Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2760

(05/2011)

SÉRIE Y: INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE PROCHAINE GÉNÉRATION

Réseaux de prochaine génération – Sécurité

Cadre de sécurité pour la mobilité dans les réseaux de prochaine génération

Recommandation UIT-T Y.2760

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE PROCHAINE GÉNÉRATION

INFRASTRUCTURE MONDIALE DE L'INFORMATION	
Généralités	Y.100–Y.199
Services, applications et intergiciels	Y.200–Y.299
Aspects réseau	Y.300–Y.399
Interfaces et protocoles	Y.400–Y.499
Numérotage, adressage et dénomination	Y.500–Y.599
Gestion, exploitation et maintenance	Y.600–Y.699
Sécurité	Y.700–Y.799
Performances	Y.800–Y.899
ASPECTS RELATIFS AU PROTOCOLE INTERNET	
Généralités	Y.1000–Y.1099
Services et applications	Y.1100–Y.1199
Architecture, accès, capacités de réseau et gestion des ressources	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interfonctionnement	Y.1400–Y.1499
Qualité de service et performances de réseau	Y.1500–Y.1599
Signalisation	Y.1600–Y.1699
Gestion, exploitation et maintenance	Y.1700–Y.1799
Taxation	Y.1800–Y.1899
Télévision IP sur réseaux de prochaine génération	Y.1900–Y.1999
RÉSEAUX DE PROCHAINE GÉNÉRATION	
Cadre général et modèles architecturaux fonctionnels	Y.2000–Y.2099
Qualité de service et performances	Y.2100–Y.2199
Aspects relatifs aux services: capacités et architecture des services	Y.2200–Y.2249
Aspects relatifs aux services: interopérabilité des services et réseaux dans les réseaux de prochaine génération	Y.2250–Y.2299
Numérotage, nommage et adressage	Y.2300–Y.2399
Gestion de réseau	Y.2400–Y.2499
Architectures et protocoles de commande de réseau	Y.2500–Y.2599
Réseaux de transmission par paquets	Y.2600–Y.2699
Sécurité	**Y.2700–Y.2799**
Mobilité généralisée	Y.2800–Y.2899
Environnement ouvert de qualité opérateur	Y.2900–Y.2999
RÉSEAUX FUTURS	Y.3000–Y.3499
INFORMATIQUE EN NUAGE	Y.3500–Y.3999

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T Y.2760

Cadre de sécurité pour la mobilité dans les réseaux de prochaine génération

Résumé

La Recommandation UIT-T Y.2720 définit le cadre de sécurité pour la mobilité dans la strate de transport des réseaux de prochaine génération (NGN, *net génération network*). Elle traite des spécifications, des mécanismes ainsi que des procédures de sécurité pour la gestion et la commande de la mobilité dans les réseaux NGN.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T Y.2760	2011-05-20	13

Mots clés

NGN, sécurité pour la mobilité.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T Y.2760

Cadre de sécurité pour la mobilité dans les réseaux de prochaine génération

1 Domaine d'application

La présente Recommandation décrit le cadre de sécurité pour la mobilité dans la strate de transport des réseaux de prochaine génération (NGN, *next generation network*). S'appuyant sur les spécifications de sécurité présentées dans [UIT-T Y.2018], elle porte sur l'authentification et la gestion des clés, l'établissement d'un contexte de sécurité, la sécurité pour la mobilité IP et la sécurité de la gestion et de la commande de la mobilité ainsi que des fonctions de transport dans la strate de transport. Les scénarios traités dans la présente Recommandation incluent la mobilité intratechnologie et intertechnologies, ainsi que la mobilité intradomaine et interdomaines.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T Q.1706] Recommandation UIT-T Q.1706/Y.2801 (2006), *Prescriptions de gestion de la mobilité pour les réseaux de prochaine génération.*

[UIT-T X.805] Recommandation UIT-T X.805 (2003), *Architecture de sécurité pour les systèmes assurant des communications de bout en bout.*

[UIT-T Y.2011] Recommandation UIT-T Y. 2011 (2004), *Principes généraux et modèle de référence général pour les réseaux de prochaine génération*.

[UIT-T Y.2012] Recommandation UIT-T Y.2012 (2010), *Prescriptions et architecture fonctionnelles du réseau de prochaine génération.*

[UIT-T Y.2014] Recommandation UIT-T Y.2014 (2010), *Fonctions de commande de rattachement au réseau dans les réseaux de prochaine génération.*

[UIT-T Y.2018] Recommandation UIT-T Y.2018 (2009), *Cadre général et architecture de gestion et de commande de la mobilité dans la strate de transport des réseaux NGN.*

[UIT-T Y.2701] Recommandation UIT-T Y.2701 (2007), *Prescriptions de sécurité des réseaux de prochaine génération de version 1*.

[UIT-T Y.2704] Recommandation UIT-T Y.2704 (2010), *Mécanismes et procédures de sécurité des réseaux NGN.*

[UIT-T Y-Sup.7] Recommandations UIT-T de la série Y – Supplément 7 (2008), *Série UIT-T Y.2000 – Supplément sur le domaine d'application de la version 2 des NGN*.

[UIT-R M.1645] Recommandation UIT-R M.1645 (2003), *Cadre et objectifs d'ensemble du développement futur des IMT-2000 et des systèmes postérieurs aux IMT-2000.*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 transfert intercellulaire (§ 6.2.2 de [UIT-T Q.1706]): capacité de fournir des services avec une certaine incidence sur les accords de niveau de service pour un objet en mouvement pendant et après un déplacement.

3.1.2 mobilité horizontale (§ 6.2.3 de [UIT-T Q.1706]): mobilité dans la même couche, suivant la définition donnée dans [UIT-R M.1645]; on parle en général de mobilité à l'intérieur de la même technologie d'accès.

3.1.3 mobilité (§ 3.2 de [UIT-T Q.1706]): capacité de l'utilisateur, ou d'autres entités mobiles, de communiquer et d'accéder à des services indépendamment de leurs déplacements ou de leur environnement technique.

3.1.4 strate de transport du réseau de prochaine génération (§ 3.10 de [UIT-T Y.2011]): partie du réseau NGN assurant les fonctions, destinées à l'utilisateur, de transfert de données, ainsi que les fonctions de commande et de gestion des ressources de transport, de sorte que ces données puissent être acheminées entre les entités de terminaison.

3.1.5 confiance (§ 3.2.9 de [UIT-T Y.2701]): on dit que l'entité X fait confiance à l'entité Y pour un ensemble d'activités si et seulement si l'entité X suppose que l'entité Y se comportera d'une certaine façon par rapport aux activités.

3.1.6 mobilité verticale (§ 6.2.3 de [UIT-T Q.1706]): mobilité entre différentes couches selon la définition donnée dans [UIT-R M.1645]; on parle en général de mobilité entre différentes technologies d'accès.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 mobilité intertechnologies: voir "mobilité verticale" au § 3.1.

3.2.2 mobilité intratechnologie: voir "mobilité horizontale" au § 3.1.

3.2.3 contexte de sécurité: ensemble de paramètres de sécurité comprenant l'identificateur, les données de clé, l'algorithme de clé, etc.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

3G troisième génération

ABG-FE entité fonctionnelle de passerelle périphérique d'accès *(access border gateway functional entity)*

AE extension d'authentification *(authentication extension)*

AKA authentification et accord de clé (*authentication and key agreement*)

AM-FE entité fonctionnelle de gestion d'accès (*access management functional entity*)

AN-FE entité fonctionnelle de nœud d'accès *(access node functional entity)*

ANI interface application-réseau (*application to network interface*)

AR-FE entité fonctionnelle de relais d'accès (*access relay functional entity*)

DDoS déni de service réparti (*distributed denial of service*)

EAP protocole d'authentification extensible (*extensible authentication protocol*)

EN-FE entité fonctionnelle de nœud d'extrémité (*edge node functional entity*)

FA agent étranger *(foreign agent)*

HA agent de rattachement *(home agent)*

HDC-FE entité fonctionnelle de commande de décision de transfert intercellulaire *(handover decision control functional entity)*

IP protocole Internet (*Internet protocol*)

L3HEF fonction d'exécution de transfert intercellulaire de couche 3 *(layer 3 handover execution function)*

MIP IP mobile *(mobile IP)*

MIPv4 IP mobile pour la version 4 du protocole Internet *(mobile IP for IP version 4*). Voir [b-IETF RFC 3220]

MIPv6 IP mobile pour la version 6 du protocole Internet *(mobile IP for IP version 6*). Voir [b-IETF RFC 3775]

MLM-FE entité fonctionnelle de gestion de localisation de mobilité (*mobility location management functional entity*)

MMCF fonctions de commande de gestion de la mobilité (*mobility management control functions*)

MN nœud mobile *(mobile node)*

MOBIKE protocole de mobilité et rattachement multiple IKEv2 (*IKEv2 mobility and multihoming protocol)*. Voir [b-IETF RFC 4555]

NACF fonctions de commande de rattachement au réseau (*network attachment control functions*)

NGN réseau de prochaine génération (*next generation network*)

NID-FE entité fonctionnelle de distribution des informations de réseau (*network information distribution functional entity*)

NNI interface réseau-réseau (*network to network interface*)

PKI infrastructure de clé publique (*public key infrastructure*)

PMIPv6 protocole IPv6 pour proxy mobile (*proxy mobile IPv6*). Voir [b-IETF RFC 5213]

RAN réseau d'accès radio (*radio access network*)

RRP réponse d'enregistrement (*registration reply*)

RRQ demande d'enregistrement (*registration request*)

TAA-FE entité fonctionnelle d'authentification et d'autorisation de transport (*transport authentication and authorization functional entity*)

TLM-FE entité fonctionnelle de gestion de localisation de transport (*transport location management functional entity*)

TLS sécurité dans la couche transport (*transport layer security*)

TTLS sécurité dans la couche transport avec tunnellisation (*tunnelled transport layer security*)

TUP-FE entité fonctionnelle de profil d'utilisateur de transport (*transport user profile functional entity*)

UE équipement d'utilisateur (*user equipment*)

UNI interface utilisateur-réseau (*user to network interface*)

WiMax interopérabilité mondiale des accès hyperfréquence (*worldwide interoperability for microwave access*)

WLAN réseau local sans fil (*wireless LAN*)

5 Spécifications de sécurité pour la mobilité dans les NGN

Les NGN prennent en charge plusieurs technologies d'accès, par exemple les technologies WLAN, WiMax et RAN 3G [UIT-T Y.2012]. Au nombre de leurs fonctionnalités, on trouve la prise en charge de la mobilité, qui comprend le nomadisme et le transfert intercellulaire. Dans le cas des NGN de version 2, le transfert intercellulaire peut avoir lieu entre réseaux d'accès ou à l'intérieur d'un réseau d'accès [UIT-T Y-Sup.7].

Les NGN prennent en charge les fonctionnalités suivantes:

1) Modèle de confiance: le modèle de confiance pour la sécurité des NGN définit trois zones de sécurité: la zone de confiance, la zone de confiance mais vulnérable et la zone non fiable [UIT-T Y.2701]. Selon ce modèle, le réseau d'accès doit passer par une passerelle de sécurité avant d'accéder au réseau central.

2) Les NGN prennent en charge plusieurs technologies d'accès.

3) Les NGN prennent en charge plusieurs protocoles de mobilité, par exemple MIPv4, MIPv6, DSMIPv6, PMIPv6 et MOBIKE.

4) Les NGN prennent en charge plusieurs équipements UE radioélectriques, par exemple WLAN, WiMax, RAN 3G, etc.

5) Les NGN assurent la continuité du service en cas de transfert intercellulaire entre des systèmes d'accès hétérogènes.

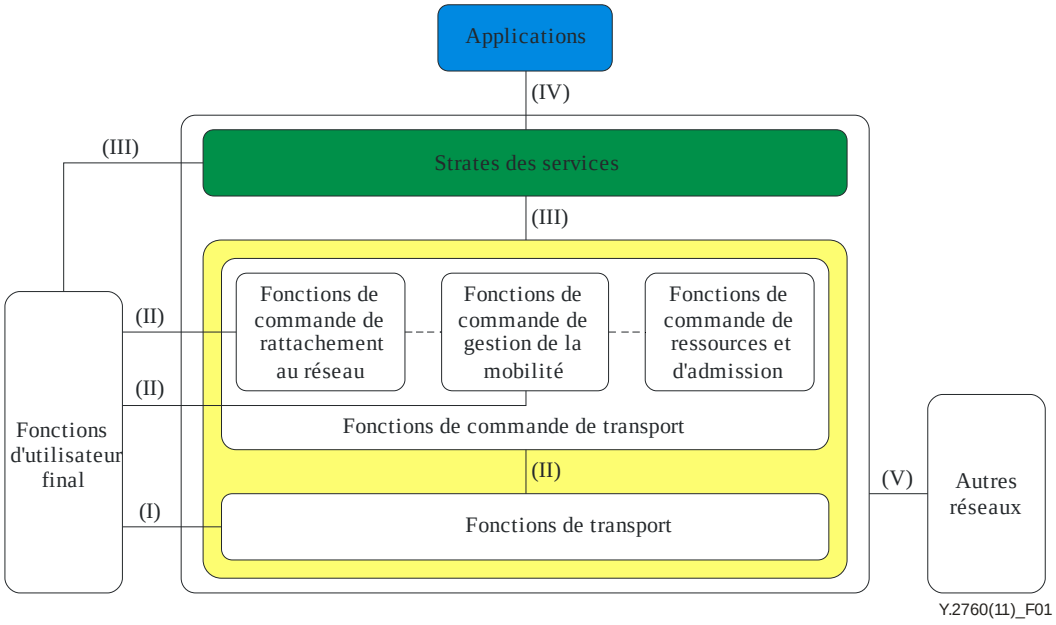

Figure 1 – Architecture de sécurité pour la mobilité dans les NGN

Cinq groupes de fonctionnalités de sécurité sont définis pour:

(I) Assurer la sécurité dans la couche de transport entre les fonctions d'utilisateur final et les fonctions de transport, comme la sécurité de l'accès qui peut être assurée de façon physique ou logique entre fonctions d'utilisateur final, et l'entité du réseau d'accès dans les fonctions de transport. I) concerne également la sécurité de l'interface UNI entre les fonctions d'utilisateur final et les fonctions de transport.

