Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2704

(01/2010)

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

Réseaux de prochaine génération – Sécurité

Mécanismes et procédures de sécurité des réseaux NGN

Recommandation UIT-T Y.2704

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.2704

Mécanismes et procédures de sécurité des réseaux NGN

Résumé

La Recommandation Y.2701, *Prescriptions de sécurité des réseaux de prochaine génération de version 1*, énonce les prescriptions de sécurité des réseaux de prochaine génération (NGN, *next generation network*) et des interfaces associées (par exemple, UNI, NNI et ANI). La Recommandation UIT-T Y.2704 décrit certains mécanismes de sécurité qui peuvent être utilisés pour satisfaire aux prescriptions énoncées dans la Recommandation Y.2701 et spécifie l'ensemble d'options correspondant à chaque mécanisme donné. Plus précisément, la présente Recommandation décrit les mécanismes d'identification, d'authentification et d'autorisation, examine la sécurité du transport pour la signalisation et les fonctions d'exploitation, d'administration, de maintenance et de fourniture (OAMP, *operations, administration, maintenance and provisionning*), ainsi que la sécurité des médias, traite des mécanismes relatifs à la piste de vérification de sécurité et décrit enfin la procédure d'approvisionnement. Les mécanismes de sécurité décrits dans la présente Recommandation reposent sur le modèle de confiance défini dans la Recommandation UIT-T Y.2701.

La liste des mécanismes de sécurité décrits dans la présente Recommandation n'est pas exhaustive. Outre les mécanismes spécifiés dans la présente Recommandation pour la protection de la sécurité des réseaux NGN, les fournisseurs de réseaux NGN sont encouragés à fournir, en fonction des besoins, des outils, capacités et mesures opérationnelles supplémentaires en matière de sécurité.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T Y.2704	2010-01-29	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

Recommandation UIT-T Y.2704

Mécanismes et procédures de sécurité des réseaux NGN

1 Domaine d'application

La Recommandation [UIT-T Y.2701], *Prescriptions de sécurité des réseaux de prochaine génération de version 1*, énonce les prescriptions de sécurité pour les réseaux de prochaine génération (NGN, *next generation network*) et les interfaces associées (par exemple, UNI, NNI et ANI), y compris un modèle de confiance. Les mécanismes de sécurité retenus pour mettre en œuvre ces prescriptions consisteront en différentes options, les options incompatibles étant contre-indiquées dans la mesure où elles ont tendance à introduire des vulnérabilités en matière de sécurité, rendant l'interopérabilité plus difficile à atteindre.

La présente Recommandation met par conséquent en évidence certains mécanismes de sécurité importants qui peuvent être utilisés pour satisfaire aux prescriptions de [UIT-T Y.2701], et spécifie l'ensemble d'options à utiliser pour chaque mécanisme retenu en vue de limiter les problèmes d'interopérabilité et d'incompatibilité. La liste des mécanismes décrits dans la présente Recommandation n'est pas exhaustive. Outre les mécanismes spécifiés dans la présente Recommandation pour la protection de la sécurité des réseaux NGN, les fournisseurs de réseaux NGN sont encouragés à fournir, en fonction des besoins, des outils, capacités et mesures opérationnelles supplémentaires en matière de sécurité.

La présente Recommandation est destinée à être utilisée avec [UIT-T Y.2701] afin de définir un cadre pour la sécurité des réseaux NGN. Il convient de l'employer avec d'autres Recommandations relatives à la sécurité et d'autres spécifications, selon le cas, pour des questions particulières liées à la sécurité.

NOTE – Les mécanismes d'identification et d'authentification décrits dans la présente Recommandation se rapportent au domaine plus vaste connu généralement sous le nom de "gestion des identités" (IdM, *identity management*).

1.1 Hypothèses

La présente Recommandation repose sur les hypothèses suivantes:

1) Le groupement des entités fonctionnelles, définies dans [UIT-T Y.2012], dans un élément de réseau donné, variera en fonction du fabricant.

2) Chaque fournisseur NGN a des responsabilités particulières dans son domaine en ce qui concerne la sécurité, par exemple, implémenter les services et pratiques de sécurité applicables pour a) se protéger; b) garantir que la sécurité de bout en bout n'est pas compromise dans son réseau; et c) garantir une grande disponibilité et une grande intégrité des communications dans les NGN.

3) Dans chaque domaine de réseau, des politiques seront établies et appliquées en ce qui concerne les accords sur le niveau de service (SLA, *service level agreement*) afin de garantir la sécurité du domaine considéré et la sécurité des interconnexions de réseau. On suppose que les accords SLA préciseront les services, mécanismes et pratiques de sécurité à implémenter pour protéger les réseaux interconnectés et les communications (trafic de signalisation/commande, trafic support et trafic de gestion) via les interfaces UNI, ANI et NNI.

4) La présente Recommandation porte sur la sécurité assurée par le biais du réseau et repose sur une architecture en couches, avec la sécurité périmétrique des domaines de confiance, la sécurité physique des équipements de fournisseur et éventuellement l'utilisation du chiffrement.

1.2 Aperçu général

La présente Recommandation est structurée comme suit:

- Section 2 (Références) – Cette section contient les références normatives.
- Section 3 (Définitions) – Cette section contient les définitions des termes utilisées dans la présente Recommandation.
- Section 4 (Abréviations et acronymes) – Cette section contient la liste des abréviations et des acronymes utilisés dans la présente Recommandation.
- Section 5 (Conventions) – Cette section est délibérément laissée en blanc.
- Section 6 (Menaces et risques pour la sécurité) – Cette section précise les menaces et les risques liés à la sécurité pour les réseaux NGN.
- Section 7 (Modèle de confiance pour la sécurité) – Cette section décrit brièvement le modèle de confiance défini dans [UIT-T Y.2701].
- Section 8 (Identification, authentification et autorisation) – Cette section énonce les mécanismes et les mesures de sécurité pour l'identification, l'authentification et l'autorisation.
- Section 9 (Sécurité du transport pour le trafic de signalisation et OAMP) – Cette section décrit les mécanismes utilisés pour le chiffrement et la protection de l'intégrité du trafic de signalisation et OAMP.
- Section 10 (Sécurité des médias) – Cette section présente les mécanismes utilisés pour la protection des médias (c'est-à-dire le trafic support).
- Section 11 (Fonctions OAMP) – Cette section donne des informations et des références pour la piste de vérification de sécurité, le piégeage et la journalisation des événements de sécurité.
- Section 12 (Approvisionnement d'équipements dans la zone non fiable) – Cette section donne des informations sur l'approvisionnement d'équipements d'abonné dans la zone non fiable.
- Appendice I – Exemples de mécanismes d'assurance de l'adresse d'origine et application au mécanisme d'identification et d'authentification de l'abonné.
- Appendice II – Sécurité pour l'interconnexion des services de télécommunication d'urgence
- Appendice III – Bonnes pratiques de sécurité
- Bibliographie

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

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

[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*.

[UIT-T Y.2703] Recommandation UIT-T Y.2703 (2009), *Application du service AAA dans les réseaux NGN*.

[UIT-T Y.2720] Recommandation UIT-T Y.2720 (2009), *Cadre de gestion d'identité des réseaux NGN*.

[UIT-T X.509] Recommandation UIT-T X.509 (2008) | ISO/CEI 9594-8:2008, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*.

[UIT-T X.660] Recommandation UIT-T X.660 (2008) | ISO/CEI 9834-1:2008, *Technologies de l'information – Interconnexion des systèmes ouverts – Procédures opérationnelles des organismes d'enregistrement de l'OSI: procédures générales et arcs sommitaux de l'arborescence des identificateurs d'objet ASN.1*.

[UIT-T X.1035] Recommandation UIT-T X.1035 (2007), *Protocole d'échange de clés avec authentification par mot de passe*.

[IETF RFC 4302] IETF RFC 4302 (2005), *IP Authentication Header*.

[IETF RFC 4303] IETF RFC 4303 (2005), *IP Encapsulating Security Payload (ESP)*.

[IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs.

3.1.1 actif [UIT-T Y.2701]: quelque chose qui a de la valeur pour l'organisation, ses activités et sa continuité.

3.1.2 élément en limite [UIT-T Y.2701]: élément de réseau qui assure des fonctions permettant de raccorder différents domaines de sécurité et administratifs.

3.1.3 réseau d'entreprise [UIT-T Y.2701]: réseau privé qui prend en charge de multiples utilisateurs et qui peut se situer en de multiples endroits (par exemple, une entreprise ou un campus).

3.1.4 élément en limite de domaine [UIT-T Y.2701]: élément en limite contrôlé uniquement par le fournisseur, assurant des fonctions de sécurité avec d'autres domaines de réseau.

3.1.5 service de télécommunications d'urgence (ETS, *emergency telecommunications service*) [b-UIT-T E.107]: service national offrant des télécommunications prioritaires aux utilisateurs autorisés en cas de catastrophe et de situation d'urgence.

3.1.6 élément en limite de réseau [UIT-T Y.2701]: élément en limite contrôlé uniquement par le fournisseur, assurant des fonctions de sécurité avec des équipements terminaux.

3.1.7 domaine de sécurité [UIT-T Y.2701]: un ensemble d'éléments, une politique de sécurité, une autorité de sécurité et un ensemble d'activités liées à la sécurité, les éléments étant gérés conformément à la politique de sécurité. La politique sera administrée par l'autorité de sécurité. Un domaine de sécurité donné peut couvrir plusieurs zones de sécurité.

3.1.8 jeton de sécurité [b-UIT-T X.810]: ensemble des données protégées par un ou plusieurs services de sécurité et des informations de sécurité utilisées pour la fourniture de ces services de sécurité, qui sont transférées entre les entités communiquantes.

3.1.9 zone de sécurité [UIT-T Y.2701]: UIT-T Y.2701 définit trois zones de sécurité: 1) zone de confiance; 2) zone de confiance mais vulnérable; et 3) zone non fiable. Une zone de sécurité est définie par son contrôle opérationnel, son emplacement et sa connectivité aux autres dispositifs/éléments de réseau.

3.1.10 élément en limite d'équipement terminal [UIT-T Y.2704]: élément en limite assurant des fonctions de sécurité entre l'équipement local d'abonné et le réseau du fournisseur de service.

3.1.11 confiance [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.

3.1.12 zone de confiance mais vulnérable [UIT-T Y.2701]: du point de vue d'un fournisseur NGN, zone de sécurité contenant des dispositifs/éléments de réseau dont l'exploitation (l'approvisionnement et la maintenance) est assurée par le fournisseur NGN. Les équipements peuvent être sous le contrôle de l'abonné ou du fournisseur NGN. En outre, ils peuvent être situés à l'intérieur ou à l'extérieur du domaine du fournisseur NGN. Ils communiquent à la fois avec des éléments situés dans la zone de confiance et avec des éléments situés dans la zone non fiable, ce qui explique pourquoi ils sont "vulnérables". Sur le plan de la sécurité, leur principale fonction est d'assurer une protection à toute épreuve des éléments de réseau situés dans la zone de confiance contre les attaques provenant de la zone non fiable.

3.1.13 zone de confiance [UIT-T Y.2701]: du point de vue d'un fournisseur NGN, domaine de sécurité contenant les éléments de réseau et systèmes du fournisseur NGN qui ne communiquent jamais directement avec les équipements d'abonné. Les éléments de réseau NGN situés dans ce domaine présentent les caractéristiques communes suivantes: ils sont entièrement sous le contrôle du fournisseur NGN concerné, ils sont situés dans ses locaux (ce qui assure la sécurité physique) et ils communiquent uniquement avec des éléments situés dans le domaine "de confiance" et avec des éléments situés dans le domaine "de confiance mais vulnérable".

3.1.14 zone non fiable [UIT-T Y.2701]: du point de vue d'un fournisseur NGN, zone incluant tous les éléments des réseaux d'abonné ou éventuellement des réseaux homologues ou d'autres zones du fournisseur NGN en dehors du domaine initial, qui sont raccordés aux éléments en limite du fournisseur NGN.

3.1.15 utilisateur [b-UIT-T Y.2091]: utilisateur final, personne, abonné, système, équipement, terminal (par exemple, télécopieur, ordinateur personnel), entité (fonctionnelle), processus, application, fournisseur ou réseau d'entreprise.

3.1.16 réseau d'utilisateur [UIT-T Y.2701]: réseau privé constitué d'équipements terminaux qui peuvent avoir de multiples utilisateurs.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit le terme suivant:

3.2.1 authentificateur: élément de réseau facilitant l'identification et l'authentification d'abonnés, de dispositifs ou d'utilisateurs finals. Par exemple, des éléments en limite avec une fonctionnalité d'agent utilisateur dos à dos (B2BUA, *back-to-back user agent*) ou une entité fonctionnelle relais de commande de session d'appel (P-CSC-FE, *proxy call session control functional entity*) peuvent être des authentificateurs d'abonnés à des services reposant sur le protocole SIP.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants.

3G troisième génération (*3rd generation*)

AGW passerelle d'accès (*access gateway*)

AH	en-tête d'authentification (*authentication header*)
AKA	authentification et concordance de clés (*authentication and key agreement*)
ANI	interface application-réseau (*application-to-network interface*)
AS/WS	serveur d'application/serveur web (*application server/web server*)
AuC	centre d'authentification (*authentication centre*)
B2BUA	agent utilisateur dos à dos (*back-to-back user agent*)
BE	élément en limite (*border element*)
BSR	routeur de station de base (*base station router*)
CA	autorité de certification (*certification authority*)
COPS	service commun de politique ouverte (*common open policy service*)
CRL	liste de révocation de certificats (*certificate revocation list*)
CSC-FE	entité fonctionnelle de contrôle de session d'appel (*call session control functional entity*)
DBE	élément en limite de domaine (*domain border element*)
DNS	système de noms de domaine (*domain name system*)
DoS	déni de service (*denial of service*)
DTMF	multifréquence bitonalité (*dual-tone multi-frequency*)
ECC	cryptographie à courbe elliptique (*elliptic curve cryptography*)
ESP	protocole de sécurité d'encapsulation (*encapsulating security protoco*l)
ETS	service de télécommunications d'urgence (*emergency telecommunications service*)
FE	entité fonctionnelle (*functional entity*)
GBA	architecture d'amorçage générique (*generic bootstrapping architecture*)
GW	passerelle (*gateway*)
HMAC	code d'authentification de message avec hachage (*hash message authentication code*)
HTTP	protocole de transfert hypertexte (*hypertext transfer protocol*)
I-CSC-FE	entité fonctionnelle interrogatrice de contrôle de session d'appel (*interrogating call session control functional entity*)
ID	identité (*identity*)
IdM	gestion des identités (*identity management*)
IDPS	systèmes de détection et de prévention des intrusions (*intrusion detection and prevention systems*)
IDS	systèmes de détection des intrusions (*intrusion detection systems*)
IKE	échange de clés Internet (*Internet key exchange*)
IMS	sous-système multimédia IP (*IP multimedia subsystem*)
IP	protocole Internet (*Internet protocol*)
LAN	réseau local (*local area network*)
MD5	algorithme 5 de résumé de message (*message digest 5*)

MIB	base d'informations de gestion (*management information base*)
MPLS	commutation multiprotocolaire par étiquetage (*multiprotocol label switching*)
MRP-FE	entité fonctionnelle de traitement des ressources médias (*media resource processing functional entity*)
MS	station mobile (*mobile station*)
NAC-FE	entité fonctionnelle de contrôle d'accès au réseau (*network access control functional entity*)
NAPT	traduction d'adresse et d'accès réseau (*network address and port translation*)
NAT	traduction d'adresse de réseau (*network address translation*)
NBE	élément en limite de réseau (*network border element*)
NE	élément de réseau (*network element*)
NGN	réseau de prochaine génération (*next generation network*)
NNI	interface réseau-réseau (*network-to-network interface*)
OAMP	exploitation, administration, maintenance et fourniture (*operations, administration, maintenance and provisioning*)
OID	identificateur d'objet (*object identifier*)
ONU	unités de réseau optique (*optical network units*)
PAK	clé authentifiée par mot de passe (*password authenticated key*)
P-CSC-FE	entité fonctionnelle relais de commande de session d'appel (*proxy call session control functional entity*)
POTS	service téléphonique ordinaire (*plain old telephone service*)
QS	qualité de service
RAC-FE	entité fonctionnelle de contrôle des ressources et d'admission (*resource and admission control functional entity*)
RADIUS	service d'authentification à distance des utilisateurs entrants (*remote authentication dial in user service*)
RAN	réseau d'accès radio (*radio access network*)
RGT	réseau de gestion des télécommunications
RNIS	réseau numérique à intégration de services
RTPC	réseau téléphonique public commuté
RTSP	protocole d'écoulement en temps réel (*real-time streaming protocol*)
SAA-FE	entité fonctionnelle d'authentification et d'autorisation de service (*service authentication and authorization functional entity*)
SASL	couche simple d'authentification et de sécurité (*simple authentication and security layer*)
S-CSC-FE	entité fonctionnelle serveur de commande de session d'appel (*serving call session control functional entity*)
SDP	protocole de description de session (*session description protocol*)
SIM	module d'identité d'abonné (*subscriber identity module*)
SIP	protocole d'ouverture de session (*session initiation protocol*)

SLA accord sur le niveau de service (*service level agreement*)

SL-FE entité fonctionnelle de localisation d'abonnement (*subscription locator functional entity*)

SNMP protocole simple de gestion de réseau (*simple network management protocol*)

SRTP protocole de transport en temps réel sécurisé (*secure real time protocol*)

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

TCP protocole de commande de transmission (*transmission control protocol*)

TE équipement terminal (*terminal equipment*)

TE-BE élément en limite d'équipement terminal (*terminal equipment border element*)

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

TRIP routage téléphonique sur IP (*telephony routing over IP*)

UA agent d'utilisateur (*user agent*)

UDP protocole datagramme d'utilisateur (*user datagram protocol*)

UE équipement d'utilisateur (*user equipment*)

UICC carte de circuits intégrés universelle (*universal integrated circuit card*)

UMTS système de télécommunications mobiles universelles (*universal mobile telecommunications system*)

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

URL identificateur uniforme de ressources (*uniform resource locator*)

USIM module d'identité d'abonné universel (*universal subscriber identity module*)

VLAN réseau local virtuel (*virtual LAN*)

VPN réseau privé virtuel (*virtual private network*)

WLAN réseau local sans fil (*wireless LAN*)

xDSL ligne d'abonné numérique x (*x digital subscriber line*)

5 Conventions

Aucune.

6 Menaces et risques pour la sécurité

Se reporter au § 4 de la Recommandation [UIT-T Y.2701] pour une description des menaces et des risques en matière de sécurité supposés pour l'environnement NGN.

7 Modèle de confiance pour la sécurité

Le choix de mécanismes de sécurité par un fournisseur NGN dépend du modèle de confiance applicable. La présente Recommandation repose sur l'utilisation du modèle de confiance défini dans [UIT-T Y.2701]. Ce modèle de confiance pour la sécurité des réseaux NGN est décrit brièvement dans la présente section.

L'architecture fonctionnelle de référence des NGN définit des entités fonctionnelles (FE, *functional entity*). Toutefois, comme les aspects de sécurité de réseau dépendent dans une large mesure de la façon dont les entités fonctionnelles sont groupées physiquement, l'architecture de sécurité des NGN

est fondée sur les éléments de réseau (NE, *network element*) physiques, à savoir des boîtes concrètes qui contiennent une ou plusieurs entités fonctionnelles. La façon dont ces entités fonctionnelles sont groupées dans les éléments de réseau dépendra du fabricant et du fournisseur NGN.

7.1 Modèle de confiance pour un seul réseau

Le présent paragraphe définit trois zones de sécurité:

1) zone de confiance;

2) zone de confiance mais vulnérable;

3) zone non fiable.

chacune étant caractérisée par son contrôle opérationnel, son emplacement et sa connectivité aux autres dispositifs/éléments de réseau. Ces trois zones apparaissent dans le modèle de confiance pour la sécurité illustré sur la Figure 1.

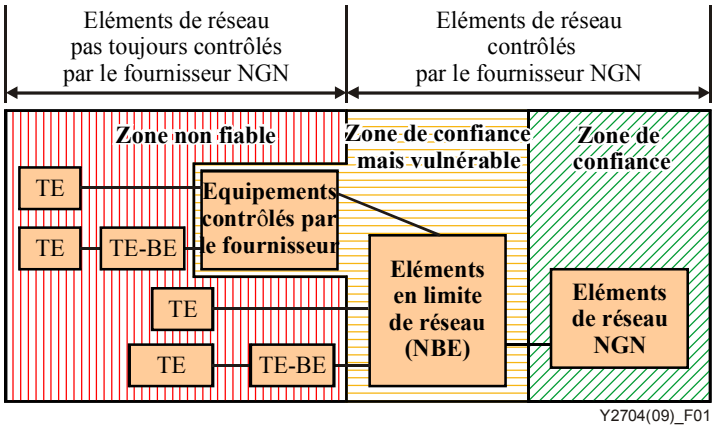


Figure 1 – Modèle de confiance pour la sécurité/[UIT-T Y.2701]

Une "zone de sécurité de réseau de confiance", ou "zone de confiance" en abrégé, est une zone contenant les éléments de réseau et systèmes d'un fournisseur NGN qui ne communiquent jamais directement avec les équipements d'abonné ou d'autres domaines. Les éléments de réseau NGN situés dans cette zone présentent les caractéristiques communes suivantes:

1) ils sont entièrement sous le contrôle du fournisseur NGN (pour l'approvisionnement, la maintenance et le contrôle d'exploitation);

2) ils sont situés dans son domaine; et

3) ils communiquent uniquement avec d'autres éléments situés dans la zone "de confiance" et avec des éléments situés dans la zone "de confiance mais vulnérable".

