Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2703

(01/2009)

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

Réseaux de prochaine génération – Sécurité

Application du service d'authentification, d'autorisation et de comptabilité dans les réseaux de prochaine génération

Recommandation UIT-T Y.2703

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 futurs	Y.2600–Y.2699
Sécurité	**Y.2700–Y.2799**
Mobilité généralisée	Y.2800–Y.2899
Environnement ouvert de qualité opérateur	Y.2900–Y.2999

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

Recommandation UIT-T Y.2703

Application du service d'authentification, d'autorisation et de comptabilité dans les réseaux de prochaine génération

Résumé

La Recommandation UIT-T Y.2703 décrit une application de l'authentification, de l'autorisation et de la comptabilité (AAA, *authentication, authorization and accounting*) pour les réseaux de prochaine génération (NGN, *next generation network*) de version 1.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T Y.2703	2009-01-23	13

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

		Page
1	Domaine d'application	1
2	Références	1
3	Définitions	1
	3.1 Termes définis ailleurs	1
	3.2 Termes définis dans la présente Recommandation	2
4	Abréviations et acronymes	2
5	Conventions	2
6	Concepts généraux relatifs au service AAA	2
	6.1 Aperçu	2
	6.2 Processus AAA	3
	6.3 Procédure AAA	3
7	Modèle d'application pour l'authentification et l'autorisation dans les NGN	3
8	Architecture AAA dans les NGN	5
	8.1 Accès de l'utilisateur au réseau	6
	8.2 Rattachement d'un utilisateur à un service de réseau	7
	8.3 Authentification et autorisation d'un utilisateur pour l'accès à un service de tiers	7
9	Inscription	8
10	Authentification	8
	10.1 Entités d'authentification	8
	10.2 Procédure d'authentification	8
11	Autorisation	10
	11.1 Aspects relatifs à l'autorisation dans un NGN	10
	11.2 Entités d'autorisation	10
	11.3 Procédure d'autorisation	11
12	Comptabilité	11
	12.1 Comptabilité de la sécurité	11
	12.2 Fonctions de la comptabilité de la sécurité	12
Appendice I – Protocole d'authentification pour le service AAA dans les NGN		13
	I.1 Protocole EAP pour le service AAA dans les NGN	13
	I.2 Protocoles AAA	14
Appendice II – Certificats numériques X.509 en tant que justificatifs d'identité		15
Appendice III – Authentification et autorisation: cas d'utilisation		16
	III.1 Authentification et autorisation d'utilisateur pour l'accès au réseau	16
	III.2 Authentification et autorisation d'un utilisateur par un fournisseur de service NGN pour l'accès à un service/à une application	18
	III.3 Authentification et autorisation d'un fournisseur NGN par un utilisateur	20

Page

III.4 Authentification et autorisation d'un fournisseur de service/application tiers par un fournisseur NGN 21

III.5 Utilisation d'un service d'authentification et d'autorisation de tiers 22

Bibliographie..... 24

Recommandation UIT-T Y.2703

Application du service d'authentification, d'autorisation et de comptabilité dans les réseaux de prochaine génération

1 Domaine d'application

La présente Recommandation décrit une application de l'authentification, de l'autorisation et de la comptabilité (AAA) dans les réseaux de prochaine génération (NGN), compte tenu de [b-UIT-T Y.2201] (*Spécifications des réseaux de prochaine génération de version 1*), [b-UIT-T Y.2012] (*Prescriptions fonctionnelles et architecture du réseau de prochaine génération version 1*), [b-UIT-T Y.2701] (*Prescriptions de sécurité des réseaux de prochaine génération de version 1*) et [b-UIT-T Y.2702] (*Spécifications d'authentification et d'autorisation dans les réseaux de prochaine génération de version 1*). La présente Recommandation porte sur le processus d'authentification, d'autorisation et de comptabilité lors de l'accès à un NGN au moyen d'un client AAA et d'un serveur AAA. Toutefois, la présente Recommandation n'examine la fonction de comptabilité que du point de vue de sa contribution à la comptabilité de la sécurité.

Le domaine d'application de la présente Recommandation est le suivant:

1) Processus d'inscription
2) Fonctions et procédures d'authentification
3) Fonctions et procédures d'autorisation
4) Fonctions et procédures de comptabilité de la sécurité

2 Références

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 authentification [b-UIT-T X.811]: attestation de l'identité revendiquée par une entité.

3.1.2 certificat d'authentification [b-UIT-T X.811]: certificat de sécurité qui est garanti par une autorité d'authentification et qui peut être utilisé pour attester l'identité d'une entité.

3.1.3 informations d'authentification (AI, *authentication information*) [b-UIT-T X.811]: renseignements utilisés aux fins de l'authentification.

3.1.4 autorisation [b-UIT-T X.800]: attribution de droits, comprenant la permission d'accès sur la base de droits d'accès.

3.1.5 déclarant [b-UIT-T X.811]: entité qui est ou qui représente une entité principale à des fins d'authentification. Un déclarant comporte les fonctions nécessaires pour engager des échanges pour authentification au nom d'une entité principale.

3.1.6 journal d'audit de sécurité [b-UIT-T X.800]: données collectées et pouvant éventuellement être utilisées pour permettre un audit de sécurité.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit le terme suivant:

3.2.1 comptabilité de la sécurité: rôle consistant à suivre les actions ou événements liés à la sécurité qui peuvent être inclus comme ressources dans la fonction d'audit de sécurité.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

AAA authentification, autorisation et comptabilité (*authentication, authorization and accounting*)

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

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

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

ID identité – telle qu'elle est définie par le réseau, le service ou l'entité faisant l'objet d'un accès

NAS serveur d'accès au réseau (*network access server*)

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

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

NP fournisseur de réseau (*network provider*)

OAMP exploitation, administration, maintenance et fourniture (*operations, administration, maintenance and provision*)

RACF fonction de contrôle d'accès aux ressources (*resource access control function*)

SCTP protocole de transport de contrôle de flux (*stream control transport protocol*)

SR ressource de service (*service resource*)

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

TE équipement terminal (*terminal equipment*)

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

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

5 Conventions

Aucune.

6 Concepts généraux relatifs au service AAA

Le présent paragraphe porte sur les concepts généraux relatifs au service AAA.

6.1 Aperçu

Le service d'authentification, d'autorisation et de comptabilité fournit les fonctions permettant de vérifier l'identité d'un utilisateur (authentification), de lui donner un accès aux services (autorisation) et fournit un moyen permettant de mesurer la consommation des ressources (comptabilité).

6.2 Processus AAA

Les différents processus inclus dans le cadre AAA sont les suivants:

L'authentification valide l'identité de l'utilisateur final avant d'autoriser l'accès au réseau. L'utilisateur final présente un ensemble de justificatifs d'identité, par exemple une combinaison nom d'utilisateur/mot de passe, une clé de sécurité, un certificat ou des données biométriques (par exemple, empreintes digitales). Ces justificatifs d'identité sont normalement convenus pendant le processus d'inscription. La vérification des justificatifs d'identité conduit au processus d'autorisation.

L'autorisation définit les privilèges et services autorisés pour l'utilisateur final une fois que l'accès au réseau a été accordé. Pour cela, une adresse IP peut devoir être fournie ou un filtre peut devoir être invoqué pour déterminer quelles applications ou quels protocoles sont pris en charge. L'authentification et l'autorisation sont réalisées ensemble dans le contexte d'une gestion AAA.

La comptabilité donne la méthodologie de collecte des informations sur la consommation des ressources par l'utilisateur final, informations qui peuvent ensuite être traitées à des fins de facturation, d'audit et de planification de capacité. Certaines données comptables sont utiles pour élaborer un journal d'audit de sécurité.

Ces trois processus sont centralisés dans un ensemble de fonctions qui, ensemble, constituent le contrôle d'accès.

6.3 Procédure AAA

Le système de service AAA est composé d'un serveur AAA et d'un client AAA.

Le serveur AAA a accès à une base de données de profils d'utilisateur et à des données de configuration. Il communique avec des clients AAA qui résident dans des éléments de réseau comme le serveur d'accès au réseau (NAS) et les routeurs, pour assurer des services AAA répartis.

Les grandes étapes des scénarios de service AAA sont les suivantes:

- L'utilisateur final se raccorde au dispositif de point d'entrée et demande l'accès au réseau.
- Le client AAA retransmet les justificatifs d'identité/d'authentification de l'utilisateur final au serveur AAA.
- Le serveur AAA authentifie l'utilisateur sur la base de ces justificatifs. Si l'authentification aboutit, le serveur détermine alors quel(s) service(s) est (sont) autorisés et retourne une réponse d'acceptation ou de rejet et d'autres données utiles au client AAA.
- Le client AAA indique à l'utilisateur final que l'accès aux ressources spécifiées a été accordé ou refusé.

Le client AAA envoie un message de comptabilité au serveur AAA pendant l'établissement et la terminaison de la connexion en vue de la collecte et du stockage des relevés.

7 Modèle d'application pour l'authentification et l'autorisation dans les NGN

La présente Recommandation est basée sur les exigences de sécurité pour les NGN énoncées dans [b-UIT-T Y.2701] et le modèle de référence pour l'authentification dans les NGN présenté dans [b-UIT-T Y.2702]. Sur le modèle de référence pour l'authentification dans les NGN (Figure 7-1), figurent huit points de référence pour l'authentification, dont trois sont pris en considération dans la présente Recommandation.

Ce sont:

(1) accès d'un utilisateur au réseau;

(2) accès d'un utilisateur à un service fourni par le réseau;

(4) accès du fournisseur de service à l'utilisateur de destination.

Les points de référence (1) et (4) renvoient au transport de trafic d'utilisateur et peuvent être considérés comme dépendant du contrôle d'accès "horizontal" au niveau de la commande de transport, tandis que les points de référence (2) et (8) peuvent être considérés comme dépendant des données de commande entre les couches de commande de transport et de service et donc comme étant "verticaux". Cette relation est illustrée sur la Figure 7-2.