(II) Assurer la sécurité dans la couche de commande entre les fonctions d'utilisateur final et l'entité fonctionnelle de commande de transport. II) s'occupe également de la sécurité dans l'interface des messages de commande entre l'entité fonctionnelle de transport et l'entité fonctionnelle de commande de transport. II) concerne la sécurité de l'interface UNI entre les fonctions d'utilisateur final et les fonctions de commande de transport.

(III) Assurer la sécurité de l'interface entre les fonctions d'utilisateur final et la strate des services. III) s'occupe également de la sécurité dans l'interface des messages de commande entre l'entité fonctionnelle de commande de transport et la strate des services. III) concerne la sécurité de l'interface UNI entre les fonctions d'utilisateur final et la strate des services.

(IV) Assurer la sécurité de l'interface entre la strate des services et les applications. IV) concerne la sécurité de l'interface ANI entre les fonctions d'utilisateur final et les fonctions de transport.

(V) Assurer la sécurité de l'interface entre le réseau NGN et d'autres réseaux, dans la couche de transport et dans la couche de commande. V) concerne la sécurité de l'interface NNI entre le réseau NGN et d'autres réseaux.

Les principes énoncés dans [UIT-T X.805] s'appliquent aux menaces de sécurité et aux spécifications de sécurité identifiées dans la présente Recommandation.

5.1 Menaces de sécurité

Les menaces de sécurité ci-après sont identifiées dans [UIT-T Y. 2018]:

T1 L'équipement UE peut perdre son autorisation d'entamer la signalisation de la mobilité avec l'entité MLM-FE.

T2 La signalisation de la mobilité peut être falsifiée par des intrus.

T3 L'identité de l'entité MLM-FE peut être usurpée dans le but de fournir des informations erronées à l'équipement UE.

T4 Des intrus peuvent repérer l'emplacement de l'équipement UE.

T5 Une attaque par redirection du trafic peut se produire.

T6 L'attaquant peut se placer sur le trajet grâce à une attaque de l'homme du milieu.

T7 Une attaque par déni de service réparti peut consommer une partie importante des ressources de réseau.

T8 L'équipement UE peut perdre son autorisation d'obtenir des informations auprès de l'entité HDC-FE ou NID-FE.

T9 L'identité de l'entité HDC-FE ou de l'entité NID-FE peut être usurpée dans le but de transmettre des informations erronées à l'équipement UE.

T10 La signalisation entre l'équipement UE et l'entité HDC-FE ou l'entité NID-FE peut être modifiée ou interceptée.

T11 Les données du plan d'utilisateur peuvent être interceptées ou modifiées.

5.2 Spécifications de sécurité

Les spécifications de sécurité ci-après sont identifiées dans [UIT-T Y. 2018]:

R1 L'équipement UE et l'entité NID-FE doivent s'authentifier mutuellement.

R2 L'intégrité et la confidentialité de la signalisation entre l'équipement UE et l'entité MLM-FE doivent être protégées.

R3 La signalisation entre l'équipement UE et l'entité MLM-FE doit être protégée contre les attaques par répétition.

R4 La confidentialité de l'emplacement de l'équipement UE doit être assurée.

R5 L'équipement UE et l'entité HDC-FE doivent s'authentifier mutuellement.

R6 L'intégrité et la confidentialité de la signalisation entre l'équipement UE et l'entité HDC-FE doivent être protégées.

R7 La signalisation entre l'équipement UE et l'entité HDC-FE doit être protégée contre les attaques par répétition.

R8 Il faut assurer une authentification à faible temps de latence et la protection de la signalisation.

R9 Le transfert du contexte de sécurité doit être optimisé.

R10 La solution de sécurité pour la mobilité ne doit pas dépendre du support.

R11 Des mécanismes doivent permettre de protéger le trafic dans le plan d'utilisateur entre l'équipement UE et l'entité EN-FE lorsque le profil d'utilisateur le demande.

Outre les spécifications de sécurité identifiées dans [UIT-T Y.2018], il faut également tenir compte de la spécification de sécurité suivante:

R12 La sécurité doit également être prise en charge en cas de connexions multiples.

6 Fonctionnalités de sécurité prises en charge par les différentes entités fonctionnelles

Les entités fonctionnelles liées à la sécurité de la mobilité dans les NGN sont les suivantes:

- Entité fonctionnelle de profil d'utilisateur de transport (TUP-FE)
- Entité fonctionnelle d'authentification et d'autorisation de transport (TAA-FE)
- Entité fonctionnelle de gestion de localisation de mobilité (MLM-FE)
- Entité fonctionnelle de commande de décision de transfert intercellulaire (HDC-FE)
- Entité fonctionnelle de distribution des informations de réseau (NID-FE)
- Entité fonctionnelle de gestion d'accès (AM-FE)
- Fonction d'exécution de transfert intercellulaire de couche 3 (L3HEF)
- Entité fonctionnelle de nœud d'accès (AN-FE).

6.1 Entité fonctionnelle de profil d'utilisateur de transport (TUP-FE)

L'entité fonctionnelle TUP-FE stocke les données d'authentification de l'abonnement, telles que les données de clé, les méthodes d'authentification et le profil d'utilisateur de transport. Les fonctions de l'entité TUP-FE sont décrites en détail dans [UIT-T Y.2014].

6.2 Entité fonctionnelle d'authentification et d'autorisation de transport (TAA-FE)

L'entité fonctionnelle TAA-FE extrait les données d'authentification et accède aux informations d'autorisation auprès de l'entité TUP-FE. Elle peut également faire office de proxy.

Les fonctions de cette entité sont décrites en détail dans [UIT-T Y.2014].

6.3 Entité fonctionnelle de gestion de localisation de mobilité (MLM-FE)

L'entité fonctionnelle MLM-FE obtient les informations d'authentification, d'autorisation et de comptabilité auprès de la fonction NACF, effectue l'authentification mutuelle avec l'équipement UE et crée une association de sécurité entre elle et l'équipement UE. Les fonctions de cette entité sont décrites en détail dans [UIT-T Y.2018].

6.4 Entité fonctionnelle de commande de décision de transfert intercellulaire (HDC-FE)

L'entité fonctionnelle HDC-FE est nécessaire pour établir une association de sécurité avec l'équipement UE; cette entité obtient la clé de sécurité utilisée pour l'association de sécurité auprès de l'entité TAA-FE via l'entité TLM-FE. Les fonctions de cette entité sont décrites en détail dans [UIT-T Y.2018].

6.5 Entité fonctionnelle de distribution des informations de réseau (NID-FE)

L'entité fonctionnelle NID-FE est nécessaire pour établir une association de sécurité avec l'équipement UE dans le but de protéger des informations telles que les informations de sélection du réseau. Elle peut obtenir des informations de sécurité auprès de l'entité TAA-FE via l'entité TLM-FE. Les fonctions de cette entité sont décrites en détail dans [UIT-T Y.2018].

6.6 Entité fonctionnelle de gestion d'accès (AM-FE)

L'entité fonctionnelle AM-FE réexpédie les demandes d'accès au réseau à l'entité TAA-FE afin d'authentifier l'utilisateur, d'autoriser ou de refuser l'accès au réseau et d'extraire les paramètres de configuration de l'accès propres à l'utilisateur. Elle peut réutiliser les données d'enregistrement/d'authentification du réseau pour rétablir rapidement la connexion sans effectuer à nouveau la totalité de la procédure d'enregistrement/d'authentification/de configuration. Les fonctions de cette entité sont décrites en détail dans [UIT-T Y.2014].

6.7 Fonction d'exécution de transfert intercellulaire de couche 3 (L3HEF)

La fonction L3HEF est nécessaire pour établir une association de sécurité avec l'équipement UE en vue de protéger le trafic échangé entre cette entité et l'équipement. Les fonctions de cette entité sont décrites en détail dans [UIT-T Y.2018].

NOTE – La sécurité de la fonction L3HEF correspond à la spécification de sécurité consistant à assurer la protection du trafic dans le plan d'utilisateur entre l'équipement UE et l'entité EN-FE.

6.8 Entité fonctionnelle de nœud d'accès (AN-FE)

L'entité fonctionnelle AN-FE est nécessaire pour établir une association de sécurité avec l'équipement UE; elle obtient la clé de sécurité auprès de l'entité TAA-FE via l'entité AM-FE. Les fonctions de cette entité sont décrites en détail dans [UIT-T Y.2018].

7 Gestion des clés et authentification

7.1 Cadre de gestion des clés

On utilise un mécanisme de calcul de clés hiérarchiques pour assurer la sécurité de la mobilité dans les NGN. Il existe plusieurs types de données de clé dans les NGN, par exemple, la clé racine, la clé de session, etc. La clé racine est un type de justificatif à long terme qui est stocké de façon sécurisée (par exemple, clé secrète partagée ou mot de passe). La clé de session est un type de données de clé à court terme obtenue à partir de la clé racine. L'équipement UE et l'entité chargée de l'authentification dans les NGN (par exemple, l'entité TAA-FE/TUP-FE) stockent tous deux la clé racine partagée.

En règle générale, les données de clé de session sont obtenues à partir de la clé racine et d'autres paramètres de calcul des clés, comme les informations de négociation pendant la procédure d'authentification. Les données de clé de session servent à protéger le trafic de signalisation et le trafic d'utilisateur. D'autres clés peuvent être obtenues à partir de la clé de session. Le mécanisme de calcul des clés dépend de l'algorithme cryptographique ou du protocole utilisé.

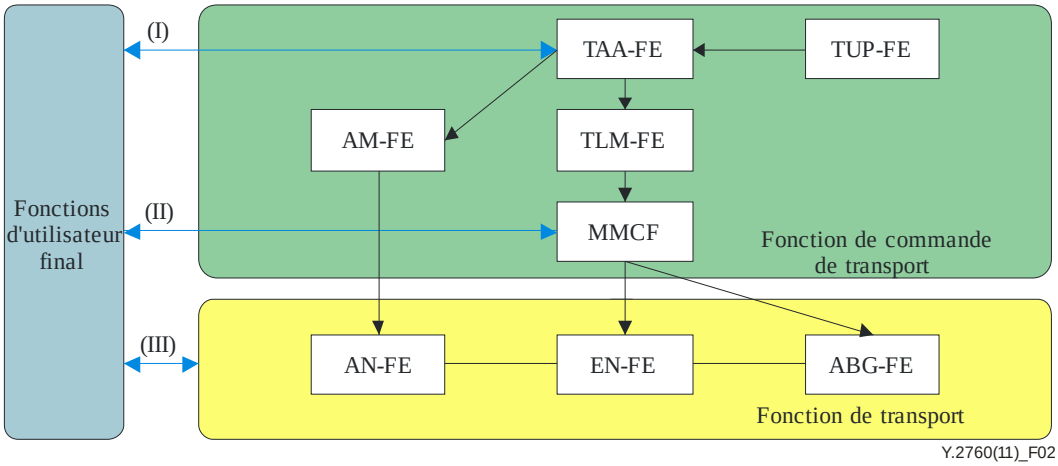

Figure 2 – Cadre générique de calcul des clés de sécurité pour la mobilité dans les NGN

Le cadre générique de calcul des clés de sécurité pour la mobilité dans les NGN est le suivant:

(I) L'équipement UE effectue la procédure d'authentification mutuelle avec les entités fonctionnelles du réseau NGN. Dans ce cadre, l'entité TUP-FE génère, à partir des données de clé racine, des vecteurs d'authentification qu'elle envoie à l'entité TAA-FE. Une fois la procédure d'authentification mutuelle menée à bien, l'entité TAA-FE et l'équipement UE génèrent les données de clé de session, lesquelles peuvent être utilisées pour calculer des données de clé de sous-session. Les données de clé de session sont transférées aux entités fonctionnelles, par exemple l'entité AM-FE ou la fonction MMCF. L'entité AM-FE et la fonction MMCF peuvent toutes deux générer des données de clé de sous-session à partir des données de clé de session reçues.

(II) Les associations de sécurité pour des points de référence situés entre l'équipement UE et la fonction MMCF reposent sur les données de clé de session fournies par l'entité TAA-FE via l'entité TLM-FE. Les données de clé de session utilisées dans l'étape II) sont obtenues ou calculées à partir des données de clé de session dans l'entité TAA-FE.

(III) Les associations de sécurité entre l'équipement UE et la couche des fonctions de transport du réseau NGN sont établies sur la base des données de clé partagée obtenues à partir des données de clé de session précédentes dans l'entité TAA-FE, dans l'entité AM-FE ou dans la fonction MMCF. L'entité AN-FE reçoit les données de clé de session de l'entité TAA-FE via l'entité AM-FE. L'entité AN-FE peut obtenir ces données directement auprès de l'entité AM-FE si celle-ci est capable de les calculer. Les entités EN-FE et ABG-FE reçoivent toutes deux de l'entité TAA-FE via l'entité TLM-FE et la fonction MMCF les données de clé obtenues. Les entités EN-FE et ABG-FE peuvent toutes deux obtenir des données de clé auprès de la fonction MMCF si celle-ci est capable de calculer les données de clé de session.

La procédure d'authentification repose sur un protocole d'authentification par question-réponse, par exemple le protocole AKA [b-3GPP TS 33.102].

