Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

H.235.9

(09/2005)

SÉRIE H: SYSTÈMES AUDIOVISUELS ET MULTIMÉDIAS

Infrastructure des services audiovisuels – Aspects système

Cadre de sécurité H.323: prise en charge des passerelles de sécurité dans les systèmes H.323

Recommandation UIT-T H.235.9

RECOMMANDATIONS UIT-T DE LA SÉRIE H

SYSTÈMES AUDIOVISUELS ET MULTIMÉDIAS

CARACTÉRISTIQUES DES SYSTÈMES VISIOPHONIQUES	H.100–H.199
INFRASTRUCTURE DES SERVICES AUDIOVISUELS	
Généralités	H.200–H.219
Multiplexage et synchronisation en transmission	H.220–H.229
Aspects système	**H.230–H.239**
Procédures de communication	H.240–H.259
Codage des images vidéo animées	H.260–H.279
Aspects liés aux systèmes	H.280–H.299
Systèmes et équipements terminaux pour les services audiovisuels	H.300–H.349
Architecture des services d'annuaire pour les services audiovisuels et multimédias	H.350–H.359
Architecture de la qualité de service pour les services audiovisuels et multimédias	H.360–H.369
Services complémentaires en multimédia	H.450–H.499
PROCÉDURES DE MOBILITÉ ET DE COLLABORATION	
Aperçu général de la mobilité et de la collaboration, définitions, protocoles et procédures	H.500–H.509
Mobilité pour les systèmes et services multimédias de la série H	H.510–H.519
Applications et services de collaboration multimédia mobile	H.520–H.529
Sécurité pour les systèmes et services multimédias mobiles	H.530–H.539
Sécurité pour les applications et services de collaboration multimédia mobile	H.540–H.549
Procédures d'interfonctionnement de la mobilité	H.550–H.559
Procédures d'interfonctionnement de collaboration multimédia mobile	H.560–H.569
SERVICES À LARGE BANDE ET MULTIMÉDIAS TRI-SERVICES	
Services multimédias à large bande sur VDSL	H.610–H.619

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

Recommandation UIT-T H.235.9

Cadre de sécurité H.323:
Prise en charge des passerelles de sécurité dans les systèmes H.323

Résumé

La présente Recommandation définit une méthode permettant de découvrir des passerelles de sécurité sur le trajet de signalisation reliant deux entités H.323 en communication, et de partager des informations relatives à la sécurité entre un portier et les passerelles de sécurité afin de préserver l'intégrité de la signalisation ainsi que le secret des communications.

Source

La Recommandation UIT-T H.235.9 a été approuvée le 13 septembre 2005 par la Commission d'études 16 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

Mots clés

Passerelle, sécurité, signalisation.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) 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 responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

© UIT 2006

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

Introduction

L'utilisation de pare-feu et/ou de dispositifs de traduction d'adresse de réseau pour assurer la sécurité du trafic entre deux régions du réseau sous des contrôles administratifs différents pose problème aux protocoles de signalisation de téléphonie qui doivent assurer l'échange des adresses de réseau aux fins de l'échange des messages de signalisation et des médias.

La Rec. UIT-T H.235.5 présente un cadre dans lequel un point d'extrémité et son portier, ou deux portiers, peuvent utiliser les messages RAS initiaux pour négocier un ensemble de secrets forts partagés entre eux, et se servir de ces secrets pour chiffrer certaines parties de messages RAS et de signalisation d'appel ultérieurs, et enfin pour authentifier ces messages. La méthode ne s'applique qu'à la signalisation à routage par portier. Des méthodes et des profils de sécurité analogues sont définis dans les Recommandations UIT-T H.235.1, H.235.2 et H.235.3. Cette sécurité peut entrer en conflit avec les passerelles de couche Application (ALG, *application layer gateway*) qui interconnectent des domaines de réseau et manipulent les adresses de signalisation et de transport de média acheminées dans les messages RAS et/ou de signalisation d'appel H.225.0 et entraîner l'échec de l'authentification des messages ainsi modifiés au niveau de la destination.

La présente Recommandation décrit un moyen simple par lequel le portier peut être informé des passerelles ALG situées sur un trajet de signalisation, et par lequel il peut partager la clé d'authentification de signalisation négociée avec ces passerelles. Les passerelles ALG pourront ainsi manipuler des données non privées, en particulier des adresses de transport, dans les messages de signalisation, et ensuite authentifier le résultat avant de transmettre les messages modifiés. Ces dispositifs sont dénommés "passerelles de sécurité" (SG, *security gateway*) dans le texte qui suit. Cette technique permet de préserver le secret des communications de bout en bout pour tout élément chiffré dans la signalisation.

Recommandation UIT-T H.235.9

Cadre de sécurité H.323: prise en charge des passerelles de sécurité dans les systèmes H.323

1 Domaine d'application

La présente Recommandation s'applique à tout portier ou point d'extrémité qui utilise les protocoles RAS H.225.0, dans les scénarios faisant intervenir une ou plusieurs passerelles de sécurité présentant le comportement prescrit.

2 Références

2.1 Références normatives

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.

– Recommandation UIT-T H.225.0 (2003), *Protocoles de signalisation d'appel et paquétisation des flux monomédias pour les systèmes de communication multimédias en mode paquet*.

– Recommandation UIT-T H.235.0 (2005), *Cadre de sécurité H.323: cadre de sécurité pour les systèmes multimédias de la série H (systèmes H.323 et autres systèmes de type H.245)*.