Le fait qu'un élément de réseau soit situé dans une zone de confiance n'implique pas que cet élément soit nécessairement sûr.

Les éléments de réseaux situés dans la zone "de confiance" seront protégés par une combinaison de diverses méthodes, par exemple sécurité physique des éléments de réseau NGN, renforcement général de la protection des systèmes, utilisation d'une signalisation sécurisée, sécurité pour les messages de gestion et utilisation d'un VPN à part dans le réseau (MPLS/)IP. La même combinaison devrait être utilisée pour sécuriser les communications dans la zone "de confiance" et avec les éléments de réseau NGN dans la zone "de confiance mais vulnérable".

Une "zone de sécurité de réseau de confiance mais vulnérable", ou "zone de confiance mais vulnérable" en abrégé, est une zone contenant des dispositifs/éléments de réseau qui communiquent avec des éléments situés dans la zone "non fiable", ce qui explique pourquoi ils sont "vulnérables". De plus, ces éléments de réseau communiquent avec des éléments situés dans la zone "de confiance".

Tout comme ces derniers, ils sont sous le contrôle du fournisseur NGN, bien qu'ils puissent être situés à l'intérieur ou à l'extérieur des locaux de celui-ci. Sur le plan de la sécurité, leur principale fonction est de protéger les éléments de réseau situés dans la zone de confiance contre les attaques provenant de la zone non fiable. La combinaison de méthodes employée pour sécuriser les communications entre les éléments de réseau NGN situés dans la zone "de confiance mais vulnérable" et ceux situés dans la zone "non fiable" peut être différente de celle employée pour sécuriser les communications dans la zone "de confiance".

Les éléments situés dans le domaine du fournisseur NGN qui peuvent être connectés à des éléments situés à l'extérieur de la zone de confiance sont appelés éléments en limite de réseau (NBE, *network border element*), par exemple:

- les éléments en limite de réseau (NBE, *network border element*) à l'interface UNI, qui assurent l'interface avec les éléments de contrôle de service ou de transport du fournisseur NGN situés dans la zone de confiance afin que l'utilisateur/l'abonné ait accès au réseau du fournisseur NGN concernant les services et/ou le transport;
- les éléments en limite de domaine (DBE, *domain border elements*), qui sont identiques aux éléments en limite de réseau, à ceci près qu'ils se trouvent à la limite de deux domaines;
- les éléments NBE de configuration et d'amorçage de dispositif (DCB-NBE, *device configuration & bootstrap NBE*), qui s'interfacent avec le système de configuration de dispositif du fournisseur NGN situé dans la zone de confiance afin de configurer les dispositifs d'utilisateur/d'abonné et les équipements du fournisseur NGN situés dans des installations extérieures;
- les éléments OAMP-NBE, qui s'interfacent avec les systèmes OAMP du fournisseur NGN situés dans la zone de confiance afin d'assurer la fourniture et la maintenance des dispositifs d'utilisateur/d'abonné et certains des équipements du fournisseur NGN situés dans des installations extérieures;
- les éléments NBE de serveur d'application/serveur web (AS/WS-NBE, *application server/web server NBE*), qui s'interfacent avec l'élément AS/WS-NBE du fournisseur NGN situé dans la zone de confiance afin que l'utilisateur/l'abonné ait accès aux services web.

La Figure 1 montre les relations entre ces éléments NBE et NE devant être protégés.

Comme exemples de dispositifs/éléments qui sont exploités par un fournisseur NGN mais qui ne sont pas situés dans ses locaux, et qui peuvent ou non être sous son contrôle, on peut citer:

- les équipements d'installations extérieures situés dans le réseau d'accès;
- le routeur de station de base (BSR, *base station router*), qui est un élément de réseau intégrant les fonctionnalités de station de base, de contrôleur de réseau radioélectrique et de routeur pour l'accès hertzien;
- l'unité de réseau optique (ONU, *optical network unit*) située dans la résidence d'un utilisateur/abonné.

La "zone de confiance mais vulnérable", qui comprend des éléments NBE, sera protégée par une combinaison de diverses méthodes, par exemple sécurité physique des éléments de réseau NGN, renforcement général de la protection des systèmes, utilisation d'une signalisation sécurisée pour tous les messages de signalisation envoyés aux éléments de réseau NGN situés dans la zone "de confiance", sécurité pour les messages OAMP, ainsi que filtres de paquets et pare-feu. Une "zone non fiable" inclut tous les éléments des réseaux d'abonné ou éventuellement des réseaux homologues ou d'autres domaines du fournisseur NGN, qui sont raccordés aux éléments en limite de réseau du fournisseur NGN. Dans la zone "non fiable", qui comprend des équipements terminaux, ces équipements ne sont pas sous le contrôle des fournisseurs NGN, et la politique de sécurité du fournisseur NGN ne pourra peut-être pas être appliquée à l'utilisateur. Il reste néanmoins souhaitable d'essayer d'appliquer certaines mesures de sécurité et, à cette fin, il est recommandé de sécuriser le trafic de signalisation, le trafic de média et le trafic OAMP et de renforcer la protection de l'élément

en limite TE-BE, situé dans la zone "non fiable". Toutefois, en raison de la communication avec les éléments de réseau situés dans cette zone, le niveau de sécurité est inférieur à celui des communications dans la zone "de confiance".

7.2 Modèle de confiance pour l'interconnexion de réseaux

Lorsqu'un NGN est raccordé à un autre réseau, la présence ou l'absence de confiance dépend:

- de l'interconnexion physique, celle-ci pouvant aller d'une connexion directe dans un bâtiment sécurisé à une connexion entre deux bâtiments (éventuellement non sécurisés) par l'intermédiaire de fonctionnalités partagées;
- du modèle d'interconnexion, le trafic pouvant être échangé directement entre les deux fournisseurs de service NGN, ou transiter par un ou plusieurs fournisseurs de transport NGN;
- des relations commerciales entre les réseaux, des clauses pénales pouvant figurer dans les accords SLA, et/ou de la confiance qu'inspirent les politiques de sécurité de l'autre fournisseur NGN; d'une manière générale, les fournisseurs NGN devraient considérer les autres fournisseurs comme non fiables.

La Figure 2 montre un exemple dans lequel un réseau connecté est considéré comme étant non fiable.

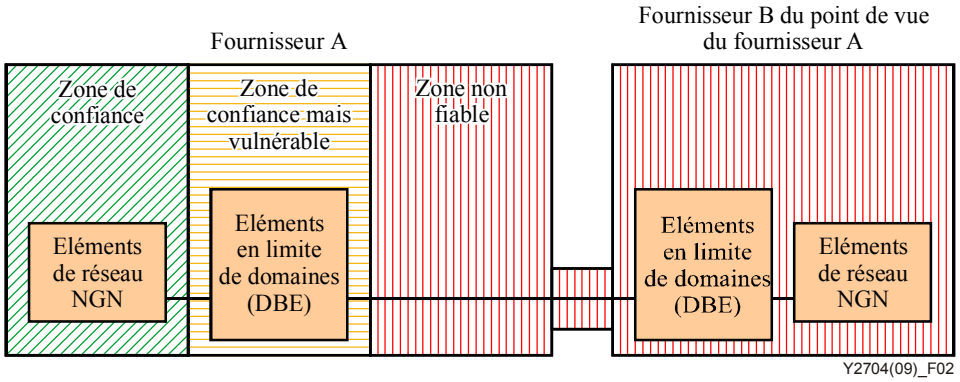


Figure 2 – Modèle de confiance pour l'interconnexion/[UIT-T Y.2701]

8 Identification, authentification et autorisation

Se reporter à [UIT-T Y.2701], [UIT-T Y.2702], [UIT-T Y.2703] et [UIT-T Y.2720] pour des informations relatives à l'identification, à l'authentification, à l'autorisation et à la gestion des identités (IdM).

La présente section décrit les mécanismes d'identification, d'authentification et d'autorisation, en particulier ceux qui se rapportent aux services fondés sur le protocole SIP. Les mécanismes se rapportant à d'autres services appellent un complément d'étude.

8.1 Abonnés

Une demande de service NGN est associée à un abonné. Cette association est déterminée par l'identification de la demande et de l'abonné. Une identification supplémentaire (et une authentification associée) de l'utilisateur final peut être nécessaire en fonction de l'accord SLA entre le fournisseur NGN et l'abonné.

Ce processus peut être exécuté à l'aide d'un élément fonctionnel (appelé authentificateur) qui facilite l'identification et l'authentification d'abonnés, de dispositifs ou d'utilisateurs finals. Par exemple, des éléments en limite de réseau (NBE, *network border element*) avec une fonctionnalité d'agent d'utilisateur dos à dos (B2BUA, *back-to-back user agent*) ou des entités fonctionnelles relais de

commande de session d'appel (P-CSC-FE, *proxy call session control functional entity*) peuvent être des authentificateurs d'abonnés pour des services fondés sur le protocole SIP. L'identification et l'authentification sont assurées par l'échange et la validation du justificatif d'identité entre l'authentificateur et l'équipement terminal.

8.2 Elément de réseau

[UIT-T Y.2701] préconise l'identification et l'authentification des éléments de réseau pour les communications.

Si l'élément en limite reçoit la demande d'un élément de réseau NGN dans la zone de confiance, l'identification associée à cette demande peut être considérée comme exacte et peut ne pas faire l'objet d'une vérification plus approfondie sous réserve de la politique de sécurité du fournisseur de réseau NGN.

Si l'élément en limite reçoit des demandes d'éléments de réseau dans la zone non fiable et dans la zone de confiance mais vulnérable, il est recommandé d'identifier et d'authentifier ces éléments de réseau et de vérifier leurs privilèges de communication. L'identification et l'authentification sont assurées par l'échange et la validation du justificatif d'identité entre l'authentificateur et les éléments de réseau.

8.3 Utilisation du justificatif d'identité pour la sécurité des réseaux NGN

Les justificatifs d'identité sont utilisés dans le cadre de la sécurité des réseaux NGN pour identifier et authentifier un dispositif, un abonné et/ou un utilisateur final. Les différents justificatifs d'identité utilisés pour identifier et authentifier un dispositif, un abonné ou un utilisateur final sont décrits dans le § 8.3.1. Ils peuvent se présenter sous deux formes différentes, à savoir soit un certificat de clé publique X.509 (décrit dans le § 8.3.2), soit une clé partagée (décrite dans le § 8.3.3). Le certificat de clé publique X.509 peut être utilisé pour assurer un transport sécurisé entre l'équipement terminal et l'authentificateur (voir le § 8.3.1) sur la base de la politique adoptée par le fournisseur NGN. La clé partagée, quant à elle, peut être utilisée soit pour assurer un transport sécurisé, soit pour obtenir ou vérifier la réponse à une question ("*challenge*") générée par l'authentificateur (voir la section § 8.3.1) sur la base de la politique adoptée par le fournisseur NGN.

8.3.1 Justificatifs d'identité du dispositif, de l'abonné et de l'utilisateur final

Trois types distincts de justificatif d'identité sont utilisés dans les réseaux NGN:

1) justificatif d'identité du dispositif;
2) justificatif d'identité de l'abonné; et
3) justificatif d'identité de l'utilisateur final.

Le justificatif d'identité du dispositif peut être fourni par le fabricant avec le dispositif. Par exemple, il peut être gravé sur le dispositif, au cours de sa fabrication, et peut comporter des informations comme le numéro de série du dispositif ou le nom du fabricant. Le justificatif d'identité du dispositif identifie ce dernier. Un fournisseur NGN peut associer le justificatif d'identité d'un dispositif à un service particulier de l'abonné afin d'éviter de recourir au justificatif d'identité de l'abonné. En pareil cas, les demandes émanant du dispositif peuvent être associées à un compte particulier sur la base de la politique du fournisseur de réseau NGN.

Le justificatif d'identité de l'abonné est utilisé pour associer l'auteur d'une demande de réseau NGN à un compte particulier. Ce justificatif est enregistré (par exemple par téléchargement, carte SIM, etc.) dans les dispositifs en mesure de l'accepter. Les justificatifs d'identité d'abonné enregistrés dans un dispositif associent l'abonné à ce dispositif. Tous les appels effectués à partir du dispositif seront associés à l'abonné dont le justificatif d'identité est enregistré dans le dispositif. Plusieurs ensembles de justificatifs d'identité peuvent figurer dans un seul dispositif, auquel cas le dispositif fournit le moyen de distinguer les différentes demandes associées à chaque abonné.

NOTE – Un client de réseau NGN peut posséder un ou plusieurs abonnements NGN associés à un ou plusieurs dispositifs, ou à aucun dispositif. En outre, l'abonnement NGN peut être associé à un ou plusieurs utilisateurs finals (l'utilisateur final n'est pas nécessairement l'abonné) qui peuvent utiliser différents dispositifs ou partager le même dispositif en fonction de la politique du fournisseur NGN.

Le justificatif d'identité d'utilisateur final est utilisé pour identifier et authentifier des utilisateurs finals particuliers du réseau. Par exemple, une carte SIM peut identifier l'utilisateur final d'un service particulier; lorsque l'utilisateur final insère sa carte SIM dans le téléphone, celle-ci est alors associée à cet utilisateur final particulier (et tous les appels sont identifiés comme provenant de cet utilisateur final). On citera également le jeton de sécurité, le jeton de matériel (un dispositif physique) ou encore le jeton de logiciel (un programme installé sur un dispositif polyvalent, tel qu'un ordinateur personnel). Ces mécanismes sont fournis à un utilisateur autorisé pour renforcer le processus d'authentification. Un jeton de sécurité peut stocker des clés cryptographiques, telles qu'une signature numérique, ou des données biométriques, telles qu'une empreinte digitale. Une demande émanant d'un dispositif NGN sera identifiée et authentifiée comme provenant de l'utilisateur final associé à ce jeton de sécurité. Dans certains scénarios (par exemple, dans le cas de la carte SIM mentionnée précédemment), il peut être possible pour plusieurs utilisateurs finals d'utiliser le service associé à un seul abonné (un compte d'abonné), les appels en provenance de chaque utilisateur final étant portés au compte de l'abonné. L'abonné et l'utilisateur final peuvent être la même personne, ou il peut y avoir plusieurs utilisateurs finals et un seul abonné. Les utilisateurs finals peuvent s'identifier et s'authentifier eux-mêmes auprès du réseau pour bénéficier de services personnels. Il est possible d'établir, au moyen du justificatif d'identité d'utilisateur final, des associations individuelles de sécurité de couche de transport entre l'équipement terminal et le réseau NGN (authentificateurs). Le fournisseur NGN associe le justificatif d'identité de l'utilisateur final à un service d'abonné particulier à des fins de facturation.

8.3.2 Certificats de clé publique X.509 utilisés comme justificatifs d'identité

Un certificat de clé publique est un document numérique indiquant l'identificateur d'une entité, ses attributs, une clé publique appartenant à l'entité et d'autres informations d'authentification (par exemple, des informations sur l'émetteur du certificat, la liste de révocation de certificats (CRL, *certificate revocation list*), les date et heure de début et de fin de la validité du certificat, etc.). La description de certains champs de base et d'extension d'un certificat de clé publique X.509 est présentée dans le Tableau 1. On se reportera à [UIT-T X. 509] pour une description détaillée des champs des certificats de clé publique X.509. Un certificat de clé publique est signé numériquement par un tiers de confiance, qui est normalement connu sous le nom d'autorité de certification (CA, *certification authority*). Celle-ci calcule un hachage (par exemple, au moyen de l'algorithme d'authentification SHA-1) de tous les champs à l'exception du champ *Valeur de signature*, le chiffre avec sa propre clé privée, puis ajoute la signature, ainsi que l'algorithme de signature appliqué, au certificat (dans le champ *Valeur de signature*).

Tableau 1 – Quelques champs de base et d'extension d'un certificat X.509

Nom du champ	Description
Sujet	Indique l'entité associée au certificat de clé publique (nom distinctif d'annuaire du sujet du certificat)
Numéro de série	Identificateur unique du certificat
Emetteur	Indique l'entité qui a signé et émis le certificat (nom distinctif d'annuaire de l'autorité de certification)
Valide à partir de	Date et heure du début de la validité du certificat
Valide jusqu'à	Date et heure de fin de validité du certificat
Clé publique	Clé publique du titulaire du certificat
Version	Version du certificat de clé publique X.509 codé

Tableau 1 – Quelques champs de base et d'extension d'un certificat X.509

Nom du champ	Description
Autre nom de sujet	Autre identificateur du titulaire du certificat
Points de répartition de liste CRL	Nom ou adresse du point de répartition de liste CRL
Accès aux informations concernant l'autorité	Nom ou adresse pour l'accès aux informations concernant l'autorité de certification
Utilisation avancée de clé	Description des objectifs pour lesquels le certificat peut être utilisé (liste des identificateurs d'objet (OID) définis par l'UIT-T | l'ISO/CEI [UIT-T X.660]
Politiques relatives aux applications	Les applications et les services qui peuvent utiliser le certificat (spécifiés par les identificateurs OID)
Nom du champ	Description
Politiques relatives aux certificats	Politiques et mécanismes utilisés par l'autorité de certification pour la réception d'une demande de traitement, d'autorisation, d'émission et de gestion des certificats
Algorithme de signature	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, SHA-1 avec RSA)
Valeur de signature	Signature réelle du certificat

Les certificats de clé publique spécifiés dans [UIT-T X.509] peuvent être utilisés par les éléments de réseau NGN pour établir des associations de sécurité avec d'autres éléments de réseau, et servir de base à l'identification et à l'authentification mutuelles. Ils peuvent également être utilisés entre l'équipement terminal et l'authentificateur pour les mêmes fins.

Pour un abonné ou un certificat d'utilisateur final, l'identificateur <identificateur de compte d'abonné> (voir le § 8.4.2), un identificateur permettant d'extraire les informations relatives au compte de l'abonné, est utilisé par l'authentificateur pour obtenir davantage d'informations sur le justificatif d'identité par l'intermédiaire des entités fonctionnelles SAA/TAA. Dans le cas d'un certificat de dispositif, le nom du fabricant du dispositif et le numéro de série de ce dernier sont utilisés par l'authentificateur pour déterminer l'<identificateur de compte d'abonné > associé (valide seulement si le dispositif a été associé à un abonné), puis cet identificateur est utilisé pour obtenir davantage d'informations sur le justificatif d'identité par l'intermédiaire des entités fonctionnelles SAA/TAA.

Les certificats d'utilisateur final, de service et de dispositif pourront être utilisés pour créer des connexions de sécurité TLS entre le dispositif et l'authentificateur (voir le § 9.1.2), ou des connexions IPsec par authentification de l'échange de clés Internet (IKE, *Internet key exchange*) (voir le § 9.2.4.3).

8.3.3 Clés partagées utilisées comme justificatifs d'identité

La clé partagée peut être utilisée pour renforcer la sécurité de l'accès au réseau NGN. Dans ce cas, une copie de la clé partagée est remise à l'abonné ou à l'utilisateur final, et une autre copie est stockée dans les entités fonctionnelles appropriées, telles que les entités fonctionnelles de profil d'utilisateur de service (SUP-FE, *service user profile functional entities*) ou dans les entités fonctionnelles de profil d'utilisateur de transport (TUP-FE, *transport user profile functional entities*). Chaque clé doit posséder un nom unique, lequel est utilisé par l'authentificateur pour obtenir davantage d'informations sur le justificatif d'identité.

En cas d'utilisation de clés prépartagées, la force du système dépend de la force du secret partagé. L'objectif est d'empêcher que le secret partagé soit le maillon faible de la chaîne de sécurité. Cela

suppose que son entropie (caractère aléatoire) soit aussi élevée que celle du chiffre utilisé. En d'autres termes, il est recommandé que le secret partagé possède au moins 128-160 bits d'entropie.

Il convient de noter qu'il existe certaines différences entre la cryptographie symétrique et la cryptographie asymétrique, décrite au § 8.3.2, et de prendre en considération ce qui suit :

– une entité doit disposer d'un ensemble de clés symétriques distinct pour chacun des partenaires avec qui elle communique;
– les clés doivent être configurées, établies, et conservées de manière sécurisée;
– une entité doit faire confiance à son partenaire concernant la non-divulgation de la clé partagée.

8.3.4 Informations fournies dans les entités fonctionnelles SUP/TUP pour chaque ensemble de justificatifs d'identité

Les entités fonctionnelles SUP/TUP sont les répertoires contenant tous les justificatifs d'identité (de dispositifs, d'abonnés et d'utilisateurs finals) devant être utilisés pour accéder à l'infrastructure NGN. Elles sont généralement implémentées comme une partie intégrante de l'authentificateur afin d'optimiser le traitement des demandes d'authentification. Toutefois, pour assurer la mobilité, l'authentificateur peut avoir besoin de consulter un serveur distant d'entités fonctionnelles SAA/TAA afin d'obtenir des informations sur les justificatifs d'identité. L'identificateur de compte d'abonné, ou le nom de la clé sera utilisé pour extraire ces informations par le biais des entités fonctionnelles SAA/TAA.

Les informations relatives à la sécurité ci-après, qui sont associées à chaque ensemble de justificatifs d'identité, doivent être fournies dans les entités fonctionnelles, telles que les entités fonctionnelles SUP/TUP stockant les justificatifs d'identité:

1) l'identificateur de compte d'abonné ou le nom de la clé;
2) le fait que l'identification et l'authentification de l'utilisateur final soient requises ou non pour cet abonné;
3) le fait que ces justificatifs d'identité décrivent un abonné ou un utilisateur final; et
4) les valeurs autorisées de l'en-tête "Origine" ("*From*") dans les demandes.

On trouvera ci-après quelques exemples d'informations stockées dans les répertoires de justificatifs d'identité, tels que les entités fonctionnelles SUP/TUP.

