UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T J.125

(04/2004)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

SÉRIE J: RÉSEAUX CÂBLÉS ET TRANSMISSION DES SIGNAUX RADIOPHONIQUES, TÉLÉVISUELS ET AUTRES SIGNAUX MULTIMÉDIAS

Services interactifs pour la distribution de télévision numérique

Confidentialité des liaisons pour les implémentations de câblo-modems

Recommandation UIT-T J.125

Recommandation UIT-T J.125

Confidentialité des liaisons pour les implémentations de câblo-modems

Résumé

La présente Recommandation était l'Annexe O de l'Annexe B/J.112. Comme elle est également applicable aux services de confidentialité offerts dans la couche de commande MAC pour J.112, elle est devenue une Recommandation à part entière (J.125). Cette Recommandation, souvent désignée par l'expression *Interface de confidentialité de base Plus* ou *BPI+* a les deux objectifs suivants:

- offrir aux utilisateurs de câblo-modems la confidentialité des données dans tout le réseau en câble;
- offrir aux câblo-opérateurs une protection des services, c'est-à-dire empêcher des utilisateurs non autorisés d'avoir accès aux services de commande MAC par interface radioélectrique du réseau.

L'interface BPI+ offre un niveau de confidentialité des données, dans tout le réseau en câble à support partagé, égal ou supérieur à celui qui est offert par les services d'accès au réseau par ligne spécialisée (modems analogiques ou lignes d'abonnés numériques).

Source

La Recommandation UIT-T J.125 a été approuvée le 22 avril 2004 par la Commission d'études 9 (2001-2004) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

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 J.125

Confidentialité des liaisons pour les implémentations de câblo-modems

1 Domaine d'application

La présente Recommandation traite des services de confidentialité (cryptage et authentification) offerts dans la couche de commande MAC pour les communications DOCSIS entre système CMTS et câblo-modem (CM). Cette Recommandation, souvent désignée par l'expression *Interface de confidentialité de base Plus* ou *BPI+* a les deux objectifs suivants:

- offrir aux utilisateurs de câblo-modems la confidentialité des données dans tout le réseau en câble, et
- offrir aux câblo-opérateurs une protection des services, c'est-à-dire empêcher des utilisateurs non autorisés d'avoir accès aux services de commande MAC par interface radioélectrique du réseau.

L'interface BPI+ offre un niveau de confidentialité des données, dans tout le réseau en câble à support partagé, égal ou supérieur à celui qui est offert par les services d'accès au réseau par ligne spécialisée (modems analogiques ou lignes d'abonnés numériques).

2 Références

2.1 Références normatives

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[SCTE22-2] ANSI/SCTE 22-2 2002, *DOCSIS 1.0 Part 2: Baseline Privacy Interface Specification*, www.scte.org.

[SCTE23-3] ANSI/SCTE 23-3 2003, *DOCSIS 1.1 Part 3: Operations Support System Interface*, www.scte.org.

[SCTE79-2] ANSI/SCTE 79-2 2002, *DOCS 2.0 Operations Support System Interface*, www.scte.org.

[J.112-B] Recommandation UIT-T J.112 Annexe B (2004), *Spécifications de l'interface du service de transmission de données par câble: interface radioélectrique*.

[J.122] Recommandation UIT-T J.122 (2002), *Systèmes de transmission de deuxième génération pour les services interactifs de télévision par câble – Câblo-modems pour protocole IP*.

[FIPS-46-3] Federal Information Processing Standards Publications 46-3, *Data Encryption Standard (DES)*, octobre 1999.

[FIPS-140-2] Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, mai 2001.

[FIPS-180-2] Federal Information Processing Standards Publication 180-2, *Secure Hash Standard (SHS)*, août 2002.

[PKCS #7] IETF RFC 2315 (1998), *PKCS #7: Cryptographic Message Syntax Version 1.5*.

[RFC2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication*.

[RFC3083] IETF RFC 3083 (2001), *Baseline Privacy Interface Management Information Base for DOCSIS Compliant Cable Modems and Cable Modem Termination Systems*.

[RFC3280] IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[RSA3] *PKCS #1: RSA Cryptography Specifications Version 2.0*, octobre 1998.

[X.509] Recommandation UIT-T X.509 (2000) | ISO/CEI 9594-8:2001, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*.

2.2 Références informatives

[SCTE22-1] ANSI/SCTE 22-1 2002, *DOCSIS 1.0 Part 1: Radio Frequency Interface,* www.scte.org.

[SCTE22-3] ANSI/SCTE 22-3 2002, *DOCSIS 1.1 Part 3: Operations Support System Interface*, www.scte.org.

[DOCSIS4] *Data-Over-Cable Service Interface Specifications, Cable Modem to Customer Premise Equipment Interface Specification*, SP-CMCI-I09-030730.

[DOCSIS8] *Management Information Base for DOCSIS Cable Modems and Cable Modem Termination Systems for Baseline Privacy Plus*, draft-ietf-ipcdn-bpiplus-mib-05.txt, 8 mai, 2001.

[FIPS-74] Federal Information Processing Standards Publication 74, *Guidelines for Implementing and Using the NBS Data Encryption Standard*, avril 1981.

[FIPS-81] Federal Information Processing Standards Publication 81, *DES Modes of Operation*, décembre 1980 (Includes Change Notice, novembre 1981).

[FIPS-186-2] Federal Information Processing Standards Publication 186-2, *Digital Signature Standard (DSS)*, janvier 2000.

[RFC2868] IETF RFC 2868 (2000), *RADIUS Attributes for Tunnel Protocol Support*.

[RSA1] RSA Laboratories, *PKCS #1: RSA Encryption Standard, Version 1.5*, RSA Security, Inc., Bedford, MA, novembre 1993.

[RSA2] RSA Laboratories, *Some Examples of the PKCS Standards*, RSA Data Security, Inc., Redwood City, CA, novembre 1993.

3 Termes et définitions

La présente Recommandation définit les termes suivants:

3.1 DOCSIS: terme désignant un système ou un équipement conforme à chacune des séries de spécifications des *Cable Television Laboratories, Inc.* ("*CableLabs*") que l'on peut trouver à l'adresse: http://www.cablemodem.com/specifications/.

3.2 DOCSIS 1.0: système ou équipement conforme aux spécifications *Data Over Cable Service Interface Specifications* suivantes: [SCTE22-1], [SCTE22-2], [SCTE22-3], [DOCSIS4].

3.3 DOCSIS 1.1: système ou équipement conforme aux spécifications *Data Over Cable Service Interface Specifications* suivantes: [[J.112-B], [SCTE23-3], [DOCSIS4] et à la présente Recommandation.

3.4 DOCSIS 2.0: système ou équipement conforme aux spécifications *Data Over Cable Service Interface Specifications* suivantes: [J.122], [SCTE79-2], [DOCSIS4] et à la présente Recommandation.

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

BPI+ interface de confidentialité de base plus (*baseline privacy interface plus*)

BPKM gestion des clés de confidentialité de base (*baseline privacy key management*)

CBC concaténation de blocs chiffrants (*cipher block chaining*)

CM câblo-modem

CMTS système de terminaison de câblo-modem (*cable modem termination system*)

DES norme des Etats-Unis pour le chiffrement des données (*US data encryption standard*)

HMAC adressage dispersé sur clés calculées pour l'authentification des messages (*keyed-hashing for message authentication*)

QS qualité de service

RSA laboratoires RSA (*RSA laboratories*)

SA association de sécurité (*security association*)

SAID identificateur d'association de sécurité (*security association identifier*)

SID identificateur de service (*service identifier*)

TEK clés de cryptage du trafic (*traffic encryption key*)

5 Arrière-plan et aperçu général de la confidentialité de base plus

Les câblo-opérateurs sont intéressés par la mise en place de systèmes de communication rapides en mode paquet sur des réseaux de distribution de télévision par câble pouvant prendre en charge une grande variété de services. Les services envisagés par les câblo-opérateurs sont en particulier les suivants: accès IP (*Internet protocol*) à grande vitesse, téléphonie en mode paquet, service de vidéoconférence, équivalent du relais de trames, et bien d'autres services.

Le service prévu permettra un transfert transparent du trafic IP dans les deux sens, entre la tête de réseau du système en câble et les locaux d'abonné, sur un réseau entièrement composé de câbles coaxiaux ou sur un réseau hybride à fibre optique/câble coaxial, comme cela est représenté de manière simplifiée sur la Figure 5-1.

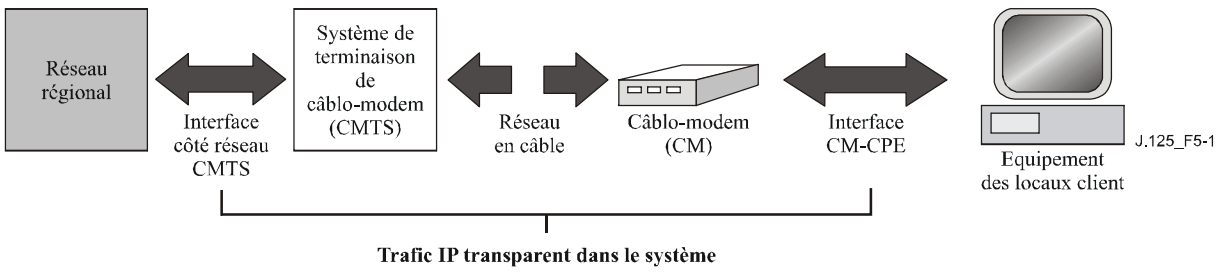


Figure 5-1/J.125 – Trafic IP transparent dans le système de données sur câble

Le canal de transmission par le système en câble est réalisé à la tête du réseau par un système de terminaison de câblo-modem (CMTS, *cable modem termination system*) et par un câblo-modem (CM) dans chaque local d'abonné. Dans la tête de réseau (ou dans le concentrateur), l'interface avec le système de transmission de données par câble est appelée interface entre système de terminaison de câblo-modem et côté réseau (CMTS-NSI, *cable modem termination system – network-side interface*). Dans les locaux d'abonné, l'interface est appelée interface entre câblo-modems et équipement des locaux client (CMCI). L'objectif est que les opérateurs transfèrent de manière transparente le trafic IP entre ces interfaces, y compris les datagrammes, les protocoles DHCP, ICMP et l'adressage de groupe IP (diffusion et multidiffusion), entre autres signaux.

L'interface de confidentialité de base plus (BPI+) offre aux utilisateurs de câblo-modems la confidentialité des données dans le réseau en câble en effectuant un cryptage des flux de trafic entre CM et CMTS. La confidentialité de base est la version originale de cette fonctionnalité et est détaillée dans la référence [SCTE22-2]. La confidentialité de base plus est la version mise à jour de cette fonctionnalité et le sujet de la présente Recommandation. Voir l'Annexe C pour un examen détaillé des différences entre les deux versions.

Par ailleurs, l'interface BPI+ offre aux câblo-opérateurs une protection robuste contre le vol de service. Les services de communication sécurisée de données de commande DOCSIS MAC s'inscrivent dans les trois catégories suivantes:

- services de données IP à grande vitesse avec meilleur effort;
- services de données de QS (par exemple, à débit binaire constant);
- services multidiffusés de groupe IP.

Par l'interface BPI+, le système CMTS protège contre l'accès non autorisé à ces services de transport de données en appliquant le cryptage des flux de trafic associés dans tout le réseau en câble. L'interface BPI+ fait appel à un protocole de gestion de clés de client/serveur authentifiées dans lequel le CMTS-serveur commande la distribution des données de cryptage aux CM clients.