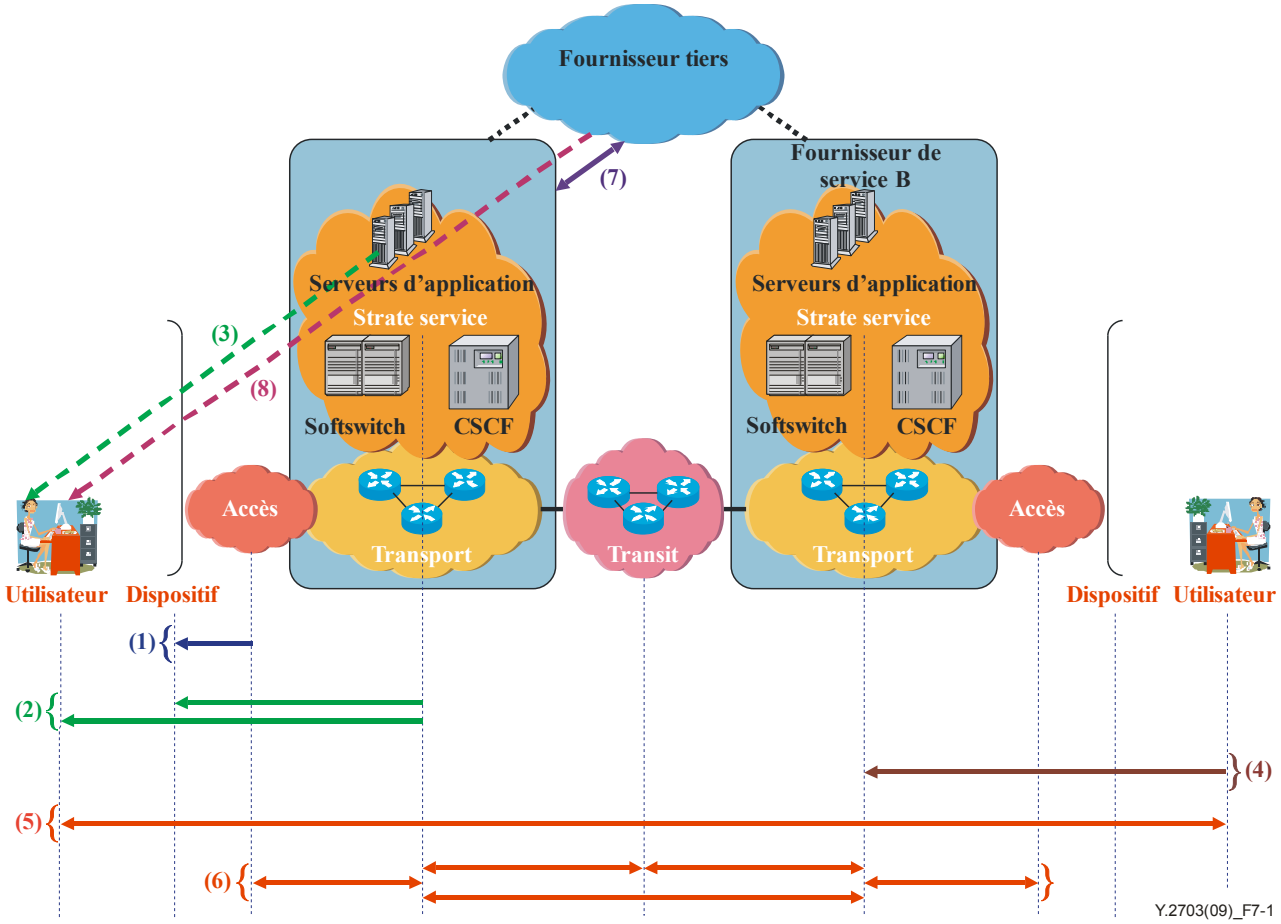

Figure 7-1 – Modèle architectural de référence de bout en bout (Y.2702)

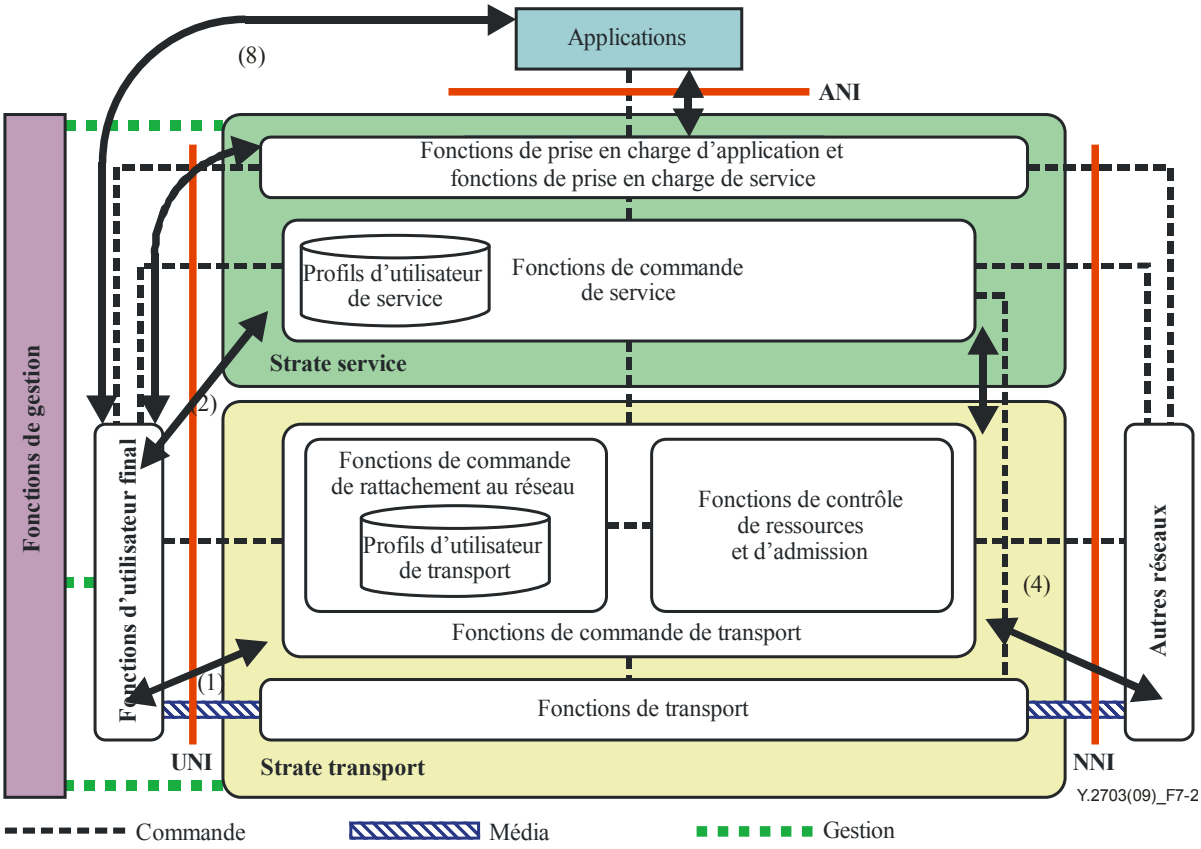

Figure 7-2 – Architecture du NGN et domaines liés au service AAA (Y.2702)

8 Architecture AAA dans les NGN

Le présent paragraphe décrit la relation entre le modèle de référence AAA et le modèle architectural fonctionnel décrit dans [b-UIT-T Y.2012].

8.1 Accès de l'utilisateur au réseau

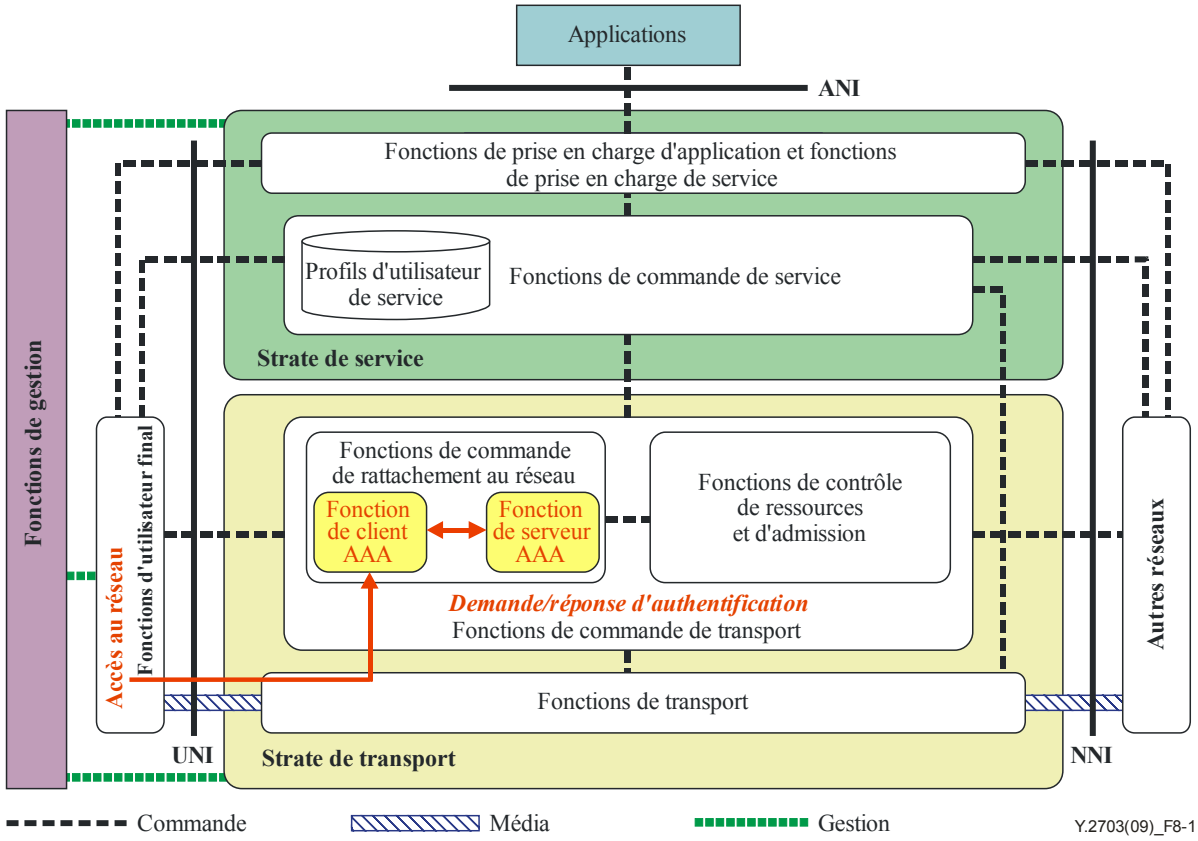

Figure 8-1 – Authentification et autorisation d'un utilisateur pour l'accès au réseau

La Figure 8-1 illustre l'application du service AAA pour l'accès d'un utilisateur au réseau (application de type 1 sur la Figure 7-1 ci-dessus).