7.2 Authentification

7.2.1 Procédure générique d'authentification

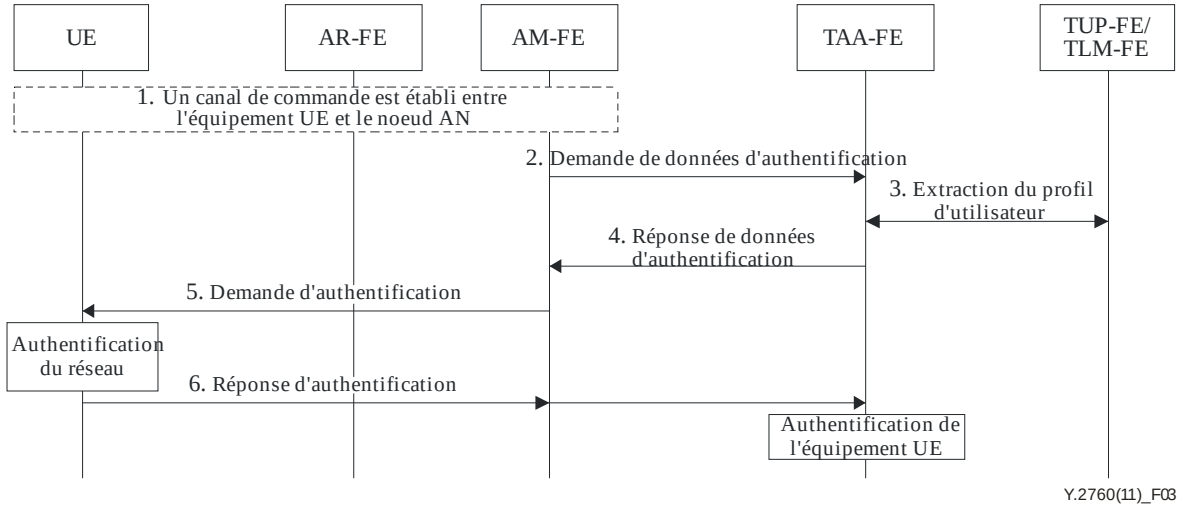

Figure 3 – Procédure générique d'authentification

1) Le canal de commande entre l'équipement UE et les fonctions du réseau d'accès est établi (la procédure n'entre pas dans le champ d'application de la présente Recommandation).

2) L'entité AM-FE envoie les informations d'équipement UE à l'entité TAA-FE pour demander les données d'authentification.

3) L'entité TAA-FE extrait les informations d'authentification de la demande d'authentification, qui comprend l'identificateur d'abonné utilisateur et les informations de réseau d'accès, interagit avec l'entité TUP-FE/TLM-FE pour obtenir le profil d'utilisateur et les vecteurs d'authentification, qui comprennent le jeton d'authentification et les données de clé de session.

4) L'entité TAA-FE envoie la réponse de données d'authentification, dont le jeton d'authentification, à l'entité AM-FE.

5) L'entité AM-FE envoie la demande d'authentification à l'équipement UE. L'équipement UE extrait le jeton d'authentification de la demande d'authentification, génère les vecteurs d'authentification locale qui comprennent les données de clé de session obtenues à partir du jeton d'authentification et de la clé racine. L'équipement UE authentifie le réseau en validant le jeton d'authentification reçu.

6) L'équipement UE envoie la réponse d'authentification, qui comprend le jeton d'authentification qu'il a généré, à l'entité AM-FE. L'entité AM-FE réexpédie les informations à l'entité TAA-FE. L'entité TAA-FE extrait le jeton d'authentification et vérifie que le jeton d'authentification reçu a été validé pour authentifier l'équipement UE.

7.2.2 Procédure générique de réauthentification rapide

La réauthentification rapide est utilisée pour réduire le temps de latence du transfert intercellulaire. L'entité TUP-FE/TLM-FE n'intervient pas dans cette procédure, qui permet d'effectuer plus rapidement l'authentification et réduit la charge de l'entité TUP-FE/TLM-FE. Il est recommandé que l'équipement UE et les entités d'authentification du réseau NGN prennent en charge la procédure générique de réauthentification rapide.

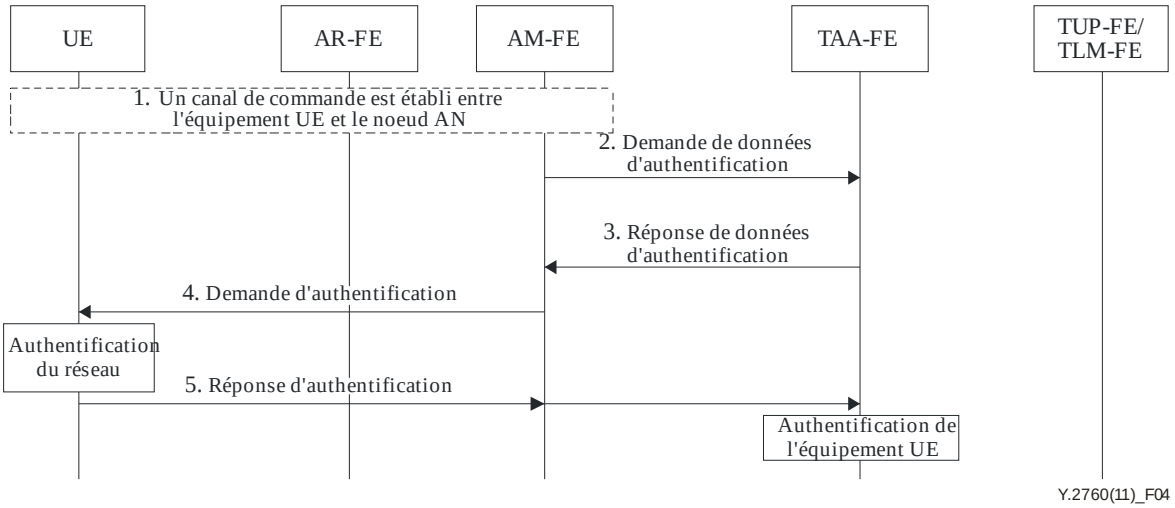

Figure 4 – Procédure générique de réauthentification rapide

Lorsqu'on applique la procédure ci-après, on part du principe que l'équipement UE et l'entité TAA-FE prennent en charge la réauthentification rapide.

1) Le canal de commande entre l'équipement UE et les fonctions du réseau d'accès est établi (la procédure n'entre pas dans le champ d'application de la présente Recommandation).

2) L'entité AM-FE envoie les informations d'équipement UE à l'entité TAA-FE pour demander les données d'authentification.

3) L'entité TAA-FE envoie la réponse de données d'authentification, dont le jeton d'authentification, à l'entité AM-FE.

4) L'entité AM-FE envoie la demande d'authentification à l'équipement UE. L'équipement UE extrait le jeton d'authentification de la demande d'authentification, génère les vecteurs d'authentification locale, qui comprennent les données de clé de session obtenues à partir du jeton d'authentification et de la clé racine. L'équipement UE authentifie le réseau en validant le jeton d'authentification reçu.

5) L'équipement UE envoie la réponse d'authentification, qui comprend le jeton d'authentification qu'il a généré, à l'entité AM-FE. L'entité AM-FE réexpédie les informations à l'entité TAA-FE. L'entité TAA-FE extrait le jeton d'authentification et vérifie que le jeton d'authentification reçu a été validé pour authentifier l'équipement UE.

Lorsque l'équipement UE réutilise les données de clé de session, les informations de réauthentification rapide sont utilisées uniquement pour l'authentification mutuelle. Lorsque l'équipement UE ne réutilise pas la clé de session, l'équipement UE et l'entité d'authentification (par exemple l'entité TAA-FE/TUP-FE) génèrent tous deux une nouvelle clé de session à partir des données de clé de session et des informations de réauthentification rapide.

7.2.2.1 Réauthentification rapide optimisée

Pour la réauthentification rapide optimisée, un équipement UE qui a été auparavant authentifié par le NGN génère les informations d'authentification. Cette procédure est différente de la procédure générique de réauthentification, dans laquelle l'équipement UE commence par authentifier le NGN, lequel génère ensuite un jeton authentifié.

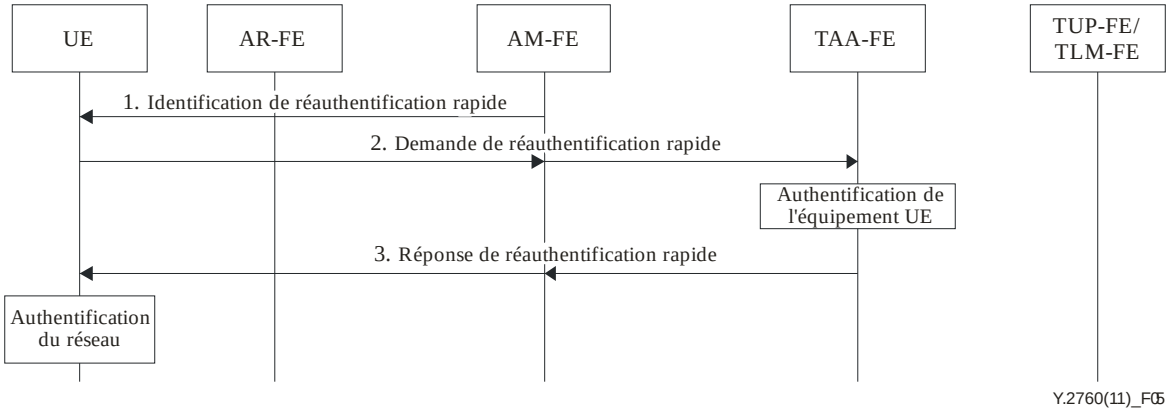

Figure 5 – Procédure de réauthentification rapide optimisée

1) Le canal de commande entre l'équipement UE et les fonctions du réseau d'accès est établi (la procédure n'entre pas dans le champ d'application de la présente Recommandation). L'entité AM-FE envoie l'indication de réauthentification optimisée à l'équipement UE, qui indique que l'entité TAA-FE prend en charge la réauthentification rapide optimisée.

2) L'équipement UE génère le vecteur d'authentification et envoie une demande de réauthentification optimisée à l'entité TAA-FE via l'entité AM-FE. La demande de réauthentification optimisée comprend un jeton d'authentification et les informations de réauthentification. L'entité TAA-FE génère un vecteur d'authentification locale et de nouvelles données de clé de session à partir des informations de réauthentification et des données de clé de session. L'entité TAA-FE authentifie l'équipement UE en validant le jeton d'authentification reçu.

3) L'entité TAA-FE envoie la réponse de réauthentification, qui comprend le jeton d'authentification, à l'équipement UE via l'entité AM-FE. L'équipement UE authentifie le réseau grâce à son propre vecteur d'authentification. Une fois l'authentification menée à bien, l'équipement UE peut générer des données de clé de sous-session.

7.2.3 Authentification intradomaine

7.2.3.1 Authentification avec une seule connexion réseau

Dans le cas d'une seule connexion réseau, l'équipement UE peut détecter des réseaux différents, mais il ne peut accéder qu'à un seul réseau à la fois. La préauthentification signifie que l'équipement UE et le réseau cible s'authentifient mutuellement par l'intermédiaire d'un réseau de desserte avant que l'équipement UE effectue un transfert intercellulaire vers le réseau cible. Lorsque l'équipement UE ne peut être connecté qu'à un seul réseau, il utilise la préauthentification pour assurer la continuité du service et réduire le temps de latence. La procédure de préauthentification est analogue à la procédure générique d'authentification. L'entité AM-FE du réseau de desserte et l'entité AM-FE du réseau cible interviennent dans la procédure de préauthentification si besoin est.

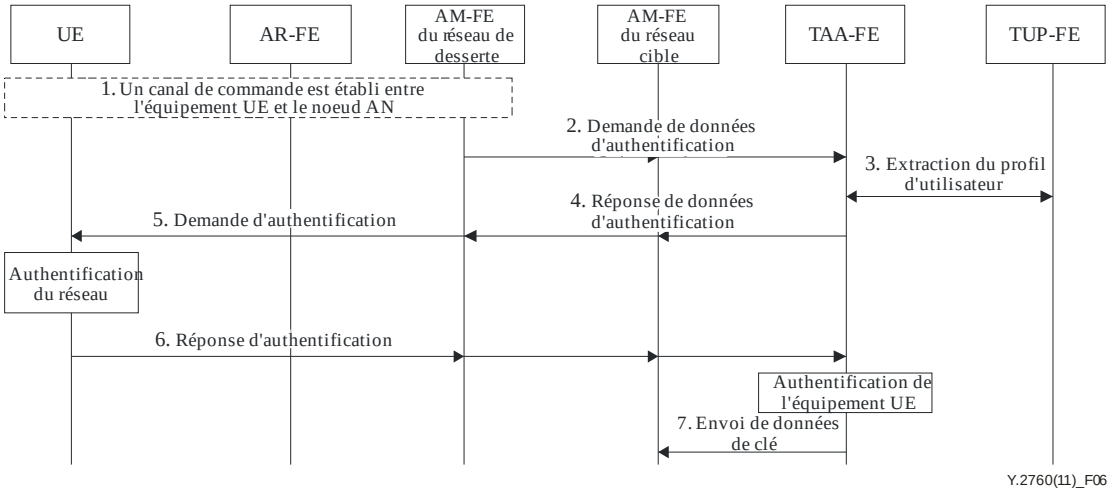

Figure 6 – Procédures de préauthentification fondée sur une seule connexion réseau

1) Le canal de commande entre l'équipement UE et les fonctions du réseau d'accès est établi (la procédure n'entre pas dans le champ d'application de la présente Recommandation).

2) L'entité AM-FE envoie une demande de données d'authentification, qui comprend les informations d'abonné, à l'entité TAA-FE. La demande de données d'authentification est réexpédiée par l'entité AM-FE du réseau de desserte et l'entité AM-FE du réseau cible.

3) L'entité TAA-FE extrait le profil d'utilisateur en interagissant avec l'entité TUP-FE.

4) L'entité TAA-FE envoie la réponse de données d'authentification, qui comprend le jeton d'authentification, à l'entité AM-FE du réseau cible et à l'entité AM-FE du réseau de desserte.

5) L'entité AM-FE du réseau de desserte envoie la demande d'authentification à l'équipement UE. L'équipement UE extrait le jeton d'authentification et authentifie le réseau en utilisant ses propres informations d'authentification. Une fois l'authentification menée à bien, l'équipement UE génère des données de clé de session.

6) L'équipement UE envoie la réponse d'authentification à l'entité AM-FE du réseau de desserte, laquelle réexpédie les informations, qui comprennent le jeton d'authentification, aux entités AM-FE et TAA-FE du réseau cible. L'entité TAA-FE extrait le jeton d'authentification et authentifie l'équipement UE. Une fois l'authentification menée à bien, l'entité TAA-FE génère des données de clé de session à partir desquelles il est possible d'obtenir des données de clé de sous-session si besoin est.

7) L'entité TAA-FE envoie les données de clé à l'entité AM-FE du réseau cible, qui seront utilisées une fois que l'équipement UE aura effectué le transfert intercellulaire vers le réseau cible pour protéger la communication entre l'équipement UE et le réseau cible.

