Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

H.235.0

(09/2005)

SÉRIE H: SYSTÈMES AUDIOVISUELS ET MULTIMÉDIAS

Infrastructure des services audiovisuels – Aspects système

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.235.0

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.235.0

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)

Résumé

La présente Recommandation décrit des améliorations apportées dans le cadre de la série des Recommandations H.3xx afin d'y introduire des services de sécurité tels que *l'authentification* et le *secret des communications* (chiffrement des données). Le procédé qui est proposé est applicable aussi bien aux simples conférences point à point qu'aux conférences point à multipoint, à partir de tous les terminaux faisant appel au protocole de commande décrit dans la Rec. UIT-T H.245. Il est aussi applicable aux systèmes H.323 qui utilisent le protocole RAS et/ou de signalisation d'appel H.225.0.

Par exemple, les systèmes H.323 fonctionnent sur des réseaux en mode paquet qui n'offrent pas une qualité de service garantie. La sûreté et la qualité du service offert par le réseau de base sont absentes pour les mêmes raisons techniques. Des communications sûres et en temps réel sur des réseaux non sûrs soulèvent généralement deux grands types de préoccupation: *l'authentification* et le *secret des communications*.

La présente Recommandation décrit l'infrastructure de sécurité et les techniques spécifiques de secret des communications que les systèmes multimédias conformes à la série H.3xx doivent utiliser. Elle traite de questions relatives aux conférences interactives, c'est-à-dire, entre autres domaines, l'authentification et le secret des communications pour tous les flux de média échangés en temps réel au cours d'une conférence. La présente Recommandation indique le protocole et les algorithmes nécessaires entre les entités H.323.

La présente Recommandation fait appel aux capacités générales qui sont décrites dans la Rec. UIT-T H.245: toute norme appliquée conjointement avec ce protocole de commande pourra donc utiliser ce cadre de sécurité. L'on prévoit que, dans la mesure du possible, d'autres terminaux selon la série H pourront interfonctionner et utiliser directement les méthodes décrites ci-après. Dans un premier temps, la présente Recommandation ne définira pas une implémentation complète dans tous les domaines mais portera plus précisément sur l'authentification des points d'extrémité et sur le secret des communications multimédias.

La présente Recommandation prévoit la possibilité de négocier les services et les capacités de façon générique. Elle prévoit également la possibilité de sélectionner les techniques et capacités cryptographiques utilisées. Leur mode d'emploi particulier dépend des capacités des systèmes, des exigences d'application et des contraintes propres aux politiques de sécurité. La présente Recommandation prend en compte divers algorithmes cryptographiques, avec diverses options adaptées à différents objectifs, comme les longueurs des clés. Certains algorithmes cryptographiques peuvent être attribués à des services de sécurité spécifiques (par exemple un algorithme pour un chiffrement rapide du flux de média et un autre pour le chiffrement des données de signalisation).

Il convient également de noter que certains des algorithmes ou mécanismes cryptographiques dont on dispose pourront être réservés à l'exportation ou à d'autres fins nationales (par exemple avec des clés de longueur limitée). La présente Recommandation prend en compte la signalisation d'algorithmes bien connus, en plus de celle d'algorithmes cryptographiques non normalisés ou privatifs. Aucun algorithme n'est spécifiquement prescrit mais il est fortement conseillé que les points d'extrémité prennent en charge autant d'algorithmes applicables que possible dans un souci d'interopérabilité. Ceci est à rapprocher de l'idée que la conformité à la Rec. UIT-T H.245 ne garantit pas l'interopérabilité de deux codecs d'entité.

Pour la version 4 de la Rec. UIT-T H.235, l'ancienne version 3 est transformée en un ensemble de Recommandations de la sous-série H.235.x, qui est restructurée. Des nouvelles Recommandations UIT-T (H.235.8 et H.235.9) ont été ajoutées à cet ensemble; les autres Recommandations de la sous-série ont été élargies avec de nouvelles fonctionnalités (les Recommandations UIT-T H.235.3, H.235.5). La Rec. UIT-T H.235.0 contient le cadre de sécurité H.323 avec un texte commun et des informations générales utiles pour toutes les Recommandations de la sous-série H.235.x.

Les nouveaux Appendices IV, V et VI/H.235.0 donnent le mappage entre le texte, les figures et les tableaux de la version 3 de la Rec. UIT-T H.235 (2003) – y compris le Corrigendum 1 et les Amendements relatifs – et la nouvelle structure.

Source

La Recommandation UIT-T H.235.0 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

Authentification, certificat, chiffrement, gestion de clés, intégrité, profil de sécurité, sécurité multimédia, signature numérique.

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.

TABLE DES MATIÈRES

Recommandation UIT-T H.235.0

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)

1 Domaine d'application

L'objectif principal de la présente Recommandation est de définir un cadre de sécurité applicable à l'authentification, au secret des communications et à l'intégrité dans le cadre des protocoles actuels de la série H. Le texte de la présente Recommandation donne des détails sur l'implémentation avec le protocole de la Rec. UIT-T H.323. On prévoit que ce cadre fonctionnera en liaison avec d'autres protocoles de la série H qui utilisent le protocole de commande de la Rec. UIT-T H.245 et/ou qui utilisent le protocole RAS et/ou de signalisation d'appel H.225.0.

Les objectifs complémentaires de la présente Recommandation sont les suivants:

1) développer une architecture de sécurité sous la forme d'un cadre extensible et souple, permettant d'implémenter un système de sécurité pour les terminaux conformes à la série H et les autres systèmes de type H.323. Ce cadre devra être fourni au moyen des capacités offertes par des services souples et indépendants, telles que la capacité de négocier et de sélectionner les techniques cryptographiques utilisées, ainsi que la façon de les utiliser;
2) assurer la sécurité de toutes les communications résultant de l'utilisation de protocoles H.3xx, ce qui suppose de s'intéresser à l'établissement des connexions, à la commande d'appel et à l'échange de médias entre toutes les entités. Il faut donc pouvoir utiliser des communications confidentielles (secret des communications) et pouvoir exploiter des fonctions d'authentification d'homologue ainsi que de protection de l'environnement de l'utilisateur contre les attaques qu'il pourrait subir;
3) la présente Recommandation ne doit pas interdire l'intégration d'autres fonctions de sécurité dans des entités H.3xx, pouvant les protéger contre des attaques issues du réseau;
4) la présente Recommandation ne doit pas limiter les possibilités d'évolution dans les Recommandations de la série H.3xx, selon les nécessités. Il peut s'agir aussi bien du nombre d'utilisateurs protégés que des niveaux de sécurité procurés;
5) le cas échéant, tous les mécanismes et toutes les capacités doivent être fournis indépendamment des topologies ou des technologies de transport sous-jacentes. D'autres moyens, hors du domaine d'application de la présente Recommandation, peuvent être requis pour contrer les menaces de ce type;
6) des dispositions doivent être prises pour le fonctionnement en environnement mixte (entités sécurisées et entités non sécurisées);
7) la présente Recommandation doit offrir la possibilité de distribuer des clés de session associées à la méthode cryptographique utilisée. (Ce qui n'implique pas que la gestion de certificats fondée sur des clés publiques doive faire partie de la présente Recommandation.);
8) la présente Recommandation propose deux profils de sécurité qui facilitent l'interopérabilité, l'un simple, mais sûr, de type à mot de passe (voir la Rec. UIT-T H.235.1), l'autre de type à signature utilisant des signatures numériques, des certificats et une infrastructure de clés publiques (voir la Rec. UIT-T H.235.2), qui n'est pas sujet aux limitations du profil H.235.1.

L'architecture de sécurité décrite dans la présente Recommandation ne part pas du principe que les participants se connaissent déjà. Elle suppose cependant que des précautions appropriées ont été prises pour protéger physiquement les points d'extrémité conformes à la série H. La principale menace de sécurité pour les communications est donc supposée être une indiscrétion dans le réseau ou une autre méthode de détournement de flux de média.

La Rec. UIT-T H.323 donne la possibilité de conduire une conférence en mode audio, vidéo ou données entre plusieurs correspondants; mais elle ne donne pas à chaque participant la possibilité d'authentifier l'identité des autres participants. Elle ne permet pas non plus de privatiser les communications (c'est-à-dire de chiffrer les flux).

Les terminaux de type Rec. UIT-T H.323, Rec. UIT-T H.324 et Rec. UIT-T H.310 font appel aux procédures de signalisation par canal logique selon la Rec. UIT-T H.245, dans laquelle le contenu de chaque canal logique est décrit dès l'ouverture du canal. Des procédures sont prévues pour exprimer les capacités du récepteur et de l'émetteur. Les transmissions sont limitées à ce que les récepteurs peuvent décoder et ces derniers peuvent demander aux émetteurs un mode préférentiel particulier. Les capacités de sécurité de chaque point d'extrémité sont communiquées de la même façon que toutes les autres capacités de communication.

Certains terminaux de la série H (H.323) peuvent être utilisés en configuration multipoint. Le mécanisme de sécurité décrit dans la présente Recommandation permettra un fonctionnement sûr dans les environnements mettant en œuvre une exploitation par ponts de conférence (MCU) aussi bien centralisés que décentralisés.

1.1 Structure des Recommandations de la sous-série H.235.x

La Figure 1 illustre la structure des Recommandations de la sous-série H.235.x relatives au cadre de sécurité. La présente Recommandation contient un texte commun et des informations générales utiles pour toutes les Recommandations de la sous-série H.235.x.

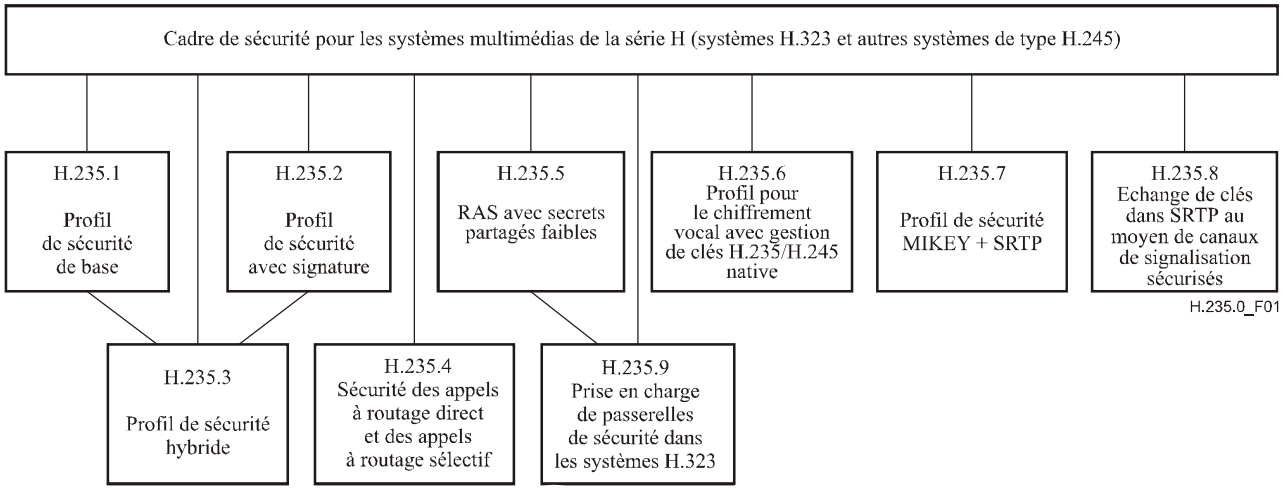


Figure 1/H.235.0 – Structure des Recommandations de la sous-série H.235

Les traits verticaux sur la Figure 1 indiquent les dépendances directes par rapport au texte principal H.235.0; il peut y avoir des dépendances plus indirectes par rapport à d'autres Recommandations UIT-T H.235.x. Plusieurs Recommandations peuvent être utilisées conjointement et de façon complémentaire (voir aussi le § 6.9).

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 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 (2003), *Sécurité et chiffrement pour les terminaux multimédias de la série H (terminaux H.323 et autres terminaux de type H.245)* plus Amendement 1 (2004) et Corrigendum 1 (2005).

– 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.235.4 (2005), *Cadre de sécurité H.323: sécurité des appels à routage direct et des appels à routage sélectif*.

– 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.235.6 (2005), *Cadre de sécurité H.323: profil pour le chiffrement vocal avec gestion de clés native dans les systèmes H.235/H.245*.

– Recommandation UIT-T H.235.7 (2005), *Cadre de sécurité H.323: utilisation du protocole de gestion de clés MIKEY avec le protocole de transport en temps réel sécurisé (SRTP) dans les systèmes H.235*.

– Recommandation UIT-T H.235.8 (2005), *Cadre de sécurité H.323: échange de clés dans le protocole SRTP au moyen de canaux de signalisation sécurisés*.

– Recommandation UIT-T H.235.9 (2005), *Cadre de sécurité H.323: prise en charge des passerelles de sécurité dans les systèmes H.323*.

– 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*.

– Recommandation UIT-T H.530 (2002), *Procédures de sécurité symétrique pour la mobilité des systèmes H.323 selon la Recommandation H.510, plus Corrigendum 1 (2003)*.

– Recommandation UIT-T Q.931 (1998), *Spécification de la couche 3 de l'interface utilisateur-réseau RNIS pour la commande de l'appel de base*.

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

ISO 7498-2:1989, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité*.

– Recommandation UIT-T X.803 (1994) | ISO/CEI 10745:1995, *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de sécurité pour les couches supérieure*s.

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

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

– ISO/CEI 9798-2:1999, *Technologies de l'information – Techniques de sécurité – Authentification d'entité – Partie 2: Mécanismes utilisant des algorithmes de chiffrement symétriques*.

– ISO/CEI 9798-3:1998, *Technologies de l'information – Techniques de sécurité – Authentification d'entité – Partie 3: Mécanismes utilisant des techniques de signature numériques*.

– ISO/CEI 9798-4:1999, *Technologies de l'information – Techniques de sécurité – Authentification d'entité – Partie 4: Mécanismes utilisant une fonction cryptographique de vérification*.

– ISO/CEI 15946-1:2002, *Technologies de l'information – Techniques de sécurité – Techniques cryptographiques basées sur les courbes elliptiques – Partie 1: Généralités*.

– ISO/CEI 15946-2:2002, *Technologies de l'information – Techniques de sécurité – Techniques cryptographiques basées sur les courbes elliptiques – Partie 2: Signatures digitales*.

– ATM Forum: af-sec-0100.002 (2001), *ATM Security Specification Version 1.1*.

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

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

– IETF RFC 2407 (1998), *The Internet IP Security Domain of Interpretation for ISAKMP*.

– IETF RFC 2408 (1998), *Internet Security Association and Key Management Protocol (ISAKMP)*.

– IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS)*.

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

– IETF RFC 3830 (2004), *MIKEY: Multimedia Internet KEYing*.

2.2 Références informatives

[Daemon] DAEMON (J.), *Cipher and Hash function design*, Ph.D. Thesis, Katholieke Universiteit Leuven, March 1995.

[ESP] IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP)*.

[OAKLEY] IETF RFC 2412 (1998), *The OAKLEY Key Determination Protocol*.

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

[ISO|CEI 14888-3] ISO/CEI 14888-3:1998, *Technologies de l'information – Techniques de sécurité – Signatures digitales avec appendice – Partie 3: Mécanismes fondés sur certificat*.

[J.170] Recommandation UIT-T J.170 (2005), *Spécification de la sécurité sur IPCablecom*.

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

[Schneier] SCHNEIER (B.), *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition, John Wiley & Sons, Inc., 1995.

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

3 Termes et définitions

Dans la présente Recommandation, les définitions figurant au § 3/H.323, au § 3/H.225.0 et au § 3/H.245 s'appliquent, en plus de celles du présent paragraphe. Certains des termes suivants sont utilisés selon la définition donnée dans les Recommandations UIT-T X.800 | ISO 7498-2, X.803 | ISO/CEI 10745, X.810 | ISO/CEI 10181-1 et X.811 | ISO/CEI 10181-2.

3.1 contrôle d'accès: précaution prise contre l'utilisation non autorisée d'une ressource, y compris l'utilisation d'une ressource d'une façon non autorisée (Rec. UIT-T X.800).

3.2 authentification: attestation de l'identité revendiquée par une entité (Rec. UIT-T X.811 | ISO/CEI 10181-2).

3.3 autorisation: octroi d'une permission sur la base d'une identité authentifiée.

3.4 attaque: activités entreprises pour contourner ou exploiter des déficiences constatées dans les mécanismes de sécurité d'un système. Une attaque directe d'un système exploite des déficiences dans les algorithmes, principes ou propriétés sous-tendant un mécanisme de sécurité. Les attaques indirectes consistent à contourner le mécanisme ou à en provoquer une utilisation incorrecte par le système.

3.5 certificat: ensemble de données relatives à la sécurité, émis par une autorité de sécurité ou par un tiers de confiance en même temps que des informations de sécurité qui sont utilisées pour fournir les services d'intégrité et d'authentification d'origine des données (Rec. UIT T X.810 | ISO/CEI 10181-1). Dans la présente Recommandation, ce terme désigne les certificats de "clé publique" qui sont des valeurs représentant la clé publique d'un détenteur (et d'autres informations facultatives), ces valeurs ayant été vérifiées et signées par une autorité de confiance sous une forme infalsifiable.

3.6 chiffre: algorithme cryptographique ou transformée mathématique.

3.7 confidentialité: caractéristique qui empêche la divulgation des informations à des individus, entités ou processus non autorisés.

3.8 algorithme cryptographique: fonction mathématique qui calcule un résultat à partir d'une ou de plusieurs valeurs d'entrée.

3.8 *bis* EC-GDSA: signature numérique à courbe elliptique avec appendice analogue à l'algorithme de signature numérique NIST (DSA); (voir aussi ISO/CEI 15946-2, chapitre 5).

3.8 *ter* système cryptographique à courbe elliptique: système cryptographique à clé publique (voir la section 8.7 de "*ATM forum security specification*" *version 1.1*).

3.8 *quat* système de concordance de clés à courbe elliptique – Diffie-Hellman: système de concordance de clés Diffie-Hellman utilisant la cryptographie à courbe elliptique.

3.9 chiffrement: processus consistant à rendre des données illisibles par des entités non autorisées après application d'un algorithme cryptographique (ou de chiffrement). Le déchiffrement est l'opération inverse par laquelle le texte chiffré est transformé en texte clair.

3.10 intégrité: caractéristique de données qui n'ont pas été altérées de façon non autorisée.

3.11 gestion de clés: production, stockage, distribution, suppression, archivage et application de clés conformément à une politique de sécurité (Rec. UIT-T X.800).

3.12 flux de média: flux audio, vidéo ou de données, ou combinaison quelconque de ces types de flux. Les flux de média acheminent des données d'utilisateur ou d'application (charge utile) mais pas de données de commande.

3.13 non-répudiation: protection contre le déni, par une des entités impliquées dans une communication, d'avoir participé à tout ou partie de celle-ci.

3.14 secret des communications: mode de communication dans lequel seules les parties explicitement habilitées peuvent interpréter la communication. Le secret des communications est normalement réalisé par chiffrement et par partage de clé(s) pour accéder au chiffre.

3.15 canal privé: dans la présente Recommandation, un canal privé est celui qui résulte d'une négociation préalable par canal sécurisé et qui peut servir à acheminer des flux de média.

3.16 cryptographie à clé publique: système de chiffrement qui fait appel (pour le chiffrement et le déchiffrement) à des clés asymétriques liées par une relation mathématique qui ne peut logiquement pas être calculée.

3.17 profil de sécurité: (sous-) ensemble cohérent de procédures et caractéristiques interopérables, tirées de la Rec. UIT-T H.235, très utiles pour sécuriser des communications multimédias H.323 entre des entités concernées dans un scénario donné.

3.18 spamming (submersion): attaque de type déni de service se produisant lorsqu'un nombre excessif de données non autorisées sont envoyées à un système. Un cas particulier est le spamming de médias par l'envoi de paquets RTP à des ports UDP. Généralement, le système est submergé de paquets et le traitement correspondant nécessite de précieuses ressources.

3.19 algorithme cryptographique symétrique (à clé secrète): algorithme permettant de réaliser le chiffrement ou le déchiffrement correspondant, dans lequel la même clé est requise à la fois pour le chiffrement et pour le déchiffrement (Rec. UIT-T X.810 | ISO/CEI 10181-1).