– Recommandation UIT-T H.235.1 (2005), *Cadre de sécurité H.323: profil de sécurité de base.*

– Recommandation UIT-T H.235.2 (2005), *Cadre de sécurité H.323: profil de sécurité avec signature.*

– Recommandation UIT-T H.235.3 (2005), *Cadre de sécurité H.323: profil de sécurité hybride.*

– Recommandation UIT-T H.235.5 (2005), *Cadre de sécurité H.323: cadre de l'authentification sécurisée pendant l'échange de messages RAS au moyen de secrets partagés faibles.*

– Recommandation UIT-T H.245 (2005), *Protocole de commande pour communications multimédias*.

– Recommandation UIT-T H.323 (2003), *Systèmes de communication multimédia en mode paquet*.

2.2 Références informatives

– IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

– IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*.

– IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.

3 Définitions

La présente Recommandation définit les termes suivants:

3.1 passerelle de couche Application (ALG, *application layer gateway*): dispositif compatible avec des protocoles qui interconnectent deux régions de réseau ou plus et qui est capable d'interpréter et de modifier les protocoles de couche Application afin de fournir les traductions d'adresse de transport ainsi que d'autres fonctions. Une passerelle ALG peut assurer les fonctions de traduction d'adresse de réseau (NAT) et de pare-feu au niveau transport de façon interne ou peut les commander de façon externe.

3.2 adresse locale: adresse de transport figurant dans un domaine d'adresse locale.

3.3 passerelle média (MG, *media gateway*): dispositif qui interconnecte deux domaines de réseau ou plus et qui peut être commandé par un autre dispositif (par exemple, une passerelle de sécurité) afin de fournir des flux de média commandés entre deux domaines. La passerelle MG assure en fait les fonctions de traduction d'adresse de réseau ou de pare-feu programmable et fonctionne au niveau de la couche Transport ou à des niveaux inférieurs.

3.4 traduction d'adresse de réseau (NAT, *network address translation*): opération qui consiste à mapper des adresses de transport de réseau d'un domaine de réseau à un autre.

3.5 micro-trou: trajet de flux à travers une passerelle de sécurité (ou une passerelle de média sous son contrôle) que des paquets ou des messages sont autorisés à emprunter pour passer d'un domaine à un autre. Un micro-trou est généralement caractérisé par quatre adresses de transport (l'adresse d'origine dans le domaine A, l'adresse du domaine A dans la passerelle de sécurité, l'adresse du domaine B dans la passerelle de sécurité et l'adresse de destination dans le domaine B), et par d'autres caractéristiques telles que le protocole de transport et la direction. L'adresse d'origine peut ne pas être spécifiée (par exemple pour un port d'écoute).

3.6 domaine: région du réseau qui partage un espace d'adresse de réseau commun; on part du principe que des domaines différents utilisent des espaces d'adresse incompatibles, conflictuels ou privés.

3.7 passerelle de sécurité (SG, *security gateway*): dispositif installé entre au moins deux régions de réseau IP, qui assure des fonctions de sécurité telles que la validation ou la limitation de flux de paquets et le mappage d'adresses de transport entre deux régions du réseau. Dans le cadre de la présente Recommandation, on part du principe que la passerelle de sécurité est une passerelle au niveau application qui est compatible avec les protocoles de signalisation H.323.

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

ALG passerelle de couche Application (*application layer gateway*)

GCF confirmation de portier (*GatekeeperConfirm*)

GK portier (*gatekeeper*)

GRJ rejet de portier (*GatekeeperReject*)

LCF confirmation d'emplacement (*LocationConfirm*)

LRQ demande de localisation (*LocationRequest*)

MG passerelle média (*media gateway*)

NAT traduction d'adresse de réseau (*network address translation*)

OID identificateur d'objet (*object identifier*)

RAS enregistrement, admission et statut (*registration admission and status*)

SG passerelle de sécurité (*security gateway*)

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

5 Conventions

La présente Recommandation définit divers identificateurs d'objet (OID, *object identifier*) destinés à la signalisation des capacités relatives à la sécurité, des procédures et des algorithmes de sécurité. Ces identificateurs renvoient à une arborescence de valeurs attribuées pouvant provenir de sources extérieures ou faisant partie d'une arborescence d'identificateurs d'objets gérés par l'UIT-T. Les identificateurs d'objet qui concernent spécifiquement la Rec. UIT-T H.235 se présentent de la manière suivante dans le texte:

"OID" = {itu-t (0) recommendation (0) h (8) 235 version (0) **V N**} où **V** représente symboliquement un simple chiffre décimal précisant la version correspondante de la Rec. UIT-T H.235; par exemple 1, 2, 3 ou 4. **N** représente symboliquement un nombre décimal identifiant de manière univoque l'instance de l'identificateur d'objet et par conséquent, la procédure, l'algorithme ou la capacité de sécurité.

L'identificateur d'objet codé en ASN.1 est donc constitué d'une séquence de nombres. Pour des raisons de commodité, pour chaque OID, une notation mnémonique textuelle condensée telle "OID" est utilisée dans le texte. Un mappage est donné entre chaque chaîne OID et la séquence de nombres ASN.1. Les implémentations conformes à la Rec. UIT-T H.235 doivent uniquement utiliser les nombres codés en ASN.1.

Hypothèses de base

La présente Recommandation examine un modèle de réseau IP dans lequel des régions de réseau multiples, appelées domaines, sont interconnectées par des dispositifs appelés passerelles de sécurité (SG, *security gateway*), qui sont compatibles avec le protocole H.323 et qui sont destinés à commander les flux d'information entre les domaines de réseau qu'ils interconnectent. Les passerelles de sécurité sont censées examiner les messages de signalisation circulant entre les domaines, assurer leur validité, extraire les informations relatives aux adresses de transport échangées, utiliser ces informations de transport pour construire des trajets de flux appropriés entre les domaines et, enfin, modifier en conséquence les adresses de transport pour le domaine auquel le message est transmis. Les passerelles de sécurité doivent évidemment faire en sorte que les trajets de signalisation passent par elles, mais elles peuvent commander un autre dispositif afin de prendre en charge tout flux de média établi. Le protocole de commande appliquée entre la passerelle de sécurité et la "passerelle média" n'est pas spécifié dans la présente Recommandation.