7.2.4 Authentification interdomaines

Un domaine administratif différent signifie un fournisseur de réseau NGN différent. On trouvera ci-après la description d'une procédure d'authentification pour les transferts intercellulaires de l'équipement UE entre des domaines administratifs différents.

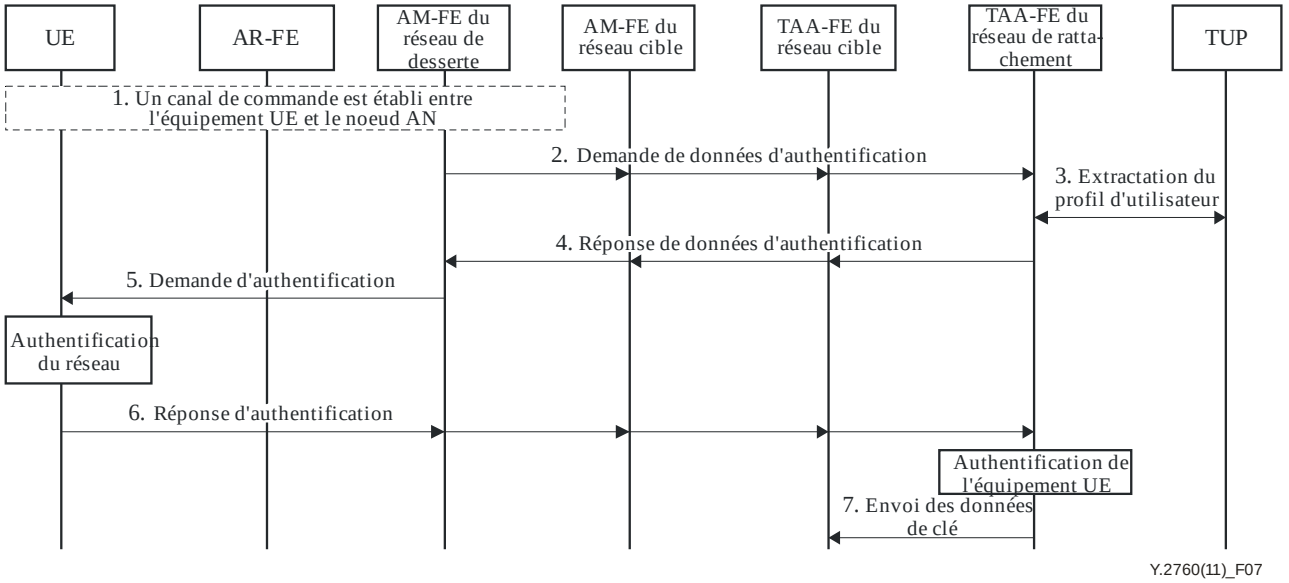

Figure 7 – Procédure d'authentification entre des domaines différents

1) Le canal de commande entre l'équipement UE et les fonctions du réseau d'accès est établi (la procédure n'entre pas dans le champ d'application de la présente Recommandation).

2) L'entité AM-FE du réseau de desserte envoie la demande de données d'authentification, qui comprend les informations d'abonné, à l'entité TAA-FE du réseau de rattachement. La demande de données d'authentification est réexpédiée par les entités AM-FE et TAA-FE du réseau cible. L'entité TAA-FE du réseau de rattachement extrait le profil d'utilisateur en interagissant avec l'entité TUP-FE.

3) L'entité TAA-FE extrait le profil d'utilisateur en interagissant avec l'entité TUP-FE.

4) L'entité TAA-FE du réseau de rattachement envoie la réponse de données d'authentification, qui comprend le jeton d'authentification, à l'entité AM-FE du réseau de desserte. La réponse de données d'authentification est réexpédiée par les entités TAA-FE et AM-FE du réseau cible.

5) L'entité AM-FE du réseau de desserte envoie la demande d'authentification à l'équipement UE. L'équipement UE extrait le jeton d'authentification et authentifie le réseau en utilisant ses propres informations d'authentification. Une fois l'authentification menée à bien, l'équipement UE calcule des données de clé de session.

6) L'équipement UE envoie la réponse d'authentification, qui comprend le jeton d'authentification, à l'entité TAA-FE du réseau de rattachement, laquelle extrait le jeton d'authentification et authentifie l'équipement UE. Une fois l'authentification menée à bien, l'entité TAA-FE du réseau de rattachement génère des données de clé de session à partir desquelles il est possible d'obtenir des données de clé de sous-session si besoin est.

7) Une fois l'authentification menée à bien, l'entité TAA-FE du réseau de rattachement envoie les données de clé à l'entité TAA-FE du réseau cible, qui seront utilisées une fois que l'équipement UE aura effectué le transfert intercellulaire depuis le réseau de desserte vers le réseau cible pour protéger la communication entre l'équipement UE et le réseau cible.

7.2.5 Mécanismes de mise en correspondance des données de clé dans l'authentification

Lorsqu'un équipement UE se déplace d'un réseau de desserte vers un réseau cible, l'authentification mutuelle est exécutée et les données de clé de session sont calculées. Un réseau NGN prend en charge différents mécanismes de calcul des clés et la mise en correspondance des données de clé permet de coordonner les données de clé utilisées pour les différents mécanismes de calcul des clés.

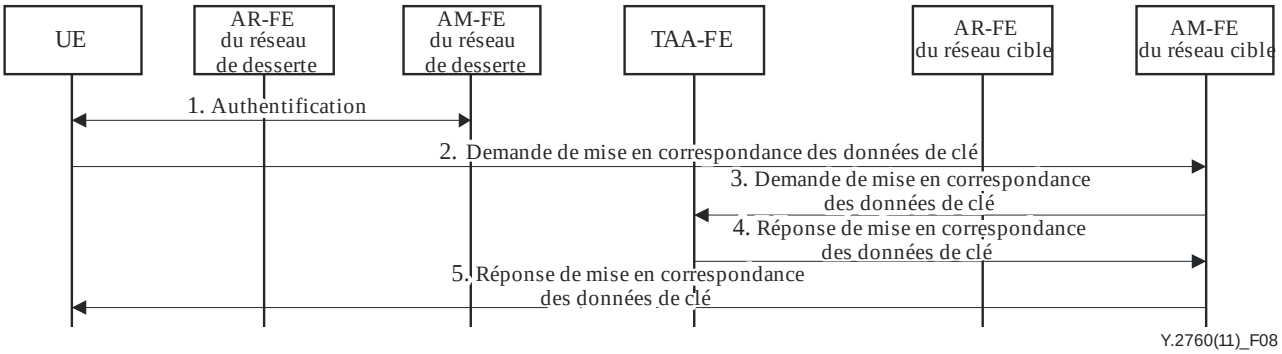

Figure 8 – Procédure de mise en correspondance des données de clé

1) La connexion est établie entre l'équipement UE et l'entité TAA-FE, la procédure d'authentification est finie et les données de clé de session sont générées.

2) L'équipement UE détecte un réseau cible et prépare le transfert intercellulaire vers le réseau cible. Il envoie une demande de mise en correspondance des données de clé à l'entité AM-FE du réseau cible. La demande de mise en correspondance des données de clé comprend les informations de mise en correspondance telles que le mécanisme de calcul des clés utilisé et les mécanismes de calcul de clé pris en charge.

3) L'entité AM-FE du réseau cible envoie la demande de mise en correspondance des données de clé à l'entité TAA-FE.

4) L'entité TAA-FE reçoit la demande de mise en correspondance des données de clé et met en correspondance les données de clé dans le réseau de desserte et les données de clé dans le réseau cible et envoie la réponse de mise en correspondance des données de clé à l'entité AM-FE du réseau cible.

5) L'entité AM-FE du réseau cible envoie la réponse de mise en correspondance à l'équipement UE. L'équipement UE met en correspondance les données de clé dans le réseau de desserte et les données de clé dans le réseau cible. L'équipement UE et l'entité TAA-FE ont tous deux échangé les données de clé dans le réseau cible, qui sont utilisées pour protéger le trafic entre l'équipement UE et le réseau cible.

7.2.6 Authentification fondée sur plusieurs accès réseaux

L'authentification fondée sur plusieurs accès réseaux signifie que l'équipement UE est capable de communiquer avec plusieurs réseaux d'accès en même temps. Dans ce cas, il se connecte au réseau cible et effectue une procédure d'authentification mutuelle avant de se déconnecter du réseau de desserte. La procédure d'authentification mutuelle est la procédure générique décrite dans la Figure 3. Une fois l'authentification mutuelle menée à bien, l'équipement UE et l'entité TAA-FE génèrent des données de clé de session partagée et l'entité TAA-FE envoie les données de clé de session à l'entité AM-FE du réseau cible. Lorsque l'équipement UE se déplace vers le réseau cible, le trafic entre cet équipement et le réseau cible est protégé par les données de clé de session ou les données de clé de sous-session obtenues à partir de la clé de session.

7.2.7 Authentification fondée sur plusieurs connexions

L'expression "plusieurs connexions" signifie que l'équipement UE conserve plusieurs connexions réseau en même temps. Les caractéristiques offertes à l'utilisateur, telles que la largeur de bande, le temps de transfert et la sécurité varieront en fonction du type de connexion réseau. Le cas de figure prévoyant plusieurs connexions à des domaines administratifs différents ne relève pas du champ d'application de la présente Recommandation.

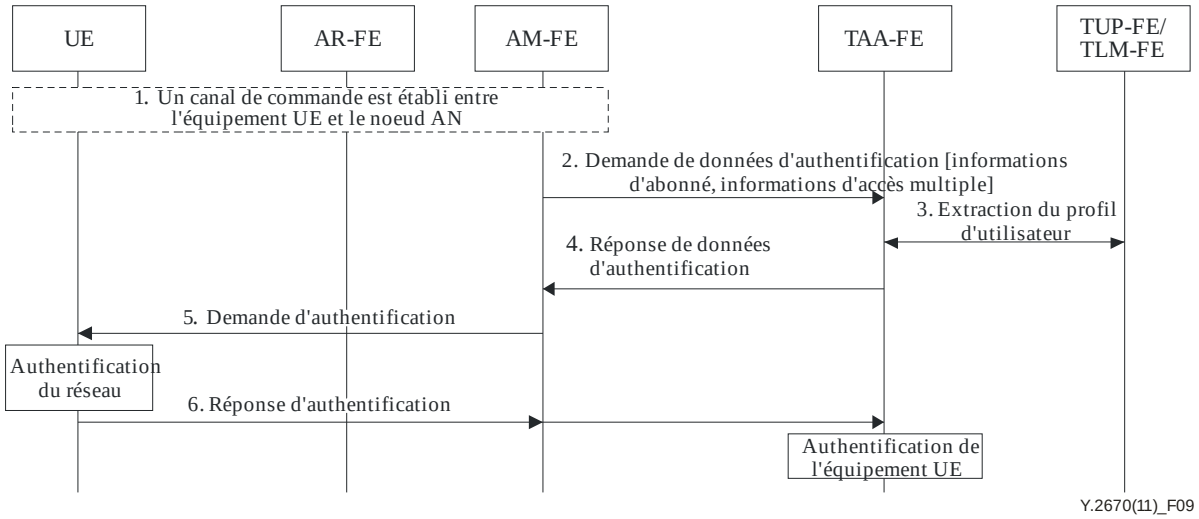

Figure 9 – Authentification fondée sur plusieurs connexions

1) Le canal de commande entre l'équipement UE et les fonctions du réseau d'accès est établi (la procédure n'entre pas dans le champ d'application de la présente Recommandation). L'équipement UE obtient les informations auprès du réseau d'accès et une indication que l'authentification avec accès multiple est prise en charge.

2) L'entité AM-FE envoie une demande de données d'authentification à l'entité TAA-FE. La demande de données d'authentification comprend les informations d'équipement UE comme les informations d'abonné (par exemple identificateur d'abonné utilisateur) et les informations d'accès multiple (par exemple, indication d'accès multiple et identificateur de l'interface d'accès multiple).

3) L'entité TAA-FE obtient les informations d'authentification et interagit avec l'entité TUP-FE/TLM-FE pour obtenir le profil d'utilisateur et le vecteur d'authentification. Le vecteur d'authentification est généré par l'entité TUP-FE/TLM-FE. Le jeton d'authentification est inclus dans le vecteur d'authentification.

4) L'entité TAA-FE envoie la réponse de données d'authentification, qui comprend le jeton d'authentification, à l'entité AM-FE.

5) L'entité AM-FE envoie la demande d'authentification à l'équipement UE. L'équipement UE génère les jetons d'authentification locale à partir des informations d'authentification contenues dans le message de demande d'authentification. Il authentifie le réseau en vérifiant que le jeton d'authentification reçu a été validé grâce aux jetons d'authentification locale. Une fois l'authentification menée à bien, l'équipement UE génère des données de clé de session à partir des informations d'authentification. S'il est indiqué qu'il s'agit d'un accès multiple, l'équipement UE génère des données de clé pour plusieurs sessions à partir des informations d'accès multiple.

6) L'équipement UE envoie le message de réponse d'authentification à l'entité AM-FE. L'entité AM-FE réexpédie les informations, qui comprennent le jeton d'authentification généré par l'équipement UE, à l'entité TAA-FE. L'entité TAA-FE extrait le jeton d'authentification contenu dans le message de réponse d'authentification et authentifie l'équipement UE à partir du vecteur d'authentification dans l'entité TAA-FE. Une fois l'authentification menée à bien, l'entité TAA-FE génère des données de clé de session conformément au jeton d'identification. S'il est indiqué qu'il s'agit d'un accès multiple, l'entité TAA-FE génère des données de clé pour plusieurs sessions à partir des informations d'accès multiple.

8 Etablissement du contexte de sécurité

8.1 Transfert du contexte de sécurité entre l'entité AM-FE du réseau de desserte et l'entité AM-FE du réseau cible

Le trafic concernant le transfert du contexte de sécurité entre l'entité AM-FE du réseau de desserte et l'entité AM-FE du réseau cible devrait être protégé. On assure la sécurité entre l'entité AM-FE du réseau de desserte et l'entité AM-FE du réseau cible en établissant une association de sécurité. Si les deux entités AM-FE sont situées dans la même zone, l'association de sécurité n'est pas nécessaire. Si les deux entités AM-FE sont situées dans des zones différentes, par exemple dans des domaines d'opérateur différents, le mécanisme de sécurité crée une association de sécurité conformément à la politique de l'opérateur ou à l'accord conclu avec celui-ci.