Pour un certificat de dispositif NGN d'équipement terminal prenant en charge quatre lignes du service téléphonique ordinaire, avec les numéros 212-555-1111-1113 et 1151:

Compte d'abonné:	123-456789
En-tête "Origine":	sip:212-555-111[1-3]@NGN .ngn.com
	| sip:212-555-1151@NGN .ngn.com
Chaîne de caractères d'identité:	sip:212-555-1111@NGN .ngn.com
Type de justificatif d'identité:	abonné
Identificateur d'utilisateur final obligatoire:	non

Pour un certificat d'abonné attribué à la famille de John Doe:

Compte d'abonné:	famille Doe
En-tête "Origine":	sip:*Doe@NGN .ngn.com
Chaîne de caractères d'identité:	sip:Doe@NGN .ngn.com
Type de justificatif d'identité:	abonné
Identificateur d'utilisateur final obligatoire:	non

Pour une clé prépartagée attribuée à la famille de John Doe:

Nom de la clé:	JohnDoe
Clé:	dfe56131d1958046689d83306477ecc
En-tête "Origine":	sip:*Doe@NGN .ngn.com
Chaîne de caractères d'identité:	sip:Doe@NGN .ngn.com
Type de justificatif d'identité:	abonné
Identificateur d'utilisateur final obligatoire:	non

Pour un élément en limite d'équipement terminal desservant l'entreprise Acme Widget:

Compte d'abonné:	Acme Widget Company
En-tête "Origine":	sip:*@acme.com
Chaîne de caractères d'identité:	sip:acme.com
Type de justificatif d'identité:	abonné
Identificateur d'utilisateur final obligatoire:	non

Pour un utilisateur final de l'entreprise Acme Widget:

Compte d'abonné:	Acme Widget Company
En-tête "Origine":	sip:bob@acme.com
Chaîne de caractères d'identité:	sip:bob@acme.com
Type de justificatif d'identité:	utilisateur final

8.4 Identification et authentification des abonnés

8.4.1 Stratégie d'ensemble

L'identité de l'expéditeur dans le protocole SIP figure généralement dans l'en-tête "Origine". Toutefois, l'identification de l'abonné au moyen de l'en-tête "Origine" dans une demande SIP présente des risques d'attaques par usurpation et n'est donc pas utilisée lorsqu'un degré élevé de garantie de l'identité d'abonné est requis. Dans ce cas, la valeur de l'en-tête "Origine" sera comparée avec l'identité d'abonné obtenue par un autre moyen.

Afin de réduire au minimum les effets sur le délai d'établissement d'un appel, on déterminera l'identification et l'authentification de l'abonné à partir de l'adresse d'origine du réseau (l'adresse d'origine figurant dans l'en-tête de paquet IP) ou à partir de l'association de sécurité de transport (l'association établie au moyen, par exemple, des mécanismes IPsec ou TLS entre le dispositif d'origine et l'authentificateur) chaque fois que cela est possible. Lorsque ces techniques ne permettent pas d'obtenir une identification cohérente avec l'en-tête "Origine" dans la demande SIP, une question ("*challenge*") est émise par l'expéditeur; si la réponse contient le justificatif d'identité correct, la demande sera traitée. Ces procédures sont décrites plus en détail dans les paragraphes qui suivent.

Les procédures énoncées dans le § 8.4.2 décrivent la manière dont l'authentificateur déduit, sur la base de l'adresse d'origine du réseau, que:

1) soit l'abonné ne peut pas être déterminé au moyen de cette méthode;

2 soit l'abonné est déterminé et correspond à la valeur de l'en-tête "Origine" de la demande;

3) soit l'abonné est déterminé mais ne correspond pas à la valeur de l'en-tête "Origine" de la demande.

Les procédures énoncées dans le § 8.4.3 décrivent la manière dont l'authentificateur déduit, sur la base de l'association de sécurité de transport, que:

1) soit l'abonné ne peut pas être déterminé au moyen de cette méthode;
2) soit l'abonné est déterminé et correspond à la valeur de l'en-tête "Origine" de la demande;
3) soit l'abonné est déterminé mais ne correspond pas à la valeur de l'en-tête "Origine" de la demande.

Les actions exécutées ensuite par l'authentificateur sont présentées dans le Tableau 2.

Tableau 2 – Actions de l'authentificateur pour chaque résultat d'authentification

Détermination de l'abonné à partir de l'adresse d'origine	Détermination de l'abonné à partir de l'association de sécurité de transport	Actions de l'authentificateur
N/A	N/A	Utilisation de la question/réponse
N/A	Correspondance	OK
N/A	Divergence	Utilisation de la question/réponse
Correspondance	N/A	OK
Correspondance	Correspondance	OK
Correspondance	Divergence	Utilisation de l'identité d'abonné à partir de l'adresse d'origine du réseau
Divergence	N/A	Utilisation de la question/réponse
Divergence	Correspondance	Utilisation de l'identité d'abonné à partir de l'association de sécurité de transport
Divergence	Divergence	Utilisation de la question/réponse
N/A = non applicable		

Si l'action résultant consiste à utiliser une question/réponse, les procédures énoncées dans le § 8.4.4 seront appliquées.

Outre la stratégie décrite dans les § 8.4.2 à 8.4.4, il est possible d'utiliser aussi l'architecture d'amorçage générique (GBA, *generic bootstrapping architecture*) pour l'identification et l'authentification d'abonnés. Cette procédure est décrite dans le § 8.4.5.

Les stratégies d'authentification décrites dans la présente Recommandation sont des exemples types, chaque fournisseur NGN ayant le choix d'appliquer les stratégies qu'il souhaite (par exemple, une seule procédure décrite dans les paragraphes qui suivent).

8.4.2 Identification de l'abonné par l'adresse d'origine du réseau

Il s'agit de la manière la plus simple d'identifier l'abonné, consistant à utiliser uniquement sur l'adresse d'origine fournie avec les paquets IP. L'authentificateur consulte une liste d'adresses IP préalablement fournie établissant une correspondance avec l'<identificateur de compte d'abonné>; si l'adresse d'origine de la demande figure dans cette liste, l'authentificateur considère que la demande provient de cet abonné. L'<identificateur de compte d'abonné> est ensuite utilisé pour obtenir le justificatif d'identité de l'abonné par l'intermédiaire des entités fonctionnelles SAA/TAA, et en vérifier la cohérence avec la valeur de l'en-tête "Origine".

Si la valeur de l'en-tête "Origine" est compatible avec l'abonné, il y a "correspondance"; si la valeur de l'en-tête "Origine" n'est pas compatible avec l'abonné, il y a "divergence"; si l'adresse IP d'origine ne figure dans aucune des séries d'adresses préalablement fournies, elle est alors considérée comme étant "non applicable".

L'efficacité de cette méthode d'identification de l'abonné dépend de la garantie de l'adresse d'origine. Cela suppose que l'adresse IP ne puisse être utilisée que par l'abonné légitime auquel l'adresse est attribuée. A cet effet, les deux mécanismes indiqués ci-après sont nécessaires pour les entités fonctionnelles de traitement du transport et de commande du transport, et doivent être correctement coordonnés: 1) gestion stricte d'un mappage entre un abonné et l'adresse qui lui a été attribuée; et 2) prévention de l'usurpation d'adresse sur la base de ces informations gérées. Se reporter à l'Appendice I pour avoir des exemples des mécanismes susmentionnés et des explications sur leur coordination.

8.4.3 Identification de l'abonné par l'association de sécurité TLS/IPsec

Si un transport TLS sécurisé a été établi pour le trafic de signalisation entre le dispositif d'origine et l'authentificateur, et s'il a été authentifié au moyen d'un certificat d'élément TE-BE X.509 (voir le § 8.3.2), l'authentificateur vérifie si l'en-tête "Origine" correspond aux valeurs autorisées de l'abonné identifié dans l'<identificateur de compte d'abonné>.

Si un transport sécurisé (par IPsec ou TLS) a été établi pour le trafic de signalisation entre le dispositif d'origine et l'authentificateur, et s'il a été authentifié au moyen d'un certificat de dispositif NGN d'équipement terminal X.509 (voir les § 8.3.1 et 8.3.2), l'authentificateur utilise alors les informations concernant le fabricant du dispositif et le numéro de série du dispositif pour déterminer l'<identificateur de compte d'abonné> associé (applicable uniquement si le dispositif a été associé à un abonné). L'<identificateur de compte d'abonné> est employé pour obtenir le justificatif d'identité de l'abonné, dont on vérifie la cohérence avec la valeur de l'en-tête "Origine".

Si un transport sécurisé (par IPsec ou TLS) a été établi pour le trafic de signalisation entre le dispositif d'origine et l'authentificateur, et s'il a été authentifié au moyen d'un certificat d'abonné NGN d'équipement terminal X.509 (voir les § 8.3.1 et 8.3.2), l'authentificateur utilise alors l'<identificateur de compte d'abonné> pour obtenir le justificatif d'identité de l'abonné par l'intermédiaire des entités fonctionnelles SAA/TAA. L'authentificateur vérifie ensuite la cohérence du justificatif d'identité de l'abonné avec la valeur de l'en-tête "Origine".

Si un transport sécurisé (par IPsec ou TLS) a été établi pour le trafic de signalisation entre le dispositif d'origine et l'authentificateur, et s'il a été authentifié au moyen d'un certificat d'utilisateur final NGN d'équipement terminal X.509 (voir les § 8.3.1 et 8.3.2), l'authentificateur utilise l'<identificateur de compte d'abonné> pour obtenir le justificatif d'identité de l'abonné par l'intermédiaire des entités fonctionnelles SAA/TAA. L'authentificateur vérifie ensuite la cohérence du justificatif d'identité de l'abonné avec la valeur de l'en-tête "Origine".

Si un transport sécurisé (par IPsec ou TLS) a été établi pour le trafic de signalisation entre le dispositif d'origine et l'authentificateur, et s'il a été authentifié au moyen d'une clé prépartagée (voir le § 9.2.4.3.1), l'authentificateur utilise le nom de clé pour obtenir le justificatif d'identité de l'abonné par l'intermédiaire des entités fonctionnelles SAA/TAA. L'authentificateur vérifie ensuite la cohérence du justificatif d'identité de l'abonné avec la valeur de l'en-tête "Origine".

Si un transport sécurisé n'a pas été utilisé entre le dispositif d'origine et l'authentificateur, ou si une connexion TLS "client anonyme" a été utilisée, cette méthode est alors considérée comme étant "non applicable".

8.4.4 Identification de l'abonné par la question/réponse

Le mécanisme question/réponse est une version plus sûre du système dépassé identificateur d'utilisateur/mot de passe (lors de l'envoi d'un identificateur d'utilisateur et d'un mot de passe pour une demande de service, ces informations sont facilement reproduites pour obtenir ultérieurement un service frauduleux). Dans un mécanisme question/réponse, le serveur envoie une question au client, en lui demandant d'exécuter une opération de chiffrement à l'aide d'une clé partagée. Le résultat de ce calcul est indiqué dans la réponse et est ensuite vérifié par le serveur. Si l'échange est intercepté

par des tiers, la reproduction est impossible tant que le serveur ne réutilise jamais une ancienne question.

Le protocole d'échange clé authentifiée par mot de passe (PAK, *password authenticated key*) constitue l'une des méthodes importantes de type question/réponse qui allient la commodité des méthodes d'authentification reposant sur un mot de passe et la sécurité des méthodes reposant sur le mécanisme question/réponse. Le protocole PAK assure l'authentification mutuelle des deux parties par la création d'une clé cryptographique symétrique dans le cadre d'un échange Diffie-Hellman. L'échange Diffie-Hellman assure la confidentialité totale vers l'avant (*perfect forward secrecy*), propriété d'un protocole de création de clés garantissant que la compromission d'une clé de session ou d'une clé privée à long terme après une session donnée ne provoque pas la compromission d'une session précédente. En outre, la méthode d'authentification PAK protège l'échange contre les attaques par entremetteurs (*man-in-the-middle*). L'authentification repose sur un secret préalablement partagé, qui est protégé (qui reste non révélé) des intrus, empêchant ainsi les attaques de type dictionnaire hors ligne. Ainsi, ce protocole peut être utilisé dans toute une série d'applications faisant intervenir des secrets prépartagés utilisant des mots de passe pouvant être faibles. Le protocole PAK est spécifié dans [UIT-T X.1035] et dans [b-TIA 683-D].

Un mécanisme de question/réponse suppose un échange de message supplémentaire entre l'authentificateur et le point d'extrémité d'origine, ainsi que la réalisation préalable d'un calcul par ce dernier. Il peut donc avoir une incidence sur le temps de réponse perçue par l'utilisateur. Dans le cadre de la sécurité des réseaux NGN, il s'agira d'utiliser le mécanisme de question/réponse uniquement dans le cas où cela est absolument indispensable pour atteindre le niveau nécessaire d'identification et d'authentification.

Si une connexion de transport sécurisé (par IPsec ou TLS) a été établie pour le trafic de signalisation entre le dispositif d'origine et l'authentificateur, et qu'une demande préalable dans un délai configurable avec le même contenu d'en-tête "Origine" a été authentifiée avec succès par l'authentificateur, l'authentification est alors considérée comme étant réussie et la demande est acceptée. Dans le cas de la signalisation d'établissement d'appel, étant donné que la première demande sur une nouvelle connexion est généralement "REGISTER", ce mécanisme de question/réponse sera exécuté à un moment qui n'affecte pas le délai d'établissement de l'appel.

Les demandes d'authentification nécessitant d'importants calculs, il est essentiel que l'authentificateur limite la fréquence des interrogations aux entités fonctionnelles SAA/TAA. Les limites fixées dans le présent paragraphe peuvent être appliquées, que les entités fonctionnelles SAA/TAA fassent partie intégrante de l'authentificateur ou qu'elles soient indépendantes. Une attaque par déni de service consiste simplement pour un point d'extrémité donné à inonder l'authentificateur de demandes incorrectes (si, pour chaque demande, un calcul cryptographique est requis dans les entités fonctionnelles SAA/TAA, le service est essentiellement retardé ou bloqué pour toutes les demandes valides ou invalides). Pour faire face à ces attaques, l'authentificateur peut rejeter localement une demande s'il existe une demande d'autorisation en instance provenant du même point d'extrémité. Selon une variante légèrement plus complexe de cette méthode, l'authentificateur rejette localement une demande s'il y a eu au moins XXX demandes au total au cours des YYY secondes passées (les valeurs XXX et YYY sont configurables dans l'authentificateur). En outre, l'authentificateur peut délibérément attendre un certain délai configurable avant de répondre à une demande d'autorisation défavorable. Cela permet aussi de prévenir divers types d'attaques par "craquage de mot de passe".

8.4.4.1 Mécanisme de question/réponse avec signalisation SIP depuis le dispositif d'origine

Si le dispositif d'origine utilise le protocole de signalisation SIP, les mécanismes d'authentification de mandataire définis dans [b-IETF RFC 3261] peuvent être utilisés à titre facultatif pour implémenter une question/réponse. Voir le § 22.2 de [b-IETF RFC 3261], la section 3 de [b-IETF RFC 2617] et la section 3 de [b-IETF RFC 3310].

L'authentificateur répond à la demande SIP au moyen d'une réponse 407 (authentification de mandataire requise). Cette réponse comporte un en-tête d'authentification de mandataire contenant les éléments suivants: mécanisme d'authentification de type "Digest", domaine "NGN .ngn.net", paramètre qop "auth", paramètre "Nonce" contenant une valeur cryptographiquement aléatoire de 16 octets (sous forme hexadécimale), éventuellement valeur du paramètre "Opaque" et algorithme "MD5" ou "AKAv1-MD5" en fonction de l'accord de service conclu avec le client.

On trouvera ci-après un exemple d'en-tête d'authentification de mandataire contenu dans une réponse 407:

```
Proxy-Authenticate: Digest realm="NGN .ngn.com", qop="auth",
nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="", stale=FALSE, algorithm=MD5
```

Le dispositif d'origine répond à la réponse 407 par une demande régénérée, contenant un en-tête d'authentification de mandataire. On vérifie si cet en-tête contient les informations suivantes: mécanisme d'authentification "Digest", paramètre "Realm" identique à celui de la réponse 407, paramètre "Nonce" identique à celui de la réponse 407 et paramètre "Opaque" identique à celui de la réponse 407. L'en-tête d'authentification de mandataire comprend également un paramètre "Username" indiquant le nom de clé, un paramètre "Uri" correspondant au champ "Request-URI" de la demande et un paramètre "Response" représentant le hachage, tel que spécifié dans [b-IETF RFC 2617] ou [b-IETF RFC 3310].

On trouvera ci-après un exemple d'en-tête d'authentification de mandataire dans une demande réémise:

```
Proxy-Authorization: Digest username="bob", realm="NGN .ngn.com",
nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="", uri="sip:5551212@ngn.com",
response="dfe56131d1958046689d83306477ecc"
```

Les mécanismes d'"authentification d'utilisateur à utilisateur" définis dans [b-IETF RFC 3261] peuvent également être utilisés pour implémenter une question/réponse. Pour de plus amples détails, se reporter au § 22.2 de [b-IETF RFC 3261], à la section 3 de [b-IETF RFC 2617] et à la section 3 de [b-IETF RFC 3310].

Si une demande doit être dupliquée, divers éléments de réseau NGN (par exemple, les éléments fonctionnels MGC-FE) et/ou des équipements de terminal souhaiteront peut-être envoyer une question au dispositif d'origine. L'élément de réseau duplicateur (par exemple, l'élément fonctionnel S-CSC) regroupe toutes ces questions et les place dans une seule réponse que l'élément de réseau duplicateur envoie au dispositif d'origine. A la réception de la réponse contenant plusieurs questions, le dispositif d'origine indique plusieurs justificatifs d'identité dans une demande et la soumet à nouveau.

8.4.4.2 Mécanisme de question/réponse avec un protocole de signalisation différent du protocole SIP utilisé par le dispositif d'origine

Si le dispositif d'origine est censé utiliser le protocole SIP, mais émet sa demande au moyen d'un protocole de signalisation autre que le protocole SIP, le mécanisme de question/réponse est considéré comme ayant échoué. La demande est rejetée.

8.4.5 Architecture d'amorçage générique (GBA)

L'architecture d'amorçage générique (GBA, *generic bootstrapping architecture*) spécifie une procédure d'amorçage indépendante de l'accès. Elle fournit un cadre pour l'authentification mutuelle d'utilisateurs finals, la fonction d'application de réseau (NAF, *network application function*) pouvant être utilisée pour l'identification et l'authentification d'abonnés dans le réseau NGN. Pour de plus amples informations sur l'architecture GBA, se reporter à [b-ETSI TS 133 220].

8.5 Identification et authentification d'utilisateurs finals

8.5.1 Stratégie d'ensemble

Alors que l'identification de l'abonné est absolument nécessaire pour l'infrastructure NGN, l'identification de l'utilisateur final est un service facultatif, pouvant être demandé par l'abonné ou requis par le service. Ce type d'identification est généralement utilisé lorsqu'il s'agit de fournir des services additionnels, comme la mobilité des personnes ou la présence, pour lesquels l'identité de l'utilisateur soumettant la demande est requise. Lorsqu'un abonné souhaite ce niveau supplémentaire d'identification, il est nécessaire que tous les dispositifs de point d'extrémité concernés soient en mesure d'inclure des justificatifs d'identité supplémentaires d'utilisateur final ou d'utiliser un certificat d'utilisateur final au lieu d'un certificat d'abonné.

L'authentificateur peut identifier et authentifier l'utilisateur final selon deux méthodes différentes. La première méthode fait intervenir l'association de la sécurité de la couche de transport utilisée pour l'échange de signalisation. Si cette association de sécurité est établie avec un certificat d'utilisateur final (ou si une clé prépartagée est associée à un seul utilisateur final), l'identification de l'utilisateur final est terminée. La seconde méthode fait intervenir un mécanisme de question/réponse dans lequel le nom de clé indiqué dans la réponse est associé à un seul utilisateur final. Ces deux méthodes sont décrites plus en détail dans les paragraphes qui suivent.

Un dispositif NGN évolué peut avoir plusieurs identités (par exemple, un certificat d'abonné et un ou plusieurs certificats d'utilisateur final pour la ou les personnes utilisant actuellement le dispositif). Un tel dispositif établit en principe plusieurs connexions TLS avec l'authentificateur (une connexion distincte pour chaque certificat). Il envoie ensuite des demandes à l'authentificateur lors de la connexion de signalisation appropriée en fonction de l'identité souhaitée pour l'appel.

Un problème se pose lorsque le justificatif d'identité d'un seul utilisateur est toujours valide longtemps après que celui-ci n'est plus "actif". Si l'association de sécurité du transport a été établie sur la base d'un certificat d'utilisateur final, l'abonné peut exiger une activité continue afin de maintenir la validité de l'authentification. Sans cette activité, l'authentificateur met fin à la connexion de transport sécurisée et exige que le dispositif d'origine établisse à nouveau la connexion avec le certificat en vigueur de l'utilisateur final (ou le certificat de l'abonné ou du dispositif si le certificat de l'utilisateur final n'est pas disponible). Les conditions détaillées du comportement de l'authentificateur sont décrites dans les § 9.1.2 et 9.2.4.3.1. Ce comportement repose sur l'utilisation de deux temporisateurs: l'un qui limite la durée absolue pendant laquelle le justificatif d'identité de l'utilisateur final peut être valide pour une association de sécurité, et l'autre qui limite le temps d'inoccupation entre les demandes successives. Les valeurs de temporisation peuvent être paramétrées en fonction de l'abonné ou de l'utilisateur final, mais doivent être limitées par les valeurs maximales fixées par le fournisseur de réseau NGN.

