Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2701

(04/2007)

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

Réseaux de prochaine génération – Sécurité

Prescriptions de sécurité des réseaux de prochaine génération de version 1

Recommandation UIT-T Y.2701

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

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

DISPONIBLE	Y.1–Y.99
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
Disponible	Y.900–Y.999
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
Disponible	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
Disponible	Y.2600–Y.2699
Sécurité	**Y.2700–Y.2799**
Mobilité généralisée	Y.2800–Y.2899
Disponible	Y.2900–Y.2999

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

Recommandation UIT-T Y.2701

Prescriptions de sécurité des réseaux de prochaine génération de version 1

Résumé

La Recommandation UIT-T Y.2701 énonce les prescriptions de sécurité pour les réseaux de prochaine génération (NGN, *next generation network*) et ses interfaces (par exemple UNI, NNI et ANI). Pour ce faire, la Recommandation UIT-T X.805, *Architecture de sécurité pour les systèmes assurant des communications de bout en bout* est appliquée aux Recommandations UIT-T Y.2201, *Spécifications des réseaux de prochaine génération de version 1* et Y.2012, *Prescriptions fonctionnelles et architecture du réseau de prochaine génération version 1*.

L'objectif est d'assurer, par le biais du réseau, la sécurité des communications des utilisateurs finals à travers plusieurs domaines administratifs de réseau. La présente Recommandation ne traite pas de la sécurité des actifs des abonnés et des informations les concernant dans le domaine des abonnés (par exemple réseau d'utilisateur); elle ne traite pas non plus de l'utilisation des capacités d'application d'homologue à homologue au niveau des équipements d'abonné.

La présente Recommandation repose sur un modèle de confiance fondé sur des éléments de réseau (boîtes physiques). Les fournisseurs NGN mettront en place des éléments de réseau comportant les entités fonctionnelles définies dans la Recommandation UIT-T Y.2012. Le groupement de ces entités fonctionnelles dans un élément de réseau donné variera en fonction du fabricant. La présente Recommandation n'a donc pas pour but de représenter un groupement strict et fixe des entités fonctionnelles logiques dans les éléments de réseau physiques.

Les exigences énoncées dans la présente Recommandation devraient être considérées comme constituant un ensemble minimal d'exigences de sécurité; les fournisseurs NGN sont encouragés à prendre des mesures additionnelles à celles qui sont prévues dans les Recommandations relatives à la sécurité des NGN.

Source

La Recommandation UIT-T Y.2701 a été approuvée le 27 avril 2007 par la Commission d'études 13 (2005-2008) de l'UIT-T selon la procédure définie dans la Résolution 1 de l'AMNT.

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.2701

Prescriptions de sécurité des réseaux de prochaine génération de version 1

1 Domaine d'application

La présente Recommandation énonce les prescriptions de sécurité pour les réseaux de prochaine génération (NGN, *next generation network*) afin de contrer les menaces qui pèsent sur leur sécurité. Pour ce faire, les principes de [UIT-T X.805], *Architecture de sécurité pour les systèmes assurant des communications de bout en bout* sont appliqués à [UIT-T Y.2201], *Spécifications des réseaux de prochaine génération de version 1* et [UIT-T Y.2012], *Prescriptions fonctionnelles et architecture du réseau de prochaine génération version 1*.

Les prescriptions visent à protéger ce qui suit dans un environnement multiréseaux:

- L'infrastructure des fournisseurs de réseau et de service ainsi que les actifs (par exemple, les actifs et ressources des NGN comme les éléments de réseau, les systèmes, les composants, les interfaces ainsi que les données et les informations), les ressources, les communications (à savoir le trafic de signalisation, de gestion et de données/support) et les services associés.
- Les services et capacités des NGN (par exemple, les services vocaux, vidéo et de données).
- Les communications des utilisateurs finals et les informations les concernant (par exemple, les informations privées).

L'objectif est d'assurer, par le biais du réseau, la sécurité des communications des utilisateurs finals à travers plusieurs domaines administratifs de réseau. La présente Recommandation ne traite pas de la sécurité des actifs des abonnés et des informations les concernant dans le domaine des abonnés (par exemple, réseau d'utilisateur); elle ne traite pas non plus de l'utilisation des capacités d'application d'homologue à homologue au niveau des équipements d'abonné.

Les prescriptions énoncées dans la présente Recommandation s'appliquent à un NGN, y compris les interfaces utilisateur-réseau (UNI, *user-to-network interface*), les interfaces réseau-réseau (NNI, *network-to-network interface*) et les interfaces application-réseau (ANI, *application-to-network interface*) dans un environnement multiréseaux.

Les fournisseurs de service NGN mettront en place des "éléments de réseau" comportant les entités fonctionnelles définies dans [UIT-T Y.2012]. Le groupement de ces entités fonctionnelles dans un élément de réseau donné variera en fonction du fabricant. La présente Recommandation n'a donc pas pour but de représenter un groupement strict et fixe des entités fonctionnelles logiques dans les éléments de réseau physiques.

Les prescriptions énoncées dans la présente Recommandation devraient être considérées comme constituant un ensemble minimal d'exigences pour la sécurité des NGN et non comme un ensemble exhaustif. Par conséquent, un fournisseur NGN sera peut-être amené à prendre des mesures additionnelles à celles qui sont prévues dans les Recommandations relatives à la sécurité des NGN.

En outre, les prescriptions énoncées dans la présente Recommandation englobent certains aspects techniques de ce qu'on appelle généralement la gestion d'identité (IdM, *identity management*). Dans la pratique, la gestion d'identité désigne la "gestion par les fournisseurs NGN d'attributs fiables d'une entité telle qu'un abonné, un dispositif ou un fournisseur". Elle n'est pas destinée à indiquer la validation positive d'une personne.

Les administrations pourront exiger que les fournisseurs NGN tiennent compte de la réglementation nationale et des orientations générales nationales lors de l'implémentation de la présente Recommandation.

1.1 Principes énoncés dans la Recommandation UIT-T X.805

[UIT-T X.805] définit les dimensions de sécurité suivantes:

contrôle d'accès;

authentification;

non-répudiation;

confidentialité des données;

sécurité de la communication;

intégrité des données;

disponibilité;

respect de la vie privée.

Par ailleurs, elle identifie les menaces de sécurité suivantes.

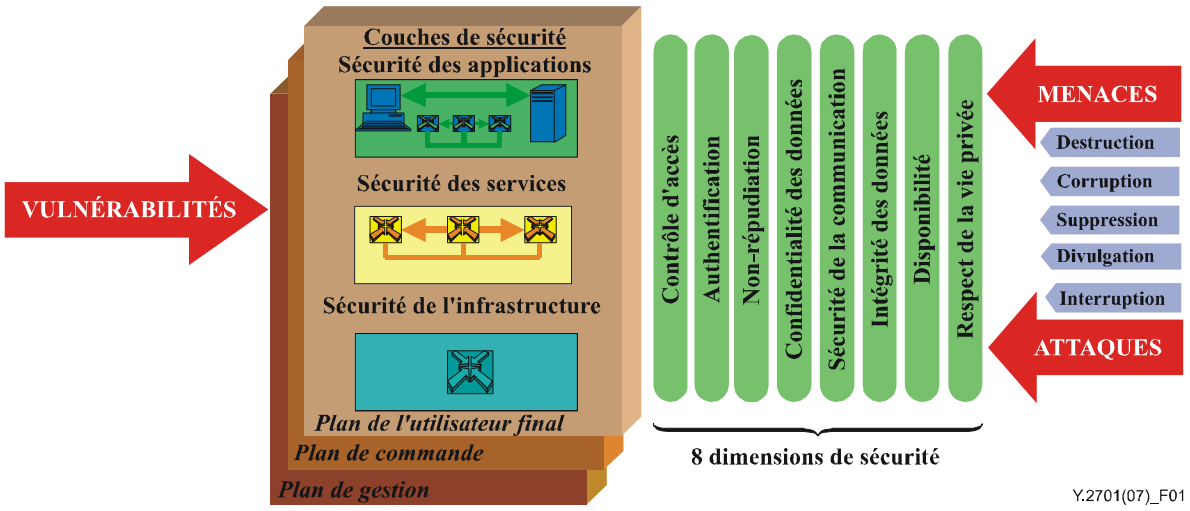


Figure 1 – Architecture de sécurité définie dans la Recommandation UIT-T X.805 (Figure 3/X.805)

On considère que la présente Recommandation s'appuie sur ces dimensions de sécurité et menaces de sécurité indiquées ci-dessus.

La présente Recommandation ne contient pas plus de détails sur la définition ou la distinction de l'utilisation des couches de sécurité X.805 (applications, services et infrastructure) et une telle distinction n'est pas nécessaire pour la conformité à la présente norme. Dans la présente Recommandation, on fait référence à une distinction du trafic dans les plans de gestion, de commande et de l'utilisateur mais le lecteur est averti que l'utilisation de cette classification dépend de la couche considérée dans une pile de protocoles. Il faudra donc faire référence à d'autres normes pour déterminer la conformité à ces distinctions. La présente norme énonce des recommandations concernant l'application des dimensions de sécurité, mais ces recommandations ne sont pas censées être exhaustives concernant l'évaluation de la sécurité des NGN.

1.2 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 forte disponibilité des communications dans les NGN.

3) Dans chaque domaine de réseau, des politiques seront établies et appliquées concernant 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) à travers 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.

1.3 Aperçu général

La présente Recommandation est organisée comme suit:

- Paragraphe 2 (Références) – Ce paragraphe contient les références normatives.
- Paragraphe 3 (Définitions et abréviations) – Ce paragraphe contient les définitions et les abréviations utilisées dans la présente Recommandation.
- Paragraphe 4 (Menaces et risques de sécurité) – Ce paragraphe précise les menaces et risques de sécurité supposés pour l'environnement des NGN. Ces menaces et risques de sécurité supposés sont utilisés pour définir les exigences de sécurité et pour déterminer les capacités et procédures de sécurité à prendre en charge.
- Paragraphe 5 (Modèle de confiance pour la sécurité) – Ce paragraphe décrit un modèle de confiance pour la sécurité des NGN. On peut utiliser ce modèle pour élaborer des relations de confiance pour la connectabilité aux interfaces UNI, ANI et NNI et pour concevoir l'architecture de sécurité.
- Paragraphe 6 (Architecture de sécurité) – Ce paragraphe décrit la relation entre l'architecture fonctionnelle des NGN définie dans [UIT-T Y.2012] et les architectures de sécurité composites.
- Paragraphe 7 (Objectifs et exigences) – Ce paragraphe décrit les objectifs et exigences générales de sécurité pour les NGN à utiliser pour définir les exigences de sécurité spécifiques pour les NGN.
- Paragraphe 8 (Exigences de sécurité spécifiques) – Ce paragraphe contient les exigences de sécurité spécifiques définies sur la base du paragraphe 7.
- Appendice I – Objectifs de sécurité et lignes directrices pour l'interconnexion des services de télécommunication d'urgence.
- Bibliographie.

La présente Recommandation a pour objet de jeter les bases de la sécurité des NGN. Diverses Recommandations associées seront élaborées dans l'avenir pour traiter de sujets spécifiques relatifs à la sécurité (par exemple, authentification et autorisation, gestion de certificat, gestion d'identité, etc.).

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

[UIT-T M.3016.1] Recommandation UIT-T M.3016.1 (2005), *Sécurité pour le plan de gestion: prescriptions de sécurité*.

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

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

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

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

3 Définitions et abréviations

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

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

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

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 actif: quelque chose qui a de la valeur pour l'organisation, ses activités et sa continuité.

3.2.2 élément en limite: élément de réseau qui assure des fonctions permettant de raccorder différents domaines de sécurité et administratifs.

3.2.3 réseau d'entreprise: réseau privé qui prend en charge de multiples utilisateurs et qui peut se situer en de multiples endroits (par exemple, une entreprise, un campus).

3.2.4 élément en limite de domaine: élément en limite contrôlé uniquement par le fournisseur, assurant des fonctions de sécurité avec d'autres domaines de réseau.

3.2.5 élément en limite de réseau: élément en limite contrôlé uniquement par le fournisseur, assurant des fonctions de sécurité avec des équipements terminaux.

3.2.6 domaine de sécurité: 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.

3.2.7 zone de sécurité: la présente Recommandation 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.

3.2.8 élément en limite d'équipement terminal: élément en limite assurant des fonctions de sécurité entre l'équipement local d'abonné et le réseau du fournisseur de service.

3.2.9 confiance: 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.

3.2.10 zone de confiance mais vulnérable: 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.

3.2.11 zone de confiance: 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".

3.2.12 zone non fiable: 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.

3.2.13 réseau d'utilisateur: réseau privé constitué d'équipements terminaux qui peuvent avoir de multiples utilisateurs.