8.2 Transfert du contexte de sécurité entre l'entité AR-FE du réseau de desserte et l'entité AR-FE du réseau cible

Lorsque l'équipement UE effectue un transfert intercellulaire entre l'entité AR-FE du réseau de desserte et l'entité AR-FE du réseau cible, le trafic concernant le transfert du contexte de sécurité entre l'entité AR-FE du réseau de desserte et l'entité AR-FE du réseau cible doit être protégé. On assure la sécurité du transfert du contexte de sécurité entre l'entité AR-FE du réseau de desserte et l'entité AR-FE du réseau cible en établissant une association de sécurité.

8.3 Transfert du contexte de sécurité entre l'équipement UE et l'entité HDC-FE

8.3.1 Transfert du contexte de sécurité déclenché par le serveur

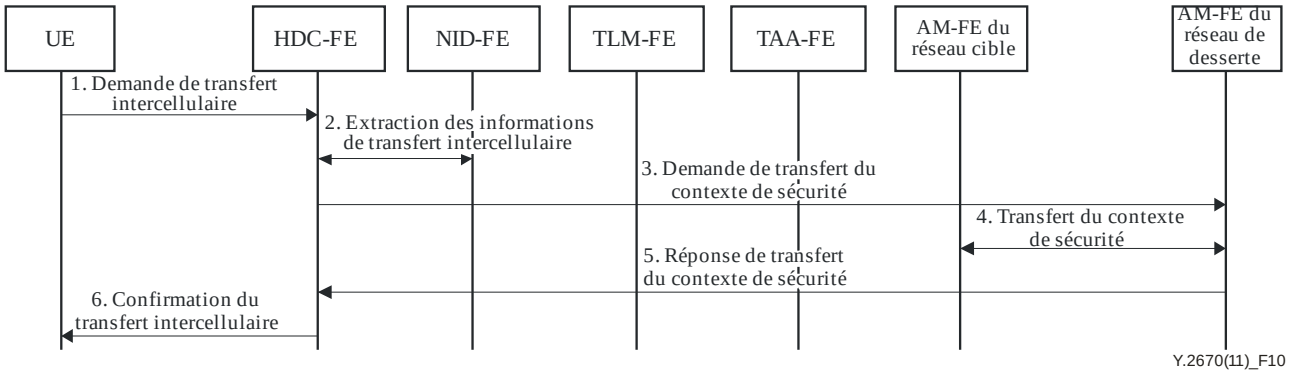

Figure 10 – Procédure de transfert du contexte de sécurité déclenché par le serveur

Lorsque l'équipement UE décide qu'un transfert intercellulaire depuis le réseau de desserte vers le réseau cible doit avoir lieu, il envoie une demande de transfert intercellulaire à l'entité HDC-FE, qui déclenche un transfert du contexte de sécurité. Une fois le transfert du contexte de sécurité effectué, l'entité AM-FE du réseau cible utilise le contexte de sécurité pour protéger le trafic entre l'équipement UE et le réseau cible. Cette opération se déroule comme suit:

1) L'équipement UE envoie une demande de transfert intercellulaire à l'entité HDC-FE.
2) L'entité HDC-FE reçoit la demande de transfert intercellulaire et interagit avec l'entité NID-FE pour obtenir les informations liées au transfert intercellulaire.
3) L'entité HDC-FE réexpédie la demande de transfert intercellulaire, qui comprend les informations liées au transfert intercellulaire, à l'entité AM-FE du réseau de desserte.
4) L'entité AM-FE du réseau de desserte interagit avec l'entité AM-FE du réseau cible pour transférer le contexte de sécurité.

5) Une fois le transfert du contexte de sécurité effectué, l'entité AM-FE du réseau de desserte envoie la réponse de transfert du contexte de sécurité à l'entité HDC-FE.

6) L'entité HDC-FE reçoit la réponse de transfert du contexte de sécurité. Si le transfert du contexte de sécurité a été effectué avec succès, l'entité HDC-FE envoie la confirmation du transfert intercellulaire à l'équipement UE.

8.3.2 Transfert du contexte de sécurité déclenché par le réseau

Lorsque l'entité HDC-FE décide d'activer l'équipement UE pour procéder à un transfert intercellulaire depuis le réseau de desserte vers le réseau cible, elle envoie un message d'amorçage de transfert intercellulaire pour déclencher un transfert du contexte de sécurité. Une fois le transfert du contexte de sécurité effectué, l'entité AM-FE du réseau cible utilise le contexte de sécurité pour protéger le trafic entre l'équipement UE et le réseau cible.

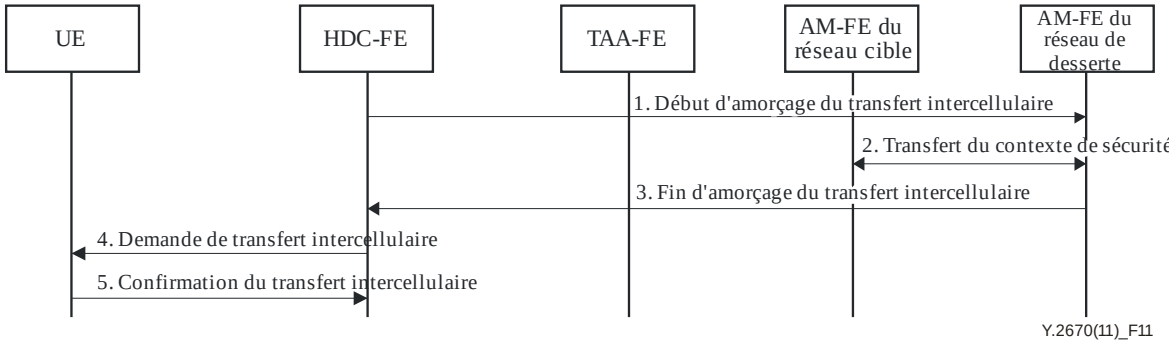

Figure 11 – Procédure de transfert du contexte de sécurité déclenché par le réseau

1) L'entité HDC-FE prépare la procédure de transfert intercellulaire et envoie un message de début d'amorçage du transfert intercellulaire à l'entité AM-FE du réseau de desserte pour déclencher un transfert du contexte de sécurité.

2) L'entité AM-FE du réseau de desserte interagit avec l'entité AM-FE du réseau cible pour transférer le contexte de sécurité.

3) Une fois le transfert du contexte de sécurité effectué, l'entité AM-FE du réseau de desserte envoie le message de fin d'amorçage du transfert intercellulaire à l'entité HDC-FE.

4) Lorsque l'entité HDC-FE reçoit le message de fin d'amorçage du transfert intercellulaire, elle commence la procédure de transfert intercellulaire en envoyant une demande de transfert intercellulaire à l'équipement UE.

5) L'équipement UE envoie le message de confirmation du transfert intercellulaire lorsque ce transfert est fini.

9 Sécurité de la mobilité IP

9.1 Sécurité de la mobilité fondée sur le serveur

Le trafic de commande de la mobilité fondée sur le serveur entre l'équipement UE et l'entité MLM-FE(C) doit être protégé. L'association de sécurité est obligatoire entre l'équipement UE et l'entité MLM-FE(C), tandis qu'elle est facultative entre l'équipement UE et l'entité MLM-FE(P).

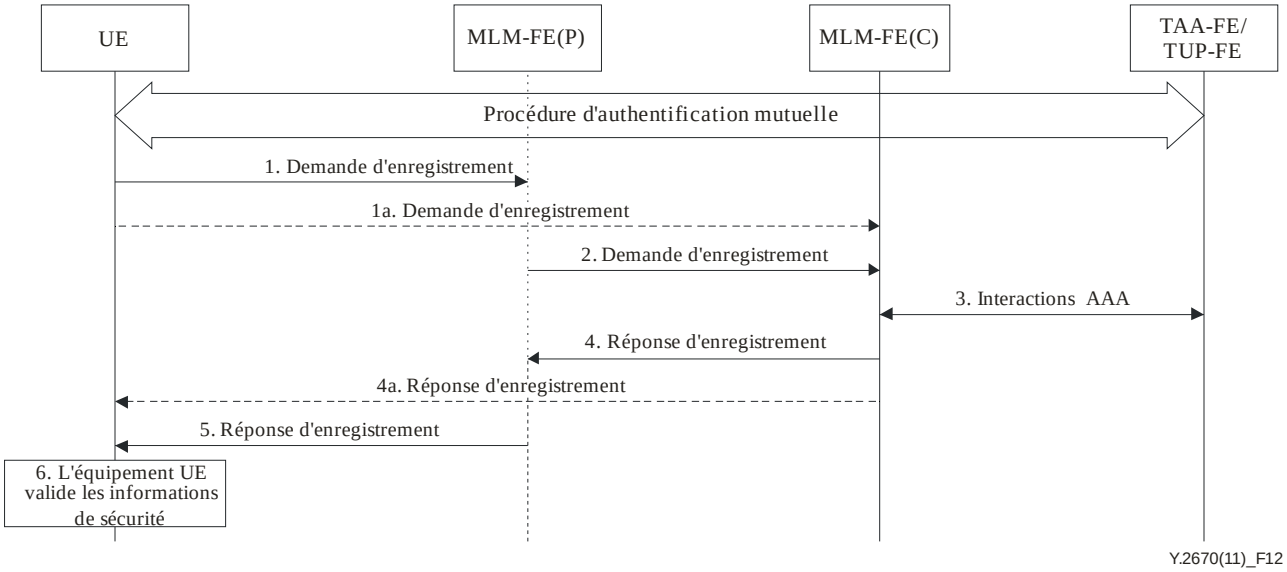

Figure 12 – Procédure de mobilité fondée sur le serveur

Lorsqu'on applique la procédure ci-après, on part du principe que l'équipement UE et l'entité TAA-FE ont mené à bien la procédure générique d'authentification.

1) L'équipement UE envoie une demande d'enregistrement à l'entité MLM-FE(P). La demande d'enregistrement comprend les informations de sécurité entre l'équipement UE et l'entité MLM-FE(C) et les informations de sécurité entre l'équipement UE et l'entité MLM-FE(P).

   - 1a. Si l'entité MLM-FE(P) n'existe pas, l'équipement UE envoie une demande d'enregistrement directement à l'entité MLM-FE(C).

2) L'entité MLM-FE(P) valide les informations de sécurité entre l'équipement UE et l'entité MLM-FE(P) et réexpédie la demande d'enregistrement à l'entité MLM-FE(C). L'entité MLM-FE(P) pourra ajouter les informations de sécurité entre les entités MLM-FE(P) et MLM-FE(C) au message d'enregistrement avant de le réexpédier.

3) L'entité MLM-FE(C) interagit avec l'entité TAA-FE/TUP-FE pour obtenir les informations d'authentification et d'autorisation.

4) L'entité MLM-FE(C) valide les informations de sécurité entre l'équipement UE et l'entité MLM-FE(C) contenues dans la demande d'enregistrement. L'entité MLM-FE(C) envoie la réponse d'enregistrement et les informations de sécurité à l'entité MLM-FE(P). La réponse d'enregistrement peut contenir les informations de sécurité entre l'équipement UE et l'entité MLM-FE(C) et les informations de sécurité entre les entités MLM-FE(P) et MLM-FE(C).

   - 4a. Si l'entité MLM-FE (P) n'existe pas, l'entité MLM-FE(C) envoie la réponse d'enregistrement directement à l'équipement UE. La réponse d'enregistrement pourra comprendre les informations de sécurité entre l'équipement UE et l'entité MLM-FE(C).

5) L'équipement MLM-FE(P) valide les informations de sécurité entre les entités MLM-FE(P) et MLM-FE(C) et envoie la réponse d'enregistrement à l'équipement UE. L'entité MLM-FE(P) pourra ajouter les informations de sécurité entre l'équipement UE et l'entité MLM-FE(P) au message de réponse d'enregistrement avant de le réexpédier.

6) L'entité MLM-FE(C) valide les informations de sécurité entre l'équipement UE et l'entité MLM-FE(C) et crée l'association de sécurité entre l'équipement UE et l'entité MLM-FE(C). Si l'entité MLM-FE(P) existe, l'équipement UE valide les informations de sécurité entre l'équipement UE et l'entité MLM-FE(P) et crée l'association de sécurité entre l'équipement UE et l'entité MLM-FE(P).

9.2 Sécurité de la mobilité fondée sur le réseau

La protection du trafic de commande de la mobilité fondée sur le réseau entre deux entités du réseau dans une zone de confiance ou dans une zone de confiance mais vulnérable est facultative et dépend de la politique de l'opérateur. Les mécanismes permettant d'assurer la sécurité du trafic de commande de la mobilité fondée sur le réseau reposent sur les mécanismes de sécurité décrits dans [UIT-T Y.2704].

10 Sécurité entre l'équipement UE et l'entité HDC-FE

Le flux d'informations entre l'équipement UE et l'entité HDC-FE sert à acheminer les informations permettant de prendre la décision de transfert intercellulaire. L'équipement UE et l'entité HDC-FE devraient établir une association de sécurité pour protéger le flux d'informations entre l'équipement UE et l'entité HDC-FE.

10.1 Création d'une association de sécurité entre l'équipement UE et l'entité HDC-FE déclenchée par le serveur

Dans le cadre de la procédure de création d'une association de sécurité déclenchée par le serveur, l'équipement UE déclenche la procédure permettant de créer une association de sécurité entre l'équipement UE et l'entité HDC-FE, décrite à la Figure 13. Deux conditions préalables doivent être réunies pour permettre la création d'une association de sécurité entre l'équipement UE et l'entité HDC-FE déclenchée par le serveur. Premièrement, l'équipement UE et l'entité TAA-FE doivent posséder des données de clé prépartagée, lesquelles peuvent être obtenues après la procédure d'authentification mutuelle. Deuxièmement, l'équipement UE doit connaître les informations d'entité HDC-FE, telles que l'adresse, pour pouvoir envoyer une demande d'association de sécurité à l'entité HDC-FE. La façon dont l'équipement UE obtient les informations d'entité HDC-FE ne relève pas du champ d'application de la présente Recommandation. L'entité TLM-FE est utilisée pour retransmettre les informations de données de clé vers et depuis l'entité TAA-FE, mais elle n'apparaît pas dans les figures ci-après.

