entre le plan de contrôle et le plan utilisateur se fait par l'intermédiaire d'interfaces de point de référence, telles que N4 pour la communication UPF et SMF, et N9 pour les UPF dans une configuration Uplink Classifier.

2. 4. Fonctions du cœur du réseau 5G

Le cœur du réseau 5G est composé de plusieurs fonctions. Les plus importantes sont :

- **AMF (Access and Mobility management Function)** : Responsable de l'enregistrement, de l'authentification et du suivi de l'utilisateur. Un utilisateur ne peut être connecté qu'à une seule AMF à la fois.
- **AUSF (Authentication Server Function)** : Le processus d'authentification implique que l'AMF initie une demande d'authentification à l'AUSF, qui génère un défi (challenge) généralement sous forme de puzzle cryptographique pour l'équipement utilisateur (UE). L'UE répond avec des informations d'authentification, vérifiées par l'AUSF. En cas de succès, l'AUSF récupère les données spécifiques à l'utilisateur depuis l'UDM. Ces données permettent à

l'AMF de créer les contextes de session et les associations de sécurité pour l'UE, facilitant une communication sécurisée dans le réseau 5G.

- **PCF (Policy Charging Function)** : Responsable des décisions dynamiques de politique basées sur la congestion du réseau et la géolocalisation. Il peut limiter ou refuser certains services et décider également de la tarification d'un flux.
- **SMF (Session Management Function)** : Établit et gère les sessions PDU entre l'UE et l'UPF en appliquant les politiques de QoS définies par le PCF. Il est également responsable de l'attribution des adresses IP et de la sélection et gestion des UPF pour chaque PDU session PDU-UE.
- **UDM (Unified Data Management)** : Base de données centralisée et unifiée pour toutes les informations et autorisations des abonnés 5G, elle peut utiliser une base de données externe comme UDR (Dépôt unifié de données). Elle détient les clés secrètes et suit à quel AMF chaque UE est connecté.
- **AF (Application Function)** : Serveur externe qui communique avec le PCF pour demander un nouveau flux de paquets, par exemple un nœud IMS (Sous-système Multimédia IP) demandant un appel vocal. Il communique avec le PCF pour demander un nouveau flux de données en fonction des exigences de l'application.
- **NRF (Network Repository Function)** : Responsable du maintien de la liste des Fonctions Réseau et agit comme un référentiel (base de données) permettant aux fonctions de se découvrir et de communiquer entre elles, comme un DNS.
- **NSSF (Network Slice Selection Function)** : Responsable de la sélection de la tranche réseau (slice) appropriée pour un utilisateur ou une application spécifique en fonction des exigences et des règles de politique définies.
- **NEF (Network Exposure Function)** : Responsable de l'authentification et de l'autorisation des applications tierces (AF) et agit comme intermédiaire entre elles et le réseau 5G.
- **UPF (User Plane Function)** : Elle gère le transfert des paquets du plan de données entre le Réseau d'Accès Radio et le Réseau de Données, en assurant le contrôle d'accès, l'acheminement des paquets et la gestion de la QoS. Les UPF servent également de points d'ancrage pour la mobilité au sein des technologies d'accès radio et entre elles, en tant que point de session PDU externe pour se connecter au Réseau de Données (DN), et dans les cas complexes comme UPF intermédiaires (iUPFs) reliant les différents points. Les UPF s'appuient sur les

Fonctions de Gestion des Sessions (SMFs) dans le plan de contrôle pour établir les sessions PDU.

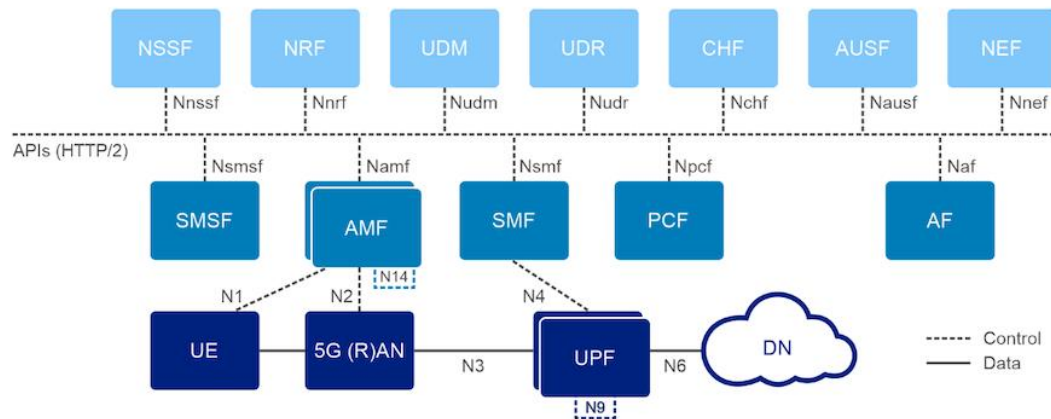


Figure 1 : Architecture du réseau 5G

3. Access and Mobility Management Function (AMF) dans la 5G

L'AMF (Access and Mobility Management Function) est un composant clé du cœur de réseau 5G, permet les échanges des messages NAS (Non-Access Stratum) entre l'UE (User Equipment) et le réseau pour la gestion de la mobilité et de l'accès. Les messages passent physiquement par le gNodeB, mais ne sont pas interprétés par celui-ci, ce qui permet un dialogue direct entre l'UE et l'AMF, selon le principe du NAS.

Plus précisément L'AMF gère les échanges de signalisation entre le terminal et lui-même pour l'enregistrement, la gestion de la mobilité lorsque l'UE se déplace, ainsi que la gestion des connexions. Elle s'occupe également de la joignabilité de l'UE, c'est-à-dire la capacité à envoyer des messages de paging à l'UE sur plusieurs cellules, comme en 4G. Les messages échangés entre l'UE et l'AMF sont chiffrés, et une gestion de l'intégrité est appliquée pour assurer la sécurité des signalisations.

L'AMF prend également en charge l'authentification des accès et la gestion des autorisations. Elle peut aussi servir de relais pour d'autres services, comme la géolocalisation, où les messages de localisation transitent par l'AMF. Enfin, l'AMF dispose de fonctions de notifications d'événements de mobilité de l'UE, qu'elle transmet à des prestataires externes ou des fournisseurs de services.

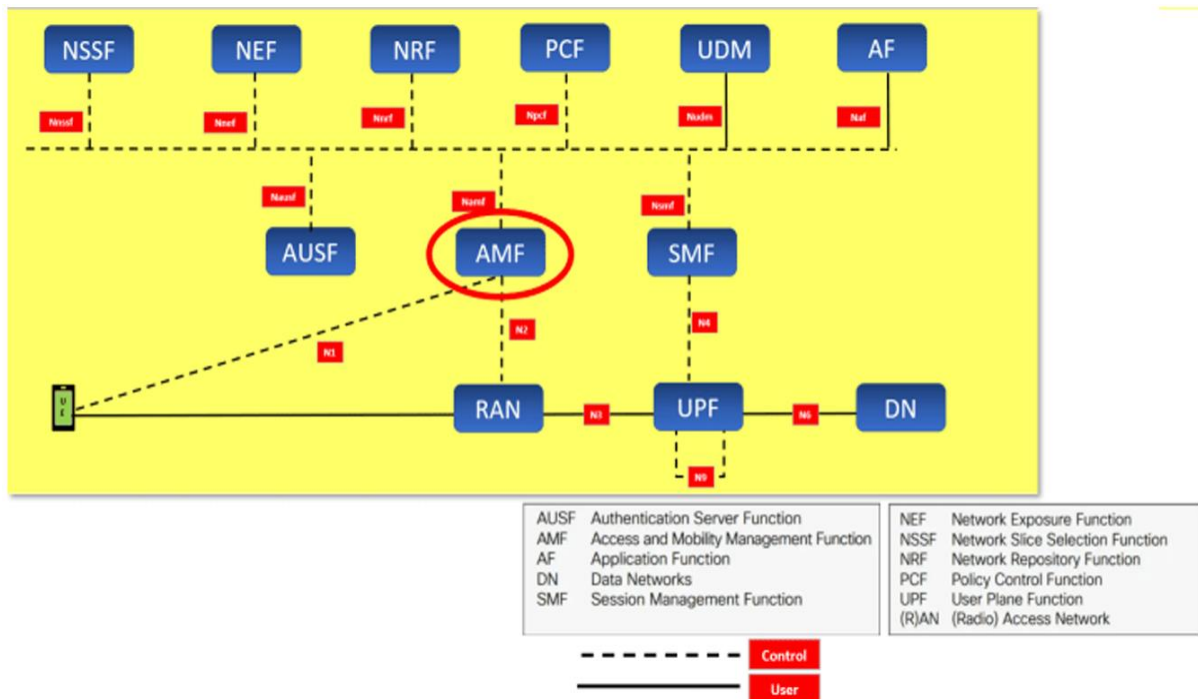


Figure 2 : L'AMF dans l'architecture du réseau 5G

3. 1. Comparaison entre l'AMF et le MME

L'AMF exécute la plupart des fonctions que le MME (Mobility Management Entity) réalise dans le réseau 4G, à l'exception de certaines d'entre elles.

L'établissement des sessions PDU est pris en charge par le **Session Management Function (SMF)**, tandis que l'authentification et la sécurité sont gérées par l'**Authentication Server Function (AUSF)** une autre fonction réseau dans la 5G. Cela montre que l'architecture 5G est plus distribuée que celle du MME en 4G, ce qui la rend plus efficace. Fondamentalement, le principe principal de l'architecture 5G est la séparation du plan de contrôle et du plan utilisateur.

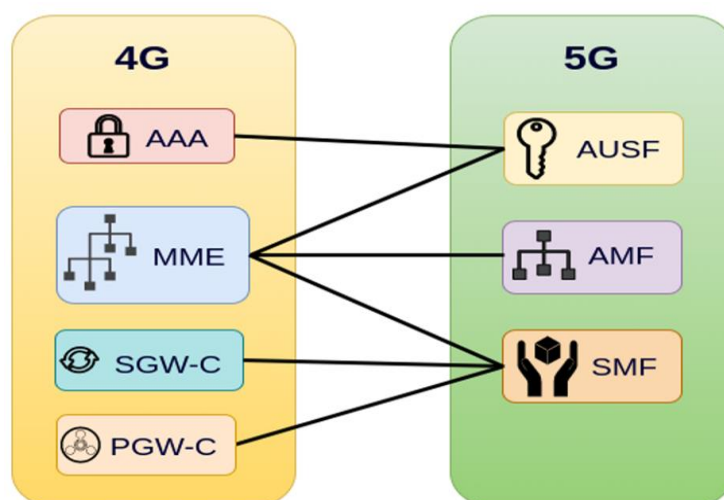


Figure 3 : Equivalence entre les composants de la 4G et 5G

3. 2. Fonctionnalités principales de l'AMF

1. Enregistrement des appareils : L'AMF est responsable de l'enregistrement des appareils 5G sur le réseau et de l'attribution d'identifiants uniques.
2. Gestion des accès : L'AMF gère les fonctions d'authentification, d'autorisation et de comptabilité (AAA), vérifiant l'identité des appareils et leur accès au réseau.
3. Gestion de la mobilité : L'AMF suit la localisation de l'UE et gère les handovers entre les cellules, maintenant la connectivité de l'UE pendant ses déplacements.
4. Exécution des politiques réseau : L'AMF applique les politiques réseau, telles que la Qualité de Service (QoS) et les politiques de tarification.
5. Gestion des sessions : L'AMF supervise l'établissement, la modification et la terminaison des sessions 5G en coordination avec le SMF.
6. Sélection de la UPF : L'AMF choisit l'UPF appropriée pour transmettre les données utilisateurs.
7. Gestion des données d'abonnés : Elle stocke et gère les données d'abonnement de l'utilisateur.
8. Gestion de la sécurité : L'AMF garantit la sécurité des appareils et du réseau.
9. Découpage réseau (Network Slicing) : L'AMF gère le découpage réseau, créant des segments virtuels avec des ressources dédiées.
10. Gestion des interfaces réseau : L'AMF communique avec d'autres fonctions réseau via plusieurs interfaces standardisées (N1, N2, N8, N11, N14, N15, N17, N22, N26).

3. 3. Interactions des interfaces AMF

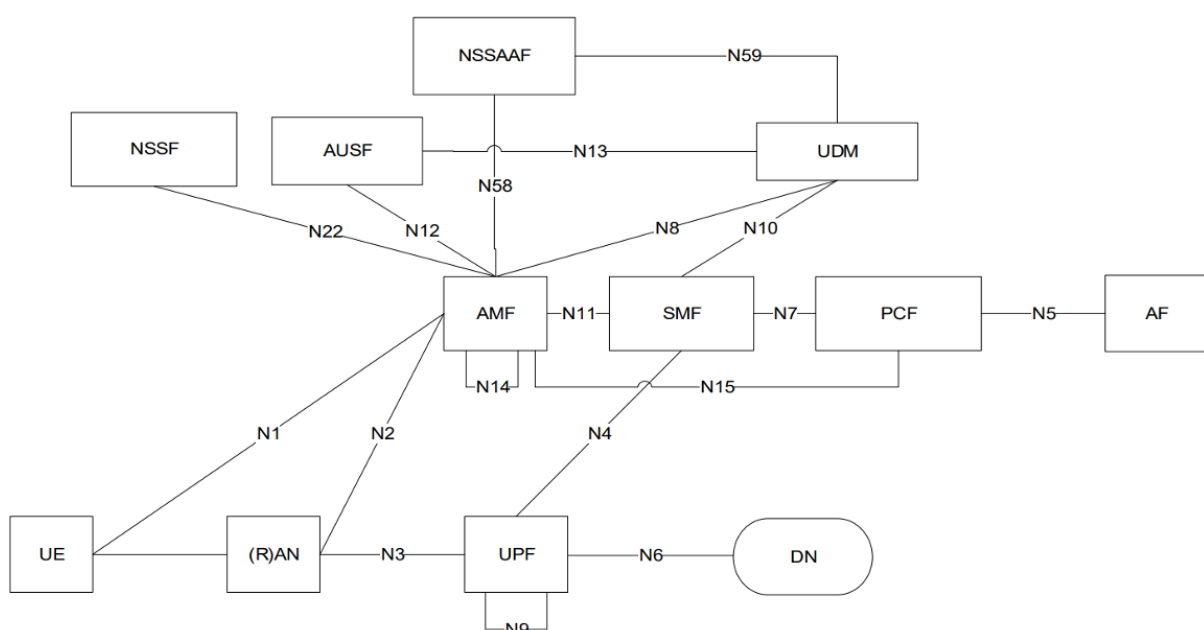


Figure 4 : Interactions des interfaces de L'AMF

- N1/N2 : Ces interfaces permettent à l'AMF de recevoir des informations sur les sessions et la connexion via le gNB.
- N8 : L'AMF interagit avec l'UDM pour récupérer les données d'abonnement des utilisateurs via cette interface.
- N11 : L'AMF interagit avec le SMF pour la gestion des sessions PDU, notamment pour ajouter, modifier ou supprimer des sessions.
- N14 : Cette interface est utilisée pour transmettre le contexte de l'UE entre deux AMFs durant les handovers, facilitant ainsi la continuité des services.
- N15 : Elle est utilisée pour la transmission et la suppression des politiques d'accès et de mobilité entre l'AMF et le Policy Control Function (PCF).
- N17 : L'AMF utilise cette interface pour émuler l'Equipment Identity Register (EIR), permettant des services d'identification d'équipement.
- N22 : L'AMF sélectionne les meilleures fonctions réseau (NF) avec l'aide de l'NSSF (Network Slice Selection Function), qui fournit la localisation des fonctions réseau à l'AMF.
- N26 : Cette interface est essentielle pour transférer le contexte d'authentification et de gestion de session de l'UE lorsque l'UE se déplace entre les systèmes 5GS et 4G-EPS.

3. 3. Comment sélectionner un AMF ?

Dans un réseau 5G, un **gNB** (gNodeB) peut être connecté à plusieurs **AMF** (Access and Mobility Management Functions). Le choix de l'AMF avec lequel le gNB va communiquer pour chaque flux de trafic dépend de plusieurs facteurs.