Afin de mettre les services d'un portier appartenant à un domaine à la disposition de points d'extrémité ou de portiers appartenant à un autre domaine, une passerelle de sécurité peut fournir une adresse de découverte de portier dans chaque domaine qu'elle dessert, dans lequel ne figure aucun portier connu. La passerelle SG transmettrait ensuite tout message de découverte, reçu à l'une de ces adresses, au portier en question après avoir effectué tout traitement nécessaire du message H.323. Un exemple de configuration, représentant un portier desservant des points d'extrémité dans plusieurs domaines de réseau, est illustré dans la Figure 1.

En fait, les passerelles de sécurité doivent représenter le portier dans chacun des domaines qu'elles desservent (à l'exception évidemment du domaine dans lequel figure le portier; par exemple, le domaine A pour le portier A sur le schéma). La passerelle de sécurité B fournit des adresses de découverte des deux portiers représentés dans la figure; elle assure donc un trajet entre deux portiers pour la signalisation des messages LRQ/LCF. A noter également qu'une passerelle SG ne doit pas nécessairement fournir l'accès à chaque portier figurant dans chaque domaine. Par exemple, dans la Figure 1, la passerelle de sécurité A peut être configurée de manière à fournir uniquement une adresse de découverte du portier A dans le domaine B.

On part du principe que chaque portier connaît un nom unique pour chaque passerelle SG figurant dans le système et que les deux entités partagent également un secret fort sur le plan cryptographique qui leur permet de communiquer de façon sûre. La manière dont ces identités et les clés correspondantes sont négociées ou échangées est examinée ci-après, mais n'est pas l'objet principal de la présente Recommandation. Les secrets partagés devraient être uniques pour chaque paire passerelle SG/portier. Afin de faire en sorte que le trafic RAS et de signalisation d'appel passe par les passerelles de sécurité, on part du principe que celles-ci modifieront les adresses RAS et de signalisation d'appel échangées.