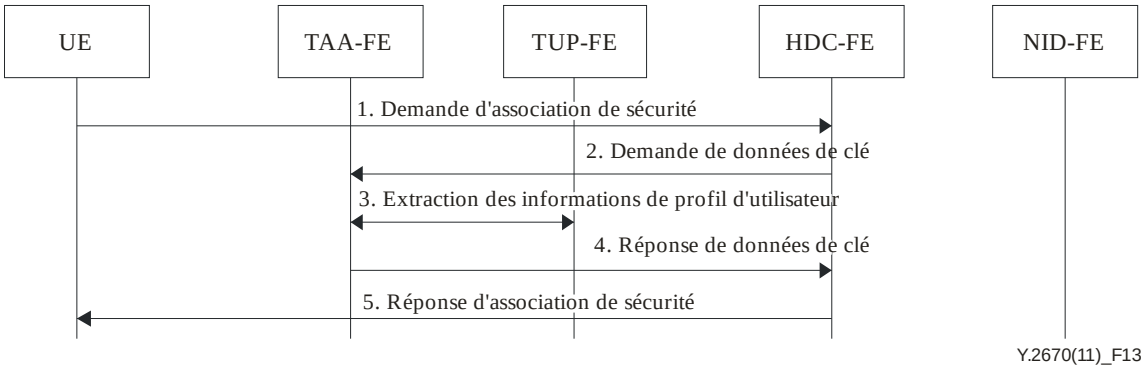

Figure 13 – Procédure de création d'une association de sécurité déclenchée par le serveur

1) L'équipement UE génère des données de clé partagée pour créer une association avec l'entité HDC-FE conformément aux informations d'authentification. L'équipement UE envoie la demande d'association de sécurité, qui contient les informations d'authentification et les informations d'équipement UE, à l'entité HDC-FE.

2) L'entité HDC-FE envoie la demande de données de clé, qui comprend les informations d'entité HDC-FE, les informations d'authentification et les informations d'équipement UE, à l'entité TAA-FE.

3) L'entité TAA-FE extrait les informations de profil d'utilisateur en interagissant avec l'entité TUP-FE et vérifie que l'entité HDC-FE est autorisée à créer une association de sécurité avec l'équipement UE.

4) L'entité TAA-FE génère des données de clé pour l'entité HDC-FE conformément aux informations d'authentification, aux informations d'entité HDC-FE et aux informations d'équipement UE lorsque l'entité HDC-FE est autorisée à créer une association de sécurité avec l'équipement UE. L'entité TAA-FE envoie une réponse de données de clé, qui comprend des informations comme les données de clé pour l'entité HDC-FE et la durée de vie de la clé, à l'entité HDC-FE.

5) L'entité HDC-FE envoie la réponse d'association de sécurité pour informer que l'association de sécurité entre l'équipement UE et l'entité HDC-FE est établie.

10.2 Création d'une association de sécurité entre l'équipement UE et l'entité HDC-FE déclenchée par le réseau

Dans le cadre de la procédure de création d'une association de sécurité déclenchée par le réseau, le réseau déclenche la procédure permettant de créer une association de sécurité entre l'équipement UE et l'entité HDC-FE décrite dans la Figure 14. Deux conditions préalables doivent être réunies pour permettre la création d'une association de sécurité entre l'équipement UE et l'entité HDC-FE déclenchée par le réseau. Premièrement, l'équipement UE et l'entité TAA-FE doivent posséder des données de clé partagée, lesquelles peuvent être générées après la procédure d'authentification mutuelle. Deuxièmement, l'entité HDC-FE doit connaître les informations d'équipement UE, telles que les informations d'abonné ou les informations de localisation, pour pouvoir envoyer les informations d'association de sécurité à l'équipement UE. La façon d'obtenir les informations d'équipement UE pour l'entité HDC-FE ne relève pas du champ d'application de la présente Recommandation.

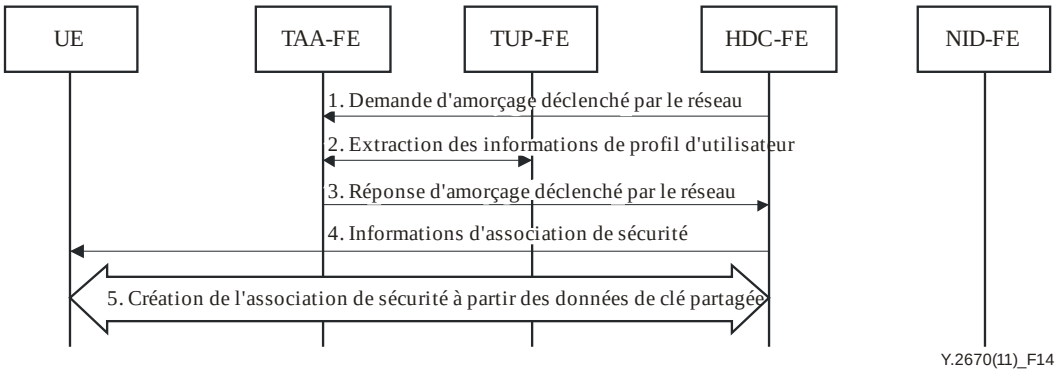

Figure 14 – Procédure de création d'une association de sécurité déclenchée par le réseau

1) L'entité HDC-FE envoie une demande d'amorçage déclenché par le réseau, qui comprend les informations d'entité HDC-FE et les informations d'équipement UE, à l'entité TAA-FE.

2) L'entité TAA-FE extrait les informations de profil d'utilisateur en interagissant avec l'entité TUP-FE et vérifie que l'entité HDC-FE est autorisée à créer une association de sécurité avec l'équipement UE.

3) L'entité TAA-FE génère des données de clé pour l'entité HDC-FE conformément aux informations d'entité HDC-FE et aux informations d'équipement UE lorsque l'entité HDC-FE est autorisée à déclencher la création d'une association de sécurité avec l'équipement UE. L'entité TAA-FE envoie la réponse d'amorçage déclenché par le réseau, qui comprend les informations d'authentification comme les données de clé pour l'entité HDC-FE et la durée de vie de la clé, à l'entité HDC-FE.

4) L'entité HDC-FE envoie les informations d'association de sécurité, qui comprennent les informations d'authentification, à l'équipement UE pour créer une association de sécurité.

5) L'équipement UE génère des données de clé pour l'entité HDC-FE conformément aux informations d'authentification contenues dans les informations d'association de sécurité et valide les informations d'association de sécurité. L'association de sécurité est créée entre l'entité HDC-FE et l'équipement UE.

10.3 Préétablissement d'une association de sécurité entre l'équipement UE et l'entité HDC-FE fondé sur une infrastructure PKI

La procédure d'établissement d'une association de sécurité entre l'équipement UE et l'entité HDC-FE fondé sur une infrastructure PKI est décrite dans la Figure 15. Pour pouvoir appliquer la procédure d'établissement d'une association de sécurité entre l'équipement UE et l'entité HDC-FE, l'équipement UE doit connaître les informations d'entité HDC-FE, comme l'adresse, pour pouvoir envoyer la demande d'association de sécurité à l'entité HDC-FE. La façon dont l'équipement UE obtient les informations d'entité HDC-FE ne relève pas du champ d'application de la présente Recommandation.

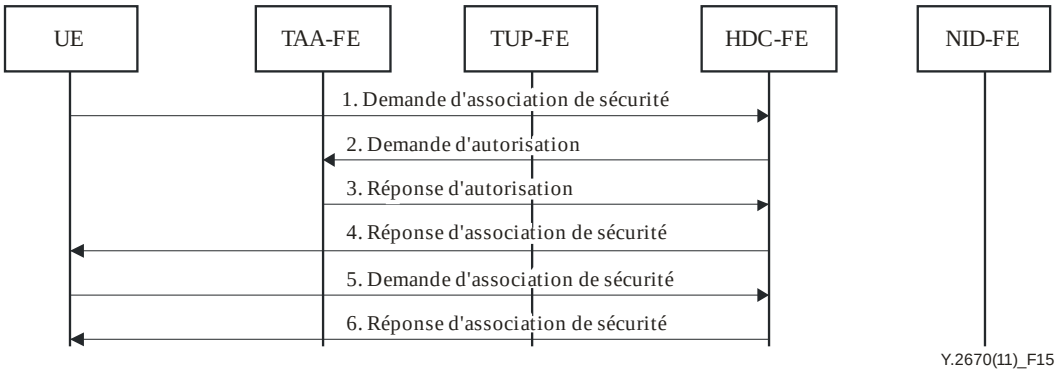

Figure 15 – Procédure d'établissement d'une association de sécurité fondé sur une infrastructure PKI

1) L'équipement UE envoie une demande d'association de sécurité, qui comprend le certificat d'équipement UE et les informations d'équipement UE, à l'entité HDC-FE.

2) L'entité HDC-FE valide le certificat d'équipement UE et envoie une demande d'autorisation, qui comprend les informations d'équipement UE et les informations d'entité HDC-FE, à l'entité TAA-FE.

3) L'entité TAA-FE vérifie l'autorisation sur la base des informations d'équipement UE et des informations d'entité HDC-FE. Si l'équipement UE est autorisé à utiliser l'entité HDC-FE, l'entité TAA-FE envoie une réponse d'autorisation, qui contient les informations d'autorisation et le certificat de serveur, à l'entité HDC-FE.

4) L'entité HDC-FE reçoit les informations d'autorisation et envoie une réponse d'association de sécurité, qui comprend le certificat de serveur, à l'équipement UE.

5) S'il faut des données de clé partagée entre l'équipement UE et l'entité TAA-FE, l'entité TAA-FE envoie des informations de calcul de clé à l'équipement UE lors de l'étape 4). L'équipement UE génère des données de clé partagée à partir des informations de calcul de clé et des informations de calcul de clé locale reçues. L'équipement UE envoie les informations de calcul de clé locale à l'entité HDC-FE.

6) L'entité HDC-FE génère des données de clé à partir des informations de calcul de clé et des informations de calcul de clé locale reçues. L'entité HDC-FE envoie la réponse d'association de sécurité à l'équipement UE. L'association de sécurité entre l'équipement UE et l'entité HDC-FE est établie.

11 Sécurité entre l'équipement UE et l'entité NID-FE

11.1 Etablissement d'une association de sécurité entre l'équipement UE et l'entité NID-FE déclenché par le serveur

La procédure d'établissement d'une association de sécurité entre l'équipement UE et l'entité NID-FE déclenché par le serveur est présentée dans la Figure 16. Pour pouvoir appliquer la procédure d'établissement d'une association de sécurité entre l'équipement UE et l'entité NID-FE, les conditions suivantes doivent être réunies: 1) l'équipement UE et l'entité TAA-FE doivent avoir des données de clé partagée, lesquelles peuvent être générées après la procédure d'authentification mutuelle; 2) l'équipement UE doit connaître les informations d'entité NID-FE, telles que l'adresse, pour pouvoir envoyer une demande d'association de sécurité à l'entité NID-FE. La façon dont l'équipement UE obtient les informations d'entité NID-FE ne relève pas du champ d'application de la présente Recommandation.

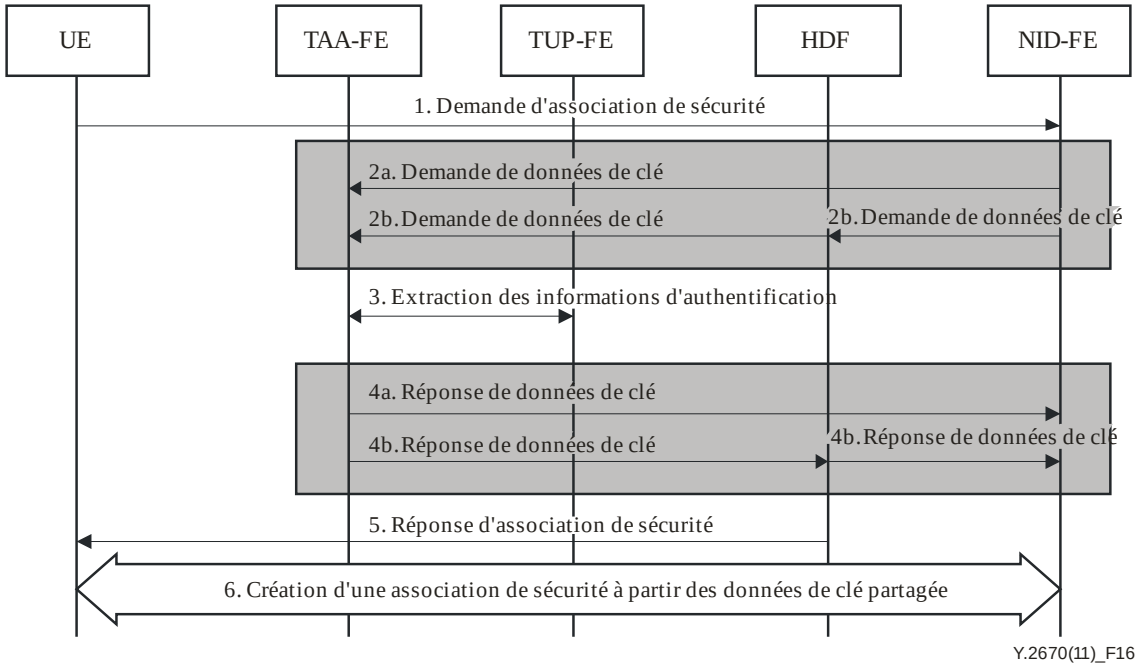

Figure 16 – Etablissement d'une association de sécurité déclenché par le serveur

1) L'équipement UE envoie une demande d'association de sécurité à l'entité NID-FE.

2) L'entité NID-FE envoie une demande de données de clé, qui comprend les informations de l'entité NID-FE et les informations d'équipement UE, à l'entité TAA-FE. Si l'entité NID-FE ne prend pas en charge l'envoi d'une demande d'authentification directement à l'entité TAA-FE, elle envoie une demande d'authentification à l'entité TAA-FE via l'entité HDC-FE.