Sélection de l'AMF par le gNB :

Le gNB peut sélectionner l'AMF approprié en fonction de certains paramètres lorsqu'une UE (User Equipment) initie une connexion. Le processus suit généralement ce flux :

1. Identifiant AMF :

Le gNB reçoit une liste d'adresses AMF depuis le **Network Repository Function (NRF)**. Cette liste comprend des AMF capables de desservir l'UE en fonction de sa **zone de suivi** (Tracking Area) et des exigences du **slice réseau**.

2. Informations spécifiques à l'UE :

Le gNB peut également tenir compte des informations spécifiques à l'UE, comme les **NSSAI** (Network Slice Selection Assistance Information), le niveau de priorité, ainsi que la capacité de l'AMF à gérer certains types de services (par exemple, **IoT**, **URLLC** -

communications ultra-fiables à faible latence, ou **eMBB** - services de large bande mobile).

3. Équilibrage de charge :

Si plusieurs AMF peuvent servir l'UE, le gNB peut mettre en œuvre des techniques d'**équilibrage de charge**, en choisissant un AMF en fonction de la charge actuelle du réseau ou des politiques prédéfinies. Cependant, le gNB ne dispose pas forcément de toutes les informations détaillées sur la charge exacte appliquée à chaque AMF auquel il est connecté. Un mécanisme de signalisation permet à l'AMF de notifier au gNB, via un message **NGAP**, lorsqu'il est surchargé.

Sélection de l'AMF par l'UE :

Dans certains cas, l'UE peut participer à la sélection de l'AMF, notamment lors de l'enregistrement initial ou des **handover** (transferts). L'UE fournit alors des informations spécifiques au gNB, comme les **NSSAI** pris en charge et les préférences en matière de **PLMN** (Public Land Mobile Network).

Sélection d'un AMF assistée par le NRF :

1. Slicing réseau :

Le **NRF** aide à découvrir les AMF compatibles avec les **slices réseau** requis (en fonction des NSSAI). Par exemple, un UE nécessitant un slice pour l'URLLC sera dirigé vers un AMF prenant en charge ce service.

2. Pooling d'AMF :

Si plusieurs AMF sont disponibles dans un pool, le gNB et le NRF peuvent appliquer des politiques de répartition de charge pour garantir une utilisation efficace des ressources réseau.

Sélection dynamique d'AMF pour la mobilité :

Pour les sessions en cours, si l'UE se déplace entre différentes **zones de suivi**, le gNB peut décider de communiquer avec un nouvel AMF, déclenchant ainsi une **mise à jour de l'enregistrement de mobilité**. Le gNB peut procéder à une nouvelle sélection d'AMF en fonction de la nouvelle localisation de l'UE ou des conditions du réseau.

Redondance et basculement :

En cas de **défaillance** ou de **surcharge** d'un AMF, le gNB peut basculer vers un autre AMF pour assurer la continuité du service. Cela garantit une **haute disponibilité** et renforce la **robustesse** du réseau cœur 5G.

Procédure d'enregistrement (Network Registration)

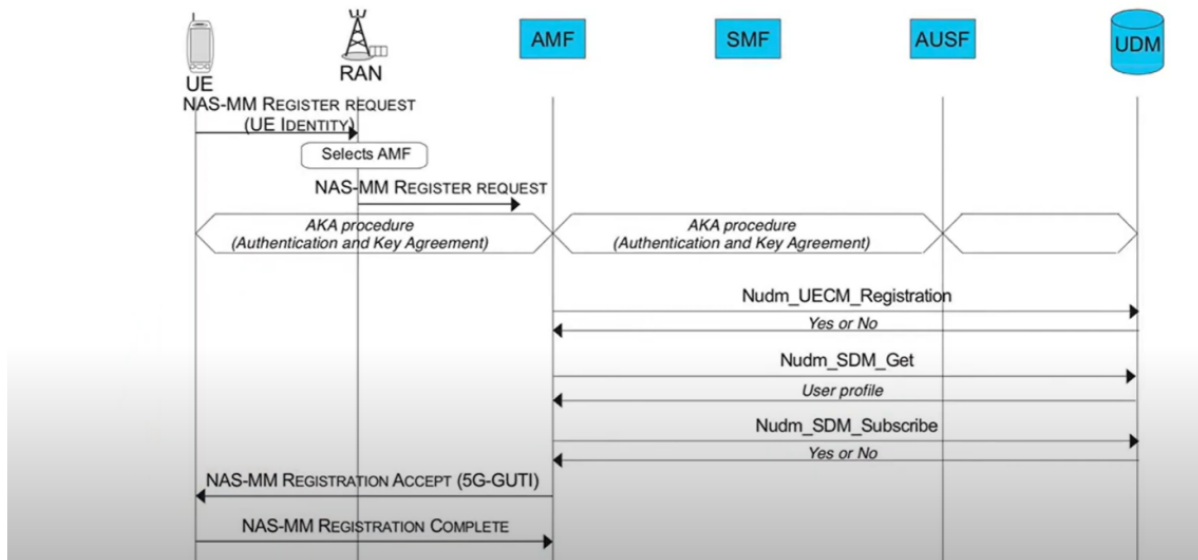


Figure 5 : Procédure d'enregistrement

3. 4. Procédure d'Enregistrement d'un Terminal dans un Réseau 5G

Lorsqu'un terminal 5G (User Equipment, UE) est allumé dans un réseau 5G, il doit d'abord s'enregistrer auprès du réseau pour pouvoir accéder aux services de données et de téléphonie. Cette procédure implique plusieurs composants du cœur du réseau, notamment l'AMF (Access and Mobility Management Function), qui joue un rôle central dans la gestion de la mobilité et l'enregistrement de l'UE. Voici un examen plus détaillé de ce processus :

1. **État Initial du Terminal (RM-Deregistered)** : Lorsque le terminal est allumé, il est dans un état appelé RM-Deregistered (Registration Management Deregistered). Cela signifie que le réseau ne le reconnaît pas encore, et qu'il n'a donc pas accès aux services du réseau.
2. **Envoi de la Demande d'Enregistrement** : Le terminal envoie un message de Network Registration sur la voie radio via la station de base gNB (gNodeB, équivalent 5G du eNodeB en 4G). Ce message inclut l'identité de l'UE, ce qui permet au réseau de l'identifier. Le gNB sélectionne un AMF pour traiter cette demande. Plusieurs AMF peuvent être disponibles, mais le gNB choisit celui qui est le mieux adapté en fonction des conditions du réseau.

3. **Transmission via NAS** : La demande d'enregistrement est transmise de manière transparente du gNB vers l'AMF en utilisant le protocole NAS (Non-Access Stratum). Le NAS est un
4. protocole de signalisation utilisé entre l'UE et les fonctions réseau, comme l'AMF, qui n'implique pas directement la couche d'accès radio.
5. **Authentication** : Procédure AKA, une fois que l'AMF reçoit la demande d'enregistrement, il lance la procédure AKA (Authentication and Key Agreement) pour vérifier l'identité de l'UE. Cette procédure fait intervenir plusieurs fonctions réseau :
 - a. **AUSF** (Authentication Server Function) : C'est la fonction responsable de l'authentification. Elle interagit avec l'AMF et l'UE pour générer et valider des clés de sécurité.
 - b. **UDM** (Unified Data Management) : Il contient le profil de l'abonné, y compris ses informations d'authentification et ses autorisations. Il joue un rôle clé dans la validation de l'authenticité du terminal.
6. **Vérification des Droits d'Enregistrement** : Après l'authentification, l'AMF vérifie auprès de l'UDM si l'abonné a le droit de s'enregistrer sur le réseau. L'UDM envoie une réponse positive ou négative. Si la réponse est positive, l'AMF procède aux étapes suivantes. La communication entre l'AMF et l'UDM se fait via l'interface SBI (Service-Based Interface), qui permet des échanges rapides et simples basés sur des requêtes-réponses.
7. **Récupération du Profil de l'Abonné**
Une fois l'enregistrement validé, l'AMF récupère le profil de l'abonné depuis l'UDM. Ce profil contient des informations critiques telles que :
 - a. Les droits d'accès réseau.
 - b. Les droits de mobilité (si l'abonné peut se déplacer entre différentes zones du réseau sans interruption de service).
8. **Attribution d'une Identité Temporaire (GUTI)**
L'AMF attribue ensuite une identité temporaire au terminal, appelée 5G-GUTI (Globally Unique Temporary Identity), qui sert à identifier le terminal de manière unique dans le réseau. Cela permet d'éviter l'utilisation de l'identité permanente de l'abonné, garantissant une meilleure confidentialité. Le 5G-GUTI est envoyé au terminal dans un message Registration Accept, indiquant que le terminal est désormais enregistré sur le réseau.
9. **Fin de la Procédure d'Enregistrement**
Le terminal confirme l'enregistrement en envoyant un message Registration

Complete. À ce stade, le terminal passe en état RM-Registered, signifiant qu'il est officiellement reconnu par le réseau et prêt à utiliser les services.

3. 5. Établissement de la Session PDU (Protocol Data Unit)

L'enregistrement du terminal ne suffit pas pour commencer à échanger des données. Il faut encore établir une session PDU, qui permet de créer un lien entre le terminal et le réseau de données. Cette session est gérée par plusieurs fonctions :

1. **Demande d'Établissement de Session** : Le terminal envoie une requête pour établir une session PDU, en précisant son 5G-GUTI. Ce message est transmis à l'AMF.
2. **Sélection du SMF** : L'AMF sélectionne un SMF (Session Management Function) pour gérer la session PDU. Le SMF joue un rôle crucial en vérifiant les droits de l'abonné liés à l'établissement de cette session. Le profil de l'abonné est à nouveau récupéré pour déterminer quel type de session PDU peut être établi (par exemple, pour des données Internet ou des services spécifiques).
3. **Sélection de l'UPF et Allocation d'une Adresse IP** : Le SMF sélectionne un UPF (User Plane Function) pour gérer le transfert des données entre le terminal et le réseau. Le SMF alloue ensuite une adresse IP au terminal, nécessaire pour permettre la transmission des données IP. L'UPF attribue également un TEID (Tunnel Endpoint Identifier), utilisé pour identifier la session PDU.
4. **Notification au gNB et au Terminal** : Le TEID est transmis au gNB via l'AMF, permettant la mise en place du tunnel de données entre le gNB et l'UPF. Le terminal est informé de l'adresse IP qui lui a été allouée via un message Session Establishment Accept, transmis de manière transparente par le gNB.
5. **Finalisation de la Session** : À la fin de cette procédure, le terminal passe à l'état CM-Connected, ce qui signifie qu'il est connecté au réseau radio et qu'un tunnel de données est établi entre le gNB et l'UPF. Le terminal peut désormais échanger des données avec le réseau.

4. Les Services de l'AMF

4.1. Définition

Le réseau 5G se caractérise par son architecture en mode « Service-Based Architecture », où les différentes fonctions réseau (NF) communiquent entre elles en utilisant le Service Based Protocol. Les communications entre les différentes NF sont basées sur les services proposés par chacun de ces NF. Chaque service est composé d'un serveur et d'un client, et est conçu pour exécuter une fonction spécifique. Dans cette partie on détaillera les différents services que propose l'AMF, en donnant dans un premier temps la définition de ces services et dans un second temps les opérations de services, qui ont chacun un rôle bien défini au sein de ces services.

4.2. Namf_Communication

4.2.1. Définition

Ce service permet à un NF de communiquer avec l'User Equipment (UE) en utilisant l'interface N1 pour échanger les messages de signalisation NAS (Non-Access Stratum). Le Namf_Communication permet aussi de communiquer avec le AN (Access Network).

4.2.2. Les opérations de service

4.2.2.1. UEContextTransfer

4.2.2.1.1. Définition

Utilisé dans le cas d'un handover ou d'un changement d'AMF, UEContextTransfer permet de transférer des informations (comme l'état d'enregistrement, les clés de sécurité, les informations de session, etc.) d'un UE, notamment en raison de la migration de l'UE entre différentes zones ou régions de couverture réseau. Cela permet de maintenir une expérience fluide, même lorsque l'UE se déplace dans des zones gérées par différents AMF.

4.2.2.1.2. Fonctionnement

Voici un schéma qui explique le fonctionnement de UEContextTransfer avec les différentes étapes :

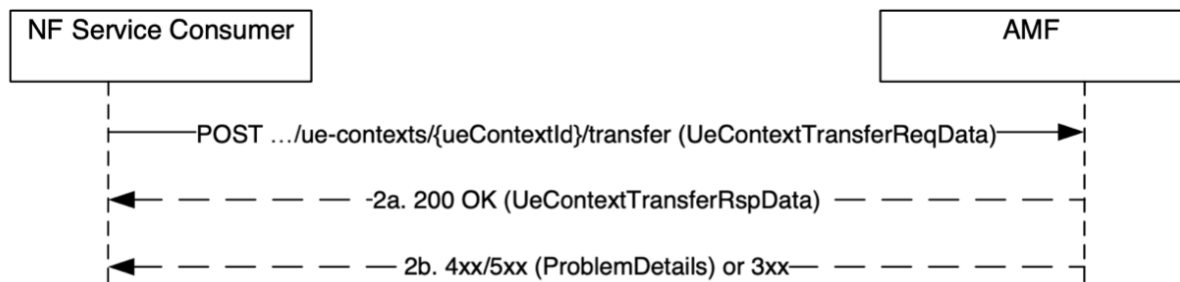


Figure 6 : Fonctionnement du UEContextTransfer

Etape 1 : Un NF (ex : un AMF cible), doit envoyer une requête HTTP POST "UeContextTransferReqData". Pour un enregistrement initial de l'UE, le NF cible doit définir l'attribut "reason" sur « INIT_REG ». Pour un enregistrement dû à un changement d'AMF, le NF cible doit définir l'attribut "reason" sur « MOBI_REG ».

Etape 2.a) : En cas de succès, l'AMF (source) doit répondre « 200 OK » (UeContextTransferRspData).

Etape 2.b) : En cas d'échec ou de redirection, l'un des codes d'état HTTP approprié (par exemple, "403 Forbidden") indiquant l'erreur doit être retourné. Le message doit contenir un objet ProblemDetails avec "detail" défini sur l'une des erreurs d'application correspondantes.

4.2.2.2. RegistrationStatusUpdate

4.2.2.2.1. Définition

Utilisée pour mettre à jour le statut d'enregistrement, qui avait été précédemment modifié par le UEContextTransfer, d'un UE au sein du réseau 5G.

4.2.2.2.2. Fonctionnement

Voici un schéma qui explique le fonctionnement de RegistrationStatusUpdate avec les différentes étapes :

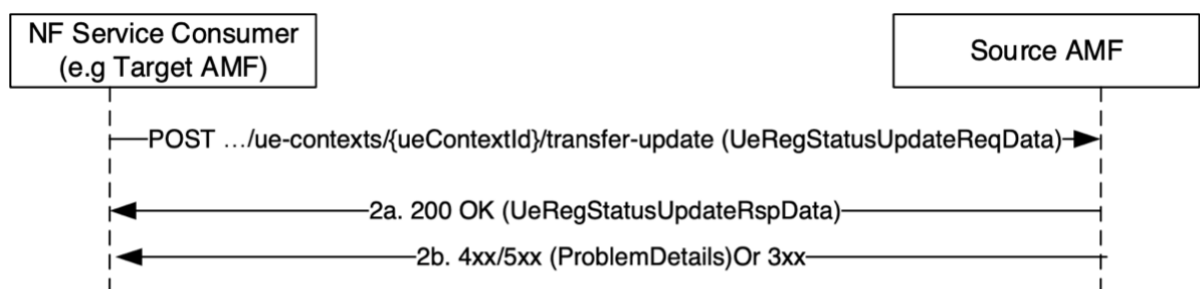


Figure 7 : Fonctionnement du RegistrationStatusUpdate

Etape 1 : Le NF (ex : l'AMF cible), doit envoyer une requête POST "UeRegStatusUpdateReqData". La requête doit également inclure l'attribut « transferStatus » défini sur "TRANSFERRED" si l'opération de service

“UeContextTransfer” a été complété avec succès ou sur "NOT_TRANSFERRED" dans le cas contraire.

Etape 2.a) : En cas de succès, l'AMF (source) doit répondre « 200 OK » (UeRegStatusUpdateRspData).

Etape 2.b) : En cas d'échec ou de redirection, l'un des codes d'état HTTP indiquant l'erreur doit être retourné. Le message doit contenir un objet ProblemDetails avec "detail" défini sur l'une des erreurs d'application correspondantes.