Dès qu'une entité des fonctions de commande de transport (généralement l'entité fonctionnelle T-14 (AM-FE)) détecte une demande de connexion provenant du terminal d'un utilisateur, elle commence à remplir le rôle de client AAA. Elle demande aux entités des fonctions de commande de transport qui jouent le rôle de serveur AAA (par exemple les entités fonctionnelles T-11 (TAA-FE) et T-12 (TUP-FE)) d'authentifier l'utilisateur et d'autoriser l'utilisation de ressources NGN. On peut utiliser des protocoles comme RADIUS ou Diameter pour cette procédure de demande et réponse. Sur la base d'une demande provenant d'un client AAA, un serveur AAA authentifie l'utilisateur en utilisant des procédures explicites (par exemple EAP) ou implicites (par exemple authentification de la ligne d'accès). Après l'autorisation réussie d'un utilisateur en fonction de son profil (généralement géré par l'entité fonctionnelle TUP-FE), le serveur AAA demande à la fonction RACF de réserver et d'attribuer des ressources NGN pour cet utilisateur. Une fois que c'est fait, le serveur AAA indique au client AAA qu'il a la permission de raccorder cet équipement d'utilisateur.

8.2 Rattachement d'un utilisateur à un service de réseau

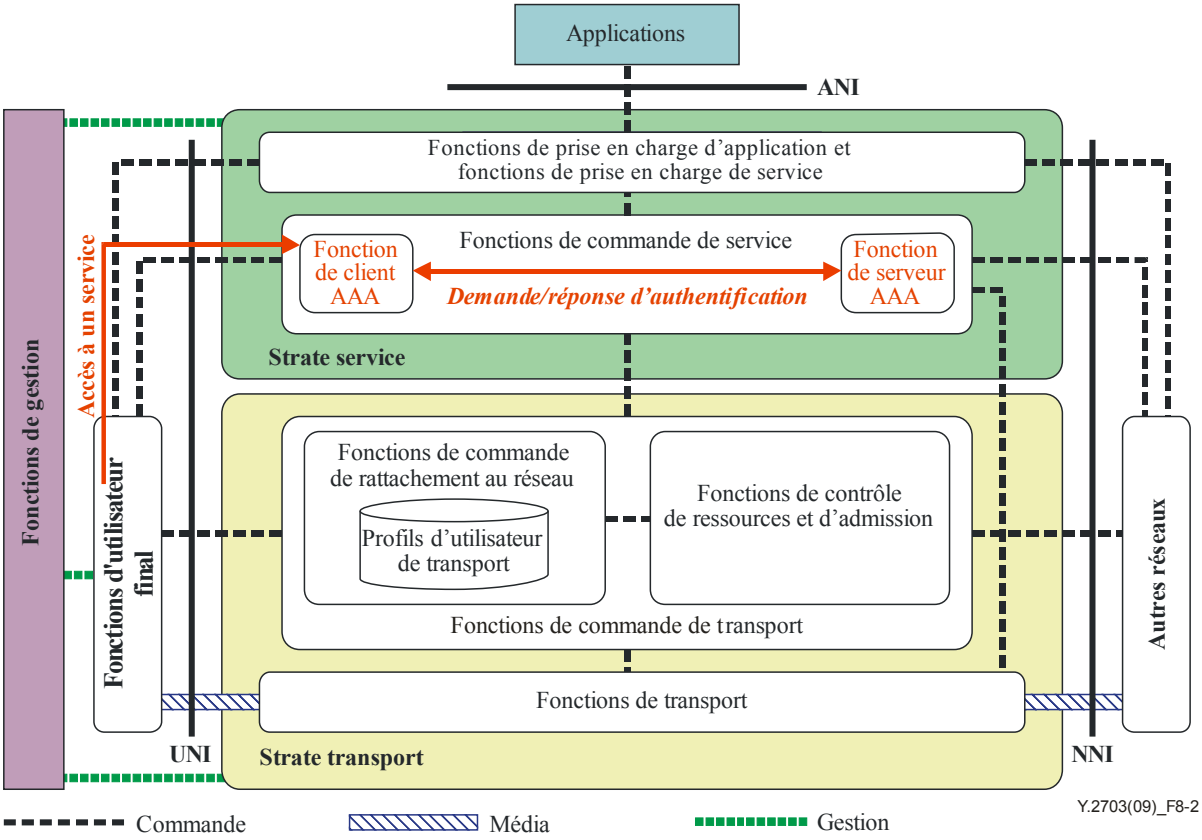

Figure 8-2 – Authentification et autorisation d'un utilisateur pour l'accès à un service

La Figure 8-2 illustre l'application du service AAA pour l'accès d'un utilisateur à un service (application de type 2 sur la Figure 7-1 ci-dessus).

De manière analogue au cas précédent illustré sur la Figure 8-1, un client AAA des fonctions de commande de service (généralement l'entité fonctionnelle S-1 (S-CES-FE)) détecte une demande de connexion provenante du terminal d'un utilisateur. Il demande à un serveur AAA (par exemple l'entité fonctionnelle S-5 (SUP-FE) ou S-6 (SAA-FE)) de procéder à l'authentification et à l'autorisation pour le service demandé. La demande de service est accordée ou rejetée en fonction du résultat de l'authentification et de l'autorisation.

Une fois que l'utilisateur est raccordé au réseau ou au service, chaque client AAA communique à son serveur AAA les informations sur les ressources NGN consommées par l'utilisateur pour aider un serveur AAA à collecter les informations de comptabilité associées à l'utilisateur.

8.3 Authentification et autorisation d'un utilisateur pour l'accès à un service de tiers

Les services de tiers accessibles par le biais de l'interface ANI ne sont pas abordés dans les NGN de version 1. Par conséquent, l'authentification et l'autorisation d'un utilisateur pour l'accès à des services de tiers n'entrent pas dans le domaine d'application de la présente Recommandation. La présente Recommandation n'illustre pas le modèle de référence pour les services de tiers. Toutefois, un cas d'utilisation illustrant l'authentification et l'autorisation associées à un service de tiers est décrit dans l'Appendice III.

9 Inscription

Avant que le service AAA puisse être assuré, il faut d'abord identifier l'entité à authentifier, par exemple l'utilisateur ou le dispositif. Les justificatifs d'identité qui identifient l'entité sont établis par le biais d'un processus d'inscription qui établit l'identité unique d'un utilisateur/dispositif. Les justificatifs d'identité sont utilisés dans le processus d'authentification chaque fois que l'accès à un ou plusieurs services est demandé. Le processus d'inscription peut inclure l'acceptation de conditions générales ainsi que des arrangements financiers. On désigne par inscription la vérification initiale de l'identité et des justificatifs d'identité, tandis qu'on parle d'enregistrement pour l'accès ultérieur aux services et les contrôles des justificatifs d'identité. Les arrangements précis pour l'inscription dépendront des politiques du fournisseur, de la nature des services, etc.

10 Authentification

La présente Recommandation utilise les concepts de base de l'authentification décrits dans [b-UIT-T X.811]. Des services et des capacités d'authentification pour l'accès à un réseau ou à un service sont nécessaires afin de réduire les menaces associées aux tentatives d'obtention d'un accès non autorisé. On trouvera d'autres informations sur les certificats numériques dans l'Appendice II.

10.1 Entités d'authentification

Le terme "déclarant" est employé pour décrire une entité qui demande une authentification. Un déclarant comporte les fonctions nécessaires pour participer à des échanges pour authentification.

Le client AAA assure une fonction spécialisée qui fait partie du chemin d'accès entre le déclarant et l'entité de vérification pour chaque demande d'accès et applique la décision prise par le vérificateur.

Dans le contexte d'une gestion AAA, le serveur AAA est l'entité de vérification, qui envoie un certificat d'authentification au déclarant dès que l'authentification a abouti.

10.2 Procédure d'authentification

Dans le contexte d'une gestion AAA, le serveur AAA assure le service d'authentification de l'utilisateur. Il identifie l'entité demandant un accès de façon suffisante pour déterminer quels services peuvent être autorisés pour l'accès et taxés. Un certificat d'authentification peut être délivré par le serveur AAA.

10.2.1 Authentification réussie

Les étapes suivantes et la Figure 10-1 donnent un exemple de flux de messages pour une authentification réussie.

Etape 1: Une entité demande au client AAA un accès

Etape 2: Le client AAA demande au serveur AAA une authentification de l'entité.

Etape 3: Le serveur AAA demande au client AAA les justificatifs d'identité de l'entité avant de commencer l'authentification.

Etape 4: Le client AAA demande à l'entité le ou les justificatifs d'identité nécessaires pour l'authentification.

Etape 5: L'entité, qui est désormais un déclarant, envoie au client AAA le ou les justificatifs d'identité demandés.

Etape 6: Le client AAA retransmet au serveur AAA le ou les justificatifs d'identité nécessaires en vue de l'authentification.

Etape 7: Le serveur AAA compare le ou les justificatifs d'identité reçus avec le profil d'utilisateur du déclarant.

Etape 8: Si les justificatifs d'identité ont pu être vérifiés, le serveur AAA passe au processus d'autorisation sans informer le client AAA ou le déclarant.

Etape 9: Après le processus d'autorisation, le serveur AAA envoie un message d'autorisation d'accès au client AAA.

Etape 10: Le client AAA retransmet le message d'autorisation d'accès au déclarant.

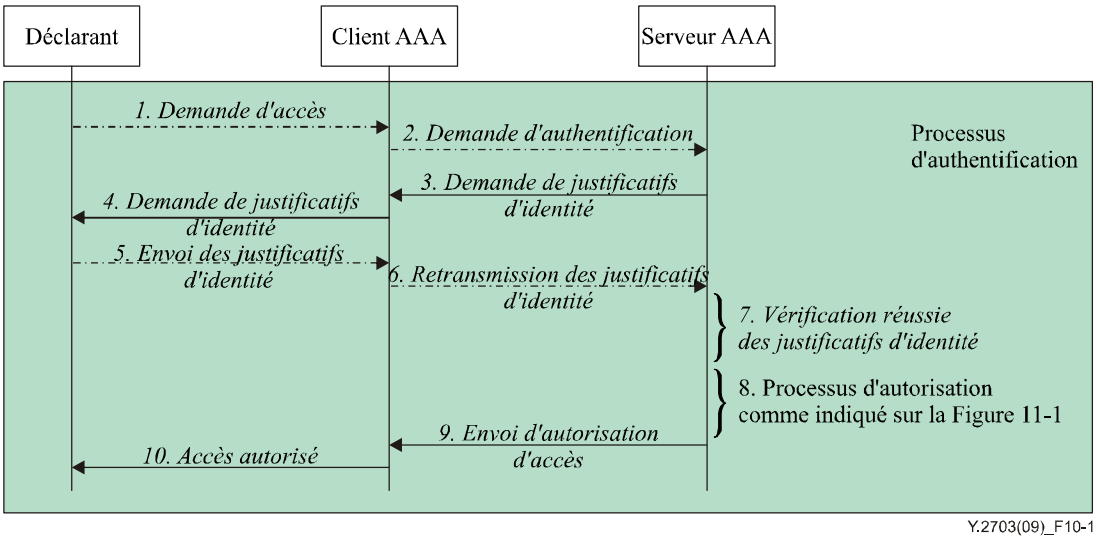

Figure 10-1 – Flux de messages pour une authentification réussie

10.2.2 Echec de l'authentification

Les étapes suivantes et la Figure 10-2 donnent un exemple de flux de messages pour un échec de l'authentification.