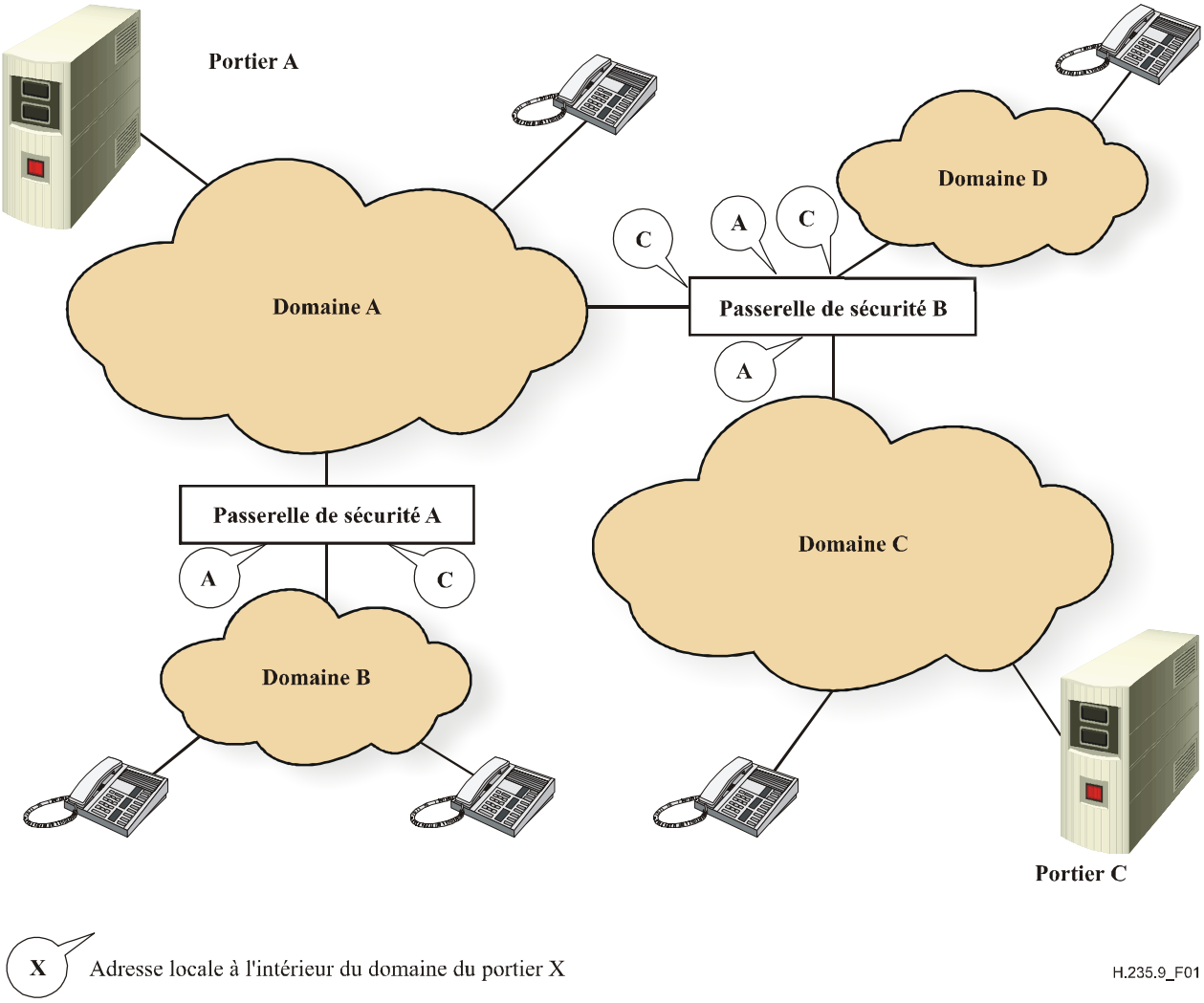


Figure 1/H.235.9 – Configuration de passerelle de sécurité

Par ailleurs, le moyen par lequel le routage et/ou la traduction d'adresse pour le processus de découverte initial est établi, qui n'est pas le thème principal de la présente Recommandation, est examiné ci-après. L'établissement d'adresses ultérieures ainsi que toute traduction nécessaire sont censés être réalisés dans le cadre du fonctionnement des passerelles de sécurité.

6 Fonctionnement de base

Dans la description qui suit, on part du principe que chaque passerelle de sécurité présente dans le système s'est enregistrée auprès de chaque portier qu'elle est censée desservir. Cette opération sera décrite en détail ultérieurement. En ce qui concerne le fonctionnement de base, on suppose que la passerelle SG s'est identifiée auprès de chaque portier, avec lequel elle partage un secret unique fort,

et fournit une ou plusieurs adresses "locales" de découverte de ce portier. Les détails concernant l'enregistrement de la passerelle SG seront examinés dans un paragraphe ultérieur. Les paragraphes qui suivent décrivent la manière dont les passerelles de sécurité participent à l'enregistrement des points d'extrémité afin d'obtenir un accès à la clé d'authentification de bout en bout négociée entre le portier et le point d'extrémité.

6.1 Découverte d'un portier par un point d'extrémité

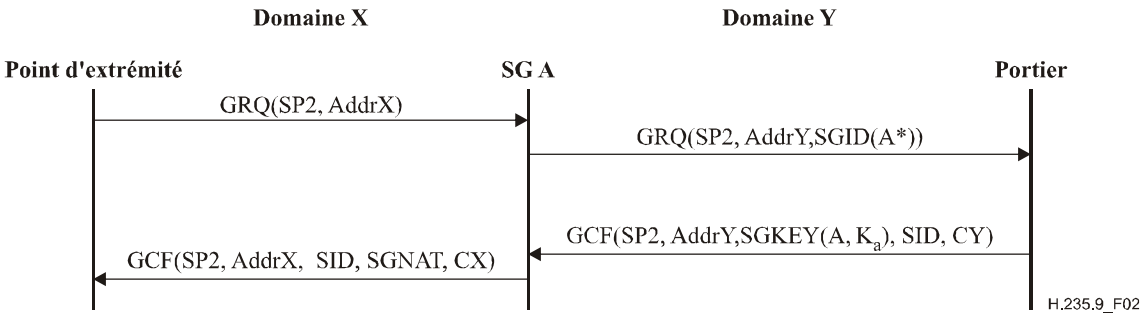
Lorsqu'un point d'extrémité envoie un message de demande de portier (GRQ, *gatekeeper request*) à une adresse de découverte de portier et que ce message est transmis à un ou plusieurs portiers par l'intermédiaire d'une passerelle SG, cette dernière peut ajouter un jeton **ClearToken** à l'élément **token** du message GRQ étant donné qu'elle manipule les adresses à l'intérieur de ce message. Ce **ClearToken** sera identifié comme un jeton d'identification de passerelle SG (jeton id-SG) (au moyen de son **tokenOID**) et contiendra une chaîne d'identification identifiant de façon univoque la passerelle SG. Celle-ci devrait supprimer du profil **authenticationCapability** du message GRQ tout mécanisme **AuthenticationMechanism** particulier (par exemple, TLS selon les normes RFC 2246 et RFC 3546 ou IPsec selon la norme RFC 2401), dont elle ne peut prendre en charge la procédure d'authentification de message. Cela garantit que le portier choisira un profil compatible avec la passerelle de sécurité. La première passerelle de sécurité qui reçoit le message GRQ doit inclure un élément identifiant l'adresse de découverte à laquelle elle a reçu le message GRQ du point d'extrémité.

On suppose implicitement que chaque passerelle SG manipulera tout champ d'adresse de signalisation à l'intérieur du message GRQ et de tous les messages RAS ultérieurs afin de faire en sorte que tous les messages de signalisation passent par la passerelle SG aux fins du traitement des adresses.

6.2 Distribution de la clé d'authentification au point d'extrémité

Lorsque le message GRQ arrivera au niveau du portier (GK, *gatekeeper*), ce dernier le traitera, y compris le jeton id-SG. En partant du principe qu'il jouera le rôle de portier du point d'extrémité, le portier se préparera à renvoyer un message de confirmation de portier (GCF, *GatekeeperConfirm*) au point d'extrémité. Il inclura alors dans ce message le mécanisme **AuthenticationMechanism** choisi ainsi qu'un **ClearToken** clé-SG (identifié par son **tokenOID**) pour la passerelle de sécurité identifiée par le jeton id-SG reçu. Ce jeton de clé inclura l'identification de la passerelle SG, l'identification du portier GK, un vecteur d'initialisation ainsi que la clé d'authentification de session chiffrée au moyen du vecteur d'initialisation et du secret partagé entre la passerelle SG et le portier. L'algorithme de chiffrement doit être négocié au cours de l'enregistrement de la passerelle SG, ou doit être préconfiguré.