4.2.2.3. CreateUEContext/ ReleaseUEContext/ RelocateUEContext/ CancelRelocateUEContext

4.2.2.3.1. Définition

CreateUEContext, est utilisé dans le cas d'un handover pour permettre à un NF (ex : l'AMF source) de créer les informations d'un UE dans un autre NF (ex : l'AMF cible) lorsque l'UE quitte la zone de couverture de l'AMF source et que celui-ci ne peut plus assurer ses services à l'UE.

ReleaseUEContext, est utilisée pour supprimer les informations associées à un UE lorsque celui-ci n'est plus actif ou lorsqu'il est en phase de déconnexion.

RelocateUEContext, est utilisé par exemple par un AMF source vers un AMF cible, lors d'un transfert de l'EPS (Evolved Packet System) vers la 5GS avec une réaffectation de l'AMF, pour relocaliser les informations de l'UE dans l'AMF cible.

CancelRelocateUEContext, est utilisé pour annuler l'opération “RelocateUEContext”.

4.2.2.3.2. Fonctionnement

Voici un schéma qui explique le fonctionnement de CreateUEContext/ ReleaseUEContext/ RelocateUEContext/ CancelRelocateUEContext avec les différentes étapes :

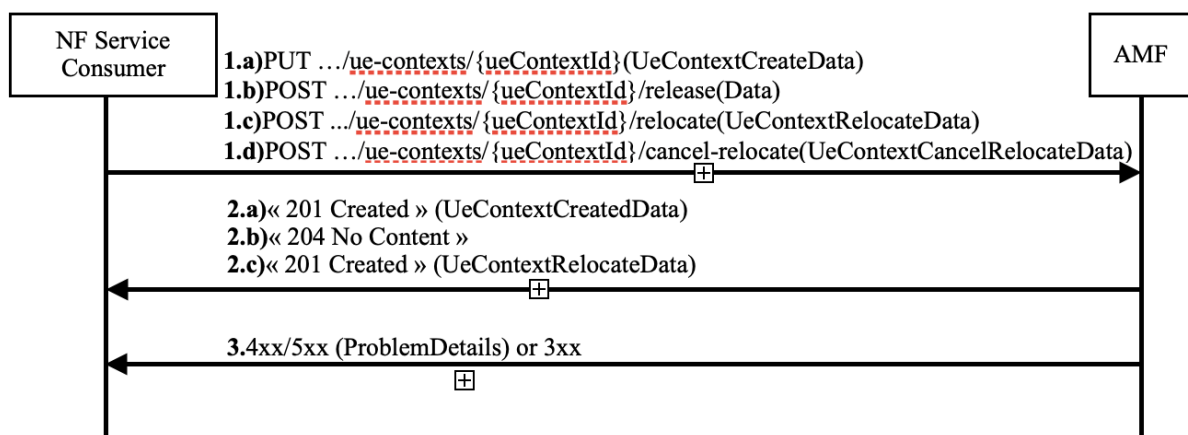


Figure 8 : CreateUEContext/ReleaseUEContext/RelocateUEContext/CancelRelocateUEContext

Etape 1.a) : Pour l'opération « CreateUEContext » le NF doit envoyer une requête PUT "UeContextCreateData".

1.b) : Pour l'opération « ReleaseUEContext » le NF doit envoyer une requête POST qui doit contenir toutes les données qui doivent être transmises à l'AMF cible.

1.c) : Pour l'opération « RelocateUEContext » le NF doit envoyer une requête POST "UeContextRelocateData".

1.d) : Pour l'opération « CancelRelocateUEContext » le NF doit envoyer une requête POST "UeContextCancelRelocateData".

Etape 2.a) et Etape 2.c) : Pour l'opération « CreateUEContext » et l'opération « RelocateUEContext »: En cas de succès, l'AMF cible doit répondre avec le code "201 Created" si la requête est acceptée, accompagné d'un en-tête HTTP Location pour indiquer l'emplacement de la nouvelle ressource créée.

Etape 2.b) : Pour l'opération « ReleaseUEContext » et l'opération « CancelRelocateUEContext » : En cas de succès, un "204 No Content" doit être retourné par l'AMF cible.

Etape 3 : Pour toutes les opérations : En cas d'échec ou de redirection, l'un des codes d'état HTTP indiquant l'erreur doit être retourné.

4.2.2.4. N1N2MessageTransfer/ N1N2Transfer Failure Notification

4.2.2.4.1. Définition

N1N2MessageTransfer est utilisé par un NF pour transférer simultanément les messages de signalisation des couches N1 et/ou N2, vers l'UE et/ou le 5G-AN.

N1N2Transfer Failure Notification est utilisé par l'AMF pour informer un NF qui est à l'origine de l'opération N1N2MessageTransfer, que l'AMF n'a pas réussi à livrer le message N1 à l'UE, car l'UE n'a pas répondu.

4.2.2.4.2. Fonctionnement

Voici un schéma qui explique le fonctionnement de N1N2MessageTransfer/ N1N2Transfer Failure Notification avec les différentes étapes :

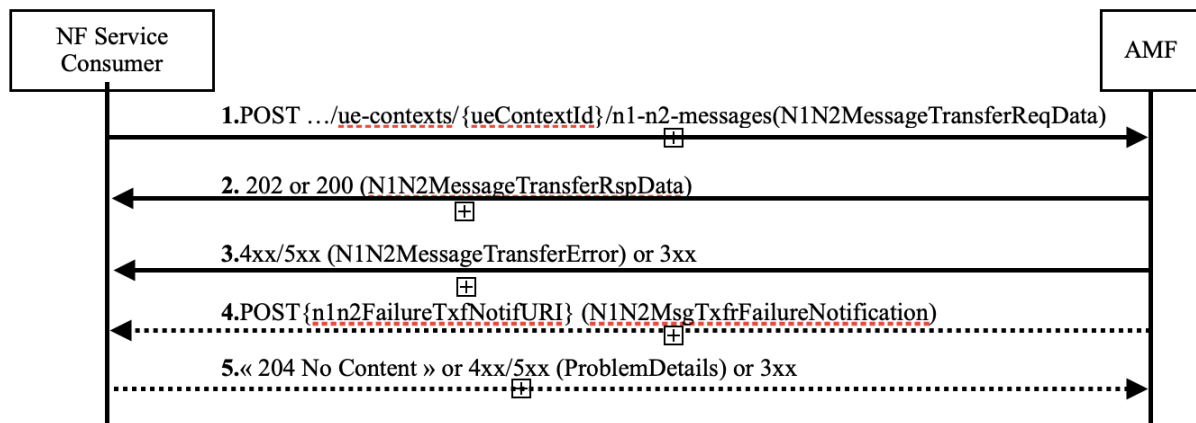


Figure 9 : N1N2MessageTransfer/N1N2Transfer Failure Notification

Etape 1 : Le NF doit envoyer une requête POST pour transférer les messages de signalisation N1 et N2.

Etape 2 : Cas 1, si l'UE est en CM_CONNECTED, l'AMF transfère le message à l'UE. L'AMF répond ensuite avec un "200 OK".

Cas 2, si l'UE est en CM_IDLE et que le flag Asynchronous Transfer est activé, l'AMF stocke le message dans un emplacement connu dans le CDL (Common Data Layer), et une réponse 202 est envoyée par l'AMF avec WAITING_FOR_ASYNCHRONOUS_TRANSFER comme cause. Le message sauvegardé est envoyé à l'UE lorsque ce dernier passe à CM_CONNECTED.

Cas 3, si l'UE est en CM_IDLE et que le flag SkipInd est activé dans le message N1N2TransferReqData reçu, l'AMF n'envoie pas le message N1 à l'UE. Dans ce cas, l'AMF envoie une réponse "200 OK" avec N1_MSG_NOT_TRANSFERRED comme cause. De plus, le message n'est pas envoyé à l'UE lorsque celui-ci passe à CM_CONNECTED dans ce scénario.

Cas 4, si l'UE est en CM_IDLE et que le flag Asynchronous Transfer n'est pas activé, l'AMF stocke le message dans un emplacement et une réponse 202 est envoyée avec ATTEMPTING_TO_REACH_UE comme cause. Le message sauvegardé est envoyé à l'UE lorsque celle-ci passe à l'état CM_CONNECTED.

Etape 3 : En cas d'échec ou de redirection, l'un des codes d'état HTTP indiquant l'erreur doit être retourné. Le corps du message doit contenir un objet N1N2MessageTransferError. Mais aussi une structure, ProblemDetails avec "detail" défini sur l'une des erreurs d'application correspondantes.

Etape 4 : Si l'opération N1N2MessageTransfer échoue l'AMF doit envoyer une requête POST d'échec au NF.

Etape 5 : Le NF doit envoyer une réponse « 204 No Content » après avoir reçu la notification de l'AMF. Sinon en cas d'échec ou de redirection, l'un des codes d'état HTTP indiquant l'erreur doit être retourné.

4.2.2.5. N1N2MessageSubscribe/ N1N2MessageUnSubscribe

4.2.2.5.1. Définition

N1N2MessageSubscribe est utilisée par un NF (ex:PCF) pour que l'AMF puisse lui envoyer des notifications de messages N1 d'un type spécifique (ex : UPDP) ou d'informations N2 d'un type spécifique.

N1N2MessageUnSubscribe est utilisée par un NF pour que l'AMF arrête de lui envoyer des notifications de messages N1.

4.2.2.5.2. Fonctionnement

Voici un schéma qui explique le fonctionnement de N1N2MessageSubscribe/ N1N2MessageUnSubscribe avec les différentes étapes :

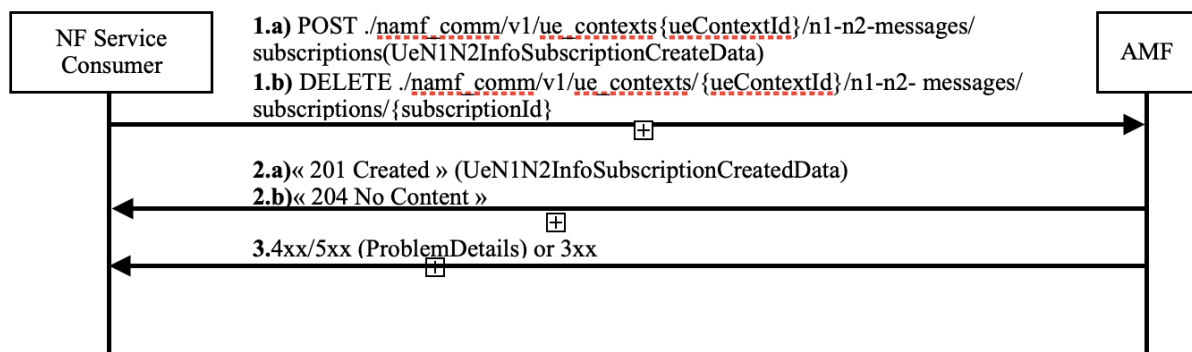


Figure 10 : N1N2MessageSubscribe/N1N2MessageUnSubscribe

Etape 1.a) : Pour l'opération « N1N2MessageSubscribe » le NF doit envoyer une requête POST. Le corps de la requête POST doit contenir, le type de message N1 et/ou N2 à notifier.

1.b) : Pour l'opération « N1N2MessageUnSubscribe » le NF doit envoyer une requête DELETE.

Etape 2.a) : Pour l'opération « N1N2MessageSubscribe », l'AMF doit répondre avec le code "201 Created" si la requête est acceptée.

2.b) : Pour l'opération « N1N2MessageUnSubscribe », si la requête est acceptée, l'AMF doit répondre « 204 No Content ».

Etape 3 : Pour les deux opérations, en cas d'échec ou de redirection, l'un des codes d'état HTTP indiquant l'erreur doit être retourné.

4.2.2.6. N1MessageNotify/ N2InfoNotify

4.2.2.6.1. Définition

N1MessageNotify permet à l'AMF de notifier le NF d'un message N1 particulier qui concerne un UE.

N2InfoNotify permet à l'AMF de notifier le NF que des informations N2 ont été reçues de la part du AN.

4.2.2.6.2. Fonctionnement

Voici un schéma qui explique le fonctionnement de N1MessageNotify/N2InfoNotify avec les différentes étapes :

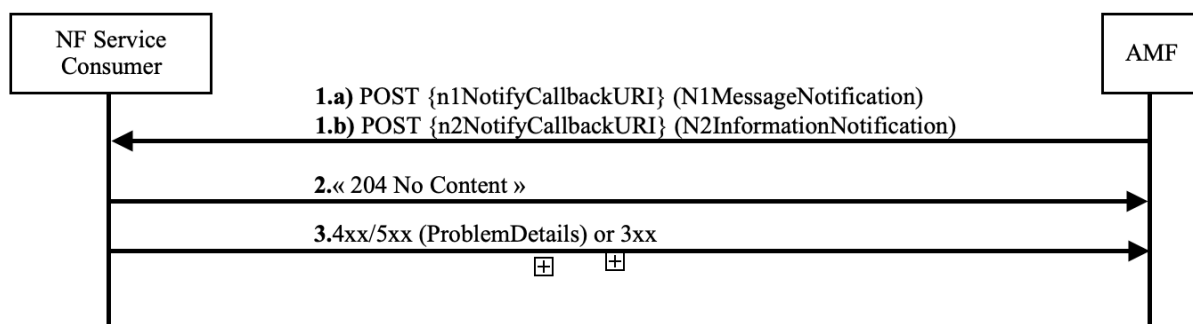


Figure 11 : N1MessageNotify/N2InfoNotify

Etape 1.a) : Pour l'opération « N1MessageNotify », l'AMF doit envoyer une requête HTTP POST (N1MessageNotification).

1.b) : Pour l'opération « N2InfoNotify », l'AMF doit envoyer une requête HTTP POST (N2InformationNotification).

Etape 2 : Pour les deux opérations, en cas de succès, un "204 No Content" sera envoyé.

Etape 3 : Pour les deux opérations, en cas d'échec ou de redirection, l'un des codes d'état HTTP approprié indiquant l'erreur doit être retourné. Le corps du message doit

contenir un objet ProblemDetails avec "detail" défini sur l'une des erreurs d'application correspondantes.

4.2.2.7. NonUeN2MessageTransfer

4.2.2.7.1. Définition

NonUeN2MessageTransfer permet de transférer des messages N2 vers des entités autres qu'un UE.

4.2.2.7.2. Fonctionnement

Voici un schéma qui explique le fonctionnement de NonUeN2MessageTransfer avec les différentes étapes :

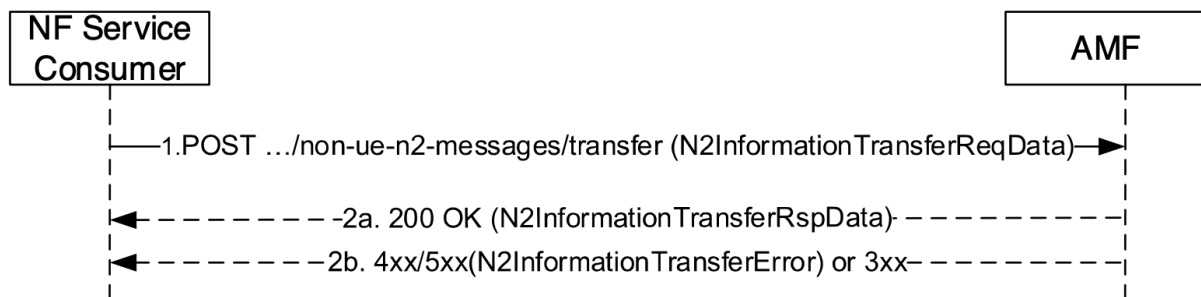


Figure 12 : NonUeN2MessageTransfer

Etape 1 : Le NF doit envoyer une requête HTTP POST (N2InformationTransferReqData).

Etape 2.a) : En cas de succès, un "200 OK" (N2InformationTransferRspData) sera envoyé par l'AMF.

2.b) : En cas d'échec ou de redirection, l'un des codes d'état HTTP approprié indiquant l'erreur doit être retourné. Le corps du message doit contenir une structure N2InformationTransferError avec également un objet ProblemDetails avec "detail" défini sur l'une des erreurs d'application correspondantes.