5.1 Vue architecturale d'ensemble

Le service de confidentialité de base plus se compose des deux protocoles suivants:

- un protocole d'encapsulation pour le cryptage des paquets de données dans le réseau en câble. Ce protocole définit:
  1) le format de trame pour le transport de paquets de données chiffrées dans les trames de commande DOCSIS MAC;
  2) un ensemble de suites cryptographiques prises en charge, c'est-à-dire de paires de données chiffrées et d'algorithmes d'authentification;
  3) les règles d'application de ces algorithmes aux paquets de données en trames de commande DOCSIS MAC;
- un protocole de gestion de clés (gestion des clés de confidentialité de base ou "BPKM") assurant la distribution sécurisée des données de cryptage entre le système CMTS et les câblo-modems. C'est grâce à ce protocole de gestion de clés que CM et CMTS synchronisent les données de cryptage. Par ailleurs, le système CMTS utilise ce protocole pour appliquer l'accès conditionnel aux services du réseau.

5.1.1 Cryptage des paquets de données

Les services de cryptage de l'interface BPI+ sont définis comme étant un ensemble de services étendus à l'intérieur de la sous-couche de commande DOCSIS MAC. Les informations d'en-tête de paquet propres à l'interface BPI+ sont placées dans un élément d'en-tête étendu de confidentialité de base lui-même contenu dans l'en-tête étendu de commande DOCSIS MAC.

A la date de parution de la présente Recommandation, l'interface BPI+ prend en charge un seul algorithme de cryptage de données en paquet: le mode de concaténation de blocs chiffrants (CBC, *cipher block chaining*) de l'algorithme de cryptage de données selon la norme DES des Etats-Unis d'Amérique [FIPS-46-2], [FIPS-81]. L'interface BPI+ n'apparie pas la concaténation CBC de la norme DES avec un quelconque algorithme d'authentification de données en paquets. D'autres algorithmes de cryptage de données pourront être pris en charge dans d'ultérieures améliorations de la spécification du protocole BPI+ et ces algorithmes pourront être appariés avec des algorithmes d'authentification de données.

L'interface BPI+ chiffre un paquet de données de trame DOCSIS MAC. L'en-tête de la trame DOCSIS MAC n'est pas chiffré. Les messages de gestion DOCSIS MAC DOIVENT être envoyés non codés afin de faciliter l'inscription, la télémétrie et le fonctionnement normal de la sous-couche DOCSIS MAC[1].

Le paragraphe 6 spécifie le format des trames DOCSIS MAC qui transportent des charges utiles de données chiffrées en mode paquet.

5.1.2 Protocole de gestion de clés

Les CM utilisent le protocole de gestion de clés de confidentialité de base afin d'obtenir du système CMTS les autorisations et les données de calcul des clés de trafic et afin de prendre en charge la réautorisation périodique ainsi que le rafraîchissement de ces clés. Le protocole de gestion de clés utilise les certificats numériques X.509 [ITU1], l'algorithme de cryptage de clé publique RSA [RSA3] et le triple calcul DES à deux clés afin d'assurer les échanges de clés entre CM et CMTS.

Le protocole de gestion de clés de confidentialité de base est conforme à un modèle de client/serveur où le CM, qui est un "client" de gestion BPKM, demande les données de calcul de clé et où le CMTS, qui est un "serveur" de gestion BPKM, répond à ces demandes en veillant à ce que les clients CM ne reçoivent que les données de calcul de clé qui leur sont autorisées. Le protocole de gestion BPKM utilise la messagerie de gestion DOCSIS MAC.

L'interface BPI+ utilise la cryptographie par clé publique afin d'établir un secret partagé (c'est-à-dire une clé d'autorisation) entre CM et CMTS. Le secret partagé est ensuite utilisé pour assurer les échanges ultérieurs de clés de cryptage du trafic par gestion BPKM. Ce mécanisme à deux niveaux pour la distribution des clés permet de rafraîchir les clés de cryptage du trafic sans entraîner la redondance des opérations à clés publiques, grandes consommatrices de calculs.

Un système CMTS authentifie un CM client au cours de l'échange d'autorisation initial. Chaque CM achemine un unique certificat numérique X.509 qui est émis par le fabricant du CM. Ce certificat numérique contient la clé publique du CM ainsi que d'autres informations d'identification comme l'adresse MAC du CM, l'identificateur du fabricant et le numéro de série. Lorsqu'il demande une autorisation, le CM présente à un CMTS son certificat numérique. Le CMTS vérifie le certificat numérique puis utilise la clé publique vérifiée pour coder une clé d'autorisation qu'il renvoie au CM demandé.

Le système CMTS associe une identité authentifiée de câblo-modem à un abonné payant et donc aux services de transmission de données auxquelles cet abonné est autorisé à accéder. Muni de la clé d'autorisation, le système CMTS établit donc une identité authentifiée de client CM et détermine les services (c'est-à-dire les clés spécifiques de cryptage du trafic) auxquels le CM est autorisé à accéder.

---

[1] Les en-têtes DOCSIS MAC des unités PDU de données en paquets et les messages de gestion DOCSIS MAC non BPI+ PEUVENT être chiffrés lorsqu'ils font partie d'un paquet fragmenté et concaténé [J.112-B] ou [J.122].

Etant donné que le système CMTS authentifie le CM, il peut protéger contre une attaque faisant appel à un modem *cloné*, simulant un modem d'abonné normal. L'utilisation des certificats X.509 empêche que des modems clonés transmettent à un CMTS de faux justificatifs.

Les CM DOIVENT avoir des paires de clés privées/publiques RSA installées en usine ou comporter un algorithme interne permettant de produire dynamiquement de telles paires de clés. Si un CM se fonde sur un algorithme interne pour produire sa paire de clés RSA, ce CM DOIT produire cette paire de clés avant sa première initialisation de confidentialité de base, décrite au § 5.2.1. Les CM possédant des paires de clés RSA installées en usine DOIVENT posséder également des certificats X.509 installés en usine. Les câblo-modems qui se fondent sur des algorithmes internes pour produire une paire de clés RSA DOIVENT prendre en charge un mécanisme permettant d'installer un certificat X.509 émis par le fabricant à la suite de la production des clés.

Le protocole de gestion BPKM est décrit en détail dans le paragraphe 7.

5.1.3 Associations de sécurité de l'interface BPI+

Une association de sécurité (SA, *security association*) de l'interface BPI+ est l'ensemble des informations de sécurité qui sont partagées par un système CMTS et par un ou plusieurs de ses CM clients afin de prendre en charge des communications sécurisées dans le réseau en câble. L'interface BPI+ définit trois types d'association de sécurité: *primaire, statique, dynamique*. Une association de sécurité primaire est rattachée à un seul CM. Elle est établie lorsque ce CM effectue l'inscription DOCSIS MAC. Les associations de sécurité statiques sont préconfigurées dans le système CMTS. Les associations de sécurité dynamiques sont établies et supprimées, dynamiquement, en réponse à la création et à la suppression de flux de trafic (aval) spécifiques. Les associations SA aussi bien statiques que dynamiques peuvent être partagées par de multiples CM.

Une information partagée d'association de sécurité comporte des clés de cryptage du trafic et des vecteurs d'initialisation de concaténation CBC. Afin de prendre en charge, dans les futures versions améliorées de l'interface BPI+, d'autres algorithmes de cryptage et d'authentification des données, les paramètres d'association de sécurité BPI+ comportent un identificateur de suite cryptographique qui indique l'appariement particulier d'algorithmes de cryptage et d'authentification de données en paquet, employé par l'association de sécurité. Lors de la parution de la présente Recommandation, les deux seuls algorithmes de cryptage de données en paquet pris en charge sont le DES 56 bits et DES 40 bits. Aucun des deux n'est apparié à un algorithme d'authentification de données en mode paquet[2].

L'interface BPI+ identifie les associations de sécurité au moyen d'un *identificateur d'association de sécurité (SAID)* de 14 bits.

Chaque CM (activé par interface BPI+) établit avec son CMTS une association de sécurité primaire à titre exclusif. Tout le trafic amont d'un CM DOIT être chiffré conformément à l'association de sécurité primaire et exclusive du CM. L'identificateur SAID correspondant à une SA primaire de CM DOIT être égal à l'identificateur de service primaire (SID) DOCSIS 1.1 ou DOCSIS 2.0 du CM, [J.112-B] ou [J.122]. D'autre part, bien que tout le trafic unidiffusé en aval vers un ou des dispositifs CPE situés derrière le CM soit chiffré selon l'association de sécurité primaire et exclusive du CM, certains flux de trafic unidiffusés en aval peuvent être chiffrés selon l'un des trois types d'association SA. Un paquet de données IP multidiffusé en aval est cependant destiné normalement à de multiples CM: il est donc plus susceptible d'être chiffré selon les SA statiques ou dynamiques, auxquelles de multiples CM peuvent accéder, que selon une SA primaire qui est limitée à un seul CM.

---

[2] L'interface BPI+ chiffre un code CRC Ethernet/802.3 d'unité PDU en mode paquet. Bien que ce mécanisme offre un certain degré d'authentification des données, il n'assure pas une authentification cryptographiquement sécurisée des données.

Le câblo-modem conforme DOIT prendre en charge une SA primaire, une ou plusieurs SA dynamiques, et une ou plusieurs SA statiques. Le CMTS conforme DOIT prendre en charge une SA primaire, une ou plusieurs SA dynamiques, et PEUT prendre en charge une ou plusieurs SA statiques. Les spécifications BPI+ ne spécifient pas le nombre de SA statiques et dynamique requises pour ces services.

Au moyen du protocole de gestion BPKM, un CM demande à son CMTS les données de calcul de clés d'une association de sécurité. Le CMTS veille à ce que chaque CM client n'accède qu'aux associations de sécurité dont l'accès lui est autorisé.

Dans une association de sécurité, un matériel de calcul de clés (comme une clé DES et un vecteur d'initialisation de concaténation CBC) possède une durée de vie limitée. Lorsque le système CMTS achemine un matériel de calcul de clés SA vers un CM, il transfère également à celui-ci la durée de vie qui reste à ce matériel. C'est au CM qu'il appartient de demander au CMTS un nouveau matériel de calcul de clés avant que l'ensemble du matériel de calcul de clés que le CM détient actuellement expire dans le système CMTS. Le protocole BPKM spécifie la façon dont CM et CMTS conservent le synchronisme des clés.

5.1.4 Identificateurs SID de QS et identificateurs SAID d'interface BPI+

L'élément d'en-tête étendu BPI+ des trames DOCSIS MAC aval contient l'identificateur SAID d'interface BPI+ selon lequel la trame aval est chiffrée. Si la trame aval est un paquet unidiffusé vers l'adresse d'un équipement CPE situé derrière un CM particulier, cette trame sera normalement chiffrée selon l'association SA primaire de ce CM, auquel cas l'identificateur SAID sera égal à l'identificateur SID primaire du CM cible. Si la trame aval est un paquet multidiffusé qui est destiné à être reçu par de multiples CM, l'élément d'en-tête étendu contiendra l'identificateur SAID statique ou dynamique qui a été appliqué à ce groupe multidiffusé. L'identificateur SAID (primaire, statique ou dynamique), en combinaison avec d'autres champs de données contenus dans l'élément d'en-tête étendu aval, indique à un modem récepteur l'ensemble particulier du matériel de calcul de clés qui est requis pour déchiffrer le champ de données chiffrées en mode paquet de la trame DOCSIS MAC.