3.20 menace: violation potentielle de la sécurité (Rec. UIT-T X.800 | ISO 7498-2).

4 Symboles et abréviations

La présente Recommandation utilise les abréviations suivantes:

X || Y	Concatenation de X et Y
3DES	triple DES
AES	norme de chiffrement perfectionné (*advanced encryption standard*)
ALG	passerelle de couche Application (*application layer gateway*)
ASN.1	notation de syntaxe abstraite numéro un (*abstract syntax notation one*)
BES	serveur d'arrière (*back-end server*)
CA	autorité de certification (*certification authority*)
CBC	chaînage de blocs chiffrants (*cipher block chaining*)
CFB	chiffrement avec bouclage (*cipher feedback*)

CRL	liste de révocation de certificat (*certificate revocation list*)
DES	norme de chiffrement des données (*data encryption standard*)
DH	Diffie-Hellman
DNS	système de dénomination de domaine (*domain name system*)
DSS	norme de signature numérique (*digital signature standard*)
DTMF	multifréquence à deux tonalités (*dual tone multi-frequency*)
ECB	mode dictionnaire (*electronic code book*)
ECC et EC	système cryptographique à courbe elliptique (*elliptic curve cryptosystem*) (voir la section 8.7 de "*ATM Forum Security Specification*" *Version 1.1*). Système cryptographique de clé publique
EC-GDSA	signature numérique à courbe elliptique avec appendice analogue à l'algorithme de signature numérique NIST (DSA); (voir aussi ISO/CEI 15946-2, chapitre 5)
ECKAS-DH	système de concordance de clés à courbe elliptique – Diffie-Hellman (*elliptic curve key agreement scheme – Diffie-Hellman*)
EOFB	mode avec bouclage de sortie amélioré (*enhanced output feedback mode*)
EP	point d'extrémité (*endpoint*)
GK	portier (*gatekeeper*)
GW	passerelle (*gateway*)
ICV	valeur de contrôle d'intégrité (*integrity check value*)
ID	identificateur
IETF	groupe de travail d'ingénierie Internet (*Internet engineering task force*)
IPsec	sécurité du protocole Internet (*Internet protocol security*)
ISAKMP	protocole d'association de sécurité Internet et de gestion de clés (*Internet security association key management protocol*)
ISO	Organisation Internationale de Normalisation (*International Organization for Standardization*)
IV	vecteur d'initialisation (*initialization vector*)
LDAP	protocole rapide d'accès à l'annuaire (*lightweight directory access protocol*)
MAC	code d'authentification de message (*message authentication code*)
MC	contrôleur de multidiffusion (*multicast controller*)
MCU	unité de commande multipoint, pont de conférence (*multipoint control unit*)
MPS	flux de charge utile multiple (*multiple payload stream*)
NAT	traduction d'adresse de réseau (*network address translation*)
OCSP	protocole de statut de certificat en ligne (*online certificate status protocol*)
OFB	mode avec bouclage de sortie (*output feedback mode*)
OID	identificateur d'objet (*object identifier*)
PDU	unité de données protocolaire (*protocol data unit*)
PKI	infrastructure de clé publique (*public key infrastructure*)

PRF	fonction pseudo-aléatoire (*pseudo-random function*)
Q&A	question et réponse (*question and answer*)
QS	qualité de service
RAS	enregistrement, admission et statut (*registration, admission and status*)
RSA	algorithme à clé publique de Rivest, Shamir et Adleman (*Rivest, Shamir and Adleman (public key algorithm)*)
RTC	service ordinaire
RTCP	protocole de commande de transport en temps réel (*real-time transport control protocol*)
RTP	protocole de transport en temps réel (*real-time transport protocol*)
SASET	type de point d'extrémité simple audio sécurisé (*secure audio simple endpoint type*)
SDU	unité de données de service (*service data unit*)
SHA1	algorithme de hachage sécurisé n° 1 (*secure hash algorithm 1*)
SRTP	protocole de transport en temps réel sécurisé (*secure real-time transport protocol*)
SSL	couche de connecteurs sécurisée (*secure socket layer*)
TLS	sécurité de la couche de transport (*transport level security*)
TSAP	point d'accès au service de transport (*transport service access point*)
TTP	tiers de confiance (*trusted third party*)
UDP	protocole datagramme d'utilisateur (*user datagram protocol*)
XOR, ⊕	OU exclusif

5 Conventions

Dans la présente Recommandation, les conventions suivantes s'appliquent:

– la forme "doit/doivent" indique une disposition obligatoire;

– la forme "devrait/devraient" indique une mesure suggérée mais facultative;

– la forme "peut/peuvent" indique une action possible plutôt qu'une action recommandée.

Sauf mention explicite d'une autre Recommandation, les références aux paragraphes, sous-paragraphes, annexes et appendices se rapportent à ceux de la présente Recommandation. Par exemple, la référence "1.4" correspond au § 1.4 de la présente Recommandation. La référence "6.4/H.245" correspond au § 6.4 de la Rec. UIT-T H.245.

La présente Recommandation décrit l'utilisation de "n" types de message différents: H.245, RAS, Q.931, etc. Pour établir une distinction entre ces différents types de message, la convention suivante est utilisée: les noms de messages et de paramètres H.245 se composent de plusieurs mots concaténés et écrits en gras (**maximumDelayJitter**); les noms de message RAS sont représentés par des abréviations à trois lettres (**ARQ**); les noms de message Q.931 se composent d'un ou de deux mots dont la première lettre est en majuscule (**Call Proceeding**).

La présente Recommandation utilise la notion consistant à mettre une structure de données ASN.1 composite à NULL; par exemple, "**paramS** mis à NULL" (voir les § 7/H.235.1, 8/H.235.1, 9.1/H.235.1, 9.2/H.235.1, 7/H.235.2, 9/H.235.2, 15.1/H.235.2 et 15.2/H.235.2). Cela signifie que tous les éléments optionnels de la SEQUENCE considérée (c'est-à-dire **Params**) sont absents.

La présente Recommandation définit divers identificateurs d'objet (OID) destinés à la signalisation des capacités de sécurité, des procédures et des algorithmes de sécurité. Ces identificateurs se rapportent à une arborescence de valeurs attribuées pouvant provenir de sources extérieures ou faisant partie d'une arborescence d'identificateurs d'objet entretenue par l'UIT-T. Les identificateurs d'objet qui sont liées à la Rec. UIT-T H.235 présentent l'aspect suivant:

"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 numéro 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 numéros. Pour des raisons de commodité, pour chaque OID, une notation mnémonique textuelle condensée est utilisée dans le texte, par exemple "OID". Un mappage est donné entre chaque chaîne OID et la séquence de numéros ASN.1. Les implémentations conformes à la Rec. UIT-T H.235 doivent uniquement utiliser les numéros codés en ASN.1.

6 Introduction au système

La Figure 2 donne un aperçu général du domaine d'application de la présente Recommandation dans le cadre de la Rec. UIT-T H.323.

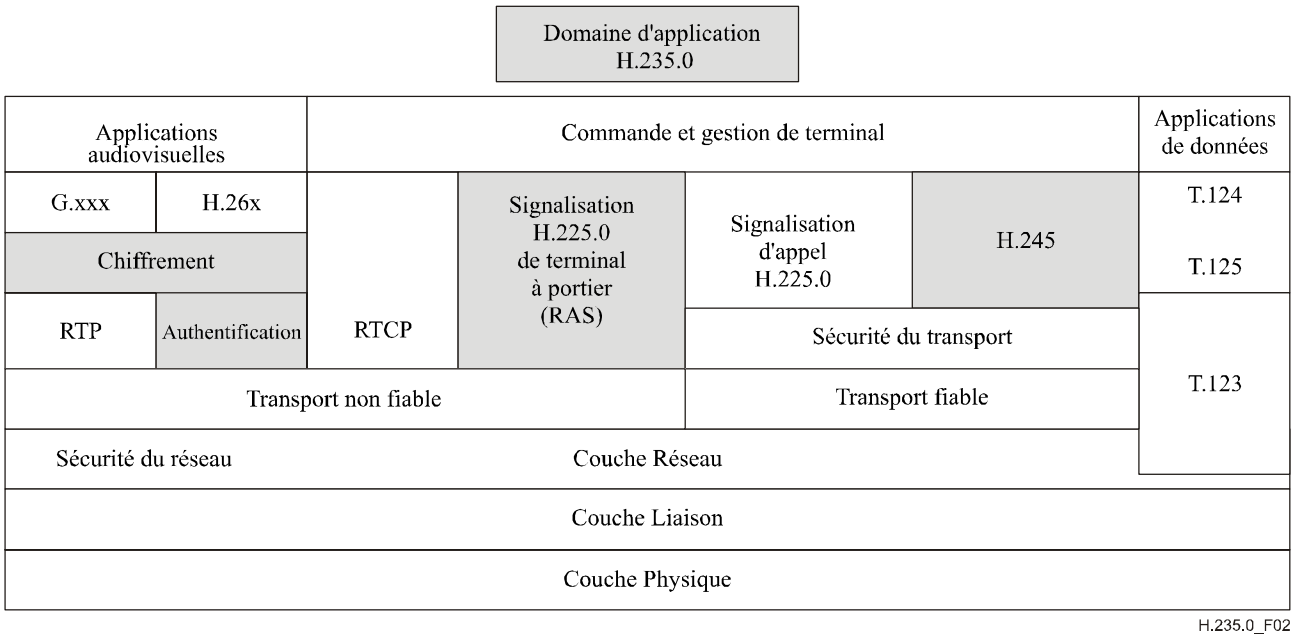


Figure 2/H.235.0 – Aperçu général

Pour les flux de la Rec. UIT-T H.323, la signalisation de l'utilisation du protocole TLS (RFC 2246, RFC 3546), IPsec ou d'un mécanisme privé sur le canal de commande H.245 doit être effectuée sur le canal H.225.0 sécurisé ou non sécurisé, pendant l'échange initial de messages Q.931.

6.1 Résumé

1) le canal de signalisation d'appel peut être sécurisé au moyen du protocole TLS (RFC 2246, RFC 3546) ou IPsec (RFC 2401, [ESP]) en un port sécurisé bien connu (Rec. UIT-T H.225.0);

2) les utilisateurs peuvent être authentifiés soit au cours de la connexion d'appel initiale, soit au cours du processus de sécurisation du canal H.245 et/ou par échange de certificats sur le canal H.245;

3) les capacités de chiffrement d'un canal de média sont déterminées par des extensions du mécanisme existant de négociation de capacité;

4) la distribution initiale par l'entité maîtresse des données de clé s'effectue par les messages H.245 **OpenLogicalChannel** ou **OpenLogicalChannelAck**;

5) la redéfinition des clés peut s'effectuer par les commandes H.245: **EncryptionUpdateCommand**, **EncryptionUpdateRequest**, **EncryptionUpdate** et **EncryptionUpdateAck**;

6) la distribution des données de clé est protégée par l'exploitation du canal H.245 en tant que canal privé ou par protection spécifique des données de clé par échange des certificats sélectionnés;

7) les protocoles de sécurité présentés sont conformes à des normes ISO publiées ou à des normes proposées par l'IETF.

6.2 Authentification

Le processus d'authentification vérifie que ceux qui répondent sont bien ceux qu'ils disent être. L'authentification peut être réalisée dans le cadre de l'échange de certificats de clé publique ou dans celui d'un échange faisant appel à un secret, partagé entre les entités en cause. Il peut s'agir d'un mot de passe statique ou d'un autre type d'information arbitraire.

La présente Recommandation décrit le protocole d'échange des certificats mais ne spécifie pas les critères permettant de les vérifier et de les accepter les uns en fonction des autres. En général, les certificats donnent au vérificateur une certaine garantie que celui qui présente le certificat est la personne qu'il déclare être. L'échange de certificats a pour objet d'authentifier *l'utilisateur* du point d'extrémité et non simplement le point d'extrémité physique. L'utilisation de certificats numériques permet de prouver, par protocole d'authentification, que ceux qui répondent possèdent les clés privées correspondant aux clés publiques contenues dans les certificats. Cette authentification protège contre les attaques par intercepteur (*man-in-the-middle*) mais ne prouve pas automatiquement l'identité de ceux qui répondent. Pour cela, il faut normalement qu'une certaine politique s'applique au reste du contenu des certificats. Pour les certificats d'autorisation par exemple, le certificat contiendra normalement l'identification du fournisseur de service ainsi qu'une certaine identification du compte d'utilisateur, prescrite par le fournisseur de service.

Le cadre d'authentification présenté dans la présente Recommandation ne prescrit pas le contenu des certificats (c'est-à-dire qu'il ne spécifie pas de politique relative aux certificats) au-delà de ce qui est requis par le protocole d'authentification. Une application utilisant ce cadre pourra toutefois imposer des prescriptions politiques de haut niveau comme la présentation du certificat à l'utilisateur pour approbation. Cette politique de haut niveau pourra soit être automatisée au sein de l'application soit nécessiter une interaction humaine.

Pour l'authentification qui ne fait pas appel à des certificats numériques, la présente Recommandation indique la signalisation permettant de réaliser divers scénarios d'épreuve/réponse. Cette méthode d'authentification nécessite une coordination préalable entre les entités communicantes, de façon qu'un secret partagé soit obtenu. Un exemple de cette méthode serait celui d'un client abonné à un service.

Une troisième option permet de réaliser l'authentification dans le contexte d'un protocole de sécurité distinct tel que TLS (RFC 2246, RFC 3546) ou RFC 2409 [IKE].

Des entités homologues peuvent prendre en charge une authentification aussi bien bidirectionnelle qu'unidirectionnelle. Cette authentification peut se produire sur tout ou partie des voies de communication.

Tous les mécanismes d'authentification spécifiques qui sont décrits dans la présente Recommandation sont identiques aux algorithmes mis au point par l'ISO (ou en sont dérivés), comme spécifié dans les Parties 2 et 3 de l'ISO/CEI 9798 ou sont fondés sur des protocoles IETF.

6.2.1 Certificats

La normalisation des certificats, y compris leur production, leur administration et leur distribution, est hors du domaine d'application de la présente Recommandation. Les certificats utilisés pour établir des canaux sûrs (signalisation d'appel et/ou commande d'appel) doivent être conformes aux prescriptions de tout protocole qui a été négocié pour sécuriser ces canaux.

Il est à noter que, pour l'authentification utilisant des certificats de clé publique, les points d'extrémité sont appelés à fournir des signatures numériques utilisant la valeur de clé privée associée. Le seul échange de certificats de clé publique ne suffit pas à protéger contre les attaques par intercepteur. Les protocoles H.235 sont conformes à cette exigence.

6.3 Sécurité lors de l'établissement d'appel

Il y a au moins deux raisons pour sécuriser le canal d'établissement d'appel (par exemple pour des systèmes H.323 utilisant le protocole Q.931). La première est l'exécution d'une authentification simple, avant d'accepter l'appel. La deuxième vise à permettre une autorisation d'appel. Si cette fonction est souhaitée dans le terminal conforme à la série H, il convient d'utiliser un mode de communication sécurisé (tel que TLS/IPsec pour H.323) avant l'échange des messages de connexion d'appel. En variante, l'autorisation peut être donnée sur la base d'une authentification propre au service, dont les contraintes de politique sont hors du domaine d'application de la présente Recommandation.

6.4 Sécurité de la commande d'appel (H.245)

Le canal de commande d'appel (H.245) devrait également être sécurisé de quelque façon, afin d'offrir ensuite un média secret. Le canal H.245 doit être sécurisé par un quelconque mécanisme de secret des communications (dont la négociation comporte l'option "aucun"). Les messages H.245 sont utilisés pour signaler les algorithmes et clés de chiffrement utilisés dans les canaux de média partagés et privés. Cette capacité permet de chiffrer, canal logique par canal logique, différents canaux de média au moyen de différents mécanismes. Par exemple, lors de conférences multipoint centralisées, différentes clés peuvent être utilisées pour les différents flux destinés à chaque point d'extrémité. Cela permet de privatiser les flux de média destinés à chaque point d'extrémité de la conférence. Pour utiliser les messages H.245 de manière sûre, l'ensemble du canal H.245 (canal logique 0) devrait être ouvert après sécurisation négociée.

Le mécanisme par lequel un canal H.245 est sécurisé dépend des terminaux série H utilisés. La seule exigence imposée à tous les systèmes utilisant cette structure de sécurité est que chacun d'eux possède une certaine capacité permettant de négocier et/ou de signaler que le canal H.245 doit être exploité d'une certaine manière sécurisée avant d'être effectivement initialisé. Par exemple, les systèmes H.323 utiliseront les messages de signalisation de connexion H.225.0 pour réaliser cette condition.

6.5 Secret des communications de flux de média

La présente Recommandation décrit le secret des communications de flux de média acheminés par transport en mode paquet. Ces canaux peuvent être unidirectionnels dans le cadre de la définition des canaux logiques H.245. Il n'est pas prescrit que ces canaux soient unidirectionnels dans la couche Physique ou Transport.

Une première étape pour réaliser le secret des communications de média devrait être la fourniture d'un canal de commande privé permettant d'établir des bases de construction de clés et/ou l'établissement des canaux logiques devant transporter les flux de média chiffrés. A cette fin, lors du fonctionnement en conférence sécurisée, tout point d'extrémité participant peut utiliser un canal H.245 chiffré. Cette procédure permet de protéger la sélection des algorithmes cryptographiques et les clés de chiffrement transmises dans la commande H.245 **OpenLogicalChannel**.

Le canal H.245 sécurisé peut être exploité avec des caractéristiques différentes des canaux de média privés, dans la mesure où il procure un niveau de secret des communications acceptable par les deux parties. Il permet aux mécanismes de sécurité protégeant les flux de média et tous canaux de commande de fonctionner de manière totalement indépendante, en fournissant des niveaux de robustesse et de complexité totalement différents.

S'il est prescrit que le canal H.245 soit exploité de manière non chiffrée, les clés spécifiques de chiffrement de média peuvent être chiffrées séparément par les parties engagées, de la manière qui a été signalée et convenue. Un canal logique de type **h235Control** peut être utilisé pour fournir les données permettant de protéger les clés de chiffrement de média. Ce canal logique peut être exploité dans n'importe quel mode négocié à cette fin.

Le secret (chiffrement) des communications de données acheminées dans les canaux logiques doit avoir la forme spécifiée par la commande **OpenLogicalChannel**. Les informations d'en-tête propres à la couche Transport ne doivent pas être chiffrées. Le secret des communications de données doit être fondé sur un chiffrement de bout en bout.

6.6 Eléments de confiance

La base de l'authentification (confiance) et du secret des communications est définie par les terminaux du canal de communication. Pour un canal d'établissement de connexion, ces terminaux peuvent être ceux de l'appelant et d'un élément hôte du réseau. Par exemple, un poste téléphonique "escompte" que le commutateur du réseau le connectera au poste dont le numéro a été composé. C'est pourquoi toute entité à laquelle aboutit un canal de commande H.245 chiffré ou un canal logique de type **encryptedData** doit être considérée comme un élément de confiance de la connexion. Ces entités peuvent être des ponts de conférence ou des passerelles. Le résultat de la confiance en un élément est l'assurance de pouvoir révéler en confiance à cet élément le mécanisme de secret des communications (algorithme et clé).

Compte tenu de ce qui précède, il incombe aux participants du trajet de communication d'authentifier tout un chacun des éléments "de confiance". Pour cela, on procédera normalement à un échange de certificats comme dans le cas de l'authentification de bout en bout normale. La présente Recommandation ne prescrira aucun niveau spécifique d'authentification et se limitera à suggérer que ce niveau soit acceptable par toutes les entités faisant appel aux éléments de confiance. Les détails relatifs à un modèle de confiance et à une politique de certificats feront l'objet d'un complément d'étude.

Le secret des communications ne peut être garanti entre les deux points d'extrémité que s'il est prouvé que les connexions entre éléments de confiance sont protégées contre les attaques par intercepteur.

6.6.1 Dépôt de clé

Bien que cela ne soit pas spécifiquement requis pour le fonctionnement, la présente Recommandation contient des dispositions pour conférer aux entités utilisant le protocole H.235 la capacité dite "tiers de confiance" (TTP, *trusted third party*) dans le cadre des éléments de signalisation.