Etape 1: Une entité demande au client AAA un accès

Etape 2: Le client AAA demande au serveur AAA une authentification de l'entité.

Etape 3: Le serveur AAA demande au client AAA les justificatifs d'identité de l'entité avant de commencer l'authentification.

Etape 4: Le client AAA demande à l'entité le ou les justificatifs d'identité nécessaires pour l'authentification.

Etape 5: L'entité, qui est désormais un déclarant, envoie au client AAA le ou les justificatifs d'identité demandés.

Etape 6: Le client AAA retransmet au serveur AAA le ou les justificatifs d'identité nécessaires en vue de l'authentification.

Etape 7: Le serveur AAA compare le ou les justificatifs d'identité reçus avec le profil d'utilisateur du déclarant.

Etape 8: Si les justificatifs d'identité n'ont pas pu être vérifiés, le serveur AAA envoie un message de refus d'accès au client AAA.

Etape 9: Le client AAA retransmet le message de refus d'accès au déclarant.

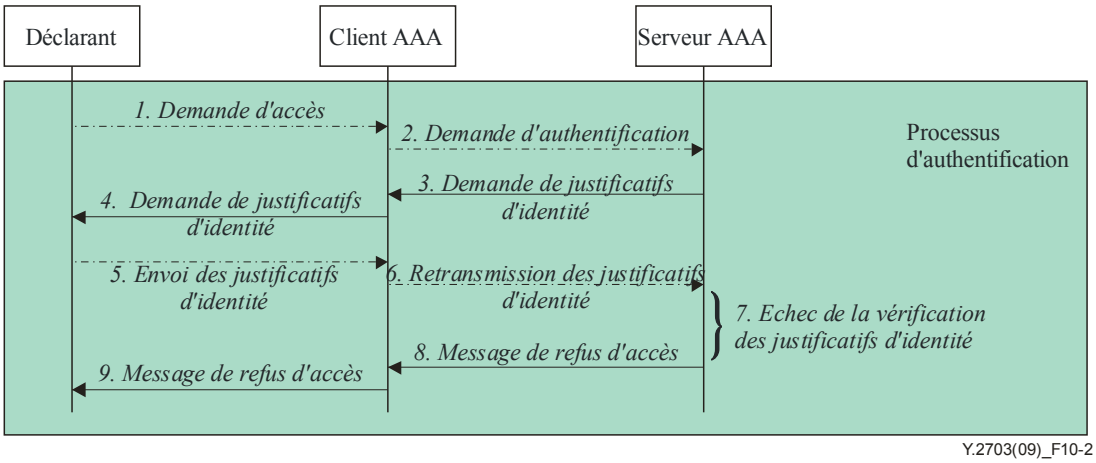

Figure 10-2 – Flux de messages pour un échec de l'authentification

11 Autorisation

L'autorisation est définie comme le fait de déterminer si un certain privilège peut être accordé à celui qui présente un justificatif d'identité particulier. Le privilège peut être le droit d'accéder à une ressource de service (SR) et peut inclure la lecture, l'écriture ou la modification de ressources suivant la politique. Le processus d'autorisation suit l'authentification et approuve ou refuse l'accès au service NGN suivant les résultats des étapes d'authentification précédentes et la politique.

11.1 Aspects relatifs à l'autorisation dans un NGN

L'autorisation a pour objet de fournir et de contrôler l'accès aux services autorisés pour l'utilisateur authentifié. Dans un NGN, le serveur AAA communique avec les éléments de réseau contenant les privilèges d'accès des entités inscrites.

La présente Recommandation considère l'authentification et l'autorisation comme des processus associés, normalement effectués l'un après l'autre pour les entités inscrites chaque fois qu'un accès est demandé. Toutefois, la politique d'un fournisseur peut permettre à une entité de demander des droits d'accès/d'utilisation immédiats sans nouvelle authentification ou inscription. Ce cas n'est pas examiné.

Le processus d'autorisation d'un utilisateur pour un service est réalisé par le serveur AAA, qui communique avec les éléments de réseau appropriés et reçoit de leur part les informations d'autorisation. Dès que le processus d'autorisation est achevé par le serveur AAA, les informations d'acquittement sont retransmises à l'utilisateur demandant le service.

La réception des informations d'acquittement constitue l'aboutissement de l'ensemble des processus d'authentification et d'autorisation, et l'entité qui a demandé l'accès est considérée comme étant raccordée au réseau ou à la ressource de service autorisée.

11.2 Entités d'autorisation

Le processus d'autorisation est réalisé automatiquement par le serveur AAA après l'authentification, sans l'intervention de l'entité qui a demandé l'accès. Le serveur AAA contient une fonction spécialisée qui prend les décisions d'autorisation en appliquant les règles relatives au contrôle d'accès.

11.3 Procédure d'autorisation

La procédure relative au processus d'autorisation est illustrée sur la Figure 11-1:

Etape A: Dès que l'authentification de l'entité a abouti, le serveur AAA identifie les services et ressources disponibles et accessibles pour le déclarant.

Etape B: Dès que l'étape A est terminée, le serveur AAA recommande aux fonctions de commande de transport et de service d'attribuer les services et ressources autorisés au déclarant.

Etape C: Le serveur AAA envoie un message d'autorisation d'accès au client AAA.

Etape D: Le client AAA retransmet le message d'autorisation d'accès au déclarant.

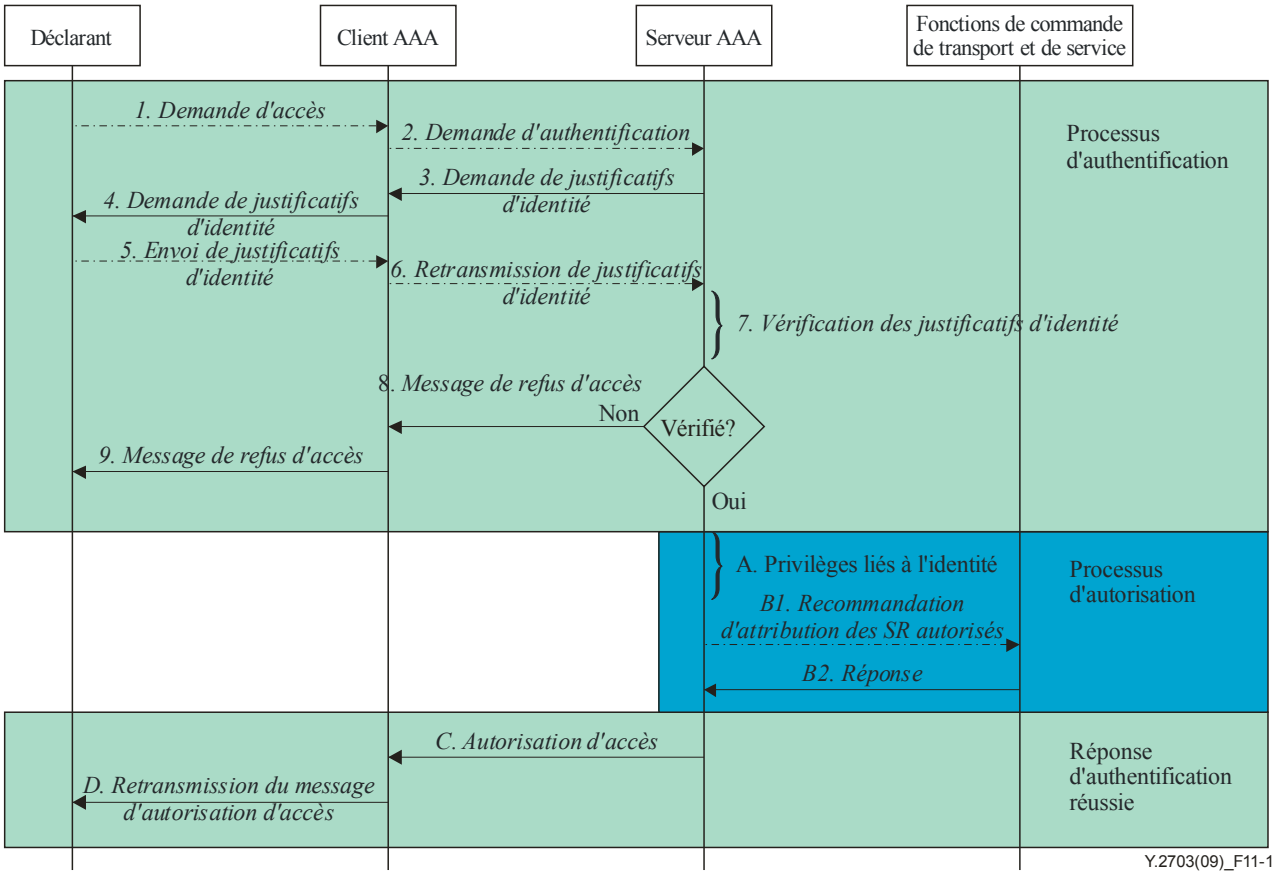

Figure 11-1 – Flux de messages pour le processus d'autorisation

12 Comptabilité

Le dernier "A" de l'acronyme "AAA" désigne la comptabilité (*accounting* en anglais). Dans le contexte AAA, la comptabilité inclut un élément de sécurité qui peut être utilisé en association avec d'autres données relatives aux événements de sécurité afin de prendre en charge une fonction de comptabilité.

12.1 Comptabilité de la sécurité

La comptabilité des événements de sécurité utilise la partie de la fonction de comptabilité qui fournit les données de comptabilité qui sont ensuite utilisées pour élaborer un journal d'audit de sécurité à utiliser par la fonction d'audit de sécurité. Les informations contenues dans le journal d'audit de sécurité dépendent des besoins et de la politique d'audit de sécurité identifiés par le fournisseur NGN pour ce contexte particulier, par exemple les instants de début et de fin de l'accès – ayant abouti ou échoué – à un réseau ou à un service, le service faisant l'objet d'un accès et

les informations d'identité de l'entité qui a demandé l'accès (dans le cas d'une authentification réussie). La fonction d'audit réelle n'entre pas dans le domaine d'application de la présente Recommandation. La procédure de comptabilité de la sécurité est illustrée sur la Figure 12-1.