8.5.2 Identification de l'utilisateur final par l'association de sécurité TLS/IPsec

Si un transport TLS sécurisé a été établi pour le trafic de signalisation entre le dispositif d'origine et l'authentificateur, et s'il a été authentifié au moyen d'un certificat d'élément TE-BE X.509 (voir le § 8.6), l'authentificateur vérifie si l'en-tête "Origine" correspond aux valeurs autorisées pour l'abonné identifié dans l'<identificateur de compte d'abonné> figurant dans le certificat.

Si un transport sécurisé (par IPsec ou TLS) a été établi pour le trafic de signalisation entre le dispositif d'origine et l'authentificateur, et s'il a été authentifié au moyen d'un certificat d'utilisateur final NGN d'équipement terminal X.509 (voir le § 8.6), l'authentificateur utilise alors l'<identificateur de compte d'abonné> pour obtenir le justificatif d'identité de l'abonné par l'intermédiaire des entités fonctionnelles SAA/TAA. L'authentificateur vérifie ensuite la cohérence du justificatif d'identité de l'abonné avec la valeur de l'en-tête "Origine". Si un transport IPsec sécurisé a été établi pour le trafic de signalisation entre le dispositif d'origine et l'authentificateur (voir le § 8.4.4) et que ce transport sécurisé a été authentifié avec une clé prépartagée (voir le § 9.2.4.3.1), l'authentificateur utilise le nom de clé pour obtenir le justificatif d'identité de l'abonné

par l'intermédiaire des entités fonctionnelles SAA/TAA. L'authentificateur vérifie ensuite la cohérence du justificatif d'identité d'abonné avec la valeur de l'en-tête "Origine".

8.5.3 Identification de l'utilisateur final au moyen du mécanisme question/réponse

Les procédures applicables au mécanisme question/réponse pour l'identification d'un utilisateur final sont identiques à celles utilisées pour identifier l'abonné (voir le § 8.4.4).

La seule différence réside dans le fait que l'authentificateur vérifie les informations relatives au nom de clé extraites par les entités fonctionnelles SAA/TAA pour savoir si la clé est associée à l'utilisateur final. Si tel est le cas, l'identification de l'utilisateur final a réussi.

Si l'authentificateur a déjà exécuté une procédure question/réponse pour identifier l'abonné, et que la clé nommée renvoyée dans la réponse n'a pas permis d'identifier un utilisateur final, l'identification de l'utilisateur final a échoué. Si un mécanisme question/réponse n'a pas été nécessaire pour identifier l'abonné, une question est à présent émise.

8.6 Identification et authentification par l'élément TE-BE

Les procédures d'identification et d'authentification exécutées par un élément TE-BE sont identiques à celles exécutées par un authentificateur à deux différences près:

1) L'élément TE-BE peut être configuré avec tous les justificatifs d'identité nécessaires pour identifier et authentifier le ou les abonnées et les utilisateurs finals qu'il dessert, étant donné qu'il n'a pas accès à la fonction répartie des entités fonctionnelles SAA/TAA dont dispose l'authentificateur.
2) La demande réémise en réponse à une question de l'authentificateur, contenant l'en-tête "Autorisation de mandataire ", est transmise à l'authentificateur au lieu d'être traitée par l'élément TE-BE.

8.6.1 Utilisation de certificats X.509

Une association de sécurité existe entre chaque élément TE-BE et au moins un élément NBE, établie avec le certificat X.509 délivré à l'élément TE-BE. Les demandes reçues par l'élément NBE suivent les procédures d'identification et d'authentification énoncées dans le § 8.4.3, ce qui conduit l'élément TE-BE à effectuer une vérification minimale de l'identification. Lorsqu'un mécanisme de question/réponse est nécessaire (par exemple, pour un utilisateur "itinérant"), l'échange s'effectuera entre le point d'extrémité d'origine et l'élément NBE et transitera de façon transparente par l'élément TE-BE.

Un transport sécurisé entre le point d'extrémité et l'élément TE-BE est facultatif. Il est prévu que l'adresse d'origine du réseau identifie de façon adéquate la plupart des demandes.

Les points d'extrémité s'enregistrent auprès de l'élément NBE via l'élément TE-BE.

8.7 Interface entre l'authentificateur et les entités fonctionnelles SAA/TAA

8.7.1 Utilisation du protocole RADIUS et de ses extensions

Les entités fonctionnelles SAA/TAA contiennent le point de décision, et les entités fonctionnelles SUP/TUP sont les répertoires contenant tous les justificatifs d'identité des utilisateurs finals et des dispositifs dans l'infrastructure NGN. Certaines fonctions des entités fonctionnelles SAA/TAA, telles que l'authentification, peuvent être réparties afin d'optimiser la performance des demandes d'authentification.

Deux protocoles concurrents sont généralement utilisés pour la communication entre l'authentificateur et les entités fonctionnelles SAA/TAA: le protocole RADIUS [b-IETF RFC 2865] (bien connu et bien pris en charge) et le protocole Diameter [b-IETF RFC 3588] (défini pour corriger plusieurs défauts du protocole RADIUS). L'objectif final de l'infrastructure NGN est de migrer vers le protocole Diameter; toutefois, il est reconnu que les implémentations actuelles des serveurs sont

fondées sur le protocole RADIUS, et que les nombreuses extensions spécifiques du protocole RADIUS de base ont été élaborées pour répondre aux besoins de cette fonction d'authentification. Même si la version de la présente Recommandation est fondée sur le protocole RADIUS avec l'extension décrite dans [b-IETF RFC 5090], il est probable qu'une version future se fonde sur le protocole Diameter avec l'extension décrite dans [b-IETF RFC 4740].

L'authentificateur devient un client RADIUS et le serveur des entités fonctionnelles SAA/TAA devient un serveur RADIUS, comme il est défini dans [b-IETF RFC 2865]. Ils peuvent tous les deux implémenter les extensions pour l'authentification Digest SIP, comme il est indiqué dans [b-IETF RFC 5090]. La connexion entre l'authentificateur et les entités fonctionnelles SAA/TAA peuvent être sécurisées au moyen du mécanisme IPsec avec authentification mutuelle.

Grâce aux extensions [b-IETF RFC 4590], l'authentificateur lance une demande de protocole RADIUS avec les paramètres de l'en-tête d'authentification de mandataire; le serveur RADIUS calcule la réponse prévue et la renvoie à l'authentificateur. L'authentificateur valide ensuite la demande en comparant la réponse réelle reçue du point d'extrémité avec la réponse prévue.

On trouvera ci-après un exemple de message envoyé par l'authentificateur aux entités fonctionnelles SAA/TAA:

```
Code = 1 (Access-Request)
      Identifier = 1
      Length = 164
      Authenticator = 56 7b e6 9a 8e 43 cf b6 fb a6 c0 f0 9a 92 6f 0e
      Attributes:
      NAS-IP-Address = d5 89 45 26 (213.137.69.38)
      NAS-Port-Type = 5 (Virtual)
      User-Name = "bob"
      Digest-Response (206) = "2ae133421cda65d67dc50d13ba0eb9bc"
      Digest-Attributes (207) = [Realm (1) = "NGN .ngn.com"]
      Digest-Attributes (207) = [Nonce (2) = "ea9c8e88df84f1cec4341ae6cbe5a359"]
      Digest-Attributes (207) = [Method (3) = "INVITE"]
      Digest-Attributes (207) = [URI (4) = "sip:5551212@ngn.com"]
      Digest-Attributes (207) = [Algorithm (5) = "md5"]
      Digest-Attributes (207) = [User-Name (10) = "bob"]
On trouvera ci-après un exemple de réponse envoyée par les entités fonctionnelles
SAA/TAA à l'authentificateur:
Code = 2 (Access-Accept)
      Identifier = 1
      Length = 20
      Authenticator = 6d 76 53 ce aa 07 9a f7 ac b4 b0 e2 96 2f c4 0d
      Attributes:
      Digest-Response (206) = "dfe56131d1958046689d83306477ecc"
```

8.7.2 Association de sécurité pour la signalisation de transport

Lorsqu'un certificat X.509 est utilisé pour l'établissement de l'association de sécurité pour la signalisation de transport, les entités fonctionnelles SUP/TUP stockent (selon une indexation par l'<identificateur de compte d'abonné>) l'ensemble des en-têtes acceptables "Origine" pouvant figurer dans les demandes en provenance de cette source, qui seront comparées à l'en-tête "Origine" fourni dans la demande.

Si une clé prépartagée est utilisée pour l'établissement de l'association de sécurité pour la signalisation de transport (par exemple, le fournisseur de service d'échange de trafic), les entités fonctionnelles SUP/TUP stockent (selon une indexation par le nom de clé) l'ensemble des en-têtes "Origine" acceptables pouvant figurer dans les demandes en provenance de cette source, qui seront comparées à l'en-tête "Origine" fourni dans la demande.

8.8 Identification et authentification du trafic support

Il est parfois souhaitable d'identifier un flux de trafic support individuel en vue de renforcer la sécurité, par exemple, pour faire face aux attaques frauduleuses, telles que les attaques par usurpation d'identité ou par injection RTP. Dans le réseau NGN, le trafic support peut être identifié par un quintuplet contenant:

- l'adresse IP d'origine;
- l'adresse IP de destination;
- le port d'origine;
- le port destination; et
- le numéro de protocole.

Le mécanisme d'identification décrit dans le présent paragraphe fait appel à cet identificateur pour l'authentification de chaque paquet. Il repose sur l'utilisation d'un secret partagé et de la fonction de hachage cryptographique, à savoir le code d'authentification de message avec hachage (HMAC, *hash message authentication code*). Se reporter à [b-NIST FIPS 198-1] pour de plus amples informations.

Les entités participant au processus d'authentification – la fonction d'utilisateur final et l'entité fonctionnelle de nœud d'accès – sont décrites dans [UIT-T Y.2701] et sont illustrées par la Figure 3, l'interface UNI étant prise comme exemple.

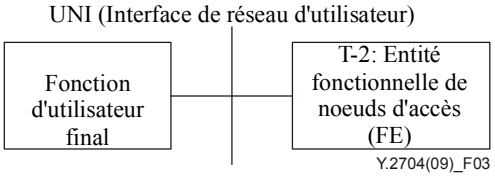


Figure 3 – Entités de réseau NGN intervenant dans la procédure d'authentification – Exemple de l'interface UNI

La description du mécanisme repose sur les conventions suivantes:

- *F* est un identificateur (quintuplet) du trafic support.
- *K* est un secret partagé que possèdent la fonction d'utilisateur final et l'entité fonctionnelle de nœud d'accès.
- *P* est un paquet que la fonction utilisateur final a l'intention d'envoyer à l'entité fonctionnelle de nœud d'accès.
- *i* est un numéro de séquence d'un paquet incrémenté par les deux parties communicantes. Cette valeur est codée sur 64 bits.
- *t* est une horodate – une valeur codée sur 64 bits indiquant le temps en secondes. Cela peut être également une valeur de circonstance.
- *(P', Q)* est un paquet reçu par l'entité fonctionnelle de nœud d'accès.

Lorsque la fonction d'utilisateur final souhaite envoyer un paquet *P* à l'entité fonctionnelle de nœud d'accès, il calcule d'abord une quantité *H(F, t+i, K)*, qui est une fonction de hachage d'une concaténation de *F*, *t+i* et *K*, puis relie cette quantité au paquet *P.* Ainsi, le paquet entier envoyé par la fonction d'utilisateur final à l'entité fonctionnelle de nœud d'accès est *[P, H(F, t+i, K)]*. Lorsque l'entité fonctionnelle de nœud d'accès reçoit un paquet (*P', Q*), il calcule la quantité *H(F, t+i, K)*. En cas d'utilisation d'une horodate, l'entité fonctionnelle de nœud d'accès calcule les valeurs de hachage pour toutes les valeurs de *t* qui sont comprises dans l'intervalle convenu pour la différence de temps entre la fonction d'utilisateur final et l'entité fonctionnelle de nœud d'accès (cela doit être exécuté une seule fois au début d'une session). Dans ce cas, l'entité fonctionnelle de nœud d'accès cherche une correspondance entre la valeur *Q* et toute valeur parmi les valeurs de hachage calculées. S'il y a

correspondance, le paquet est authentifié. La valeur correspondante de *t* sera utilisée pour les paquets du flux.

Si une valeur de circonstance est utilisée, l'entité fonctionnelle de nœud d'accès vérifie simplement si la valeur calculée du hachage est égale à la valeur *Q*. Si tel est le cas, le paquet est authentifié.

Dans un environnement présentant des risques de pertes de paquets, incrémenter simplement la valeur i de paquet en paquet peut ne pas être suffisant. Dans ce cas, l'entité fonctionnelle de nœud d'accès fera peut-être une recherche entre *i* et *i+d* (d étant un petit nombre) pour resynchroniser *i*.

Ce mécanisme d'authentification aide à faire face aux attaques frauduleuses, telles que les attaques par usurpation d'identité ou par injection RTP.

Il permet en outre d'authentifier le trafic généré par l'utilisateur sans avoir à révéler l'identité de ce dernier.

Pour permettre cette configuration, il est proposé que la fonction d'utilisateur final et l'entité fonctionnelle de nœud d'accès conviennent du format de l'identificateur *F*, du secret partagé *K*, de la fonction de hachage *H*, du temps de la synchronisation exact pour démarrer l'horodate *t*, du moment où la quantité hachée peut être ajoutée au paquet *P* et de la manière de procéder, de la valeur de d et du démarrage de la resynchronisation de *i*.

L'utilisation de ce mécanisme relève de la politique de sécurité de l'opérateur du réseau. D'autres mécanismes peuvent être utilisés pour l'authentification des flux, par exemple le mécanisme IPsec. Alors qu'IPsec nécessite le chiffrement du paquet IP entier (dans le mode de tunnellisation) ou de la charge utile (dans le mode de transport), le présent mécanisme exige seulement le calcul de la fonction de hachage *H(F, t+i, K)*, qui peut être effectué plus rapidement et avec moins de ressources de calcul.

9 Sécurité du transport pour le trafic de signalisation et OAMP

Le mécanisme de sécurité du transport est utilisé dans l'infrastructure NGN pour garantir la confidentialité et l'intégrité des données de signalisation et des messages OAMP. La présente section a pour objet de spécifier le profil des protocoles TLS et IPsec devant être utilisés par les éléments de réseau d'infrastructure NGN comme deux mécanismes de sécurité importants. La liste des mécanismes utilisés n'est pas exhaustive, d'autres implémentations pouvant être adoptées en fonction de la politique du fournisseur de réseau NGN.

Dans la zone de confiance et la zone de confiance mais vulnérable, le tunnel de réseau VPN (par exemple, IPsec ou TLS) est nécessaire pour sécuriser les messages OAMP. Le § 9.1 présente le profil des cas d'utilisation du mécanisme TLS et le § 9.2 le profil correspondant pour les cas d'utilisation du mécanisme IPsec. Entre l'élément TE-BE et l'élément OAMP-NBE (c'est-à-dire entre la zone de confiance et la zone de confiance mais vulnérable), le mécanisme IPsec est utilisé pour la création d'un tunnel VPN. Le § 9.3 indique le profil applicable au mécanisme IPsec.

Alors que la sécurité des médias n'est pas requise au sein de l'infrastructure des réseaux NGN, certains éléments en limite mettent en œuvre la sécurité des médias pour desservir des points d'extrémité spécifiques. Pour ces éléments, le profil applicable aux protocoles de sécurité des médias est présenté dans la section 10.

9.1 Protocole TLS

Dans l'infrastructure NGN, le protocole TLS est souvent utilisé pour sécuriser divers types de trafic de signalisation (par exemple, SIP, COPS, TRIP ou HTTP) entre éléments de réseau situés dans la zone de confiance. Il est également pris en charge par les éléments en limite susceptibles de

recevoir des données de signalisation chiffrées des points d'extrémité des clients, et par l'élément TE-BE pour la communication avec un élément NBE. Les spécifications propres à chaque type d'élément de réseau sont énoncées dans la Recommandation [UIT-T Y.2701].

Le protocole TLS est défini dans [b-IETF RFC 5246]. Il assure la confidentialité et l'intégrité des données via un protocole de couche de transport fiable, tel que TCP ou SCTP.

Sauf indication contraire dans le présent paragraphe, il est souhaitable que les éléments de réseau d'infrastructure NGN exigeant le protocole TLS soient conformes à la norme TLS [b-IETF RFC 5246] et aux spécifications de la norme [b-IETF RFC 3261] relatives à une utilisation dans le protocole SIP. Même si le protocole TLS prend en charge la négociation et l'utilisation de méthodes de compression, la compression ne peut pas être utilisée dans l'infrastructure NGN en raison de la dégradation de la performance.

9.1.1 Systèmes cryptographiques

Un système cryptographique combine la méthode d'agrément de clé authentifiée utilisée dans la prise de contact TLS, et les algorithmes de chiffrement et d'authentification utilisés pour sécuriser la couche basse (*record layer*). Les systèmes cryptographiques sont négociés de la façon suivante: le client TLS présente dans le message "Client Hello" une liste de systèmes cryptographiques pris en charge, et le serveur y répond en indiquant dans le message "Server Hello" le système cryptographique retenu.

De nombreux facteurs influent sur le choix de l'algorithme de chiffrement. On trouvera ci-après des exemples des facteurs les plus courants:

1) Exigence en termes de sécurité
   - Valeur des données (pour l'organisation et/ou pour d'autres entités – plus la valeur des données est élevée, plus le chiffrement exigé est fort).
   - Valeur temporelle des données (si les données sont de valeur, mais seulement pendant une courte période (par exemple en termes de jours et non en termes d'années), il est possible d'utiliser un algorithme de chiffrement plus faible).
   - Menace envers les données (plus le niveau de menace est élevé, plus le chiffrement requis est fort).
   - Autres mesures de protection qui sont en place et qui peuvent éviter de recourir à un chiffrement plus fort – par exemple, au moyen de méthodes de protection des communications, telles que l'utilisation de circuits spécialisés par opposition à l'Internet public.
2) Exigence en termes de performance (des exigences de performance plus élevées peuvent nécessiter le recours à des ressources système supplémentaires, telles qu'un accélérateur cryptographique matériel, ou un chiffrement plus faible).
3) Ressources système (un nombre plus faible de ressources (par exemple, pour le traitement, la mémoire, etc.) peut nécessiter un chiffrement plus faible).
4) Restrictions relatives à l'importation, à l'exportation ou à l'utilisation.
5) Systèmes de chiffrement pris en charge par les éléments de réseau.
6) Systèmes de chiffrement pris en charge par les dispositifs d'utilisateur.

Le Tableau 3 contient une liste de systèmes cryptographiques pouvant être utilisés dans un réseau NGN (la liste n'est pas exhaustive).

Tableau 3 – Systèmes cryptographiques possibles dans un réseau NGN

Nom du système cryptographique	Référence	Echange de clés	Algorithme de chiffrement	Algorithme de hachage
TLS_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	RSA	AES-128 en mode CBC	SHA-1
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	b-IETF RFC 5246	Mode éphémère Diffie-Hellman avec signatures RSA	AES-128 en mode CBC	SHA-1
TLS_RSA_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 2246]	RSA	3DES en mode CBC	SHA-1
TLS_DHE_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 5246]	Mode éphémère Diffie-Hellman avec signatures RSA	3DES en mode CBC	SHA-1
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	[b-IETF RFC 4132]	RSA	Camellia-128 en mode CBC	SHA-1
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	[b-IETF RFC 4132]	Mode éphémère Diffie-Hellman avec signatures RSA	Camellia-128 en mode CBC	SHA-1

Les systèmes cryptographiques du Tableau 4, décrits dans [b-IETF RFC 5246], [b-IETF RFC 4132] et [b-IETF RFC 4492], peuvent également être utilisés à titre facultatif par des éléments de réseau quelconques.