4.2.2.8. NonUeN2InfoSubscribe/ NonUeN2InfoUnSubscribe

4.2.2.8.1. Définition

NonUeN2InfoSubscribe est utilisée par un NF (ex: CBCF ou PWS-IWF) pour que l'AMF puisse lui envoyer des notifications d'informations N2 d'un type spécifique (ex : PWS Indications) qui ne sont pas associées à un UE.

NonUeN2InfoUnSubscribe est utilisée par un NF pour cesser les opérations de **NonUeN2InfoSubscribe**.

Pour ces deux opérations de services le fonctionnement est très similaire à celui des étapes de la Figure 10.

4.2.2.9. NonUeN2InfoNotify

4.2.2.9.1. Définition

NonUeN2InfoNotify permet à l'AMF de notifier le NF que des informations N2 Non-UE ont été reçues de la part du 5G-AN.

Pour cette opération de service, le fonctionnement est très similaire à celui des étapes de la Figure 4.2.2.6.2. N1MessageNotify//N2InfoNotify.

4.2.2.10. AMFStatusChangeSubscribe/ AMFStatusChangeUnSubscribe/ AMFStatusChangeNotify

4.2.2.10.1. Définition

AMFStatusChangeSubscribe est une opération de service utilisée par un NF (ex: SMF ou PCF) pour que l'AMF puisse lui informer des changements tels que le changement de disponibilité d'un UE, la déconnexion d'un AMF, ou d'autres changements pertinents au contexte de l'UE. Le NF peut aussi demander des modifications tels que les types de messages N1 ou N2 pour lesquels il reçoit des notifications ou ajuster la fréquence de mise à jour de certains événements, comme les changements d'état d'un UE.

AMFStatusChangeUnSubscribe est utilisé par un NF pour cesser les opérations de **AMFStatusChangeSubscribe**.

AMFStatusChangeNotify permet à un NF qui s'était précédemment abonné au **AMFStatusChangeSubscribe** de recevoir des notifications de changement de statut de l'AMF.

4.2.2.10.2. Fonctionnement

Voici un schéma qui explique le fonctionnement de **AMFStatusChangeSubscribe/ AMFStatusChangeUnSubscribe/ AMFStatusChangeNotify** avec les différentes étapes :

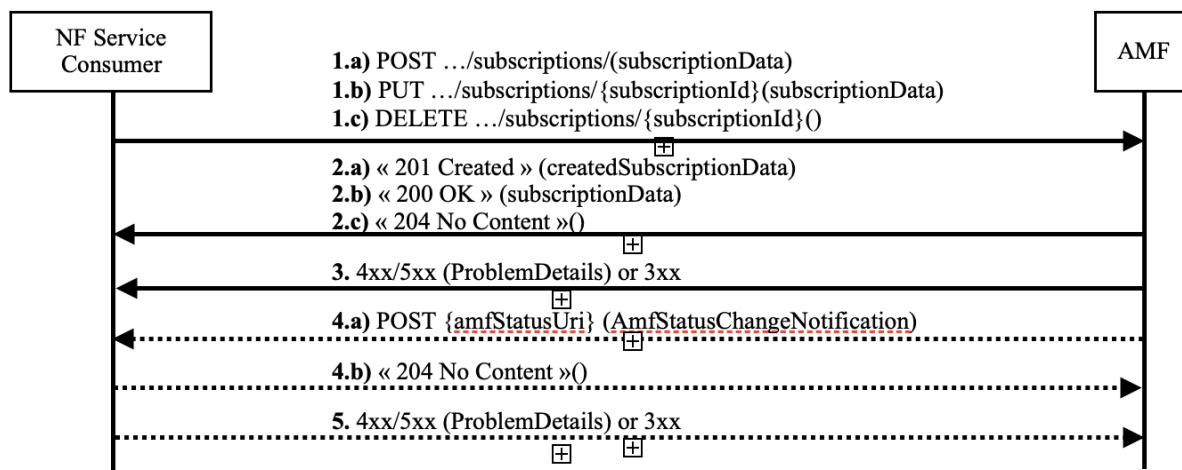


Figure 13 : AMFStatusChangeSubscribe/AMFStatusChangeUnSubscribe/AMFStatusChangeNotify

Etape 1.a) : Pour l'opération « AMFStatusChangeSubscribe », le NF doit envoyer une requête POST. La requête doit également inclure les données indiquant le ou les GUAMI (Globally Unique AMF Identifier) pris en charge par l'AMF, pour lesquels le NF souhaite recevoir une notification de changement de statut.

1.b) : Pour la modification, le NF doit envoyer une requête PUT. La requête doit inclure les nouvelles données qui remplaceront les anciennes données dans l'AMF.

1.c) : Pour l'opération « AMFStatusChangeUnSubscribe », le NF doit envoyer une requête DELETE.

Etape 2.a) : Pour l'opération « AMFStatusChangeSubscribe », l'AMF doit répondre avec le code "201 Created" si la requête est acceptée.

2.b) : Pour la modification, si succès, un "200 OK" sera retourné.

2.c) : Pour l'opération « AMFStatusChangeUnSubscribe », si la requête est acceptée, l'AMF doit répondre « 204 No Content ».

Etape 4.a) : Pour l'opération « AMFStatusChangeNotify », l'AMF doit envoyer une requête qui inclut le(s) GUAMI(s) indiqués par le NF lors de l'opération AMFStatusChangeSubscribe.

4.b) : Pour l'opération « AMFStatusChangeNotify », le NF doit envoyer un « 204 No Content » à l'AMF, si succès.

Etape 3 et 5 : Pour toutes les opérations de services, en cas d'échec ou de redirection, l'un des codes d'état HTTP approprié indiquant l'erreur doit être retourné.

Le corps du message doit contenir un objet ProblemDetails avec "detail" défini sur l'une des erreurs d'application correspondantes.

4.2.2.11. EBIAssignment

4.2.2.11.1. Définition

Une opération dans lequel l'AMF, attribue des identifiants (bearers) à un UE. Cette opération permet d'établir ou modifier les connexions de données entre l'UE et l'AMF.

4.2.2.11.2. Fonctionnement

Voici un schéma qui explique le fonctionnement de EBIAssignment avec les différentes étapes :

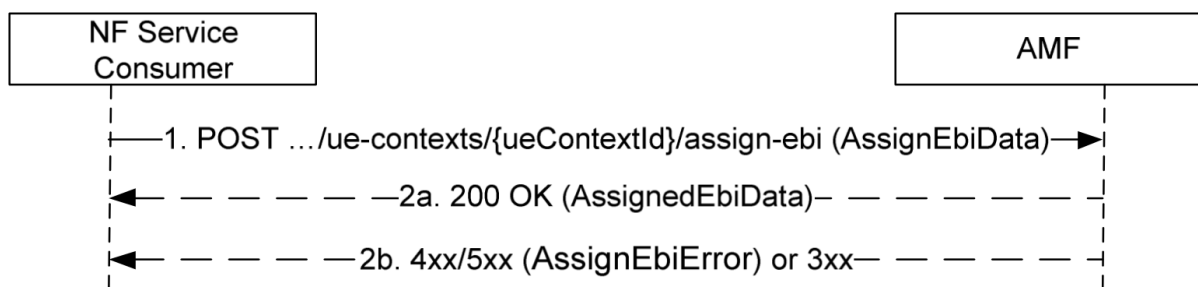


Figure 14 : EBIAssignment

Etape 1 : Le NF (ex : SMF) envoie la requête « assign-ebi » à l'AMF.

Etape 2.a) : En cas de succès, l'AMF envoie un « 200 OK ».

2.b) : En cas d'échec ou de redirection, l'un des codes d'état HTTP approprié indiquant l'erreur doit être retourné. Le message doit inclure AssignEbiError avec également un objet ProblemDetails avec "detail" défini sur l'une des erreurs d'application correspondantes.

4.3. Namf_EventExposure Service

4.3.1. Définition

Ce service permet à l'AMF d'envoyer des informations pertinentes d'un ou de plusieurs UE (ex : sa dernière localisation connue, le changement de son fuseau d'horaire, sa présence dans un AOI (Area of Interest) précis etc..), à d'autres NF.

4.3.2. Les opérations de service

4.3.2.1. Subscribe/ Unsubscribe/ Notify

4.3.2.1.1. Définition

Subscribe est utilisé par un NF (ex : NEF) pour demander à l'AMF de surveiller un ou plusieurs événements qui peut lui sembler utile concernant un ou plusieurs UE. Le NF peut aussi demander la modification de ces événements créé par lui-même auprès de l'AMF.

Unsubscribe est utilisé par un NF pour supprimer un événements créé par lui-même auprès de l'AMF.

Notify permet à l'AMF d'envoyer une notification au NF, lorsqu'un événement pertinent (ex : changement d'AMF) se produit.

4.3.2.1.2. Fonctionnement

Voici un schéma qui explique le fonctionnement de Subscribe/Unsubscribe/Notify avec les différentes étapes :

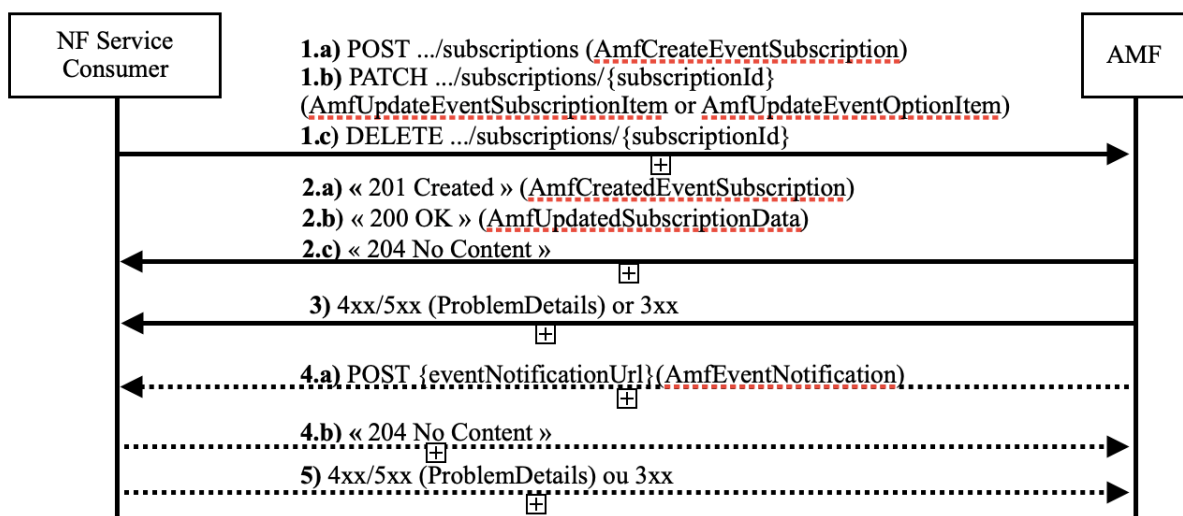


Figure 15 : Subscribe/Unsubscribe/Notify

Etape 1.a) : Pour l'opération « Subscribe », le NF doit envoyer une requête POST qui peut aussi contenir une durée d'expiration, donné par le NF, représentant la durée pendant laquelle l'AMF doit transmettre les informations de/des UE demandé par le NF. Au-delà de cette durée l'AMF ne doit plus transmettre ces informations au NF.

1.b) : Pour la modification, Le NF Service Consumer doit envoyer une requête PATCH.

1.c) : Pour l'opération « Unsubscribe », le NF Service Consumer doit envoyer une requête DELETE.

Etape 2.a) : Pour l'opération « Subscribe », l'AMF doit répondre avec le code "201 Created" si la requête est acceptée.

2.b) : Pour la modification, si succès, un "200 OK" sera retourné.

2.c) : Pour l'opération « Unsubscribe », si la requête est acceptée, l'AMF doit répondre « 204 No Content ».

Etape 4.a) : Pour l'opération « Notify », l'AMF doit envoyer une requête POST pour envoyer une notification.

4.b) Pour l'opération « Notify », le NF Service Consumer doit envoyer un « 204 No Content » à l'AMF, si succès.

Etape 3 et 5 : Pour les toutes les opérations de services, en cas d'échec ou de redirection, l'un des codes d'état HTTP approprié indiquant l'erreur doit être retourné. Le corps du message doit contenir un objet ProblemDetails avec "detail" défini sur l'une des erreurs d'application correspondantes.

4.4. Namf_MT Service

4.4.1. Définition

Ce service est conçu pour gérer les communications entrantes vers l'UE, celui-ci joue un rôle crucial dans la gestion des sessions de données et des appels entrants, en permettant au réseau de notifier et de gérer la connectivité avec les UE lorsqu'ils sont en mode IDLE (inactif) ou CM-CONNECTED (connecté).

Les fonctionnalités clés du service sont :

- Le Paging, une procédure qui permet au réseau de localiser un UE qui est en mode IDLE. Une fois localisé, le réseau utilise le paging pour envoyer un message à l'UE, l'invitant à passer en mode CM-CONNECTED pour pouvoir recevoir ses données ou un appel. Le Namf_MT peut aussi notifier d'autres NF pertinentes que le UE est en mode CM-CONNECTED.
- La réponse au NF demandeur que l'UE est connectée.

4.4.2. Les opérations de service

4.4.2.1. EnableUEReachability

4.4.2.1.1. Définition

Permet d'assurer le NF que l'UE est accessible pour les communications entrantes.

4.4.2.1.2. Fonctionnement

Voici un schéma qui explique le fonctionnement de EnableUEReachability avec les différentes étapes :

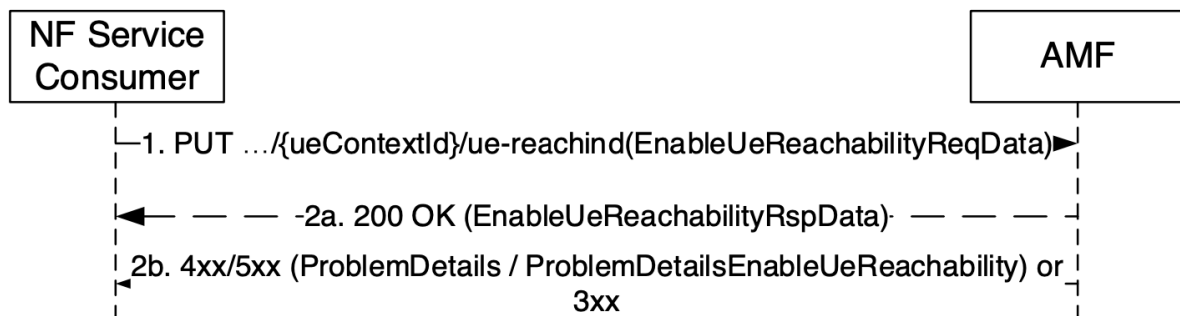


Figure 16 : EnableUEReachability

Etape 1 : Le NF envoie une requête PUT (EnableUeReachabilityReqData).

Etape 2.a) : En cas de succès, si l'UE est en CM-CONNECTED, l'AMF doit répondre "200 OK" (EnableUeReachabilityRspData). Si l'UE est CM-IDLE et que le message NAS doit être envoyé via l'accès 3GPP, l'AMF doit effectuer un paging de l'UE. Lorsque l'UE devient CM-CONNECTED, "200 OK"(EnableUeReachabilityRspData) doit être retourné.

2.b) : En cas d'échec ou de redirection, l'un des codes d'état HTTP approprié (par exemple, '404 Not Found') indiquant l'erreur doit être retourné. Pour une réponse 4xx/5xx, le corps du message doit contenir une structure ProblemDetails ou ProblemDetailsEnableUeReachability avec l'attribut "cause" défini sur l'une des erreurs d'application. L'AMF doit répondre avec le code d'état "403 Forbidden" si l'UE se trouve dans une zone non autorisée, l'AMF doit donc définir l'erreur d'application comme "UE_IN_NON_ALLOWED_AREA" dans la réponse POST.

4.4.2.2. ProvideDomainSelectionInfo

4.4.2.2.1. Définition

A pour but d'informer les NF sur le domaine approprié à utiliser pour acheminer les communications vers un UE cible. Cela inclut notamment des informations pour le routage d'appels vocaux, de messages, et d'autres types de données.