12.2 Fonctions de la comptabilité de la sécurité

Dans le cadre de la comptabilité de la sécurité, les fonctions réalisées sont notamment les suivantes:

1) Saisie: acquisition des données détectables relatives à un événement et fourniture des informations utiles pour le contexte de sécurité. Les données à saisir peuvent notamment être les suivantes:
   - résultats de l'authentification;
   - informations liées à la révocation de l'authentification et/ou d'un certificat;
   - informations sur la garantie d'authentification;
   - autres informations liées au processus d'authentification.
2) Stockage: conservation des représentations produites par la fonction de saisie.
3) Examen: l'objet est de décrire de façon précise l'événement en vérifiant l'exactitude de ce qui a été saisi et de distinguer les faits en examinant ce qui a été saisi.
4) Rapport: transmission d'informations provenant de la fonction d'examen à une fonction d'audit.
5) Audit: vérification de la question de savoir si un rapport de comptabilité de la sécurité est correct ou conforme à la politique d'utilisation et aux lignes directrices relatives à la sécurité. La fonction d'audit peut nécessiter une capacité d'alerte immédiate.

Il convient de noter que seule la saisie est une fonction AAA, le stockage, l'examen, le rapport et l'audit étant des fonctions de gestion. Ces dernières n'entrent pas dans le domaine d'application de la présente Recommandation.

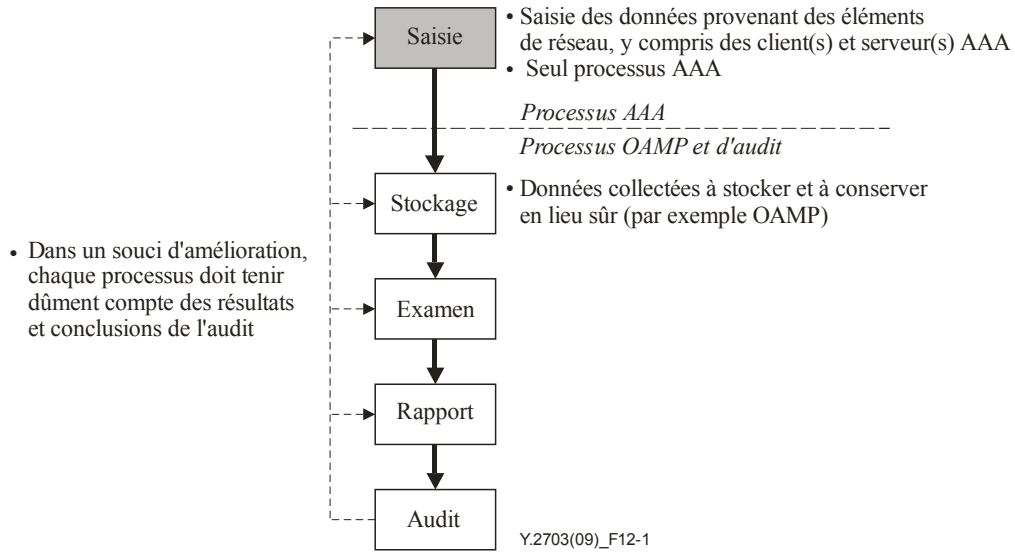

Figure 12-1 – Exemple de processus de comptabilité de la sécurité

Appendice I

Protocole d'authentification pour le service AAA dans les NGN

(Le présent Appendice ne fait pas partie intégrante de la présente Recommandation)

Le présent Appendice traite du protocole EAP qui est transporté sur les couches de liaison de données et des protocoles AAA qui fournissent le cadre AAA au niveau des diverses applications.

I.1 Protocole EAP pour le service AAA dans les NGN

Le protocole EAP définit un cadre d'authentification qui prend en charge diverses méthodes d'authentification. Il est exécuté sur l'homologue et le serveur d'authentification via l'authentificateur. Il est transporté directement sur les couches de liaison de données telles que IEEE 802 et PPP (protocole point à point).

Toutefois, en raison de la caractéristique de dépendance vis-à-vis de la liaison, le protocole EAP a besoin de la couche inférieure, par exemple EAPoL, IEEE 802.1X ou IEEE 802.11i. La Figure I.1 décrit le modèle de multiplexage EAP. La couche de la méthode EAP inclut l'algorithme d'authentification. L'homologue et l'authentificateur EAP ont respectivement une fonctionnalité de client d'authentification et d'authentificateur. La couche EAP assure la distribution des messages EAP. La couche inférieure envoie ou reçoit les trames EAP entre l'homologue et l'authentificateur. Etant donné que la couche de liaison est constituée de plusieurs protocoles de liaison, le protocole EAP nécessite diverses couches inférieures pour chacun des protocoles de liaison.

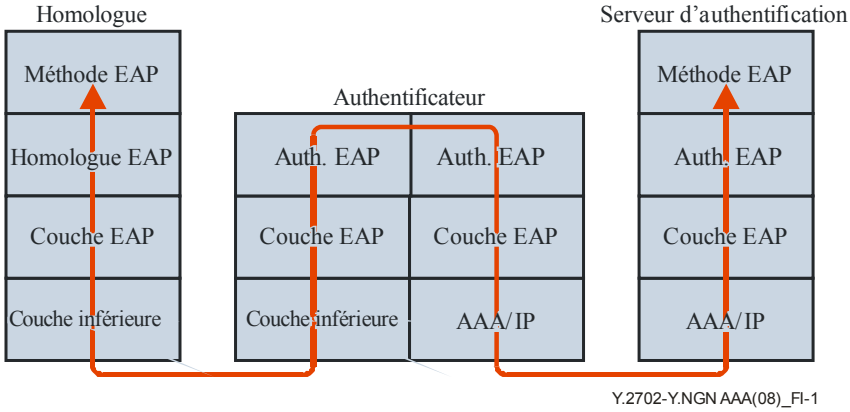

Figure I.1 – Modèle de retransmission EAP

Le protocole EAP nécessite une couche inférieure pour la distribution fiable des messages, la détection des erreurs et le classement dans le bon ordre:

- Etant donné que le protocole EAP ne sait pas que l'homologue reçoit le message provenant de l'authentificateur, il a besoin d'un canal fiable entre l'homologue et l'authentificateur.
- Le protocole EAP ne garantit pas que les messages EAP soient distribués à leur destination sans erreur. Il a besoin d'une fonction de détection des erreurs de la part de la couche inférieure.
- Pour une raison ou pour une autre, il se peut que l'ordre des messages EAP soit modifié ou que certains messages soient dupliqués. Le protocole EAP nécessite donc une détection de duplication et un classement dans le bon ordre afin de garantir des opérations correctes.
- La couche inférieure ne sait pas si la couche supérieure inclut ou pas un protocole d'authentification. Le protocole EAP nécessite une indication du protocole d'authentification.

I.2 Protocoles AAA

Les protocoles AAA tels que RADIUS ont initialement été déployés pour assurer un accès PPP commuté terminal/serveur. Le protocole Diameter a été élaboré lorsque l'Internet s'est généralisé et que de nouvelles technologies d'accès ont été mises en place. Le Tableau I.1 compare les protocoles AAA.

Tableau I.1 – Comparaison des protocoles AAA

	RADIUS	**DIAMETER**
Taille du réseau	Petite	Grande
Transport	UDP	SCTP/TCP
Chiffrement	Mot de passe uniquement	Totalité du paquet
Authentification/autorisation	Combinaison	Combinaison
Norme	IETF	IETF
Architecture du protocole	C/S	P2P
Evolutivité	Faible	Elevée

Dans le cas du protocole RADIUS, la gestion d'ensembles de lignes série et de modems dispersés pour un grand nombre d'utilisateurs peut se traduire par la nécessité d'un support administratif important. Etant donné que les ensembles de modems sont, par définition, des liaisons vers l'extérieur, une attention particulière doit être portée à la sécurité, à l'autorisation et à la comptabilité. Pour cela, la meilleure solution est de gérer une seule "base de données" d'utilisateurs, permettant l'authentification (vérification du nom d'utilisateur et du mot de passe), ainsi que des informations de configuration indiquant le type de service à fournir à l'utilisateur.

Le protocole Diameter de base proprement dit peut être utilisé pour des applications de comptabilité, mais pour l'authentification et l'autorisation, il est toujours étendu pour une application particulière.

Appendice II

Certificats numériques X.509 en tant que justificatifs d'identité

(Le présent Appendice ne fait pas partie intégrante de la présente Recommandation)

Une méthode couramment employée pour fournir la garantie d'authentification consiste à utiliser des certificats numériques tels qu'ils sont décrits dans [b-UIT-T X. 509] et [b-UIT-T X.811]. Le certificat défini dans [b-UIT-T X.509], qui est largement utilisé, contient les types de données suivants:

– ***version*** représente la version du certificat codé. La version du certificat sera égale à v3 si le composant extensions figure dans le certificat. Elle doit être égale à v2 ou v3 si le composant issuerUniqueIdentifier (*identificateur unique de l'émetteur*) ou subjectUniqueIdentifier (*identificateur unique du sujet*) est présent.

– Le composant ***serialNumber*** (*numéro de série*) est un nombre entier attribué par l'autorité de certification à tout certificat. La valeur de serialNumber doit être unique pour tout certificat émis par une autorité de certification donnée (c'est-à-dire que le nom de l'émetteur et le numéro de série identifient un certificat unique).

– Le composant ***signature*** contient l'identificateur d'algorithme de l'algorithme et de la fonction de hachage utilisés par l'autorité de certification pour la signature du certificat (par exemple les chiffrements md5WithRSAEncryption, sha-1WithRSAEncryption, id-dsa-with-sha1, etc.).

– Le composant ***issuer*** (*émetteur*) indique l'entité qui a signé et émis le certificat.

– Le composant ***validity*** (*validité*) est l'intervalle de temps pendant lequel l'autorité de certification garantit qu'elle maintiendra des informations concernant le statut du certificat.

– Le composant ***subject*** (*sujet*) indique l'entité associée à la clé publique qui se trouve dans le champ "clé publique du sujet".

– Le composant ***subjectPublicKeyInfo*** (*informations de clé publique du sujet*) est utilisé pour véhiculer la clé publique en cours de certification et indiquer l'algorithme dont cette clé publique constitue une instance (par exemple, le chiffrement rsaEncryption, dhpublicnumber, id-dsa, etc.).

– Le composant ***issuerUniqueIdentifier*** est utilisé pour identifier sans ambiguïté un émetteur en cas de réutilisation d'un nom.

– Le composant ***subjectUniqueIdentifier*** est utilisé pour identifier sans ambiguïté un sujet en cas de réutilisation d'un nom.

– Le champ ***extensions*** permet l'ajout de nouveaux champs à la structure.

Appendice III

Authentification et autorisation: cas d'utilisation

(Le présent Appendice ne fait pas partie intégrante de la présente Recommandation)

Le cas d'utilisation du service AAA décrit dans le présent Appendice est basé sur le modèle de référence contenu dans [b-UIT-T Y.2702].

III.1 Authentification et autorisation d'utilisateur pour l'accès au réseau

Des services d'authentification et d'autorisation pour l'accès au réseau sont nécessaires pour vérifier les identités et pour déterminer si l'accès doit être accordé aux équipements d'utilisateur final.