Etant donné que tout le trafic amont d'un CM est chiffré selon son unique association de sécurité primaire, les trames DOCSIS MAC amont n'ont pas besoin, contrairement aux trames DOCSIS MAC aval, de transporter un identificateur SAID d'interface BPI+ dans leur en-tête étendu. En revanche, l'élément d'en-tête étendu de confidentialité de base contient l'identificateur de QS qui désigne le flux de service amont sur lequel la trame DOCSIS MAC est transportée.

L'élément d'en-tête étendu de confidentialité de base sert à plusieurs fins dans les trames DOCSIS MAC amont d'unité PDU de données en mode paquet. En plus de l'identification de l'ensemble particulier du matériel de calcul de clés utilisé pour coder les données en mode paquet d'une trame, cet élément offre un mécanisme permettant d'émettre des requêtes de largeur de bande portées, tout en pouvant transporter des données de commande de fragmentation. Ces deux dernières fonctions sont rattachées à un identificateur SID de QS particulier. C'est pourquoi les éléments d'en-tête étendu de confidentialité de base contiennent un identificateur de QS plutôt qu'un identificateur SAID primaire d'interface BPI+, que l'on peut déduire de l'identificateur SID de QS.

5.2 Aperçu général des opérations

5.2.1 Initialisation du câblo-modem

[J.112-B] ou [J.122] subdivise l'initialisation du câblo-modem en la séquence de tâches suivante:

- analyse du canal aval et calage du synchronisme avec le système CMTS;
- obtention des paramètres d'émission;
- exécution de la télémétrie;

- établissement de la connexité IP (DHCP);
- détermination de l'heure locale;
- transfert des paramètres opérationnels (téléimportation du fichier de paramètres par protocole TFTP);
- inscription du système CMTS.

L'établissement de la confidentialité de base fait suite à l'inscription du système CMTS.

Si un câblo-modem doit fonctionner en mode confidentialité de base, le réglage d'activation de confidentialité (type 29) du fichier de configuration de style DOCSIS 1.1 ou 2.0 DOIT être explicitement/implicitement mis sur activation, indépendamment de la présence des réglages de configuration de confidentialité de base (type 17). En d'autres termes, les réglages de configuration de confidentialité de base ne doivent pas nécessairement être présents dans le fichier de configuration pour faire fonctionner la confidentialité de base. Ces réglages de configuration supplémentaires sont définis dans l'Annexe A.

Après avoir effectué son inscription, le système CMTS attribue au CM qui s'inscrit un ou plusieurs identificateurs de service (SID) statiques qui correspondent à la classe de service préconfigurée statiquement dans ce CM. Le premier identificateur SID statique qui a été attribué au cours du processus d'inscription est le SID primaire, qui servira également de SAID primaire d'interface BPI+ pour le CM. Si un CM est configuré de façon à assurer la confidentialité de base, l'inscription du CMTS est immédiatement suivie de l'initialisation des fonctions de sécurité du CM en termes de confidentialité de base.

L'initialisation de la confidentialité de base commence par l'envoi au CMTS par le CM d'un message d'information d'authentification avec le certificat CA du fournisseur du CM et d'une demande d'autorisation contenant:

- les données d'identification du CM (comme l'adresse MAC);
- la clé publique RSA du CM;
- un certificat X.509 vérifiant le lien entre les données d'identification du CM et la clé publique du CM;
- une liste de capacités de sécurité du CM (c'est-à-dire les appariements particuliers d'algorithmes de cryptage et d'authentification pris en charge par le CM);
- l'identificateur SAID primaire du CM (c'est-à-dire le SID primaire).

Si le système CMTS détermine que le CM demandeur est autorisé à recevoir l'identificateur SAID primaire de la demande d'autorisation, ce CMTS renvoie une réponse d'autorisation contenant une clé d'autorisation à partir de laquelle CM et CMTS calculent les clés nécessaires pour sécuriser les demandes ultérieures de clés de cryptage de trafic d'un CM ainsi que les réponses du CMTS à ces demandes. Le CMTS chiffre la clé d'autorisation avec la clé publique du câblo-modem récepteur.

La réponse d'autorisation contient également une liste de descripteurs d'association de sécurité désignant les associations SA primaires et statiques auxquelles le CM demandeur est autorisé à accéder. Chaque descripteur SA se compose d'une série de paramètres SA, y compris l'identificateur SAID, le type et les données cryptographiques de l'association SA. La liste contient au moins une entrée, qui est un descripteur de l'association de sécurité primaire du CM. Les autres entrées sont facultatives et décrivent toute association SA statique à laquelle le CM peut accéder par préconfiguration.

Après avoir réussi les opérations d'authentification et d'autorisation auprès du système CMTS, le câblo-modem envoie à celui-ci des demandes de clé de cryptage du trafic à utiliser avec chacun de ses identificateurs SAID. Les demandes de clé de trafic d'un CM sont authentifiées au moyen d'un calcul de dispersion sur clés calculées (par l'algorithme HMAC [RFC 2104]). La clé d'authentification de message est calculée d'après la clé d'autorisation obtenue au cours de l'échange

d'autorisation antérieur. Le CMTS renvoie des réponses de clés contenant des clés de cryptage de trafic (TEK, *traffic encryption keys*), qui sont codées par triple algorithme DES avec une clé de cryptage de clés calculée d'après la clé d'autorisation. Comme les demandes de clés, les réponses de clés sont authentifiées par dispersion sur clés calculées, la clé d'authentification de message étant déduite de la clé d'autorisation.

L'initialisation de la confidentialité de base se termine lorsque le CMTS envoie ou lorsque le CM reçoit les messages de réponses de clés avec tous les identificateurs SAID dans le message de réponse d'autorisation.

5.2.2 Mécanisme de mise à jour des clés de câblo-modem

Les clés de cryptage du trafic que le système CMTS remet aux câblo-modems clients ont une durée de vie limitée. Le CMTS indique une durée de vie restante de clé, en même temps que la valeur de celle-ci, dans les réponses de clés qu'il envoie à son CM client. Le CMTS détermine les clés qui sont actuellement valides en éliminant les clés périmées et en produisant de nouvelles clés. Il appartient à chaque câblo-modem de veiller à ce que les clés qu'il utilise correspondent à celles que le CMTS utilise. A cette fin, les câblo-modems recherchent le moment où l'expiration d'une clé de SAID est prévue et émettent une nouvelle demande de clé visant la plus récente clé antérieure au moment de cette expiration.

Par ailleurs, les câblo-modems sont tenus de renouveler périodiquement leur autorisation auprès du système CMTS. Comme c'est le cas avec les clés de cryptage du trafic, une clé d'autorisation a une durée de vie limitée, qui est indiquée par le CMTS au CM en même temps que la valeur de clé. Il appartient à chaque câblo-modem de renouveler cette autorisation et d'obtenir une clé d'autorisation actualisée (ainsi qu'une liste à jour des descripteurs d'association SA) avant que le CMTS fasse expirer la clé d'autorisation actuelle du CM.

L'initialisation de la confidentialité de base et la mise à jour des clés sont implémentées dans le protocole de gestion de clés de confidentialité de base qui est défini en détail au § 7.

6 Formats des trames de gestion DOCSIS MAC

Lors du fonctionnement après activation d'une interface BPI+, à n'importe quel moment après la fin de l'initialisation de la confidentialité de base, le CM et le CMTS DOIVENT crypter les régions contenant des unités PDU de données des deux types suivants de trames DOCSIS MAC qu'ils émettent dans le réseau en câble, et NE DOIVENT transmettre AUCUN de ceux-ci sur le réseau en câble sans l'avoir crypté, à moins que les spécifications DOCSIS le permettent explicitement ou que l'opérateur le prévoie explicitement:

- trames MAC contenant des unités PDU de données en paquets de longueur variable;
- trames MAC de fragmentation.

Dans chacun de ces deux cas, un élément d'en-tête étendu de confidentialité de base, contenu dans l'en-tête de trame DOCSIS MAC, identifie l'association de sécurité et le matériel de calcul de clés correspondant, afin de chiffrer l'unité PDU de données.

6.1 Format des trames MAC à unités PDU de données en mode paquet de longueur variable

La Figure 6-1 illustre le format d'une unité PDU de données en mode paquet de longueur variable DOCSIS contenant un élément d'en-tête étendu (EH, *extended header*) de confidentialité et une charge utile d'unité PDU en mode paquet chiffrée.

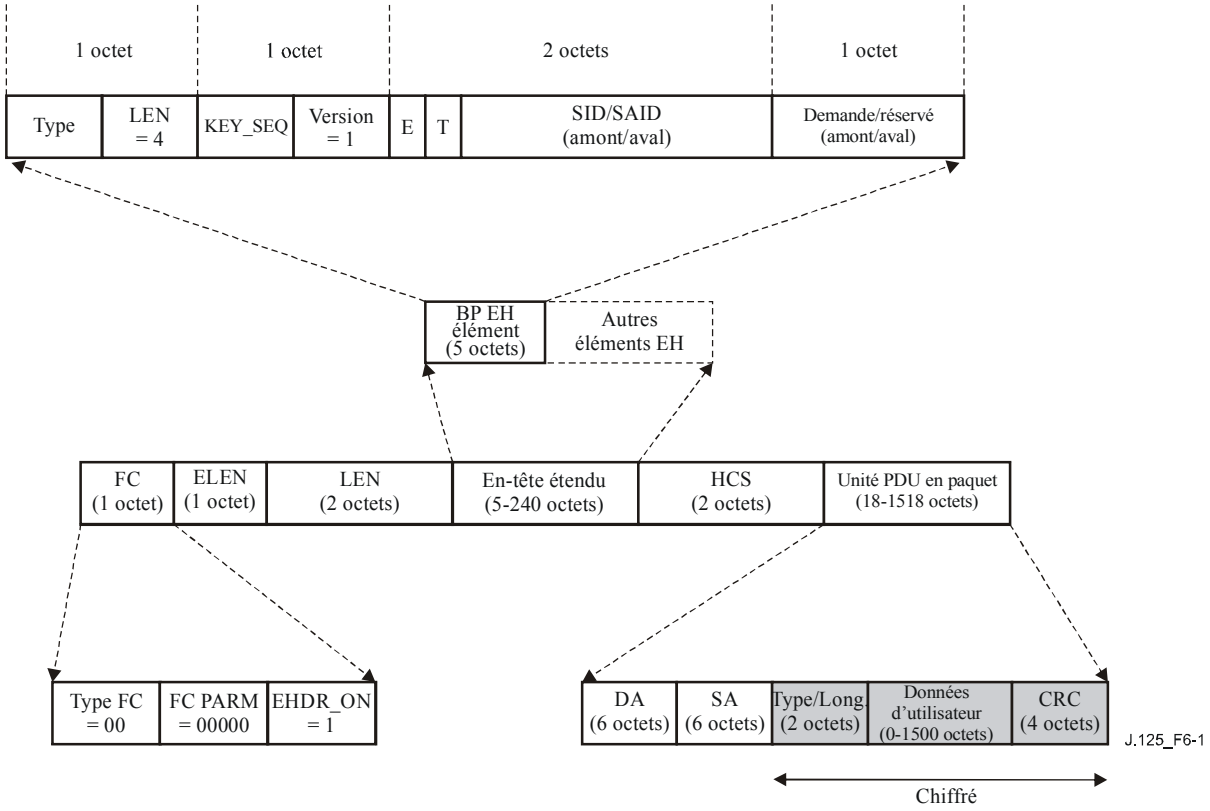


Figure 6-1/J.125 – Format d'une unité PDU de données en mode paquet de longueur variable DOCSIS avec élément EH de confidentialité

Les douze premiers octets de l'unité PDU en mode paquet, contenant les adresses Ethernet/802.3 de destination et de départ (DA/SA), ne sont pas chiffrés. La transmission non codée de l'adresse de destination et de départ d'une trame offre aux vendeurs une plus grande flexibilité quant à la façon dont ils intègrent le cryptage/déchiffrage dans la fonctionnalité DOCSIS MAC. Les vendeurs ont par exemple la possibilité de choisir entre un filtrage initial d'après les adresses DA/SA ou d'après l'identificateur SID. Le code CRC d'adresse Ethernet/802.3 de l'unité PDU en paquet est chiffré.