4.4.2.2.2. Fonctionnement

Voici un schéma qui explique le fonctionnement de ProvideDomainSelectionInfo avec les différentes étapes :

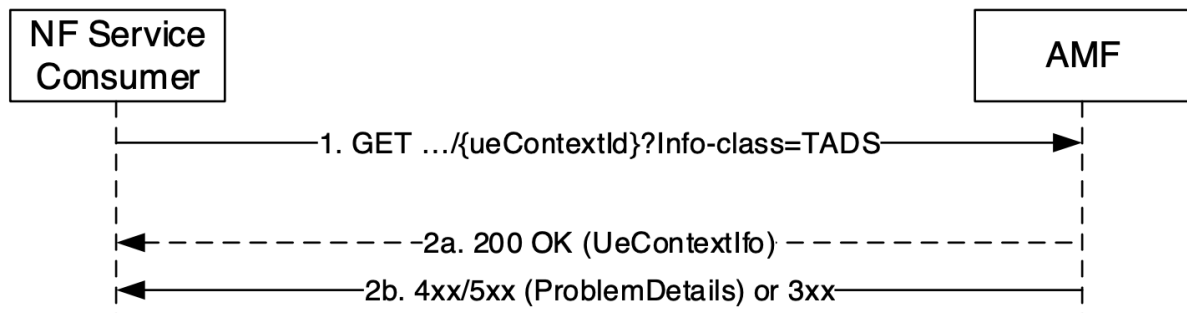


Figure 17 : ProvideDomainSelectionInfo

Etape 1 : Le NF doit envoyer une requête GET.

Etape 2.a) : En cas de succès, l'AMF doit renvoyer un code d'état "200 OK"(UeContextInfo).

2.b) : En cas d'échec ou de redirection, l'un des codes d'état HTTP approprié (par exemple, '404 Not Found') indiquant l'erreur doit être retourné. Le corps du message doit contenir un objet ProblemDetails avec "detail" défini sur l'une des erreurs d'application correspondantes.

4.5. Namf_Location Service

4.5.1. Définition

Ce service est utilisé par les NF pour demander à l'AMF d'effectuer des requêtes de positionnement et de fournir des informations sur la localisation de l'UE. Il est aussi utilisé pour notifier, par la suite, des événements liés aux changements de localisation d'un ou plusieurs UE aux NF.

4.5.2. Les opérations de service

4.5.2.1. ProvidePositioningInfo

4.5.2.1.1. Définition

Utilisé par un NF (ex:GMLC) pour demander la position géodésique (latitude, longitude) actuelle ou différée et, éventuellement, la localisation civique (adresse, etc.) de l'UE.

4.5.2.1.2. Fonctionnement

Voici un schéma qui explique le fonctionnement de ProvidePositioningInfo avec les différentes étapes :

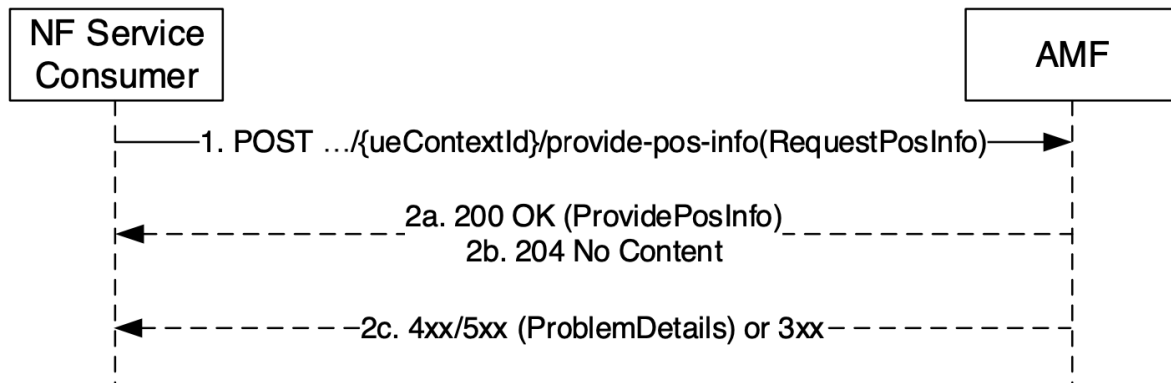


Figure 18 : ProvidePositioningInfo

Etape 1 : Le NF Service Consumer doit envoyer une requête POST. La requête POST peut contenir une indication d'une demande de positionnement provenant d'un client des services d'urgence ou bien des services commerciaux mais aussi la qualité de service (QoS) requise ainsi que les formes de Geographical Area Description (GAD) prises en charge.

Etape 2.a) : En cas de succès, un "200 OK" doit être retourné.

2.b) : En cas d'acceptation, un "204 No Content" doit être retourné pour accuser réception que l'AMF prend en charge et accepte une demande de localisation différée.

2.c) : En cas d'échec ou de redirection, l'un des codes d'état HTTP approprié (par exemple, '404 Not Found') indiquant l'erreur doit être retourné. Le corps du message doit contenir un objet ProblemDetails avec "detail" défini sur l'une des erreurs d'application correspondantes.

4.5.2.2. Eventnotify

4.5.2.2.1. Définition

Permet à l'AMF de notifier le NF (ex : GMLC) des informations liées à la localisation de l'UE utiles pour les services d'urgence ou la localisation différée, c'est-à-dire l'initiation, le transfert, la fin d'un service d'urgence ou bien l'achèvement, l'activation de la localisation différée.

4.5.2.2.2. Fonctionnement

Voici un schéma qui explique le fonctionnement de Eventnotify avec les différentes étapes :

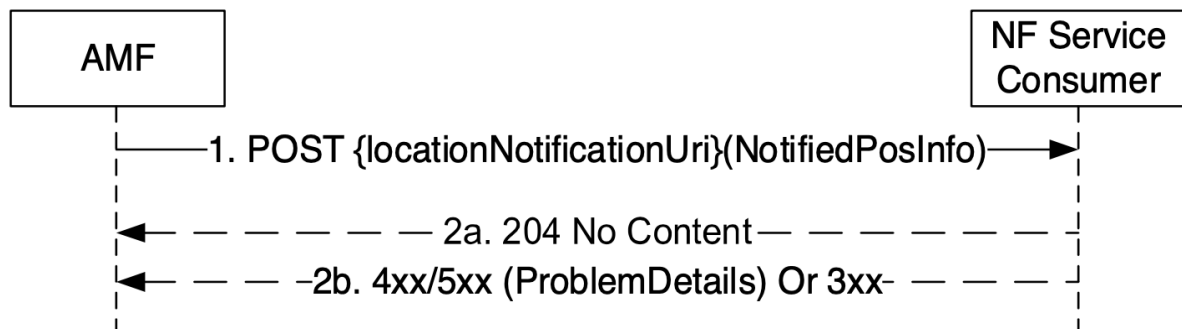


Figure 19 : EventNotify

Etape 1 : L'AMF doit envoyer une requête POST. La requête doit inclure l'identification de l'UE (SUPI ou PEI), et peut inclure, la localisation géodésique, la localisation civique etc...

Etape 2.a) : En cas de succès, un "204 No Content" doit être retourné par le NF.

2.b) : En cas d'échec ou de redirection, l'un des codes d'état HTTP approprié (par exemple, "403 Forbidden") indiquant l'erreur doit être retourné. Le corps du message doit contenir un objet ProblemDetails avec "detail" défini sur l'une des erreurs d'application correspondantes.

4.5.2.3. ProvideLocationInfo

4.5.2.3.1. Définition

Permet à un NF (ex : UDM) de demander le Network Provided Location Information (NPLI) d'un ou plusieurs UE cibles. Cela permet notamment de récupérer les informations sur le fuseau horaire de l'UE ainsi que les informations de localisation de l'utilisateur à partir du Access Network.

4.5.2.3.2. Fonctionnement

Voici un schéma qui explique le fonctionnement de ProvideLocationInfo avec les différentes étapes :

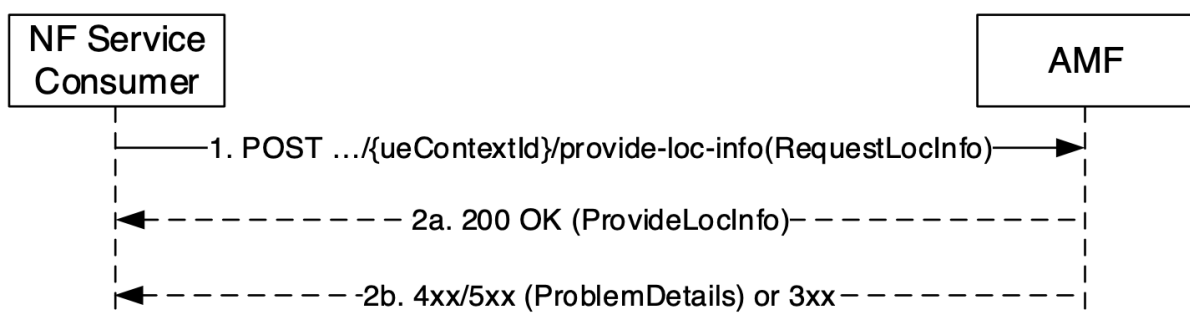


Figure 20 : ProvideLocationInfo

Etape 1 : Le NF doit envoyer une requête POST, qui doit contenir (RequestLocInfo) indiquant quel type d'informations sur la localisation le NF souhaite obtenir. Si le NF souhaite obtenir les informations sur la localisation actuelles de l'UE cible, il doit définir l'attribut "reqCurrentLoc" sur « true ».

Etape 2.a) : En cas de succès, un "200 OK" (ProvideLocInfo) doit être renvoyée incluant le NPLI de l'UE cible.

- Si l'attribut "reqCurrentLoc" est défini sur "true" et que l'UE est en RM-REGISTERED et CM-IDLE sur un accès 3GPP, l'AMF doit initier une procédure de paging vers l'UE. Si la procédure de paging est réussie, l'AMF doit renvoyer les informations de localisation actuelles et définir l'attribut "currentLoc" sur "true" dans la réponse. Si l'UE ne répond pas au paging, l'AMF doit fournir la dernière localisation connue et définir l'attribut "currentLoc" sur "false" dans la réponse.

- Si l'attribut "reqCurrentLoc" est défini sur "true" et que l'UE est en RM-REGISTERED et CM-CONNECTED sur un accès 3GPP, l'AMF doit suivre la procédure de rapport de localisation NG-RAN, pour déclencher un rapport unique et autonome. Si NG-RAN rapporte la localisation actuelle de l'UE, l'AMF doit définir l'attribut "currentLoc" sur "true" dans la réponse. Si NG-RAN rapporte la dernière localisation connue de l'UE avec un horodatage, l'AMF doit définir l'attribut "currentLoc" sur "false" dans la réponse.

- Si l'UE est dans l'état RM-REGISTERED sur un accès non-3GPP, l'AMF doit inclure les dernières informations de localisation d'accès non-3GPP.

2.b) : En cas d'échec ou de redirection, l'un des codes d'état HTTP approprié (par exemple, "403 Forbidden") indiquant l'erreur doit être retourné. Le corps du message doit contenir un objet ProblemDetails avec "detail" défini sur l'une des erreurs d'application correspondantes.

4.5.2.4. CancelLocation

4.5.2.4.1. Définition

Permet à un NF de demander l'annulation de la notification qui concerne la localisation de l'UE qui avaient été précédemment demandés.

4.5.2.4.2. Fonctionnement

Voici un schéma qui explique le fonctionnement de CancelLocation avec les différentes étapes :

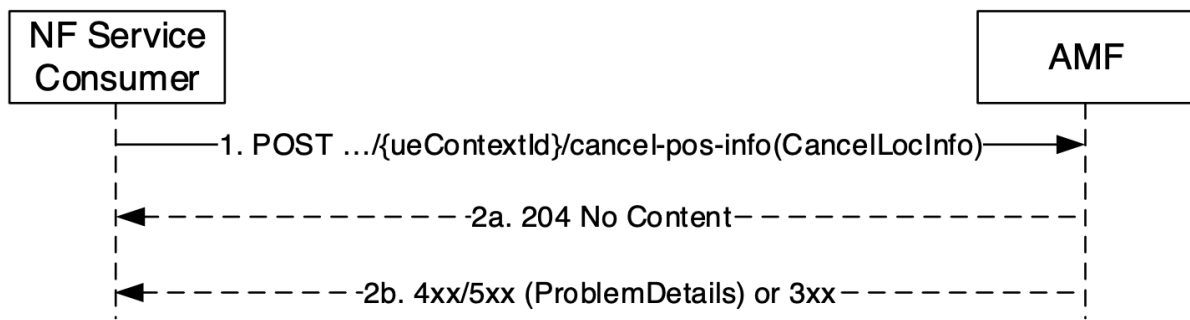


Figure 21 : CancelLocation

Etape 1 : Le NF doit envoyer une requête POST (CancelLocInfo).

Etape 2.a) : En cas de succès, un "204 No Content" doit être retourné par l'AMF.

2.b) : En cas d'échec ou de redirection, l'un des codes d'état HTTP approprié (par exemple, "403 Forbidden") indiquant l'erreur doit être retourné. Le corps du message doit contenir un objet ProblemDetails avec "detail" défini sur l'une des erreurs d'application correspondantes.

5. APIs de l'AMF

Les fonctions du cœur de réseau sont conçues pour communiquer à l'aide d'une architecture basée sur les services (Service based architecture), où chaque NF expose ses services via des API REST basées sur HTTP/2 (Chaque service expose sa propre API).

5. 1. Format général des routes

Le format général d'une route d'API est :

```
{apiRoot}/{apiName}/{apiVersion}/{apiSpecificResourceUriPart}
```

Tel que:

- **apiRoot** est une concaténation des parties suivantes :
 - Scheme : **http** ou **https**
 - La chaîne : **://**
 - Autorité : hôte et numéro de port facultatif \
 - Préfixe API (optionnel) : **/**
- **apiName** indique le nom de l'API.
- **apiVersion** indique le premier champ (majeur) de la version de l'API

Tous les headers HTTP standards sont supportés. Quant au Content type, les types supportés sont :

- **JSON** : indiqué par le content type "application/json"

- **The Problem Detail JSON Object** : indiqué par le content type "application/problem+json"
- **Multipart messages** : Afin de transférer les information N1 et/ou N2 de manière opaque. Il est indiqué par le content type "multipart/related" et il contient :
 - Un corp JSON (JSON body)
 - Un ou plusieurs corps binaires (binary bodies) qui incluent les N1 et/ou N2 payload avec des content subtypes spécifiques au fournisseur 3gpp et qui sont vnd.3gpp.ngap ou vnd.3gpp.5gnas

5. 2. API du service Namf_Communication

La route de l'API du service Namf_Communication est :

```
{apiRoot}/namf-comm/v1/
```

Elle a la structure des URI suivante :