La capacité de récupérer les clés de chiffrement de média perdues doit être prise en charge par les installations lorsqu'une telle capacité est souhaitable ou requise.

Le dépôt de clé est une fonctionnalité qui est souvent désignée par le terme "tiers de confiance" (TTP). Cette fonctionnalité reste à étudier.

6.7 Non-répudiation

A étudier.

6.8 Sécurité dans un environnement de mobilité

Des systèmes H.323 peuvent être mis en place dans un environnement de mobilité conformément à la Rec. UIT-T H.510. Les procédures et protocoles de sécurité applicables à ces systèmes sont décrits dans la Rec. UIT-T H.530. La Rec. UIT-T H.530 met en œuvre des protocoles et des procédures issus de la présente Recommandation.

6.9 Profils de sécurité

La présente Recommandation fait référence à un certain nombre de profils de sécurité H.235 (H.235.1, H.235.2, H.235.3, H.235.4, H.235.5, H.235.6, H.235.7, H.235.8, H.235.9). Un profil de sécurité spécifie un usage particulier des fonctionnalités ou d'un sous-ensemble des fonctionnalités H.235 correspondant à des environnements bien définis avec une applicabilité bien délimitée.

Selon l'environnement et l'application, les profils de sécurité peuvent être implémentés sélectivement ou en totalité. En général, dans les systèmes H.235, la partie identificateur d'objet des messages de signalisation indique les profils de sécurité mis en œuvre. Dans ces systèmes, les profils de sécurité doivent, en principe, être choisis en fonction des besoins.

Optionnellement, les points d'extrémité peuvent, dans les messages **RRQ/GRQ**, proposer initialement et simultanément plusieurs profils de sécurité et laisser le portier choisir le profil le plus approprié et indiquer en réponse dans le message **RFC/GCF**. Les transactions **LRQ/LCF** entre portiers peuvent également acheminer plusieurs profils de sécurité. Lors du calcul des signatures numériques ou des valeurs de hachage pour assurer l'intégrité des messages, tout d'abord les valeurs de hachage et les signatures numériques qui n'assurent pas l'intégrité des messages devraient être calculées sur le sous-ensemble du champ et insérées dans le message, les signatures numériques et les valeurs de hachage qui assurent l'intégrité des messages devraient être mises à "0" dans le tampon de messages, ensuite, toutes les signatures numériques et valeurs de hachage devraient être calculées en utilisant ce tampon, puis insérées dans le message.

Chacune des Recommandations de la sous-série définit un profil de sécurité H.235.0. Un tel profil est généralement composé d'une instanciation de la Rec. UIT-T H.235.0 propre à un scénario particulier et/ou inclut une spécification de caractéristiques de sécurité particulières ou une combinaison de mécanismes de sécurité/profils de sécurité.

Tous les profils de sécurité sont facultatifs dans la Rec. UIT-T H.235.0.

La Figure 3 illustre certaines combinaisons types et possibles de profils de sécurité. Un trait plein indique que la combinaison des deux profils de sécurité concernés est définie et possible. Un trait en pointillés indique que la combinaison est généralement possible mais qu'elle n'est peut-être pas très utile. L'absence de trait indique que la combinaison n'est pas encore définie.

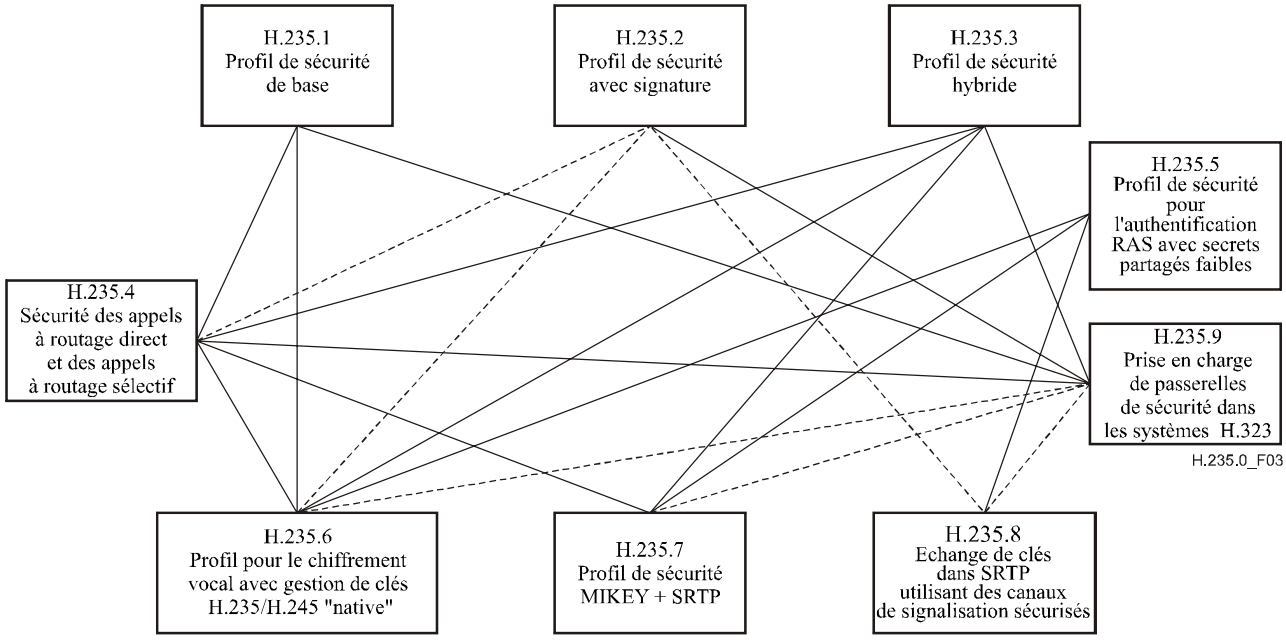


Figure 3/H.235.0 – Illustration de combinaisons de profils de sécurité

6.10 Franchissement sécurisé de dispositifs NAT/pare-feu

La Rec. UIT-T H.235.9 spécifie des procédures permettant de découvrir la présence de passerelles de sécurité (passerelles ALG par exemple) sur le trajet de signalisation RAS H.225.0 entre deux entités H.323 (portier, point d'extrémité) et permettant à un portier et à une passerelle de sécurité d'échanger des informations de sécurité afin de préserver l'intégrité et le secret des communications des données de signalisation.

Les Recommandations UIT-T H.235.1 (Procédure IA) et H.235.2 (procédure d'authentification seule) offrent des procédures spécifiques complémentaires permettant à l'authentification de messages fondée sur H.235 associée aux protocoles RAS et de signalisation d'appel H.225.0 de franchir les dispositifs NAT/pare-feu.

7 Procédures d'établissement de connexion

Comme indiqué dans le § 6 (Introduction au système), aussi bien le canal de connexion d'appel (H.225.0 pour terminaux série H.323) que le canal de commande d'appel (H.245) doivent fonctionner dans le mode négocié, sécurisé ou non sécurisé, à partir du premier échange de messages. Pour le canal de connexion d'appel, le mode de sécurité est déterminé *a priori* (pour un terminal H.323, un point TSAP sécurisé par TLS (port 1300) doit être utilisé pour les messages Q.931). Pour le canal de commande d'appel, le mode de sécurité est déterminé par les informations transmises dans le protocole d'établissement de connexion initial, utilisé par le terminal série H.

Lorsqu'il n'y a pas de chevauchement entre capacités de sécurité, le terminal appelé peut refuser la connexion. L'erreur renvoyée ne devrait pas contenir de renseignements sur l'absence de concordance entre les capacités de sécurité. Le terminal appelant devra déterminer l'origine du problème par d'autres moyens. Lorsque le terminal appelant reçoit un message sans capacités de sécurité suffisantes, il devrait mettre fin à l'appel.

Si les terminaux appelant et appelé ont des capacités de sécurité compatibles, chaque extrémité doit partir du principe que le canal H.245 doit fonctionner dans le mode sécurisé qui a été négocié. L'échec d'établissement du canal H.245 dans le mode sécurisé déterminé devrait être considéré comme une erreur de protocole et la connexion devrait être fermée.

La Rec. UIT-T H.235.6 décrit des procédures complémentaires d'établissement de connexion de sécurité incluant la gestion de clés (voir § 7 et 8/H.235.6).

8 Signalisation et procédures d'authentification

L'authentification est généralement fondée sur une méthode à secret partagé (la connaissance de cette information secrète permet d'être authentifié) ou à clé publique avec certifications (la possession de la clé privée est la preuve de l'identité). Un secret partagé et l'emploi subséquent de la cryptographie symétrique nécessitent un contact préalable entre les entités communicantes. Un face à face préalable ou un contact sécurisé peut être remplacé par la production ou l'échange de la clé partagée secrète par des méthodes fondées sur la cryptographie à clé publique, par exemple l'échange de clés Diffie-Hellman. Pour la production et l'échange de la clé, les parties communicantes doivent être authentifiées, par exemple au moyen de messages à signature numérique; à défaut, les parties communicantes ne savent pas avec certitude avec qui elles partagent l'information secrète.

La présente Recommandation propose des méthodes d'authentification fondées sur l'abonnement, c'est-à-dire qu'il faut un contact préalable pour partager une information secrète et des méthodes d'authentification dans lesquelles la cryptographie par clé publique est utilisée directement pour l'authentification ou pour la production du secret partagé.

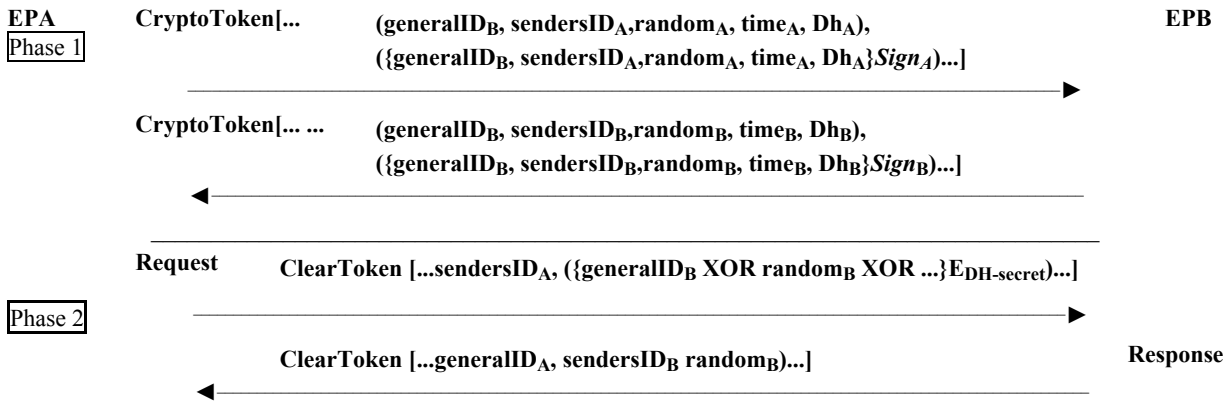
8.1 Echange Diffie-Hellman avec authentification facultative

Cette méthode ne vise pas à réaliser une authentification absolue au niveau de l'utilisateur. Elle assure une signalisation permettant de constituer un secret partagé entre deux entités, pouvant conduire à des données de calcul de clés pour des communications privées.

A l'issue de cet échange, les deux entités posséderont une clé secrète partagée ainsi qu'un algorithme sélectionné qui leur permettra d'utiliser cette clé. Cette clé secrète partagée pourra ensuite être utilisée dans tout échange ultérieur de type demande/réponse. Il convient de noter que, dans de rares cas, l'échange Diffie-Hellman peut produire des clés notoirement *faibles* pour certains algorithmes. Dans ces cas, chaque entité devrait se déconnecter et se reconnecter afin d'établir un nouveau jeu de clés.

La première phase de la Figure 4 montre les données échangées lors d'un échange Diffie-Hellman. La deuxième phase permet à celui qui répond d'authentifier des messages de demande propres à une application ou à un protocole. On notera qu'une nouvelle valeur aléatoire peut être renvoyée avec chaque réponse.

NOTE – Si les messages sont échangés sur un canal non sécurisé, il faut utiliser des signatures numériques (ou toute autre méthode d'authentification de l'origine) pour authentifier les parties entre lesquelles l'information secrète sera partagée. Un élément facultatif de signature (indiqué ci-dessous en ***italiques***) peut aussi être fourni.



[... ...] indique une séquence de jetons.

() indique un jeton particulier, qui peut contenir des éléments multiples.

{}E$_{DH-secret}$ indique que les valeurs contenues sont chiffrées au moyen de la méthode de secret Diffie-Hellman.

Le point d'extrémité B (EPB) connaît la clé secrète partagée qu'il faut utiliser pour déchiffrer l'identificateur **generalID$_B$** en l'associant à l'identificateur **generalID$_A$**, qu'il convient de transmettre également dans le message, dans le champ **generalID$_A$**. On notera que la valeur chiffrée dans la phase 2 est transmise dans le champ **generalID** d'un jeton **clearToken**, afin de simplifier le codage.

Figure 4/H.235.0 – Echange Diffie-Hellman avec authentification facultative

8.2 Authentification sur abonnement

Bien que les procédures décrites ici (ainsi que les algorithmes ISO dont elles sont issues) soient de nature bidirectionnelle, elles ne peuvent être utilisées que dans un seul sens si l'authentification n'est requise que dans ce sens. Les procédures en deux et en trois passages sont décrites. L'authentification mutuelle en deux passages peut être faite dans un sens seulement si les messages provenant du sens opposé ne doivent pas être authentifiés. Ces échanges partent du principe que chaque extrémité possède un certain identificateur bien connu (comme un identificateur en mode texte) qui l'identifie sans équivoque. Dans le cas de la procédure en deux passages, on suppose en outre qu'il existe une référence temporelle acceptable de part et d'autre (permettant de déterminer les horodates). La valeur de la dérive temporelle acceptable relève d'une décision de l'implémentation locale. La procédure en trois passages utilise un numéro produit aléatoirement et qui ne peut pas être découvert (auquel peut être ajoutée la valeur d'un compteur séquentiel "random") pour l'épreuve proposée par l'authentificateur. Ce numéro aléatoire est destiné à la protection contre les attaques par réexécution. Contrairement aux procédures en deux passages, les procédures en trois passages n'authentifient pas le premier message (initial) contenant l'épreuve de l'expéditeur.

Il existe trois variantes différentes d'implémentation, selon les exigences:

1) authentification par mot de passe avec chiffrement symétrique;

2) authentification par mot de passe avec hachage;

3) authentification par certificat avec signatures.

Dans tous les cas, le jeton contiendra les informations décrites dans les paragraphes suivants, selon la variante choisie. On notera que, dans tous les cas, l'identificateur **generalID** peut être connu par examen de la configuration ou d'un répertoire, plutôt que par échange protocolaire dans la bande. Pour simplifier le traitement au niveau du destinataire, l'expéditeur doit inclure son identité dans l'identificateur **sendersID** et mettre l'identificateur **generalID** à l'identification du destinataire.

NOTE 1 – Chaque fois que des horodates sont produites et transmises dans le cadre d'un échange de sécurité, le réalisateur doit prendre les précautions suivantes: la granularité de l'horodate doit être suffisamment fine pour garantir l'incrémentation à chaque nouveau message. En l'absence de cette garantie, des attaques par réexécution sont possibles (par exemple, si l'horodate n'augmente qu'en minutes, un point d'extrémité "C"

peut usurper l'adresse d'un point d'extrémité "A" pendant la minute qui suit le moment où le point d'extrémité "A" a envoyé un message au point d'extrémité "B").

NOTE 2 – Si le message est multidiffusé, il n'est pas sécurisé.

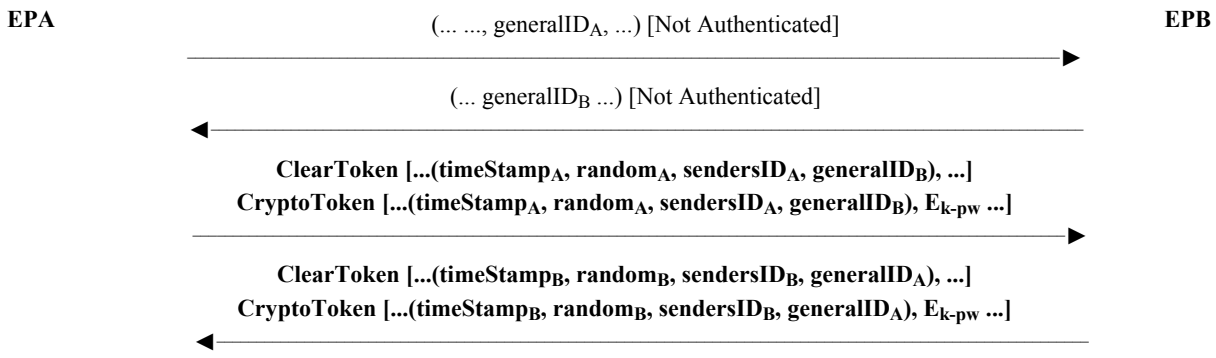
8.2.1 Authentification par mot de passe avec chiffrement symétrique

Les Figures 5 et 6 montrent le format du jeton et l'échange de messages requis pour exécuter ce type d'authentification, respectivement en deux et en trois passages. Ce protocole est fondé sur les § 5.2.1 (deux passages) et 5.2.2 (trois passages) de l'ISO/CEI 9798-2. On suppose qu'un identificateur et le mot de passe associé sont échangés lors de l'abonnement. La clé de chiffrement a une longueur de N octets (comme indiqué par l'identificateur d'algorithme). Elle est formée comme suit:

– si la longueur du mot de passe = N, clé = mot de passe;

– si la longueur du mot de passe < N, la clé est bourrée de zéros;

– si la longueur du mot de passe > N, les N premiers octets sont attribués à la clé, puis le $N + M^e$ octet du mot de passe est combiné par un OU exclusif avec le $Mmod(N)^e$ octet (pour tous les octets au-delà de N). (En d'autres termes, tous les octets "surnuméraires" du mot de passe sont successivement repliés sur la clé par application de la fonction OU exclusif.)



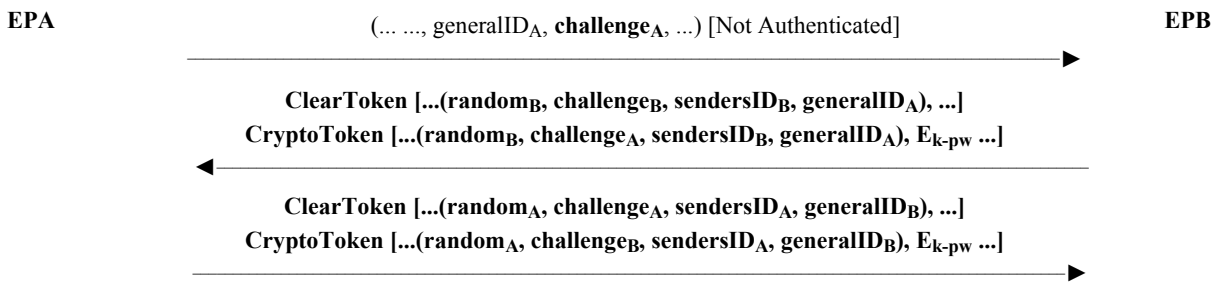
NOTE 1 – Le jeton envoyé en retour par le point d'extrémité EPB est facultatif; s'il est omis, l'authentification est à sens unique.

NOTE 2 – La variable **E_{k-pw}** indique des valeurs qui sont chiffrées au moyen de la clé "k" calculée à partir du mot de passe "pw".

NOTE 3 – **random** est un compteur croissant monotone qui confère l'unicité à plusieurs messages possédant la même horodate.

NOTE 4 – Dans le troisième message, le point EPA fournit un **ClearToken** distinct qui est identifié au moyen du même identificateur OID que celui de **CryptoToken**; il en est de même pour le quatrième message et inversement.

Figure 5/H.235.0 – Authentification par mot de passe avec chiffrement symétrique; deux passages



NOTE 1 – L'épreuve **challenge$_A$** et le **CryptoToken** chiffré envoyé en retour par B à A ne sont pas nécessaires en cas d'authentification à sens unique.

NOTE 2 – La variable **E$_{k-pw}$** indique une fonction de chiffrement qui est chiffrée au moyen de la clé "k" calculée à partir du mot de passe "pw".