Le système CMTS inclut l'élément EH de confidentialité de base dans toutes les unités PDU de données en paquet aval qu'il chiffre selon l'interface BPI+. De même, un CM inclut l'élément EH de confidentialité de base dans toutes les unités PDU de données en paquet amont qu'il chiffre selon l'interface BPI+. Si plusieurs éléments d'en-tête étendu sont présents dans l'en-tête DOCSIS MAC, l'élément d'en-tête étendu de confidentialité de base DOIT être le premier.

L'élément d'en-tête étendu de confidentialité utilise deux valeurs de type d'élément EH: BPI_UP et BPI_DOWN, utilisés respectivement avec les unités PDU amont et aval de données en paquet. [J.112-B] ou [J.122] définit les valeurs spécifiques de type d'élément EH qui sont attribuées à BPI_UP et à BPI_DOWN.

Les quatre bits de plus fort poids du champ de valeur d'un élément d'en-tête étendu BPI+ contiennent un numéro de séquence de clé, KEY_SEQ. Compte tenu du fait que le matériel de calcul de clés associé à un identificateur SAID d'interface BPI+ possède une durée de vie limitée et que le système CMTS rafraîchit périodiquement ce matériel de calcul de clés d'identificateur SAID, le CMTS gère un numéro de séquence de clé de 4 bits indépendamment pour chaque SAID et attribue aux CM clients ce numéro de séquence de clé en même temps que le matériel de calcul de clés d'identificateur SAID. Le CMTS incrémente le numéro de séquence de clé à chaque nouveau matériel de calcul de clés produit. L'élément EH de confidentialité intègre ce numéro de séquence, ainsi que l'identificateur SAID, afin d'identifier la production spécifique de ce matériel de calcul de

clés de SAID utilisé pour chiffrer l'unité PDU de données en paquet rattachée. Comme il s'agit d'un champ de 4 bits, le numéro de séquence revient à 0 après avoir atteint la valeur 15.

Un CM ou un CMTS, lorsqu'il compare un numéro de séquence de clé de trame reçu avec ce qu'il estime être le numéro de séquence de clé "actuel", peut facilement reconnaître une perte de synchronisme de clés avec son homologue. Un CM DOIT conserver les deux plus récentes productions de matériel de calcul de clés pour chaque identificateur SAID d'interface BPI+. Cette tenue à disposition des deux plus récentes productions de clé est nécessaire pour assurer un service ininterrompu au cours d'une transition de clé d'identificateur SAID.

Le champ de 4 bits qui suit la séquence KEY_SEQ contient un numéro de version de protocole qui est mis à 1 dans les en-têtes DOCSIS MAC d'unité PDU de données en paquet de longueur variable.

Les deux octets suivants contiennent les 2 bits d'état de cryptage et le champ de 14 bits des identificateurs SID/SAID (SID pour les trames amont et SAID pour les trames aval). Le bit d'état de cryptage ENABLE indique si le cryptage est activé ou désactivé pour l'unité PDU considérée. Si le bit ENABLE est à 0, l'unité PDU de données en paquet n'est pas chiffrée et l'élément EH de confidentialité de base DOIT être ignoré (à l'exception de la demande de largeur de bande facultativement portée, voir ci-dessous). Le bit TOGGLE DOIT correspondre à l'état du bit de plus faible poids (LSB, *least significant bit*) du numéro de séquence de clé (KEY_SEQ).

Le protocole de gestion DOCSIS MAC [J.112-B] ou [J.122] définit un élément EH de demande de portage d'une demande de largeur de bande dans une transmission de données. La confidentialité de base définit un mécanisme additionnel pour le portage des demandes de largeur de bande: le dernier octet de l'élément EH amont de confidentialité de base (type d'élément EH = BPI_UP) achemine facultativement en portage une demande d'attribution de largeur de bande. Si une demande est portée, l'octet représente le nombre de mini-intervalles demandé. L'identificateur SID de 14 bits contenu dans l'élément EH amont de confidentialité de base désigne le SID auquel la demande de bande est applicable. Si l'élément EH de confidentialité de base ne porte aucune demande, l'octet de demande est mis à zéro. Une demande portée dans un élément EH de confidentialité de base DOIT être traitée, quel que soit l'état du bit ENABLE.

Dans les paquets aval (type d'élément d'en-tête étendu = BPI_DOWN), le quatrième et dernier octet est réservé et mis à zéro.

Tableau 6-1/J.125 – Résumé du contenu des deux éléments EH de confidentialité de base

EH_TYPE	EH_LEN	EH_VALUE
BPI__UP Voir [J.112-B] ou [J.122]	4	KEY_SEQ (4 bits), version (4 bits), SID (2 octets), demande [portée] (1 octet) [CM → CMTS] Champ KEY_SEQ (4 bits): numéro de séquence de clé Le champ de version (4 bits) est défini ainsi: 0x1 Le champ SID est défini ainsi: Bit[15]: ENABLE: 1..cryptage activé; 0..cryptage désactivé Bit[14]: TOGGLE: 1..clé impaire; 0..clé paire Bits[13..0]: identificateur de service. Le champ de demande contient le nombre de mini-intervalles demandé pour la largeur de bande amont.

Tableau 6-1/J.125 – Résumé du contenu des deux éléments EH de confidentialité de base

EH_TYPE	EH_LEN	EH_VALUE
BPI__DOWN Voir [J.112-B] ou [J.122]	4	KEY_SEQ (4 bits), version (4 bits), SID (2 octets), champ réservé (1 octet) [CMTS → CM] Champ KEY_SEQ (4 bits): numéro de séquence de clé Le champ de version (4 bits) est défini ainsi: 0x1 Le champ SAID est défini ainsi: Bit[15]: ENABLE: 1..cryptage activé; 0..cryptage désactivé Bit[14]: TOGGLE: 1..clé impaire; 0..clé paire Bits[13..0]: ID d'association de sécurité. Le champ réservé est mis à 0.

Dans le cas d'unités PDU de données en paquet chiffrées et émises dans un intervalle de conflit de données amont, l'identificateur SID contenu dans l'élément EH de confidentialité de base DOIT désigner le SID de QS. Il NE DOIT PAS désigner l'identificateur de service multidiffusé d'intervalle de conflit demande/données.

6.2 Format de trame MAC de fragmentation

Afin d'assurer la fragmentation des trames DOCSIS MAC amont, DOCSIS 1.1 ou DOCSIS 2.0 a remanié l'élément EH de confidentialité de base de façon qu'il achemine les champs de commande de cryptage comme de fragmentation [J.112-B] ou [J.122]. Lors du fonctionnement dans ce double rôle, l'élément EH de confidentialité de base amont (élément EH de type BPI_UP) est étendu d'un octet, l'octet final servant de champ de commande de fragmentation. La Figure 6-2 illustre le format d'une trame MAC de fragmentation DOCSIS contenant une charge utile de fragmentation chiffrée.

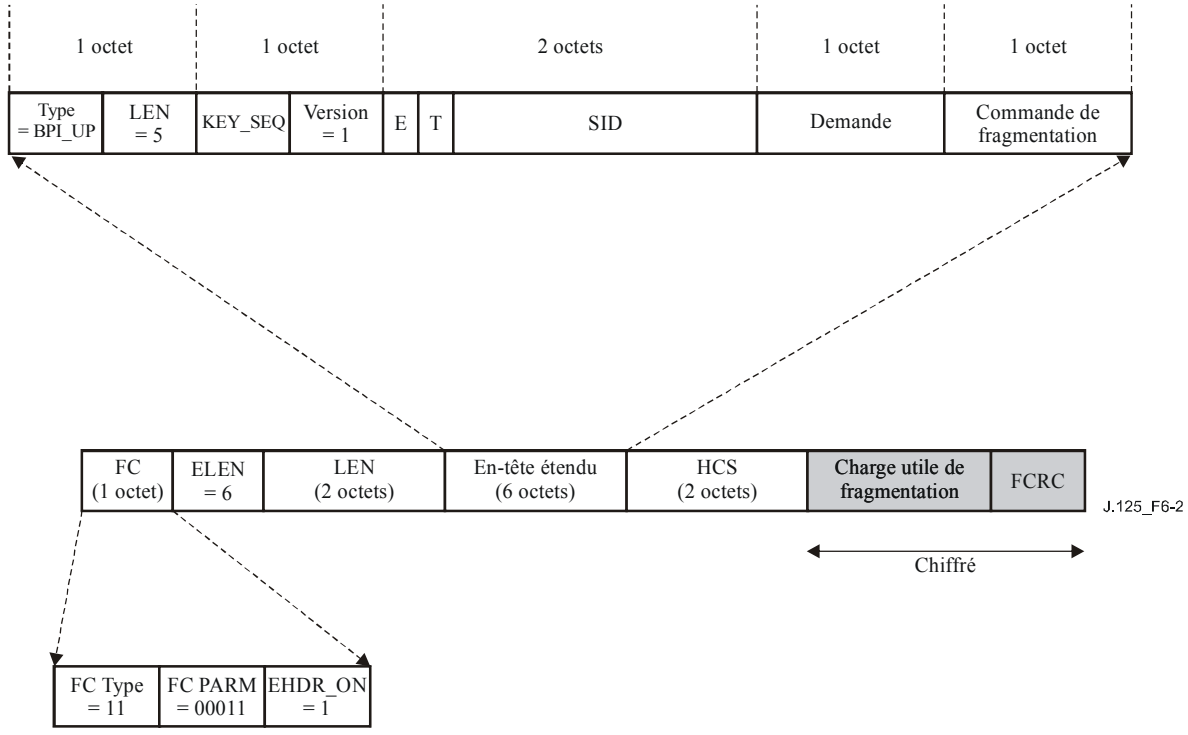


Figure 6-2/J.125 – Format d'une trame DOCSIS MAC de fragmentation avec charge utile chiffrée

Une trame DOCSIS MAC est identifiée comme une trame de fragmentation si FC Type = 11 et FC PARM = 00011. Contrairement aux trames MAC d'unité PDU de données en paquet, les trames MAC de fragmentation ont un en-tête étendu MAC de longueur fixe (6 octets) contenant l'élément EH de confidentialité de base "étiré".

L'en-tête de fragmentation MAC est suivi d'une charge utile de fragments et d'un CRC de fragments. Lorsque le cryptage de confidentialité de base est appliqué à une trame MAC de fragmentation, l'*ensemble* de la charge utile est chiffré en même temps que le CRC de fragments. En d'autres termes, contrairement au cryptage de confidentialité de base des unités PDU de données en paquet, il n'y a pas de décalage de 12 octets dans la charge utile avant le début du cryptage.[3]

Le champ LEN de l'élément EH de confidentialité de base des trames MAC de fragmentation est de 5 au lieu de 4 afin de tenir compte de l'octet du champ de commande de fragmentation additionnel. Le champ KEY_SEQ, le champ VERSION, les fanions ENABLE et TOGGLE et le champ SID sont les mêmes que dans une trame MAC d'unité PDU de données en paquet amont.