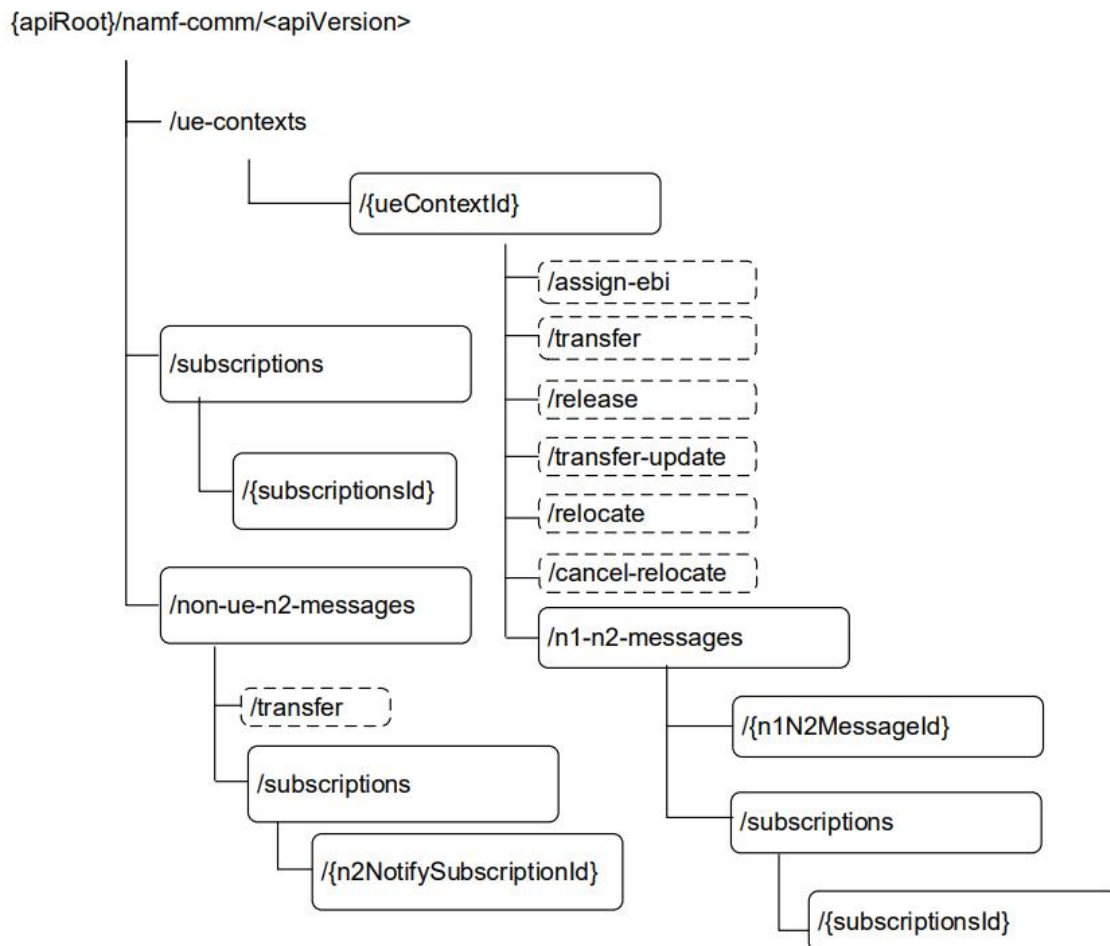


Figure 22 : Structure URI de l'api du service Namf_Communication

La table 1 explique chacune des ressources URI de la structure ci-dessus

Nom de la ressource	URI de la ressource	Methode HTTP	Description
Individual ueContext	/ue-contexts/{ueContextId}	PUT	CreateUEContext
	/ue-contexts/{ueContextId}/release	Release (POST)	ReleaseUEContext
	/ue-contexts/{ueContextId}/assign-ebi	Assign-ebi	EBIAssignment
	/ue-contexts/{ueContextId}/transfer	Transfer(POST)	UEContextTransfer
	/ue-contexts/{ueContextId}/transfer-update	transferupdate (POST)	RegistrationStatusUpdate
	/ue-contexts/{ueContextId}/relocate	relocate (POST)	RelocateUEContext
	/ue-contexts/{ueContextId}/cancel-relocate	Cancel-relocate (POST)	CancelRelocateUEContext
n1N2Message collection	/ue-contexts/{ueContextId}/n1-n2-messages	POST	N1N2MessageTransfer
N1N2 Subscriptions Collection for Individual UE Contexts	/ue-contexts/{ueContextId}/n1-n2-messages/subscriptions	POST	N1N2MessageSubscribe
N1N2 Individual Subscription	/ue-contexts/{ueContextId}/n1-n2-messages/subscriptions/{subscriptionId}	DELETE	N1N2MessageUnSubscribe
subscriptions collection	/subscriptions	POST	AMFStatusChangeSubscribe
individual subscription	/subscriptions/{subscriptionId}	PUT	AMFStatusChangeSubscribe
		DELETE	AMFStatusChangeUnSubscribe
Non UE N2Messages collection	/non-ue-n2-messages/transfer	Transfer(POST)	NonUEN2MessageTransfer
Non UE N2Messages Subscriptions collection	/non-ue-n2-messages/subscriptions	POST	NonUEN2InfoSubscribe
Non UE N2 Message Notification Individual Subscription	/non-ue-n2-messages/subscriptions/{n2NotifySubscriptionId}	DELETE	NonUEN2InfoUnsubscribe

Table 1 : ressources URI de l'api du service Namf_Communication

5. 2. 1. Individual ueContext

Cette ressource représente un ueContext individuel identifié par le ueContextId. UeContextId représente l'identifiant temporaire 5G globalement unique ou l'identifiant permanent de l'abonnement ou l'identifiant permanent de l'équipement.

5. 2. 2. N1N2 Subscriptions Collection for Individual UE Contexts

Cette ressource représente la collection sous un contexte UE individuel pour stocker les abonnements aux notifications des types de messages N1 et N2 spécifiques à l'UE.

5. 2. 3. N1N2 Individual Subscription

Cette ressource représente l'abonnement individuel aux notifications des types de messages N1 et N2 spécifiques à l'UE.

5. 2. 4. N1N2 Messages Collection

Cette ressource représente la collection sur laquelle les messages N1 relatifs à l'UE et le transfert d'informations N2 sont lancés et les informations N1 relatives à l'UE sont stockées temporairement jusqu'à ce que l'UE soit joignable.

5. 2. 5. Subscriptions collection

Cette ressource représente une collection d'abonnements de consommateurs de services NF au changement d'état de l'AMF identifié par le(s) GUAMI(s).

5. 2. 6. individual subscription

Cette ressource représente un abonnement individuel d'un consommateur de service NF au changement d'état de l'AMF identifié par le(s) GUAMI(s).

5. 2. 7. Non UE N2 Messages Collection

Cette ressource représente la collection sur laquelle sont spécifiées les opérations personnalisées de transfert du message N2 vers le réseau 5G-AN.

5. 3. API du service Namf_EventExposure

La route de l'API du service Namf_EventExposure est :

```
{apiRoot}/namf-evts/v1/
```

Elle a la structure des URI suivante :

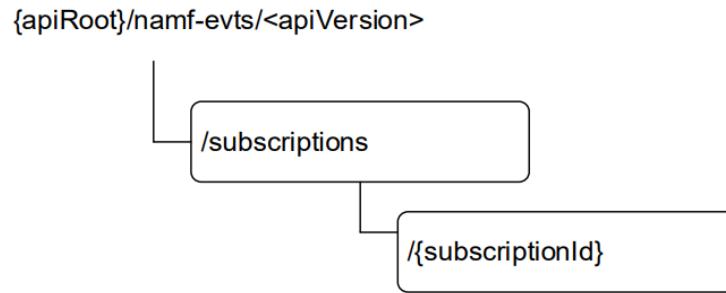


Figure 23 : Structure URI de l’api du service Namf_EventExposure

La table 2 explique chacune des ressources URI de la structure ci-dessus

Nom de la ressource	URI de la ressource	Methode HTTP	Description
Subscriptions collection	/subscriptions	POST	Associé à l'opération de service Subscribe, quand créer un abonnement
Individual subscription	/{subscriptionId}	PATCH	Associé à l'opération de service S'abonner, quand modifier
		DELETE	Associé à l'opération de service « Unsubscribe » (désabonnement)

Table 2 : ressources URI de l’api du service Namf_EventExposure

5. 3. 1. Subscriptions collection

Cette ressource représente une collection d'abonnements créés par les consommateurs du service NF du service Namf_EventExposure.

5. 3. 2. Individual subscription

Cette ressource représente un individu de l'abonnement créé par les consommateurs du service NF du service Namf_EventExposure.

5. 4. API du service Namf_MT

La route de l’API du service Namf_MT est :

```
{apiRoot}/namf-mt/v1/
```

Elle a la structure des URI suivante :

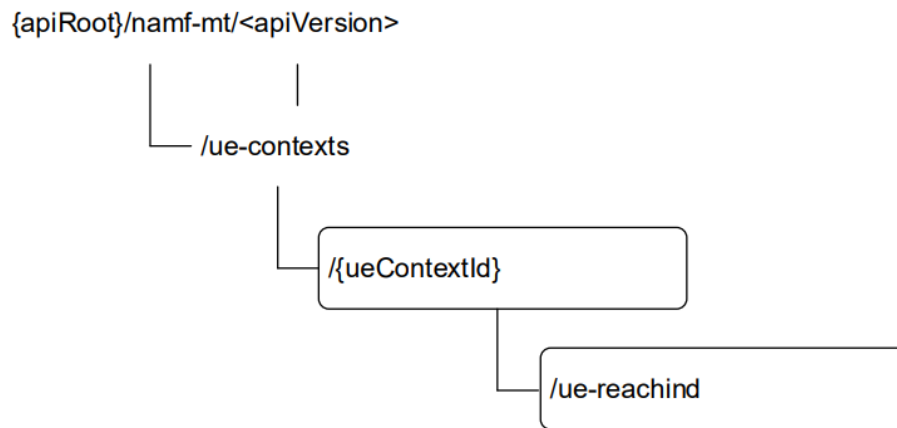


Figure 24 : Structure URI de l'api du service Namf_MT

La table 3 explique chacune des ressources URI de la structure ci-dessus

Nom de la ressource	URI de la ressource	Methode HTTP	Description
ueReachInd	{apiRoot}/namf-mt//uecontexts/{ueContextId}/ue-reachind	PUT	Mettre à jour le ueReachInd en UE Reachable
ueContext	{apiRoot}/namf-mt//ue-contexts/{ueContextId}	GET	Correspond à l'opération de service suivante : ProvideDomainSelecti onInfo

Table 3 : ressources URI de l'api du service Namf_MT

5. 4. 1. ueReachInd

Cette ressource représente le ueReachInd pour un SUPI

5. 4. 2. ueContext

Cette ressource représente l'UeContext d'un UE

5. 5. API du service Namf_Location

La route de l'API du service Namf_Location est :

```
{apiRoot}/namf-loc/v1/
```

Elle a la structure des URI suivante :

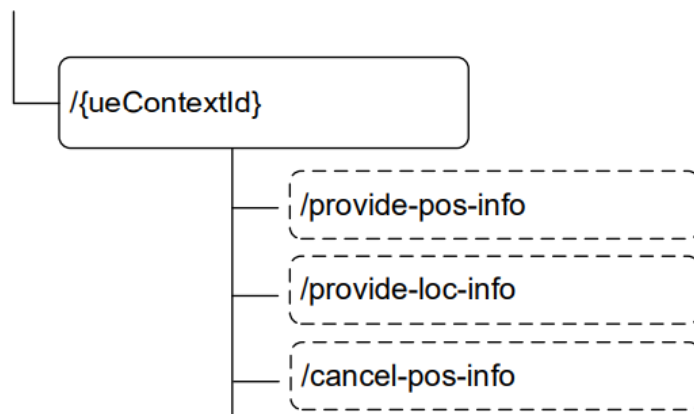


Figure 25 : Structure URI de l’api du service Namf_ Location

La table 4 explique chacune des ressources URI de la structure ci-dessus

Nom de la ressource	URI de la ressource	Methode HTTP	Description
Individual UE context	/provide-pos-info	provide-pos-info (POST)	ProvidePositioningInfo
	/provide-loc-info	provide-loc-info (POST)	ProvideLocationInfo
	/cancel-pos-info	cancel-pos-info (POST)	CancelLocation

Table 4 : ressources URI de l’api du service Namf_ Location

5. 5. 1 Individual UE context

Cette ressource représente un ueContextId individuel.

6. Les interactions entre AMF et NF

L’AMF est au cœur du réseau 5G elle interagit avec de nombreuses NF. Cette partie a pour but d’expliquer ces différentes interactions que ce soit du côté AMF et du côté des autres NF.

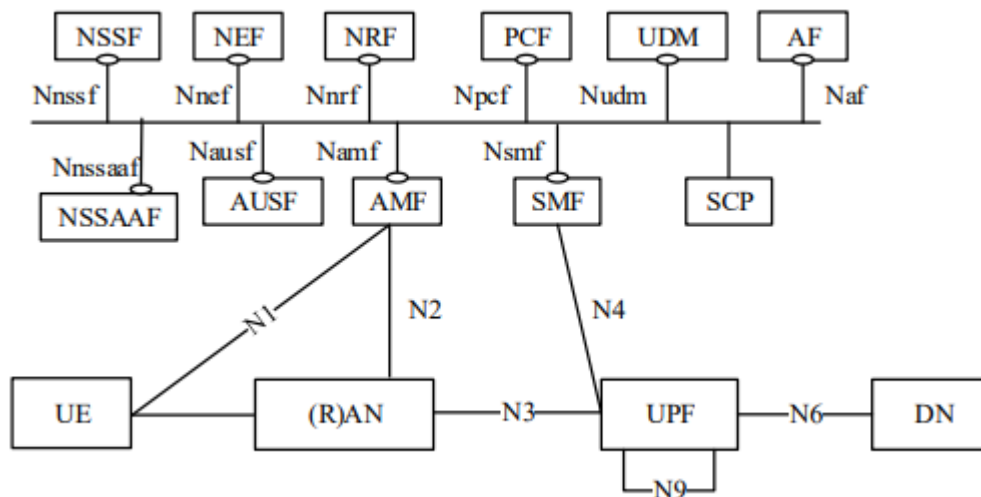


Figure 26 : Architecture 5G (2)

6.1 AMF et AUSF (Authentication Server Function)

3GPP TS 29.509 version 16.10.0:

-5.2 Nausf_UEAuthentication Service

L'interaction AMF et AUSF permet de garantir un accès sécurisé et l'authentification de l'UE (User Equipment) pour se connecter au réseau 5G.

AUSF effectue une vérification d'authentification entre l'UE et le service réseau. Cela permet ainsi d'empêcher les appareils non autorisés à accéder au réseau.

Cette authentification se déroule en plusieurs étapes :

D'abord l'UE qui souhaite accéder au réseau 5G envoie une demande à l'AMF via le RAN.

Ensuite l'AMF transmet une demande avec les informations d'identification à l'AUSF via l'interface N12.

L'AUSF vérifiera alors ses informations avec l'aide de l'UDM qui stocke les données de l'abonnement de l'UE qui seront récupérés.

Pour l'authentification l'AUSF peut utiliser deux méthodes:

- 5G-AKA : Vérification mutuelle avec clé pré-partagés
- EAP-AKA : Méthode qui permet plus de flexibilité et de compatibilité (Wi-Fi...)

Enfin, une fois la validation finie, si valide l'AUSF envoie à l'AMF un token SUPI (Subscription Permanent Identifier) et clé de sessions pour sécuriser et permettre l'accès au réseau à l'UE.

Si la validation n'est pas valide, l'AUSF avertit l'AMF et ce dernier doit en informer l'UE.

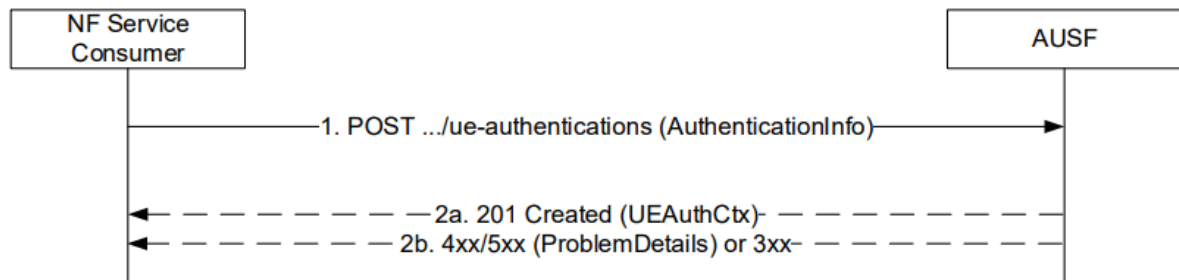


Figure 27 : Schéma de demande d'authentification

NF Service Consumer représente ici l'AMF

étape 2a. : succès de l'authentification

étape 2b. : échec de l'authentification

Cette authentification permet alors une communication sécurisée et cryptée entre l'UE et le cœur du réseau. Cette authentification doit être périodiquement renouvelée surtout quand l'UE change de réseau.

6.2 AMF et UDM (Unified Data Management)

3GPP TS 29.503 version 16.16.0:

-5.2 Nudm_SubscriberDataManagement Service

-5.3 Nudm_UEContextManagement Service

L'interaction AMF et UDM permet à l'AMF d'accéder aux données d'abonnement et les données de sécurité ainsi que les paramètres de mobilités de l'UE pour gérer l'accès de dernier au réseau.

UDM gère les données des UE, il stocke les données d'abonnements et d'authentification, les profils de services et politique de réseau.

L'UE qui souhaite s'inscrire au réseau envoie une demande d'enregistrement à l'AMF via le RAN. L'AMF doit donc vérifier si l'UE est autorisée à accéder au réseau. L'AMF communique alors avec l'UDM pour accéder à ses services via l'interface N8.