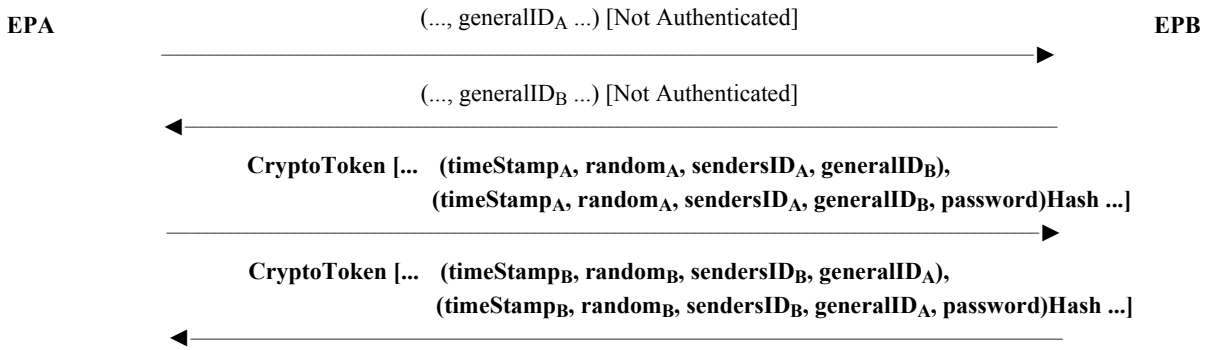
NOTE 3 – Dans le troisième message, le point EPA envoie une nouvelle épreuve **challenge$_A$** en clair dans un **ClearToken** distinct qui est identifié au moyen du même identificateur OID que celui de **CryptoToken**. Le point EPA renvoie également, en réponse, l'épreuve **challenge$_B$** chiffrée; il en est de même pour le deuxième message et inversement.

NOTE 4 – S'il y a plusieurs messages en attente, l'épreuve doit être rendue unique par **random** (c'est-à-dire un compteur croissant monotone).

Figure 6/H.235.0 – Authentification par mot de passe avec chiffrement symétrique; trois passages

8.2.2 Authentification par mot de passe avec hachage

Les Figures 7 et 8 montrent le format du jeton et l'échange de messages requis pour exécuter ce type d'authentification, respectivement en deux et en trois passages. Ce protocole est fondé sur les § 5.2.1 et 5.2.2 de l'ISO/CEI 9798-4; on suppose qu'un identificateur et le mot de passe associé sont échangés au moment de l'abonnement. La Rec. UIT-T H.235.1 contient la description détaillée de la procédure de hachage en deux passages.

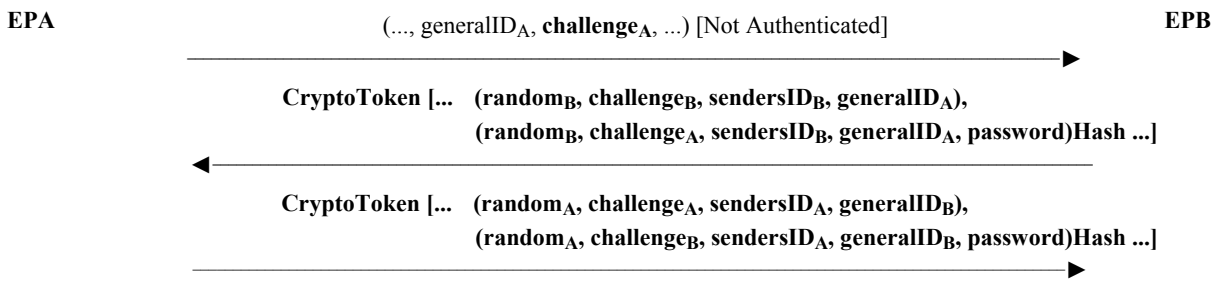


NOTE 1 – Le jeton envoyé en retour par l'extrémité EPB est facultatif; s'il est omis, l'authentification est à sens unique.

NOTE 2 – La variable **Hash** indique une fonction de hachage qui agit sur les valeurs contenues.

NOTE 3 – **random** est un compteur croissant monotone qui confère l'unicité à plusieurs messages possédant la même horodate.

Figure 7/H.235.0 – Authentification par mot de passe avec hachage; deux passages



NOTE 1 – Le jeton envoyé en retour par l'extrémité EPB est facultatif; s'il est omis, l'authentification est à sens unique.

NOTE 2 – La variable **Hash** indique une fonction de hachage qui agit sur les valeurs contenues.

NOTE 3 – Dans le troisième message, le point EPA envoie une nouvelle épreuve **challenge$_A$** en clair dans le **ClearToken** intégré dans **cryptoHashedToken**. Le point EPA renvoie en réponse l'épreuve **challenge$_B$** hachée; il en est de même pour le deuxième message et inversement.

NOTE 4 – S'il y a plusieurs messages en attente, l'épreuve doit être rendue unique par **random** (compteur croissant monotone).

Figure 8/H.235.0 – Authentification par mot de passe avec hachage; trois passages

NOTE 1 – La structure **cryptoHashedToken** est utilisée pour le transfert des paramètres utilisés dans cet échange. Les versions "en clair" des paramètres nécessaires pour calculer la valeur hachée sont incluses dans cette structure. Les réalisateurs doivent inclure l'horodate dans les **hashedVals** et *ne* doivent *pas* inclure le mot de passe (par exemple, le mot de passe et le "**generalID**" devraient être connus *a priori* par le destinataire; ce qui précède peut être omis).

NOTE 2 – La fonction de hachage doit être appliquée à la structure **EncodedGeneralToken** qui englobe au moins les champs ID, horodate et mot de passe. La valeur du mot de passe NE doit PAS être acheminée dans **ClearToken**.

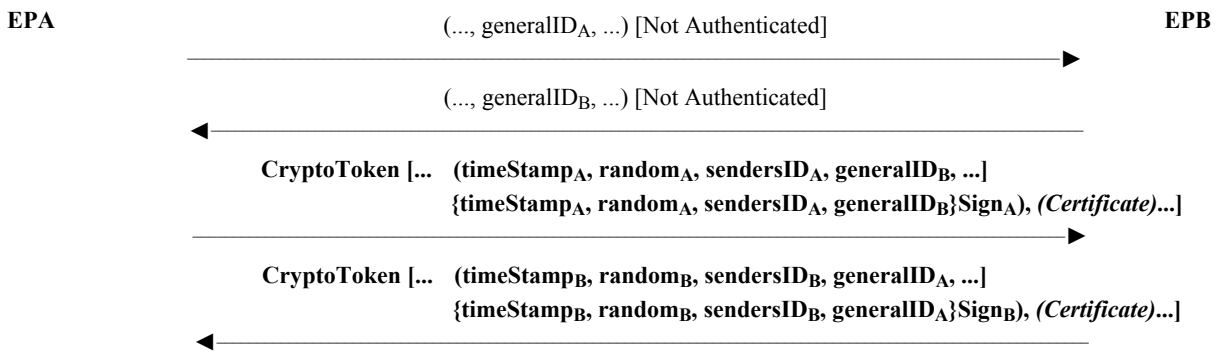
NOTE 3 – Les réalisateurs devraient s'assurer que les mots de passe entrés par l'utilisateur présentent une entropie suffisante. Les mots de passe trop courts ou qui sont sensibles aux attaques de type dictionnaire devraient être refusés. Il peut être intéressant, dans certains cas, de faire passer le mot de passe entré par l'utilisateur par une fonction de hachage cryptographique et d'utiliser les bits de sortie.

8.2.3 Authentification par certificat avec signatures

Les Figures 9 et 10 montrent le format du jeton et l'échange de messages requis pour exécuter ce type d'authentification. Ce protocole est fondé sur le § 5.2.1 de l'ISO/CEI 9798-3; on suppose qu'un identificateur et le certificat associé sont attribués/échangés lors de l'abonnement. La Rec. UIT-T H.235.2 contient la description détaillée de la procédure de signature en deux passages.

NOTE 1 – Un élément facultatif de certificat (indiqué ci-dessous en ***italique***) peut aussi être fourni.

NOTE 2 – Si le message est multidiffusé, l'identificateur de la destination (**generalID$_B$** pour les messages provenant de A et inversement) ne doit pas être inclus dans le jeton **ClearToken**.



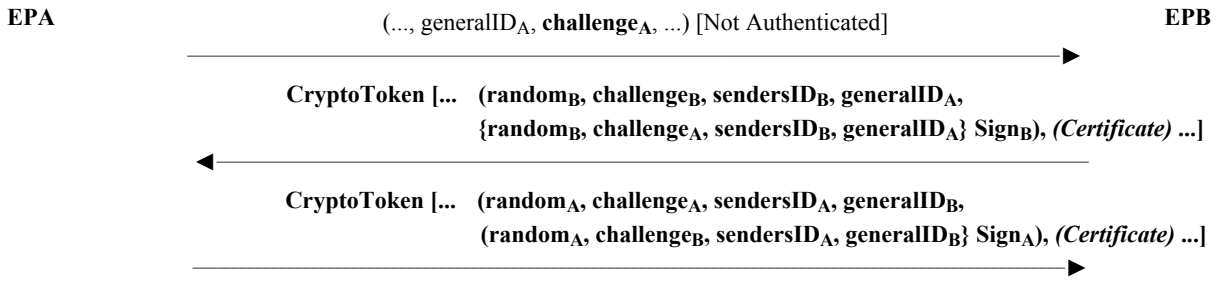
NOTE 1 – Le jeton envoyé en retour par l'extrémité EPB est facultatif; s'il est omis, l'authentification est à sens unique.

NOTE 2 – Un certificat de type "payment" peut, facultativement, être inclus par l'expéditeur situé au point EPA.

NOTE 3 – La variable **Sign** indique une fonction de signature (issue du certificat associé) qui est exécutée sur les valeurs contenues.

NOTE 4 – **random** est un compteur croissant monotone qui confère l'unicité à plusieurs messages possédant la même horodate.

Figure 9/H.235.0 – Authentification par certificat avec signature; deux passages



NOTE 1 – Le jeton envoyé en retour par l'extrémité EPB est facultatif; s'il est omis, l'authentification est à sens unique.

NOTE 2 – Un certificat de type "payment" peut, facultativement, être inclus par l'expéditeur situé au point EPA.

NOTE 3 – La variable **Sign** indique une fonction de signature (issue du certificat associé) qui est exécutée sur les valeurs contenues.

NOTE 4 – Dans le troisième message, le point EPA envoie une nouvelle épreuve **challenge$_A$** en clair avec le **GeneralToken** codé incorporé. Le point EPA renvoie également en réponse l'épreuve **challenge$_B$** signée; il en est de même pour le deuxième message et inversement.

NOTE 5 – Si plusieurs messages sont en attente, l'épreuve doit être rendue unique par **random** (compteur croissant monotone).

Figure 10/H.235.0 – Authentification par certificat avec signature; trois passages

8.2.4 Utilisation du secret partagé et des mots de passe

Dans la présente Recommandation, certaines techniques cryptographiques symétriques sont appliquées aux fins de l'authentification, de l'intégrité et de la confidentialité. Les termes "mot de passe" et "secret partagé" sont ici employés lorsqu'on utilise des techniques symétriques. On entend par le terme générique de "secret partagé" une chaîne binaire arbitraire. Cette chaîne peut être attribuée ou configurée au moment de l'abonnement de l'utilisateur ou faire partie d'un calcul dans la bande (par exemple secret partagé déterminé à partir d'un échange Diffie-Hellman).

Un mot de passe peut être assimilé à une chaîne de caractères alphanumériques qui peut être mémorisée par les utilisateurs. Evidemment, l'utilisation des mots de passe ne va pas sans certaines précautions: pour offrir des garanties de sécurité suffisantes, les mots de passe doivent être choisis aléatoirement dans un grand espace, ils doivent présenter une entropie suffisante de manière à ne pas pouvoir être découverts et, enfin, ils doivent être régulièrement modifiés. Les règles de création et de mise à jour des mots de passe n'entrent pas dans le cadre de la présente Recommandation.

Une méthode efficace pour tirer parti des mots de passe et des secrets partagés consiste à transformer la chaîne du mot de passe de l'utilisateur en une chaîne binaire de longueur fixe qui devient ainsi le secret partagé, au moyen d'une fonction de hachage unilatéral robuste sur le plan cryptographique.

A titre d'exemple, dans le cas du profil de sécurité visé dans la Rec. UIT-T H.235.1, la fonction de hachage SHA1 appliquée à la chaîne du mot de passe produit un secret partagé de 20 octets. Le hachage présente l'avantage de non seulement occulter le mot de passe proprement dit mais aussi de définir un format de chaîne binaire de longueur fixe sans réellement réduire l'entropie pour autant.

Par conséquent,

secret partagé: = SHA1 (mot de passe).

8.3 Procédures et signalisation RAS pour l'authentification

La présente Recommandation n'indiquera explicitement aucune forme de secret des communications de messages entre portiers et points d'extrémité. Il existe deux types d'authentification pouvant être utilisés. Le premier type est fondé sur un chiffrement symétrique ne nécessitant aucun contact préalable entre le point d'extrémité et le portier. Le deuxième type est fondé sur un abonnement et aura deux formes: mot de passe ou certificat. Toutes ces formes sont issues des procédures indiquées aux § 8, 8.2.1, 8.2.2 et 8.2.3. Dans la présente Recommandation, les étiquettes génériques (des points EPA et EPB), indiquées dans les paragraphes précédents, représenteront respectivement le point d'extrémité et le portier.

8.3.1 Authentification entre point d'extrémité et portier (non fondée sur abonnement)

Ce mécanisme peut fournir au portier un lien cryptographique établissant qu'un point d'extrémité donné, qui s'était préalablement enregistré, est bien celui qui émet les messages RAS ultérieurs. Il convient de noter que ce procédé peut ne pas fournir au point d'extrémité une quelconque authentification du portier, à moins que l'élément facultatif de signature soit inclus. L'établissement de la relation d'identité s'effectue lorsque le terminal émet la demande **GRQ**, comme indiqué au § 7.2.1/H.323. L'échange Diffie-Hellman s'effectue conjointement avec les messages **GRQ** et **GCF**, comme indiqué dans la première phase du § 8. La clé secrète partagée doit ensuite être utilisée pour toute demande **RRQ/URQ** subséquente, envoyée par le terminal au portier. Si un portier fonctionne dans ce mode et reçoit une demande **GRQ** sans jeton contenant la valeur *DHset* ou une valeur algorithmique acceptable, il doit renvoyer, dans le message de rejet **DRJ**, le code de cause **securityDenial** ou tout autre code d'erreur de sécurité approprié conformément au § 11.1.

La clé secrète partagée Diffie-Hellman qui a été créée au cours de l'échange de messages **GRQ/GCF** peut être utilisée pour l'authentification dans des messages de type **xRQ** ultérieurs. Les procédures suivantes doivent être utilisées pour réaliser ce mode d'authentification.

Terminal (**xRQ**)

1) le terminal doit fournir toutes les informations contenues dans le message, comme décrit dans les paragraphes appropriés de la Rec. UIT-T H.225.0;
2) le terminal doit chiffrer l'identificateur **GatekeeperIdentifier** (renvoyé dans le message **GCF**) au moyen de la clé secrète partagée qui a été négociée. Ce cryptogramme doit être transmis dans un jeton **clearToken** (voir § 8.1) en tant qu'identificateur **generalID**.

Les 16 bits du compteur **random** puis du numéro **requestSeqNum** doivent être combinés par l'opérateur OU exclusif avec chacun des 16 bits de l'identificateur **GatekeeperIdentifier**. Si cet identificateur **GatekeeperIdentifier** ne se termine pas par une limite paire à la 16^{e} position, les 8 derniers bits de l'identificateur **GatekeeperIdentifier** doivent être combinés par l'opérateur OU exclusif avec l'octet de plus faible poids de la valeur du compteur **random** puis avec celui du numéro **requestSeqNum**. L'identificateur **GatekeeperIdentifier** doit être chiffré au moyen de

l'algorithme sélectionné dans le message **GCF** (algorithmOID) et au moyen de l'intégralité du secret partagé.

L'exemple suivant donne un aperçu de cette procédure:

RND16: valeur à 16 bits du compteur Random;

SQN16: valeur à 16 bits du numéro requestSeqNum;

BMPX: le X^e caractère BMP de l'identificateur GatekeeperIdentifier

BMP1' = (BMP1) XOR (RND16) XOR (SQN16)

BMP2' = (BMP2) XOR (RND16) XOR (SQN16)

BMP3' = (BMP3) XOR (RND16) XOR (SQN16)

BMP4' = (BMP4) XOR (RND16) XOR (SQN16)

BMP5' = (BMP5) XOR (RND16) XOR (SQN16)

:

:

BMPn' = (BMPn) XOR (RND16) XOR (SQN16)

Afin de relier cryptographiquement ce message et les messages ultérieurs avec l'entité qui s'est enregistrée initialement (le point d'extrémité qui a émis la demande **RRQ**), la valeur la plus récente du compteur **random** qui a été renvoyée doit être utilisée (cette valeur peut être plus récente que celle qui a été renvoyée dans le message **RCF** faisant suite à un message **xCF** ultérieur).

Portier (**xCF/xRJ**)

1) le portier doit chiffrer son identificateur **GatekeeperIdentifier** (conformément à la procédure ci-dessus) avec la clé secrète partagée qui est associée au pseudonyme du point d'extrémité; il doit ensuite le comparer à la valeur contenue dans la demande **xRQ**;
2) le portier doit renvoyer un message de rejet **xRJ** si les deux valeurs chiffrées ne correspondent pas;
3) en cas de correspondance, le portier doit appliquer toute logique locale éventuelle puis répondre par un message **xCF** ou **xRJ**;
4) si un message **xCF** est envoyé par le portier, il devrait contenir un identificateur **EndpointIdentifier** assigné et une nouvelle valeur dans le champ **random** d'un jeton **clearToken**.

Pour la représentation graphique de cet échange, voir la phase 2 de la Figure 4. Le portier connaît la clé secrète partagée qu'il faut utiliser pour déchiffrer l'identificateur de portier indiqué par le pseudonyme dans le message.

8.3.2 Authentification entre point d'extrémité et portier (fondée sur abonnement)

Tous les messages RAS autres que **GRQ/GCF** devraient contenir les jetons d'authentification requis par le mode de fonctionnement spécifique. Il existe trois variantes différentes qui peuvent être implémentées, selon les exigences et l'environnement:

1) authentification par mot de passe avec chiffrement symétrique;
2) authentification par mot de passe avec hachage;
3) authentification par certificat avec signatures.

Dans tous les cas, le jeton contiendra les informations décrites dans les paragraphes suivants, selon la variante choisie. Si un portier fonctionne en mode sécurisé et reçoit un message RAS sans valeur de jeton acceptable, il doit renvoyer un code de cause **securityDenial** ou tout autre code d'erreur de sécurité approprié conformément au § 11.1 dans le message de rejet. Dans tous les cas, le jeton

renvoyé par le portier est facultatif: s'il est omis, seule une authentification à sens unique est effectuée.

8.3.2.1 Authentification par mot de passe avec chiffrement symétrique

La phase de découverte du portier (**GRQ**, **GCF** et **GRJ**) peut échouer comme indiqué sur la Figure 11, ou au contraire aboutir, au moyen du paramètre **cryptoTokens**.