Sur le trajet de retour en direction du point d'extrémité, le message GCF passe par la passerelle SG qui a fourni le jeton id-SG. Celle-ci doit analyser le message afin d'obtenir l'identificateur de session ainsi que son propre jeton de clé. Elle doit ensuite déchiffrer la clé d'authentification de session et l'utiliser pour authentifier le message reçu. Si le message est authentique, la passerelle SG manipulera les adresses de transport comme il convient, puis reconstruira le message sans son propre jeton de clé-SG, insérera un jeton NAT-SG s'il n'y en a pas déjà un, et authentifiera le message reconstruit avant de l'envoyer. L'identificateur de session et la clé d'authentification doivent être préservés en vue de leur utilisation avec les messages RAS et de signalisation d'appel ultérieurs pour cette session. La séquence de base des messages passant par une passerelle SG unique est représentée dans la Figure 2. A noter par ailleurs que la passerelle SG doit préparer les micro-trous déterminés à partir du message GCF (par exemple, un micro-trou RAS et d'autres micro-trous pour des adresses de portier).

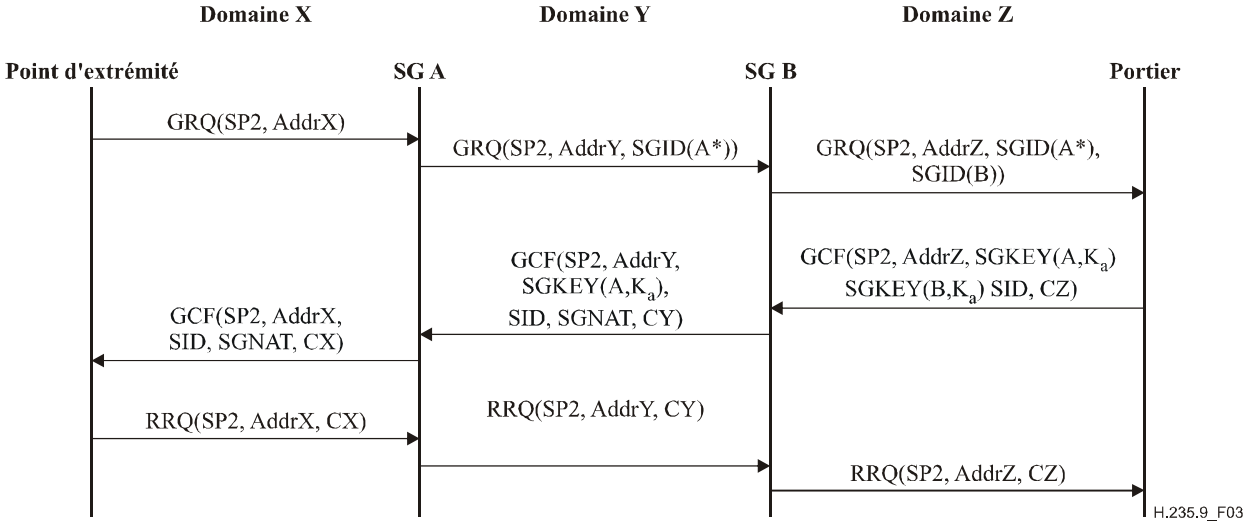


SP2 = profil de sécurité H.235.5
Addrx = adresses dans le domaine x
SGID(A*) = ClearToken id-SG indiquant la présence de la passerelle SG A
(* indique que le SGID inclut une adresse de découverte utilisée par le message GRQ)
SID = identificateur de session (attribué par le portier)
Ka = clé d'authentification de message pour l'identificateur SID
SGKEY(A, K_a) = ClearToken clé-SG avec K_a chiffrée au moyen de la clé secrète de A
SGNAT = ClearToken NAT-SG
Cx = somme de contrôle du message (calculée au moyen de la K_a négociée) dans le domaine x

Figure 2/H.235.9 – Echange de base de messages passant par une passerelle SG

Ce schéma peut facilement s'étendre à une série de passerelles SG situées entre le point d'extrémité et le portier. Chaque passerelle SG ajoute son propre ClearToken dans le message GRQ, au moment où celui-ci la traverse, et retire son propre ClearToken de réponse du message GCF au moment où celui-ci est transmis en retour, du portier vers le point d'extrémité. La première passerelle SG sur le trajet de retour en direction du point d'extrémité doit insérer le jeton NAT-SG dans le message GCF. Cette opération est représentée dans la Figure 3. Pour le traitement des messages RAS ultérieurs, on montre la transformation des adresses de transport dans un message RRQ et la somme de contrôle recalculée.

Une séquence analogue peut être réalisée dans un échange de messages LRQ/LCF, au moyen des mêmes éléments de message, les résultats pouvant être utilisés pour traiter et authentifier les messages de signalisation ultérieurs pour cette session.



SP2 = profil de sécurité H.235.5
Addrx = adresses dans le domaine x
SGID(A*) = ClearToken id-SG indiquant la présence de la passerelle SG A
(* indique la présence d'une adresse de découverte utilisée par le point d'extrémité)
SID = identificateur de session (attribué par le portier)
Ka = clé d'authentification de message pour l'identificateur SID
SGKEY(A, K_a) = ClearToken clé-SG avec K_a chiffrée au moyen de la clé secrète de A
SGNAT = ClearToken NAT-SG
Cx = somme de contrôle du message dans le domaine x

Figure 3/H.235.9 – Echange à deux niveaux de messages passant par deux passerelles SG

6.3 Manipulation des adresses

Etant donné que chaque message de signalisation H.225.0 ou H.245 passe par la passerelle SG, cette dernière doit examiner et modifier toutes les adresses de transport qui y sont acheminées, de façon qu'elles soient valides dans le domaine suivant à travers lequel le message circulera. Cela suppose que la passerelle SG peut avoir à créer de nouveaux micro-trous pour prendre en charge les flux de signalisation et/ou de média associés que ces adresses sont censées établir. A noter que certaines adresses représentent des ports d'écoute qui doivent être ouverts "au cas où"; un micro-trou entièrement spécifié sera créé dans le cas où un paquet arrive au port d'écoute.