3.3 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivant:

3G	troisième génération
AGW	passerelle d'accès (*access gateway*)
ANI	interface application-réseau (*application-to-network interface*)
B2BUA	agent d'utilisateur dos à dos (*back-to-back user agent*)
BE	élément en limite (*border element*)

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*)
ETS	service de télécommunication d'urgence (*emergency telecommunications service*)
FE	entité fonctionnelle (*functional entity*)
GW	passerelle (*gateway*)
I-CSC-FE	entité fonctionnelle interrogatrice de contrôle de session d'appel (*interrogating call session control functional entity*)
IMS	sous-système multimédia IP (*IP multimedia subsystem*)
IP	protocole Internet (*Internet protocol*)
LAN	réseau local (*local area network*)
MPLS	commutation multiprotocolaire par étiquetage (*multi-protocol label switching*)
MRP-FE	entité fonctionnelle de traitement des ressources médias (*media resource processing functional entity*)
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*)
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*)
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*)

S-CSC-FE entité fonctionnelle serveur de commande de session d'appel (*serving call session control functional entity*)

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*)

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

TE équipement terminal (*terminal equipment*)

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

UA agent d'utilisateur (*user agent*)

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

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

VLAN réseau local virtuel (*virtual LAN*)

W-CDMA accès multiple par répartition en code large bande (*wideband code division multiple access*)

WLAN réseau local sans fil (*wireless LAN*)

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

4 Menaces et risques de sécurité

La présente Recommandation repose sur l'hypothèse que les systèmes, les composants, les interfaces, les informations, les ressources, les communications (à savoir le trafic de signalisation, de gestion et de données/support) et les services qui constituent un NGN seront exposés à diverses menaces et divers risques en termes de sécurité. Ces menaces et ces risques dépendront d'un certain nombre de facteurs. En outre, les utilisateurs finals seront eux aussi exposés à certaines menaces (par exemple, l'accès non autorisé à des informations privées).

Menaces visant les NGN:

- reconnaissance non autorisée, par exemple analyse à distance du système pour déterminer les points faibles (balayages, interrogation de port, tables de routes, etc.);
- effraction/prise de contrôle d'un dispositif entraînant des anomalies et des erreurs dans les audits de configuration;
- destruction d'informations et/ou d'autres ressources;
- corruption ou modification d'informations;
- vol, suppression ou perte d'informations et/ou d'autres ressources;
- divulgation d'informations; et
- interruption de services et déni de services.

Par ailleurs, il est évident que les NGN seront exploités dans un environnement différent de l'environnement du RTPC et pourront donc être exposés à des types différents de menaces et d'attaques venant de l'intérieur ou de l'extérieur. Les NGN pourront être connectés directement ou indirectement à des réseaux de confiance, à des réseaux non fiables et à des équipements terminaux, et seront donc exposés aux risques et menaces associés à la connectivité aux réseaux non sécurisés et aux équipements locaux d'abonné. Par exemple, le NGN d'un fournisseur pourra être connecté

directement ou indirectement (à savoir par le biais d'un autre réseau) à ce qui suit, comme illustré sur la Figure 2:

- d'autres fournisseurs de service, et leurs applications;
- d'autres NGN;
- d'autres réseaux IP;
- le réseau téléphonique public commuté (RTPC);
- des réseaux d'entreprise;
- des réseaux d'utilisateur;
- des équipements terminaux;
- d'autres domaines de transport de NGN.

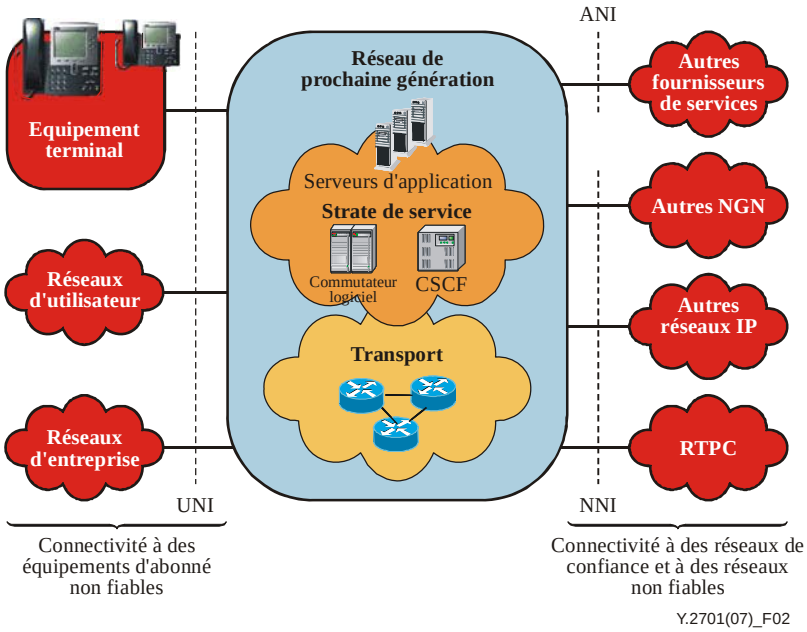


Figure 2 – Connectivité aux réseaux et aux utilisateurs

Dans l'environnement en évolution, la sécurité à travers plusieurs domaines de fournisseur de réseau dépend de ce que tous les fournisseurs choisissent de faire pour sécuriser leurs réseaux. L'accès non autorisé au réseau d'un fournisseur peut facilement conduire à l'exploitation d'un réseau interconnecté et des services qui lui sont associés. C'est un exemple de l'exploitation du maillon faible, qui peut menacer l'intégrité du réseau d'un fournisseur et la continuité du service avec la réception de divers types d'attaques.

Chaque fournisseur NGN est responsable de la sécurité dans son domaine. Chaque fournisseur NGN est chargé de concevoir et d'implémenter des solutions de sécurité en appliquant une politique propre au réseau pour les relations de confiance (paragraphe 5), afin de répondre aux besoins propres à son réseau et de respecter les objectifs de sécurité globaux de bout en bout à travers plusieurs domaines de fournisseur de réseau.

5 Modèle de confiance pour la sécurité

Le présent paragraphe définit le modèle de confiance pour la sécurité des NGN.

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, 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.

5.1 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 3.

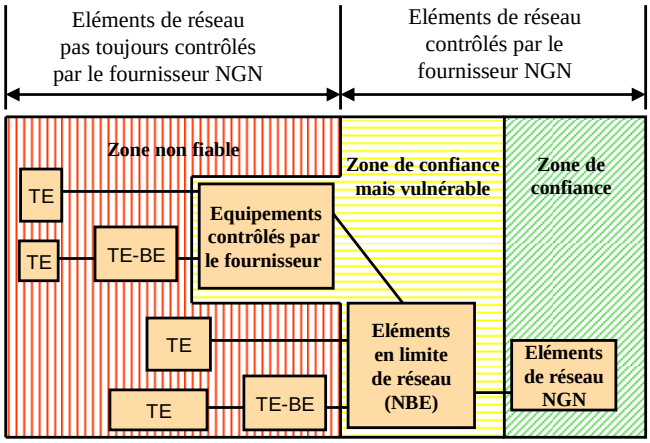


Figure 3 – Modèle de confiance pour la sécurité

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: ils sont entièrement sous le contrôle du fournisseur NGN, ils sont situés dans son domaine et ils communiquent uniquement avec des éléments situés dans la zone "de confiance" et avec des éléments situés dans la zone "de confiance mais vulnérable". Le fait qu'un élément soit situé dans une zone de confiance n'implique pas que cet élément soit lui-même sûr.

La zone "de confiance" 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, sécurité pour les messages OAMP et VPN à part dans le réseau (MPLS/)IP pour les communications dans la zone "de confiance" et avec les éléments de réseau NGN dans la zone "de confiance mais vulnérable". Voir le paragraphe 8 pour plus de détails.

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 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 des locaux 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 de protéger les éléments de réseau situés dans la zone de confiance contre les attaques provenant de la zone non fiable.

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 s'interfacent 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;
- l'élément en limite de domaine (DBE, *domain border element*), qui est un équipement du même type que l'élément en limite de réseau à ceci près qu'il se trouve en limite de domaine;
- 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;
- l'élément OAMP-NBE, qui s'interface 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 des équipements du fournisseur NGN situés dans des installations extérieures;
- l'élément NBE de serveur d'application/serveur web (AS/WS-NBE, *application server/web server NBE*), qui s'interface 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.

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;
- les unités de réseau optiques (ONU, *optical network unit*) situées dans la résidence d'un utilisateur/abonné.

La "zone de confiance mais vulnérable", comportant les 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 selon les besoins. Voir le paragraphe 8 pour plus de détails.

Une "zone non fiable" inclut tous les éléments des réseaux d'abonné ou éventuellement des réseaux homologues ou d'autres domaines du fournisseur NGN en dehors du domaine initial, qui sont raccordés aux éléments en limite de réseau du fournisseur NGN. Dans la zone "non fiable", comportant les équipements terminaux, ces équipements peuvent ne pas être sous le contrôle des fournisseurs NGN, auquel cas la politique de sécurité du fournisseur ne pourra peut-être pas être appliquée à l'utilisateur. Il est 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 OAM&P et de renforcer la protection de l'élément en limite TE-BE, situé dans la zone "non

fiable". Toutefois, faute de sécurité physique, ces mesures ne peuvent pas être considérées comme étant d'une sécurité absolue. Voir le paragraphe 8 pour plus de détails.

5.2 Modèle de confiance pour l'interconnexion de réseaux

Lorsqu'un NGN est raccordé à un autre réseau, la confiance dépend:

- de l'interconnexion physique, celle-ci pouvant aller d'une connexion directe dans un bâtiment sécurisé à des 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, des clauses pénales pouvant figurer dans les accords SLA, et/ou de la confiance en la politique de sécurité de l'autre fournisseur NGN;
- d'une manière générale, les fournisseurs NGN devraient considérer les autres fournisseurs comme non fiables.

La Figure 4 montre un exemple dans lequel un réseau connecté est considéré comme étant non fiable.

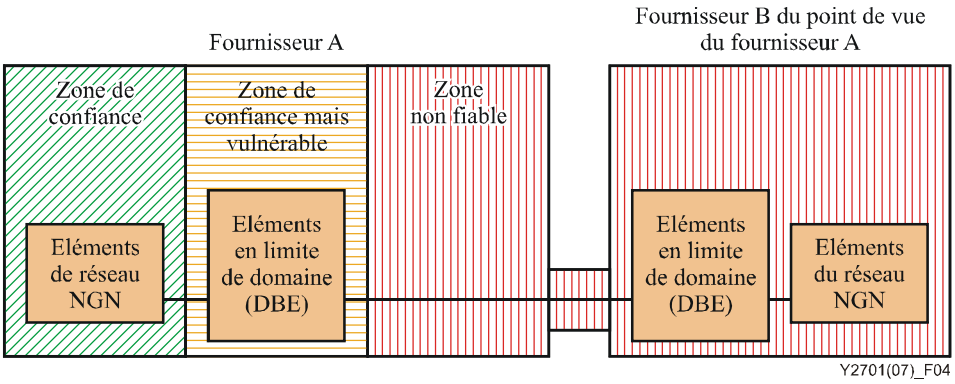


Figure 4 – Modèle de confiance pour l'interconnexion

6 Architecture de sécurité

6.1 Architecture fonctionnelle de référence des NGN

L'architecture des NGN est définie dans [UIT-T Y.2012], *Prescriptions fonctionnelles et architecture du réseau de prochaine génération version 1*, sur la base de [UIT-T Y.2201], *Spécifications des réseaux de prochaine génération de version 1*.

La Figure 5 illustre l'architecture d'un NGN du point de vue fonctionnel.