Tableau 4 – Systèmes cryptographiques possibles (facultatifs) dans un réseau NGN

Nom du système cryptographique	Référence	Echange de clés	Algorithme de chiffrement	Algorithme de hachage
TLS_DH_DSS_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	Diffie-Hellman avec signature DSS	AES-128 en mode CBC	SHA-1
TLS_DH_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	Diffie-Hellman avec signature RSA	AES-128 en mode CBC	SHA-1
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	Mode éphémère Diffie-Hellman avec signature DSS	AES-128 en mode CBC	SHA-1
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	Mode éphémère Diffie-Hellman avec signature RSA	AES-128 en mode CBC	SHA-1
TLS_RSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 5246]	RSA	AES-256 en mode CBC	SHA-1
TLS_DH_DSS_WITH_AES_256_CBC_SHA	[b-IETF RFC 5246]	Diffie-Hellman avec signature DSS	AES-256 en mode CBC	SHA-1
TLS_DH_RSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 5246]	Diffie-Hellman avec signature RSA	AES-256 en mode CBC	SHA-1
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	[b-IETF RFC 5246]	Mode éphémère Diffie-Hellman avec signature DSS	AES-256 en mode CBC	SHA-1
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 4132]	Mode éphémère Diffie-Hellman avec signatures RSA	AES-256 en mode CBC	SHA-1

Tableau 4 – Systèmes cryptographiques possibles (facultatifs) dans un réseau NGN

Nom du système cryptographique	Référence	Echange de clés	Algorithme de chiffrement	Algorithme de hachage
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	[b-IETF RFC 4132]	Diffie-Hellman avec signature DSS	Camelia-128 en mode CBC	SHA-1
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	[b-IETF RFC 4132]	Diffie-Hellman avec signature RSA	Camelia-128 en mode CBC	SHA-1
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	[b-IETF RFC 4132]	Mode éphémère Diffie-Hellman avec signature DSS	Camelia-128 en mode CBC	SHA-1
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	[b-IETF RFC 4132]	RSA	Camelia-256 en mode CBC	SHA-1
TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	[b-IETF RFC 4132]	Diffie-Hellman avec signature DSS	Camelia-256 en mode CBC	SHA-1
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	[b-IETF RFC 4132]	Diffie-Hellman avec signature RSA	Camelia-256 en mode CBC	SHA-1
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	[b-IETF RFC 4132]	Mode éphémère Diffie-Hellman avec signature DSS	Camelia-256 en mode CBC	SHA-1
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	[b-IETF RFC 4132]	Mode éphémère Diffie-Hellman avec signatures RSA	Camelia -256 en mode CBC	SHA-1
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 4492]	EC-Diffie-Hellman avec signature ECDSA	3DES en mode CBC	SHA-1
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 4492]	EC-Diffie-Hellman avec signature ECDSA	AES-128 en mode CBC	SHA-1
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 4492]	EC-Diffie-Hellman avec signature ECDSA	AES-256 en mode CBC	SHA-1
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 4492]	Mode éphémère EC-Diffie-Hellman avec signature ECDSA	3DES en mode CBC	SHA-1
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 4492]	Mode éphémère EC-Diffie-Hellman avec signature ECDSA	AES-128 en mode CBC	SHA-1
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 4492]	Mode éphémère EC-Diffie-Hellman avec signature ECDSA	AES-256 en mode CBC	SHA-1
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 4492]	EC-Diffie-Hellman avec signature RSA	3DES en mode CBC	SHA-1
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 4492]	EC-Diffie-Hellman avec signature RSA	AES-128 en mode CBC	SHA-1

Tableau 4 – Systèmes cryptographiques possibles (facultatifs) dans un réseau NGN

Nom du système cryptographique	Référence	Echange de clés	Algorithme de chiffrement	Algorithme de hachage
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 4492]	EC-Diffie-Hellman avec signature RSA	AES-256 en mode CBC	SHA-1
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 4492]	Mode éphémère EC-Diffie-Hellman avec signature RSA	3DES en mode CBC	SHA-1
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 4492]	Mode éphémère EC-Diffie-Hellman avec signature RSA	AES-128 en mode CBC	SHA-1
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 4492]	Mode éphémère EC-Diffie-Hellman avec signature RSA	AES-256 en CBC mode	SHA-1

NOTE 1 – RC-4 est un algorithme de chiffrement très apprécié et répandu, mais il ne figure pas dans la liste ci-dessus, car il ne s'agit pas d'une norme ouverte.

NOTE 2 – Le système cryptographique à courbe elliptique (ECC, *elliptic curve crytosystem*) est un système cryptographique à clé publique qui peut être souhaitable pour certaines applications de réseau NGN. Il pourrait en particulier présenter dans certains cas des avantages en termes d'efficacité. Comparé à d'autres systèmes cryptographiques courants, tels que l'algorithme RSA, l'ECC offre une sécurité équivalente pour des tailles de clé sensiblement plus petites. En outre, l'ECC offre des avantages et une efficacité en termes de calcul par rapport à certaines autres techniques de clé publique avec le même niveau de protection.

9.1.2 Utilisation de certificats TLS

TLS est un protocole client-serveur avec authentification facultative du client. Toutefois, dans la zone de confiance de l'infrastructure NGN, et entre la zone de confiance et la zone de confiance mais vulnérable, une authentification mutuelle peut être effectuée au moyen de ce protocole. Dans ce cas, le serveur TLS envoie au client une demande de certificat. Si un client situé dans le zone de confiance ou la zone de confiance mais vulnérable ne fournit pas un certificat de client, la demande de connexion peut être rejetée par le serveur. Les certificats de client et de serveur TLS devraient tous les deux se conformer aux spécifications de certification d'infrastructure NGN énoncées dans le § 8.3. La vérification des certificats peut être effectuée suivant les spécifications de ce paragraphe. Avant d'établir une connexion TLS, le serveur ou le client TLS peut valider le système distant qui correspond à son certificat.

Entre la zone de confiance mais vulnérable et la zone non fiable, le serveur TLS peut envoyer au client une demande de certificat. S'il ne possède pas de certificat, le client répond par un message vide de certificat de client et la session est établie en tant que client anonyme.

Lorsqu'un élément NBE accepte une connexion authentifiée avec un point d'extrémité sur la base d'un certificat d'utilisateur final NGN (voir le § 8.5.2), il peut appliquer deux temporisateurs à la connexion. Le premier temporisateur, T1, se déclenche à l'établissement de la connexion. Le second temporisateur, T2, se déclenche à l'établissement de la connexion et remis à zéro chaque fois qu'une demande est reçue par l'élément NBE au cours de la connexion. Lorsque l'un ou l'autre temporisateur atteint sa valeur limite (qui peut dépendre des valeurs indiquées dans le certificat), la connexion est réinitialisée par l'élément NBE et sera établie à nouveau par le point d'extrémité afin de réinitialiser le certificat de l'utilisateur final NGN.

9.1.3 Gestion des clés de session

Les sessions TLS établies entre les différents éléments de réseau d'infrastructure NGN sont censées être de longue durée. Il importe par conséquent de modifier périodiquement les clés de session. On peut modifier les clés de session TLS après une certaine période configurable.

9.2 Utilisation du mécanisme IPsec dans la zone de confiance et dans la zone de confiance mais vulnérable

Dans l'infrastructure de réseau NGN, le mécanisme IPsec peut être utilisé pour sécuriser divers types de trafic (par exemple, SNMP ou RADIUS) entre divers éléments de réseau situés dans la zone de confiance. Des spécifications propres à chaque type d'élément de réseau sont énoncées dans [ITU-T Y.2701].

Comme il est décrit de manière générale dans [b-IETF RFC 4301], IPsec est composé d'un certain nombre d'éléments différents. Ces éléments peuvent être utilisés pour assurer la confidentialité, l'intégrité ou la protection contre les répétitions. Certains de ces éléments peuvent être configurés manuellement, mais un élément de gestion de clé sera généralement utilisé. En outre, la décision concernant l'utilisation du mécanisme IPsec est en principe contrôlée par une base de données de politique. Le présent paragraphe a pour objet de décrire le sous-ensemble d'éléments IPsec dont la mise en œuvre est obligatoire.

Dans les éléments de réseau qui utilisent le mécanisme IPsec, il est recommandé de s'assurer que les connexions sécurisées par le protocole TLS ne sont pas exécutées via IPsec.

NOTE – Les éléments de réseau utilisant IPsec devraient s'assurer que les flux de médias sécurisés par le protocole SRTP ou RC-4 ne sont pas exécutés via IPsec. Il s'agit d'éviter un double chiffrement et, ainsi, un gaspillage des ressources NGN. Il convient également de noter qu'une tunnellisation du chiffrement peut se produire depuis l'utilisateur final.

9.2.1 En-tête d'authentification et protocole de sécurité d'encapsulation

L'en-tête d'authentification (AH, *authentification header*), décrit dans [IETF RFC 4302] et [b-IETF RFC 4835] et le protocole de sécurité d'encapsulation (ESP, *encapsulating security protocol*), décrit dans [IETF RFC 4303], sont les deux types possibles de protocole de sécurité en mode filaire. Les deux assurent facultativement la protection contre les répétitions. Le protocole ESP est utilisé généralement pour assurer la confidentialité, l'intégrité et l'authentification du trafic. Il peut également assurer l'intégrité et l'authentification sans la confidentialité, ou seulement la confidentialité. Le protocole AH protège des parties de l'en-tête IP précédent, notamment les adresses d'origine et de destination. Il peut aussi protéger les options IP qui doivent traverser des routeurs intermédiaires mais qui doivent rester intactes et authentiques lorsqu'elles sont remises au système de réception. Cela étant, l'utilisation de ces options IP est extrêmement rare.

Des éléments de réseau d'infrastructure NGN peuvent prendre en charge le protocole ESP, comme défini dans [IETF RFC 4303]. Les champs ESP_DES (40 et 56 bits), ESP_3DES, ESP_AES [b-IETF RFC 3602] et ESP_CAMELLIA [b-IETF RFC 4312] peuvent être pris en charge dans le mode d'enchaînement de blocs chiffrés (CBC, *cipher block chaining*). Les éléments de réseau qui prennent en charge le champ ESP_NULL NE peuvent PAS utiliser ce champ lorsqu'ils communiquent avec un autre élément de réseau d'infrastructure NGN. L'algorithme de chiffrement réel utilisé dans le protocole ESP est négocié lors de la gestion des clés.

Toutes les implémentations du protocole ESP sont requises par [b-IETF RFC 4301] pour pouvoir prendre en charge le concept d'associations de sécurité (SA, *security associations*), et [b-IETF RFC 4301] spécifie un modèle général pour le traitement du trafic IP se rapportant aux associations de sécurité. Même si des implémentations IPsec particulières ne doivent pas nécessairement être conformes en tout point à ce modèle générique, le comportement extérieur de toute implémentation IPsec peut correspondre au comportement extérieur du modèle général. Cela garantit que les éléments n'acceptent pas de trafic en provenance d'adresses inconnues et n'envoient pas ou

n'acceptent pas de trafic non sécurisé (lorsqu'une sécurité est nécessaire). Les éléments de réseau d'infrastructure NGN qui implémentent IPsec peuvent présenter un comportement qui corresponde au modèle général décrit dans [b-IETF RFC 4301].

9.2.2 Mode transport ou tunnel

Les protocoles AH et ESP peuvent tous les deux être utilisés soit dans le mode transport soit dans le mode tunnel. Dans le mode tunnel, l'en-tête IPsec est suivi d'un en-ête IP interne. Il s'agit de l'utilisation normale pour les réseaux privés virtuels (VPN, *virtual private nteworks*), et cela est généralement nécessaire lorsque l'une ou l'autre extrémité du trajet protégé par IPsec n'est pas le point de destination final (par exemple, lorsque IPsec est implémenté dans un pare-feu ou un routeur). Le mode transport est préféré pour les communications point à point.

Les éléments de réseau d'infrastructure NGN peuvent prendre en charge IPsec dans le mode transport.

9.2.3 Protection contre les reproductions

Les éléments de réseau d'infrastructure NGN peuvent utiliser le service facultatif IPsec de protection contre les reproductions (service antireproductions). Ce service peut être activé à tout moment dans ces éléments. Un numéro de séquence IPsec situé en dehors de la fenêtre de protection contre les reproductions est marqué comme une reproduction et le paquet est rejeté. Lorsque le service antireproductions est activé, un numéro de séquence IPsec ne peut pas déborder et revenir à 0. Une nouvelle association de sécurité doit préalablement être créée, comme spécifié dans [IETF RFC 4303].

9.2.4 Gestion des clés

Tous les systèmes cryptographiques requièrent une gestion des clés. Même si IPsec offre des systèmes de gestion de clés manuels et automatiques, les systèmes manuels ne sont pas aussi adaptables que les systèmes automatiques et n'offrent pas une protection contre les reproductions. Tous les systèmes de gestion de clés assurent l'authentification. Les éléments de réseau d'infrastructure NGN devraient implémenter l'un des mécanismes automatiques d'échange de clés décrits dans le présent paragraphe.

Lorsque l'échange IKE n'est pas utilisé pour la gestion de clés, un autre protocole de gestion de clés disposant d'une interface avec la couche IPsec est alors nécessaire pour la création, la mise à jour ou la suppression d'associations de sécurité IPsec. Les associations de sécurité IPsec peuvent être établies ou rétablies automatiquement si nécessaire. Cela suppose que la couche IPsec dispose également d'un moyen de signaler une application de gestion de clés lorsqu'il faut établir une nouvelle association de sécurité (par exemple, lorsque l'ancienne association est sur le point d'expirer ou s'il n'en existe encore aucune sur une interface particulière). En outre, il peut être nécessaire pour certains éléments en limite d'exécuter plusieurs protocoles de gestion de clés (par exemple, IKE pour sécuriser les connexions OAMP et PKINIT). En pareils cas, il est recommandé d'utiliser l'interface PF_KEY [b-IETF RFC 2367].

9.2.4.1 Identificateurs de transformation

L'identificateur de transformation IPsec est utilisé dans le cadre des procédures de gestion de clés pour négocier un algorithme de chiffrement utilisé par le protocole ESP dans IPsec. Il est aussi utilisé aussi par le protocole IKE pour sécuriser ses messages en phase 1 et en phase 2. [b-IETF RFC 5282] présente une liste des identificateurs de transformation IPsec disponibles. Dans l'infrastructure de réseau NGN, la transformation IDs ESP_3DES (valeur 0x03, avec taille de clé de 192 bits, mode CBC) et ESP_CAMELLIA (valeur 0x16, avec clé codée sur 128 bits, mode CBC) [b-IETF RFC 4312] peut être prise en charge. Il est recommandé de prendre en charge la transformation ID ESP_AES (valeur 0x0C, avec clé codée sur 128, mode CBC). Le protocole IKE permet de négocier la taille de clé de chiffrement. Ainsi, pour augmenter la taille de clé pour l'un des algorithmes ci-dessus, le protocole IKE utilisera cette fonction intégrée.

Pour l'ensemble de ces transformations, le vecteur d'initialisation CBC (IV) est acheminé en clair à l'intérieur de la charge utile de chaque paquet ESP [b-IETF RFC 2451]. L'algorithme AES-128, défini dans [b-NIST FIPS 197] et [b-IETF RFC 3602] peut être utilisé dans le mode CBC avec une taille de bloc de 128 bits et un vecteur d'initialisation généré de façon aléatoire. L'algorithme AES-128 nécessite 10 tours d'opérations cryptographiques [b-IETF RFC 3602]. L'algorithme Camellia-128, défini dans [b-IETF RFC 3713] et [b-IETF RFC 4312] peut être utilisé en mode CBC avec une taille de bloc de 128 bits et un vecteur d'initialisation généré de façon aléatoire. Il nécessite 18 tours d'opérations cryptographiques [b-IETF RFC 3713]

9.2.4.2 Algorithmes d'authentification

L'algorithme d'authentification IPsec est utilisé dans le cadre des procédures de gestion de clés pour négocier un algorithme d'authentification de paquets. [b-IETF RFC 5282] présente une liste d'algorithmes d'authentification IPsec disponibles. Dans l'infrastructure de réseau NGN, les algorithmes d'authentification HMAC-MD5-96 (valeur 0x01, taille de clé de 128 bits, définis dans [b-IETF RFC 2403]) et HMAC-SHA-1-96 (valeur 0x02, taille de clé de 160 bits, définis dans [b-IETF RFC 4835]) peuvent être pris en charge.

9.2.4.3 Echange de clés Internet (IKE)

L'échange de clés Internet (IKE, *Internet key exchange*) est un mécanisme d'échange de clés automatisé, qui est spécifié par la norme [b-IETF RFC 2409]. La gestion de clé IKE est totalement asynchrone par rapport aux messages de données et n'introduit aucun retard dans l'établissement des communications. A titre exceptionnel, une erreur peut survenir lorsque l'un des points d'extrémité perd de manière inattendue l'association de sécurité.

L'échange IKE est un protocole de gestion de clés entre entités homologues qui consiste en deux phases. Dans la première phase, un secret partagé est négocié au moyen d'un échange de clés Diffie-Hellman. Ce secret est ensuite utilisé pour authentifier la seconde phase durant laquelle est négocié un autre secret, utilisé pour calculer les clés applicables au protocole ESP IPsec.

9.2.4.3.1 Première phase de l'échange IKE

Trois modes différents sont définis pour l'authentification durant la première phase de l'échange IKE. L'authentification IKE avec chiffrement de clé publique NE DOIT PAS être utilisé dans l'infrastructure NGN, car cela oblige l'expéditeur à connaître déjà la clé publique du récepteur. L'authentification IKE avec signatures et l'authentification IKE avec clés prépartagées peuvent être prises en charge.

L'IKE définit des ensembles spécifiques de paramètres Diffie-Hellman (à savoir, des nombres premiers et des générateurs) pouvant être utilisés dans la première phase de l'échange. Le premier groupe peut être pris en charge dans certains éléments de réseau d'infrastructure NGN, et il est recommandé de prendre en charge les groupes restants.

En cas d'utilisation de l'authentification IKE avec signatures, le client et le serveur peuvent échanger des certificats X.509 (voir le § 8.3.2). Les certificats peuvent être vérifiés comme spécifié dans le § 8.3.

Lorsqu'un élément en limite de réseau accepte une connexion authentifiée avec un point d'extrémité sur la base d'un certificat d'utilisateur final de réseau NGN), l'élément NBE peut implémenter deux temporisateurs sur la connexion. Le premier temporisateur, T1, est déclenché à l'établissement de la connexion. Le second, T2, est déclenché à l'établissement de la connexion et est remis à zéro chaque fois qu'une demande est reçue par l'élément NBE au cours de la connexion. Lorsque l'un ou l'autre temporisateur atteint sa valeur limite (qui peut dépendre des valeurs figurant dans le certificat), la connexion est réinitialisée par l'élément NBE et sera rétablie par le point d'extrémité de manière à réinitialiser le certificat d'utilisateur final NGN.

Dans le cas d'une authentification IKE au moyen de clés prépartagées, une clé fournie par un certain mécanisme hors bande (manuel, par exemple) est utilisée pour authentifier l'échange. Les implémentations peuvent permettre l'utilisation d'une clé prépartagée d'au moins 128 octets. La vérification des spécifications relatives aux clés prépartagées n'est pas nécessaire dans les éléments de réseau. Les implémentations peuvent prendre en charge le mode agressif, défini au paragraphe 5.4 de [b-IETF RFC 2409], et utiliser le nom de la clé comme identité de l'initiateur/du répondeur. On sait que l'utilisation conjointe du mode agressif de l'authentification IKE v1 [b-IETF RFC 2409] et d'une clé prépartagée n'est pas sans risque. En effet, en mode agressif, une valeur de hachage du secret est transmise en clair dans le réseau; si le trafic IP est intercepté par un intrus, la clé peut alors être retrouvée avec une attaque en force hors ligne. Il est recommandé d'utiliser une clé prépartagée d'une longueur minimale de 128 bits afin d'éviter un calcul exhaustif de celle-ci à partir de sa valeur de hachage.

En cas d'utilisation de clés prépartagées, la force du système dépend de la force du secret partagé. L'objectif est d'empêcher que le secret partagé soit le maillon faible de la chaîne de sécurité. Cela suppose que son entropie (caractère aléatoire) soit aussi élevée que celle du chiffre utilisé. En d'autres termes, il est recommandé que le secret partagé possède au moins 128-160 bits d'entropie.

9.2.4.3.2 Seconde phase de l'échange IKE

Une association de sécurité ESP IPsec est établie pendant la seconde phase de l'échange IKE, qui comprend les clés et les suites de chiffrement ESP. Un secret partagé de seconde phase est établi, après quoi toutes les informations de clé IPsec sont générées à partir de ce secret au moyen de la fonction irréversible spécifiée dans [b-IETF RFC 2409]. Le secret de seconde phase est établi à partir de justificatifs temporaires chiffrés qui sont échangés par les deux parties. Un autre échange Diffie-Hellman est autorisé par la norme [b-IETF RFC 2409] en plus des justificatifs temporaires chiffrés, mais ne peut pas être utilisé dans les éléments de réseau d'infrastructure NGN, ceci afin d'éviter les altérations de qualité associées.

9.3 Protocole de concordance de clés entre la zone non fiable et la zone de confiance mais vulnérable

Le protocole de concordance de clés (AKA, *authentication and key agreement*) spécifié pour le réseau IMS peut également être utilisé selon le cas. Le protocole AKA du système de télécommunications mobiles universelles (UMTS, *universal mobile telecommunications system*) assure l'authentification mutuelle de la station mobile et du réseau. Il s'agit d'un protocole de type question réponse qui utilise une clé *K* à long terme partagée entre le module d'identité d'abonné universel (USIM, *universal subscriber identity module*) et le centre d'authentification (AuC, *authentication center*). Ces entités reposent respectivement sur la carte de circuits intégrés universelle (UICC, *universal integrated circuit card*) de la station mobile et sur le réseau domestique de la station mobile. Le protocole AKA est spécifié dans [b-3GPP TS 33.102].

Même si le mécanisme AKA est généralement utilisé pour l'authentification de dispositifs hertziens équipés de cartes intelligentes (par exemple, UICC), rien n'empêche dans les spécifications AKA d'utiliser ce mécanisme pour l'authentification des dispositifs fixes capables d'exécuter l'application USIM.

9.4 Sécurité IPsec entre la zone non fiable et la zone de confiance mais vulnérable

L'élément TE-BE est un élément de réseau NGN situé dans la zone non fiable. Toutefois, il est toujours géré par l'opérateur NGN et doit accéder aux systèmes OAMP situés dans la zone de confiance. Par conséquent une entité OAMP-SE, située dans la zone de confiance mais vulnérable, sert de point de relais pour les messages OAMP.

L'élément TE-BE permet de garantir que les connexions sécurisées par TLS, de même que les flux de média sécurisés à l'aide de la sécurité de média SRTP, ne sont pas exécutées dans le tunnel VPN IPsec.

Le tunnel VPN IPsec peut utiliser le protocole ESP IPsec [IETF RFC 4303] en mode tunnel [b-IETF RFC 4301].

Le service de protection contre les reproductions IPsec peut être activé à tout moment.

Le tunnel VPN IPsec peut prendre en charge les identificateurs de transformation ESP_3DES (avec taille de clé de 192 bits, en mode CBC) et ESP_CAMELLIA (avec clé codée sur 128 bits et mode CBC) [b-IETF RFC 4312]. Il est recommandé que le tunnel VPN IPsec prenne en charge l'identificateur de transformation ESP_AES (avec clé codée sur 128 bits et mode CBC).

Le tunnel VPN IPsec peut prendre en charge les algorithmes d'authentification HMAC-MD5-96 (taille de clé de 128 bits), et HMAC-SHA-1-96 (taille de clé de 160 bits).