Chaque passerelle SG peut examiner chaque adresse de transport de destination reçue pour vérifier que celle-ci représente effectivement une adresse de destination sur cette passerelle. Considérons l'exemple de configuration de domaines et de trajets de média donnée dans la Figure 4. Un flux de média entre un point d'extrémité situé dans le domaine B et un point d'extrémité situé dans le domaine C doit circuler à travers les passerelles SG B et C, comme le montre le flux "1". Si la passerelle SG B n'effectue aucun traitement spécial, un flux de média entre deux points d'extrémité situés dans le domaine B suivra un trajet équivalent qui le mènera au domaine A et le ramènera au domaine B, comme le montre le flux "2". Si elle constate que les adresses d'origine et de destination fournies au flux dans le domaine A sont en fait des adresses sur la passerelle SG B, celle-ci peut "court-circuiter" le flux de deux manières: soit en acheminant le flux en interne, comme le montre le flux "3" (représenté sur la passerelle SG C pour des raisons de clarté), soit, si elle constate que les deux points d'extrémité appartiennent au domaine B, en modifiant les adresses des points d'extrémité dans le domaine B afin d'acheminer le flux directement entre les points d'extrémité, comme le montre le flux "4". A noter que les adresses de "point d'extrémité", telles que vues par la passerelle SG B, peuvent en fait être des adresses sur une passerelle SG (appelée D) reliée à un autre domaine. Une fois que la passerelle SG B a modifié les adresses de façon à effectuer un routage "direct" entre les adresses sur la passerelle SG D, cette dernière peut ensuite court-circuiter les flux de la même manière.

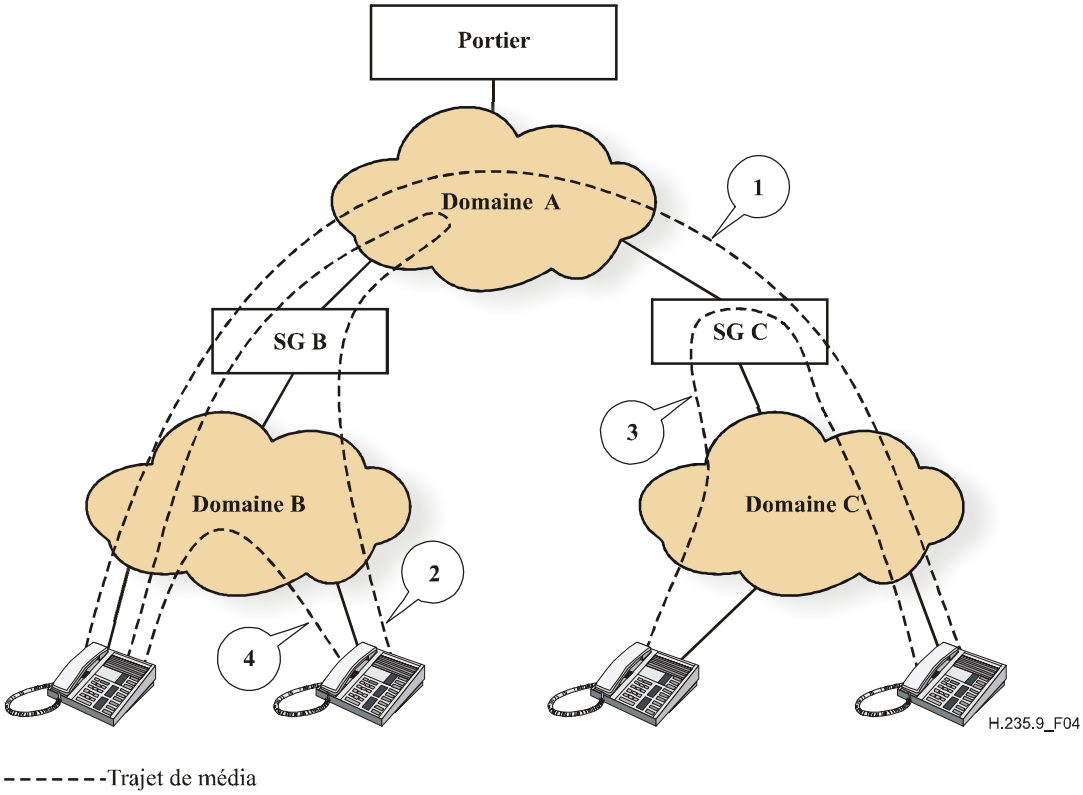


Figure 4/H.235.9 – Trajets de médias

Une configuration qui n'est pas représentée sur ce schéma est le cas dans lequel les flux de médias passent d'une région à une autre par l'intermédiaire de plusieurs passerelles SG. Si un point d'extrémité s'enregistre et se signale via une passerelle SG et qu'un autre point d'extrémité situé dans la même région se signale via une seconde passerelle SG, il sera difficile pour l'une ou l'autre passerelle SG de découvrir que les deux points d'extrémité se trouvent dans le même domaine, ou de déterminer les adresses à utiliser pour le point d'extrémité qui se signale via l'autre passerelle SG. Pour éviter ce problème, il est pratique d'utiliser une seule passerelle SG qui soit capable de traiter le niveau prévu de signalisation; la charge de traitement de flux de média peut être reléguée à des passerelles média distinctes sous le contrôle de la passerelle SG.