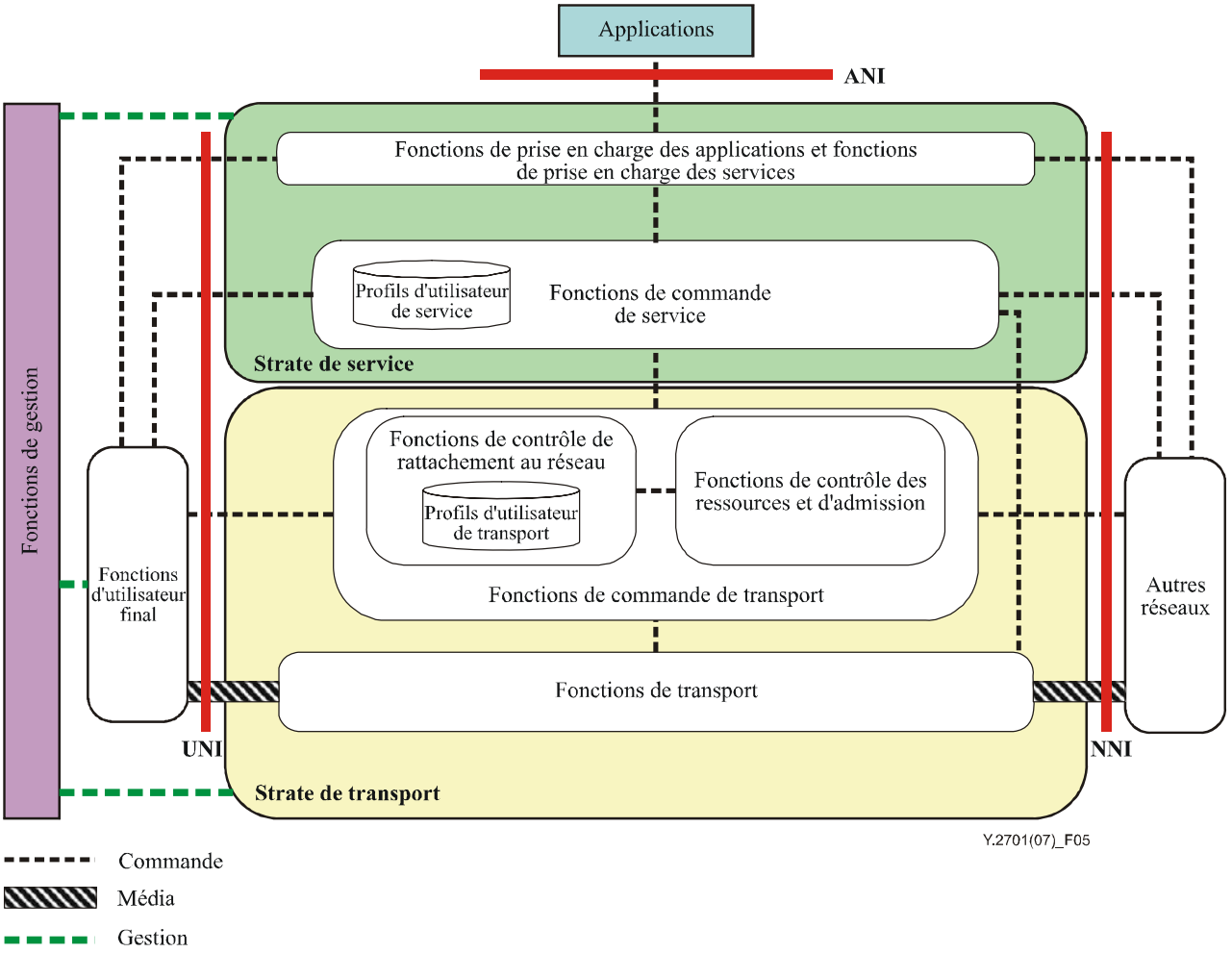


Figure 5 – Aperçu de l'architecture d'un NGN (Figure 1/Y.2012)

Le NGN prend en charge un point de référence vers les fonctions d'utilisateur final, appelé interface utilisateur-réseau (UNI, *user-to-network interface*), et un point de référence vers les autres réseaux, appelé interface réseau-réseau (NNI, *network-to-network interface*). Il prend aussi en charge un point de référence vers le groupe fonctionnel des applications, appelé interface application-réseau (ANI, *application-to-network interface*), permettant à l'application de capacités NGN de créer et de mettre en place des applications pour les utilisateurs NGN.

La strate de transport du NGN de version 1 assure des services de connectivité IP aux utilisateurs NGN sous le contrôle des fonctions de commande de transport, y compris les fonctions de contrôle de rattachement au réseau (NACF, *network attachment control function*) et les fonctions de contrôle des ressources et d'admission (RACF, *resource and admission control function*).

La strate de service fournit des services et applications à l'utilisateur final en utilisant les fonctions de prise en charge des applications et les fonctions de prise en charge des services ainsi que des fonctions de commande connexes.

Les fonctions d'utilisateur final sont des fonctions raccordées aux réseaux d'accès NGN et aucune hypothèse n'est faite au sujet des diverses interfaces d'utilisateur final et des divers réseaux d'utilisateur final.

Les fonctions de gestion permettent de gérer le NGN afin de fournir les services NGN avec la qualité, la sécurité et la fiabilité attendues.

Pour de plus amples détails, on se reportera à [UIT-T Y.2012].

6.2 Projection sur l'architecture fonctionnelle des NGN

La présente Recommandation décrit la méthode de sécurisation fondée sur le modèle de confiance illustré au paragraphe 5, à savoir un NGN composé d'un domaine de confiance (zone verte), d'un domaine non fiable (zone rouge) et d'un domaine de confiance mais vulnérable (zone jaune) entre les deux premiers.

L'un des points essentiels de la sécurisation fondée sur ce modèle est la méthode de transmission du trafic de signalisation, du trafic de média et du trafic OAMP du domaine non fiable au domaine de confiance. Diverses méthodes sont possibles, le fournisseur NGN faisant son choix en fonction de sa politique. On donne ci-après des exemples de ces méthodes.

a) Installer des éléments de réseau pour faire aboutir le trafic (par exemple, agent B2BUA pour la signalisation SIP) entre la zone verte et la zone rouge. Un tel élément de réseau reçoit un paquet en provenance de la zone rouge, l'examine, le rejette s'il est incorrect et copie éventuellement la partie nécessaire pour reconstituer un paquet correct pour la zone verte. Dans ce cas, les éléments de réseau qui font aboutir le trafic deviennent des éléments de réseau de la zone jaune.

b) Contrôler le trafic dans la couche média (par exemple, ouvrir et fermer un port particulier (micro-ouverture) au niveau du pare-feu et garantir que seuls les éléments de réseau (et les utilisateurs) autorisés peuvent envoyer du trafic aux équipements situés dans la zone verte). Dans ce cas, les éléments de réseau qui contrôlent le trafic deviennent des éléments de réseau de la zone jaune.

c) Utiliser un chiffrement de bout en bout entre l'émetteur et le récepteur.

Dans l'architecture fonctionnelle illustrée dans [UIT-T Y.2012] (Figure 6 de la présente Recommandation), la signalisation SIP générée par la fonction d'utilisateur final (elle est généralement non fiable car le fournisseur NGN ne peut pas confirmer que la fonction n'est pas falsifiée) est transmise à l'entité S-2 (P-CSC-FE). Les éléments de réseau qui contiennent une entité P-CSC-FE sont donc considérés comme des éléments de réseau de la zone jaune ou comme des éléments de réseau de la zone verte du fait des fonctions de pare-feu. Si les éléments de réseau qui contiennent une entité S-1 (S-CSC-FE) sont séparés des éléments de réseau qui contiennent une entité P-CSC-FE, ils sont considérés comme des éléments de réseau de la zone verte.

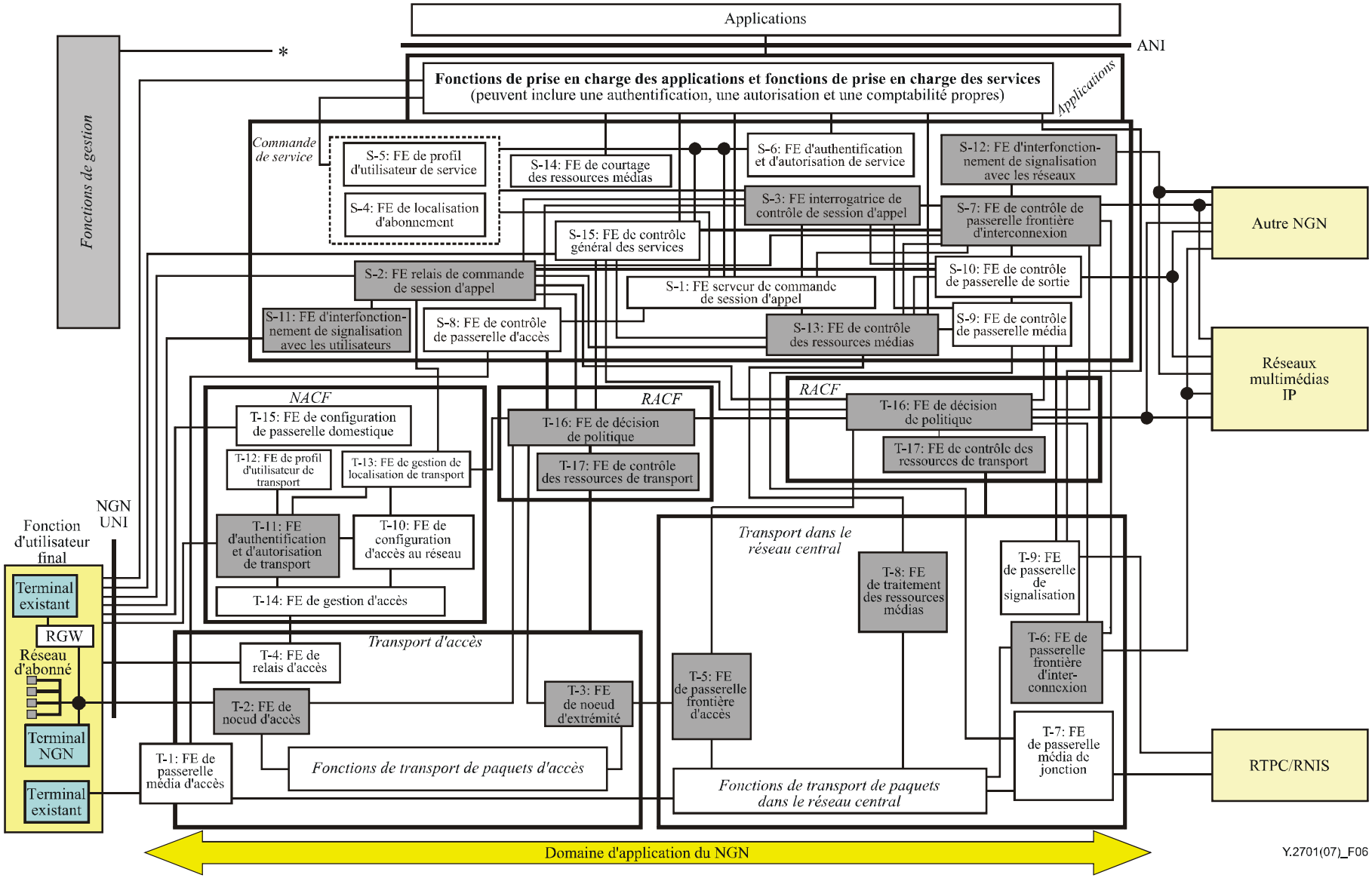


Figure 6 – Architecture fonctionnelle généralisée (Figure 3/Y.2012)

6.3 Identification des ressources de NGN à protéger sur le plan de la sécurité

Chaque fournisseur de réseau doit, dans son réseau, identifier les actifs, les ressources, les informations et les interfaces à protéger (par exemple, éléments de réseau, interfaces (UNI, ANI et NNI), systèmes de gestion ainsi que communications de signalisation, de gestion et de média/support) ainsi que les menaces qui doivent être réduites. Lors de l'identification des ressources de NGN à protéger contre les menaces de sécurité, il faut tenir compte de l'architecture stratifiée théorique définie dans [UIT-T Y.2012] ainsi que de la réalisation concrète des entités fonctionnelles.

Les tableaux qui suivent donnent des exemples d'actifs, de ressources et d'interfaces de NGN à protéger contre les menaces de sécurité; ils sont organisés comme suit:

- Tableau 1 – Exemple d'actifs, de ressources et d'informations liés à l'interface UNI
- Tableau 2 – Exemple d'actifs, de ressources, d'informations et d'interfaces liés à la strate de transport
- Tableau 3 – Exemple d'actifs, de ressources, d'informations et d'interfaces liés à la strate de service
- Tableau 4 – Exemple d'actifs, de ressources, d'informations et d'interfaces liés à la gestion

Les exemples donnés dans les Tableaux 1 à 4 ne sont pas exhaustifs.

Tableau 1 – Exemple d'actifs, de ressources et d'informations liés à l'interface UNI

Exemples	Objectifs et buts
Ressources d'utilisateur final: • Dispositifs d'utilisateur • Passerelles de réseau d'utilisateur • Passerelles de réseau d'entreprise	a) Protéger les équipements d'utilisateur final rattachés au réseau (par exemple, terminaux, passerelles de réseau d'utilisateur et passerelles de réseau d'entreprise) contre les attaques provenant du réseau (par exemple, les attaques visant à détruire, corrompre ou modifier les équipements d'utilisateur). b) Assurer une protection contre l'interruption des services (par exemple, attaques par déni de service) et garantir la disponibilité des services. c) Protéger le réseau contre l'accès non autorisé (par exemple, utilisateurs et dispositifs d'utilisateur non autorisés).
Informations d'utilisateur final: • Informations d'abonnement • Informations d'identité • Informations d'emplacement	a) Assurer une protection contre la corruption ou la modification d'informations. b) Assurer une protection contre le vol, la suppression ou la perte (par exemple, vol d'identité). c) Assurer une protection contre la divulgation (par exemple, accès non autorisé aux informations d'emplacement).
Informations de fournisseur NGN • Informations d'identité	a) Assurer une protection contre la corruption ou la modification d'informations. b) Assurer une protection contre le vol, la suppression ou la perte (par exemple, vol d'identité). c) Assurer une protection contre la divulgation (par exemple, accès non autorisé aux informations d'emplacement).