La génération et la gestion de clé pour le tunnel VPN IPsec peuvent être effectuées au moyen du protocole IKE [b-IETF RFC 2409], en utilisant une authentification d'échange IKE avec signatures numériques ou une authentification IKE avec une clé prépartagée. En cas d'utilisation de l'authentification d'échange IKE avec signatures numériques, le client comme le serveur peuvent échanger des certificats X.509, lesquels peuvent être vérifiés.

10 Sécurités des médias

Le chiffrement de média n'est pas requis dans l'infrastructure de réseau NGN, mais sa prise en charge peut être nécessaire pour les clients qui souhaitent l'utiliser, ce qui supposera peut-être la prise en charge du protocole de chiffrement de média SRTP [b-IETF RFC 3711]. Dans la présente section, on part du principe que les éléments en limite de réseau (c'est-à-dire la limite du domaine du fournisseur de réseau) effectuent le chiffrement/déchiffrement même si cette action est également possible à partir d'une plate-forme distincte partagée entre plusieurs éléments NBE. Dans les deux cas, les fonctions de chiffrement et de déchiffrement doivent être situées au même endroit que les autres fonctionnalités de traitement de média, telles que la détection et le transcodage multifréquence bitonalité (DTMF, *dual-tone multi-frequency*).

Compte tenu de l'exigence de connecter les abonnés souhaitant le chiffrement de média sur leur liaison d'accès avec ceux qui ne le souhaitent pas (ou qui ne prennent pas en charge cette fonction), cinq cas distincts doivent être pris en considération, comme le montre la Figure 4.

Le premier cas, qui est le plus simple, est celui dans lequel aucun des points d'extrémité ne souhaite le chiffrement. Le média sera acheminé de la source à la destination, par l'intermédiaire des éléments en limite, sans qu'il soit procédé à un chiffrement sur aucune des liaisons. Ni l'élément en bordure de réseau (NBE) #1 (desservant l'expéditeur), ni l'élément en limite de réseau (NBE) #2 (desservant le destinataire) n'effectue un chiffrement ou un déchiffrement.

Le deuxième cas est celui dans lequel l'expéditeur souhaite un flux de média chiffré, mais pas le destinataire: l'élément NBE #1 agit comme un point de relais de chiffrement/déchiffrement. L'élément NBE #1 reçoit le flux chiffré de l'expéditeur, le déchiffre et le transmet, via l'infrastructure NGN, à l'élément NBE #2, lequel le transmet (toujours non chiffré) au destinataire. Dans le sens inverse, l'élément NBE #1 reçoit le média non chiffré via l'infrastructure NGN et le chiffre avant de l'envoyer à l'expéditeur. Ainsi, le média sur le tronçon leg#1 (entre l'expéditeur et l'élément NBE #1) est chiffré, alors que les médias sur les tronçons leg#2 (entre l'élément NBE #1 et l'élément NBE #2) et le tronçon leg#3 (entre l'élément NBE #2 et le destinataire) ne le sont pas.

Dans le troisième cas, le destinataire souhaite un flux de média chiffré mais pas l'expéditeur. L'élément NBE #2 agit comme un point de relais de chiffrement/déchiffrement. L'élément NBE #1 reçoit le média non chiffré de l'expéditeur et le transmet (toujours non chiffré) à l'élément NBE #2 via l'infrastructure NGN. L'élément NBE #2 le chiffre et le transmet au destinataire. Dans le sens inverse, l'élément NBE #2 reçoit le flux de média chiffré du point d'extrémité de destination et le déchiffre avant de le retransmettre via l'infrastructure NGN. L'élément NBE #1 transmet le média

non chiffré à l'expéditeur. Ainsi, les médias sur les tronçons #1 et #2 ne sont pas chiffrés, alors que le média sur le tronçon #3 est chiffré.

Dans le quatrième cas, l'expéditeur et le destinataire souhaitent tous les deux un média chiffré, mais ni l'un ni l'autre ne prennent en charge des mécanismes de chiffrement compatibles, ou l'infrastructure NGN offre un certain type de service évolué (tel qu'un système de détection par multifréquence bitonalité (DTMF) pour applications de carte d'appel). Les éléments NBE #1 et NBE #2 agissent tous les deux comme des points de relais de chiffrement/déchiffrement. L'élément NBE #1 reçoit le flux chiffré de l'expéditeur, le déchiffre et le transmet à l'élément NBE #2 via l'infrastructure NGN. L'élément NBE #2 le chiffre et le transmet au destinataire. Dans le sens inverse, l'élément NBE #2 reçoit le média chiffré du point d'extrémité de destination et le déchiffre avant de le retransmettre via l'infrastructure NGN. L'élément NBE #1 reçoit le média non chiffré et le chiffre avant de l'envoyer à l'expéditeur. Ainsi, les médias sur les tronçons #1 et #3 sont chiffrés, alors que le média transmis via l'infrastructure NGN (tronçon #2) ne l'est pas.

Dans le cinquième cas, l'expéditeur et le destinataire souhaitent tous les deux un média chiffré, prennent en charge des mécanismes de chiffrement compatibles, sans que l'infrastructure NGN n'offre de service évolué. L'élément NBE #1 reçoit le média chiffré de l'expéditeur et le transmet, via l'infrastructure NGN, à l'élément NBE #2, lequel le transmet inchangé au destinataire. Dans le sens inverse, l'élément NBE #2 reçoit le média chiffré du destinataire et le transmet inchangé via l'infrastructure NGN à l'élément NBE #1, qui le transmet inchangé à l'expéditeur. Ainsi, le média est chiffré sur les trois tronçons. La signalisation nécessaire dans cette configuration sort du cadre de la présente Recommandation.

Le chiffrement de média décrit dans la présente section assure l'authentification, la confidentialité et l'intégrité des messages.

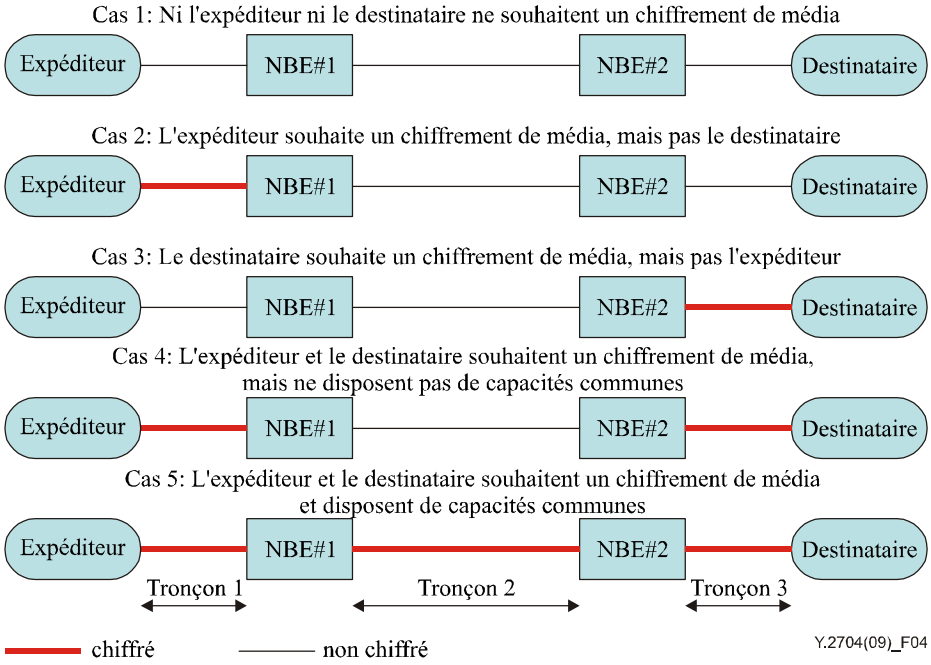


Figure 4 – Rapport entre le chiffrement de média, les capacités des éléments en limite et le souhait de l'expéditeur/du destinataire

10.1 Protocole SRTP

Le protocole de transport réel sécurisé (SRTP, *secure real time protocol*), décrit dans la norme [b-IETF RFC 3711], est défini comme étant un profil du protocole RTP [b-IETF RFC 3550]. Il est destiné à être implémenté entre l'application RTP et la couche transport dans la pile de protocoles (interception d'un paquet RTP et transmission d'un paquet SRTP équivalent du côté émission et

interception du paquet SRTP et transmission d'un paquet RTP équivalent au-dessus de la pile du côté réception). Il permet essentiellement de chiffrer la charge utile du paquet RTP et d'ajouter une étiquette d'authentification à la fin du paquet du côté émission, puis de vérifier cette étiquette et de déchiffrer la charge utile du côté réception.

10.1.1 Algorithmes de chiffrement et d'authentification

Un élément NBE utilisant le protocole SRTP peut prendre en charge le chiffrement AES en mode compteur [b-IETF RFC 3711]. Pour de plus amples informations, se reporter également à la norme [b-NIST FIPS SP 800-38a]. L'élément NBE peut prendre en charge l'algorithme HMAC-SHA1 pour générer la vérification de l'intégrité des messages, avec une longueur d'étiquette de 80 bits.

10.1.2 Négociation de suites chiffrantes et génération de clés

En mode SRTP, la génération de clés peut s'effectuer de plusieurs façons:

1) par approvisionnement (via l'élément d'approvisionnement d'équipement terminal);

2) par l'utilisation des informations de clé générées par le dispositif de point d'extrémité et prises en charge par le protocole de description de session (SDP, *session description protocol*) [b-IETF RFC 4566] dans les demandes INVITE;

3) par l'échange des informations de clé au moyen d'un protocole distinct de gestion de clés et par leur superposition au moyen du protocole SDP.

Pour chaque abonné, l'élément NBE peut obtenir des entités fonctionnelles SAA/TAA la clé maître SRTP, à partir de laquelle seront calculées les clés de session préliminaires de chiffrement et d'authentification. Une clé maître SRTP d'une longueur de 128 bits peut être prise en charge. L'algorithme de calcul de clé décrit dans la norme [b-IETF RFC 3711] peut être pris en charge. La clé de chiffrement préliminaire peut être codée sur 128 bits, la clé "sel" de session préliminaire sur 112 bits et la clé d'authentification préliminaire sur 160 bits. Lorsqu'une nouvelle clé maître SRTP est créée pour un abonné, l'élément NBE est en mesure de l'utiliser immédiatement.

Si le message SDP contenu dans la demande INVITE présente "RTP/SAVP" comme valeur de protocole de média dans la ligne "m=", sans valeur de clé dans une ligne "k="et sans attribut "a=crypto", alors l'élément NBE peut utiliser les clés préliminaires générées par le système d'approvisionnement comme les clés réelles pour la session considérée. La suite chiffrante n'est pas négociable dans ce cas.

Si le message SDP contenu dans la demande INVITE présente "RTP/SAVP" comme valeur de protocole de média dans la ligne "m=", sans attribut "a=crypto" et avec une valeur de clé dans une ligne " k= ", alors l'élément NBE peut utiliser la clé contenue dans la ligne " k= " comme la clé maître SRTP, et générer, à partir de cette clé, les clés de session et d'authentification. La suite chiffrante n'est pas négociable dans ce cas.

Si le message SDP contenu dans la demande INVITE présente "RTP/SAVP" comme valeur de protocole de média dans la ligne "m=", avec un attribut "a=crypto", alors l'élément NBE peut appliquer les spécifications de la norme [b-IETF RFC 4568] pour générer les clés de session et d'authentification. Par exemple, l'entrée de message SDP "a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline: PS1uQCVeeCFCanVmcjkpPywjNWhcYD0mXXtxaVBR|2^20|1:4" indique que la suite chiffrante est AES_CM_128_HMAC_SHA1_80, et le paramètre key_param est défini par le texte commençant par "inline:". Dans le paramètre key_param, le premier champ contient la clé maître jointe au "sel" maître, concaténée puis codée en base 64. On trouvera dans le § 5.2 de la norme [b-IETF RFC 4568] la liste des suites chiffrantes valables, dont l'une est retenue pour l'échange d'offres/de réponses SDP.

Si le message SDP contenu dans la demande INVITE présente "RTP/SAVP" comme valeur de protocole de média dans la ligne "m=", avec un attribut "a=key-mgmt", alors l'élément NBE peut appliquer les spécifications de la norme [b-IETF RFC 4567] pour générer des clés et des paramètres de sécurité. Par exemple, "a=key-mgmt:mikey AQAFgM0XflABAAAAAAAAAAAA ..." indique

que le protocole de gestion de clé est mikey [b-IETF RFC 3830], le texte restant représentant les données de gestion de clé codées en base 64 [b-IETF RFC 4648].

10.1.3 Interface d'authentification entre élément de réseau NGN et serveur de jetons de sécurité

Les éléments de réseau NGN peuvent implémenter la couche SASL [b-IETF RFC 4422] protégeant leurs fonctions OAMP. La couche SASL peut inclure une vérification de l'authentification sur la base d'un jeton de sécurité, comme il est défini dans la norme [b-IETF RFC 2808]. Cette fonction est identifiée par la clé SASL "jeton de sécurité". L'utilisateur souhaitant un accès aux fonctions OAMP fournit:

1) une identité d'autorisation (qui permet aux administrateurs systèmes de se connecter avec une identité d'utilisateur différente; si le champ est vide, le paramètre est positionné par défaut sur la valeur de l'identité d'authentification);
2) une identité d'authentification (une identité dont le mot de passe sera utilisé);
3) la valeur du numéro NIP de l'utilisateur et le mot de passe de 6 chiffres du jeton de sécurité.

L'élément de réseau NGN peut implémenter un client conforme à une entité fonctionnelle SAA/TAA dans le cadre du traitement SASL de jeton de sécurité. L'élément de réseau NGN collecte les justificatifs d'identité d'utilisateur présentés, puis les envoie au serveur de jetons de sécurité. Les champs collectés comprennent le nom d'utilisateur, le code NIP et la valeur du jeton de sécurité actuellement présenté. L'élément de réseau reçoit en retour un message d'état d'acceptation, de refus ou de nouvelle tentative. En cas de réussite, la couche SASL permet à l'utilisateur d'accéder aux fonctions OAMP, sur la base du niveau d'accès associé à ce nom d'utilisateur.

11 Fonctions OAMP

Il convient de tenir un journal d'audit pour toutes les tentatives d'accès aux fonctions OAMP (réussies ou échouées), et pour toutes les modifications et toutes les fermetures de section associées. Les événements considérés comme importants dans le cadre de la politique du fournisseur de réseau NGN seront également consignés.

Dans la présente section sont décrits certains mécanismes portant sur d'importantes fonctions. La liste de ces mécanismes n'est pas exhaustive, d'autres implémentations pouvant être adoptées en fonction de la politique du fournisseur de réseau NGN.

NOTE – Il est nécessaire d'assurer la sécurité de la journalisation des événements. Pour des informations complémentaires, se reporter à [UIT-T Y.2701] et [b-UIT-T M.3016.0].

11.1 Interface d'élément de réseau avec systèmes de journalisation

Il est recommandé que les éléments de réseau envoient leurs informations de journalisation à un serveur de journalisation distant. Les éléments qui utilisent le protocole Syslog [b-IETF RFC 5424] pour exécuter cette fonction peuvent appliquer les spécifications énoncées dans le présent paragraphe.

Les éléments de réseau utilisant le protocole Syslog peuvent comprendre un horodateur, dont la référence temporelle est fondée sur la valeur reçue d'une source temporelle fiable via le protocole SNTP/NTP, et qui peut indiquer l'horodatage en temps UTC. Le nom de serveur (s'il est fourni) ou l'adresse IP des éléments peuvent figurer dans l'en-tête de message Syslog.

11.2 Utilisation du protocole SNMP par les éléments de réseau

Il est essentiel que les éléments de réseau NGN puissent être gérés à partir d'une plate-forme distante. Le mécanisme normalisé qui le permet est le protocole SNMP. La version 3 de ce protocole [b-IETF RFC 3413], [b-IETF RFC 3414], et [b-IETF RFC 3415] a permis de corriger de nombreuses

défaillances relatives à la sécurité qui étaient présentes dans la version 2, et est diffusée de plus en plus largement.

Il est recommandé que les éléments de réseau envoient leurs informations de journalisation à un serveur de journalisation distant. Pour cela, ils peuvent utiliser le protocole SNMP, compte tenu des mises en garde relatives à la version 3 du protocole SNMP, indiquées dans la présente Recommandation.

Le protocole SNMP est défini par une architecture globale [b-IETF RFC 3411], par le mécanisme visant à nommer les objets et les événements (base MIB) [b-IETF RFC 1155], [b-IETF RFC 1212], [b-IETF RFC 1215], [b-IETF RFC 2578], [b-IETF RFC 2579], et [b-IETF RFC 2580] et par des opérations associées [b-IETF RFC 3416] et [b-IETF RFC 3417]. Pour une présentation plus détaillée des documents décrivant le cadre de gestion actuel des normes Internet, se reporter à la section 7 de [b-IETF RFC 3410].

Chaque élément de réseau NGN peut implémenter un client SNMP. Si la version 1 ou la version 2 du protocole SNMP est utilisée, et si la politique de sécurité du fournisseur de réseau NGN l'exige, chaque élément doit utiliser le mode de transport UDP sur IPSec. Chaque instance d'un message peut être codée au moyen des règles de codage de base du protocole ASN.1 [b-UIT-T X.690] dans un seul datagramme UDP. Le client peut utiliser le port d'écoute 161 pour les applications du répondeur à la commande, et le port d'écoute 162 pour les applications du récepteur de notification.

Les éléments de réseau NGN sont tenus d'implémenter toutes les bases MIB nécessaires pour signaler les événements de sécurité et les enregistrements d'audit.

11.3 Gestion des correctifs de sécurité

L'installation et la maintenance régulières de correctifs de sécurité sur les éléments et les serveurs de réseau NGN permettent de réduire au minimum la vulnérabilité de ces derniers aux attaques et aux défaillances involontaires. Il est indispensable de mettre en place une stratégie globale de gestion des correctifs, portant notamment sur les procédures d'installation et de vérification, et sur les plates-formes.

11.4 Gestion des versions

Il est essentiel de sauvegarder les différentes configurations des éléments de réseau, ainsi que les changements qui sont apportés à ces éléments. Cette sauvegarde de système a pour principal objectif de permettre un rétablissement du système en cas de perturbations matérielles ou logicielles susceptibles d'entraîner une corruption d'un logiciel ou des données système associées. Une sauvegarde système peut inclure les types d'information suivants:

- données et logique du client;
- connectivité du trafic du réseau (infrastructure, liaisons, etc.);
- l'opérateur du réseau NGN et le logiciel d'application fourni par le vendeur;
- le système d'exploitation;
- la configuration du matériel.

Il est nécessaire de tenir à jour un enregistrement permanent des opérations d'approvisionnement, de façon que tous les éléments de réseau puissent être mis à jour compte tenu des opérations d'approvisionnement qui sont intervenues depuis la dernière sauvegarde.

La plate-forme d'approvisionnement peut fournir les fonctionnalités suivantes.

- un journal des activités d'approvisionnement pour chacun des éléments de réseau qui assurent directement l'approvisionnement;
- au moins une justification des activités d'approvisionnement sur une semaine pour chaque élément de réseau.

La plate-forme d'approvisionnement peut autoriser les utilisateurs à analyser manuellement les activités d'approvisionnement enregistrées pour chaque élément de réseau. La description d'activité fournie à l'utilisateur est nécessaire pour récapituler la taille, le nombre et les types des transactions pendant un intervalle de temps donné.

La plate-forme d'approvisionnement peut offrir un outil permettant de réapprovisionner un élément de réseau donné en y entrant à nouveau des données. Cet outil devrait permettre de choisir les date et heure de début et de fin du réapprovisionnement en données. Sur la base des date et heure de début et de fin spécifiées, la plate-forme d'approvisionnement devrait entrer automatiquement à nouveau toutes les données intermédiaires dans l'élément de réseau spécifié.

11.5 Opérations d'enregistrement d'audit, d'interception et de journalisation au niveau de l'élément TE-BE

Toutes les spécifications relatives à l'enregistrement d'audit, à l'interception et à la journalisation pour des éléments de réseau NGN s'appliquent à l'élément TE-BE.

L'élément TE-BE est connecté aux systèmes OAMP par l'intermédiaire d'un tunnel de réseau VPN. Ainsi, il envoie ses messages de journalisation, reçoit les demandes SNMP et envoie les réponses correspondantes via ce réseau VPN. Il n'est pas recommandé que l'élément TE-BE accepte des demandes OAMP sur une autre interface.

Les spécifications relatives au tunnel de réseau VPN sont détaillées dans le § 9.4.

12 Approvisionnement d'équipements dans la zone non fiable

Tous les équipements des locaux client sont configurés par l'élément d'approvisionnement d'équipement terminal. Cet élément est situé dans la zone de confiance et ne peut communiquer avec les équipements terminaux que par l'intermédiaire de l'élément en limite de réseau (NBE), comme le montre la Figure 2. Un équipement terminal ou un élément TE-BE peut authentifier et établir une association de sécurité avec l'élément NBE avant de pouvoir obtenir le fichier de configuration de la part de l'élément d'approvisionnement d'équipement terminal. L'élément NBE peut prendre en charge à la fois le protocole TLS et le protocole IPsec pour établir une association de sécurité avec les équipements terminaux (y compris l'élément TE-BE). Pour plus de détails, se reporter aux § 9.1 et 9.2.

Dans ce contexte, l'équipement contrôlé par le fournisseur peut être traité comme une partie de l'élément NBE.

L'élément d'approvisionnement d'équipement terminal comprend l'adresse d'une entité NBE parmi les données de configuration téléchargées vers le dispositif authentifié. Il peut aussi comprendre un certificat utilisé pour authentifier l'abonné avec l'élément NBE, comme il est décrit au § 8.4.