7 Détails concernant la signalisation

La prise en charge de cette capacité est identifiée le plus efficacement au moyen d'un identificateur d'objet (OID) normalisé dans les jetons **ClearToken** applicables. Dans le texte qui suit, ces jetons seront dénommés "jetons SG". Cela permet à la capacité en question d'être ignorée par tout portier récepteur (ou passerelle intermédiaire ou un autre dispositif qui ne participe pas). L'identificateur d'objet attribué sera utilisé pour identifier des jetons **ClearToken** contenant les éléments suivants:

- **tokenOID –** mis à l'identificateur d'objet attribué à cette capacité, dénommé "SG1" (voir le § 11);
- **generalID –** s'il est présent, il est mis au nom de la passerelle SG vers laquelle ce **ClearToken** est dirigé (utilisé dans le jeton clé-SG);
- **sendersID –** mis au nom de la passerelle SG qui a créé ce **ClearToken** (utilisé dans le jeton id-SG);
- **profileInfo –** contient les informations spécifiques acheminées par ce **ClearToken**, telles qu'indiquées dans le Tableau 1.

Tableau 1/H.235.9 – Eléments de profil pour la découverte de passerelle SG

Nom de l'élément	Valeur de l'identificateur de l'élément	Type d'élément (longueur)	Description de l'élément
TokenType	1	Entier	0 = jeton id-SG 1 = jeton clé-SG 2 = jeton NAT-SG 3 = jeton enregistrement-SG
EncryptedKey	2	Octets (16 pour SP2)	Clé d'authentification de session du profil de sécurité indiqué, chiffrée au moyen du secret partagé entre la passerelle SG spécifiée et le portier. Envoyée dans le jeton clé-SG. Le vecteur d'initialisation nécessaire pour le déchiffrement est spécifié dans ProfileElement.paramS.
ServedRealm	3	Nom	Nom du domaine dans lequel la passerelle SG peut/devrait fournir une adresse de découverte de portier.

8 Considérations relatives à la configuration des passerelles SG

Les procédures décrites dans la présente Recommandation dépendent des moyens utilisés par les passerelles SG dans le réseau pour découvrir les trajets vers le ou les portiers dont les services doivent être mis à la disposition d'utilisateurs situés dans différents domaines du réseau. Chaque passerelle SG doit pouvoir contacter son ou ses portiers situés dans un premier domaine, et offrir l'accès à ces portiers à partir de points d'extrémité (ou d'autres portiers) situés dans un second domaine. Par exemple, dans la Figure 3, la passerelle SG B a accès au portier dans le domaine Z. Elle peut en outre offrir un accès au portier pour des éléments situés dans le domaine Y. Par conséquent, la passerelle SG A peut accéder au portier via la passerelle SG B. Une fois qu'elle a accès au portier, la passerelle SG B peut fournir un accès à des entités situées dans le domaine X. Cela suppose que les passerelles SG elles-mêmes utilisent un protocole de découverte tel que RAS. Ces procédures pourraient également être utilisées pour identifier chaque passerelle SG ayant accès à un portier donné, et pour négocier un ensemble de clés afin de protéger les échanges de messages signalisation entre les utilisateurs.

8.1 Enregistrement de passerelles SG

Une passerelle SG peut jouer le rôle de représentant, dans un domaine, d'un portier situé dans un autre domaine auquel la passerelle SG a accès. Par exemple, dans la Figure 1, la passerelle SG A peut offrir une représentation (une adresse de découverte) dans le domaine B pour le portier situé dans le domaine A (une fois qu'elle connaît l'adresse de découverte du portier dans le domaine A). Cette technique peut s'appliquer à plusieurs niveaux de passerelles SG; étant donné que chaque passerelle SG découvre un portier (ou un représentant), elle peut fournir une adresse de découverte de ce portier dans un ou plusieurs nouveaux domaines, les passerelles SG connectées à ce ou ces domaines pouvant alors découvrir ces nouvelles adresses.

Les passerelles SG doivent appliquer les procédures RAS H.225.0 pour découvrir des portiers et s'enregistrer auprès d'eux dans tout domaine auquel elles souhaitent offrir des services en tant que passerelles de sécurité. Une passerelle SG doit s'identifier comme un point d'extrémité de type **passerelle**. Elle peut spécifier la prise en charge de protocole H.323 si elle souhaite spécifier des préfixes pris en charge et/ou des limitations de largeur de bande, mais cela n'est pas une obligation. Des procédures de sécurité normalisées telles que celles décrites dans les

Recommandations UIT-T H.235.1, H.235.2, H.235.3 et H.235.5 doivent être utilisées pour authentifier la passerelle SG auprès du portier et pour négocier des secrets partagés sécurisés à utiliser dans les procédures décrites ci-dessous. Les procédures H.235.1, H.235.2, H.235.3 et H.235.5 peuvent être appliquées pour le passage par d'autres passerelles de sécurité conformes à la présente Recommandation. La passerelle SG doit par ailleurs inclure un jeton ClearToken enregistrement-SG dans le message RRQ qu'elle envoie au portier. Ce jeton, qui sert à identifier la passerelle comme étant une passerelle SG, doit contenir un élément **ServedRealm** pour chaque nouveau domaine que la passerelle SG desservira. Chaque élément représente une potentielle nouvelle adresse de découverte de portier dans son domaine respectif. Chaque passerelle SG peut être configurée de manière à limiter les domaines auxquels elle fournira les adresses de découverte d'un portier particulier. Par exemple, dans la Figure 1, la passerelle SG B peut être configurée de façon à ne pas fournir d'adresse de découverte du portier C dans le domaine D, ce qui oblige les points d'extrémité du domaine D à s'enregistrer auprès du portier A. Dans la mesure où elle ne lance ni ne reçoit pas d'appels elle-même, la passerelle SG n'a pas besoin de fournir une adresse de signalisation d'appel au cours de son enregistrement; elle peut fournir une SÉQUENCE vide pour **callSignalAddress** dans le message RRQ. Le portier doit répondre de la même façon dans **callSignalAddress** du message RCF.