L'AMF peut demander alors les données d'abonnement, les politiques de réseaux, les restrictions d'accès de l'UE. L'UDM récupère alors les données du profil de l'UE stocker dans l'UDR (Unified Data Repository) et les autres informations et les renvoie à l'AMF.

L'AMF récupère alors ces données et peut alors s'occuper de l'enregistrement avec le profil et les informations de sécurité fournis. Il pourra aussi utiliser ses données pour s'occuper de l'allocation des tranches de réseaux (avec NSSF) ainsi que gérer de manière fluides les handovers à travers le réseau.

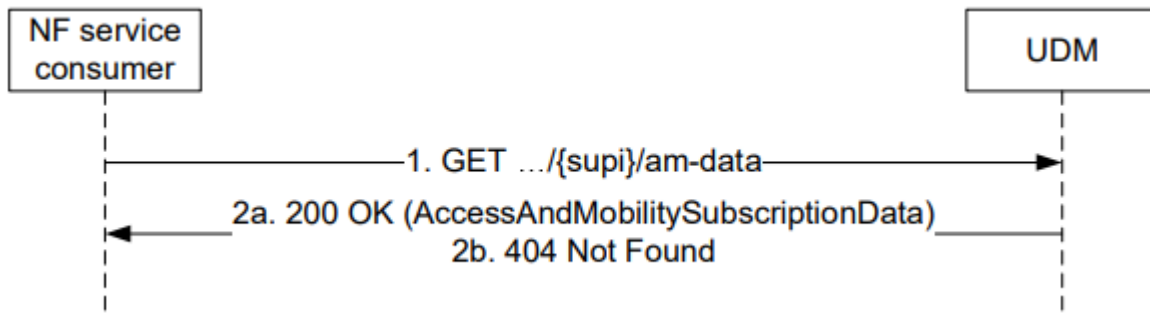


Figure 28 : Schéma de demande de donnée d'un UE

Etape 1 : Récupère les données liées au SUPI

Etape 2 : Réussite ou Introuvable

Après l'inscription l'AMF communique périodiquement avec l'UDM pour mettre à jour la localisation de l'UE si elle change. Aussi si les données d'abonnement changent l'UDM envoie une mise à jour à l'AMF qui pourra imposer la politique de réseau. L'UDM fournit aussi des paramètres de sécurité afin de sécuriser la communication entre le réseau et l'UE.

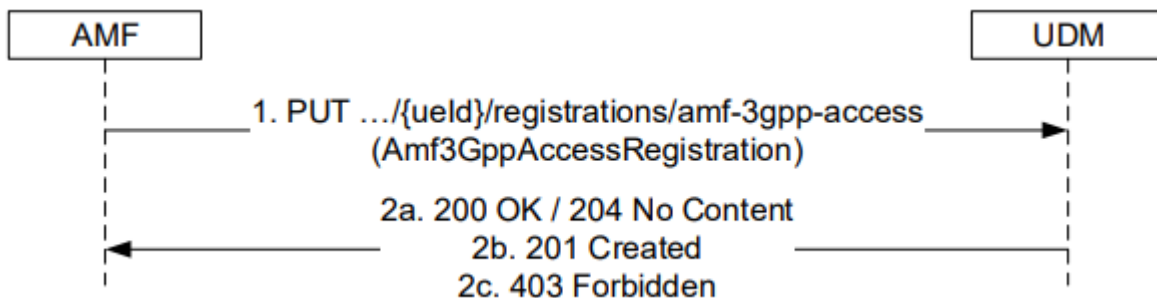


Figure 29 : Schéma de demande de mise à jour

étape 2a. : Enregistrement réussi

étape 2b. : User non connu, stockage des infos dans l'UDM

étape 2c. : Echec de l'enregistrement (Problème dans les données d'abonnements)

Quand l'UE se déconnecte, l'AMF informe l'UDM afin que l'UE soit marquée comme inactive et permet de ne pas allouer des ressources inutilement.

L'interaction permet alors à l'AMF de pouvoir connecter l'UE grâce à ses données d'abonnements fournis par l'UDM en sécurisant et assurant une bonne qualité de service sur le réseau. Elle gère aussi les informations de mobilités permettant la gestion des handovers.

6.3 AMF et NSSF (Network Slice Selection Function)

3GPP TS 29.531 version 16.10.0:

-5.2 Nnssf_NSSelection Service

-5.3 Nnssf_NSSAIAvailability Service

L'interaction AMF et NSSF permet d'allouer correctement les tranches (slices) du réseau pour permettre aux UE de les utiliser.

NSSF s'occupe d'allouer dynamiquement et flexiblement les tranches du réseau disponible aux UE.

L'UE qui souhaite occuper le réseau, adresse alors une demande à l'AMF en pouvant indiquer des préférences ou des exigences sur les tranches de réseau : faible latence ou bande passante élevée.

L'AMF contacte alors la NSSF via l'interface N22 et lui envoie des détails comme : les exigences de l'UE, l'ID du réseau ou bien les données d'abonnement obtenue grâce à l'UDM.

NSSF évaluera cette requête en jugeant la demande avec la capacité disponible et ses détails. Elle renvoie alors à l'AMF la ou les tranches appropriées (Single – Network Slice Selection Assistance Information (S-NSSAI)) ainsi que leurs paramètres QoS. S'il n'y a pas de disponibilité alors NSSF renverra d'autre disponibilité ou bien des alternatives pour l'UE via l'AMF.

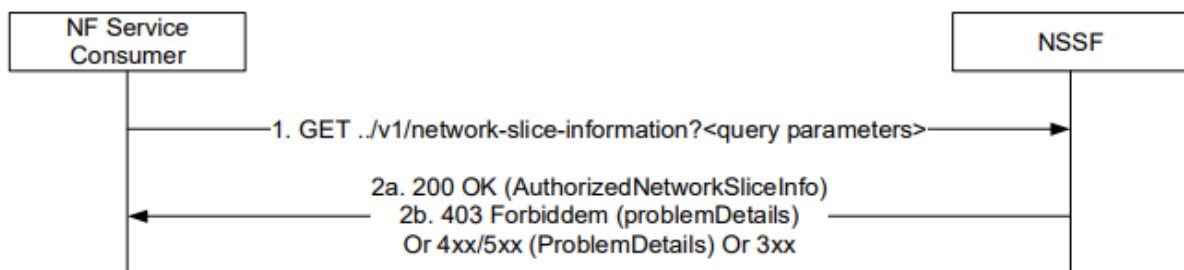


Figure 30 : Schéma d'allocation de NSSAI

NF Service Consumer représente ici l'AMF

étape 2a. : Tranches disponible

étape 2b. : Tranches indisponible ou autres erreurs

Après avoir reçu la sélection de tranches l'AMF assure que l'UE se connecte bien à cette sélection et assure sa préservation tout le long de la session. L'AMF devra ainsi continuellement manager la connexion au gré du mouvement de l'UE en gérant les handovers, il devra alors redemander à la NSSF pour modifier la sélection de tranches.

L'AMF pourra aussi utiliser d'autre services de NSSF pour modifier la S-NSSAI : Mettre à jour, s'abonner, se désabonner, notifier, supprimer ou changer les options.

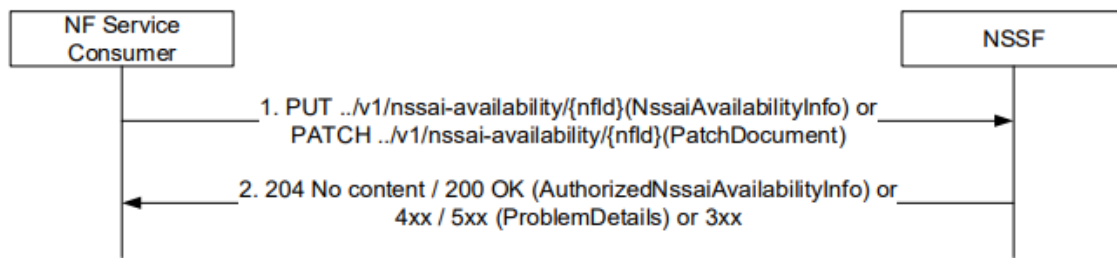


Figure 31 : Schéma de mise à jour de S-NSSAI

Cette allocation est une pierre angulaire de la 5G. L'AMF grâce à NSSF peut allouer dynamiquement les tranches de réseau en assurant la qualité de service et les besoins des utilisateurs liés à leur abonnement.

6.4 AMF et SMF (Session Management Function)

3GPP TS 29.502 version 16.16.0:

-5.2 Nsmf_PDUSession Service

L'interaction AMF et SMF permet de gérer la session des utilisateurs tout le long de leurs sessions. Elle permet de garantir l'établissement, la modification et la libération des sessions des UE, tout en assurant la continuité du réseau tant que l'UE se déplace à travers ce dernier.

SMF s'occupe de gérer les sessions PDU (Protocol Data Unit). Cette gestion inclut alors : l'allocation des adresses IP pour l'UE, Configurer la QoS, gérer le routage du trafic ainsi que sa politique de réseau.

L'UE qui souhaite se connecter au réseau et établir une session de données (PDU), fait une requête à l'AMF qui ce dernier met en place le processus avec l'aide de la SMF, cette communication se fait via l'interface N11.

L'AMF doit alors choisir la SMF approprié, et l'AMF lui envoie alors le S-NSSAI obtenu grâce à la NSSF, le réseau auquel l'UE veut se connecter ainsi que les paramètres de QoS voulue.

SMF crée alors la session, elle : alloue alors une adresse IP pour l'UE, établit avec l'UPF (User Plane Function) une liaison entre données de l'UE et données du réseau et établit les QoS de la session (Selon les besoins de l'UE, latence ou bande passante). L'UE reçoit alors ces informations via l'AMF et peut envoyer et recevoir des données à travers le réseau.

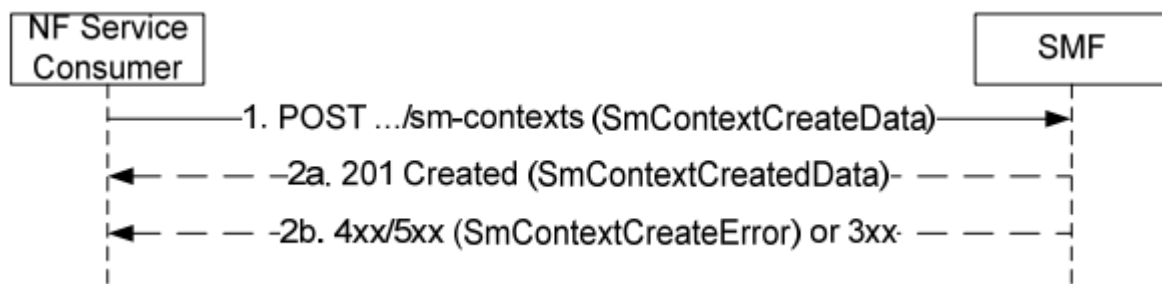


Figure 32 : Schéma Création d'une session de données

La session PDU une fois créer peut alors être modifier par les 3 acteurs:

- UE (changement dans la QoS, besoin d'autre services)
- AMF (Mobilité dans le réseau)
- SMF (Changement dans le réseau)

AMF et SMF continue à communiquer durant toute la session pour garantir la tenue du réseau pour l'UE.

L'AMF gère la mobilité de l'UE et informe la SMF pour assurer que la session PDU reste active et interrompu. Dès que l'AMF détecte que l'UE bouge à travers le réseau (d'une cellule à une autre par exemple) alors l'AMF en notifie la SMF en communiquant sa zone ou l'ID de la cellule pour que ce dernier ajuste le routage de la session de données. SMF doit alors reconfigurer l'UPF pour assurer que le routage soit optimal.

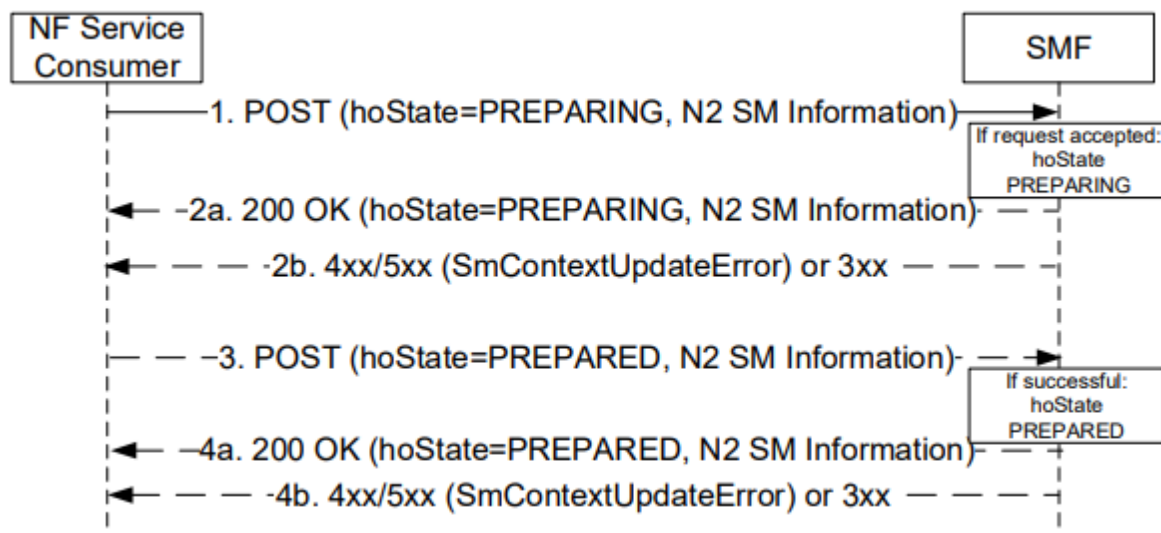


Figure 33 : Schéma Préparation d'un Handover

-AMF demande à la SMF de se préparer (1.), la SMF répond qu'elle est prête (2a.) et l'AMF (3.) exécute le transfert. La SMF répond si c'est bon (4a.).

Cette coordination entre AMF et SMF permet d'assurer que les services d'appel audio ou diffusions vidéo ne soit pas interrompus quand l'UE bouge à travers le réseau.

Quand l'UE n'a plus besoin de la session, elle en informe l'AMF pour que la SMF libère la session. La SMF désalloue alors l'adresse IP, les ressources de QoS et supprime le chemin entre l'UE et l'UPF de la session.

L'interaction entre AMF et SMF est essentielle pour gérer les sessions PDU. Elle permet d'assurer les mouvements de l'UE dans le réseau en maintenant le routage et la configuration de la session. Elle permet ainsi une connexion sans coupure même si l'UE se déplace.

6.5 AMF et PCF (Policy Control Function)

3GPP TS 29.513 version 16.13.0:

-5.1 AM Policy Association Management

-5.6 UE Policy Association Management

L'interaction AMF et PCF garantit que les sessions utilisateurs sont configurées et gérées conformément aux politiques réseaux définies, y compris celle liées à l'allocation des ressources, à la QoS et à la facturation.

PCF contrôle et applique les politiques liées à la qualité du service (QoS), la facturation et la gestion des ressources.

Quand l'UE souhaite établir une session PDU, elle envoie une requête à l'AMF. L'AMF fait alors une demande des politiques réseaux à la PCF, et envoie les données de l'UE tel que : son ID, le service demandé, et les détails de la session.

PCF évalue alors cette demande et détermine la politique du réseau basé sur le type d'abonnement, le type de service et la condition du réseau (Utilise les données de l'UDR). Cette politique contient alors : les paramètres QoS (Bande Passante, Latence et priorité de la session), les règles de facturation et les conditions d'accès au réseau.

Elle renvoie ces informations à l'AMF qui devra alors les appliquer : par exemple elle applique les paramètres QoS en se coordonnant avec la SMF et initie la session avec l'UE.