Tableau 1 – Exemple d'actifs, de ressources et d'informations liés à l'interface UNI

Exemples	Objectifs et buts
Interfaces UNI	a) Strate de transport – Protéger sur le plan de la sécurité le trafic de média/support aux interfaces UNI. b) Strate de service (commande de service) – Protéger sur le plan de la sécurité la signalisation et la gestion aux interfaces UNI (par exemple, SIP, HTTPs, RNIS et H.248). c) Strate de service (prise en charge des applications et des services) – Protéger sur le plan de la sécurité les fonctions de commande d'application et de service aux interfaces UNI (par exemple, signalisation dans la bande).

Tableau 2 – Exemple d'actifs, de ressources, d'informations et d'interfaces liés à la strate de transport

Exemples	Buts et objectifs
Ressources de la strate de transport: • Eléments de réseau de transport (par exemple, routeurs IP, noeuds MPLS) • Liaisons de transmission • Informations de routage (par exemple, serveurs DNS) • Informations de profil d'utilisateur de transport (par exemple, bases de données et répertoires de données de transport)	a) Protéger l'ensemble des éléments de réseau, composants et fonctions de transport contre l'accès non autorisé. b) Protéger l'intégrité des éléments, composants et fonctions de transport. c) Protéger la disponibilité des éléments de réseau, composants et fonctions de transport. Protection contre l'interruption des services (par exemple, contre les attaques par déni de service). d) Assurer une protection contre la divulgation de toute information privée d'utilisateur ou de réseau.
Communications intersystèmes de la strate de transport (communications à l'intérieur du réseau d'un fournisseur de réseau)	a) Protéger sur le plan de la sécurité le trafic de média/support entre les systèmes à l'intérieur du réseau d'un fournisseur. b) Protéger sur le plan de la sécurité la signalisation et la gestion de la commande de transport (par exemple, OSPF) à l'intérieur du réseau d'un fournisseur. c) Sécuriser la signalisation entre systèmes de la strate de service (par exemple, serveurs d'application) et systèmes de la strate de transport (par exemple, routeurs IP).
Interfaces et communications de transport	a) Protéger sur le plan de la sécurité le trafic de média/support aux interfaces UNI, NNI et ANI de transport. b) Protéger sur le plan de la sécurité la signalisation et la gestion de la commande de transport (par exemple, OSPF) aux interfaces UNI, NNI et ANI de transport.

Tableau 3 – Exemple d'actifs, de ressources, d'informations et d'interfaces liés à la strate de service

	Exemples	Buts et objectifs
Strate de service – Commande de service	Strate de service – Ressources de commande de service • Eléments de réseau de commande de service (par exemple, CSC-FE, SL-FE, MRP-FE, passerelles, S/BC)	a) Protéger l'ensemble des éléments de réseau, composants et fonctions de commande de service contre l'accès non autorisé. b) Protéger l'intégrité des éléments de réseau, composants et fonctions de commande de service, y compris la protection contre la corruption ou la modification d'informations. c) Protéger la disponibilité des éléments de réseau, composants et fonctions de commande de service. Assurer une protection contre l'interruption des services (à savoir contre les attaques par déni de service).
	Strate de service – Informations de commande de service • Informations d'abonné (par exemple, bases de données et répertoires de données contenant des profils d'utilisateur et des profils de service) • Informations de fournisseur NGN (par exemple, bases de données et répertoires de données contenant des informations de routage, de numérotage et d'adressage)	a) Assurer une protection contre la corruption ou la modification de données et d'informations. b) Assurer une protection contre le vol, la suppression ou la perte (par exemple, vol d'identité). c) Assurer une protection contre la divulgation (par exemple, accès non autorisé aux informations privées d'utilisateur ou de réseau).
	Strate de service – Communications intersystèmes de commande de service	Protéger sur le plan de la sécurité la signalisation intersystèmes (par exemple, SIP, RADIUS, Diameter) à l'intérieur du réseau d'un fournisseur de réseau (par exemple, signalisation de CSCF à HSS).
	Interfaces et communications	Protéger sur le plan de la sécurité la signalisation et la gestion aux interfaces UNI, NNI et ANI.
Strate de service – Prise en charge des applications et des services	Strate de service – Ressources de prise en charge des applications et des services: • Eléments de réseau et plates-formes de prise en charge des applications et des services (par exemple, serveurs, bases de données, portails web d'application)	a) Protéger l'ensemble des éléments de réseau, composants et fonctions de prise en charge des services contre l'accès non autorisé. b) Protéger l'intégrité des éléments de réseau, composants et fonctions de prise en charge des services, y compris la protection contre la corruption ou la modification d'informations. c) Protéger la disponibilité des éléments de réseau, composants et fonctions de prise en charge des services. d) Assurer une protection contre l'interruption des services (à savoir contre les attaques par déni de service).

Tableau 3 – Exemple d'actifs, de ressources, d'informations et d'interfaces liés à la strate de service

	Exemples	Buts et objectifs
	Strate de service – Informations de prise en charge des applications et des services: • Informations d'application et de service • Informations d'abonnement	a) Assurer une protection contre la corruption ou la modification de données et d'informations. b) Assurer une protection contre le vol, la suppression ou la perte (par exemple, vol d'identité). c) Assurer une protection contre la divulgation (par exemple, accès non autorisé aux informations privées d'utilisateur ou de réseau).
	Interfaces	a) Protéger sur le plan de la sécurité les éléments de réseau et les ressources concernant l'accès par d'autres fournisseurs d'application (par exemple, passerelles Parlay et Open Mobile Alliance). b) Protéger sur le plan de la sécurité les interfaces UNI, NNI et ANI. c) Protéger sur le plan de la sécurité le trafic de signalisation et de gestion aux interfaces ANI.

Tableau 4 – Exemple d'actifs, de ressources, d'informations et d'interfaces liés à la gestion

Exemples	Buts et objectifs
Ressources de gestion • Systèmes de gestion de la strate de transport (par exemple, systèmes de gestion des éléments de réseau, de gestion du réseau et de gestion des services) • Systèmes de gestion de la strate de service (par exemple, systèmes de gestion des éléments de réseau, de gestion du réseau et de gestion des services)	a) Protéger l'ensemble des éléments de réseau, composants, fonctions et interfaces de gestion contre l'accès non autorisé. b) Protéger l'intégrité des éléments de réseau, composants, fonctions et interfaces de gestion, y compris la protection contre la corruption ou la modification d'informations. c) Protéger la disponibilité des éléments de réseau, composants, fonctions et interfaces de gestion. Protection contre l'interruption des services (à savoir contre les attaques par déni de service).
Communications intersystèmes à l'intérieur du réseau d'un fournisseur de réseau	a) Protéger sur le plan de la sécurité le trafic de gestion entre les systèmes de gestion à l'intérieur d'un réseau (par exemple, strate de service). b) Protéger sur le plan de la sécurité le trafic de gestion entre, d'une part, le réseau d'utilisateur et, d'autre part, la strate de transport et la strate de service du fournisseur de réseau.
Interfaces et communications intersystèmes	a) Sécuriser les interfaces de gestion de réseau internes et toutes les interfaces de gestion UNI, NNI et ANI. b) Protéger sur le plan de la sécurité le trafic de gestion aux interfaces UNI, ANI et NNI.

7 Objectifs et exigences

7.1 Objectifs généraux de sécurité

On donne ci-après la liste des objectifs généraux de sécurité servant de base aux exigences énoncées dans la présente Recommandation.

- Les fonctionnalités de sécurité des NGN devraient être extensibles et suffisamment souples pour répondre aux divers besoins.
- Les exigences de sécurité devraient tenir compte de la qualité de fonctionnement, de la capacité d'utilisation, de l'évolutivité et des contraintes de coût des NGN.
- Les méthodes de sécurisation devraient être fondées sur les normes de sécurité applicables qui existent et qui sont bien comprises.
- L'architecture de sécurité des NGN devrait être globalement évolutive (à l'intérieur du domaine d'un fournisseur de réseau, à travers plusieurs domaines de fournisseur de réseau, concernant la mise en place de fonctionnalités de sécurité).
- L'architecture de sécurité des NGN devrait respecter la séparation logique ou physique du trafic de signalisation et de commande, du trafic d'utilisateur et du trafic de gestion.
- Les fonctionnalités de sécurité des NGN devraient être mises en place et gérées de façon fiable.
- Un NGN devrait être sécurisé du point de vue de tous: fournisseur de service, fournisseur de réseau et abonné.
- Les méthodes de sécurisation ne devraient généralement pas affecter la qualité des services offerts.
- Les fonctionnalités de sécurité devraient pouvoir être mises en place et configurées de façon simple et fiable par les abonnés et les fournisseurs (fonctionnalités prêtes à l'emploi).
- Des niveaux de sécurité appropriés devraient être maintenus même en cas d'utilisation de la fonctionnalité de multidiffusion.
- Les capacités de découverte de service devraient prendre en charge divers critères de délimitation (par exemple, emplacement, coût, etc.) pour donner des résultats adéquats, avec des mécanismes appropriés pour garantir la sécurité et le respect de la vie privée.
- Le système de résolution d'adresse devrait être un système spécial utilisé uniquement par le réseau considéré, certaines mesures de sécurité devant être mises en place. Ce système peut utiliser des bases de données qui sont internes ou externes à un domaine.
- Les principes et les objectifs généraux de sécurité applicables à la gestion sécurisée du RGT, décrits au paragraphe 7 de [UIT-T M.3016.0], devraient être suivis.

7.2 Objectifs de sécurité à travers plusieurs domaines de fournisseur de réseau

L'objectif général est d'assurer, via le réseau, la sécurité des communications de bout en bout à travers plusieurs domaines de fournisseur. Pour cela, la sécurité de la communication de bout en bout est assurée bond par bond à travers les différents domaines de fournisseur. La Figure 7 illustre le concept général de sécurité des communications de bout en bout entre utilisateurs finals assurée par le biais du réseau. Chaque segment de réseau a des responsabilités spécifiques en matière de sécurité dans sa zone de sécurité afin de faciliter la sécurité et la disponibilité des communications de NGN à travers plusieurs réseaux.

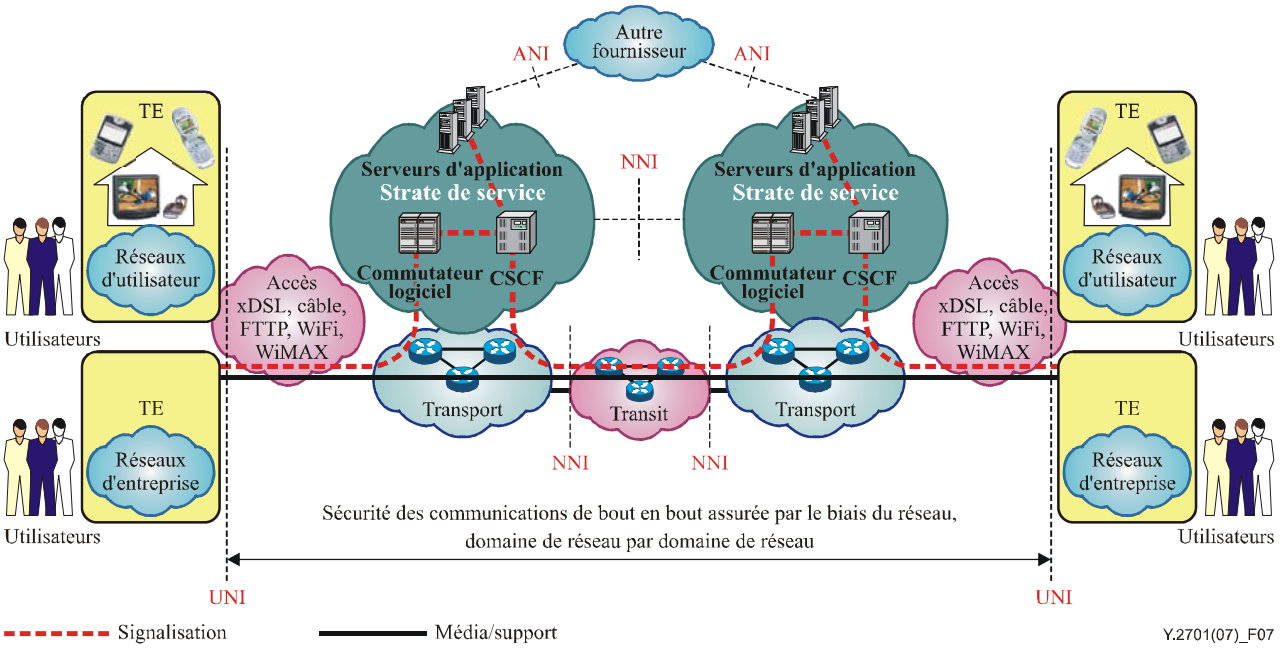


Figure 7 – Sécurité des communications à travers plusieurs réseaux

Comme décrit au § 5.2, le modèle de confiance entre les NGN interconnectés dépend de plusieurs aspects comme les interconnexions physiques, les modèles d'interconnexion et les relations commerciales.