Tableau 6-2/J.125 – Contenu d'un élément EH de confidentialité de base d'une trame DOCSIS MAC de fragmentation

EH_TYPE	EH_LEN	EH_VALUE
BPI__UP Voir [J.112-B] ou [J.122]	5	KEY_SEQ (4 bits), version (4 bits), SID (2 octets), demande [portée] (1 octet), commande de fragmentation (1 octet) [CM → CMTS] Champ KEY_SEQ (4 bits): numéro de séquence de clé Le champ de version (4 bits) est défini ainsi: 0x1 Le champ SID est défini ainsi: Bit[15]: ENABLE: 1..cryptage activé; 0..cryptage désactivé Bit[14]: TOGGLE: 1..clé impaire; 0..clé paire Bits[13..0]: Identificateur de service. Le champ de demande contient le nombre de mini-intervalles demandé pour la largeur de bande amont. Le champ de commande de fragmentation contient des informations de commande propres à la fragmentation; voir [J.112-B] ou [J.122] pour les détails.

L'opération de fragmentation neutralise l'interface BPI+ en ce sens que le CM doit d'abord déterminer si un paquet sera ou non fragmenté en fonction de la grandeur de l'attribution (nombre de mini-intervalles attribué par un CMTS à un CM dans une table MAP d'attribution de largeur de bande amont, [J.112-B] ou [J.122]). Si le paquet doit être fragmenté, le cryptage BPI+ DOIT intervenir fragment par fragment et sur l'unité PDU dans son ensemble. Chaque fragment aura son propre en-tête de fragmentation et sera chiffré séparément. Si le paquet ne doit pas être fragmenté, il DOIT être chiffré comme un seul élément, avec un unique en-tête de confidentialité.

[3] Dans les trames non fragmentées, les 12 premiers octets sont laissés non codés afin de permettre un filtrage d'adresses DA/SA avant déchiffrage. Dans les trames fragmentées, le filtrage d'adresses DA/SA ne peut pas intervenir avant le réassemblage des paquets: il n'y a donc aucun intérêt à prendre en charge le décalage de 12 octets lors du cryptage des trames MAC de fragmentation.

6.3 Prescriptions relatives à l'utilisation d'un élément d'en-tête étendu BP dans un en-tête MAC

Si l'interface BPI+ n'est pas activée dans un flux de trafic aval particulier (par exemple, un trafic unidiffusé de CM ou un groupe IP multidiffusé particulier), l'élément d'en-tête étendu BP NE DEVRAIT PAS être utilisé.

Si l'interface BPI+ n'est pas activée pour le trafic unidiffusé d'un CM, les trames amont fragmentées DOIVENT utiliser l'élément d'en-tête étendu BP mais avec le bit de cryptage ENABLE désactivé (0). Ainsi l'en-tête étendu peut toujours être utilisé pour des demandes de largeur de bande facultativement portée en accord avec les règles de fragmentation décrites dans [J.112-B] ou [J.122].

Dans le cas des trames MAC composées seulement d'un en-tête de gestion MAC et d'un en-tête étendu (EHDR), la confidentialité de base DOIT être désactivée. Un en-tête étendu de confidentialité de base EHDR PEUT être présent dans ces trames mais le bit de cryptage DOIT être désactivé afin d'annuler la confidentialité.

7 Protocole de gestion de clés de confidentialité de base (BPKM)

7.1 Modèles à états

7.1.1 Introduction

Le protocole de gestion BPKM est spécifié par deux modèles à états distincts mais interdépendants: un modèle à états d'autorisation (automate à états d'autorisation) et un modèle à états de clés de service opérationnel (automate à états de clés de cryptage du trafic ou TEK). Le présent paragraphe ne définit ces deux modèles à états qu'à titre documentaire et ne devrait pas être considéré comme imposant une implémentation concrète.

L'autorisation du câblo-modem, contrôlée par l'automate à états d'autorisation, est un processus comportant les opérations suivantes:

- authentification par le système CMTS de l'identité d'un CM client;
- fourniture par le CMTS au CM authentifié d'une clé d'autorisation permettant de calculer une clé de cryptage de clé (KEK, *key encryption key*) et des clés d'authentification de message;
- fourniture par le CMTS au CM authentifié des identités (c'est-à-dire des identificateurs SAID) et des propriétés des associations de sécurité primaires et statiques pour lesquelles ce CM est autorisé à obtenir des informations de cryptage.

La clé KEK résulte d'un triple cryptage DES sur deux clés. Elle est utilisée par le système CMTS pour coder les clés de cryptage du trafic (TEK, *traffic encryption key*) qu'il envoie au modem. Les clés TEK servent à chiffrer le trafic de données d'utilisateur. Le CM et le CMTS utilisent des clés d'authentification de message pour authentifier, au moyen d'un résumé de message chiffré, les demandes et les réponses relatives aux clés qu'ils échangent.

Après avoir obtenu l'autorisation initiale, un câblo-modem sollicite périodiquement une nouvelle autorisation auprès du système CMTS. La réautorisation est également gérée par l'automate à états d'autorisation du CM. Un CM DOIT conserver son statut d'autorisation auprès du CMTS pour être en mesure de rafraîchir les clés de cryptage de trafic proches de la péremption. Les automates à états de clés TEK gèrent le rafraîchissement des clés de cryptage du trafic.

Un câblo-modem commence le processus d'autorisation par l'envoi à son système CMTS d'un message d'information d'authentification contenant le certificat X.509 du fabricant du CM. Le message d'information d'authentification est strictement informatif, c'est-à-dire que le CMTS peut

choisir de ne pas en tenir compte. Il permet cependant au système CMTS de connaître les certificats de fabrication de ses CM clients.

Le câblo-modem envoie un message de demande d'autorisation à son CMTS immédiatement après avoir envoyé le message d'information d'authentification. Il s'agit d'une demande de clé d'autorisation, ainsi que d'une demande des identificateurs SAID désignant les éventuelles associations de sécurité statiques auxquelles le CM est autorisé à participer. La demande d'autorisation comprend les éléments suivants:

- l'identificateur du fabricant et le numéro de série du câblo-modem;
- l'adresse de gestion MAC du câblo-modem;
- la clé publique du câblo-modem;
- un certificat X.509 émis par le fabricant et associant la clé publique du câblo-modem à ses autres informations d'identification;
- une description des algorithmes cryptographiques pris en charge par le câblo-modem demandeur: les capacités cryptographiques d'un CM sont présentées au CMTS sous la forme d'une liste d'identificateurs de suite cryptographique, indiquant chacun une paire particulière d'algorithmes de cryptage et d'authentification de données en paquet pris en charge par le CM;
- l'identificateur SAID primaire du câblo-modem, *qui est égal à l'identificateur SID primaire du CM* (l'identificateur SID primaire est le premier identificateur SID statique que le CMTS attribue à un CM au cours de l'inscription de gestion MAC à l'interface RF).

En réponse à un message de demande d'autorisation, un CMTS valide l'identité du CM demandeur, détermine l'algorithme de cryptage et la base protocolaire qu'il partage avec le CM, DOIT activer une clé d'autorisation pour le CM, le code au moyen de la clé publique du CM et la lui renvoie dans un message de réponse d'autorisation qui comprend:

- une clé d'autorisation chiffrée par la clé publique du CM;
- un numéro de séquence de clé de 4 bits, permettant de différencier des générations successives de clés d'autorisation;
- une durée de vie de clé;
- les identités (c'est-à-dire les identificateurs SAID) et les propriétés de l'unique association de sécurité primaire et de zéro, une ou de plusieurs associations de sécurité statiques pour lesquelles le CM est autorisé à obtenir des informations de cryptage.

Si le CMTS prend en charge les associations SA statiques, la réponse d'autorisation au CM DOIT identifier l'association SA statique associée au CM en plus de l'association SA primaire dont l'identificateur SAID correspond à l'identificateur de meilleur effort du CM demandeur. La réponse d'autorisation NE DOIT PAS identifier d'associations SA dynamiques.

Le système CMTS déterminera, dans sa réponse à une demande d'autorisation de CM, si le câblo-modem demandeur, dont l'identité peut être vérifiée au moyen du certificat numérique X.509, est autorisé à recevoir les services unidiffusés de base. Il déterminera également les services préconfigurés statiquement (c'est-à-dire les identificateurs SAID statiques) auxquels l'utilisateur du câblo-modem s'est inscrit.

NOTE 1 – Les services protégés qu'un CMTS met à la disposition d'un CM client peuvent dépendre des suites cryptographiques particulières dont le CM et le CMTS partagent la prise en charge.

Dès qu'il obtient l'autorisation, un CM crée un automate à états de clés TEK particulier pour chacun des identificateurs SAID désignés dans le message de réponse d'autorisation. Chaque automate à états de clés TEK fonctionnant à l'intérieur du CM est chargé de gérer le matériel de calcul de clés associé à son identificateur SAID respectif. Les automates à états de clés TEK envoient périodiquement au CMTS des messages de demande de clé afin de demander un rafraîchissement

du matériel de calcul de clés pour leurs identificateurs SAID respectifs. Une demande de clé contient les éléments suivants:

- des informations d'identification uniques pour le câblo-modem, composées de l'identificateur du fabricant, du numéro de série, de l'adresse de gestion MAC et de la clé publique à codage RSA;
- de l'identificateur SAID dont le matériel de calcul de clés est en cours de demande;
- d'un résumé de message à cryptage HMAC, authentifiant la demande de clé.

Le système CMTS DOIT répondre à une demande de clé par un message de réponse de clé contenant le matériel de calcul de clés actif du CMTS pour un identificateur SAID spécifique, si le CMTS valide le résumé HMAC du message de demande de clé, l'identité du CM demandeur et l'identificateur SAID. Ce matériel de calcul de clés comprend les éléments suivants:

- la clé de cryptage de trafic à triple codage DES;
- le vecteur d'initialisation de concaténation CBC;
- un numéro de séquence de clé;
- la durée de vie restante de la clé;
- un message chiffré HMAC authentifiant la réponse de clé.

La clé de cryptage du trafic (TEK) contenue dans la réponse de clé est à triple codage DES (mode cryptage-déchiffrage-cryptage (EDE, *encrypt-decrypt-encrypt*)). Elle utilise une clé de cryptage de clé (KEK) à triple codage DES, calculée sur la clé d'autorisation.

NOTE 2 – A tout moment, le système CMTS conserve deux ensembles actifs de matériel de calcul de clés pour chaque identificateur SAID. Les durées de vie de ces deux générations se superposent de façon que chaque génération devienne active à la mi-vie de la génération précédente et arrive à expiration à la mi-vie de la génération suivante. Un système CMTS comporte, dans ses réponses de clé, *les deux* générations actives du matériel de calcul de clés d'un identificateur SAID.

La réponse de clé fournit au CM demandeur, en plus de la clé TEK et du vecteur d'initialisation de concaténation CBC, la durée de vie restante de chacun des deux ensembles de matériel de calcul de clés. Le CM récepteur utilise ces durées de vie restante pour estimer le moment où le CMTS invalidera une clé TEK particulière et donc le moment où il convient de programmer de futures demandes de clé de façon que le CM demande et reçoive un nouveau matériel de calcul de clés avant que le CMTS fasse expirer le matériel de calcul de clés actuellement détenu par le CM.