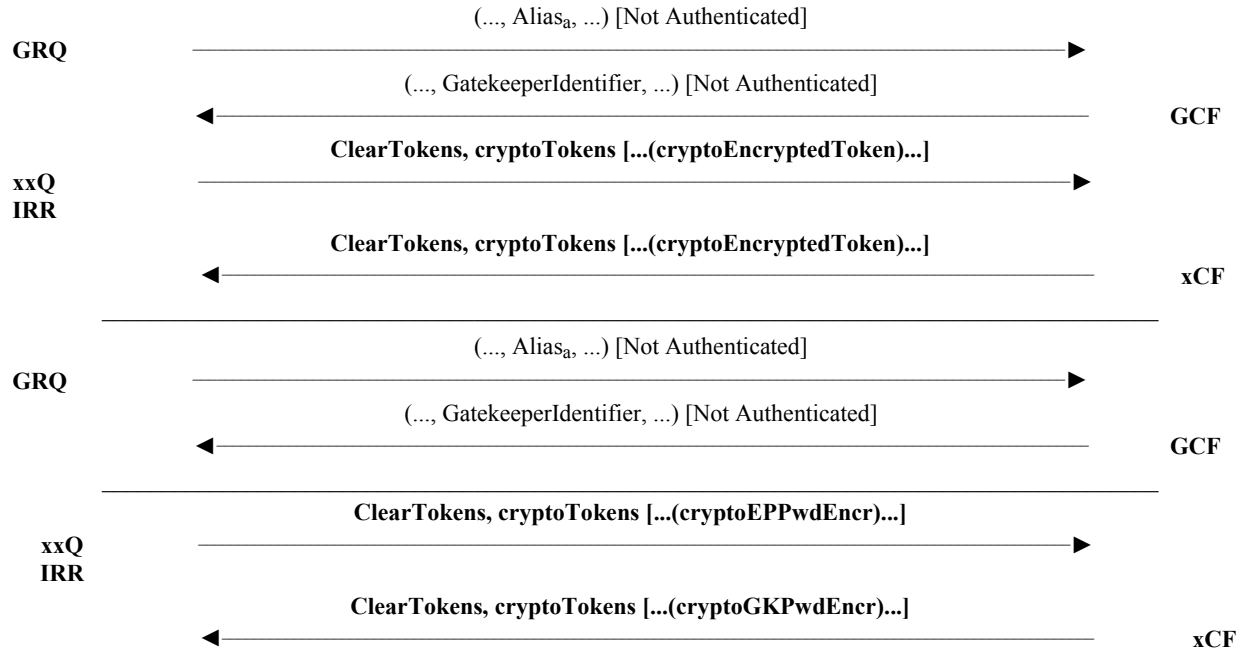


Figure 11/H.235.0 – Authentification par mot de passe avec chiffrement symétrique

8.3.2.2 Authentification par mot de passe avec hachage

La phase de découverte du portier (**GRQ**, **GCF** et **GRJ**) peut échouer comme indiqué sur la Figure 12, ou au contraire aboutir, conformément à la Rec. UIT-T H.235.1, au moyen du paramètre **cryptoTokens**.

Figure 12/H.235.0 – Authentification par mot de passe avec hachage

8.3.2.3 Authentification par certificat avec signatures

La phase de découverte du portier (**GRQ**, **GCF** et **GRJ**) peut échouer comme indiqué sur la Figure 13, ou au contraire aboutir, conformément à la Rec. UIT-T H.235.2, au moyen du paramètre **cryptoTokens**.

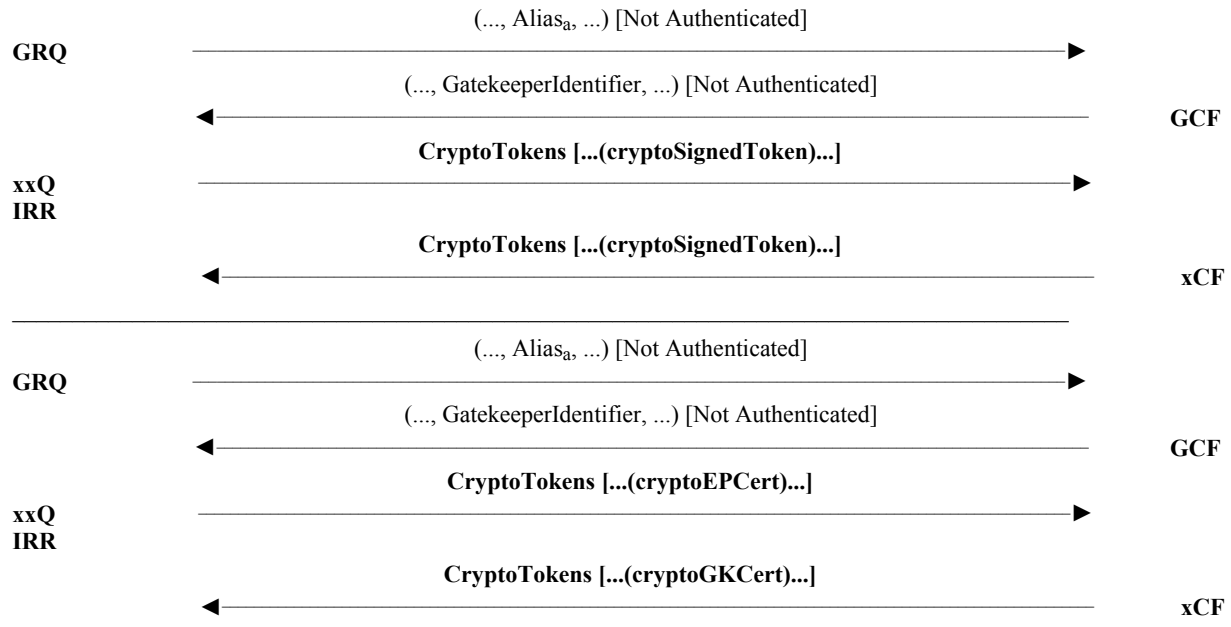


Figure 13/H.235.0 – Authentification par certificat avec signatures

8.4 Gestion de clés sur le canal RAS

Dans certaines circonstances, il est souhaitable que les clés de session (RAS) soient distribuées par un portier à un ou plusieurs points d'extrémité placés sous son contrôle, ou par un point d'extrémité à un autre. Dans le mécanisme qui est proposé, on suppose que le portier et le point d'extrémité partagent une clé secrète forte ou connaissent chacun la clé publique de l'autre. On peut citer en exemple le cas d'un portier routeur qui envoie une clé de session à un point d'extrémité dans un

message RAS (par exemple **RCF** ou **ACF**) à utiliser pour le chiffrement d'un canal de signalisation routé par le portier. Un autre exemple est celui d'un portier émettant une clé de session à utiliser pour le chiffrement de communications RAS successives (par exemple **RRQ** ou **ARQ**).

Ce mécanisme est analogue à celui utilisé pour la distribution des clés de session de média. Il peut être utilisé pour éviter d'avoir à négocier une clé dans certaines circonstances.

Pour le transfert des clés, le champ optionnel **h235Key** de **ClearToken** devrait être utilisé dans la H.235v3 ou ultérieur. La souplesse offerte par l'élément **H235Key** permettra de transporter les éléments de clé de chiffrement en utilisant:

- un canal sécurisé (option **secureChannel**) en supposant que le canal RAS ou de signalisation d'appel est sécurisé par d'autres moyens (IPsec/SSL, etc.);
- un secret de chiffrement partagé sur un canal en clair (choix **sharedSecret**), ou de même et de préférence le choix **secureSharedSecret**;
- un chiffrement et un certificat de clé publique sur un canal en clair (option **certProtectedKey**).

L'utilisation des clés de session RAS échangées et leur application aux messages RAS ou de signalisation d'appel et/ou aux canaux de transport appellent un complément d'étude.

9 Authentification asymétrique et échange de clés au moyen de systèmes de chiffrement à courbe elliptique

La présente Recommandation propose des techniques sophistiquées à courbe elliptique s'appliquant à la signature, à la gestion des clés et au chiffrement. Les principaux avantages par rapport aux techniques asymétriques "classiques" telles que l'algorithme RSA sont:

- des clés cryptographiques plus courtes assurant une sécurité comparable à celle de l'algorithme RSA: généralement, la longueur des clés des systèmes de chiffrement à courbe elliptique est de 160 bits, soit l'équivalent, au plan de la sécurité, à une clé RSA de 1024 bits. La clé plus courte consomme moins de mémoire de stockage et rend l'utilisation des systèmes cryptographiques à courbe elliptique particulièrement attrayants dans les cartes à puce et autres dispositifs à faible capacité de mémoire. Dans le contexte H.323, les types de point d'extrémité simple audio sécurisé (SASET, *secured audio simple endpoint type*) fondés sur l'Annexe J/H.323 doivent être peu onéreux et conviennent donc fort bien au déploiement des techniques à courbe elliptique;
- la grande vitesse de traitement atteinte tant au niveau du logiciel que du matériel: plus les clés sont courtes, plus le traitement est rapide, ce qui se traduit par une réponse interactive (utilisateur) plus rapide.

Tous les renseignements généraux, explications et procédures de traitement concernant la cryptographie à courbe elliptique sont donnés dans *ATM Security Specification Version 1.1,* section 8.7. Il est recommandé de coder les points elliptiques dans leur notation affine, non comprimée, sans recourir à la méthode de compression/décompression des points. D'autres informations à ce sujet figurent dans l'ISO/CEI 15946-1 et l'ISO/CEI 15946-2.

9.1 Gestion de clés

Les systèmes de concordance de clés de type Diffie-Hellman à courbe elliptique sont analogues au cas classique mod-p, également défini dans la présente Recommandation. Deux cas peuvent se présenter:

- courbes elliptiques sur un champ principal: **eckasdhp** contient la courbe elliptique et les paramètres Diffie-Hellman;

- courbes elliptiques de caractéristique 2: **eckasdh2** contient la courbe elliptique et les paramètres Diffie-Hellman.

La structure ECKASDH se rapporte aux deux cas. Quelques exemples de courbes elliptiques sont énumérés dans l'ISO/CEI 15946-1. Toute autre courbe elliptique appropriée peut être utilisée.

En raison de la structure ordonnée qu'offre la signalisation du jeton **ClearToken**, **dhkey** et **eckasdhkey** ne doivent pas être présents en même temps; un des deux seulement sera présent lors de l'application de l'échange de clés Diffie-Hellman.

Remarque – Il ne faut pas confondre les paramètres secrets choisis aléatoirement, ***a*** par la partie A et ***b*** par la partie B, avec les coefficients ***a*** et ***b*** de Weierstrass.

9.2 Signature numérique

Le champ **ECGDSASignature** contient les valeurs **r** et **s** de la signature numérique à courbe elliptique calculée. La section 8.7.3 de l'*ATM Security Specification Version 1.1* et le chapitre 5 de l'ISO/CEI 15946-2 contiennent des informations complémentaires sur l'algorithme de signature EC-GDSA.

La signature numérique à courbe elliptique **ECGDSA** doit être codée en ASN.1 puis placée dans le champ **signature** de la macro **SIGNED** de la présente Recommandation. En ce qui concerne la signature numérique, l'expéditeur doit inclure l'identificateur d'objet dans **algorithmOID** permettant au destinataire de déterminer l'utilisation d'une signature numérique à courbe elliptique.

10 Fonction pseudo aléatoire (PRF)

Le présent paragraphe définit une fonction pseudo-aléatoire PRF (*pseudo-random function*) dans le but de déduire des clés dynamiques à partir d'éléments de clé statique et d'une valeur aléatoire.

NOTE – Cette fonction PRF est identique à la fonction PRF MIKEY (voir RFC 3830, section 4.1.2).

La méthode de calcul de la clé fait appel aux paramètres d'entrée suivants:

- *inkey*: clé d'entrée de la fonction de dérivation;
- *inkey_len*: longueur en bits de la clé d'entrée;
- *label*: étiquette spécifique, dépendant du type de clé à obtenir et de la valeur aléatoire **challenge**;
- *outkey_len*: longueur souhaitée en bits de la clé de sortie.

La fonction pseudo-aléatoire a pour résultat:

- *outkey*: clé de sortie de la longueur désirée.

Cette fonction PRF doit utiliser la fonction PRF définie dans la norme RFC 3830, section 4.1.2.

11 Reprise sur erreur de sécurité

La présente Recommandation ne spécifie ni ne préconise de méthodes permettant aux points d'extrémité de surveiller le secret absolu de leurs communications. Elle recommande cependant des mesures à prendre lors de la détection d'une perte du secret des communications.

Si l'un des points d'extrémité détecte une brèche dans la sécurité du canal de connexion d'appel (par exemple un canal H.225.0 pour des systèmes H.323), il devrait immédiatement fermer la connexion conformément aux procédures protocolaires appropriées au point d'extrémité en question (pour le § 8.5/H.323 à l'exception de l'étape B-5).

Si l'un des points d'extrémité détecte une brèche dans la sécurité du canal H.245 ou du canal logique de données sécurisé (**h235Control**), il devrait immédiatement fermer la connexion conformément

aux procédures protocolaires appropriées au point d'extrémité en question (pour le § 8.5/H.323 à l'exception de l'étape B-5).

Si l'un des points d'extrémité détecte une perte du secret des communications sur l'un des canaux logiques, il devrait immédiatement demander une nouvelle clé (par une demande **encryptionUpdateRequest**) et/ou fermer le canal logique. A la discrétion du pont de conférence, une perte du secret des communications sur un canal logique peut causer la fermeture de tous les autres canaux logiques et/ou le recalcul de leurs clés. Le pont de conférence doit envoyer une demande de mise à jour **encryptionUpdateRequest** et une mise à jour **encryptionUpdate** à tous les points d'extrémités affectés.

A la discrétion du pont de conférence, une erreur de sécurité sur un canal individuel peut provoquer la fermeture des connexions à tous les points d'extrémité de la conférence – ce qui met fin à celle-ci.

11.1 Signalisation des erreurs

Un portier disposant de capacités de sécurité ou une autre entité H.225.0 avec sécurité améliorée doit fournir des indications d'erreur. Les erreurs de sécurité indiquent que cette entité n'a pas été en mesure de traiter correctement le message reçu. Chaque fois que cela est possible, un code d'erreur détaillé doit être fourni.

- **securityWrongSyncTime** indique que l'expéditeur a rencontré un problème de sécurité avec des horodates inappropriées. Cela peut être dû à un problème avec le chronoserveur, une perte de synchronisation ou un temps de propagation excessif sur le réseau.
- **securityReplay** indique qu'une attaque par réexécution a été constatée. C'est le cas lorsque le même numéro de séquence apparaît plusieurs fois pour une horodate donnée.
- **securityWrongGeneralID** indique une non-concordance de l'identificateur général dans le message. Cela peut être dû à un adressage erroné.
- **securityWrongSendersID** indique une non-concordance de l'identificateur de l'expéditeur dans le message. Cela peut être dû à une entrée erronée de l'utilisateur.
- **securityIntegrityFailed** indique un échec de contrôle d'intégrité/signature. Dans le cas de la Rec. UIT-T H.235.1, cela peut être dû à un mot de passe erroné ou mal saisi pendant la demande initiale ou être dû à une attaque active. Pour ce qui est des Recommandations UIT-T H.235.2 et H.235.3, cette erreur indique que la vérification de signature numérique dans le message a échoué. Cela peut être dû à une clé privée/publique erronée ou à une attaque active.
- **securityWrongOID** indique toute non-concordance dans les identificateurs OID de jeton (en clair ou chiffré) ou des identificateurs OID d'algorithme. Cette erreur indique les différents algorithmes/profils de sécurité implémentés.
- **securityDHmismatch** indique toute non-concordance entre les paramètres Diffie-Hellman échangés. Cette erreur pourrait indiquer les différents ensembles de paramètres DH voire les différents algorithmes de chiffrement vocal implémentés.
- **securityCertificateExpired** indique qu'un certificat a expiré.
- **securityCertificateDateInvalid** indique qu'un certificat n'est pas encore valide.
- **securityCertificateRevoked** indique qu'on a constaté qu'un certificat était révoqué.
- **securityCertificateNotReadable** indique que le certificat n'a pas pu être correctement décodé en ASN.1 ou se trouve dans un format non valable.
- **securityCertificateSignatureInvalid** indique que la signature du certificat n'est pas correcte.
- **securityCertificateMissing** indique qu'un certificat était attendu mais qu'il manque ou que le certificat n'a pas pu être localisé.

- **securityCertificateIncomplete** indique que certaines extensions de certificat attendues ne sont pas présentes.
- **securityUnsupportedCertificateAlgOID** indique que certains algorithmes de chiffrement (par exemple un algorithme de hachage ou avec des signatures numériques) utilisés dans le certificat ne sont pas compris ou ne sont pas pris en charge. Dans la réponse renvoyée, l'expéditeur peut envoyer plusieurs certificats acceptables dans des jetons différents afin de faciliter la sélection d'un certificat approprié par le destinataire.
- **securityUnknowCA** indique que le certificat CA/racine n'a pu être trouvé ou que le certificat n'a pas pu être associé à une autorité CA de confiance.

Dans tous les autres cas où l'opération de sécurité H.235 a échoué, l'erreur **securityDenial** pour la signalisation RAS H.225.0 ou l'erreur **securityDenied** pour la signalisation d'appel H.225.0 doit être renvoyée.

NOTE 1 – Les erreurs securityWrongSyncTime, securityReplay, securityWrongGeneralID, securityWrongSendersID, SecurityIntegrityFailed, securityDHmismatch et securityWrongOID peuvent se produire dans les profils de sécurité H.235.1, H.235.2 ou H.235.3.

NOTE 2 – Les erreurs securityCertificateExpired, securityCertificateDateInvalid, securityCertificateRevoked, securityCertificateNotReadable, securityCertificateSignatureInvalid, securityCertificateMissing, securityCertificateIncomplete, securityUnsupportedCertificateAlgOID et securityUnknownCA peuvent se produire dans les profils de sécurité H.235.2 ou H.235.3.