3) L'entité TAA-FE interagit avec l'entité TUP-FE et génère des données de clé pour l'entité NID-FE.

4) L'entité TAA-FE envoie la réponse de données de clé, qui comprend les informations d'authentification, à l'entité HDC-FE. Les informations d'authentification sont composées des données de clé partagée et de la durée de vie de la clé. Si l'entité TAA-FE ne prend pas en charge l'envoi d'une demande d'authentification directement à l'entité NID-FE, elle envoie une demande d'authentification à l'entité NID-FE via l'entité HDC-FE.

5) L'entité NID-FE envoie la réponse d'association de sécurité, qui comprend les informations d'authentification, à l'équipement UE protégé par les données de clé partagée.

6) L'équipement UE génère les données de clé partagée et valide la réponse d'association de sécurité. L'association de sécurité est créée par l'entité NID-FE et l'équipement UE d'après les données de clé partagée.

11.2 Etablissement d'une association de sécurité entre l'équipement UE et l'entité NID-FE déclenché par le réseau

La procédure d'établissement d'une association de sécurité entre l'équipement UE et l'entité NID-FE déclenché par le réseau est présentée dans la Figure 17. Pour pouvoir appliquer la procédure d'établissement d'une association de sécurité entre l'équipement UE et l'entité NID-FE, les conditions suivantes doivent être réunies: 1) l'équipement UE et l'entité TAA-FE doivent avoir des données de clé partagée, lesquelles peuvent être générées après la procédure d'authentification mutuelle; 2) l'équipement UE doit connaître les informations d'entité NID-FE, telles que l'adresse, pour pouvoir envoyer la demande d'association de sécurité à l'entité NID-FE. La façon dont l'équipement UE obtient les informations d'entité NID-FE ne relève pas du champ d'application de la présente Recommandation.

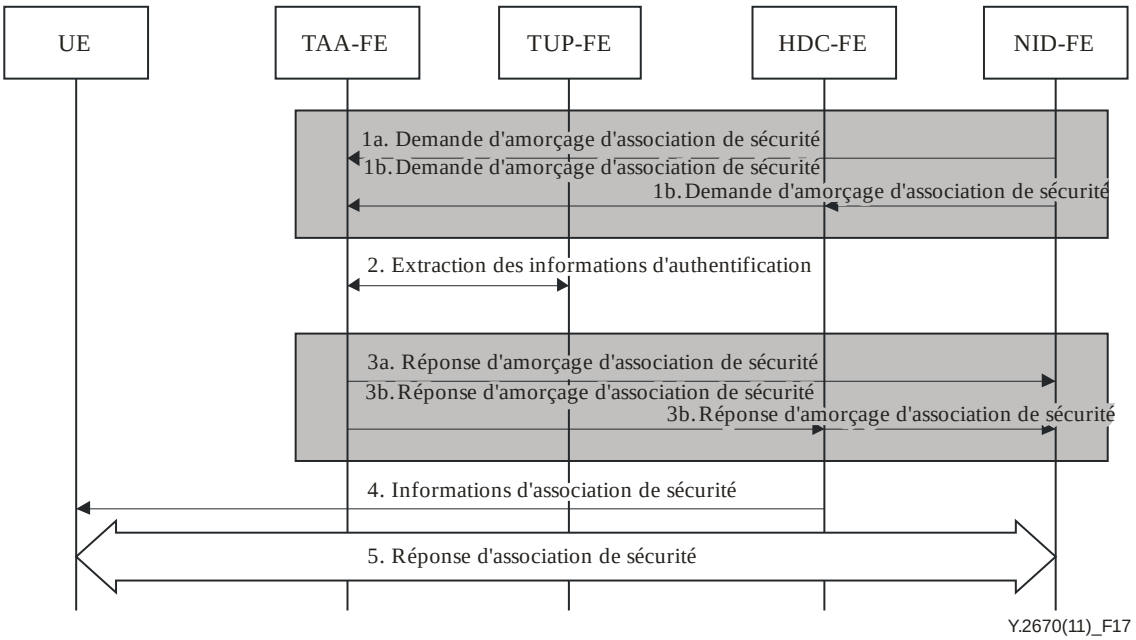

Figure 17 – Etablissement d'une association de sécurité déclenché par le réseau

1) L'entité NID-FE envoie une demande d'amorçage d'association de sécurité, qui comprend les informations d'entité NID-FE, à l'entité TAA-FE. Si l'entité NID-FE ne prend pas en charge l'envoi d'une demande d'amorçage d'association de sécurité directement à l'entité TAA-FE, elle envoie une demande l'amorçage d'association de sécurité à l'entité TAA-FE via l'entité HDC-FE.

2) L'entité TAA-FE interagit avec l'entité TUP-FE et génère des données de clé pour l'entité NID-FE.

3) L'entité TAA-FE envoie une réponse d'amorçage d'association de sécurité, qui contient les informations d'authentification, à l'entité NID-FE. Les informations d'authentification comprennent les données de clé et la durée de vie de la clé. Si l'entité TAA-FE ne prend pas en charge l'envoi d'une réponse d'amorçage d'association de sécurité directement à l'entité NID-FE, elle envoie une réponse d'amorçage d'association de sécurité à l'entité NID-FE via l'entité HDC-FE.

4) L'entité NID-FE envoie les informations d'association de sécurité, qui comprennent les informations d'authentification, à l'équipement UE protégé par les données de clé partagée.

5) L'équipement UE génère les données de clé partagée et valide les informations d'association de sécurité. L'association de sécurité est créée par l'entité NID-FE et l'équipement UE d'après les données de clé partagée.

11.3 Etablissement d'une association de sécurité entre l'équipement UE et l'entité NID-FE fondé sur une infrastructure PKI

La procédure d'établissement d'une association de sécurité entre l'équipement UE et l'entité NID-FE fondé sur une infrastructure PKI est décrite dans la Figure 18. Pour pouvoir appliquer la procédure d'établissement d'une association de sécurité entre l'équipement UE et l'entité HDC-FE, l'équipement UE doit connaître les informations d'entité NID-FE, comme l'adresse, pour pouvoir envoyer la demande d'association de sécurité à l'entité NID-FE. La façon dont l'équipement UE obtient les informations d'entité NID-FE ne relève pas du champ d'application de la présente Recommandation.

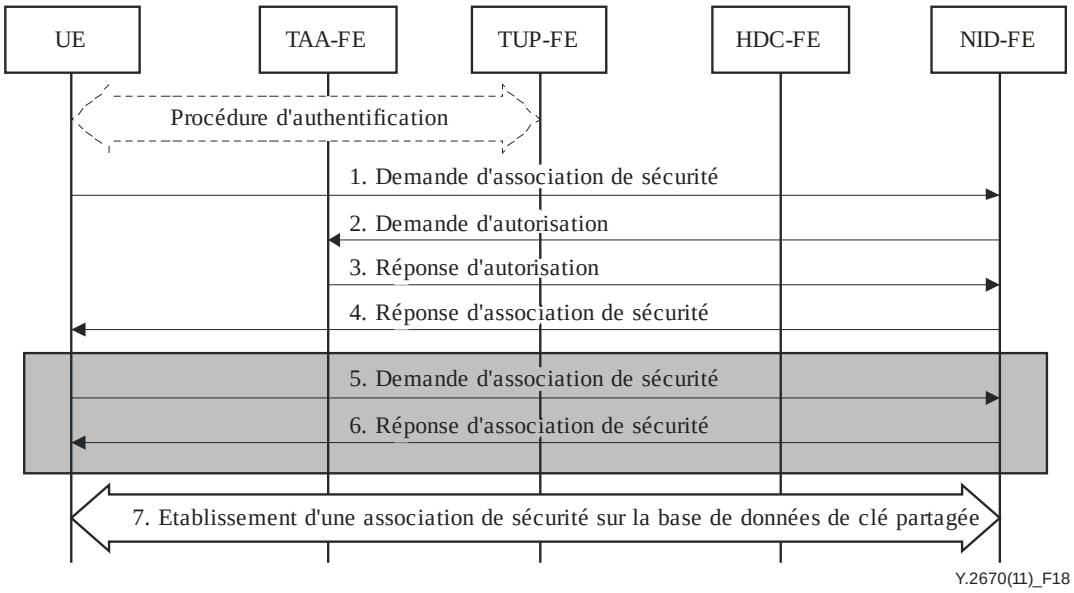

Figure 18 – Etablissement d'une association de sécurité fondé sur une infrastructure PKI

Une fois la procédure d'authentification entre l'entité TUP-FE et l'entité TAA-FE achevée, la procédure ci-après est appliquée.

1) L'équipement UE envoie une demande d'association de sécurité, qui comprend le certificat d'équipement UE et les informations d'équipement UE, à l'entité NID-FE.

2) L'entité NID-FE valide le certificat d'équipement UE et envoie une demande d'autorisation, qui comprend les informations d'équipement UE et les informations d'entité NID-FE, à l'entité TAA-FE.

3) L'entité TAA-FE vérifie l'autorisation sur la base des informations d'équipement UE et des informations d'entité NID-FE. Si l'équipement UE est autorisé à utiliser l'entité NID-FE, l'entité TAA-FE envoie une réponse d'autorisation, qui contient les informations d'autorisation et le certificat de serveur, à l'entité NID-FE.

4) L'entité NID-FE reçoit les informations d'autorisation et envoie une réponse d'association de sécurité, qui comprend le certificat de serveur, à l'équipement UE.

5) S'il faut des données de clé partagée entre l'équipement UE et l'entité TAA-FE, l'entité TAA-FE envoie les informations de calcul de clé à l'équipement UE lors de l'étape 4). L'équipement UE génère des données de clé partagée à partir des informations de calcul de clé et des informations de calcul de clé locale reçues. L'équipement UE envoie les informations de calcul de clé locale à l'entité NID-FE dans le cadre d'une demande d'association de sécurité.

6) L'entité NID-FE génère les données de clé à partir des informations de calcul de clé et des informations de calcul de clé locale reçues. L'entité NID-FE envoie la réponse d'association de sécurité à l'équipement UE.

7) L'association de sécurité entre l'équipement UE et l'entité NID-F est établie.

12 Sécurité des fonctions de transport

12.1 Sécurité entre l'équipement UE et l'entité fonctionnelle de nœud d'accès

Le trafic entre l'équipement UE et l'entité AN-FE devrait être protégé. L'association de sécurité entre l'équipement UE et l'entité AN-FE repose sur les données de clé partagée. Une fois la procédure d'authentification entre l'équipement UE et l'entité TAA-FE menée à bien, l'équipement UE et l'entité TAA-FE génèrent tous deux des données de clé, comme la clé de session, pour protéger le trafic entre l'équipement UE et l'entité AN-FE. L'entité TAA-FE envoie les données de clé à l'entité AN-FE via les entités AM-FE et AR-FE.

12.2 Sécurité entre l'équipement UE et la fonction L3HEF (fonction d'exécution de transfert intercellulaire de couche 3)

Le trafic entre l'équipement UE et la fonction L3HEF devrait être protégé. L'association de sécurité entre l'équipement UE et la fonction L3HEF repose sur les données de clé prépartagée. Une fois la procédure d'authentification mutuelle menée à bien, l'équipement UE et l'entité TAA-FE génèrent tous deux les données de clé, comme la clé de session, pour protéger le trafic entre l'équipement UE et la fonction L3HEF. La fonction L3HEF obtient les données de clé auprès de l'entité TAA-FE directement ou via l'entité AM-FE ou HDC-FE.

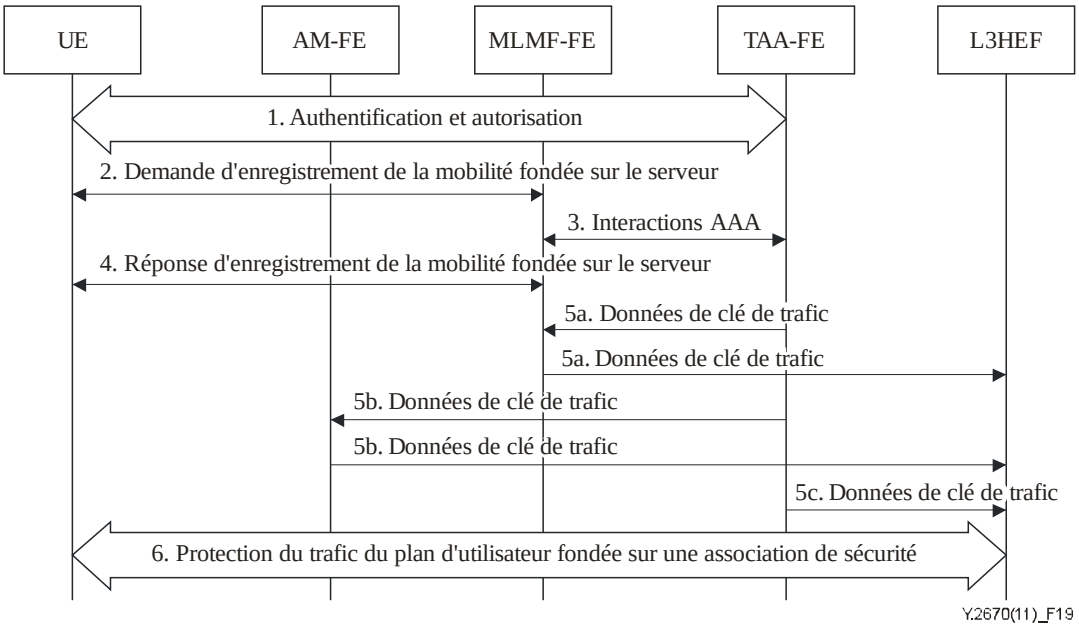

Figure 19 – Procédure permettant d'assurer la sécurité du trafic dans le plan d'utilisateur entre l'équipement UE et la fonction L3HEF

1) La connexion est établie entre l'équipement UE et l'entité TAA-FE. Une fois l'authentification mutuelle terminée, l'équipement UE et l'entité TAA-FE disposent de données de clé partagée, comme les données de clé transitoire et les données de clé de session.

2) L'équipement UE envoie une demande d'enregistrement de la mobilité fondée sur le serveur à l'entité MLM-FE pour créer une association de sécurité de mobilité fondée sur le serveur.