7.3 Exigences propres aux dimensions de sécurité

Les objectifs décrits ici sont propres à certaines dimensions de sécurité, telles que l'authentification. Ils sont communs à toutes les interfaces.

7.3.1 Contrôle d'accès

Les fournisseurs NGN doivent restreindre l'accès aux abonnés autorisés. L'autorisation peut être donnée par le fournisseur qui offre l'accès ou par d'autres fournisseurs après validation par des processus d'authentification et de contrôle d'accès.

Le NGN doit empêcher l'accès non autorisé, par exemple par des intrus qui se font passer pour des utilisateurs autorisés.

7.3.2 Authentification

Les fournisseurs NGN doivent prendre en charge des capacités d'authentification des abonnés, des équipements, des éléments de réseau et des autres fournisseurs, notamment (la liste n'est pas exhaustive):

1) Capacités d'authentifier les utilisateurs souhaitant accéder au réseau de transport (par exemple, authentification et autorisation d'un dispositif d'utilisateur final, d'une passerelle de réseau d'utilisateur ou d'une passerelle de réseau d'entreprise pour obtenir l'accès ou le rattachement au réseau de transport).

2) Capacités d'authentifier les utilisateurs souhaitant accéder à des services au début ou au cours de la fourniture de services (par exemple, authentification d'un utilisateur, d'un dispositif ou d'une combinaison utilisateur/dispositif, l'authentification s'appliquant à l'accès aux services/applications NGN).

3) Capacités pour un utilisateur NGN d'authentifier le fournisseur NGN sur chaque strate (par exemple, un utilisateur authentifiant l'identité du fournisseur NGN connecté ou du fournisseur de service) si la politique de sécurité l'exige.

4) Capacités permettant de procéder à une authentification entre utilisateurs homologues (par exemple, authentification de l'utilisateur appelé et de l'entité d'origine ou de l'origine des données) en tant que services ou éléments de service de réseau.

5) Capacités permettant de procéder à une authentification bilatérale entre deux fournisseurs NGN sur chaque strate pour l'échange du trafic de signalisation, de gestion et de média/support (par exemple, authentification des réseaux directement interconnectés et des réseaux distants à travers les interfaces NNI).

6) Capacités permettant de procéder à une authentification des autres fournisseurs de service à travers les interfaces ANI. Des méthodes fondées ou non sur le module SIM doivent être prises en charge.

NOTE – L'authentification d'une entité n'est pas destinée à indiquer la validation positive d'une personne.

7.3.3 Non-répudiation

La présente Recommandation ne spécifie pas d'exigences de sécurité relatives à la non-répudiation.

7.3.4 Confidentialité des données

Les fournisseurs NGN doivent protéger la confidentialité du trafic d'abonné par des moyens cryptographiques ou par d'autres moyens.

Les fournisseurs de NGN doivent protéger la confidentialité des messages de commande par des moyens cryptographiques ou par d'autres moyens si la politique de sécurité le demande.

Les fournisseurs NGN doivent protéger la confidentialité du trafic de gestion par des moyens cryptographiques ou par d'autres moyens.

7.3.5 Sécurité de la communication

Les fournisseurs NGN doivent offrir des mécanismes garantissant que les informations ne sont pas détournées ou interceptées de façon illégale.

7.3.6 Intégrité des données

Les fournisseurs NGN doivent protéger l'intégrité du trafic d'abonné par des moyens cryptographiques ou par d'autres moyens.

Les fournisseurs NGN doivent protéger l'intégrité des messages de commande par des moyens cryptographiques ou par d'autres moyens si la politique de sécurité le demande.

Les fournisseurs NGN doivent protéger l'intégrité du trafic de gestion par des moyens cryptographiques ou par d'autres moyens.

7.3.7 Disponibilité

Un NGN doit être doté de capacités de sécurité permettant aux fournisseurs NGN d'empêcher ou de mettre fin aux communications avec les équipements d'utilisateur final non conformes, par exemple, pour réduire les attaques par déni de service, la propagation des virus ou des vers et d'autres types d'attaques. Ces capacités peuvent être suspendues pour permettre les communications d'urgence. Les éléments de réseau internes à un NGN peuvent aussi faire l'objet de virus, de vers ou d'autres attaques. Des mesures analogues permettant de mettre en quarantaine des éléments de réseau sont également nécessaires.

Un NGN devrait être doté de capacités de sécurité permettant à un fournisseur NGN de rejeter les paquets et le trafic considérés comme nuisibles par la politique de sécurité applicable.

Un NGN doit être doté de capacités permettant de prendre en charge des fonctions et procédures de rétablissement en cas de catastrophe. Les exigences spécifiques sortent du cadre de la présente Recommandation.

7.3.8 Respect de la vie privée

Un NGN doit être doté de capacités permettant de protéger les informations privées d'abonné telles que l'emplacement des données, les identités, les numéros de téléphone, les adresses de réseau ou les données de comptabilité des appels, conformément à la réglementation et à la législation nationales. Les exigences spécifiques relatives au respect de la vie privée relèvent de la compétence nationale et sortent du cadre de la présente Recommandation.

8 Exigences de sécurité spécifiques

Le présent paragraphe traite des exigences spécifiques de sécurité pour chacun des éléments de réseau de l'infrastructure de NGN. Toutefois, comme bon nombre des besoins de sécurité seront les mêmes pour les divers types d'éléments de réseau, les exigences globales de sécurité sont énoncées en premier, au § 8.1.

Les éléments en limite peuvent être intégrés ou à part, suivant l'implémentation.

8.1 Exigences de sécurité communes pour les éléments de réseau NGN

Ces exigences s'appliquent aux éléments de réseau NGN situés dans la zone de confiance ou dans la zone de confiance mais vulnérable. Il est souhaitable que les dispositifs présents dans la zone non fiable suivent ces exigences.

On donne ci-après la liste des exigences générales de sécurité:

L'interopérabilité doit être prise en charge par les différents éléments de réseau NGN, notamment parmi les divers mécanismes de sécurité de NGN. Des fonctionnalités de sécurité normalisées minimales doivent être disponibles dans le monde entier.

L'authentification et l'autorisation doivent être réalisées à la fois dans la strate de service et dans la strate de transport (utilisateur-réseau, réseau-utilisateur, réseau-réseau). Cela devrait aussi être possible dans le cas d'une traversée de dispositif NAPT.

Un élément de réseau NGN doit être doté de mesures de sécurité contre l'accès non autorisé aux ressources de réseau, aux dispositifs, aux services et aux données d'abonné (profil), par exemple pour bloquer le trafic non autorisé.

L'infrastructure de NGN doit permettre aux fournisseurs de limiter la visibilité de la topologie et des ressources de réseau aux entités autorisées.

L'infrastructure de NGN doit prendre en charge plusieurs zones de sécurité. Un isolement en termes de sécurité peut être exigé entre les différentes zones de sécurité.

L'infrastructure de NGN doit garantir la confidentialité et l'intégrité des flux de signalisation/commande et des flux de gestion qu'elle transporte.

L'infrastructure de NGN devrait garantir la confidentialité et l'intégrité des flux de média qu'elle transporte.

Un NGN doit garantir de façon satisfaisante la sécurité des éléments de réseau raccordés à des ressources de gestion (OSS, base de données, etc.) ou à des ressources de service.

Les exigences de sécurité applicables à la gestion sécurisée du RGT doivent être conformes à celles qui sont indiquées au paragraphe 10.1 de [UIT-T M.3016.0] et décrites plus en détail au paragraphe 6 de [UIT-T M.3016.1].

La fonctionnalité de sécurité doit être mise en application au niveau des éléments en limite de réseau (NBE ou TE-BE, à savoir les éléments de réseau présents dans la zone de confiance mais vulnérable). Elle comporte des fonctions telles que le contrôle d'accès appliqué aux paquets de données et aux informations de signalisation conformément aux politiques spécifiées (par exemple, refus du trafic provenant de certaines applications ou de certains utilisateurs).

Les éléments de réseau NGN sensibles, en particulier les éléments en limite de réseau, peuvent réaliser une séparation logique et/ou physique des conduits de transport conformément aux politiques de sécurité en place, par exemple la séparation entre les flux de commande et/ou de gestion et les flux de média en utilisant des interfaces différentes du point de vue logique ou des plans d'adresses différents, et en utilisant un réseau de transport réel ou virtuel différent du point de vue physique (virtuel comme un réseau VPN ou un réseau VLAN).

Un NGN doit assurer un stockage sûr des données liées à la sécurité (par exemple, les données d'identité et de justificatif d'identité). Ce stockage doit être distinct du répertoire de données général qui contient les informations liées aux services des abonnés. Le NGN doit disposer d'une politique de sécurité qui inclut un ensemble de règles déterminant le trafic qui doit être protégé, par exemple sur la base de contrats, le type de protection qui est utilisé, la fréquence avec laquelle les clés de session sont changées et les règles déterminant la conformité d'un dispositif en termes de sécurité.

Le NGN doit pouvoir surveiller le trafic dans le réseau et établir un descriptif des événements de réseau qui devraient être considérés comme normaux.

Le NGN doit pouvoir détecter, signaler et réduire les occurrences d'événements de réseau anormaux.

8.1.1 Politique de sécurité

La politique de sécurité est un ensemble de règles établies par l'autorité de sécurité régissant l'utilisation et la mise en place de services et de fonctionnalités de sécurité. Les fournisseurs NGN doivent élaborer une politique de sécurité appropriée et doivent être chargés de l'appliquer à tous les éléments de réseau et dispositifs qui sont sous leur contrôle.

8.1.2 Renforcement de la protection et désactivation de service

Tous les éléments de réseau NGN doivent pouvoir être configurés pour assurer les services minimaux requis pour prendre en charge l'infrastructure de NGN du fournisseur NGN. Tout service ou port de couche transport qui n'est pas requis pour le fonctionnement correct de l'élément de réseau NGN doit être désactivé sur tous les systèmes et éléments de réseau. En outre, les applications doivent tourner avec les privilèges minimaux (par exemple, sur les plates-formes "UNIX/Linux", les applications ne devraient pas tourner en tant que racine si les privilèges de racine ne sont pas indispensables). Le système d'exploitation (OS, *operating system*) de base prenant en charge un élément de réseau NGN doit pouvoir être configuré spécifiquement pour la sécurité et sa protection doit pouvoir être renforcée comme il convient. Aucune "porte dérobée" n'est permise (accès logiciel destiné à contourner les mécanismes habituels de contrôle d'accès) dans les éléments de réseau NGN, quels qu'ils soient.

Outre le renforcement de la protection, des contrôles d'accès physiques et logiques doivent être mis en place pour respecter les bonnes pratiques applicables.

8.1.3 Journal d'audit, piégeage et journalisation

Tous les éléments de réseau NGN doivent pouvoir créer un journal d'audit dans lequel sont enregistrés les événements liés à la sécurité conformément à la politique de sécurité du fournisseur NGN. Des mécanismes sont nécessaires pour empêcher toute modification non autorisée ou non détectée.

Le journal d'audit doit pouvoir être géré et les données anciennes figurant dans le journal d'audit doivent pouvoir être transférées sur un autre support, par exemple un support amovible, pour un stockage de longue durée. L'interface considérée doit permettre aux administrateurs autorisés de transférer les données anciennes du journal d'audit vers un support amovible. Cette capacité doit être protégée par une autorisation spécifique de gestion du journal d'audit.

Le § 10.1.2.6.3 de [UIT-T M.3016.0] et les § 6.6 et 6.7 de [UIT-T M.3016.1] décrivent plus en détail les exigences de sécurité concernant la journalisation et l'audit liés à la sécurité.

8.1.4 Horodatage et source de temps

Les éléments de réseau NGN doivent pouvoir utiliser une source de temps fiable à la fois pour l'horloge de système et pour l'horodatage du journal d'audit. Une source de temps fiable désigne ici une source de temps dont la résistance aux modifications non autorisées peut être vérifiée. Une fiabilité transitive est acceptable: une source de temps qui repose sur une source de temps fiable est elle-même une source de temps fiable acceptable.

8.1.5 Attribution des ressources et traitement des exceptions

Chaque élément de réseau NGN doit pouvoir limiter la quantité de ses ressources importantes (par exemple, mémoire) qu'il attribue pour répondre à des demandes. Grâce à ces limites, les effets négatifs des attaques par déni de service peuvent être réduits. Une concurrence s'exerce entre les ressources utilisées pour répondre aux demandes et les autres demandes d'utilisation de ressources du système. En outre, chaque application NGN spécifique doit pouvoir limiter sa propre utilisation de ressources importantes qu'elle attribue pour répondre aux demandes.