Le fonctionnement de programmation des demandes de clé par l'automate à états de clés TEK, combiné au système de mise à jour et d'utilisation du matériel de calcul de clés d'identificateur SAID dans le CMTS (voir § 9) garantit que le CM sera en mesure d'échanger continuellement avec le CMTS un trafic chiffré.

Un CM DOIT rafraîchir périodiquement sa clé d'autorisation en renvoyant au CMTS une demande d'autorisation. La réautorisation est identique à l'autorisation, sauf que le CM n'envoie pas de messages d'information d'authentification au cours des cycles de réautorisation. La description de l'automate à états d'autorisation dans le § 7.1.2 indique clairement le moment où les messages d'information d'authentification sont envoyés.

De façon à éviter des interruptions de service en cours de réautorisation, des générations successives des clés d'autorisation du CM ont des durées de vie en chevauchement. Aussi bien le CM que le CMTS DOIVENT être en mesure de prendre en charge jusqu'à deux clés d'autorisation simultanément actives au cours de ces périodes de transition. Le fonctionnement de l'algorithme de programmation des demandes d'autorisation par l'automate à états d'autorisation, combiné au système de mise à jour et d'utilisation des clés d'autorisation d'un CM client dans le CMTS (voir § 9) garantit que les CM seront en mesure de rafraîchir les informations de calcul de clé TEK sans interruption au cours des périodes de réautorisation de ce CM.

Un automate à états de clé TEK reste actif tant que:

– le CM est autorisé à fonctionner dans le domaine de sécurité du CMTS, c'est-à-dire qu'il possède une clé d'autorisation valide; *et*

– le CM est autorisé à participer à une association de sécurité particulière, c'est-à-dire que le CMTS continue à fournir du matériel de calcul de clés renouvelé au cours des cycles de réautorisation de clé.

L'automate à états d'autorisation supérieur arrête *tous* ses automates à états de clé TEK inférieurs lorsque le CM reçoit du CMTS un message de rejet d'autorisation au cours d'un cycle de réautorisation. Des automates à états de clé TEK individuels peuvent être lancés ou arrêtés au cours d'un cycle de réautorisation si les autorisations d'identificateur SAID statique d'un CM ont été modifiées entre réautorisations successives.

La communication entre automates à états d'autorisation et de clé TEK s'effectue par transmission de messages événementiels et protocolaires. L'automate à états d'autorisation produit des événements (c'est-à-dire arrêt, identificateur autorisé, autorisation en instance et autorisation effectuée) qui sont destinés à ses automates à états de clé TEK inférieurs. Les automates à états de clé TEK ne visent pas d'évènements sur l'automate à états d'autorisation supérieur. L'automate à états de clé TEK a une incidence indirecte sur l'automate à états d'autorisation par les messages qu'un système CMTS envoie en réponse aux demandes d'un modem: un CMTS PEUT répondre aux demandes de clé d'un automate TEK par un avis d'échec (c'est-à-dire par un message d'autorisation non valide) qui sera traité par l'automate à états d'autorisation.

7.1.1.1 Considérations préliminaires sur les associations de sécurité dynamiques et sur leur mappage

Le paragraphe 5 présentait les associations de sécurité dynamiques et indiquait comment un système CMTS peut établir ou éliminer une association de sécurité dynamique en réponse à la création ou à la fermeture de flux de trafic aval (par exemple, un trafic de groupe multidiffusé IP particulier). Afin qu'un CM exploite un automate à états de clé TEK de façon à obtenir le matériel de calcul de clés d'une association de sécurité dynamique, ce CM a besoin de connaître la valeur de l'identificateur SAID correspondant. Le CMTS ne prend cependant pas l'initiative de signaler aux CM clients l'existence d'associations SA dynamiques; il appartient en revanche aux CM de demander au système CMTS les mappages des identificateurs de flux de trafic (par exemple, une adresse multidiffusée en protocole IP) sur les identificateurs SAID dynamiques.

L'interface BPI+ définit un échange de messages permettant à un CM de connaître le mappage d'un flux de trafic aval sur une association de sécurité dynamique (tout le trafic amont étant chiffré selon une association de sécurité primaire de CM). Un automate à états de mappage d'association de sécurité spécifie la façon dont les câblo-modems gèrent la transmission de ces messages de demande de mappage. Actuellement, seuls les services DOCSIS de gestion multidiffusés en protocole IP utilisent ce mécanisme. D'autres services pourront ultérieurement utiliser des associations de sécurité dynamiques à l'interface BPI+.

L'automate à états d'autorisation commande l'ouverture et la fermeture d'automates à états de clé TEK associés aux associations de sécurité primaire et éventuellement statiques. Il ne commande cependant pas l'ouverture et la fermeture d'automates à états de clé TEK rattachés à des associations de sécurité dynamiques. Les CM DOIVENT implémenter les circuits logiques nécessaires pour ouvrir et fermer un automate à états de clé TEK d'association SA dynamique. La présente Recommandation d'interface ne spécifie cependant pas la façon dont il convient que les CM gèrent leurs automates à états de clé TEK d'association SA dynamique.

Une description complète du modèle à états de mappage d'une association de sécurité sera donnée dans le § 8.

7.1.1.2 Sélection des capacités de sécurité

Dans le cadre de leur échange de messages d'autorisation à l'interface BPI+, le CM fournit au CMTS une liste de toutes les suites cryptographiques (ou paires d'algorithmes de cryptage de données et d'authentification de données) prises en charge par le CM. Le CMTS choisit dans cette liste une seule suite cryptographique, qu'il utilisera avec l'association de sécurité primaire du CM demandeur. La réponse d'autorisation renvoyée au CM par le CMTS contient un descripteur d'association de sécurité primaire qui, entre autres, désigne la suite cryptographique que le CMTS a choisi d'utiliser pour l'association de sécurité primaire du CM. Un système CMTS DOIT ignorer la demande d'autorisation s'il détermine qu'aucune des suites cryptographiques offertes n'est satisfaisante.

La réponse d'autorisation contient également une liste facultative de descripteurs d'association de sécurité statique, dont chacun désigne la suite cryptographique utilisée dans l'association SA. Le choix d'une suite cryptographique d'association SA est normalement rendu indépendant des capacités cryptographiques du CM demandeur. Un CMTS PEUT inclure dans sa réponse d'autorisation des descripteurs d'association SA statique désignant des suites cryptographiques que le CM demandeur ne prend pas en charge. Si c'est le cas, le CM NE DOIT PAS ouvrir d'automates à états de clé TEK pour des associations de sécurité statiques dont les suites cryptographiques ne sont pas prises en charge par le CM.

Le cadre de sélection ci-dessus a été incorporé dans l'interface BPI+ afin de prendre en charge de futures améliorations du matériel DOCSIS et du protocole BPI+. Au moment de la parution de la présente Recommandation, les seuls algorithmes de cryptage de données en paquet pris en charge étaient la norme DES à 56 bits et la norme DES à 40 bits, aucun des deux n'étant apparié à un algorithme d'authentification de données en paquet.

7.1.2 Automate à états d'autorisation

L'automate à états d'autorisation se compose de six états et de huit événements distincts (y compris la réception de messages) qui peuvent déclencher des transitions d'état. L'automate à états finis (FSM, *finite state machine*) d'autorisation est présenté ci-dessous sous la forme graphique d'un organigramme d'états (Figure 7-1) et sous la forme tabulaire d'une matrice de transition d'états (Tableau 7-1).

L'organigramme décrit les messages de protocole transmis et les événements internes produits pour chaque transition d'état du modèle. Ce diagramme n'indique cependant pas les actions internes supplémentaires comme la réinitialisation ou l'armement de temporisateurs, qui accompagnent les transitions d'état spécifiques. Une description détaillée des actions spécifiques qui correspondent à chaque transition d'état est ajoutée à la matrice de transition d'états, laquelle DOIT être utilisée en tant que spécification définitive des actions protocolaires associées à chaque transition d'état.

Les légendes ci-après s'appliquent à l'organigramme de l'automate à états d'autorisation décrit par la Figure 7-1:

- les ovales sont des états;
- les événements sont écrits en caractères *italiques*;
- les messages sont en caractères normaux;
- les transitions d'état (c'est-à-dire les lignes qui joignent les états) sont indiquées par <ce qui provoque la transition>/<les messages et événements déclenchés par la transition>. Par exemple, l'expression "*expiration de la temporisation*/demande d'aut." signifie que l'état a reçu un événement "d'expiration de temporisation" et a envoyé un message de demande d'autorisation ("demande d'aut."). S'il y a plusieurs événements ou messages séparés par une virgule avant la barre oblique "/", *l'un quelconque* d'entre eux peut provoquer une transition. S'il y a plusieurs événements ou messages énumérés après la barre oblique, *la totalité* des actions spécifiées doit accompagner la transition.

La matrice de transition d'états d'autorisation présentée dans le Tableau 7-1 énumère les six états d'automate d'autorisation dans la rangée supérieure et les huit événements d'automate d'autorisation (y compris les réceptions de message) dans la colonne de gauche. Toute cellule contenue dans cette matrice représente une combinaison spécifique d'état et d'événement, l'événement suivant (celui vers lequel la transition a été effectuée) étant indiqué dans la cellule. Par exemple, la cellule 4-B représente la réception d'un message de réponse d'autorisation ("réponse d'aut.") lorsque l'automate est dans l'état d'attente d'autorisation ("attente d'aut."). La cellule 4-B contient le nom de l'état suivant: "autorisé". Ainsi, lorsqu'un automate à états d'autorisation de CM se trouve dans l'état d'attente d'autorisation et qu'un message de réponse d'autorisation est reçu, cet automate à états passe à l'état "autorisé". En liaison avec cette transition d'état, plusieurs actions protocolaires doivent être exécutées. Elles sont décrites dans la liste des actions protocolaires, dans la cellule 4-B du § 7.1.2.5.

Une cellule ombrée dans la matrice de transition d'états implique que l'événement spécifique ne peut pas ou ne devrait pas se produire dans cet état et que l'automate à états DOIT le négliger s'il se produit. Par exemple, si un message de réponse d'autorisation arrive pendant l'état "autorisé", il y a lieu que ce message soit négligé (cellule 4-C). Le CM PEUT cependant, en réponse à un événement inapproprié, enregistrer l'apparition de celui-ci, produire un événement de protocole SNMP ou prendre une autre mesure définie par le vendeur. Ces actions ne sont cependant pas spécifiées dans le contexte de l'automate à états d'autorisation, qui se borne à ne pas tenir compte des événements inappropriés.