III.1.1 Authentification et autorisation pour l'accès/le rattachement de dispositifs au NGN

Dans ce cas, trois types sont à considérer pour l'authentification et l'autorisation pour l'accès/le rattachement de dispositifs au NGN. Ces services et capacités identifient et authentifient les dispositifs d'utilisateur et autorisent leur accès ou leur rattachement au réseau IP d'accès.

– Identification, authentification et autorisation d'anciens TE et TE-BE pour l'accès/le rattachement au réseau IP d'accès ((1) de la Figure III.1).
– Identification, authentification et autorisation d'anciens TE et TE-BE avec IAD situés dans le domaine du client pour l'accès/le rattachement au réseau IP d'accès ((2) de la Figure III.1).
– Identification, authentification et autorisation de TE et TE-BE de NGN avec capacités IP situés dans le domaine du client pour l'accès/le rattachement au réseau IP ((3) de la Figure III.1).

Le client AAA assure le service d'authentification pour le dispositif et le fournisseur de réseau: il permet automatiquement au dispositif d'accéder au fournisseur de réseau selon qu'il est nécessaire.

La procédure d'identification correspondant au cas (1) de la Figure III.1 est la suivante:

Etape 1: La passerelle (déclarant) demande au client AAA l'accès/le rattachement au réseau.

Etape 2: Le client AAA demande l'identification de la passerelle au serveur AAA (vérificateur), qui identifie la passerelle.

Etape 3: Le serveur AAA envoie les résultats d'identification au client AAA.

Etape 4: Le client AAA retransmet les résultats à la passerelle et stocke la liste d'accès de la passerelle.

Dans les cas (2) et (3), ce sont respectivement l'IAD et le TE de NGN qui font office de déclarant. Le reste du processus est identique à la procédure applicable dans le cas (1).

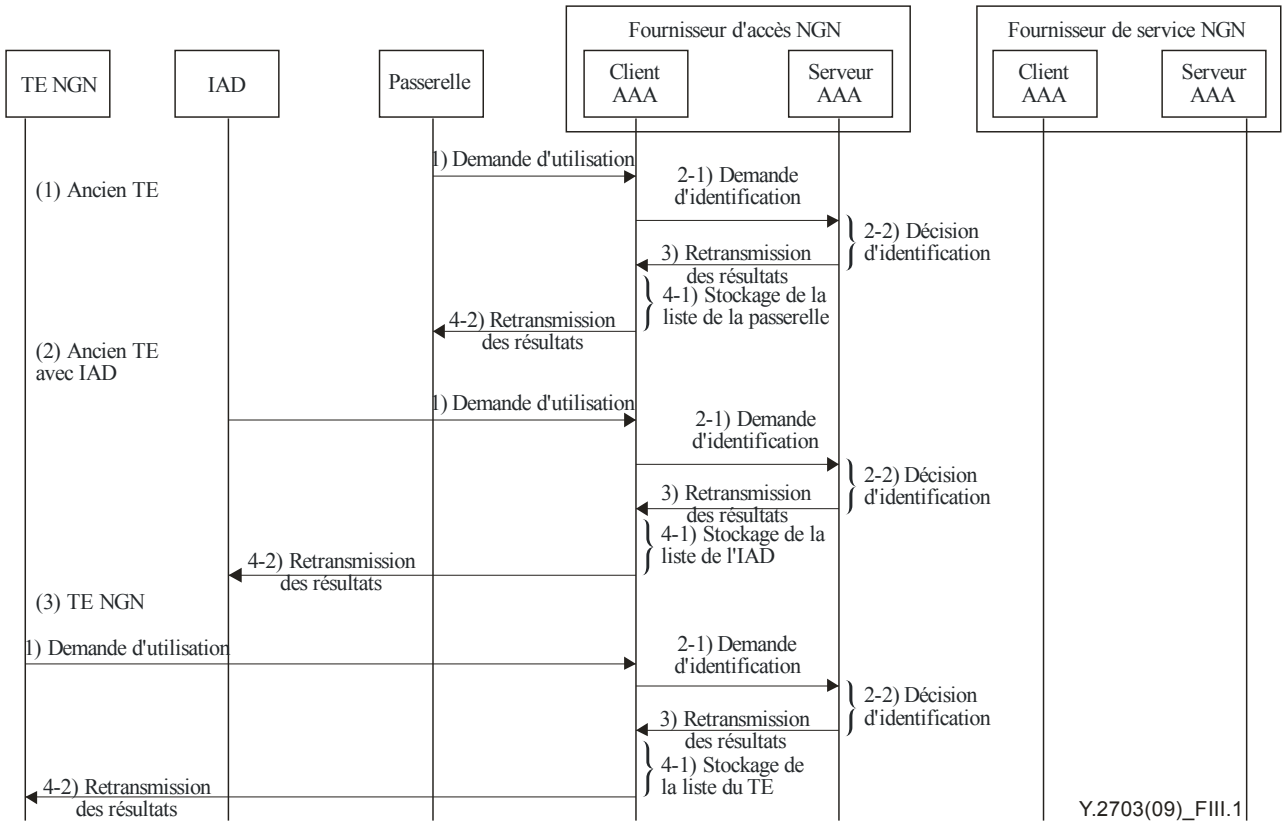

Figure III.1 – Procédure d'identification d'un dispositif pour l'accès à un réseau NGN

III.1.2 Authentification et autorisation regroupées pour l'accès/le rattachement de dispositifs au NGN et pour les services/applications

Dans ce cas, trois types sont à considérer pour l'authentification et l'autorisation pour l'accès/le rattachement de dispositifs au NGN. Ces services et capacités regroupent l'authentification du dispositif d'utilisateur par le fournisseur d'accès NGN et par le fournisseur de service NGN, comme suit:

– Services et capacités permettant au fournisseur de service NGN d'identifier et d'autoriser implicitement les anciens TE et TE-BE ((1) de la Figure III.2).

– Services et capacités permettant au fournisseur de service NGN d'identifier et d'autoriser implicitement les anciens TE et TE-BE avec IAD ((2) de la Figure III.2).

– Services et capacités permettant au fournisseur de service NGN d'identifier, d'authentifier et d'autoriser directement les TE et TE-BE de NGN situés dans le domaine du client ((3) de la Figure III.2).

Le client AAA assure le service d'authentification pour le dispositif et le fournisseur de service/application: il permet automatiquement au dispositif d'accéder au fournisseur de service/application selon qu'il est nécessaire.

La procédure d'identification correspondant au cas (1) de la Figure III.2 est la suivante:

Etape 1: La passerelle (déclarant) demande l'utilisation d'un service/d'une application au client AAA.

Etape 2: Le client AAA demande l'identification de la passerelle au serveur AAA (vérificateur) situé dans le domaine du réseau d'accès et le serveur AAA identifie la passerelle.

Etape 3: Le serveur AAA envoie simultanément les résultats de l'identification au client AAA et au serveur AAA situés dans le domaine du fournisseur de service NGN.

Etape 4: Le client AAA retransmet les résultats à la passerelle et stocke la liste d'accès de la passerelle.

La procédure d'identification correspondant au cas (2) de la Figure III.2 est la suivante:

Etape 1: L'IAD (déclarant) demande l'utilisation d'un service/d'une application au client AAA.

Etape 2: Le client AAA demande l'identification de l'IAD au client AAA situé dans le domaine du fournisseur de service NGN et le serveur AAA (vérificateur) situé dans le domaine du fournisseur de service NGN identifie l'IAD.

Etape 3: Le serveur AAA envoie les résultats d'identification au client AAA.

Etape 4: Le client AAA retransmet les résultats à l'IAD et stocke la liste d'accès de l'IAD.

Dans le cas (3), c'est le TE de NGN qui est le déclarant. Le reste du processus est identique à la procédure applicable dans le cas (2).

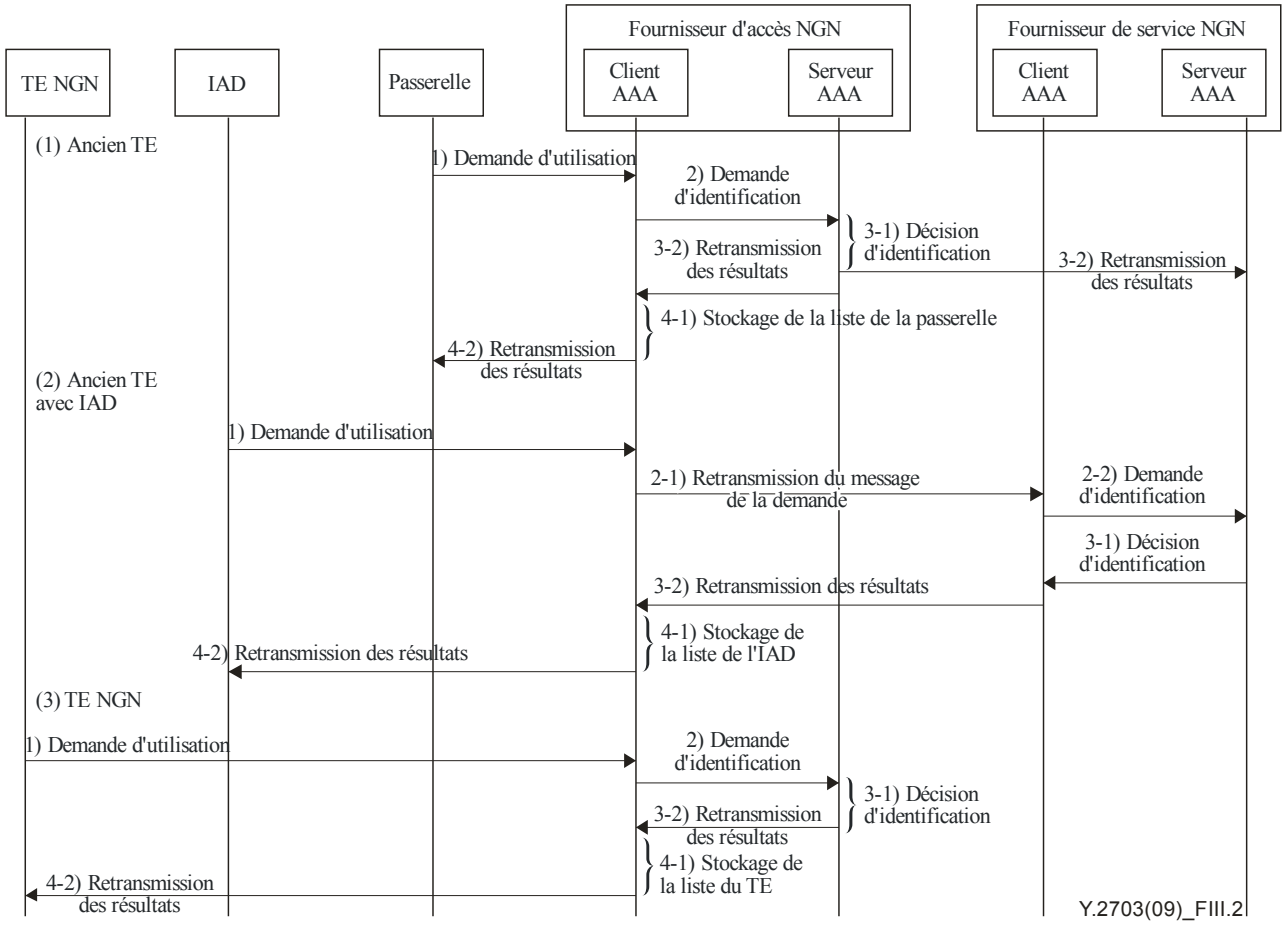

Figure III.2 – Procédure d'identification d'un dispositif pour l'utilisation d'un service ou d'une application

III.2 Authentification et autorisation d'un utilisateur par un fournisseur de service NGN pour l'accès à un service/à une application

Dans ce cas, trois types sont à considérer pour l'authentification et l'autorisation pour un service ou une application dans un scénario comportant plusieurs fournisseurs de réseau:

– Authentification indirecte d'un dispositif d'utilisateur par le fournisseur de service NGN par le biais de relations de confiance avec le fournisseur d'accès NGN ((1) de la Figure III.3).