Le but est de limiter l'effet des salves d'activité afin qu'elles n'affectent pas les autres demandes de service, ce qui, par ailleurs, permet à l'application (et au système d'application) de pouvoir signaler aux systèmes de surveillance que l'application et/ou sa plate-forme peut faire l'objet d'une attaque par déni de service. L'élément de réseau NGN doit disposer d'une interface pour la surveillance de l'utilisation des ressources.

L'élément de réseau NGN doit rejeter purement et simplement tout paquet non conforme au protocole ou au format attendu et, conformément à la politique de sécurité, il doit pouvoir créer une entrée de journal pour chacun de ces événements. Le "rejet pur et simple" vise à piéger et journaliser le paquet reçu et à le rejeter sans envoyer de réponse indiquant le rejet (par exemple, réponse d'erreur).

Le but est de limiter les attaques potentielles provenant de paquets malveillants ou incorrects. Si l'utilisation des ressources par l'opération de journalisation est si grande qu'il y a interférence avec les autres opérations de l'élément, il va de soi qu'il convient d'arrêter la journalisation jusqu'à ce que l'utilisation des ressources revienne à un niveau acceptable.

NOTE – Cela fait partie de la gestion des ressources internes mentionnée plus haut.

8.1.6 Intégrité et surveillance du code et du système

L'élément de réseau doit pouvoir surveiller 1) sa configuration et ses logiciels, et 2) toute modification afin de détecter les modifications non autorisées, et ce, compte tenu de la politique de sécurité. Pour toute modification non autorisée, une entrée de journal doit être créée et une alarme doit être produite. Compte tenu de la politique de sécurité, l'élément de réseau doit effectuer les tâches suivantes. Il doit pouvoir examiner périodiquement ses ressources et ses logiciels à la recherche de logiciels malveillants, par exemple un virus. Il doit produire une alarme s'il découvre un logiciel malveillant au cours d'un examen.

La surveillance doit être contrôlée pour qu'elle n'ait pas d'incidence sur le déroulement des communications en temps réel sensibles au temps de transmission ou qu'elle n'entraîne pas inutilement la libération de connexions.

Le § 10.1.2.6.4 de [UIT-T M.3016.0] décrit plus en détail l'exigence de sécurité relative à l'intégrité du système.

8.1.7 Programmes de correction, corrections ponctuelles et code supplémentaire

Pour assurer la fiabilité des signaux produits par les éléments de réseau NGN d'un fournisseur NGN situés dans les réseaux non fiables, par exemple les terminaux, les logiciels du système ne doivent pas être compromis. Cela permet de garantir que des "chevaux de Troie[1]" (qui établissent une connexion de retour), des "vers" (qui produisent un trafic inutile ou transforment les systèmes en "zombies") et autres virus ne sont pas téléchargés dans les éléments de réseau NGN ou dans le système d'exploitation sous-jacent. Ces virus compromettraient l'intégrité du système, la confidentialité et/ou la disponibilité des données.

Les éléments de réseau et systèmes d'un fournisseur NGN doivent pouvoir vérifier et auditer l'ensemble de leurs logiciels. Un système OSS doit pouvoir accéder aux résultats d'audit. Cela permet d'analyser le comportement de l'infrastructure de NGN du fournisseur NGN du point de vue de la sécurité et de donner des indications aux administrateurs et fournisseurs quant aux endroits où il faut mettre en place des solutions d'atténuation.

Les programmes de correction de sécurité doivent être obtenus auprès des fabricants d'équipements et installés rapidement, une fois que le fournisseur NGN les a certifiés.

Le § I.5.2 de [UIT-T M.3016.1] contient d'autres considérations sur le processus de correction de programme, tandis que le § I.5.3.9 de [UIT-T M.3016.1] contient des considérations sur les hypothèses relatives à la sécurité pour le système d'exploitation.

8.1.8 Accès aux fonctions OAMP dans les dispositifs

Afin de protéger l'infrastructure OAMP, chaque élément de réseau NGN interne doit être géré avec une adresse IP distincte attribuée à partir d'un bloc d'adresses distinct. Chaque élément de réseau NGN interne devrait avoir une interface distincte sur le plan physique ou logique réservée exclusivement pour le trafic OAMP. Lorsqu'une interface distincte est utilisée, l'élément de réseau NGN doit rejeter purement et simplement tous les paquets reçus sur l'interface OAMP avec des adresses d'origine autres que l'adresse OAMP. L'élément de réseau NGN doit rejeter purement et simplement tous les paquets reçus sur l'interface non OAMP avec des adresses d'origine attribuées au trafic OAMP.

L'accès aux fonctions OAMP doit pouvoir être contrôlé par authentification. Une fois qu'un utilisateur a été authentifié auprès d'un système, l'élément de réseau NGN interne doit suivre toutes les modifications apportées et donner la possibilité de les annuler.

Tout emploi d'une autorisation ayant trait à la sécurité doit être journalisé dans le journal d'audit pendant un certain temps. En particulier, toutes les tentatives d'accès à l'élément de réseau – qu'elles aboutissent ou non – doivent être journalisées dans le journal d'audit.

Le trafic OAMP doit être protégé de façon fiable. Si du trafic OAMP (y compris SNMP et NTP) traverse un réseau non fiable, il doit être protégé de façon fiable (par exemple, IPsec ou MPLS, etc.).

---

[1] De nombreux chevaux de Troie jouent le rôle d'un logiciel télécommandé pour le pirate qui les distribue. Une fois qu'ils sont bien installés sur le système cible, ils établissent une connexion de retour avec le pirate pour l'informer qu'ils sont prêts à l'emploi.

8.2 Exigences pour les éléments de réseau NGN situés dans la zone de confiance

A chaque élément de réseau NGN de version 1 situé dans la zone "de confiance" doit être attribuée une adresse IP du bloc réservé aux éléments de réseau NGN internes, et c'est cette adresse qu'il faut utiliser pour l'ensemble de la signalisation. A chaque élément de réseau NGN de version 1 doit aussi être attribuée une adresse IP du bloc réservé au trafic OAMP, et c'est cette adresse qu'il faut utiliser pour l'ensemble du trafic OAMP.

Afin de préserver la confidentialité et l'intégrité des communications des abonnés, le trafic de signalisation et de média doit être protégé, soit avec un chiffrement pour le transport soit avec l'assurance que le trafic circule uniquement dans un domaine protégé.

8.3 Exigences pour les éléments en limite de réseau NGN situés dans le domaine "de confiance mais vulnérable"

Les éléments en limite de réseau constituent la principale défense contre les attaques externes, c'est-à-dire les attaques provenant de dispositifs/éléments de réseau situés dans la zone non fiable. L'ensemble du trafic provenant de dispositifs/éléments de réseau situés dans la zone "non fiable" est d'abord envoyé à un élément en limite de réseau, qui le valide avant de le transmettre à sa destination dans le domaine "de confiance". Les capacités d'établissement d'une séparation physique/logique des réseaux sont utilisées pour empêcher le trafic provenant d'un dispositif/élément de réseau situé dans la zone non fiable d'atteindre un élément de réseau situé dans le domaine "de confiance".

Les éléments en limite de réseau (NBE, *network border element*) constituent la principale défense contre les attaques visant la signalisation. L'ensemble du trafic de signalisation provenant d'une entité TE ou TE-BE située dans la zone non fiable est traité au niveau de l'élément NBE qui lui est assigné, qui retransmet la signalisation aux équipements de réseau situés dans la zone de confiance. Les capacités d'établissement d'une séparation physique/logique des réseaux au niveau de l'élément NBE sont utilisées pour empêcher le trafic provenant d'une entité TE/TE-BE située dans la zone non fiable d'atteindre un élément de réseau situé dans la zone de confiance, à l'exception du ou des éléments NBE qui lui sont assignés.

Comme pour la signalisation, les éléments NBE constituent aussi la principale défense contre les attaques visant le trafic de média. L'ensemble du trafic de média provenant d'une entité TE/TE-BE est traité au niveau d'un élément NBE, qui sert de relais pour ce trafic. L'élément NBE route les paquets de média vers la destination, à travers le domaine de confiance, seulement si ces paquets peuvent être associés à une session autorisée en cours. Les paquets de média qui ne sont pas associés à une demande de session ne sont pas valables, n'ont pas d'endroit où aller et sont rejetés. En outre, l'élément NBE vérifie l'origine du flux de média et vérifie que le débit de paquets est cohérent avec la session établie. Le trafic de média est transféré dans les installations du fournisseur NGN vers une passerelle RTPC (pour une connexion avec le RTPC) ou vers un autre élément NBE. Au deuxième élément NBE, le trafic de média est traité et retransmis à une destination de type TE.

NOTE – Le terme "session" désigne tout type de flux de média, indépendamment de la convention utilisée pour établir la session.

L'élément en limite de réseau doit prendre en charge plusieurs adresses IP ou plusieurs interfaces de réseau. L'une des adresses IP (l'adresse "interne") doit être attribuée à partir du bloc réservé aux éléments de réseau NGN de version 1 internes et c'est cette adresse (ou cette interface) qu'il faut utiliser pour l'ensemble du trafic de signalisation et de média en provenance ou à destination d'autres éléments de réseau NGN de version 1 internes. Une autre adresse IP (l'adresse "externe") doit être attribuée pour l'accès par les équipements TE et c'est cette adresse (ou cette interface) qu'il faut utiliser pour l'ensemble du trafic de signalisation et de média en provenance ou à destination d'équipements TE. Une autre adresse IP encore (l'"adresse OAMP") doit être attribuée à partir du bloc réservé au trafic OAMP, pour l'accès par les serveurs OAMP.

Afin de préserver la confidentialité des communications des abonnés contre l'écoute clandestine du trafic de signalisation, tous les messages de signalisation doivent faire l'objet d'un transport sécurisé vers les éléments de réseau NGN situés dans la zone "de confiance" ou dans la zone "de confiance mais vulnérable". Pour toutes les connexions à l'initiative d'un élément NBE utilisées pour le transfert d'informations de signalisation vers ces éléments de réseau NGN, il faut établir des canaux sécurisés, avec authentification. Tous les messages de signalisation reçus par un élément NBE à son adresse "interne" sur des canaux non sécurisés doivent être rejetés purement et simplement.

Les flux de média doivent être protégés soit avec un chiffrement pour le transport soit avec l'assurance que le trafic circule uniquement dans un réseau protégé. De plus, la garantie d'adresse d'origine en limite du réseau permettra d'empêcher aux paquets provenant de l'extérieur de déclarer provenir d'une source dont l'adresse appartient au bloc d'adresses de réseau NGN internes.

Pour les paquets de média reçus par l'élément NBE à son adresse externe, il faut vérifier s'ils correspondent à une session active (sur la base de l'échange de signalisation) et il faut comparer l'adresse d'origine à l'adresse d'origine attendue (sur la base de la description de session contenue dans l'échange de signalisation). L'élément NBE doit rejeter purement et simplement les éventuels paquets de média reçus ne correspondant pas à une session active. Il doit aussi vérifier que le débit de paquets est cohérent avec les paramètres de session négociés. Il peut vérifier que la taille de paquet est cohérente avec la session établie. Les paquets de média reçus en provenance d'une adresse IP d'origine ne correspondant pas à un expéditeur de média valable pour cet élément NBE doivent être rejetés purement et simplement.

L'élément NBE doit authentifier toutes les demandes si l'accord de service avec l'abonné le prévoit. Lorsqu'une demande est reçue sur une connexion non chiffrée, chaque demande doit être authentifiée. Lorsqu'une demande est reçue sur une connexion chiffrée qui a été créée sans authentification de l'abonné, la première demande sur cette connexion doit être authentifiée. Lorsqu'une demande est reçue sur une connexion chiffrée qui a été créée avec authentification, aucune autre authentification n'est nécessaire. Il est à noter que les demandes envoyées par le biais d'un élément TE-BE ne seront pas soumises à une authentification de dispositif, étant donné que l'élément TE-BE utilisera une connexion chiffrée vers l'élément NBE. Si la demande provient d'une adresse IP d'origine ne correspondant pas à un expéditeur de demandes valable pour cet élément NBE, elle doit être rejetée purement et simplement. Les demandes de canal sécurisé provenant d'une adresse IP d'origine ne correspondant pas à un expéditeur de demandes valable pour cet élément NBE doivent aussi être rejetées purement et simplement.

8.4 Exigences pour les éléments en limite d'équipements TE situés dans le domaine "non fiable"

Il est difficile d'assurer la sécurité physique des équipements installés sur le site de l'abonné. Il faut bien accepter que la sécurité de ces dispositifs dépend dans une large mesure de l'abonné. Cela étant, chaque dispositif doit prendre des précautions raisonnables contre les attaques, les compromissions ou autres altérations. Afin de préserver la confidentialité des communications des abonnés contre l'écoute clandestine du trafic de signalisation, les messages de signalisation doivent utiliser une connexion de signalisation sécurisée entre l'élément TE-BE et l'élément NBE. L'élément TE-BE peut assurer une fonction de relais de média.