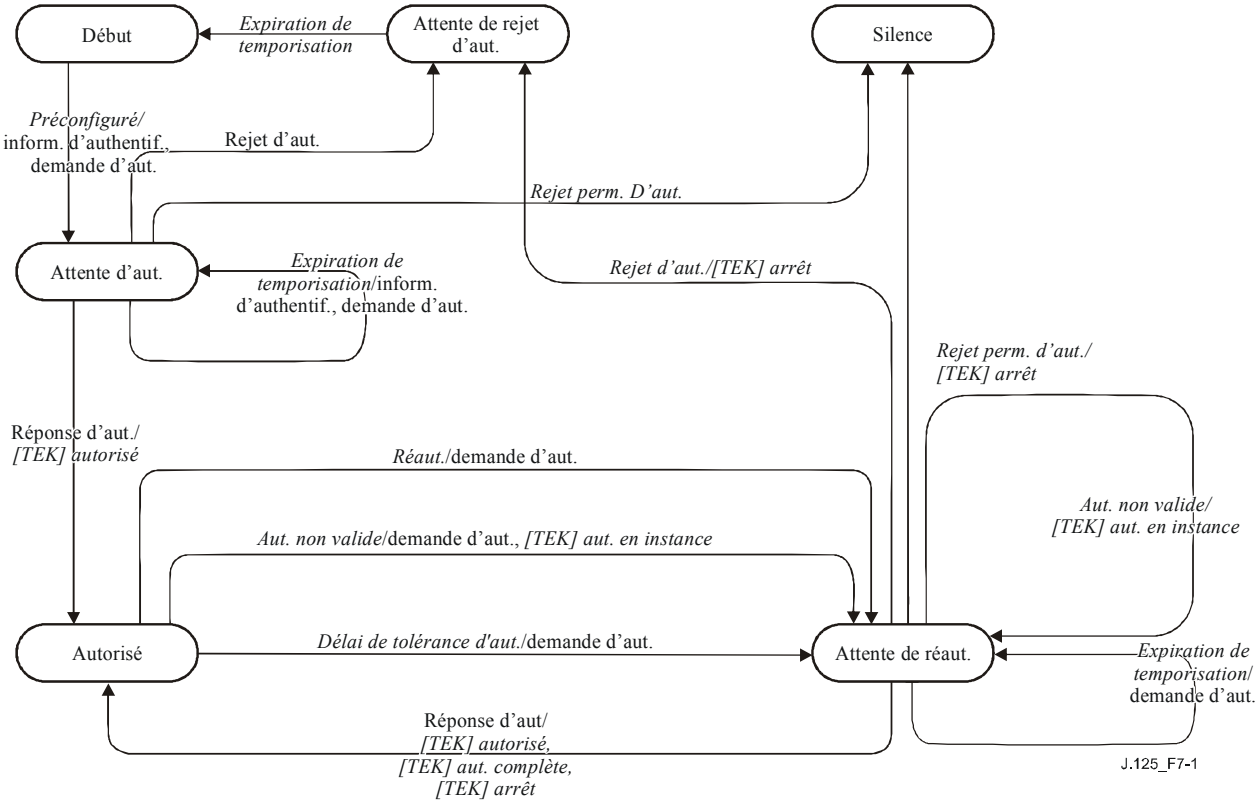


Figure 7-1/J.125 – Organigramme de l'automate à états d'autorisation

Tableau 7-1/J.125 – Matrice de transition d'état de l'automate d'autorisation

Etat / *Evénement ou message reçu*	(A) Début	(B) Attente d'aut.	(C) Autorisé	(D) Attente de réaut.	(E) Attente de rejet d'aut.	(F) Silence
(1) *Préconfiguré*	Att. d'aut.					
(2) *Rejet d'aut.*		Att. de rejet d'aut.		Att. de rejet d'aut.		
(3) *Rejet d'aut. perm.*		Silence		Silence		
(4) *Réponse d'aut.*		Autorisé		Autorisé		
(5) *Temporisation*		Att. d'aut.		Att. de réaut.	Début	
(6) *Délai de tolérance d'aut.*			Att. de réaut.			
(7) *Aut. non valide*			Att. de réaut.	Att. de réaut.		
(8) *Réaut.*			Att. de réaut.			

7.1.2.1 Etats

7.1.2.1.1 Début

Il s'agit de l'état initial de l'automate FSM, auquel aucune ressource n'est attribuée ou qui n'en utilise aucune dans cet état, par exemple, lorsque tous les temporisateurs sont désarmés et qu'aucun traitement n'est programmé.

7.1.2.1.2 Attente d'autorisation (att. d'aut.)

Le CM a reçu l'événement "Préconfiguré" indiquant qu'il a effectué l'inscription MAC à l'interface RF avec le CMTS. En réponse à la réception de cet événement, le CM a envoyé au CMTS aussi bien un message d'information d'authentification qu'un message de demande d'autorisation et il en attend la réponse.

7.1.2.1.3 Autorisé

Le CM a reçu un message de réponse d'autorisation contenant une liste d'identificateurs SAID valides pour ce CM. A ce point, le modem possède une clé d'autorisation valide et une liste d'identificateurs SAID. La transition vers cet état déclenche la création d'un unique automate FSM de clé TEK pour chacun des identificateurs SAID à confidentialité activée dans le CM.

7.1.2.1.4 Attente de réautorisation (att. de réaut.)

Le CM a émis une demande de réautorisation qui est en instance. Soit le CM est sur le point d'épuiser le délai imparti à son autorisation actuelle soit il a reçu l'indication (sous la forme d'un message d'autorisation non valide en provenance du CMTS) que son autorisation n'est plus valide. Le CM a envoyé un message de demande d'autorisation au CMTS et en attend une réponse.

7.1.2.1.5 Attente de rejet d'autorisation (att. de rejet d'aut.)

Le CM a reçu un message de rejet d'autorisation en réponse à sa dernière demande d'autorisation. Le code d'erreur de ce rejet d'autorisation indiquait que l'erreur n'était pas de nature permanente. En réponse à la réception de ce message de rejet, le CM a armé un temporisateur et est passé à l'état

d'attente de rejet d'autorisation. Il reste dans cet état jusqu'à ce que le temporisateur arrive à expiration.

7.1.2.1.6 Silence

Le CM a reçu un message de rejet d'autorisation en réponse à sa dernière demande d'autorisation. Le code d'erreur de ce rejet d'autorisation indiquait que l'erreur était de nature permanente, ce qui a déclenché une transition vers l'état de silence, dans lequel le CM NE DOIT PAS retransmettre le trafic de l'équipement CPE mais DOIT être en mesure de répondre à des demandes de gestion SNMP provenant de tout le réseau en câble. Le CMTS PEUT choisir de transférer le trafic de données vers un CM qui à l'état de silence non chiffré, ou le CMTS PEUT bloquer un tel trafic.

7.1.2.2 Messages

Les formats des messages sont définis en détail au § 7.2.

7.1.2.2.1 Demande d'autorisation (demande d'aut.)

Ce message demande une clé d'autorisation et une liste d'identificateurs SAID autorisés. Il est envoyé du CM au CMTS.

7.1.2.2.2 Réponse d'autorisation (réponse d'aut.)

Le CM reçoit une clé d'autorisation et une liste d'identificateurs SAID autorisés et statiques. Ce message est envoyé par le CMTS au CM. La clé d'autorisation est chiffrée par la clé publique du CM.

7.1.2.2.3 Rejet d'autorisation (rejet d'aut.)

La demande d'autorisation a été rejetée après avoir été envoyée par le CMTS au CM.

7.1.2.2.4 Autorisation non valide (aut. non valide)

Le système CMTS peut envoyer à un CM client un message d'autorisation non valide sous la forme:

- soit d'une indication non sollicitée; *ou*
- soit d'une réponse à un message reçu de ce CM.

Dans un cas comme dans l'autre, le message d'autorisation non valide demande au CM récepteur de renouveler son autorisation auprès de son système CMTS.

Le CMTS doit répondre à une demande de clé par un message d'autorisation non valide si:

1) le CMTS ne reconnaît pas le CM comme étant autorisé (c'est-à-dire qu'aucune clé d'autorisation valide n'est associée au CM);
2) la vérification du résumé de message chiffré contenu dans la demande de clé (dans l'attribut de résumé HMAC) a échoué.

NOTE – L'événement d'autorisation non valide, indiqué en référence aussi bien dans l'organigramme d'états que dans la matrice de transition d'états, signifie soit la réception d'un message d'autorisation non valide soit l'apparition d'un événement endogène.

7.1.2.2.5 Informations d'authentification (inform. d'authentif.)

Le message d'informations d'authentification contient le certificat X.509 du fabricant du CM, fourni par DOCSIS. Ce message, d'ordre strictement informatif, est envoyé par le CM au CMTS, ce qui PERMET à ce dernier de s'informer dynamiquement du certificat de fabrication des câblo-modems clients. En variante, un CMTS PEUT exiger la configuration hors bande de sa liste de certificats de fabrication.

7.1.2.3 Evénements

7.1.2.3.1 Préconfiguré

L'automate à états d'autorisation produit cet événement dès qu'il entre dans l'état de début si la gestion MAC à l'interface RF a effectué l'initialisation, c'est-à-dire l'inscription auprès du CMTS. Si l'initialisation MAC RF n'est pas effectuée, le CM envoie un événement de type "Préconfiguré" à l'automate FSM d'autorisation après avoir effectué l'inscription auprès du CMTS. L'événement "Préconfiguré" déclenche dans le CM le début du processus d'obtention de sa clé d'autorisation et de ses clés TEK.

7.1.2.3.2 Temporisation

Fin de la temporisation d'une retransmission ou d'une attente. Une demande est généralement réémise.

7.1.2.3.3 Délai de tolérance (délai de tolérance d'aut.)

Expiration de la temporisation de tolérance pour l'autorisation. Ce temporisateur arme une durée configurable (le délai de tolérance d'autorisation) avant que l'autorisation actuelle soit censée expirer, afin de signaler au CM qu'il doit effectuer une réautorisation avant que son autorisation actuelle expire. Le délai de tolérance d'autorisation est spécifié dans un réglage de configuration contenu dans le fichier paramétrique téléchargé par protocole TFTP.

7.1.2.3.4 Réautorisation (réaut.)

L'ensemble d'identificateurs statiques SAID autorisés du CM peut avoir changé. Cet événement est produit en réponse à un ensemble SNMP, [DOCSIS8], destiné à déclencher un cycle de réautorisation.

7.1.2.3.5 Autorisation non valide (aut. non valide)

Cet événement peut être endogène dans le CM lors d'un échec d'authentification d'un message de réponse de clé, de rejet de clé ou de clé TEK non valide. Il peut également être exogène à la suite de la réception d'un message d'autorisation non valide, envoyé au CM par le CMTS. Celui-ci répond à une demande de clé par un message d'autorisation non valide en cas d'échec de la vérification du code d'authentification du message de demande. Les deux cas indiquent que le CMTS et le CM ont perdu le synchronisme de clé d'autorisation.

Un système CMTS PEUT également envoyer à un CM un message non sollicité d'autorisation non valide, forçant un événement d'autorisation non valide.

7.1.2.3.6 Rejet d'autorisation permanent (rejet d'aut. perm.)

Le CMTS doit envoyer un message de rejet d'autorisation permanent avec le code d'erreur 6 (rejet d'autorisation permanent) en réponse à un message de demande d'autorisation dans l'un des cas suivants:

- échec lors de la validation du certificat du CM en fonction du § 12.4.2 (ce qui signifie que le certificat du CM est noté comme étant non valide);
- capacités de sécurité incompatibles.

Le document OSS [DOCSIS8] associé à l'interface BPI+ fournit une description de l'objet MIB de base du CMTS, qui commande les décisions que prend un CMTS dans le cas où l'une des conditions d'erreurs citées ci-dessus se produit.

Lorsqu'un CM reçoit un rejet d'autorisation indiquant une condition d'erreur permanente, l'automate à états d'autorisation passe à l'état de silence. Les CM DOIVENT émettre un événement DOCSIS dès qu'ils entrent dans l'état de silence.