Annexe A

ASN.1 H.235

```
H235-SECURITY-MESSAGES DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

-- EXPORTS All

ChallengeString         ::= OCTET STRING (SIZE(8..128))
TimeStamp               ::= INTEGER(1..4294967295)     -- seconds since 00:00
                                                       -- 1/1/1970 UTC
RandomVal               ::= INTEGER -- 32-bit Integer
Password                ::= BMPString (SIZE (1..128))
Identifier              ::= BMPString (SIZE (1..128))
KeyMaterial             ::= BIT STRING(SIZE(1..2048))

NonStandardParameter ::= SEQUENCE
{
     nonStandardIdentifier   OBJECT IDENTIFIER,
     data                    OCTET STRING
}

-- if local octet representations of these bit strings are used they shall
-- utilize standard Network Octet ordering (e.g., Big Endian)
DHset ::= SEQUENCE
{
     halfkey        BIT STRING (SIZE(0..2048)), -- = g^x mod n
     modSize        BIT STRING (SIZE(0..2048)), --  n
     generator      BIT STRING (SIZE(0..2048)), -- g
     ...
}
```

```
ECpoint ::= SEQUENCE -- uncompressed (x, y) affine coordinate representation of
                     -- an elliptic curve point
{
     x         BIT STRING (SIZE(0..511)) OPTIONAL,
     y         BIT STRING (SIZE(0..511)) OPTIONAL,
     ...
}

ECKASDH::= CHOICE -- parameters for elliptic curve key agreement scheme Diffie-
Hellman
{
     eckasdhp SEQUENCE -- parameters for elliptic curves of prime field
     {
          public-key    ECpoint, -- This field contains representation of
               -- the ECKAS-DHp public key value. This field contains the
               -- initiator's ECKAS-DHp public key value (aP) when this
               -- information element is sent from originator to receiver. This
               -- field contains the responder's ECKAS-DHp public key value (bP)
               -- when this information element is sent back from receiver to
               -- originator.
          modulus       BIT STRING (SIZE(0..511)), -- This field contains
               -- representation of the ECKAS-DHp public modulus value (p).
          base          ECpoint, -- This field contains representation of the
               -- ECKAS-DHp public base (P).
          weierstrassA  BIT STRING (SIZE(0..511)), -- This field contains
               -- representation of the ECKAS-DHp Weierstrass coefficient (a).
          weierstrassB  BIT STRING (SIZE(0..511)) -- This field contains
               -- representation of the ECKAS-DHp Weierstrass coefficient (b).
     },

     eckasdh2 SEQUENCE -- parameters for elliptic curves of characteristic 2
     {
          public-key    ECpoint, -- This field contains representation of
               -- the ECKAS-DH2 public key value.
               -- This field contains the initiator's ECKAS-DH2 public key value
               -- (aP) when this information element is sent from originator to
               -- receiver. This field contains the responder's ECKAS-DH2 public
               -- key value (bP) when this information element is sent back from
               -- receiver to originator.
          fieldSize     BIT STRING (SIZE(0..511)), -- This field contains
               -- representation of the ECKAS-DH2 field size value (m).
          base          ECpoint, -- This field contains representation of the
               -- ECKAS-DH2 public base (P).
          weierstrassA  BIT STRING (SIZE(0..511)), -- This field contains
               -- representation of the ECKAS-DH2 Weierstrass coefficient (a).
          weierstrassB  BIT STRING (SIZE(0..511)) -- This field contains
               -- representation of the ECKAS-DH2 Weierstrass coefficient (b).
     },
     ...
}

ECGDSASignature::= SEQUENCE -- parameters for elliptic curve digital signature
               -- algorithm
{
     r         BIT STRING (SIZE(0..511)), -- This field contains the
               -- representation of the r component of the ECGDSA digital
               -- signature.
     s         BIT STRING (SIZE(0..511)) -- This field contains the
               -- representation of the s component of the ECGDSA digital
               -- signature.
}
```

```
TypedCertificate ::= SEQUENCE
{
     type           OBJECT IDENTIFIER,
     certificate    OCTET STRING,
     ...
}

AuthenticationBES ::= CHOICE

{
     default        NULL, -- encrypted ClearToken
     radius         NULL, -- RADIUS-challenge/response
     ...

}

AuthenticationMechanism  ::= CHOICE
{
     dhExch         NULL, -- Diffie-Hellman
     pwdSymEnc      NULL, -- password with symmetric encryption
     pwdHash        NULL, -- password with hashing
     certSign       NULL, -- Certificate with signature
     ipsec          NULL, -- IPSEC based connection
     tls            NULL,
     nonStandard    NonStandardParameter, -- something else.
     ...,
     authenticationBES  AuthenticationBES, -- user authentication for BES
     keyExch   OBJECT IDENTIFIER -- key exchange profile
}

ClearToken          ::= SEQUENCE  -- a "token" may contain multiple value types.
{
     tokenOID       OBJECT IDENTIFIER,
     timeStamp      TimeStamp OPTIONAL,
     password       Password OPTIONAL,
     dhkey          DHset OPTIONAL,
     challenge      ChallengeString OPTIONAL,
     random         RandomVal OPTIONAL,
     certificate    TypedCertificate OPTIONAL,
     generalID      Identifier OPTIONAL,
     nonStandard    NonStandardParameter OPTIONAL,
     ...,
     eckasdhkey     ECKASDH OPTIONAL,  -- elliptic curve Key Agreement
                                       -- Scheme-Diffie Hellman Analogue
                                       -- (ECKAS-DH)
     sendersID      Identifier OPTIONAL,
     h235Key        H235Key OPTIONAL, -- central distributed key in V3
     profileInfo    SEQUENCE OF ProfileElement OPTIONAL  -- profile-specific
}

--   An object identifier should be placed in the tokenOID field when a
--   ClearToken is included directly in a message (as opposed to being
--   encrypted). In all other cases, an application should use the
--   object identifier { 0 0 } to indicate that the tokenOID value is not
--   present.
--   Start all the cryptographic parameterized types here...
--
```

```
ProfileElement     ::= SEQUENCE
{
     elementID     INTEGER (0..255), -- element identifier, as defined by
                                     -- profile
     paramS        Params OPTIONAL,  -- any element-specific parameters
     element       Element OPTIONAL, -- value in required form
     …
}

Element ::= CHOICE
{
     octets             OCTET STRING,
     integer            INTEGER,
     bits               BIT STRING,
     name               BMPString,
     flag               BOOLEAN,
     …
}



SIGNED { ToBeSigned } ::= SEQUENCE {
     toBeSigned         ToBeSigned,
     algorithmOID       OBJECT IDENTIFIER,
     paramS             Params,   -- any "runtime" parameters
     signature          BIT STRING -- could be an RSA or an ASN.1 coded
ECGDSA Signature
} ( CONSTRAINED BY { -- Verify or Sign Certificate -- } )


ENCRYPTED { ToBeEncrypted } ::= SEQUENCE {
     algorithmOID       OBJECT IDENTIFIER,
     paramS             Params,   -- any "runtime" parameters
     encryptedData      OCTET STRING
} ( CONSTRAINED BY { -- Encrypt or Decrypt -- ToBeEncrypted } )

HASHED { ToBeHashed } ::= SEQUENCE {
     algorithmOID       OBJECT IDENTIFIER,
     paramS             Params,   -- any "runtime" parameters
     hash               BIT STRING
} ( CONSTRAINED BY { -- Hash -- ToBeHashed } )

IV8 ::= OCTET STRING (SIZE(8)) -- initial value for 64-bit block ciphers
IV16 ::= OCTET STRING (SIZE(16)) -- initial value for 128-bit block ciphers

-- signing algorithm used must select one of these types of parameters
-- needed by receiving end of signature.

Params ::= SEQUENCE {
     ranInt         INTEGER OPTIONAL, -- some integer value
     iv8            IV8 OPTIONAL, -- 8-octet initialization vector
     ...,
     iv16           IV16 OPTIONAL,-- 16-octet initialization vector
     iv             OCTET STRING OPTIONAL, -- arbitrary length initialization
     vector
     clearSalt      OCTET STRING OPTIONAL -- unencrypted salting key for
     encryption
}

EncodedGeneralToken ::= TYPE-IDENTIFIER.&Type (ClearToken -- general usage token
-- )
PwdCertToken ::= ClearToken (WITH COMPONENTS {..., timeStamp PRESENT, generalID
PRESENT})
EncodedPwdCertToken ::= TYPE-IDENTIFIER.&Type (PwdCertToken)
```

```
CryptoToken::= CHOICE
{

     cryptoEncryptedToken SEQUENCE -- General purpose/application specific token
     {
          tokenOID       OBJECT IDENTIFIER,
          token          ENCRYPTED { EncodedGeneralToken }
     },
     cryptoSignedToken  SEQUENCE -- General purpose/application specific token
     {
          tokenOID       OBJECT IDENTIFIER,
          token          SIGNED { EncodedGeneralToken }
     },
     cryptoHashedToken SEQUENCE -- General purpose/application specific token
     {
          tokenOID            OBJECT IDENTIFIER,
          hashedVals          ClearToken,
          token HASHED { EncodedGeneralToken }
     },
     cryptoPwdEncr ENCRYPTED { EncodedPwdCertToken },
     ...
}

-- These allow the passing of session keys within the H.245 OLC structure.
-- They are encoded as standalone ASN.1 and based as an OCTET STRING within
-- H.245
H235Key   ::=CHOICE  -- This is used with the H.245 or ClearToken "h235Key"
field
{
     secureChannel           KeyMaterial,
     sharedSecret            ENCRYPTED {EncodedKeySyncMaterial},
     certProtectedKey        SIGNED {EncodedKeySignedMaterial },
     ...,
     secureSharedSecret      V3KeySyncMaterial -- for H.235 V3 endpoints
}


KeySignedMaterial ::= SEQUENCE {
     generalId      Identifier, -- slave's alias
     mrandom        RandomVal, -- master's random value
     srandom        RandomVal OPTIONAL, -- slave's random value
     timeStamp      TimeStamp OPTIONAL, -- master's timestamp for unsolicited EU
     encrptval      ENCRYPTED { EncodedKeySyncMaterial }
}
EncodedKeySignedMaterial ::= TYPE-IDENTIFIER.&Type (KeySignedMaterial)

H235CertificateSignature     ::= SEQUENCE
{
     certificate             TypedCertificate,
     responseRandom          RandomVal,
     requesterRandom         RandomVal OPTIONAL,
     signature               SIGNED { EncodedReturnSig },
     ...
}

ReturnSig ::= SEQUENCE {
     generalId               Identifier, -- slave's alias
     responseRandom          RandomVal,
     requestRandom           RandomVal OPTIONAL,
     certificate             TypedCertificate OPTIONAL -- requested certificate
}
```

```
EncodedReturnSig ::= TYPE-IDENTIFIER.&Type (ReturnSig)
KeySyncMaterial    ::= SEQUENCE
{
     generalID     Identifier,
     keyMaterial   KeyMaterial,
     ...
}
EncodedKeySyncMaterial  ::=TYPE-IDENTIFIER.&Type (KeySyncMaterial)



V3KeySyncMaterial  ::= SEQUENCE
{
     generalID               Identifier OPTIONAL, -- peer terminal ID
     algorithmOID            OBJECT IDENTIFIER OPTIONAL, -- encryption algorithm
     paramS                  Params, -- IV
     encryptedSessionKey     OCTET STRING OPTIONAL, -- encrypted session key
     encryptedSaltingKey     OCTET STRING OPTIONAL, -- encrypted media salting
                                                    -- key
     clearSaltingKey         OCTET STRING OPTIONAL, -- unencrypted media salting
                                                    -- key
     paramSsalt              Params OPTIONAL, -- IV (and clear salt) for salting
                                                    -- key encryption
     keyDerivationOID        OBJECT IDENTIFIER OPTIONAL, -- key derivation
                                                    -- method
     ...,
     genericKeyMaterial      OCTET STRING OPTIONAL -- ASN.1-encoded key material
                         -- form is dependent on associated media encryption tag

}


END  -- End of H235-SECURITY-MESSAGES DEFINITIONS
```

Annexe B

Points spécifiques de la Rec. UIT-T H.324

A étudier.

Appendice I

Détails d'implémentation H.323

I.1 Exemples d'implémentation

Les sous-paragraphes suivants décrivent des exemples d'implémentation qui pourraient être développés dans le cadre de H.235. Ils ne sont pas destinés à prendre le pas sur les nombreuses autres possibilités proposées dans la présente Recommandation. Ces paragraphes visent plutôt à donner des exemples plus concrets d'utilisation dans le cadre de la Rec. UIT-T H.323.

I.1.1 Jetons

Le présent paragraphe décrit un exemple d'utilisation de jetons de sécurité afin d'occulter ou de masquer les informations d'adressage de destination. Dans le scénario donné en exemple, un point d'extrémité souhaite établir une communication avec un autre point d'extrémité utilisant son pseudonyme bien connu. Plus précisément, ce scénario fait intervenir un point d'extrémité H.323, un portier, une passerelle avec le RTC et un poste téléphonique, comme illustré sur la Figure I.1.

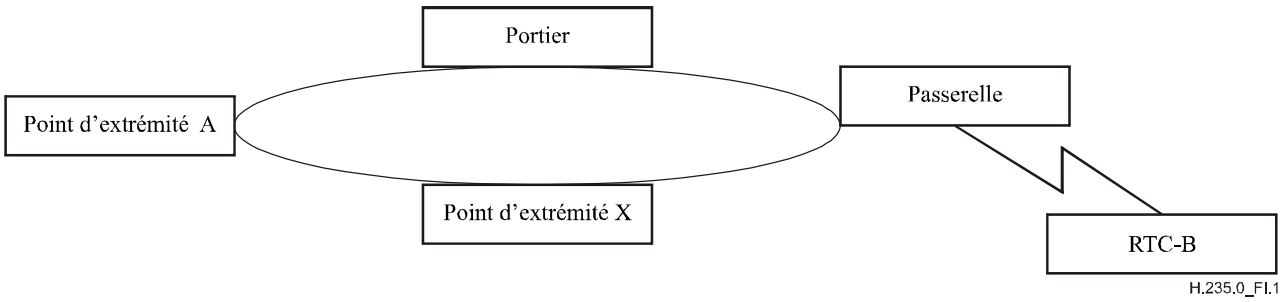


Figure I.1/H.235.0 – Jetons

Actuellement, un réseau H.323 peut fonctionner de façon analogue à un réseau téléphonique avec identification de l'appelant. Ce scénario illustre une situation dans laquelle l'*appelé* ne souhaite pas divulguer son adresse physique tout en acceptant l'établissement de l'appel. Cela peut être important dans les passerelles RTC-H.323, lorsque le numéro téléphonique de destination peut devoir rester privé.

Supposons que le point A essaye d'appeler le point RTC-B et que celui-ci ne souhaite pas divulguer au point A son numéro de téléphone selon le plan E.164. (La façon dont cette politique est établie est hors du domaine d'application de cet exemple.)

- le point A enverra une demande **ARQ** à son portier pour résoudre l'adresse du poste RTC, tel que représenté par son pseudonyme/passerelle. Le portier reconnaîtra cette adresse comme un pseudonyme "privé", sachant que pour réaliser la connexion il doit renvoyer l'adresse de la passerelle avec le RTC. (Ce cas est analogue à celui du renvoi d'adresse d'une passerelle H.320 si un point d'extrémité H.320 est appelé par un point d'extrémité H.323.);
- dans le message **ACF** renvoyé, le portier renvoie l'adresse de la passerelle avec le RTC, comme prévu. Les informations d'adressage qui sont nécessaires pour appeler le poste distant (c'est-à-dire le numéro de téléphone) sont renvoyées dans un jeton chiffré dans le message **ACF**. Ce jeton chiffré contient le numéro E.164 réel (de téléphone) du poste, qui ne peut pas être déchiffré ni compris par l'appelant (c'est-à-dire le point A);

- le point d'extrémité envoie à la passerelle (dont l'adresse de signalisation d'appel a été renvoyée dans le message **ACF**) un message SETUP contenant le ou les jetons opaques qu'il a reçus dans le message **ACF**;
- dès qu'elle reçoit le message SETUP, la passerelle envoie sa demande **ARQ** à son portier, y compris tous jetons reçus dans le message SETUP;
- le portier est en mesure de déchiffrer le ou les jetons et de renvoyer le numéro de téléphone dans le message **ACF**.

Une partie de la notation ASN.1 d'une structure de jeton est montrée ci-dessous à titre d'exemple, avec description du contenu des champs. L'on suppose que l'on utilise le paramètre **cryptoEncodedGeneralToken** pour y insérer le numéro de téléphone chiffré.

Une implémentation peut choisir un identificateur d'objet de jeton, **tokenOID**, pour indiquer que ce jeton contient le numéro de téléphone E.164. La méthode particulière qui sera utilisée pour chiffrer ce numéro de téléphone (par exemple une norme DES à 56 bits) sera incluse dans la définition "ENCRYPT' contenue dans l'identificateur d'algorithme, **algorithmOID**.

```
CryptoToken::= CHOICE
{
     cryptoEncodedGeneralToken SEQUENCE    -- General purpose/application
                                           --  specific token
     {
          tokenOID  OBJECT IDENTIFIER,
          ENCRYPTED { EncodedGeneralToken }
     },
.
.
. [abbreviated text]
.

}
```

Le jeton **CryptoToken** sera transmis dans le message SETUP (du point A à la passerelle) et dans le message **ARQ** (de la passerelle au portier) comme indiqué ci-dessus. Après avoir déchiffré le jeton (numéro de téléphone), le portier en transmet la version en clair dans le jeton **clearToken**.

I.1.2 Utilisation des jetons dans les systèmes H.323

L'utilisation des jetons **CryptoH323Tokens** tels qu'ils sont acheminés dans les messages RAS a donné lieu à une certaine confusion. Il y a deux grandes catégories de jetons **CryptoH323Tokens**: celle des jetons utilisés pour les procédures H.235 et celle des jetons utilisés d'une manière spécifique à l'application. Il convient d'utiliser ces jetons conformément aux règles suivantes:

- tous les jetons définis dans la Rec. UIT-T H.235 (par exemple **cryptoEPPwdHash**, **cryptoGKPwdHash**, **cryptoEPPwdEncr**, **cryptoGKPwdEncr**, **cryptoGKCert**, et **cryptoFastStart**) doivent être utilisés conformément aux procédures et avec les algorithmes définis dans la présente Recommandation);
- les jetons spécifiques aux applications et les jetons propriétaires doivent utiliser pour leurs échanges, le jeton **nestedcryptoToken**;
- tout jeton **nestedcryptoToken** devrait avoir un identificateur **tokenOID** (identificateur d'objet) qui l'identifie sans équivoque.

I.1.3 Utilisation de la valeur aléatoire H.235 dans les systèmes H.323

La valeur aléatoire qui est transmise dans une séquence **xRQ/xCF** entre les points d'extrémité et les portiers peut être actualisée par le portier. Comme indiqué au § 8.3.1, cette valeur aléatoire peut être rafraîchie dans tout message **xCF** en vue de l'utilisation dans des messages **xRQ** subséquents partant du point d'extrémité. Etant donné qu'il y a possibilité de perte des messages RAS (y

compris **xCF/xRJ**), la valeur aléatoire actualisée peut également se perdre. La reprise à partir d'une telle situation peut être la réinitialisation du contexte de sécurité, mais le soin en est laissé à l'implémentation.

Les implémentations qui nécessitent l'utilisation de plusieurs demandes RAS en suspens seront limitées par l'actualisation des valeurs aléatoires utilisées dans toute authentification. Si l'actualisation de cette valeur se produit à chaque réponse à une demande, les demandes parallèles sont impossibles. Une solution éventuelle consiste à disposer d'une "fenêtre" logique au cours de laquelle une valeur aléatoire reste constante. Il s'agit d'une question à résoudre au plan de l'implémentation.

I.1.4 Mot de passe

Dans cet exemple, l'on suppose que l'utilisateur est abonné au service de portier (c'est-à-dire qu'il se trouve dans la zone de celui-ci) et qu'il possède un identificateur d'abonnement et un mot de passe correspondants. Cet utilisateur va s'enregistrer auprès du portier en utilisant son identificateur d'abonnement (tel qu'il a été transmis dans un identificateur de pseudonyme H.323) et en chiffrant une chaîne d'épreuve qui lui sera présentée par le portier. Ce processus suppose que le portier connaît également le mot de passe associé à l'identificateur d'abonnement. Le portier authentifiera l'utilisateur en vérifiant que la chaîne d'épreuve a été correctement chiffrée.

La procédure d'enregistrement avec authentification par portier sera la suivante pour cet exemple:

1) si le point d'extrémité utilise une demande **GRQ** pour découvrir un portier, un des pseudonymes contenus dans le message se trouvera dans l'identificateur d'abonnement (sous forme d'identificateur **H323ID**). Le message **authenticationcapability** contiendra un mécanisme d'authentification (**AuthenticationMechanism**) de type **pwdSymEnc** et les identificateurs d'algorithme (**algorithmOID**) indiqueront l'ensemble complet des algorithmes de chiffrement pris en charge par le point d'extrémité. (Par exemple, l'un de ces algorithmes sera la norme DES à 56 bits en mode ECB);

2) le portier répondra à ce message par une confirmation **GCF** (en supposant qu'il reconnaît le pseudonyme) acheminant un élément **tokens** contenant un seul jeton en clair, **ClearToken**. Celui-ci se composera de deux parties: une épreuve (**challenge**) et une horodate (**timeStamp**). L'épreuve **challenge** sera codée sur 16 octets (pour prévenir les attaques par réexécution, le jeton en clair **ClearToken** contiendra un élément **timeStamp**). Le mode d'authentification **authenticationmode** sera mis à **pwdSymEnc** et l'identificateur d'algorithme **algorithmOID** indiquera l'algorithme de chiffrement requis par le portier (par exemple norme DES à 56 bits en mode ECB).

   Si le portier ne prend en charge aucun des identificateurs d'algorithme **algorithmOID** indiqués dans la demande **GRQ**, il répondra par un rejet **GRJ** contenant une cause **GatekeeperRejectReason** égale à **ressourceUnavailable**;

3) l'application du point d'extrémité tentera alors de s'enregistrer auprès du (d'un des) portier(s) ayant répondu par une confirmation **GCF**, en envoyant une demande **RRQ** contenant un élément **cryptoEPPwdEncr** dans le paramètre **cryptoTokens**. Cet élément **cryptoEPPwdEncr** contiendra l'identificateur de l'algorithme de chiffrement **algorithmOID** convenu lors de l'échange de messages **GRQ/GCF**, ainsi que l'épreuve chiffrée.

   La clé de chiffrement est construite sur la base du mot de passe de l'utilisateur, au moyen de la procédure décrite au § 8.2.1. La "chaîne" d'octets résultante sera alors utilisée comme clé DES pour chiffrer l'épreuve **challenge**;

4) lorsque le portier reçoit l'épreuve dans la demande **RRQ**, il la compare à une épreuve déjà chiffrée à l'identique, afin d'authentifier l'utilisateur requérant. Si les deux chaînes chiffrées ne correspondent pas, le portier répond par un message de rejet **RRJ** avec la cause **RegistrationRejectReason** mise à la valeur **securityDenial** ou un autre code d'erreur de

sécurité (voir § 11.1). Si les chaînes correspondent, le portier envoie une confirmation **RCF** au point d'extrémité;

5) si le portier reçoit une demande **RRQ** qui ne contient pas d'élément **cryptoTokens** acceptable, il doit répondre par un rejet **RRJ** avec la cause **GatekeeperRejectReason** mise à la valeur **discoveryRequired**. Le point d'extrémité, dès qu'il reçoit ce message **RRJ**, peut exécuter la découverte qui permettra au couple portier/point d'extrémité d'échanger une nouvelle épreuve.