8.4.1 Fonctions OAMP

Toutes les fonctions OAMP entre l'élément TE-BE et le fournisseur NGN doivent être protégées contre l'écoute clandestine. Comme ces fonctions peuvent être assurées dans la bande ou hors bande, ces deux cas sont traités séparément.

8.5 Recommandations en matière de sécurité pour les équipements terminaux situé dans le domaine "non fiable"

Les équipements terminaux (TE, *terminal equipment*) sont souvent hors du contrôle du fournisseur NGN. Il n'est donc pas nécessaire que le fournisseur NGN impose des exigences concernant leurs fonctionnalités de sécurité ou les politiques de sécurité qu'ils doivent appliquer; en revanche, il appartient aux divers éléments en limite de réseau de s'adapter aux politiques choisies par l'abonné et d'assurer le meilleur service possible dans ces conditions.

Les fonctionnalités de sécurité effectives des éléments en limite du fournisseur NGN doivent faire l'objet d'un complément d'étude.

Le trafic de média devrait être protégé contre l'écoute clandestine et les modifications.

Appendice I

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

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

I.1 Contexte

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.

Les services de télécommunication ETS entre différents réseaux nationaux (pays/administrations) doivent être protégés contre les menaces visant la sécurité. Pour pouvoir assurer, par le biais du réseau, la sécurité des services de télécommunication ETS de bout en bout implémentés entre différents réseaux nationaux (pays/administrations), des indications ainsi que des objectifs et exigences de sécurité communs sont nécessaires. La sécurité et la disponibilité des services de télécommunication ETS dépendront de la sécurité de chacun des réseaux intervenant dans une communication de bout en bout.

I.2 Portée/objet

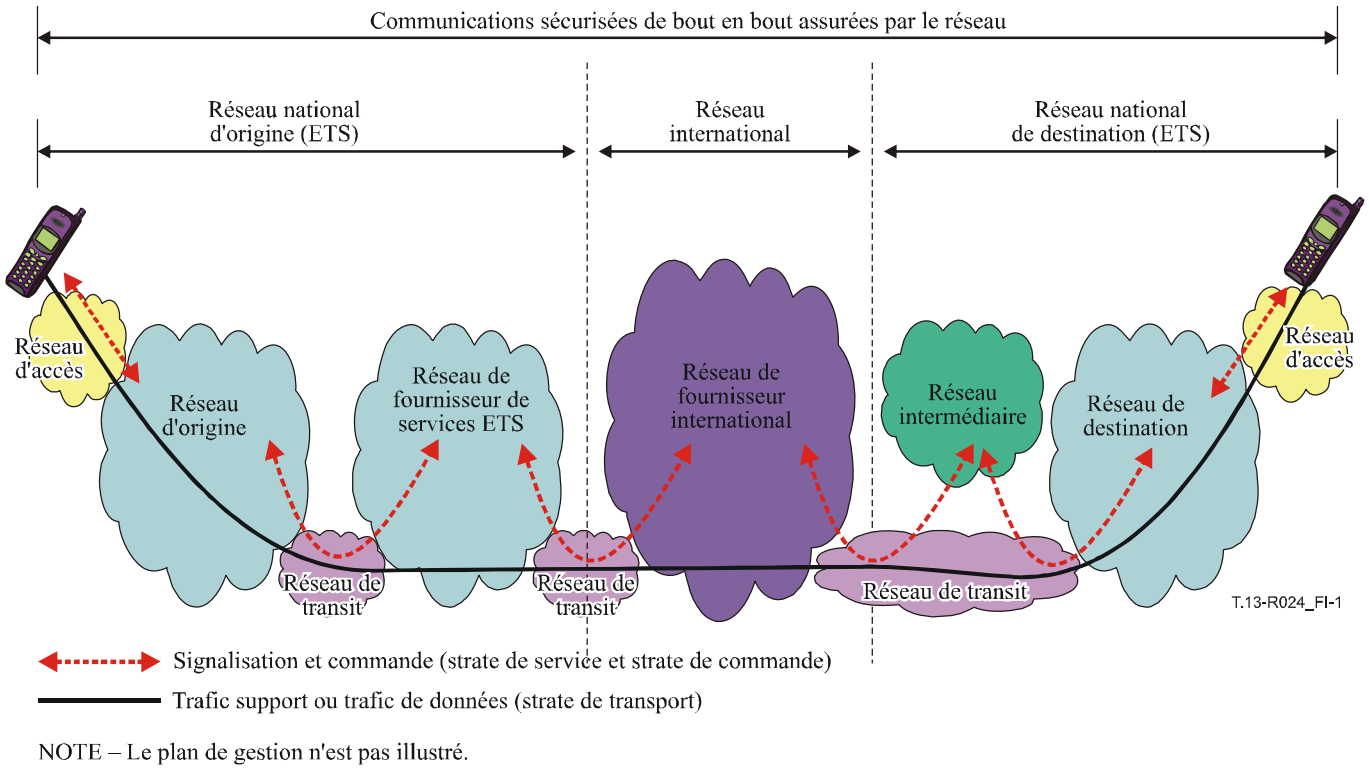
Le présent appendice énonce les objectifs et exigences de sécurité communs et donne des indications permettant d'assurer, par le biais du réseau, la sécurité des services de télécommunication ETS implémentés à travers différents réseaux nationaux (pays/administrations).

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 est limité à la prise en charge par le réseau de la sécurité des services de télécommunication ETS à travers plusieurs réseaux bond par bond. Toutefois, le NGN devrait pouvoir prendre en charge en toute transparence ces fonctions entre homologues.

Le présent appendice ne vise pas à imposer des conditions aux implémentations nationales d'un service ETS mais il vise essentiellement à assurer la prise en charge par le réseau de la sécurité des services de télécommunication ETS (communications prioritaires sécurisées de signaux vocaux, de signaux vidéo, de données et de messagerie).

I.3 Objectifs généraux

L'objectif général est le suivant: les réseaux doivent pouvoir assurer la sécurité des services de télécommunication ETS (communications prioritaires sécurisées de signaux vocaux, de signaux vidéo, de données et de messagerie) à travers différents réseaux nationaux (pays/administrations) et pouvoir protéger la disponibilité de ces services. Pour cela, il faut assurer la sécurité des communications de bout en bout qui peuvent traverser différents domaines de réseaux nationaux et internationaux de fournisseur de réseau (pays/administrations), chaque réseau étant responsable de la sécurité dans son domaine.



NOTE – Le plan de gestion n'est pas illustré.

Figure I.1 – Exemple de communications de bout en bout faisant intervenir différentes implémentations nationales de services ETS

La Figure I.1 illustre des services de télécommunication ETS de bout en bout (par exemple, communications prioritaires de signaux vocaux, de signaux vidéo, de données ou de messagerie) entre deux réseaux nationaux différents. Cet exemple montre que les communications prioritaires de bout en bout pour les services ETS peuvent faire intervenir plusieurs segments de réseau et domaines administratifs (par exemple, réseau d'accès, réseau d'origine, réseau de fournisseur de service ETS, réseau de fournisseur international, réseau intermédiaire et réseau de destination).

Chaque segment de réseau aura des attributions spécifiques en matière de sécurité dans son domaine afin de faciliter la disponibilité et la sécurité de bout en bout des services de télécommunication ETS.

On donne ci-après un ensemble minimal de grandes lignes sur la planification de la sécurité afin de protéger le trafic de signalisation, le trafic support et de données ainsi que les données et informations liées à la gestion (par exemple, informations de profil d'utilisateur) concernant les services ETS:

- Chaque domaine de réseau devrait établir et appliquer des politiques de sécurité et mettre en place des solutions d'atténuation pour les services ETS dans son domaine. Plus précisément, il est recommandé de définir des solutions d'atténuation et des pratiques de sécurité plus strictes que celles qui sont nécessaires pour les services applicatifs généraux et de les mettre en application pour les communications prioritaires ETS. Par exemple, ces solutions et pratiques devraient être conçues de manière à empêcher l'utilisation de ressources ETS par des utilisateurs non autorisés et à empêcher les attaques, notamment les attaques par déni de service.
- Chaque domaine de réseau devrait établir des relations de confiance, des méthodes et des procédures pour l'identification des services de télécommunication ETS ainsi que pour la gestion d'identité et l'authentification des utilisateurs finals et des réseaux à travers

plusieurs domaines administratifs de réseau. Par exemple, les accords sur le niveau de service (SLA, *service level agreement*) devraient définir une politique de sécurité pour l'authentification de chaque domaine lors du transfert et de la réception de services de télécommunication ETS.

- Chaque domaine administratif de réseau devrait établir et appliquer des politiques de sécurité afin de protéger les données et informations liées à la gestion des services ETS (par exemple, informations de profil d'utilisateur).

I.4 Capacités de sécurité générales

Il est recommandé que les capacités de sécurité suivantes soient prises en charge pour les services ETS:

- Capacités de sécurité afin de protéger les services de télécommunication ETS de bout en bout à travers plusieurs domaines de réseau.
- Capacités de sécurité afin de protéger la disponibilité des services de télécommunication ETS à travers plusieurs domaines de réseau.
- Capacités de sécurité afin d'assurer la gestion d'identité et l'authentification des utilisateurs finals et des réseaux à travers plusieurs domaines administratifs de réseau. Il est fortement souhaitable que l'utilisateur final n'interagisse avec un service ETS qu'une fois que les mécanismes de sécurité ont transmis le justificatif d'identité de l'utilisateur final d'un domaine administratif à l'autre.

I.5 Authentification, autorisation et contrôle d'accès

Il est recommandé que l'ensemble minimal suivant de capacités relatives à l'authentification, à l'autorisation et au contrôle d'accès soit pris en charge pour les services ETS:

- Capacités de sécurité afin de protéger les mécanismes utilisés pour authentifier et autoriser les utilisateurs finals et dispositifs ETS.
- Capacités de sécurité afin de protéger les mécanismes utilisés pour rattacher un utilisateur final ETS aux dispositifs associés.
- Capacités de sécurité afin de protéger les mécanismes utilisés pour partager les informations d'authentification (par exemple, confirmer qu'un utilisateur final a été authentifié) à travers plusieurs domaines de réseau.
- Capacités de sécurité afin de protéger les mécanismes utilisés pour l'authentification bilatérale entre un utilisateur final et des entités, notamment les mécanismes utilisés par un utilisateur final ETS pour authentifier l'appelé ou les entités en communication (par exemple, site web, serveur de contenu, etc.).
- Capacités de sécurité afin de protéger les mécanismes utilisés par un réseau pour en authentifier un autre, notamment les mécanismes utilisés pour authentifier le réseau qui transfère des services de télécommunication ETS (par exemple, réseau d'origine) et authentifier le réseau recevant les services de télécommunication ETS (par exemple, réseaux intermédiaires ou de destination).
- Capacités de sécurité afin d'assurer une protection contre l'accès non autorisé aux informations et ressources ETS (par exemple, informations d'utilisateur pour l'authentification de serveurs et de systèmes de gestion).

I.6 Confidentialité et respect de la vie privée

Il est recommandé que l'ensemble minimal suivant de capacités relatives à la confidentialité soit pris en charge:

- Capacités de sécurité afin de protéger la confidentialité du trafic de signalisation et de commande ETS.

- Capacités de sécurité afin de protéger la confidentialité du trafic support et du trafic de données ETS (par exemple, signaux vocaux, signaux vidéo ou données).
- Capacités de sécurité afin de protéger la confidentialité des identités de l'utilisateur final ETS et des entités en communication, ainsi que des informations d'abonnement.
- Capacités de sécurité afin de protéger la confidentialité de l'emplacement de l'utilisateur final ETS.

Il est recommandé que l'ensemble minimal suivant de capacités relatives au respect de la vie privée soit pris en charge:

- Capacités de sécurité afin d'assurer le respect de la vie privée concernant les informations ETS (par exemple, informations déduites de l'observation des activités dans le réseau comme les sites web visités par un utilisateur final, l'emplacement géographique d'un utilisateur final ainsi que les adresses IP et les noms DNS des dispositifs situés dans le réseau d'un fournisseur de service).
- Capacités de sécurité afin d'assurer le respect de la vie privée vis-à-vis de l'observation non autorisée d'informations d'utilisation ETS (par exemple, diagrammes d'utilisation liés au volume de trafic ETS, aux emplacements, aux informations temporelles, à la fréquence, etc.).

I.7 Intégrité des données

Il est recommandé que l'ensemble minimal suivant de capacités relatives à l'intégrité des données soit pris en charge:

- Mécanismes de sécurité afin de protéger l'intégrité des services de télécommunication ETS (par exemple, protection contre les modifications, suppressions, créations ou répétitions non autorisées), notamment les mécanismes utilisés pour signaler l'altération ou la modification d'informations.
- Mécanismes de sécurité afin de protéger l'intégrité des informations ETS (par exemple, marquage de priorité, signaux vocaux, données et signaux vidéo).
- Mécanismes de sécurité afin de protéger l'intégrité des données de configuration propres aux services ETS (par exemple, informations de priorité stockées dans des fonctions de décision de politique, niveau de priorité de l'utilisateur, etc.).