– Authentification et autorisation directes d'un dispositif d'utilisateur par le fournisseur de service NGN ((2) de la Figure III.3).

– Authentification directe de l'utilisateur par le fournisseur de service NGN ((3) de la Figure III.3).

Le client AAA assure le service d'authentification pour l'utilisateur et le fournisseur de service/application: il permet automatiquement à l'utilisateur d'accéder au fournisseur de service/application selon qu'il est nécessaire.

La procédure d'identification correspondant au cas (1) de la Figure III.3 est la suivante:

Etape 1: Le TE (déclarant) demande l'utilisation d'un service/d'une application au client AAA.

Etape 2: Le client AAA demande l'identification du dispositif au serveur AAA (vérificateur) situé dans le domaine du réseau d'accès et le serveur AAA identifie le dispositif.

Etape 3: Le serveur AAA envoie simultanément les résultats de l'identification au client AAA et au serveur AAA situés dans le domaine du fournisseur de service NGN.

Etape 4: Le client AAA retransmet les résultats au dispositif et stocke la liste d'accès du dispositif.

La procédure d'identification correspondant au cas (2) de la Figure III.3 est la suivante:

Etape 1: Le TE (déclarant) demande l'utilisation d'un service/d'une application au client AAA situé dans le domaine du fournisseur de service NGN.

Etape 2: Le client AAA demande l'identification du dispositif au serveur AAA (vérificateur) situé dans le domaine du fournisseur de service NGN et le serveur AAA identifie le dispositif.

Etape 3: Le serveur AAA envoie les résultats de l'identification au client AAA.

Etape 4: Le client AAA retransmet les résultats au dispositif et stocke la liste d'accès du dispositif.

La procédure d'authentification correspondant au cas (3) de la Figure III.3 est la suivante:

Etape 1: L'utilisateur (déclarant) demande l'utilisation d'un service/d'une application au client AAA situé dans le domaine du fournisseur de service NGN.

Etape 2: Le client AAA demande l'authentification de l'utilisateur au serveur AAA (vérificateur) situé dans le domaine du fournisseur de service NGN et l'utilisateur est authentifié.

Etape 3: Le serveur AAA envoie les résultats de l'authentification au client AAA.

Etape 4: Le client AAA retransmet les résultats à l'utilisateur et stocke la liste d'accès de l'utilisateur.

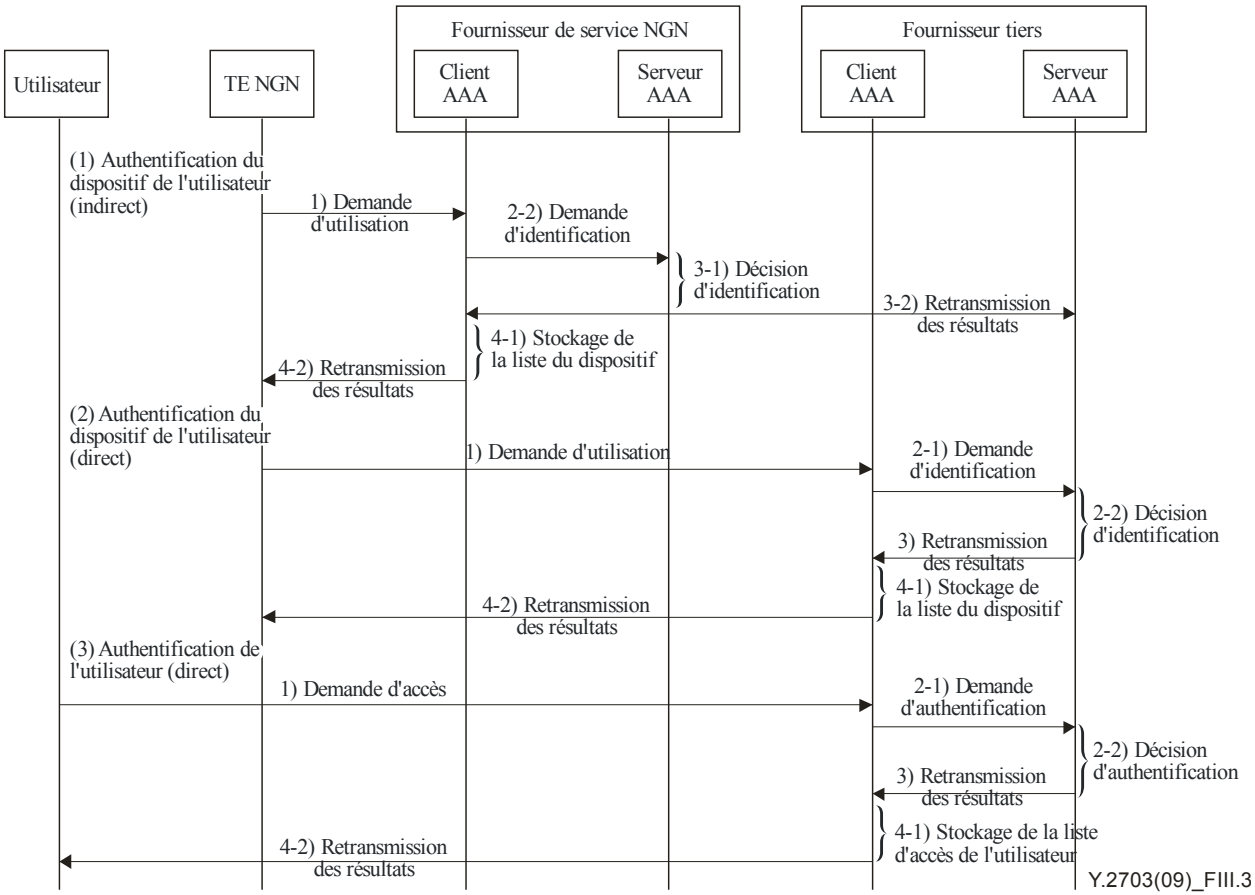

Figure III.3 – Procédure d'authentification et d'autorisation d'un utilisateur par un fournisseur de service NGN

III.3 Authentification et autorisation d'un fournisseur NGN par un utilisateur

Dans ce cas, deux types sont à considérer pour l'authentification et l'autorisation du réseau par un utilisateur:

– Authentification du fournisseur NGN par un utilisateur pour le rattachement au réseau ((1) de la Figure III.4)).

– Authentification du fournisseur NGN par un utilisateur pour l'obtention d'un service ((2) de la Figure III.4)).

Le client AAA assure le service d'authentification pour l'authentification et l'autorisation du réseau par l'utilisateur: il permet automatiquement à l'utilisateur d'accéder au fournisseur de réseau selon qu'il est nécessaire.

La procédure d'identification correspondant au cas (1) de la Figure III.4 est la suivante:

Etape 1: L'utilisateur (déclarant) demande l'authentification d'un point d'accès au réseau (NAP) au vérificateur tiers.

Etape 2: Le vérificateur tiers retransmet les informations d'authentification (AI) au NAP.

Etape 3: Un échange d'informations d'authentification a lieu entre le vérificateur tiers et le NAP.

Etape 4: Le vérificateur tiers procède à une vérification et retransmet les résultats à l'utilisateur.

La procédure d'identification correspondant au cas (2) de la Figure III.4 est la suivante:

Etape 1: L'utilisateur (déclarant) demande l'authentification du réseau au vérificateur tiers.

Etape 2: Le vérificateur tiers retransmet la demande de l'utilisateur au client AAA, lequel demande les informations d'authentification (AI) au serveur AAA.

Etape 3: Le serveur AAA envoie les informations d'authentification au client AAA et un échange d'informations d'authentification a lieu entre le vérificateur tiers et le client AAA.

Etape 4: Le vérificateur tiers procède à une vérification et retransmet les résultats à l'utilisateur.

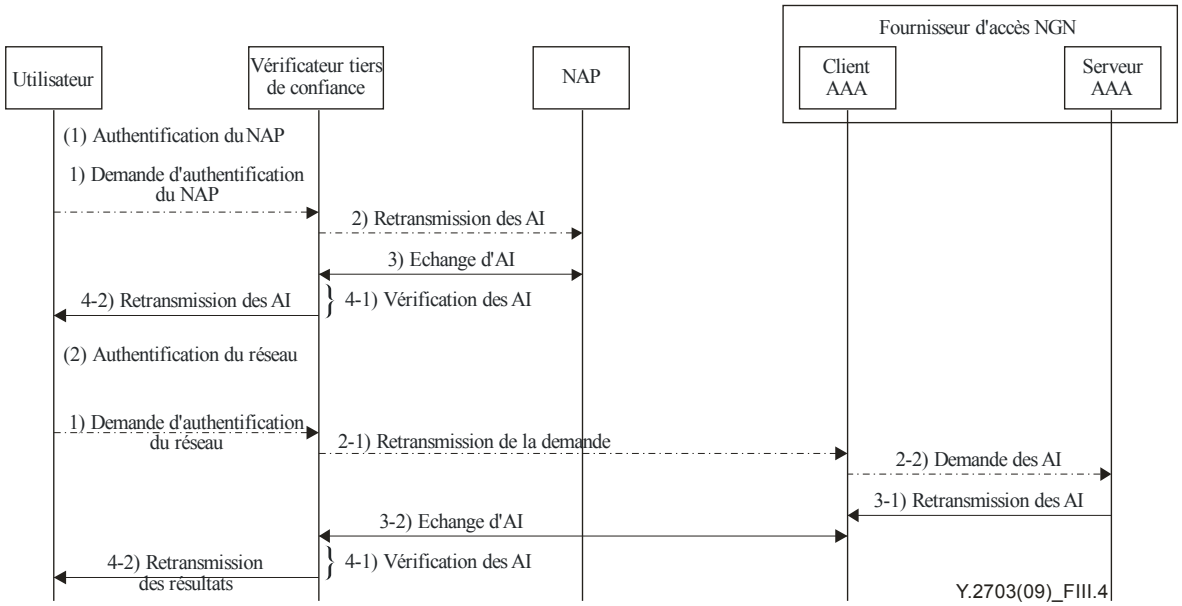

Figure III.4 – Procédure d'authentification et d'autorisation d'un fournisseur NGN par un utilisateur

III.4 Authentification et autorisation d'un fournisseur de service/application tiers par un fournisseur NGN

Dans certains scénarios, il se peut que le fournisseur d'une application ou d'un service soit différent du fournisseur NGN (fournisseur de service/application tiers). Le fournisseur NGN devra authentifier et autoriser le fournisseur de service/application tiers.