Un dispositif d'équipement terminal demandera l'approvisionnement au fournisseur de services NGN. L'élément NBE recevra cette demande et authentifiera l'équipement terminal avec les entités fonctionnelles SAA/TAA. Une fois le dispositif authentifié, l'élément en limite transmettra la demande d'approvisionnement à l'élément d'approvisionnement d'équipement terminal. Ce dernier téléchargera la configuration et/ou le micrologiciel vers l'équipement terminal. Si l'équipement terminal ne peut pas être authentifié, l'erreur sera consignée.

Appendice I

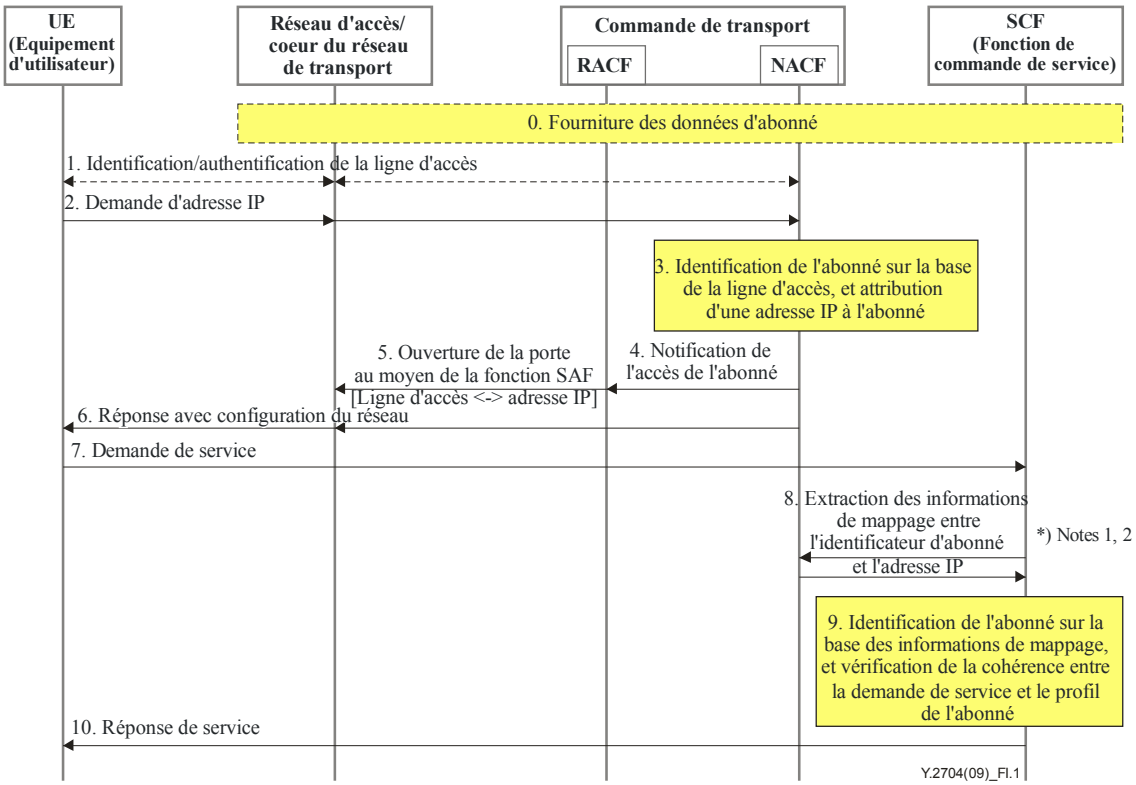
Exemples de mécanismes d'assurance de l'adresse d'origine et application au mécanisme d'identification et d'authentification de l'abonné

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

Le présent appendice donne des exemples concrets des mécanismes d'assurance de l'adresse d'origine et de leur application au mécanisme d'identification et d'authentification de l'abonné à partir de l'adresse d'origine du réseau, comme décrit dans le § 8.4.2.

I.1 Mécanisme d'identification et d'authentification de l'abonné lié à l'authentification de la ligne d'accès

Le présent paragraphe décrit un exemple de mécanisme d'identification et d'authentification de l'abonné, dans lequel une adresse IP est attribuée suite à l'authentification de la ligne d'accès. Dans cet exemple, chaque abonné est associé de façon statique à sa ligne d'accès. Ainsi, le mécanisme décrit dans cet exemple n'est applicable qu'aux services non nomades (fixes).



NOTE 1 – Les informations de mappage entre l'adresse IP et l'identificateur d'abonné peuvent être fournies par la fonction NACF à la fonction SCF au moment de l'attribution de l'adresse par la fonction NACF.

NOTE 2 – La fonction NACF peut assurer le mappage entre l'adresse IP et les informations de localisation (par exemple, l'identificateur de la ligne) au lieu du mappage entre l'adresse IP et l'identificateur d'abonné. Dans ce cas, la fonction SCF doit conserver les informations de mappage entre les identificateurs d'abonné et les emplacements, et extraire l'identificateur d'abonné des informations de localisation envoyées par la fonction NACF.

Figure I.1 – Flux de messages de haut niveau – exemple 1

Descriptions

0. Les profils d'abonné sont préconfigurés avec les entités fonctionnelles correspondantes (par exemple, les entités TUP ou SUP) dans la fonction NACF ou SCF.

   Les éléments de configuration les plus importants dans ce scénario sont les suivants:

1) La fonction NACF (généralement l'entité fonctionnelle TUP) maintient les mappages entre les identificateurs d'abonné (Identificateurs de compte d'abonné) et les identificateurs de ligne d'accès logique/physique (par exemple, l'identificateur VLAN ou port d'accès);

2) La fonction SCF (généralement l'entité fonctionnelle SUP) maintient les mappages entre les identificateurs d'abonné et les attributs ou profils des abonnés correspondants (par exemple, les valeurs de l'en-tête "Origine" dans le cas de services fondés sur le protocole SIP). Dans les cas où l'espace de nom des identificateurs d'abonné dans la fonction SCF est différent de celui de la fonction NACF, il est recommandé que la fonction SCF maintienne aussi les mappages entre ces identificateurs.

   Il est possible aussi que la fonction NACF n'ait pas à maintenir les mappages entre les identificateurs d'abonné et les identificateurs de ligne d'accès. Dans ce cas, il est recommandé que la fonction SCF maintienne les mappages entre ces deux types d'identificateur, de façon qu'elle puisse extraire un identificateur d'abonné correspondant à partir d'un identificateur de ligne d'accès.

   Sur les passerelles du réseau d'accès ou du coeur du réseau de transport, toutes les portes des lignes d'accès de l'abonné sont initialement configurées comme étant fermées, de façon que tout paquet IP entrant, à l'exception des paquets nécessaires pour le rattachement de l'équipement d'utilisateur au réseau (par exemple, l'envoi de demandes d'adresse ou de demandes d'authentification), soit supprimé.

1. Un équipement d'utilisateur se rattache au réseau d'accès par sa ligne d'accès afin d'établir la connectivité IP avec le réseau NGN. Dans cet exemple, on part du principe que l'authentification d'accès par la fonction NACF est implicite et est exécutée à l'étape N° 3. Toutefois, la fonction NACF peut également employer une méthode d'authentification d'accès explicite (par exemple, IEEE 802.1X). Dans ce cas, l'authentification d'accès au réseau est exécutée au cours de la présente phase, c'est-à-dire avant l'attribution de l'adresse IP.
2. L'équipement d'utilisateur demande l'attribution d'une adresse IP. Cela est généralement réalisé par l'envoi de messages DHCP "Discover and Request", qui sont retransmis à la fonction NACF par les passerelles.
3. Dans cet exemple, le réseau d'accès authentifie la ligne d'accès et fournit l'identificateur de ligne d'accès authentifiée (par exemple, l'identificateur VLAN ou le port d'accès) à la fonction NACF. Cette dernière peut ainsi identifier l'identificateur d'abonné de l'équipement d'utilisateur sur la base de l'identificateur de la ligne d'accès, par lequel est envoyée la demande d'adresse IP. Ensuite, la fonction NACF attribue une adresse IP à l'équipement d'utilisateur demandeur, puis enregistre les informations de mappage entre l'identificateur d'abonné et l'adresse IP attribuée.

   Ces informations de mappage peuvent être transmises de la fonction NACF à la fonction SCF et être stockées (mises en mémoire cache) dans la fonction SCF. Dans ce cas, il est possible de sauter la 8ème étape ci-après.
4. La fonction NACF notifie à la fonction RACF que l'abonné a été connecté. Cette notification comprend l'identificateur d'abonné, l'identificateur de ligne d'accès (physique/logique), l'adresse IP attribuée et les profils de qualité de service.

5. La fonction RACF prend une décision de politique sur l'attribution de ressources réseau à l'abonné et ordonne aux passerelles d'ouvrir la porte pour la ligne d'accès conformément aux règles de filtrage des paquets, définies pour accepter et transmettre les paquets IP entrants dont l'adresse d'origine est l'adresse IP attribuée à l'abonné, et de supprimer les autres paquets entrants.

   L'application du filtrage d'adresse IP d'origine coordonné avec l'authentification de ligne d'accès par la fonction NACF, décrite ci-dessus, garantit qu'une adresse IP ne peut être utilisée que par l'abonné auquel est attribuée l'adresse.

6. La fonction NACF renvoie à l'équipement d'utilisateur l'adresse IP attribuée avec d'autres paramètres de configuration de réseau (par exemple, les adresses des serveurs DNS et la fonction P-CSC-FE). Cela est généralement réalisé par l'envoi de messages DHCP "Offer and Response".

7. Après avoir obtenu la connectivité IP, l'équipement d'utilisateur envoie à la fonction SCF une demande de service (par exemple, le signal REGISTER dans le cas de services fondés sur le protocole SIP). La demande de service est transmise par les passerelles (pare-feu avec filtrage d'adresse d'origine) à la fonction SCF seulement si l'adresse d'origine de la demande est une adresse qui a été attribuée par la fonction NACF.

8. La fonction SCF extrait de la fonction NACF les informations de mappage (c'est-à-dire l'identificateur d'abonné et l'adresse IP attribuée) correspondant à l'adresse d'origine de la demande de service.

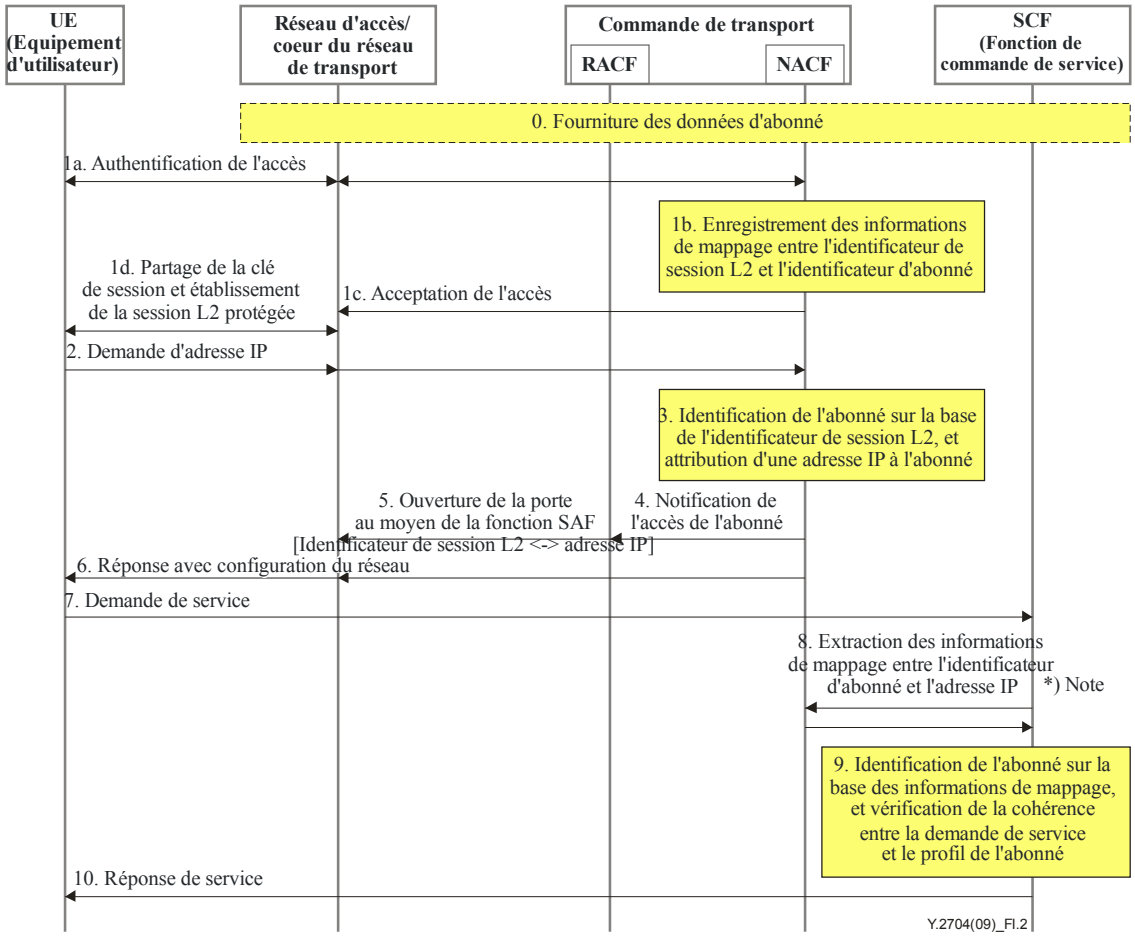
9. La fonction SCF examine la demande de service envoyée par l'abonné qui a attribué l'identificateur d'abonné contenu dans les informations de mappage extraites. Dans les cas où l'espace de nom des identificateurs d'abonné dans la fonction SCF est différent de celui des identificateurs d'abonné dans la fonction NACF, l'identificateur d'abonné extrait doit être traduit dans l'identificateur d'abonné figurant dans l'espace de nom utilisé par la fonction SCF sur la base des informations de mappage entre ces identificateurs.

   La fonction SCF extrait la valeur des attributs concernant l'identité de l'abonné (par exemple, la valeur de l'en-tête "Origine" dans le cas de services fondés sur le protocole SIP) à partir de la demande de service, et vérifie la cohérence entre ces valeurs et le profil de l'abonné correspondant.

10. Si la tentative d'authentification et d'autorisation a réussi, la fonction SCF renvoie la réponse normale afin d'offrir le service demandé (par exemple, "200 OK" dans le cas de services fondés sur le protocole SIP).

I.2 Mécanisme d'identification et d'authentification de l'abonné lié à l'authentification explicite de l'accès lors de l'établissement de la connectivité IP

Le présent paragraphe décrit un exemple de mécanisme d'identification et d'authentification de l'abonné, dans lequel une adresse IP est attribuée suite à l'authentification explicite de l'accès lors de l'établissement de la connectivité IP. Dans cet exemple, chaque abonné est associé de façon dynamique à une session L2, qui est établie au moment de l'authentification de l'accès. Ainsi, le mécanisme décrit dans cet exemple est applicable tant aux services nomades qu'aux services fixes.



NOTE – Les informations de mappage entre l'adresse IP et l'identificateur d'abonné peuvent être fournies par la fonction NACF à la fonction SCF au moment de l'attribution de l'adresse par la fonction NACF.

Figure I.2 – Flux de messages de haut niveau – exemple 2

Descriptions

0. Les profils d'abonné sont préconfigurés avec les entités fonctionnelles correspondantes (par exemple, les entités TUP ou SUP) dans la fonction NACF ou SCF. Contrairement à l'exemple précédent, la fonction NACF n'a pas à maintenir les mappages entre les identificateurs d'abonné et les identificateurs de ligne d'accès.

   Sur les passerelles du réseau d'accès ou du coeur du réseau de transport, toutes les portes des sessions d'accès L2 avec équipements d'utilisateur sont initialement configurées comme étant fermées, de façon que tout paquet IP entrant, à l'exception des paquets nécessaires pour le rattachement de l'équipement d'utilisateur au réseau (par exemple, l'envoi de demandes d'adresse et de demandes d'authentification), soit supprimé.

1a. Lorsqu'un équipement d'utilisateur demande la connectivité au réseau NGN, le réseau d'accès crée de façon dynamique une session L2 avec l'équipement d'utilisateur, et une procédure d'authentification d'accès est exécutée entre l'équipement d'utilisateur et la fonction NACF sur la base du justificatif d'identité de l'abonné (généralement au moyen d'une méthode d'authentification explicite, telle que IEEE 802.1X ou RADIUS/Diameter). Les messages de signalisation de l'authentification sont transmis par les passerelles.

1b. Au cours de la procédure d'authentification, l'identificateur de la session L2 (par exemple, l'identificateur VLAN, l'adresse L2 de l'équipement d'utilisateur, etc.) attribué à l'équipement d'utilisateur est envoyé à la fonction NACF. Une fois l'authentification effectuée avec succès, la fonction NACF enregistre cet identificateur de session L2 avec l'identificateur d'abonné authentifié.

1c. La fonction NACF notifie au réseau d'accès que l'équipement d'utilisateur a bien été authentifié et que l'accès au réseau a été autorisé (par exemple, par l'envoi d'un message "ACCESS ACCEPT" dans le cas du protocole RADIUS).

1d. A la réception de la notification, par la fonction NACF, de l'authentification réussie de l'abonné, le réseau d'accès établit une association de sécurité (SA) avec l'équipement d'utilisateur pour protéger l'intégrité et la confidentialité de la session L2. Cela est généralement réalisé au moyen des mécanismes de calcul des clés de session définis dans la norme IEEE 802.1X et de la procédure de protection définie pour chaque technologie L2 (par exemple, les protocoles TKIP/CCMP définis dans la norme IEEE 802.11i pour les réseaux locaux hertziens conformes à la norme 802.11).

Les mécanismes de sécurité décrits ci-dessus empêchent que la session L2 soit utilisée par d'autres abonnés, et fournissent les bases nécessaires pour prévenir l'usurpation d'adresses IP.

2. L'équipement d'utilisateur demande l'attribution d'une adresse IP. Cela est généralement réalisé par l'envoi de messages DHCP Discover and Request qui sont retransmis à la fonction NACF par les passerelles.

3. La fonction NACF identifie l'identificateur d'abonné de l'équipement d'utilisateur sur la base de l'identificateur de la session L2, par lequel est envoyée la demande. Ensuite, la fonction NACF attribue une adresse IP à l'équipement d'utilisateur demandeur, puis enregistre les informations de mappage entre l'identificateur d'abonné et l'adresse IP attribuée.

Ces informations de mappage peuvent être transmises de la fonction NACF à la fonction SCF et être stockées (mises en mémoire cache) dans la fonction SCF. Dans ce cas, il est possible de sauter la 8ème étape ci-après.

4. La fonction NACF notifie à la fonction RACF que l'abonné a été connecté. Cette notification comprend l'identificateur d'abonné, l'identificateur de session L2 (physique/logique), l'adresse IP attribuée et les profils de qualité de service.

5. La fonction RACF prend une décision politique sur l'attribution de ressources réseau à l'abonné et ordonne aux passerelles d'ouvrir la porte de la session L2 conformément aux règles de filtrage des paquets, définies pour accepter et transmettre les paquets IP entrants dont l'adresse d'origine est l'adresse IP attribuée à l'abonné, et de supprimer les autres paquets entrants.

L'application du filtrage d'adresse IP d'origine coordonné avec l'authentification d'accès par la fonction NACF, décrite ci-dessus, garantit qu'une adresse IP ne peut être utilisée que par l'abonné auquel est attribuée l'adresse.

Les étapes 6 à 10 sont identiques à celles de l'exemple précédent, décrit dans le § I.1.

Appendice II

Sécurité pour l'interconnexion des services de télécommunication d'urgence

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

II.1 Introduction

Un service de télécommunication d'urgence (ETS, *emergency telecommunications service*) est un service national offrant des télécommunications prioritaires aux utilisateurs autorisés ETS en cas de catastrophe ou d'urgence. L'implémentation d'un service ETS relève de la compétence nationale. Toutefois, les catastrophes/urgences peuvent dépasser les frontières géographiques; il se peut donc que les pays/administrations concluent des accords bilatéraux et/ou multilatéraux pour relier leurs systèmes ETS respectifs. Ainsi, différents réseaux nationaux regroupés au sein d'accords bilatéraux et/ou multilatéraux pourraient prendre en charge des services de télécommunication prioritaires (par exemple, téléphonie, messagerie, services de transmission vidéo et de données) dans le cadre du service ETS en cas de catastrophe ou d'urgence. La sécurité et la disponibilité des communications ETS dépendront des fonctionnalités et des mesures de sécurité appliquées dans chacun des réseaux nationaux intervenant dans une communication de bout en bout.

II.2 Domaine d'application/objet

Le présent Appendice donne des indications permettant d'assurer, par le biais du réseau, la sécurité des communications ETS à travers différents réseaux nationaux (pays/administrations).

Le présent Appendice ne porte pas sur la fonction de sécurité entre utilisateurs finals homologues fondée sur des fonctions spéciales de sécurité des équipements d'utilisateur final. Il se limite à la prise en charge par le réseau de la sécurité des services de communications ETS à travers plusieurs réseaux bond par bond. Toutefois, il est recommandé que le réseau NGN puisse prendre en charge en toute transparence ces fonctions entre homologues.

Le présent Appendice n'a pas pour objet d'imposer des conditions aux implémentations nationales d'un service ETS. Il vise essentiellement à assurer la prise en charge par le réseau de la sécurité des services de communications ETS (communications prioritaires sécurisées de signaux vocaux, de signaux vidéos, de données et de messagerie) à travers différents réseaux nationaux (pays/administrations).

II.3 Objectifs de sécurité et lignes directrices pour l'interconnexion des services de télécommunication d'urgence

Se reporter à l'Appendice I de [UIT-T Y.2701] pour des informations sur les objectifs de sécurité et les lignes directrices pour l'interconnexion des services de télécommunication d'urgence.