Le portier doit indiquer le ou les domaines auxquels la passerelle SG peut offrir des services en retournant, dans le message RCF, un jeton enregistrement-SG contenant un ou plusieurs des éléments **ServedRealm** du message RRQ de la passerelle SG. Une fois l'enregistrement terminé, la passerelle SG doit ouvrir un port d'écoute pour une adresse de découverte de portier dans chaque domaine indiqué. Des mécanismes n'entrant pas dans le cadre de la présente Recommandation peuvent être utilisés pour annoncer cette adresse de découverte dans le domaine en question. Le portier peut choisir d'utiliser les adresses de découverte fournies par la passerelle SG parmi une liste d'adresses.

Tout profil de sécurité RAS peut être utilisé, du moment que les passerelles SG sont autorisées à lire et manipuler les adresses de signalisation et de transport de média échangées, et qu'elles peuvent authentifier à nouveau le message.

Le portier peut utiliser les informations relatives au domaine de la passerelle SG pour déterminer les régions du réseau ainsi que la connectivité, et pour authentifier la passerelle SG. Le portier devrait fournir en retour à la passerelle SG les informations suivantes:

- le justificatif d'identité du portier;
- la ou les adresses d'enregistrement que la passerelle SG peut utiliser pour transmettre les demandes RAS émanant de points d'extrémité situés dans la ou les régions qu'elle dessert (le portier peut refuser de prendre en charge des points d'extrémité situés dans une ou plusieurs régions desservies par la passerelle SG).

Un enregistrement de passerelle SG réussi devrait se traduire par le partage d'une clé secrète forte entre la passerelle SG et le portier, à partir de laquelle il est possible d'obtenir des clés de chiffrement et/ou d'authentification. La clé d'authentification peut être utilisée pour authentifier la méthode d'enregistrement de la passerelle SG, et la clé de chiffrement devrait être utilisée lors des enregistrements des points d'extrémité pour chiffrer la clé d'authentification de session de ces points d'extrémité en vue de sa distribution à la passerelle SG, comme il est décrit ci-dessus.

8.2 Justificatif d'identité pour l'authentification

Contrairement aux points d'extrémité, les passerelles SG figurant dans un réseau composé de plusieurs régions devraient être relativement peu nombreuses. Dans la plupart des cas, on s'attend à ce que le service soit fourni par abonnement ou sur la base d'un autre accord contractuel; le portier possèdera donc des informations d'identification relatives aux passerelles de sécurité qui sont susceptibles de s'enregistrer auprès de lui. Dans le cas le plus simple, des mots de passe peuvent être attribués aux passerelles de sécurité, et des procédures d'authentification H.235.1, H.235.2, H.235.3,

H.235.5 ou d'épreuve-réponse peuvent être appliquées. L'utilisation de secrets préalablement partagés passe évidemment par l'emploi d'un système de distribution hors bande sécurisé.

Une autre méthode reposant sur l'emploi de certificats de clé publique est possible. Des copies du certificat du portier (ou du certificat appartenant à l'autorité qui a signé le certificat du portier) pourraient être placées au niveau des passerelles de sécurité au moyen d'un processus fiable. L'emploi de méthodes de ce type appelle un complément d'étude.

9 Considérations relatives à la sécurité

Les protocoles de ce type, permettant de modifier un message en transit, sont exposés aux attaques par déclassement ("downgrade attacks"). Par exemple, si un point d'extrémité offre des capacités de transport de média chiffré et de transport de média non chiffré, une passerelle de sécurité malveillante pourrait supprimer les offres de chiffrement et fournir simplement celles sans chiffrement, ce qui rendrait impossible le chiffrement des flux de média. Les points d'extrémité (ainsi que le portier) doivent contrer ce type d'attaque en offrant uniquement les capacités qui sont acceptables, conformément à leur propre politique de sécurité. En définitive, il incombe aux points d'extrémité et à leurs utilisateurs de veiller à établir et maintenir le niveau de sécurité approprié. Il en va de même pour le choix des profils de sécurité au cours de l'enregistrement: s'il exige une authentification forte, le point d'extrémité devrait l'indiquer expressément dans son message GRQ et ne devrait pas accepter une offre plus faible d'un portier.

10 Applicabilité

Cette méthode pourra être appliquée aussi bien aux profils de sécurité H.235.1, H.235.2 et H.235.3 qu'à ceux décrits dans la Rec. UIT-T H.235.5. Tout profil de sécurité assurant la négociation/le calcul de clés d'authentification adaptées peut être pris en charge. Les passerelles de sécurité devraient examiner les éléments des messages GRQ/GCF (par exemple, **authenticationCapability** et/ou **authenticationMode**) pour voir si le système de sécurité ou d'authentification de message négocié peut être pris en charge.

11 Identificateur d'objet

Identificateur d'objet	Valeur de l'identificateur d'objet	Description
"SG1"	{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 65 }	Jeton ClearToken contenant les éléments de profil pour la découverte de passerelle SG.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	**Systèmes audiovisuels et multimédias**
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	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 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, 2006