Le client AAA assure le service d'authentification pour l'authentification et l'autorisation du fournisseur de service/application tiers par le fournisseur NGN.

La procédure d'identification correspondant à la Figure III.5 est la suivante:

Etape 1: Le client AAA (déclarant) du fournisseur NGN demande l'authentification du fournisseur de service/application tiers au vérificateur tiers.

Etape 2: Le vérificateur tiers retransmet la demande au client AAA du fournisseur de service/application tiers et le client AAA demande les informations d'authentification (AI) au serveur AAA.

Etape 3: Le serveur AAA retransmet les informations d'authentification au client AAA et un échange d'informations d'authentification a lieu entre le vérificateur tiers et le client AAA.

Etape 4: Le vérificateur tiers procède à une vérification et retransmet les résultats au client AAA du fournisseur NGN et le serveur AAA stocke les résultats.

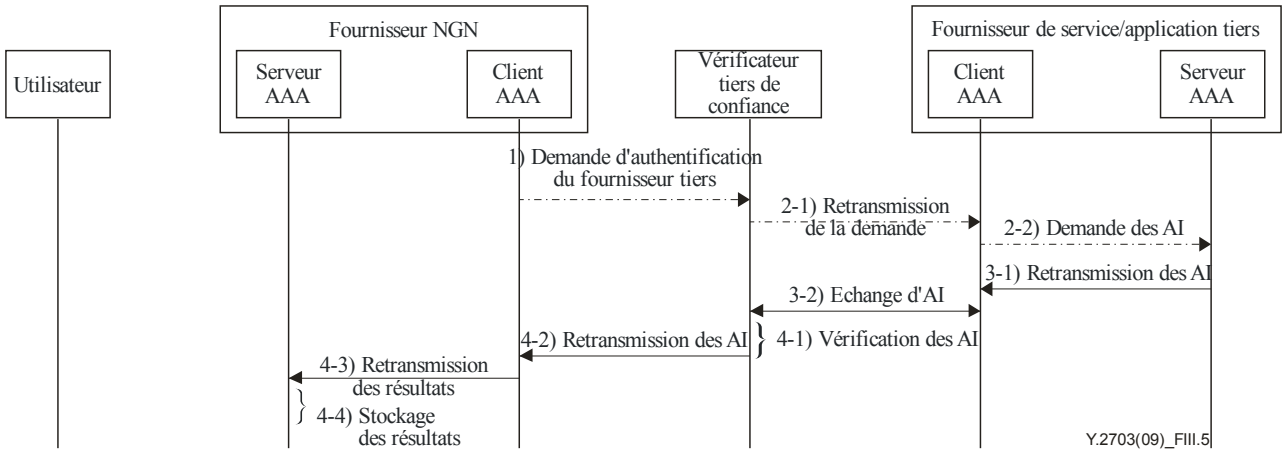

Figure III.5 – Procédure d'authentification et d'autorisation d'un fournisseur de service/application tiers par un fournisseur NGN

III.5 Utilisation d'un service d'authentification et d'autorisation de tiers

Les fournisseurs de service peuvent avoir à authentifier et autoriser un tiers. Dans ce cas, deux types sont à considérer pour l'utilisation d'un service d'authentification et d'autorisation de tiers:

– Authentification d'un utilisateur auprès d'un fournisseur de service; ((1) de la Figure III.6).

– Authentification d'un fournisseur de service auprès d'un utilisateur; ((2) de la Figure III.6).

III.5.1 Authentification d'un utilisateur auprès d'un fournisseur de service

Le client AAA assure le service d'authentification pour l'authentification et l'autorisation d'un utilisateur auprès d'un fournisseur de service: il permet automatiquement à l'utilisateur d'accéder au fournisseur de service/application tiers selon qu'il est nécessaire.

La procédure d'identification correspondant à la Figure III.6 est la suivante:

Etape 1: L'utilisateur (déclarant) demande au client AAA un accès au réseau.

Etape 2: Le client AAA demande l'authentification de l'utilisateur au serveur AAA du fournisseur de service/application tiers et ledit serveur AAA (vérificateur) authentifie l'utilisateur.

Etape 3: Le serveur AAA envoie les résultats d'authentification au client AAA.

Etape 4: Le client AAA retransmet les résultats à l'utilisateur et stocke la liste d'accès de l'utilisateur.

Etape 5: Si la demande est accordée, l'utilisateur peut accéder à la ressource spécifiée du réseau.

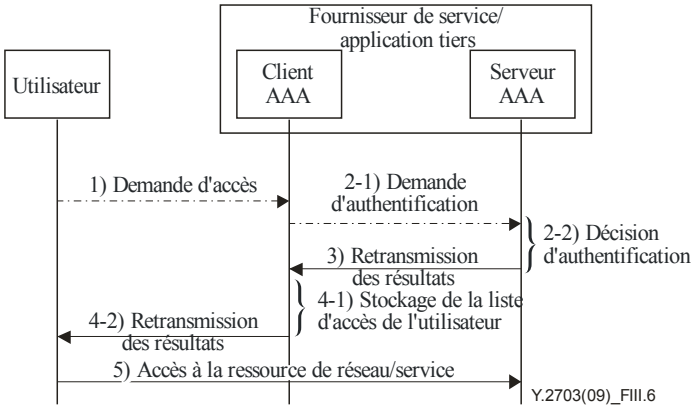

Figure III.6 – Procédure d'utilisation d'un service d'authentification et d'autorisation de tiers

III.5.2 Authentification d'un fournisseur de service auprès d'un utilisateur

Le client AAA assure le service d'authentification pour l'authentification d'un fournisseur de service auprès d'un utilisateur.

La procédure d'identification correspondant à la Figure III.7 est la suivante:

Etape 1: L'utilisateur (déclarant) situé dans le domaine du client demande l'authentification d'un fournisseur de service/application tiers au vérificateur tiers.

Etape 2: Le vérificateur tiers retransmet cette demande au client AAA du fournisseur de service/application tiers et ledit client AAA demande les informations d'authentification (AI) au serveur AAA.

Etape 3: Le serveur AAA retransmet les informations d'authentification au client AAA et un échange d'informations d'authentification a lieu entre le vérificateur tiers et le client AAA.

Etape 4: Le vérificateur tiers procède à une vérification, retransmet les résultats au client AAA du fournisseur NGN et stocke les résultats.

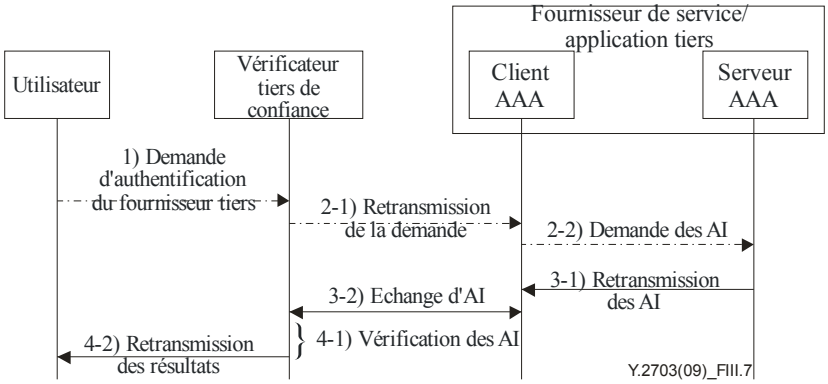

Figure III.7 – Procédure d'utilisation d'un service d'authentification et d'autorisation de tiers

Bibliographie

[b-UIT-T M.3410] Recommandation UIT-T M.3410 (2008), *Lignes directrices et exigences concernant les systèmes de gestion de la sécurité pour la gestion des télécommunications*.

[b-UIT-T Q.3201] Recommandation UIT-T Q.3201 (2007), *Architecture du protocole de signalisation de la sécurité basé sur le protocole EAP pour le rattachement au réseau*.

[b-UIT-T Q.3202.1] Recommandation UIT-T Q.3202.1 (2008), *Protocoles d'authentification basés sur le protocole EAP-AKA pour l'interfonctionnement des dispositifs 3GPP, WiMax et WLAN dans les réseaux de prochaine génération*.

[b-UIT-T X.509] Recommandation UIT-T X.509 (2005) | ISO/CEI 9594-8:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*.

[b-UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

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

[b-UIT-T X.810] Recommandation UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: aperçu général*.

[b-UIT-T X.811] Recommandation UIT-T X.811 (1995) | ISO/CEI 10181-2:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre d'authentification*.

[b-UIT-T X.812] Recommandation UIT-T X.812 (1995) | ISO/CEI 10181-3:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre de contrôle d'accès*.

[b-UIT-T X.816] Recommandation UIT-T X.816 (1995) | ISO/CEI 10181-7:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre d'audit et d'alarmes de sécurité*.

[b-UIT-T Y.2001] Recommandation UIT-T Y.2001 (2004), *Aperçu général des réseaux de prochaine génération*.

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

[b-UIT-T Y.2012] Recommandation UIT-T Y.2012 (2006), *Prescriptions fonctionnelles et architecture du réseau de prochaine génération version 1*.

[b-UIT-T Y.2201] Recommandation UIT-T Y.2201 (2007), *Spécifications des réseaux de prochaine génération de version 1*.

[b-UIT-T Y.2233] Recommandation UIT-T Y.2233 (2008), *Prescriptions et cadre général pour la prise en charge de capacités de comptabilité et de taxation dans les réseaux de prochaine génération de version 1*.

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

[b-UIT-T Y.2702] Recommandation UIT-T Y.2702 (2008), *Spécifications d'authentification et d'autorisation dans les réseaux de prochaine génération de version 1*.

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, 2010