II.4 Authentification et autorisation

Il est recommandé que les réseaux nationaux prennent en charge et implémentent les mécanismes et les capacités nécessaires pour authentifier et autoriser l'utilisateur, le dispositif, ou l'ensemble d'utilisateurs et de dispositifs ETS sur la base du niveau d'assurance nécessaire pour accéder à un service particulier (par exemple, transmission de la voix, de vidéos ou de données) et de la politique applicable.

Il est recommandé d'utiliser comme il convient les mécanismes de sécurité décrits dans le corps de la présente Recommandation pour l'identification et l'authentification d'utilisateurs et de dispositifs d'utilisateur afin de prendre en charge les différentes implémentations de services ETS dans les réseaux nationaux:

- Associations IPsec/TLS.
- Question/réponse SIP et certificats X.509.

- Architecture d'amorçage générique.

En outre, il est recommandé d'appliquer des mesures de sécurité du contrôle d'accès aux ressources ETS, de manière à détecter et prévenir tout type d'attaque par déni de service.

Se reporter également à l'Appendice I de [UIT-T Y. 2702] pour des exemples de méthodes d'authentification et d'autorisation de services ETS.

II.5 Sécurité du transport pour le trafic de signalisation et OAMP

Il est recommandé d'utiliser comme il convient les mécanismes de sécurité IPsec et TLS décrits dans le corps de la présente Recommandation afin de protéger le trafic de signalisation et OAMP dans les réseaux nationaux.

II.6 Trafic de média

Il est recommandé d'utiliser comme il convient les mécanismes de sécurité permettant d'identifier et de protéger le trafic de média, décrits dans le corps de la présente Recommandation, afin de protéger le trafic de média de service ETS dans les réseaux nationaux.

II.7 Prise en charge des fonctions de restriction de l'identification du numéro de l'appelant et de l'identification du nom de l'appelant

L'identification du numéro de l'appelant et l'identification du nom de l'appelant sont deux fonctions du réseau RTPC traditionnel qui permettent aux utilisateurs d'identifier leur correspondant. Les communications de service ETS peuvent desservir différentes communautés nationales d'utilisateurs présentant différents niveaux de vulnérabilité quant à la divulgation de ces informations à l'abonné appelé. Il est par conséquent recommandé que des mécanismes appropriés soient pris en charge pour faire appliquer la politique relative à l'affichage ou à la divulgation d'informations d'utilisateur de service ETS.

II.8 Non-traçabilité

Pour certaines communications ETS, il importe, dans toute la mesure du possible, que l'ensemble des parties ne puissent pas disposer des informations de localisation associées à l'abonné appelant ou à l'abonné appelé. En particulier, il est recommandé de supprimer toutes les informations relatives à la localisation, voire, si nécessaire, de les remplacer par des informations sans importance, selon le cas, sur la base de la politique en vigueur. Les informations relatives à la localisation concernent notamment:

1) le numéro NPA-NXX ou l'identificateur URI de l'abonné appelant ou de l'abonné appelé;
2) l'adresse géographique de l'abonné appelant ou de l'abonné appelé;
3) les coordonnées x-y de l'abonné appelant ou de l'abonné appelé;
4) les informations relatives à la cellule de l'abonné appelant ou de l'abonné appelé, par laquelle il est possible de cibler l'emplacement à partir duquel un appel est effectué;
5) l'adresse IP de l'abonné appelant ou de l'abonné appelé;
6) le central d'extrémité de l'abonné appelant ou de l'abonné appelé, ou toute autre information relative au réseau permettant de déterminer la proximité géographique de l'abonné appelant.

II.9 Chiffrement de bout en bout d'homologue à homologue

Certains utilisateurs peuvent exiger le chiffrement d'appel/de session ETS par l'équipement d'utilisateur (UE). Pour ces appels/sessions, les procédures normales d'établissement d'appel/de session ETS s'appliquent et le processus de chiffrement de bout et bout est assuré par l'équipement d'utilisateur pour les informations supports (par exemple, les signaux vocaux) transmises à l'équipement d'utilisateur de terminaison. Ce processus de chiffrement est transparent pour le réseau NGN. Toutefois, il est recommandé que le réseau NGN puisse prendre en charge de façon transparente ces fonctions d'homologue à homologue.

Appendice III

Bonnes pratiques de sécurité

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

III.1 Introduction

Pour satisfaire aux prescriptions énoncées dans [UIT-T Y.2701], des mécanismes de sécurité venant compléter ceux qui sont spécifiés dans cette Recommandation peuvent s'avérer nécessaires. Des mécanismes de sécurité conformes aux bonnes pratiques, tels que l'utilisation de pare-feu, le renforcement du système d'exploitation, le sondage de vulnérabilité ou les systèmes de détection des intrusions peuvent être employés pour sécuriser l'infrastructure de réseau NGN. Se reporter à [b-NIST SP 800-94] pour des indications sur les systèmes de détection et de prévention des intrusions (IDPS, *intrusion detection and prevention systems*) et à [b-NIST SP 800-83] pour des indications sur la prévention et le traitement des incidents par logiciels malveillants.

Le présent appendice donne un aperçu des mécanismes de sécurité conformes aux bonnes pratiques qu'il convient d'employer.

III.2 Pare-feu

Les pare-feu sont des éléments fondamentaux de l'infrastructure de sécurité, qui assurent l'isolement du réseau aux frontières entre des segments de réseau ou entre différents réseaux. Ils effectuent cet isolement sur la base de règles spécifiques de filtrage de trafic préconfigurées, et peuvent être utilisés conjointement avec d'autres mécanismes de sécurité afin d'offrir un niveau de sécurité supplémentaire. L'adjonction de pare-feu constitue une infrastructure de sécurité fondée sur une "défense en profondeur", caractérisée par la superposition de mécanismes de sécurité multiples permettant de renforcer la sécurité.

Un pare-feu analyse le trafic entrant et le trafic sortant. Il devrait donc être configuré de façon à rejeter tout le trafic qui ne soit pas expressément autorisé par les règles applicables. Un pare-feu peut aussi offrir une journalisation du trafic et déclencher des alarmes lorsque des paquets non autorisés sont détectés. Il peut physiquement constituer un élément distinct ou faire partie des logiciels installés sur le serveur lui-même. Parmi les types de pare-feu, on peut citer les pare-feu à filtrage de paquets statique, les pare-feu de couche d'application et les pare-feu de filtrage de paquets avec état. Le choix du type de pare-feu à utiliser dépendra des préférences et des besoins particuliers du client.

Les pare-feu à filtrage statique des paquets analysent les paquets entrants et sortants et appliquent un ensemble de règles pour déterminer si les paquets seront autorisés à transiter par le pare-feu ou s'ils seront supprimés. Cette détermination est généralement fondée sur les adresses IP d'origine et de destination des paquets, sur le type de protocole et sur les ports d'origine et de destination TCP. En fonction des paquets et des critères, le pare-feu supprimera ou transmettra le paquet et, éventuellement, créera une entrée de journal et/ou émettra une alarme. Certains pare-feu à filtrage statique des paquets peuvent également effectuer une inspection plus approfondie des paquets, éventuellement jusqu'à la couche d'application.

Les pare-feu de couche d'application exécutent des applications pour le compte des machines du réseau qu'ils protègent, et sont souvent appelés pare-feu "d'application". Lors de l'exécution des applications, les pare-feu de couche d'application détecteront toute éventuelle activité anormale et bloqueront dans cette éventualité les données sur les machines qu'ils protègent. Les pare-feu de couche d'application doivent être activés avec toutes les applications nécessaires et doivent exécuter ces applications pour le compte de l'ensemble des machines protégées. De ce fait, les pare-feu de couche d'application ont une grande incidence sur la qualité de fonctionnement du réseau.

Les pare-feu avec état exécutent des fonctions de filtrage de paquets analogues à celles des pare-feu de filtrage statique des paquets, en gérant des informations sur l'état des connexions de trafic. Les

informations d'état permettent aux pare-feu de prendre de meilleures décisions quant à l'autorisation ou au refus d'un trafic particulier. Par exemple, un pare-feu avec état peut être configuré pour autoriser seulement les machines situées d'un seul côté du réseau à effectuer des communications. Cela est particulièrement utile dans le cas de réseaux privés connectés à des réseaux publics.

Dans le cas de l'utilisation de pare-feu comme sécurité supplémentaire pour la couche de signalisation et de commande, il convient de configurer ceux-ci de façon à autoriser uniquement les communications souhaitées pour la signalisation et la commande entre certaines machines. Tous les autres flux de trafic sur le réseau en dehors des communications souhaitées devraient être refusés, ce qui constitue une couche de protection pour les machines concernées.

Il convient de noter que l'installation de pare-feu peut avoir des incidences sur la conception et la production des systèmes, et il peut être nécessaire de réaliser certaines applications en tenant compte des pare-feu. A noter également que les pare-feu ne protègent pas contre toutes les attaques de sécurité, telles qu'une usurpation d'informations de paquets de signalisation légitimes.

III.3 Renforcement du système d'exploitation

Les serveurs et les éléments de réseau utilisés pour les fonctions des plans de signalisation et de commande sont vulnérables à un certain nombre d'attaques, parmi lesquelles:

- les programme de type *Backdoor* (porte dérobée);
- les programmes renifleurs;
- les intercepteurs de mot de passe et les outils de craquage;
- l'exploitation de défauts dans les services de systèmes d'exploitation;
- le déni de service (DoS, *denial of service*).

Certaines de ces attaques reposent sur des techniques bien connues, faisant intervenir des scripts et d'autres outils permettant aux pirates informatiques les moins avertis d'appliquer des exploits contre les systèmes. Une fois qu'un système est compromis, un intrus peut effectuer un certain nombre d'opérations, parmi lesquelles:

- modifier ou détruire des informations;
- divulguer des informations sensibles;
- installer des logiciels malveillants afin de collecter des informations;
- utiliser le serveur compromis pour attaquer d'autres systèmes.

Il est possible d'employer des procédures de renforcement des systèmes d'exploitation pour améliorer la résistance de ces systèmes aux attaques. Ces procédures sont essentiellement des pratiques fiables qui sont appliquées lors de l'installation et de la configuration d'un système d'exploitation. Même si aucun système n'est absolument sûr, il sera plus difficile pour un pirate informatique de compromettre un système si l'on applique des procédures de renforcement du système d'exploitation.

Renforcer un système d'exploitation consiste essentiellement à imposer des contraintes aux services, aux ports et à l'accès aux applications et aux fichiers. Il s'agit également de faire en sorte que les applications ne puissent être exécutées qu'à partir d'un compte avec privilège d'accès restreint et uniquement avec les ports et les services qui sont absolument nécessaires. Il convient de consulter les fabricants de systèmes d'exploitation afin de disposer des dernières procédures de renforcement de systèmes d'exploitation et des derniers correctifs de sécurité associés.

III.4 Evaluation de la vulnérabilité

L'évaluation de la vulnérabilité des éléments d'un réseau vise à cerner les vulnérabilités, les faiblesses et les zones à risques sur le plan de la sécurité de ces derniers. Elle consiste à soumettre les systèmes à des défaillances en interrompant les services, en déjouant les contrôles de sécurité mis en place, en interceptant des données confidentielles, en obtenant l'accès non autorisé au système ou en

volant ou refusant un service. Les éléments de réseau NGN peuvent comporter une évaluation de la vulnérabilité afin que leur sécurité soit renforcée.

L'évaluation de la vulnérabilité des éléments d'un réseau peut être réalisée lors de la phase de vérification des produits, puis de façon continue, dans le cadre de la maintenance du réseau. L'avantage d'une évaluation de la vulnérabilité de la sécurité au moment de la vérification des produits réside dans le fait que l'on dispose alors déjà d'une procédure permettant de consigner et de soumettre des demandes de modification. Les évaluations régulières de la vulnérabilité sont utiles pour identifier les nouvelles menaces et vulnérabilités, et pour prendre les mesures qui s'imposent afin de limiter les problèmes identifiés.

III.5 Systèmes de détection des intrusions

Des systèmes de détection des intrusions peuvent être utilisés pour offrir une protection contre les intrusions et d'autres opérations non autorisées. Par exemple, ces systèmes peuvent servir à avertir les administrateurs de réseau de la possibilité d'un incident de sécurité (par exemple, une compromission de serveur SIP ou une attaque par déni de service).

Les systèmes de détection des intrusions (IDS, *intrusion detection systems*) peuvent être classés globalement en fonction des critères suivants:

- Détection des incidents en temps réel ou hors ligne: un système IDS en temps réel tient un journal des événements relatifs au trafic dans le réseau au fur et à mesure qu'ils se produisent. Un système IDS hors ligne analyse les intrusions selon un mode par lot après que les incidents se sont produits.
- Installation sur le réseau ou sur des serveurs: un système IDS sur le réseau fait généralement intervenir plusieurs dispositifs de surveillance installés aux points de passage obligés dans le réseau (là où l'ensemble du trafic entre deux points peut être surveillé). Un système IDS sur des serveurs nécessite que le logiciel soit installé directement sur les serveurs à protéger et qu'il surveille les connexions au réseau et les activités des utilisateurs sur ces serveurs.
- Réactif ou passif: un système IDS réactif intervient activement pour déjouer les attaques en modifiant les règles applicables aux pare-feu ou les filtres des routeurs, ou en appliquant d'autres mesures. Un système IDS passif ne fait que transmettre le problème au personnel et à d'autres systèmes de réseau.

La plupart des produits IDS commerciaux comportent à la fois des capacités de surveillance fondées sur le réseau et des capacités de surveillance fondées sur des serveurs, un dispositif de gestion central étant chargé de recevoir les rapports issus des divers dispositifs de surveillance et d'alerter les administrateurs de réseau.

Bibliographie

[b-UIT-T E.107] Recommandation UIT-T E.107 (2007), *Service de télécommunications d'urgence (ETS) et cadre d'interconnexion pour applications nationales du service ETS*.

[b-UIT-T M.3016.0] Recommandation UIT-T M.3016.0 (2005), *Sécurité pour le plan de gestion: aperçu général*.

[b-UIT-T X.690] Recommandation UIT-T X.690 (2008) | ISO/CEI 8825-1:2008, *Technologies de l'information – Règles de codage ASN.1: Spécification des règles de codage de base, des règles de codage canoniques et des règles de codage distinctive*.

[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 Y.2091] Recommandation UIT-T Y.2091 (2008), *Réseaux de prochaine génération: Termes et definitions*.

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

[b-3GPP TS 33.328] 3GPP TS 33.328, *IP Multimedia System (IMS) media plane security*.

[b-ETSI TS 133 220] ETSI TS 133 220 V9.2.0 (2010), *Generic Authentication Architecture (GAA); Generic bootstrapping architecture*.

[b-IETF RFC 1155] IETF RFC 1155 (1990), *Structure and Identification of Management Information for TCP/IP-based Internets*.

[b-IETF RFC 1212] IETF RFC 1212 (1991), *Concise MIB definitions*.

[b-IETF RFC 1215] IETF RFC 1215 (1991), *A Convention for Defining Traps for use with the SNMP*.

[b-IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

[b-IETF RFC 2367] IETF RFC 2367 (1998), *PF_KEY Key Management API, Version 2*.

[b-IETF RFC 2403] IETF RFC 2403 (1998), *The Use of HMAC-MD5-96 within ESP and AH*.

[b-IETF RFC 2409] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*.

[b-IETF RFC 2451] IETF RFC 2451 (1998), *The ESP CBC-Mode Cipher Algorithms*.

[b-IETF RFC 2578] IETF RFC 2578 (1999), *Structure of Management Information Version 2 (SMIv2)*.

[b-IETF RFC 2579] IETF RFC 2579 (1999), *Textual Conventions for SMIv2*.

[b-IETF RFC 2580] IETF RFC 2580 (1999), *Conformance Statements for SMIv2*.

[b-IETF RFC 2617] IETF RFC 2617 (1999), *HTTP Authentication: Basic and Digest Access Authentication*.

[b-IETF RFC 2808] IETF RFC 2808 (2000), *The SecurID® SASL Mechanism*.

[b-IETF RFC 2865] IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS)*.

[b-IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

[b-IETF RFC 3310] IETF RFC 3310 (2002), *Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)*.

[b-IETF RFC 3410] IETF RFC 3410 (2002), *Introduction and Applicability Statements for Internet Standard Management Framework*.

[b-IETF RFC 3411] IETF RFC 3411 (2002), *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*.

[b-IETF RFC 3413] IETF RFC 3413 (2002), *Simple Network Management Protocol (SNMP) Applications*.

[b-IETF RFC 3414] IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.

[b-IETF RFC 3415] IETF RFC 3415 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*.

[b-IETF RFC 3416] IETF RFC 3416 (2002), *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*.

[b-IETF RFC 3417] IETF RFC 3417 (2002), *Transport Mappings for the Simple Network Management Protocol (SNMP)*.

[b-IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

[b-IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol*.

[b-IETF RFC 3602] IETF RFC 3602 (2003), *The AES-CBC Cipher Algorithm and Its Use with IPsec*.

[b-IETF RFC 3711] IETF RFC 3711 (2004), *The Secure Real-time Transport Protocol (SRTP)*.

[b-IETF RFC 3713] IETF RFC 3713 (2004), *A Description of the Camellia Encryption Algorithm*.

[b-IETF RFC 3830] IETF RFC 3830 (2004), *MIKEY: Multimedia Internet KEYing*.

[b-IETF RFC 4132] IETF RFC 4132 (2005), *Addition of Camellia Cipher Suites to Transport Layer Security (TLS)*.

[b-IETF RFC 4279] IETF RFC 4279 (2005), *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*.

[b-IETF RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol*.

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Internet Key Exchange (IKEv2) Protocol*.

[b-IETF RFC 4312] IETF RFC 4312 (2005), *The Camellia Cipher Algorithm and Its Use with IPsec*.

[b-IETF RFC 4422] IETF RFC 4422 (2006), *Simple Authentication and Security Layer (SASL)*.

[b-IETF RFC 4492] IETF RFC 4492 (2006), *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)*.

[b-IETF RFC 4566] IETF RFC 4566 (2006), *SDP: Session Description Protocol*.

[b-IETF RFC 4567] IETF RFC 4567 (2006), *Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)*.

[b-IETF RFC 4568] IETF RFC 4568 (2006), *Session Description Protocol (SDP) Security Descriptions for Media Streams*.

[b-IETF RFC 4590] IETF RFC 4590 (2006), *RADIUS Extension for Digest Authentication*.

[b-IETF RFC 4648] IETF RFC 4648 (2006), *The Base16, Base32, and Base64 Data Encodings*.

[b-IETF RFC 4740] IETF RFC 4740 (2006), *Diameter Session Initiation Protocol (SIP) Application*.

[b-IETF RFC 4835] IETF RFC 4835 (2007), *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*.

[b-IETF RFC 5077] IETF RFC 5077 (2008), *Transport Layer Security (TLS) Session Resumption without Server-Side State*.

[b-IETF RFC 5090] IETF RFC 5090 (2008), *Radius Extension for Digest Authentication*.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

[b-IETF RFC 5282] IETF RFC 5282 (2008), *Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol*.

[b-IETF RFC 5424] IETF RFC 5424 (2009), *The Syslog Protocol*.

[b-ISO/CEI 15946-1] ISO/CEI 15946-1:2008, *Technologies de l'information – Techniques de sécurité – Techniques cryptographiques basées sur les courbes elliptiques. Partie 1: Généralités*.

[b-ISO/CEI 15946-2] ISO/CEI 15946-2:2002, *Technologies de l'information – Techniques de sécurité – Techniques cryptographiques basées sur les courbes elliptiques. Partie 2: Signatures numériques (ECDA)*.

[b-ISO/CEI 15946-3] ISO/CEI 15946-3:2002, *Technologies de l'information – Techniques de sécurité – Techniques cryptographiques basées sur les courbes elliptiques. Partie 3: Etablissement de clés (ECDH)*.

[b-ISO/CEI 15946-4] ISO/CEI 15946-4:2004, *Technologies de l'information – Techniques de sécurité – Techniques cryptographiques basées sur les courbes elliptiques. Partie 4: Signatures numériques offrant un message de recouvrement*.

[b-ISO/CEI 15946-5] ISO/CEI 15946-5:2008, *Technologies de l'information – Techniques de sécurité – Techniques cryptographiques basées sur les courbes elliptiques. Partie 5: Génération de courbes elliptiques*.

[b-ISO/CEI 18033-3] ISO/CEI 18033-3:2005, *Technologies de l'information – Techniques de sécurité – Algorithmes de chiffrement – Partie 3: Chiffrement par blocs*.

[b-NIST FIPS 197] NIST Federal Information Processing Standard (FIPS) 197 (2001), *Advanced Encryption Standard*.

[b-NIST FIPS 198-1] NIST Federal Information Processing Standard (FIPS) 198-1 (2008), *The Keyed-Hash Message Authentication Code*.

[b-NIST FIPS SP800-38a] NIST Federal Information Processing Standard (FIPS) *Special Publication 800-38: Recommendation for Block Cipher Modes of Operations. Methods and Techniques, décembre 2001*.

[b-NIST SP 800-44 v2] NIST Special Publication 800-44 Version 2, *Guidelines on Securing Public Web Servers*.

[b-NIST SP 800-57] NIST Special Publication 800-57, *Recommendation for Key Management – Part 1: General (Revised)*.

[b-NIST SP 800-83] NIST Special Publication 800-83 (2005), *Guide to Malware Incident Prevention and Handling*.

[b-NIST SP 800-94] NIST Special Publication 800-94, *Guide to Intrusion detection and Prevention Systems (IDPS)*.

[b-TIA 683-D] TIA Standard TIA-683-D (2006), *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*.

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