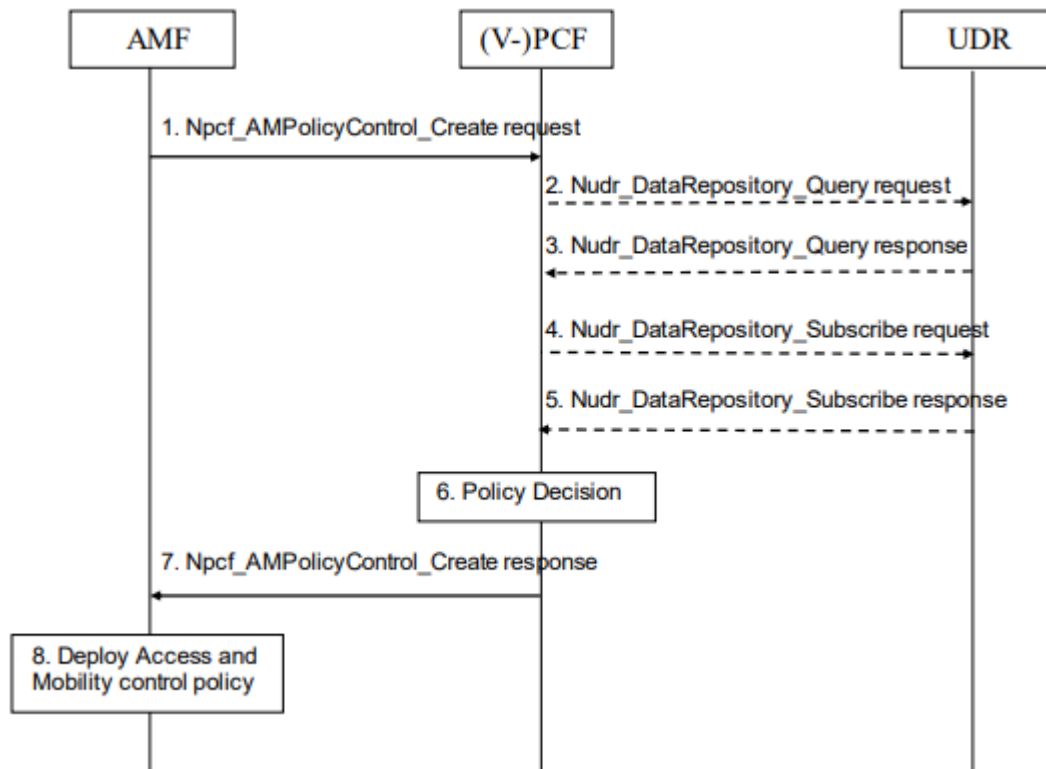


Figure 34 : Schéma Etablissement d'une politique

-L'AMF fait une demande à la PCF (1.) et PCF communique avec l'UDR (2. - 5.) pour connaître les données de l'utilisateur et choisit la politique en fonctions des données (6.). Elle renvoie alors la politique (7.) et l'AMF l'applique (8.).

L'AMF lorsque l'UE change de point d'accès envoie une requête à la PCF notifiant la nouvelle localisation. La PCF réévalue alors les politiques, en ajustant les paramètres ou les accès. L'AMF reçoit ses données afin de gérer les handovers.

L'AMF peut aussi indépendamment demander une mise à jour de la politique s'il y a des problèmes dans le réseau ou une demande de service.

Lorsqu'une session se termine l'AMF l'indique à la PCF afin de libérer les ressources.

Grâce aux données fournis par la PCF, l'AMF applique les politiques de qualité de service et de facturation garantissant une prestation de services et une gestion de ressources optimales tout en respectant les contraintes du réseau.

6.6 AMF et NRF (Network Repository Function)

3GPP TS 29.510 version 16.15.0:

-5.2 Nnrf_NFManagement Service

-5.3 Nnrf_NFDiscovery

L'interaction AMF et NRF est crucial car elle permet de découvrir les services, l'enregistrement des NF et la gestion dynamique des ressources.

NRF sert comme dépôt centralisé pour les NF, permettant alors à l'AMF et aux autres NF de se découvrir et de communiquer ensemble. Cela permet alors à l'AMF de localiser et d'interagir dynamiquement avec les autres NF (SMF, AUSF, UDM...) en temps réels.

L'AMF communique alors avec la NRF pour:

- Découvrir les NF disponibles qui sont nécessaires pour les sessions d'utilisateurs
- S'enregistre auprès de la NRF pour se dire prêt et disponibles pour être utilisés par les autres NF

Cela permet d'assurer la flexibilité et le service continu du réseau 5G.

Pour se connecter, l'AMF communique son ID et ses capacités. Après l'enregistrement la NRF confirme que l'AMF peut être découvert par d'autre NF.

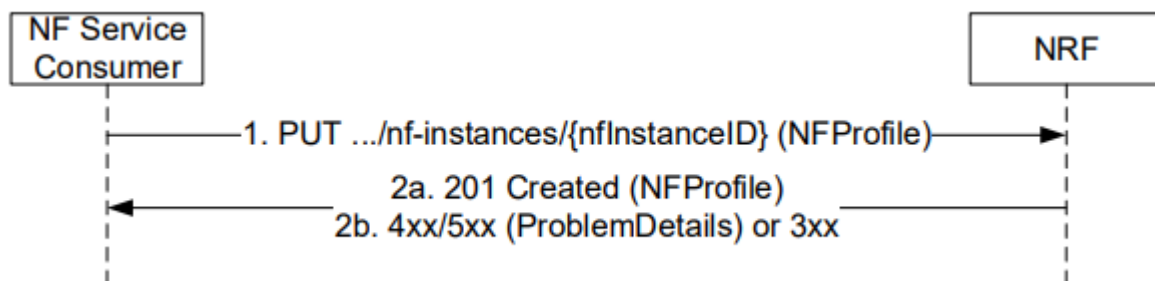


Figure 35 : Schéma d'enregistrement d'une NF

Après son enregistrement, l'AMF peut faire une requête pour trouver une NF en envoyant le type de NF recherché et les exigences demandés.

NRF cherche alors dans son répertoire les NF qui répondent à ses critères et les renvoie à l'AMF avec leur ID, localisation et capacités.

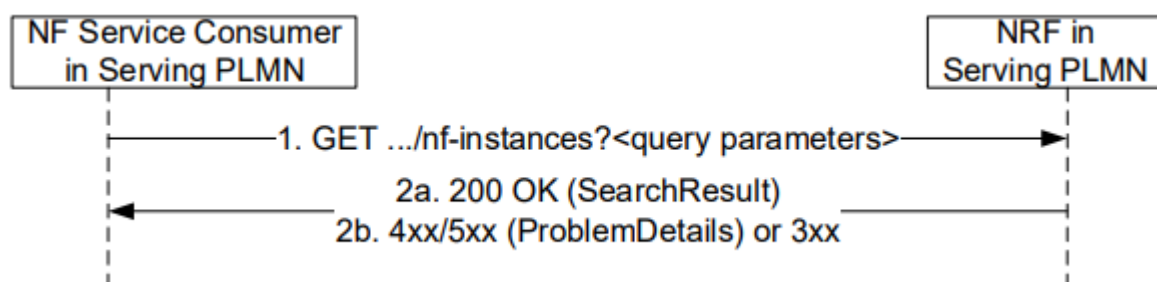


Figure 36 : Schéma de requête de découverte de services.

L'AMF peut aussi demander à la NRF si les NF découvertes sont encore disponibles ou fonctionnelles.

L'interaction entre l'AMF (ou une autre NF) et la NRF est un élément fondamental de l'architecture du réseau 5G, la découverte dynamique et l'interaction avec d'autres fonctions de manière flexible permet au réseau de s'adapter à la mobilité des

utilisateurs, aux changements de demandes de services et des conditions de réseaux et d'assurer de manière optimal les performances et l'allocation de ressource dans la 5G.

6.7 AMF et NEF (Network Exposure Function)

3GPP TS 29.522:

-4. NEF Northbound Interface

L'interaction AMF et NEF permet aux applications externes et les services tiers d'accéder et d'interagir de manière sécurisée avec les NF et données d'un utilisateur.

NEF agit comme un intermédiaire avec les parties externe comme les applications de développeurs, les fournisseurs de services tiers ou bien les plateformes IoT. Il expose le réseau via des APIs allouant donc les entités externes d'utiliser les services fournis par le réseau.

Ces applications peuvent récupérer les données via l'AMF : les activités de données de l'UE, les données de sa session, sa localisation ou bien les paramètres QoS de l'UE.

Les applications donnent à l'AMF l'ID de l'UE et les données qu'elles souhaitent et l'AMF renvoie ces données. Ces applications peuvent aussi modifier ou gérer la session de données et les paramètres QoS.

Cette interaction est donc fondamentale pour les applications externes. NEF agit comme un intermédiaire sécurisé et permettant des services aux applications externes au réseau : accès aux données, localisation, paramètres QoS et sessions de données. Elle est essentielle pour permettre à une large gamme de services et d'applications, de l'IoT aux services géolocalisés d'utiliser le réseau 5G tout en garantissant son efficacité et sa sécurité.

7. Etude de marché

7.1 Le marché en général de la 5G

<https://informationmatters.net/5g-wireless-market-size-forecasts/>

Le marché de la 5G au-delà d'être une révolution dans le domaine des télécommunications, elle est une révolution mondiale dans plusieurs domaines. Elle va changer de nombreuses facettes actuelles en révolutionnant les industries, créer de nouveaux business, améliorer les soins de santé, tout en embellissant les services aux particuliers.

Tout cela est permis aux nouvelles technologies implémentées qui donne aux réseaux des vitesses de données ultra rapides, une latence de plus en plus faible, une connectivité de plus en plus massive tout en ayant une meilleure fiabilité du réseau.

De nombreux domaines s'y intéressent :

- Industrie automobile (Voitures autonomes)
- Hôpitaux (Chirurgie à Distance)
- Gouvernement (Croissance économique)

C'est donc un intérêt quasi général qui explique ainsi la croissance exponentielle du marché de la 5G : le marché représente en 2023 environ 100 milliards \$ et pourrait atteindre 1000 milliards \$ en 2030. On estime qu'en 2028, 5 milliards d'abonnements téléphonique seront en 5G, soit plus de la moitié.

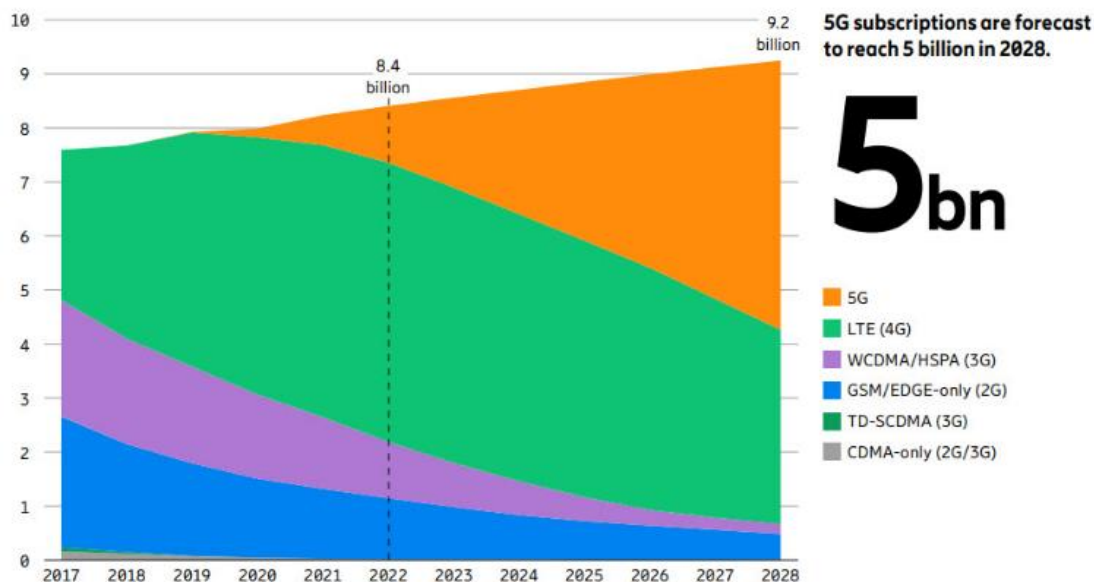


Figure 37 : Nombre d'utilisateurs par technologie

Le marché a une plus grande importance en Amérique du Nord en Europe mais surtout en Asie et particulièrement la Chine la Corée du Sud et le Japon.

7.2 Les acteurs du marché de la 5G

Les entreprises sur le marché de la 5G est segmentés en plusieurs parties :

- Composants (Hardware, Software, Services)
- Applications (Applications grand public, smart homes, voiture connectée, domaine médical)

-Autre utilisations (Industrie, Télécommunications et opérateurs mobiles, Streaming, Cloud gaming, Réalité Virtuelle)

Historiquement la 5G est portée par des entreprises chinoises spécialisées dans les équipements de télécommunications : Huawei et ZTE. Elles sont aidées par Ericsson (entreprise suédoise), avec la collaboration du plus grand opérateur du monde en termes d'utilisateurs China Mobile.

D'autres entreprises ont alors pris ce marché : Nokia (Finlande), Samsung (Corée du Sud), NEC ou Nichiden (Japon), Mavenir (USA). Elles travaillent de pair avec les opérateurs téléphoniques comme Verizon, AT&T, SK Telecom, NTT DoCoMo, Orange, Vodafone... Il y a aussi les entreprises de semi-conducteur qui sont indispensables pour ce marché : Intel, Nvidia, Qualcomm, Broadcom...

D'autres entreprises privées s'intéressent à la 5G et vendent des services liés à cette technologie :

-Les voitures autonomes avec Tesla en fer de lance mais il existe d'autres acteurs comme BMW. L'AMF a une grande place dans ce domaine car il est primordial d'avoir une bonne gestion de la mobilité pour une voiture connectée. La 5G peut être aussi installée de manière privée dans les usines.

-Amazon a des services qui utilisent la 5G comme Wavelength : elle permet de construire des applications avec une très faible latence car stockée avec AWS, elle est à la pointe du réseau 5G. Amazon propose aussi une 5G privée nommée AWS Private 5G qui permet de connecter facilement une entreprise à son propre réseau 5G. Amazon s'intéresse aussi aux Smart Cities et propose ses services avec AWS (permet une meilleure gestion de la ville avec le trafic ou l'éclairage).

-Microsoft propose aussi des réseaux privés de 5G, et intègre aussi la 5G dans son cloud Computing avec Azure

-Google propose aussi des services similaires avec Google Cloud

La 5G est un immense marché composé de nombreux acteurs qui peuvent être en concurrence ou en coopération. Maîtriser la 5G peut alors ouvrir de nombreuses voies professionnelles, que ce soit dans le côté hardware ou software, dans les entreprises de télécommunications ou bien entreprises de services (Cloud Computing, réseau privé 5G) et enfin dans les différentes industries de divertissement, médical ou bien automobile

8. Conclusion

La technologie 5G marque une avancée majeure, offrant des vitesses améliorées, une latence réduite et une connectivité massive pour des applications telles que l'IoT et les véhicules autonomes. Au cœur de cette architecture, la fonction AMF joue un rôle crucial dans la gestion des utilisateurs, de la mobilité et des connexions.

L'AMF s'intègre dans l'architecture basée sur les services (SBA) de la 5G, utilisant des APIs RESTful basées sur HTTP/2 pour communiquer efficacement avec d'autres fonctions du cœur de réseau.

Dans ce rapport, nous avons introduit le réseau 5G, ses cas d'utilisations, technologies et fonctions réseau.

9. Bibliographie

Archi 5G : 3GPP TS 23.501 version 16.20.0

Procedures 5G : 3GPP TS 23.502 version 16.19.0

AMF : 3GPP TS 29.518 version 16.16.0

AUSF : 3GPP TS 29.509 version 16.10.0

UDM : 3GPP TS 29.503 version 16.16.0

NSSF : 3GPP TS 29.531 version 16.10.0

SMF : 3GPP TS 29.502 version 16.16.0

PCF : 3GPP TS 29.513 version 16.13.0

NRF : 3GPP TS 29.510 version 16.15.0

NEF : 3GPP TS 29.522 version 16.17.0

Les Services de l'AMF (Chapitre 5, page 18 à 61) : **AMF : 3GPP TS 29.518 version 16.16.0**

Définition des Services : <https://documentation.nokia.com/mag-c/23-10-1/books/cpf/service-based-interfaces.html>

N1N2MessageTransfer:

https://www.cisco.com/c/en/us/td/docs/wireless/ucc/amf/2021-04/config-and-admin/b_ucc-5g-amf-config-and-admin-guide_2021-04/m_n1n2messagetransfer.pdf