NOTE – Le message **GRQ** peut être envoyé en mode point à point au portier.

I.1.5 Sécurité IPsec

En général, les méthodes IPsec ([RFC 2401], RFC 2406 [ESP]) et RFC 2409 [IKE] peuvent être utilisées pour assurer l'authentification et, facultativement, la confidentialité (c'est-à-dire le chiffrement) dans la couche IP de façon transparente à tout protocole (applicatif) exploité dans les couches supérieures. Pour cela, il n'est pas nécessaire de mettre à jour le protocole applicatif, mais uniquement la politique de sécurité à chaque extrémité.

Par exemple, pour tirer le meilleur parti de la sécurité IPsec pour une simple communication point à point, le scénario ci-après peut être suivi:

1) le point d'extrémité appelant et son portier détermineront par le protocole RAS la politique prescrivant l'utilisation de la sécurité IPsec (authentification et, facultativement, confidentialité). Avant l'envoi du premier message RAS du point d'extrémité au portier, le démon ISAKMP (RFC 2407)/Oakley (RFC 2412) situé au point d'extrémité négociera les services de sécurité à utiliser pour les paquets à destination et en provenance du port bien connu du canal RAS. Une fois la négociation achevée, le canal RAS fonctionne exactement comme s'il n'avait pas été sécurisé. Au moyen de ce canal sécurisé, le portier informera le point d'extrémité de l'adresse et du numéro de port du canal de signalisation d'appel se trouvant au point d'extrémité appelé;

2) après avoir obtenu l'adresse et le numéro de port du canal de signalisation d'appel, le point d'extrémité appelant met à jour dynamiquement sa politique de sécurité afin de demander la sécurité IPsec souhaitée à cette adresse pour cette paire protocole/port. Ensuite, lorsque le point d'extrémité appelant tentera de se mettre en contact avec cette paire adresse/port, les paquets seront mis en file d'attente pendant l'exécution d'une négociation ISAKMP (RFC 2407)/Oakley (RFC 2412) entre les points d'extrémité. A l'achèvement de cette négociation, une association de sécurité IPsec existera pour cette paire adresse/port et la signalisation Q.931 pourra commencer;

3) lors de l'échange des messages Q.931 SETUP et CONNECT, les points d'extrémité peuvent négocier l'utilisation de la sécurité IPsec pour le canal H.245. Cela permettra aux points d'extrémité de remettre à jour dynamiquement leurs bases de données de politiques de sécurité IPsec et d'imposer l'utilisation de la sécurité IPsec sur cette connexion;

4) comme dans le canal de signalisation d'appel, une négociation ISAKMP (RFC 2407)/Oakley (RFC 2412) transparente se déroulera avant qu'un quelconque paquet H.245 soit émis. L'authentification effectuée par cet échange ISAKMP (RFC 2407)/Oakley (RFC 2412) sera la tentative initiale d'une authentification d'utilisateur à utilisateur. Elle établira un canal (probablement) sécurisé entre les deux utilisateurs, permettant de négocier les caractéristiques du canal audio. Si, à la suite d'un dialogue interpersonnel, l'un des utilisateurs n'est pas satisfait de l'authentification, des certificats différents peuvent être choisis et l'échange ISAKMP (RFC 2407)/Oakley (RFC 2412) peut être répété;

5) après chaque authentification ISAKMP (RFC 2407)/Oakley (RFC 2412) H.245, de nouvelles données de clé sont échangées pour le canal audio RTP. Ces données sont distribuées par le maître sur le canal H.245 sécurisé. Comme le protocole H.245 est défini de façon que le maître distribue les données de clés multimédias sur le canal H.245 (afin de

permettre des communications multipoints), il n'est pas recommandé d'utiliser la méthode IPsec pour le canal RTP.

Un canal H.245 chiffré peut poser un problème pour les pare-feu proxy ou NAT car les numéros de port attribués dynamiquement sont acheminés dans le protocole H.245. Pour fonctionner correctement, de tels pare-feu devront déchiffrer, modifier et rechiffrer le protocole. C'est pourquoi le canal logique "de sécurité" a été introduit dans la Rec. UIT-T H.245. Si ce canal est utilisé, le canal H.245 peut rester non sécurisé; l'authentification et la production de clés seront effectuées avec le canal logique "de sécurité". La signalisation par canal logique permettra de protéger ce canal par la méthode IPsec et la clé secrète utilisée dans le canal logique "de sécurité" servira à protéger la synchronisation **EncryptionSync** distribuée par le maître sur le canal H.245.

I.1.6 Prise en charge des services d'arrière

Les serveurs d'arrière (BES, *back-end server*) représentent une fonction supplémentaire importante dans l'ensemble de l'environnement multimédia de type H.323. Ils fournissent, par exemple, des services pour l'authentification de l'utilisateur, pour l'autorisation de service ainsi que pour la comptabilité, la taxation et la facturation et d'autres services. Dans un modèle simple, le portier peut fournir de tels services, mais dans une architecture décomposée, il ne peut pas toujours le faire, soit parce qu'il n'a pas nécessairement accès aux bases de données BES, soit parce qu'il fait partie d'un domaine administratif différent. Par ailleurs, le terminal et l'utilisateur ne connaissent généralement pas leur serveur BES.

La Figure I.2 représente un scénario comportant un terminal multimédia (par exemple un dispositif SASET) et un portier relié à un serveur BES. La manière exacte dont le serveur BES communique avec le portier ne relève pas de la Rec. UIT-T H.323. Plusieurs méthodes et protocoles peuvent être utilisés: la technologie RADIUS (voir RFC 2865), considérée comme l'une des plus importantes, est couramment utilisée par de nombreux fournisseurs de services.

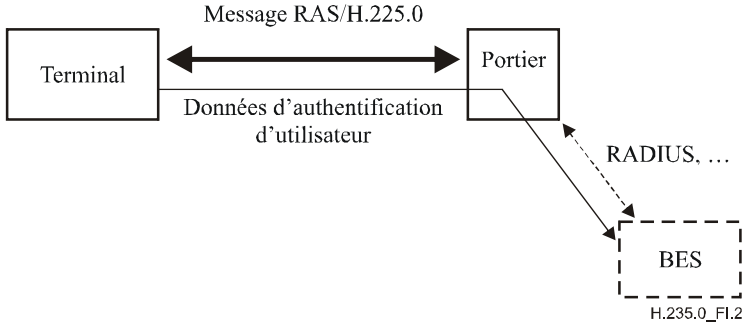


Figure I.2/H.235.0 – Scénario avec serveur d'arrière

Un portier qui prend en charge des services BES devrait proposer au moins les deux modes suivants:

1) **Le mode par défaut** (**default mode**): mode dans lequel le terminal ne connaît pas le serveur BES et dans lequel il faut une relation de confiance avec le portier. Le terminal envoie les données d'authentification de l'utilisateur sous forme chiffrée (**cryptoEncryptedToken**) au portier; celui-ci les décrypte, en extrait les informations d'authentification d'utilisateur et les envoie au serveur BES. Le chiffrement à mot de passe du jeton **ClearToken** est effectué en appliquant au jeton **CryptoToken** un secret distinct qui est connu du terminal et du portier. La clé de chiffrement pourrait être obtenue à partir du mot de passe au moyen duquel le terminal s'enregistre de manière sécurisée auprès du portier.

Le jeton **CryptoToken** achemine **cryptoEncryptedToken** dans lequel l'identificateur **tokenOID** est mis à "M" pour indiquer le mode BES par défaut; **token** contient:

- **algorithmOID** indiquant l'algorithme de chiffrement; "Y" (DES56-CBC), "Z" (3DES-OCBC); voir § 11/H.235.6;
- **paramS** est inutilisé;
- **encryptedData** est mis à la représentation en octets du jeton **ClearToken** chiffré.

Le jeton **ClearToken** contient en tant que mot de passe **password** les données d'authentification de l'utilisateur. Les informations protégées du jeton **ClearToken** pourraient être le mot de passe ou un code PIN, une identification de l'utilisateur, un numéro de carte d'appel à prépaiement ou un numéro de carte de crédit. Le **timestamp** est mis à l'heure du terminal, **random** contient un numéro de séquence croissant monotone, **sendersID** est mis à l'identificateur du terminal et **generalID** à l'identificateur du portier. La valeur initiale de l'algorithme de chiffrement doit être maintenue constante; elle ne peut pas faire partie du secret attribué au moment de l'abonnement du terminal.

NOTE – Le jeton **ClearToken** n'est pas transmis.

2) **Le mode RADIUS** (**RADIUS mode**): mode dans lequel le serveur BES et l'utilisateur du terminal ont un secret commun et dans lequel le portier ne devrait pas être "de confiance" pour l'authentification du mode en question. Le portier transmet simplement au terminal une épreuve RADIUS reçue du serveur BES dans un message *Access-Challenge* et envoie la réponse de l'utilisateur sous forme de réponse RADIUS dans un message *Access-Request* en sens inverse. Le terminal et le portier négocient cette capacité d'épreuve/réponse de **radius** dans **AuthenticationBES** de **AuthenticationMechanism** pendant la découverte du portier.

   Lorsqu'il reçoit un message RADIUS *Access-Challenge* contenant une épreuve, le portier introduit l'épreuve à 16 octets dans le champ **challenge** de **ClearToken** lorsqu'il interroge le terminal avec un message **GCF** ou tout autre message RAS. L'identificateur **tokenOID** "K" de **ClearToken** indique une épreuve RADIUS.

   Le terminal peut ensuite présenter l'épreuve à l'utilisateur et attendre la réponse entrée. Le terminal doit répondre au moyen d'un messager RAS dans lequel la réponse figure dans le champ **challenge** de **ClearToken**. L'identificateur **tokenOID** "L" de **ClearToken** indique une réponse RADIUS.

Le Tableau I.1 contient tous les identificateurs OID mentionnés.

Tableau I.1/H.235.0 – Identificateurs d'objet utilisés au § I.1.6

Désignation d'identificateur d'objet	Valeur d'identificateur d'objet	Description
"K"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 31}	Indique une épreuve RADIUS dans clearToken
"L"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 32}	Indique une réponse RADIUS (acheminée dans le champ challenge) dans ClearToken
"M"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 33}	Indique le mode BES par défaut avec mot de passe protégé dans ClearToken

Appendice II

Détails d'implémentation H.324

A étudier.

Appendice III

Autres détails d'implémentation pour la série H

A étudier.

Appendice IV

Mappage entre les paragraphes de H.235v3Amd1Cor1 et ceux des Recommandations de la sous-série H.235v4

Le présent appendice donné à titre d'information indique l'emplacement de tous les paragraphes de H.235v3Amd1Cor1 dans les Recommandations de la sous-série H.235v4.

Tableau IV.1/H.235.0 – Mappage entre les paragraphes

Paragraphe H.235v3 Amd1Cor1	Titre	Recommandation de la sous-série H.235v4.x	Paragraphe
Corps principal	–	–	–
1	Domaine d'application	H.235.0	1
2	Références normatives	H.235.0	2
		H.235.1	2
		H.235.2	2
		H.235.3	2
3	Termes et définitions	H.235.0	3
		H.235.2	3
		H.235.6	3
4	Symboles et abréviations	H.235.0	4
		H.235.3	4
		H.235.6	4
5	Conventions	H.235.0	5
		H.235.2	5
		H.235.6	5

Tableau IV.1/H.235.0 – Mappage entre les paragraphes

Paragraphe H.235v3 Amd1Cor1	Titre	Recommandation de la sous-série H.235v4.x	Paragraphe
6	Introduction au système	H.235.0	6
6.1	Résumé	H.235.0	6.1
6.2	Authentification	H.235.0	6.2
6.2.1	Certificats	H.235.0	6.2.1
6.3	Sécurité lors de l'établissement d'appel	H.235.0	6.3
6.4	Sécurité de la commande d'appel (H.245)	H.235.0	6.4
6.5	Secret des communications par flux de média	H.235.0	6.5
6.6	Eléments crédibilisés	H.235.0	6.6
6.6.1	Dépôt de clé	H.235.0	6.6.1
6.7	Non-répudiation	H.235.0	6.7
6.8	Sécurité dans un environnement de mobilité	H.235.0	6.8
6.9	Profils de sécurité	H.235.0	6.9
7	Procédures d'établissement de connexion	H.235.0	7
7.1	Introduction	H.235.0	–
8	Signalisation et procédures H.245	H.235.6	7
8.1	Fonctionnement avec canal H.245 sécurisé	H.235.6	7.1
8.2	Fonctionnement avec canal H.245 non sécurisé	H.235.6	7.2
8.3	Echange de capacités	H.235.6	7.3
8.4	Rôle de maître	H.235.6	7.4
8.5	Signalisation par canal logique	H.235.6	7.5
8.6	Sécurité avec connexion rapide (*fast connect security*)	H.235.6	7.6
8.6.1	Sécurité unidirectionnelle avec démarrage rapide	H.235.6	7.6.1
8.6.1.1	Utilisation d'algorithmes de chiffrement multiples dans la procédure fast connect	H.235.6	7.6.1.1
8.6.2	Sécurité de connexion rapide bidirectionnelle	H.235.6	7.6.2
8.7	Signaux DTMF H.245 chiffrés	H.235.6	7.7
8.7.1	Chaîne de base chiffrée	H.235.6	7.7.1
8.7.2	Chaîne iA5 chiffrée	H.235.6	7.7.2
8.7.3	Chaîne générale chiffrée	H.235.6	7.7.3
8.7.4	Liste des identificateurs d'objet	H.235.6	7.7.4

Tableau IV.1/H.235.0 – Mappage entre les paragraphes

Paragraphe H.235v3 Amd1Cor1	Titre	Recommandation de la sous-série H.235v4.x	Paragraphe
8.8	Fonctionnement en mode Diffie-Hellman	H.235.6	7.8
9	Procédures multipoint	H.235.6	8.8
9.1	Authentification	H.235.6	8.8.1
9.2	Secret des communications	H.235.6	8.8.2
10	Signalisation et procédures d'authentification	H.235.0	8
10.1	Introduction	H.235.0	---
10.2	Méthode de Diffie-Hellman avec authentification facultative	H.235.0	8.1
10.3	Authentification sur abonnement	H.235.0	8.2
10.3.1	Introduction	H.235.0	–
10.3.2	Authentification par mot de passe avec chiffrement symétrique	H.235.0	8.2.1
10.3.3	Authentification par mot de passe avec hachage	H.235.0	8.2.2
10.3.4	Authentification par certificat avec signatures	H.235.0	8.2.3
10.3.5	Utilisation du secret partagé et des mots de passe	H.235.0	8.2.4
11	Procédures de chiffrement de flux de média	H.235.6	9
11.1	Clés de session média	H.235.6	9.1
11.2	Protection du média contre la submersion	H.235.6	9.2
11.2.1	Liste des identificateurs d'objet	H.235.6	9.2.1
12	Reprise sur erreur de sécurité	H.235.0	11
13	Authentification asymétrique et échange de clés au moyen de systèmes de chiffrement à courbe elliptique	H.235.0	9
13.1	Gestion de clés	H.235.0	9.1
13.2	Signature numérique	H.235.0	9.2
Appendice I	Détails d'implémentation H.323	H.235.0	Appendice I
I.1	Méthodes de bourrage cryptographique	H.235.6	I.1
I.2	Nouvelles clés	H.235.6	8.7.2
I.3	Eléments crédibilisés H.323	H.235.6	8.7.3
I.4	Exemples d'implémentation	H.235.0	I.1
I.4.1	Jetons	H.235.0	I.1.1
I.4.2	Utilisation des jetons dans les systèmes H.323	H.235.0	I.1.2

Tableau IV.1/H.235.0 – Mappage entre les paragraphes

Paragraphe H.235v3 Amd1Cor1	Titre	Recommandation de la sous-série H.235v4.x	Paragraphe
I.4.3	Utilisation de la valeur aléatoire H.235 dans les systèmes H.323	H.235.0	I.1.3
I.4.4	Mot de passe	H.235.0	I.1.4
I.4.5	Sécurité IPsec	H.235.0	I.1.5
I.4.6	Prise en charge des services de réalisation spécialisés	H.235.0	I.1.6
Appendice II	Détails d'implémentation H.324	H.235.0	Appendice II
Appendice III	Autres détails d'implémentation pour la série H	H.235.0	Appendice III
Appendice IV	Bibliographie	H.235.0	2.2
Annexe A	**ASN.1 H.235**	**H.235.0**	**Annexe A**
Annexe B	**Points spécifiques de la Rec. UIT-T H.323**	**H.235.6**	**–**
B.1	Rappel	H.235.0	6
B.2	Signalisation et procédures	H.235.6	8
B.2.1	Compatibilité avec la Révision 1	H.235.6	8.1
B.2.2	Signalisation des erreurs	H.235.0	11.1
B.2.3	Indications de fonctionnalité de la version 3	H.235.6	8.2
B.2.4	Acheminement de la clé	H.235.6	8.3
B.2.4.1	Acheminement de clé amélioré dans la version 3 de la Rec. UIT-T H.235	H.235.6	8.3.1
B.2.5	Mode OFB amélioré	H.235.6	8.4
B.2.6	Mise à jour des clés et synchronisation	H.235.6	8.6
B.2.6.1	Mise à jour de clés sans accusé de réception	H.235.6	8.6.1
B.2.6.2	Actualisation améliorée des clés	H.235.6	8.6.2
B.2.6.3	Actualisation et synchronisation de la clé sur la base du type de charge utile	H.235.6	8.6.3
B.3	Liaisons avec les protocoles RTP/RTCP	H.235.6	9.3
B.3.1	Vecteurs d'initialisation	H.235.6	9.3.1
B.3.1.1	Vecteurs d'initialisation CBC	H.235.6	9.3.1.1
B.3.1.2	Vecteurs d'initialisation EOFB	H.235.6	9.3.1.2
B.3.2	Bourrage	H.235.6	9.3.2
B.3.3	Protection RTCP	H.235.6	9.3.3
B.3.4	Flux de charge utile sécurisée	H.235.6	9.3.4
B.3.5	Interfonctionnement avec la Rec. UIT-T J.170	H.235.6	9.3.5

Tableau IV.1/H.235.0 – Mappage entre les paragraphes

Paragraphe H.235v3 Amd1Cor1	Titre	Recommandation de la sous-série H.235v4.x	Paragraphe
B.4	Procédures et signalisation des messages d'enregistrement, admission et état (RAS) pour l'authentification	H.235.0	8.3
B.4.1	Introduction	H.235.0	–
B.4.2	Authentification entre point d'extrémité et portier (non fondée sur abonnement)	H.235.0	8.3.1
B.4.3	Authentification entre point d'extrémité et portier (fondée sur abonnement)	H.235.0	8.3.2
B.4.3.1	Mot de passe avec chiffrement symétrique	H.235.0	8.3.2.1
B.4.3.2	Mot de passe avec hachage	H.235.0	8.3.2.2
B.4.3.3	Authentification par certificat avec signatures	H.235.0	8.3.3.3
B.5	Interactions non terminales	H.235.6	8.7
B.5.1	Passerelle	H.235.6	8.7.1
B.6	Gestion de clé sur le canal RAS	H.235.0	8.4
B.7	Fonction pseudo aléatoire (PRF)	H.235.0	10
Annexe C	**Points spécifiques de la Rec. UIT-T H.324**	**H.235.0**	**Annexe B**
Annexe D	**Profil de sécurité élémentaire**	**H.235.1**	
D.1	Introduction	H.235.1	
D.2	Conventions	H.235.1	5
D.3	Domaine d'application	H.235.1	1
D.4	Abréviations	H.235.1	4
D.5	Références normatives	H.235.1	2.1
D.6	Profil de sécurité élémentaire	H.235.1	
D.6.1	Aperçu général	H.235.1	6.1
D.6.1.1	Profil de sécurité élémentaire	H.235.1	6.2
D.6.1.2	Profil de sécurité de chiffrement vocal	H.235.6	6.1
D.6.2	Authentification et intégrité	H.235.1	3.1
D.6.3	Prescriptions H.323	H.235.1	6.3
D.6.3.1	Aperçu général	H.235.1	6.4
D.6.3.2	Détails de l'authentification des messages de signalisation de type à clés symétriques (procédure I)	H.235.1	7
D.6.3.3	Calcul du hachage à mot de passe	H.235.1	7.1
D.6.3.3.1	Code HMAC-SHA1-96	H.235.1	7.2
D.6.3.3.2	Authentification et intégrité	H.235.1	7.3