I.8 Communication

Il est recommandé que la capacité minimale suivante soit prise en charge:

- Mécanismes de sécurité afin de protéger contre les intrusions les services de télécommunication ETS à partir d'un utilisateur final ETS autorisé (par exemple, mécanismes permettant d'empêcher l'interception illégale, le piratage ou la répétition de trafic de signalisation ou support/de données ETS).

I.9 Disponibilité

Il est recommandé que l'ensemble minimal suivant de capacités soit pris en charge:

- Mécanismes de sécurité afin de protéger la disponibilité des services de télécommunication ETS (par exemple, protection du trafic de signalisation et de commande et du trafic support/de données ETS contre les attaques, notamment les attaques par déni de service (DoS)).
- Mécanismes de sécurité afin de protéger la disponibilité des ressources et des informations propres aux services ETS (par exemple, bases de données d'authentification/autorisation, informations de priorité stockées dans une fonction de décision de politique, ressources de réseau dédiées contre les attaques, notamment les attaques par déni de service (DoS)).

Bibliographie

Recommandations UIT-T

[b-UIT-T E.106] Recommandation UIT-T E.106 (2003), *Plan international de priorité en période de crise destiné aux opérations de secours en cas de catastrophe.*

[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 E.115] Recommandation UIT-T E.115 (2007), *Assistance informatisée à l'annuaire.*

[b-UIT-T M.3016.2] Recommandation UIT-T M.3016.2 (2005), *Sécurité pour le plan de gestion: services de sécurité.*

[b-UIT-T M.3016.3] Recommandation UIT-T M.3016.3 (2005), *Sécurité pour le plan de gestion: mécanisme de sécurité.*

[b-UIT-T M.3016.4] Recommandation UIT-T M.3016.4 (2005), *Sécurité pour le plan de gestion: Formulaire des profils de sécurité.*

[b-UIT-T M.3060] Recommandation UIT-T M.3060/Y.2401 (2006), *Principes pour la gestion des réseaux de prochaine génération.*

[b-UIT-T X.1121] Recommandation UIT-T X.1121 (2004), *Cadre général des technologies de la sécurité pour les communications mobiles de données de bout en bout.*

[b-UIT-T X.1122] Recommandation UIT-T X.1122 (2004), *Lignes directrices pour la réalisation de systèmes mobiles sécurisés basés sur l'infrastructure de clés publiques (PKI).*

[b-UIT-T Y.1271] Recommandation UIT-T Y.1271 (2004), *Cadres généraux applicables aux spécifications et aux capacités de réseau pour la prise en charge des télécommunications d'urgence sur les réseaux à commutation de circuits et à commutation de paquets en cours d'évolution.*

[b-UIT-T Y.2000-Sup.1] Supplément 1 aux Recommandations UIT-T de la série Y.2000 (2006), *Domaine d'application des réseaux de prochaine génération de version 1.*

[b-UIT-T Y.2111] Recommandation UIT-T Y.2111 (2006), *Fonctions de commande de ressource et d'admission dans les réseaux de prochaine génération.*

Documents de l'ETSI TISPAN

[b-ETSI TR 187.002] ETSI TR 187 002 V.1.1.1 (2006), *Telecommunications and Internet converged services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN SEC); Threat and Risk Analysis.*

[b-ETSI TS 187.001] ETSI TS 187 001 V.1.1.1 (2006), *Telecommunications and Internet converged services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements.*

[b-ETSI TS 187.003] ETSI TS 187 003 V.1.1.1 (2006), *Telecommunications and Internet converged services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture.*

Documents de l'ETSI/3GPP

[b-3GPP TS 33.102] 3GPP TS 33.102 (2007), *3G security; Security architecture.*

[b-3GPP TS 33.103] 3GPP TS 33.103 (2001), *3G security; Integration guidelines.*

[b-3GPP TS 33.110] 3GPP TS 33.110 (2007), *Key establishment between a UICC and a terminal.*

[b-3GPP TS 33.120] 3GPP TS 33.120 (2001), *Security Objectives and Principles.*

[b-3GPP TS 33.200] 3GPP TS 33.200 (2004), *3G security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security.*

[b-3GPP TS 33.203] 3GPP TS 33.203 (2007), *3G security; Access security for IP-based services.*

[b-3GPP TS 33.204] 3GPP TS 33.204 (2007), *3G security; Network Domain Security (NDS); TCAP user security.*

[b-3GPP TS 33.210] 3GPP TS 33.210 (2007), *3G security; Network Domain Security; IP network layer security.*

[b-3GPP TS 33.220] 3GPP TS 33.220 (2007), *Generic Authentication Architecture (GAA); Generic bootstrapping architecture.*

[b-3GPP TS 33.310] 3GPP TS 33.310 (2007), *Network Domain Security (DNS); Authentication Framework (AF).*

[b-3GPP TR 33.901] 3GPP TR 33.901 (2001), *Criteria for cryptographic algorithm design process.*

[b-3GPP TR 33.902] 3GPP TR 33.902 (2001), *Formal Analysis of the 3G Authentication Protocol.*

[b-3GPP TR 33.908] 3GPP TR 33.908 (2001), *3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms.*

[b-3GPP TR 33.909] 3GPP TR 33.909 (2001), *3G Security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP authentication and key generation functions.*

[b-3GPP TR 33.918] 3GPP TR 33.918 (2007), *Generic Authentication Architecture (GAA); Early implementation of Hypertext Transfer Protocol over Transport Layer Security (HTTPS) connection between a Universal Integrated Circuit Card (UICC) and a Network Application Function (NAF).*

[b-3GPP TR 33.919] 3GPP TR 33.919 (2007), *3G Security; Generic Authentication Architecture (GAA); System description.*

[b-3GPP TR 33.920] 3GPP TR 33.920 (2007), *SIM card based Generic Bootstrapping Architecture (GBA); Early implementation feature.*

[b-3GPP TR 33.980] 3GPP TR 33.980 (2007), *Liberty Alliance and 3GPP security interworking; Interworking of Liberty Alliance Identity Federation Framework (ID-FF), Identity Web Services Framework (ID-WSF) and Generic Authentication Architecture (GAA).*

[b-ETSI TR 133.901] ETSI TR 133.901 V4.0.0 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security – Criteria for cryptographic Algorithm design process.*

[b-ETSI TR 133.902] ETSI TR 133.902 V4.0.0 (2001), *Universal Mobile Telecommunications System (UMTS); Formal Analysis of the 3G Authentication Protocol.*

[b-ETSI TR 133.908] ETSI TR 133.908 (2001), *Universal Mobile Telecommunications System (UMTS); Security Algorithms Group of Experts (SAGE); General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms.*

[b-ETSI TR 133.909] ETSI TR 133.909 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP authentication and key generation functions.*

[b-ETSI TR 133.919] ETSI TR 133.919 V6.2.0 (2005), *Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); System description.*

[b-ETSI TS 133.102] ETSI TS 133 102 V7.1.0 (2006), *Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture.*

[b-ETSI TS 133.103] ETSI TS 133 103 V4.2.0 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security; Integration Guidelines.*

[b-ETSI TS 133.120] ETSI TS 133 120 V4.0.0 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security; Security Principles and Objectives.*

[b-ETSI TS 133.200] ETSI TS 133 200 V6.1.0 (2005), *Universal Mobile Telecommunications System (UMTS); 3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security.*

[b-ETSI TS 133.203] ETSI TS 133 203 V6.10.0 (2006), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services.*

[b-ETSI TS 133.210] ETSI TS 133 210 V7.2.0 (2006), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS).*

[b-GPP TS 133.220] ETSI TS 133 220 V7.8.0 (2007), *Digital cellular telecommunications system; (Phase 2+); Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Generic bootstrapping architecture.*

[b-ETSI TS 133.310] ETSI TS 133 310 V7.1.0 (2006), *Universal Mobile Telecommunications System (UMTS); Network domain security; Authentication framework (NDS/AF).*

Documents de l'ATIS/3GPP2

[b-GPP2 S.S0086] 3GPP2 S.S0086 (2004), *IMS Security Framework.*

Documents IETF RFC liés à la sécurité IPsec

[b-IETF RFC 2085] IETF RFC 2085 (1997), *HMAC-MD5 IP Authentication with Replay Prevention.*

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

[b-IETF RFC 2404] IETF RFC 2404 (1998), *The Use of HMAC-SHA-1-96 within ESP and AH.*

[b-IETF RFC 2405] IETF RFC 2405 (1998), *The ESP DES-CBC Cipher Algorithm With Explicit IV.*

[b-IETF RFC 2410] IETF RFC 2410 (1998), *The NULL Encryption Algorithm and Its Use With IPsec.*

[b-IETF RFC 2411] IETF RFC 2411 (1998), *IP Security Document Roadmap.*

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

[b-IETF RFC 2709] IETF RFC 2709 (1999), *Security Model with Tunnel-mode IPsec for NAT Domains.*

[b-IETF RFC 2857] IETF RFC 2857 (2000), *The Use of HMAC-RIPEMD-160-96 within ESP and AH.*

[b-IETF RFC 3526] IETF RFC 3526 (2003), *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE).*

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

[b-IETF RFC 3664] IETF RFC 3664 (2004), *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE).*

[b-IETF RFC 4109] IETF RFC 4109 (2005), *Algorithms for Internet Key Exchange version 1 (IKEv1).*

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

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

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

[b-IETF RFC 4304] IETF RFC 4304 (2005), *Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP).*

[b-IETF RFC 4305] IETF RFC 4305 (2005), *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH).*

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

[b-IETF RFC 4307] IETF RFC 4307 (2005), *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2).*

[b-IETF RFC 4308] IETF RFC 4308 (2005), *Cryptographic Suites for IPsec.*

[b-IETF RFC 4309] IETF RFC 4309 (2005), *Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP).*

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

Documents IETF RFC liés aux extensions S/MIME

[b-IETF RFC 2311] IETF RFC 2311 (1998), *S/MIME Version 2 Message Specification.*

[b-IETF RFC 2312] IETF RFC 2312 (1998), *S/MIME Version 2 Certificate Handling.*

[b-IETF RFC 3565] IETF RFC 3565 (2003), *Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS).*

[b-IETF RFC 3657] IETF RFC 3657 (2004), *Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS).*

[b-IETF RFC 3850] IETF RFC 3850 (2004), *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling.*

[b-IETF RFC 3851] IETF RFC 3851 (2004), *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification.*

[b-IETF RFC 3852] IETF RFC 3852 (2004), *Cryptographic Message Syntax.*

[b-IETF RFC 4134] IETF RFC 4134 (2005), *Examples of S/MIME Messages.*

Documents IETF RFC liés à la sécurité TLS

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

[b-IETF RFC 2817] IETF RFC 2817 (2000), *Upgrading to TLS Within HTTP/1.1.*

[b-IETF RFC 2818] IETF RFC 2818 (2000), *HTTP Over TLS.*

[b-IETF RFC 3268] IETF RFC 3268 (2002), *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS).*

[b-IETF RFC 3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions.*

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

Divers documents IETF RFC ayant trait à la sécurité

[b-IETF i-d.SIPUAP] IETF internet-draft work in progress, draft-ietf-sipping-config-framework-08.txt (March 6, 2006), *A Framework for Session Initiation Protocol User Agent Profile Delivery.*

[b-IETF RFC 3489] IETF RFC 3489 (2003), *STUN – Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs).*

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

[b-IETF RFC 3715] IETF RFC 3715 (2004), *IPsec-Network Address Translation (NAT) Compatibility Requirements.*

[b-IETF RFC 3847] IETF RFC 3847 (2004), *Restart Signaling for Intermediate System to Intermediate System (IS-IS).*

[b-IETF RFC 3948] IETF RFC 3948 (2005), *UDP Encapsulation of IPsec ESP Packets.*

Documents IETF RFC liés au système DNS

[b-IETF RFC 4033] IETF RFC 4033 (2005), *DNS Security Introduction and Requirements.*

[b-IETF RFC 4034] IETF RFC 4034 (2005), *Resource Records for the DNS Security Extensions.*

[b-IETF RFC 4035] IETF RFC 4035 (2005), *Protocol Modifications for the DNS Security Extensions.*

Documents de la TIA

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

[b-TIA-1053] TIA Standard TIA-1053 (2005), *Broadcast/Multicast Security Framework.*

[b-TIA-1091] TIA Standard TIA-1091 (2006), *IMS Security Framework.*

Documents de l'ARIB

[b-ARIB-SS0078] ARIB STD-T64 S.S0078-0 v1.0 (2002), *Common Security Algorithms*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Disponible
Série C	Disponible
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	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
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 W	Disponible
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, 2008