3) L'entité MLM-FE obtient les données de clé en interagissant avec l'entité TAA-FE. Elle authentifie l'équipement UE d'après les données de clé. Une fois l'authentification menée à bien, l'entité MLM-FE crée une association de sécurité avec l'équipement UE d'après les données de clé.

4) L'entité MLM-FE envoie une réponse d'enregistrement de la mobilité fondée sur le serveur à l'équipement UE. L'équipement UE valide le message de réponse d'enregistrement de la mobilité fondée sur le serveur et crée une association de sécurité avec l'entité MLM-FE.

5) Une fois les associations de sécurité entre l'équipement UE et l'entité MLM-FE créées, il existe trois possibilités:

   5a. L'entité TAA-FE génère les données de clé de trafic qu'elle envoie à la fonction L3HEF via l'entité MLM-FE.

   5b. L'entité TAA-FE génère les données de clé de trafic qu'elle envoie à la fonction L3HEF via les entités MLM-FE et AM-FE.

   5c. L'entité TAA-FE envoie les données de clé de trafic directement à la fonction L3HEF.

6) La fonction L3HEF utilise les données de clé de trafic pour protéger le trafic dans le plan d'utilisateur entre l'équipement UE et la fonction L3HEF.

Appendice I

(Cet appendice fait partie intégrante de la présente Recommandation.)

I.1 Exemple de procédure complète d'authentification

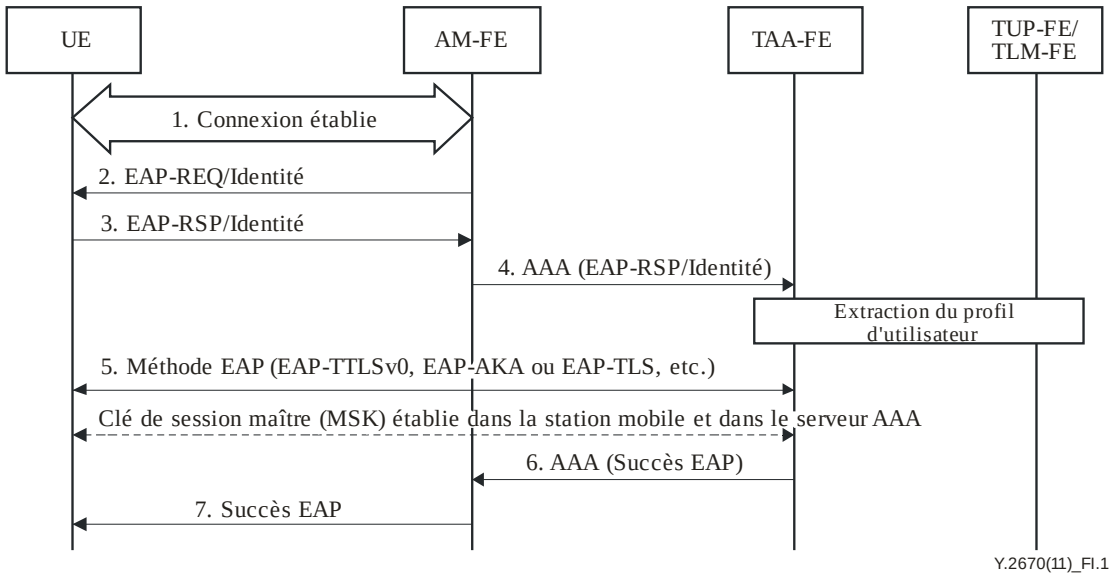

Figure I.1 – Procédure complète d'authentification

NOTE – L'identité dans les étapes 2. à 4. désigne l'identité de l'équipement UE.

La Figure I.1 décrit l'amorçage de l'authentification.

1) La connexion est établie entre l'équipement UE et l'entité AM-FE.
2) L'entité AM-FE envoie une demande EAP (EAP-REQ)/Identité à l'équipement UE [b-IETF RFC 3748].
3) L'équipement UE envoie un message de réponse EAP (EAP-RSP)/Identité.
4) L'entité AM-FE réexpédie le message EAP-RSP/Identité à l'entité TAA-FE, puis l'entité TAA-FE échange des informations avec l'entité TUP-FE/TLM-FE, qui envoie les informations d'utilisateur, dont le profil, à l'entité TAA-FE.
5) L'entité TAA-FE et l'équipement UE s'acquittent du processus de calcul et de distribution de clé. Plusieurs méthodes peuvent être envisagées, par exemple EAP-TTLS, EAP-AKA, EAP-TLS, etc.
6) L'entité TAA-FE envoie le message de succès EAP à l'entité AM-FE.
7) L'entité AM-FE informe l'équipement UE que l'authentification a été menée à bien en envoyant un message de succès EAP. Le processus d'échange de clé fondé sur le protocole EAP a donc été effectué avec succès et l'équipement UE et l'entité AM-FE partagent les données de calcul de clé obtenues pendant cet échange.

I.2 Exemple de procédure de réauthentification rapide

Pendant le transfert intercellulaire, la réauthentification rapide peut permettre d'assurer la continuité de service lorsque le temps de latence est long. Cette procédure suppose l'utilisation d'un identificateur de réauthentification rapide mais il n'est pas nécessaire que les entités TAA-FE et TUP-FE/TLM-FE échangent des informations d'authentification.

La procédure générale de réauthentification rapide est la suivante.

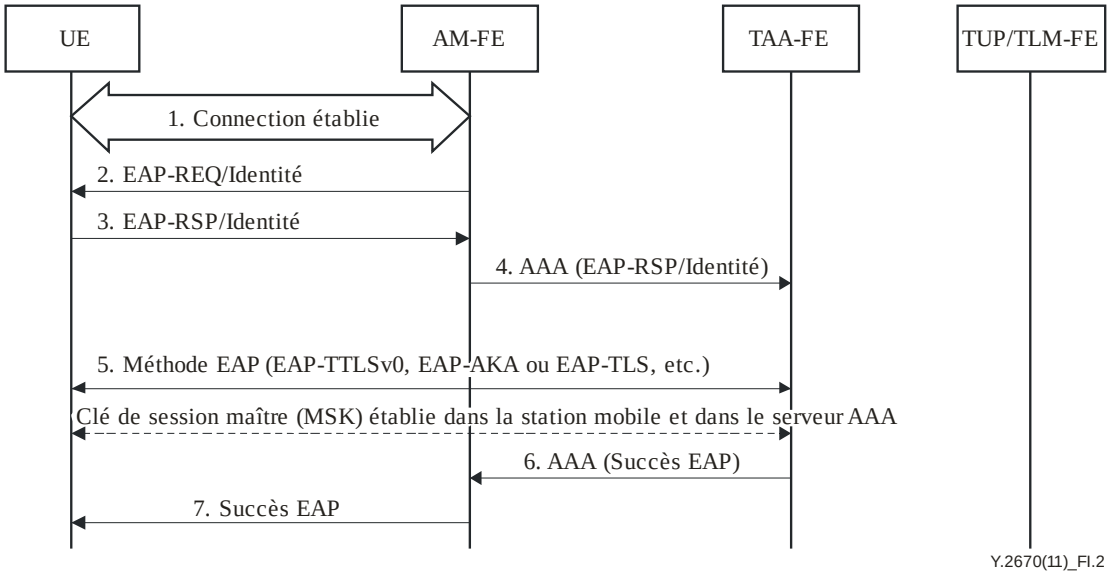

Figure I.2 – Procédure de réauthentification rapide

1) La connexion est établie entre l'équipement UE et l'entité AM-FE.
2) L'entité AM-FE envoie une demande EAP-REQ/Identité contenant l'identificateur de réauthentification à l'équipement UE.
3) L'équipement UE envoie un message de réponse EAP/Identité.
4) L'entité AM-FE réexpédie le message EAP-RSP/Identité à l'entité TAA-FE.
5) Le processus de calcul et de distribution de clé est exécuté. Plusieurs méthodes peuvent être envisagées, par exemple EAP-AKA, EAP-TLS, etc.
6) L'entité TAA-FE envoie le message de succès EAP à l'entité AM-FE.
7) L'entité AM-FE informe l'équipement UE que l'authentification a été menée à bien en envoyant un message de succès EAP. Le processus d'échange de clé fondé sur le protocole EAP a donc été effectué avec succès et l'équipement UE et l'entité AM-FE partagent les données de calcul de clé obtenues pendant cet échange.

I.3 Exemple de mobilité fondée sur le serveur

Dans le cas du protocole MIPv4, la sécurité de la mobilité IP repose sur des extensions d'authentification MIP définies dans [b-IETF RFC 3344]. Les messages de signalisation de mobilité IP doivent être protégés entre l'équipement UE et le nœud faisant office d'agent de rattachement (HA) (c'est-à-dire l'entité MLM-FE) à l'aide des extensions d'authentification MIP et, à titre facultatif, entre l'équipement UE et le nœud faisant office d'agent étranger (FA) (c'est-à-dire l'entité MLM-FE).

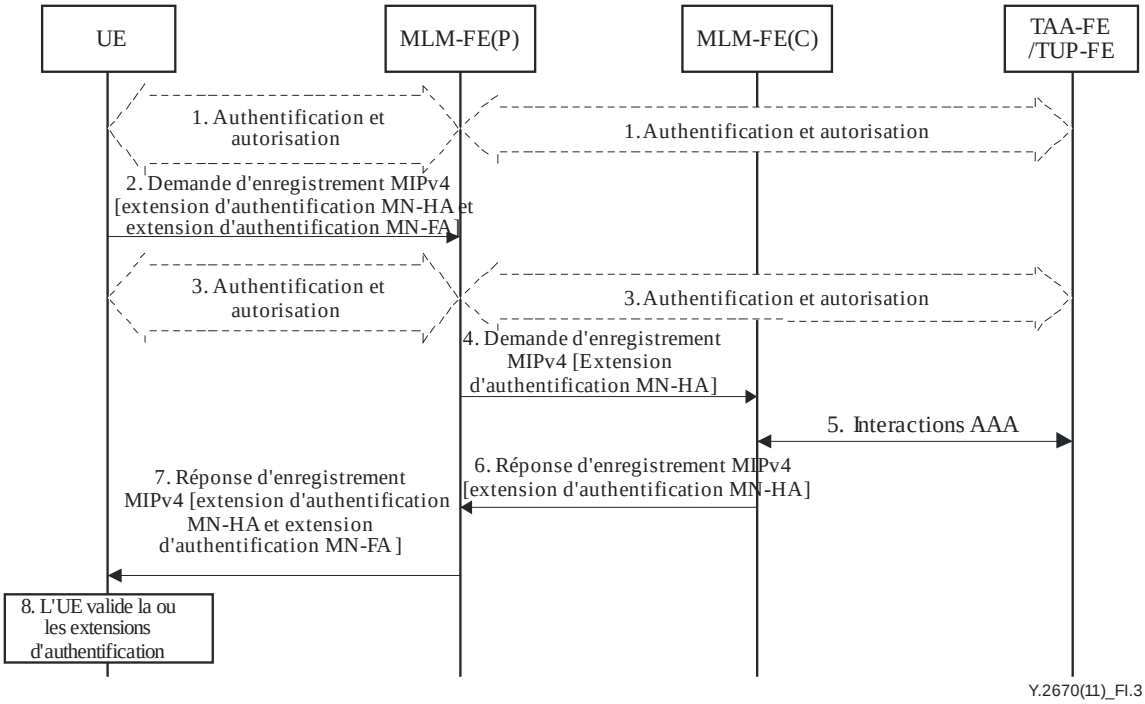

Figure I.3 – Procédure d'amorçage MIPv4

La procédure d'amorçage MIPv4 présentée dans la Figure I.3 est la suivante.

1) Une authentification et une autorisation sont créées entre l'équipement UE et l'entité MLM-FE avec l'aide de l'entité TAA-FE /TUP-FE.

2) L'équipement UE envoie un message de demande d'enregistrement (RRQ) à l'agent étranger (entité MLM-FE). L'équipement UE fait figurer l'extension d'authentification de l'agent MN-HA et, à titre facultatif, l'extension d'authentification de l'agent MN-FA comme spécifié dans [b-IETF RFC 3344].

3) La demande RRQ déclenche la procédure d'authentification de l'accès.

4) L'agent étranger traite le message conformément à [b-IETF RFC 3344] et valide l'extension d'authentification de l'agent MN-FA si elle est présente. L'agent étranger réexpédie ensuite le message RRQ à l'agent de rattachement (entité MLM-FE).

5) L'entité MLM-FE sélectionnée obtient les informations d'authentification et d'autorisation auprès de l'entité TAA-FE/TUP-FE.

6) L'entité MLM-FE valide l'extension d'authentification de l'agent MN-HA. Une fois l'extension d'authentification validée, l'entité MLM-FE envoie une réponse d'enregistrement (RRP) à l'équipement UE par l'intermédiaire de l'agent étranger.

7) L'agent étranger traite la réponse RRP conformément à [b-IETF RFC 3344]. L'agent étranger réexpédie ensuite la réponse RRP à l'équipement UE. Il fait figurer l'extension d'authentification de l'agent MN-FA, s'il a reçu l'extension d'authentification de l'agent MN-FA dans le message RRQ.

8) L'équipement UE valide l'extension d'authentification de l'agent MN-HA et celle de l'agent MN-FA, si elle est présente.

Bibliographie

[b-IETF RFC 3220] IETF RFC 3220 (2002), *IP Mobility Support for IPv4*.

[b-IETF RFC 3344] IETF RFC 3344 (2002), *IP Mobility Support for IPv4*.

[b-IETF RFC 3748] IETF RFC 3748 (2004), *Extensible Authentication Protocol (EAP)*.

[b-IETF RFC 3775] IETF RFC 3775 (2004), *Mobility Support in IPv6*.

[b-IETF RFC 4555] IETF RFC 4555 (2006), *IKEv2 Mobility and Multihoming Protocol (MOBIKE)*.

[b-IETF RFC 5213] IETF RFC 5213 (2008), *Proxy Mobile IPv6*.

[b-3GPP TS 33.102] 3GPP TS 33.102 V7.1.0 (2007), *3G Security: Security Architecture*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	**Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération**
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2012