Tableau IV.1/H.235.0 – Mappage entre les paragraphes

Paragraphe H.235v3 Amd1Cor1	Titre	Recommandation de la sous-série H.235v4.x	Paragraphe
D.6.3.3.3	Authentification seulement (procédure IA)	H.235.1	8
D.6.3.4	Présentation de l'emploi de la procédure I	H.235.1	9
D.6.3.4.1	Authentification et intégrité des messages RAS	H.235.1	9.1
D.6.3.4.2	Authentification et intégrité du message H.225.0	H.235.1	9.2
D.6.3.4.3	Authentification et intégrité de message H.245	H.235.1	9.3
D.6.4	Scénario de routage direct	H.235.1	9.4
D.6.5	Prise en charge du service de réalisation d'extrémité	H.235.1	10
D.6.6	Compatibilité avec le contexte H.235 Version 1	H.235.1	11
D.6.7	Comportement en multidiffusion	H.235.1	12
D.7	Profil de sécurité de chiffrement vocal	H.235.6	6.1
D.7.1	Gestion de clés	H.235.6	8.5
D.7.2	Mise à jour et synchronisation des clés	H.235.6	8.6
D.7.3	Normes 3-DESs en mode CBC extérieur	H.235.6	9.4
D.7.4	Algorithme DES fonctionnant en mode EOFB	H.235.6	9.5
D.7.5	Chiffrement 3-DES fonctionnant en mode EOFB externe	H.235.6	9.6
D.8	Interception licite	H.235.6	10
D.9	Liste des messages de signalisation sécurisés	H.235.1	13
D.9.1	Message RAS H.225.0	H.235.1	13.1
D.9.2	Signalisation d'appel H.225.0	H.235.1	13.2
D.9.3	Commande d'appel H.245	H.235.1	13.3
D.10	Utilisation des identificateurs sendersID et generalID	H.235.1	14
D.11	Liste d'identificateurs d'objet	H.235.1 H.235.6	15 11
D.12	Bibliographie	H.235.1 H.235.6	2.2 2.2
Annexe E	**Profil de sécurité de signature**	**H.235.2**	
E.1	Aperçu général	H.235.2	6

Tableau IV.1/H.235.0 – Mappage entre les paragraphes

Paragraphe H.235v3 Amd1Cor1	Titre	Recommandation de la sous-série H.235v4.x	Paragraphe
E.2	Conventions de spécification	H.235.2	5
E.3	Prescriptions H.323	H.235.2	6.1
E.4	Services de sécurité	H.235.2	5
E.5	Signatures numériques avec détails des paires de clés publiques/privées (procédure II)	H.235.2	7
E.6	Procédures de conférence multipoint	H.235.2	8
E.7	Authentification de bout en bout (procédure III)	H.235.2	9
E.8	Authentification seulement	H.235.2	10
E.9	Authentification et intégrité	H.235.2	11
E.10	Calcul de la signature numérique	H.235.2	12
E.11	Vérification de la signature numérique	H.235.2	13
E.12	Traitement des certificats	H.235.2	14
E.13	Exemple d'utilisation de la procédure II	H.235.2	15
E.13.1	Authentification, intégrité et non-répudiation des messages RAS	H.235.2	15.1
E.13.2	Authentification RAS seule	H.235.2	15.2
E.13.3	Authentification, intégrité et non-répudiation de message H.225.0	H.235.2	15.3
E.13.4	Authentification et intégrité de message H.245	H.235.2	15.4
E.14	Compatibilité avec le contexte H.235 version 1	H.235.2	16
E.15	Comportement en multidiffusion	H.235.2	17
E.16	Liste des messages de signalisation sécurisés	H.235.2	18
E.16.1	Message RAS H.225.0	H.235.2	18.1
E.16.2	Signalisation d'appel H.225.0	H.235.2	18.2
E.17	Utilisation des identificateurs sendersID et generalID	H.235.2	19
E.18	Liste des identificateurs d'objet	H.235.2	20
Appendice IV (Annexe E)	Bibliographie	H.235.2	2.2
Annexe F	**Profil hybride de sécurité**	**H.235.3**	
F.1	Aperçu général	H.235.3	6
F.2	Références normatives	H.235.3	2.1
F.3	Acronymes	H.235.3	4
F.4	Conventions de spécification	H.235.3	5

Tableau IV.1/H.235.0 – Mappage entre les paragraphes

Paragraphe H.235v3 Amd1Cor1	Titre	Recommandation de la sous-série H.235v4.x	Paragraphe
F.5	Prescriptions H.323	H.235.3	6.1
F.6	Authentification et intégrité	H.235.3	6.2
F.7	Procédure IV	H.235.3	7
F.8	Association de sécurité pour appels simultanés	H.235.3	8
F.9	Mise à jour de la clé	H.235.3	9
F.10	Exemples avec organigrammes	H.235.3	11
F.11	Messages multidiffusion	H.235.3	12
F.12	Liste des messages de signalisation de sécurité	H.235.3	13
F.12.1	RAS H.225.0	H.235.3	13.1
F.12.2	Signalisation d'appel H.225.0 (domaine administratif unique)	H.235.3	13.2
F.12.3	Signalisation d'appel H.225.0 (plusieurs domaines administratifs)	H.235.3	13.3
F.13	Liste d'identificateurs d'objet	H.235.3	14
Appendice IV	Bibliographie	H.235.3	2.2
Annexe G	**Utilisation du protocole de gestion de clés MIKEY en association avec le protocole de transport en temps réel sécurisé (SRTP) dans le cadre de la Rec. UIT-T H.235**	**H.235.7**	
G.1	Domaine d'application	H.235.7	1
G.2	Références	H.235.7	2
G.2.1	Références normatives	H.235.7	2.1
G.2.2	Références informatives	H.235.7	2.2
G.3	Termes et définitions	H.235.7	3
G.4	Symboles et abréviations	H.235.7	4
G.5	Conventions de spécification	H.235.7	5
G.6	Introduction	H.235.7	6
G.7	Aperçu général et scénarios	H.235.7	7
G.7.1	Exécution des protocoles MIKEY au "niveau session"	H.235.7	7.1
G.7.2	Exécution des protocoles MIKEY au "niveau média"	H.235.7	7.2
G.7.3	Négociation des capacités MIKEY	H.235.7	7.3
G.8	Profil de sécurité utilisant des techniques de sécurité symétriques	H.235.7	8
G.8.1	Terminaison d'un appel H.323	H.235.7	8.1

Tableau IV.1/H.235.0 – Mappage entre les paragraphes

Paragraphe H.235v3 Amd1Cor1	Titre	Recommandation de la sous-série H.235v4.x	Paragraphe
G.8.2	Recalcul de clé TGK et mise à jour de lot CSB	H.235.7	8.2
G.8.3	Prise en charge de la tunnellisation H.245	H.235.7	8.3
G.8.4	Algorithmes SRTP	H.235.7	8.4
G.8.5	Liste des identificateurs d'objet	H.235.7	8.5
G.9	Profil de sécurité utilisant des techniques de sécurité asymétriques	H.235.7	9
G.9.1	Terminaison d'un appel H.323	H.235.7	9.1
G.9.2	Recalcul de clé TGK et mise à jour de lot CSB	H.235.7	9.2
G.9.3	Prise en charge de la tunnellisation H.245	H.235.7	9.3
G.9.4	Algorithmes SRTP	H.235.7	9.4
G.9.5	Liste des identificateurs d'objet	H.235.7	9.5
G.I	Option MIKEY-DHHMAC	H.235.7	Appendice I
G.I.1	Terminaison d'un appel H.323	H.235.7	I.1
G.I.2	Recalcul de clé TGK et mise à jour de lot CSB	H.235.7	I.2
G.II	Utilisation de l'Annexe I/H.235.0 pour l'établissement d'un secret prépartagé	H.235.7	Appendice II
G.II.1	Terminaison d'un appel H.323	H.235.7	II.1
G.II.2	Recalcul de clé TGK et mise à jour de lot CSB	H.235.7	II.2
Annexe H	**Gestion de clés RAS**	**H.235.5**	
H.1	Introduction	H.235.5	–
H.2	Domaine d'application	H.235.5	1
H.3	Références	H.235.5	2
H.3.1	Références normatives	H.235.5	2.1
H.3.2	Références informatives	H.235.5	2.2
H.4	Définitions	H.235.5	3
H.5	Abréviations	H.235.5	4
H.6	Cadre de base	H.235.5	6
H.6.1	Capacités de négociation améliorées H.235v3	H.235.5	6.1
H.6.2	Utilisation entre le point d'extrémité et le portier	H.235.5	6.2
H.6.3	Utilisation de profils entre portiers	H.235.5	6.3

Tableau IV.1/H.235.0 – Mappage entre les paragraphes

Paragraphe H.235v3 Amd1Cor1	Titre	Recommandation de la sous-série H.235v4.x	Paragraphe
H.6.4	Chiffrement et authentification des canaux de signalisation	H.235.5	6.4
H.7	Profil de sécurité spécifique (SP1)	H.235.5	7
H.8	Extensions du cadre (à titre indicatif)	H.235.5	9
H.8.1	Utilisation de la clé maîtresse pour protéger le canal de signalisation d'appel via le protocole TLS	H.235.5	9.1
H.8.1.1	Enregistrement du point d'extrémité	H.235.5	9.1.1
H.8.2	Utilisation de certificats pour l'authentification du portier	H.235.5	9.2
H.8.3	Utilisation de mécanismes de sécurité de signalisation de remplacement	H.235.5	9.3
H.9	Menaces (à titre indicatif)	H.235.5	10
H.9.1	Attaques passives	H.235.5	10.1
H.9.2	Attaques visant la fonction de refus de service	H.235.5	10.2
H.9.3	Attaques par intercepteur	H.235.5	10.3
H.9.4	Prévoir les attaques	H.235.5	10.4
H.9.5	Demi-clé non chiffrée par le portier	H.235.5	10.5
Annexe I	**Prise en charge des appels à acheminement direct**	**H.235.4**	
I.1	Domaine d'application	H.235.4	1
I.2	Introduction	H.235.4	6
I.3	Conventions de spécification	H.235.4	5
I.4	Termes et définitions	H.235.4	3
I.5	Symboles et abréviations	H.235.4	4
I.6	Références normatives	H.235.4	2
I.7	Aperçu général	H.235.4	7
I.8	Limitations	H.235.4	8
I.9	Procédure DRC	H.235.4	9
I.10	Procédure d'obtention de la clé au moyen de la fonction PRF	H.235.4	12
I.11	Procédure de calcul de la clé en utilisant la Norme FIPS-140	H.235.4	13
I.12	Liste des identificateurs d'objet	H.235.4	14
Appendice I (Annexe I)	Bibliographie	H.235.4	2.2

Appendice V

Mappage entre les Figures de H.235v3Amd1Cor1 et celles des Recommandations de la sous-série H.235v4

Le présent appendice donné à titre d'information indique l'emplacement de toutes les figures de H.235v3Amd1Cor1 dans les Recommandations de la sous-série H.235v4.

Tableau V.1/H.235.0 – Mappage entre les Figures

Figure H.235v3 Amd1Cor1	Titre	Recommandation de la sous-série H.235v4.x	Figure
Figure 1	Echange Diffie-Hellman avec authentification facultative	H.235.0	4
Figure 2a	Authentification par mot de passe avec chiffrement symétrique; deux passages	H.235.0	5
Figure 2b	Authentification par mot de passe avec chiffrement symétrique; trois passages	H.235.0	6
Figure 3a	Authentification par mot de passe avec hachage; deux passages	H.235.0	7
Figure 3b	Mot de passe avec hachage; trois passages	H.230.0	8
Figure 4a	Authentification par certificat avec signature; deux passages	H.235.0	9
Figure 4b	Authentification par certificat avec signature; trois passages	H.235.0	10
Figure 5	Chiffrement du média	H.235.6	7
Figure 6	Déchiffrement du média	H.235.6	8
Figure 7	Format de paquets RTP pour la protection contre la submersion du média	H.235.6	9
Figure I.1	Emprunt d'un texte chiffré en mode ECB	H.235.6	I.1
Figure I.2	Emprunt d'un texte chiffré en mode CBC	H.235.6	I.2
Figure I.2a	Bourrage de zéros en mode CBC	H.235.6	I.3
Figure I.3	Bourrage de zéros en mode CFB	H.235.6	I.4
Figure I.4	Bourrage de zéros en mode OFB	H.235.6	I.5
Figure I.4.1	Mode EOFB avec bourrage de zéros	H.235.6	I.6
Figure I.5	Bourrage tel que prescrit par le protocole RTP	H.235.6	I.7
Figure I.6	Jetons	H.235.0	I.1
Figure I.7	Scénario avec serveur spécialisé	H.235.0	I.2
Figure B.1	Aperçu général	H.235.0	2

Tableau V.1/H.235.0 – Mappage entre les Figures

Figure H.235v3 Amd1Cor1	Titre	Recommandation de la sous-série H.235v4.x	Figure
Figure B.1.1	Distribution/mise à jour de clés de session du maître vers le ou les esclaves sans accusé de réception	H.235.6	4
Figure B.1.2	Mise à jour de la clé de session sur le canal logique de l'esclave	H.235.6	5
Figure B.1.3	Actualisation de la clé de session sur le canal logique du maître	H.235.6	6
Figure B.2	Mot de passe avec chiffrement symétrique	H.235.0	11
Figure B.3	Mot de passe avec hachage	H.235.0	12
Figure B.4	Authentification par certificat avec signatures	H.235.0	13
Figure D.1	Présentation de l'emploi de la procédure I dans un scénario portier à portier, les deux points d'extrémité se trouvant dans les zones de routage des portiers	H.235.1	1
Figure D.2	Emploi de la procédure I dans un scénario mixte avec le point d'extrémité 1 dans une zone à routage par portier et le point d'extrémité 2 dans une zone à routage direct	H.235.1	2
Figure D.3	Emploi de la procédure I pour un scénario dans lequel les deux points d'extrémité sont situés dans des zones utilisant un portier à routage direct	H.235.1	3
Figure D.4	Chiffrement 3-DES en mode CBC extérieur	H.235.6	10
Figure D.5	Chiffrement 3-DES en mode EOFB externe	H.235.6	11
Figure E.1	Utilisation simultanée de la sécurité bond par bond et de l'authentification de bout en bout	H.235.2	1
Figure E.2	Exemple de l'utilisation de clés publiques dans un modèle routé de portier à portier	H.235.2	2
Figure F.1	Association de sécurité pour appels simultanés	H.235.3	1
Figure F.2	Flux de messages dans un domaine administratif unique	H.235.3	2
Figure F.3	Flux de messages dans un domaine à plusieurs administrations	H.235.3	3

Tableau V.1/H.235.0 – Mappage entre les Figures

Figure H.235v3 Amd1Cor1	Titre	Recommandation de la sous-série H.235v4.x	Figure
Figure G.1	Scénario	H.235.7	1
Figure G.2	Scénario de sécurité avec MIKEY et SRTP	H.235.7	2
Figure G.3	Scénario saut par saut uniquement avec des secrets partagés	H.235.7	3
Figure G.4	Exemple dans lequel le point d'extrémité B appelle le point d'extrémité A (routage par portier) avec MIKEY-PS	H.235.7	4
Figure G.5	Traitement MIKEY-PS par le point d'extrémité B	H.235.7	5
Figure G.6	Traitement MIKEY-PS par le point d'extrémité A	H.235.7	6
Figure G.7	Exemple dans lequel le point d'extrémité B termine un appel	H.235.7	7
Figure G.8	Exemple dans lequel le point d'extrémité B met à jour une clé	H.237.7	8
Figure G.9	Scénario de bout en bout avec infrastructure PKI (plusieurs portiers)	H.235.7	9
Figure G.10	Exemple dans lequel le point d'extrémité B appelle le point d'extrémité A (routage par plusieurs portiers) avec MIKEY-PK-SIGN	H.235.7	10
Figure G.11	Traitement MIKEY-PK-SIGN par le point d'extrémité B	H.235.7	11
Figure G.12	Traitement MIKEY-PK-SIGN par le point d'extrémité A	H.235.7	12
Figure G.13	Exemple dans lequel le point d'extrémité B termine un appel	H.235.7	13
Figure G.14	Exemple dans lequel le point d'extrémité B (initiateur) lance un recalcul de clé TGK et une mise à jour de lot CSB	H.235.7	14
Figure G.I-1	Exemple dans lequel le point d'extrémité B appelle le point d'extrémité A (routage par portiers) avec MIKEY-DHHMAC	H.235.7	I.1
Figure G.I-2	Exemple dans lequel le point d'extrémité B termine un appel	H.235.7	I.2
Figure G.I-3	Exemple dans lequel le point d'extrémité B met à jour une clé	H.235.7	I.3

Tableau V.1/H.235.0 – Mappage entre les Figures

Figure H.235v3 Amd1Cor1	Titre	Recommandation de la sous-série H.235v4.x	Figure
Figure G.II-1	Exemple dans lequel le point d'extrémité B appelle le point d'extrémité A (routage sans portier) avec MIKEY-PS et la procédure DRC1/H.235.0	H.235.7	II.1
Figure H.1	Flux d'informations pour le profil de sécurité et le protocole TLS	H.235.5	1
Figure I.1	Scénario d'un appel à acheminement direct	H.235.4	1
Figure I.2	Flux de communications de base	H.235.4	2

Appendice VI

Mappage entre les Tableaux de H.235v3Amd1Cor1 et ceux des Recommandations de la sous-série H.235v4

Le présent appendice donné à titre d'information indique l'emplacement de tous les Tableaux de H.235v3Amd1Cor1 dans les Recommandations de la sous-série H.235v4.

Tableau VI.1/H.235.0 – Mappage entre les Tableaux

Tableau H.235v3 Amd1Cor1	Titre	Recommandation de la sous-série H.235v4.x	Tableau
Tableau 1	Identificateur d'objet pour le chiffrement NULL	H.235.6	2
Tableau 2	Identificateurs d'objet pour le chiffrement de signaux DTMF H.245	H.235.6	3
Tableau 3	Identificateurs d'objet utilisés pour la protection contre la submersion	H.235.6	5
Tableau I.1	Identificateurs d'objet utilisés au § I.4.6	H.235.0	I.1
Tableau D.1	Résumé des profils de sécurité de l'Annexe D	----	---
Tableau D.2	Profil de sécurité élémentaire	H.235.1	1
Tableau D.3	Profil de chiffrement vocal	H.235.6	1
Tableau D.4	Groupes de Diffie-Hellman	H.235.6	4
Tableau D.5	Utilisation des identificateurs sendersID et generalID	H.235.1	2

Tableau VI.1/H.235.0 – Mappage entre les Tableaux

Tableau H.235v3 Amd1Cor1	Titre	Recommandation de la sous-série H.235v4.x	Tableau
Tableau D.6	Identificateurs d'objet utilisés dans l'Annexe D	H.235.1 H.235.6	3 6
Tableau E.1	Profil de sécurité de signature	H.235.2	1
Tableau E.2	Utilisation des identificateurs sendersID et GeneralID	H.235.2	2
Tableau E.3	Identificateurs d'objet utilisés dans l'Annexe E	H.235.2	3
Tableau F.1	Aperçu général du profil de sécurité hybride	H.235.3	1
Tableau F.2	Identificateurs d'objet utilisés par l'Annexe F	H.235.3	2
Tableau G.1	Protocoles de gestion de clés MIKEY	H.235.7	1
Tableau H.1	Eléments de profil	H.235.5	1
Tableau I.0	Calcul des clés de chiffrement et de salage à partir d'un secret partagé	H.235.4	1
Tableau I.1	Identificateurs d'objet utilisés dans la Rec. UIT-T H.235.4	H.235.4	2

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