7.1.2.3.7 Rejet d'autorisation (rejet d'aut.)

Le CM reçoit un message de rejet d'autorisation en réponse à une demande d'autorisation. Le code d'erreur contenu dans le rejet d'autorisation n'indique pas que la défaillance est due à un état d'erreur permanente. En conséquence, l'automate à états d'autorisation arme un temporisateur d'attente et passe à l'état d'attente de rejet d'autorisation. Le CM reste dans cet état jusqu'à l'expiration du temporisateur et envoie alors une demande de réautorisation.

NOTE – Les événements suivants sont envoyés par un automate à états d'autorisation à l'automate à états de clé TEK.

7.1.2.3.8 [TEK] Arrêt

Evénement envoyé par l'automate FSM d'autorisation à un automate FSM de clé TEK actif (ne se trouvant pas dans l'état début) afin de supprimer cet automate FSM ainsi que le matériel de calcul de clés d'identificateur SAID correspondant, figurant dans la table des clés du CM.

7.1.2.3.9 [TEK] Autorisé

Evénement envoyé par l'automate FSM d'autorisation à un automate FSM de clé TEK non actif (état début) mais valide.

7.1.2.3.10 [TEK] Autorisation en instance (aut. en instance)

Evénement envoyé par l'automate FSM d'autorisation à un automate FSM de clé TEK spécifique afin de mettre cet automate en état d'attente jusqu'à que l'automate FSM d'autorisation ait pu terminer son opération de réautorisation.

7.1.2.3.11 [TEK] Autorisation complète (aut. complète)

Evénement envoyé par l'automate FSM d'autorisation à un automate FSM de clé TEK dans les états d'attente de réautorisation opérationnelle (att. de réaut. opér.) ou d'attente de réautorisation de renouvellement de clé (att. de réaut. de renouv. de clé) afin de libérer l'état d'attente déclenché par un événement d'autorisation en instance dans l'automate FSM de clé TEK.

7.1.2.4 Paramètres

Toutes les valeurs des paramètres de configuration sont spécifiées dans le fichier paramétrique téléchargé par protocole TFTP (voir Annexe A: extensions du fichier de configuration TFTP).

7.1.2.4.1 Temporisation d'attente d'autorisation (temporisation d'att. d'aut.)

Période de temporisation s'écoulant entre l'envoi des messages de demande d'autorisation et l'état d'attente d'autorisation. Voir § A.1.1.1.1.

7.1.2.4.2 Temporisation d'attente de réautorisation (temporisation d'att. de réaut.)

Période de temporisation s'écoulant entre l'envoi du message de demande d'autorisation et l'état d'attente de réautorisation. Voir § A.1.1.1.2.

7.1.2.4.3 Délai de tolérance d'autorisation (délai de tolérance d'aut.)

Durée s'écoulant avant l'expiration d'autorisation programmée, pendant laquelle le CM commence une réautorisation. Voir § A.1.1.1.3.

7.1.2.4.4 Temporisation d'attente de rejet d'autorisation (temporisation d'att. de rejet d'aut.)

Durée pendant laquelle un automate FSM d'autorisation de CM reste dans l'état d'attente de rejet d'autorisation avant de passer à l'état de Début. Voir § A.1.1.1.7.

7.1.2.5 Actions

Les actions effectuées en association avec les transitions d'état sont énumérées ci-dessous par l'expression <état> (<événement message reçu>) → <état>:

1-A Début (*préconfiguré*) → Att. d'aut.

- envoi au CMTS du message d'information d'authentification;
- envoi au CMTS du message de demande d'autorisation;
- armement du temporisateur de nouvelle demande d'autorisation en temporisation d'att. d'autorisation.

2-B Att. d'aut. (*rejet d'aut.*) → Attente de rejet d'aut.

- réinitialisation du temporisateur de nouvelle demande d'autorisation;
- armement d'un temporisateur d'attente en temporisation d'attente de rejet d'autorisation.

2-D Att. de réaut. (*rejet d'aut.*) → Attente de rejet d'aut.

- réinitialisation du temporisateur de nouvelle demande d'autorisation;
- production d'événements d'arrêt d'automate FSM de clé TEK pour tous les automates à états de clé TEK actifs;
- armement d'un temporisateur d'attente en temporisation d'attente de rejet d'autorisation.

3-B Att. d'aut. (*rejet perm. d'aut.*) → Silence

- réinitialisation du temporisateur de nouvelle demande d'autorisation;
- désactivation de toute retransmission de trafic CPE.

3-D Att. de réaut. (*rejet perm. d'aut.*) → Silence

- réinitialisation du temporisateur de nouvelle demande d'autorisation;
- production d'événement d'arrêt d'automate FSM de clé TEK pour tous les automates à états de clé TEK actifs;
- désactivation de toute retransmission de trafic CPE.

4-B Att. d'aut. (*réponse d'aut.*) → Autorisé

- réinitialisation du temporisateur de nouvelle demande d'autorisation;
- décryptage et enregistrement de la clé d'autorisation fournie avec la réponse d'autorisation;
- début des automates FSM de clé TEK pour tous les identificateurs SAID énumérés dans la réponse d'autorisation (à condition que le CM prenne en charge la suite cryptographique qui est associée à chaque identificateur SAID) et envoi d'un événement d'automate FSM de TEK autorisé à chacun des nouveaux automates FSM de clé TEK;
- armement du temporisateur de délai de tolérance d'autorisation de façon à agir au bout du nombre de secondes du "délai de tolérance d'autorisation" avant l'expiration programmée de la clé d'autorisation fournie.

4-D Att. de réaut. (*réponse d'aut.*) → Autorisé

- réinitialisation du temporisateur de nouvelle demande d'autorisation;
- décryptage et enregistrement de la clé d'autorisation fournie avec la réponse d'autorisation;
- début des automates FSM de clé TEK pour tous les identificateurs SAID récemment autorisés pouvant être énumérés dans la réponse d'autorisation (à condition que le CM prenne en charge la suite cryptographique qui est associée à chaque identificateur SAID) et envoi d'un événement d'automate FSM de TEK Autorisé à chacun des nouveaux automates FSM de clé TEK;
- production d'événements d'autorisation complète d'automate FSM de clé TEK pour tous les automates FSM de clé TEK éventuellement actifs, dont les identificateurs SAID correspondants étaient énumérés dans la réponse d'autorisation;

- production d'événements d'arrêt d'automate FSM de clé TEK pour tous les automates FSM de clé TEK éventuellement actifs, dont les identificateurs SAID correspondants n'étaient pas énumérés dans la réponse d'autorisation;
- armement du temporisateur de délai de tolérance d'autorisation de façon à agir au bout du nombre de secondes du "délai de tolérance d'autorisation" avant l'expiration programmée de la clé d'autorisation fournie.

5-B Att. d'aut. (*temporisation*) → Attente d'aut.

- envoi au CMTS du message d'information d'authentification;
- envoi au CMTS du message de demande d'autorisation;
- armement du temporisateur de nouvelle demande d'autorisation en temporisation d'attente d'autorisation.

5-D Att. de réaut. (*temporisation*) → Attente de réaut.

- envoi au CMTS du message de demande d'autorisation;
- armement du temporisateur de nouvelle demande d'autorisation en temporisation d'attente de réautorisation.

5-E Att. de rejet d'aut. (*temporisation*) → Début

- aucune action protocolaire n'est associée à la transition d'état.

6-C Autorisé (*délai de tolérance d'aut.*) → Att. de réaut.

- envoi au CMTS du message de demande d'autorisation;
- armement du temporisateur de nouvelle demande d'autorisation en temporisation d'attente de réautorisation.

7-C Autorisé (*aut. non valide*) → Att. de réaut.

- réinitialisation du temporisateur de délai d'autorisation;
- envoi au CMTS du message de demande d'autorisation;
- armement du temporisateur de nouvelle demande d'autorisation en temporisation d'attente de réautorisation;
- si l'événement d'autorisation non valide est associé à un automate FSM de clé TEK particulier, production d'un événement d'autorisation en instance d'automate FSM de clé TEK pour l'automate à états de clé TEK responsable de l'événement d'autorisation non valide (c'est-à-dire l'automate FSM de clé TEK qui soit a produit l'événement soit a envoyé le message de demande de clé auquel le CMTS a répondu par un message d'autorisation non valide).

7-D Att. de réaut. (*Aut. non valide*) → Att. de réaut.

- si l'événement d'autorisation non valide est associé à un automate FSM de clé TEK particulier, production d'un événement d'autorisation en instance d'automate FSM de clé TEK pour l'automate à états de clé TEK responsable de l'événement d'autorisation non valide (c'est-à-dire l'automate FSM de clé TEK qui soit a produit l'événement soit a envoyé le message de demande de clé auquel le CMTS a répondu par un message d'autorisation non valide).

8-C Autorisé (*réaut.*) → Att. de réaut.

- réinitialisation du temporisateur de délai d'autorisation;
- envoi au CMTS du message de demande d'autorisation;
- armement du temporisateur de nouvelle demande d'autorisation en temporisation d'attente de réautorisation.

7.1.3 Automate à états de clé TEK

L'automate à états de clé TEK se compose de six états et de neuf événements (y compris la réception de messages) qui peuvent déclencher des transitions d'état. Comme l'automate à états d'autorisation, l'automate à états de clé TEK sera présenté aussi bien sous la forme d'un organigramme d'états que sous celle d'une matrice de transition d'état. Comme dans le cas de l'automate à états d'autorisation, la matrice de transition d'état DOIT être utilisée en tant que spécification définitive des actions protocolaires associées à chaque transition d'état.

Les états ombrés sur la Figure 7-2 (opérationnel, attente de renouvellement de clé et attente de réautorisation de renouvellement de clé) possèdent un matériel de calcul de clés valide et le trafic chiffré peut être retransmis.

L'automate d'autorisation démarre un automate de clé TEK indépendant pour chacun de ses SAID autorisés.

Comme déjà mentionné au § 7.1.1, le système CMTS entretient deux clés TEK actives pour chaque identificateur SAID. Le CMTS inclut dans ses réponses de clé ces deux clés TEK, avec leur durée de vie restante. Le CMTS chiffre le trafic aval avec la plus ancienne de ses deux clés TEK et déchiffre le trafic amont avec l'ancienne ou la nouvelle clé TEK, selon celle des deux que le CM est alors en train d'utiliser. Le CM chiffre le trafic amont au moyen de la plus récente de ses deux clés TEK et déchiffre le trafic aval avec l'ancienne ou la nouvelle clé TEK, selon celle des deux que le CMTS est alors en train d'utiliser. Voir au § 9 des détails sur les exigences du CM et du CMTS en termes d'utilisation de clés.

Grâce au fonctionnement d'un automate à états de clé TEK, le CM essaye de garder ses copies de clés TEK d'identificateur SAID en synchronisme avec celles de son système CMTS. Un automate à états de clé TEK émet des demandes de clé afin de rafraîchir les copies de son matériel de calcul de clés d'identificateur SAID dès l'expiration programmée de la plus ancienne de ses deux clés TEK et avant l'expiration de sa plus récente clé TEK. Afin de tenir compte de la dérive d'horloge entre CM et CMTS et du traitement dans d'autres systèmes ainsi que des temps de transmission, le CM programme ses demandes de clé avec un nombre configurable de secondes avant l'expiration estimée de la clé TEK la plus récente dans le système CMTS. A la réception de la réponse de clé, le CM DOIT mettre à jour ses enregistrements avec les paramètres de clé TEK issus des deux clés TEK contenues dans le message de réponse de clé. La Figure 9-2 décrit la programmation par le CM de ses rafraîchissements de clé en liaison avec sa gestion de clés TEK actives dans une association de sécurité de l'interface BPI+.

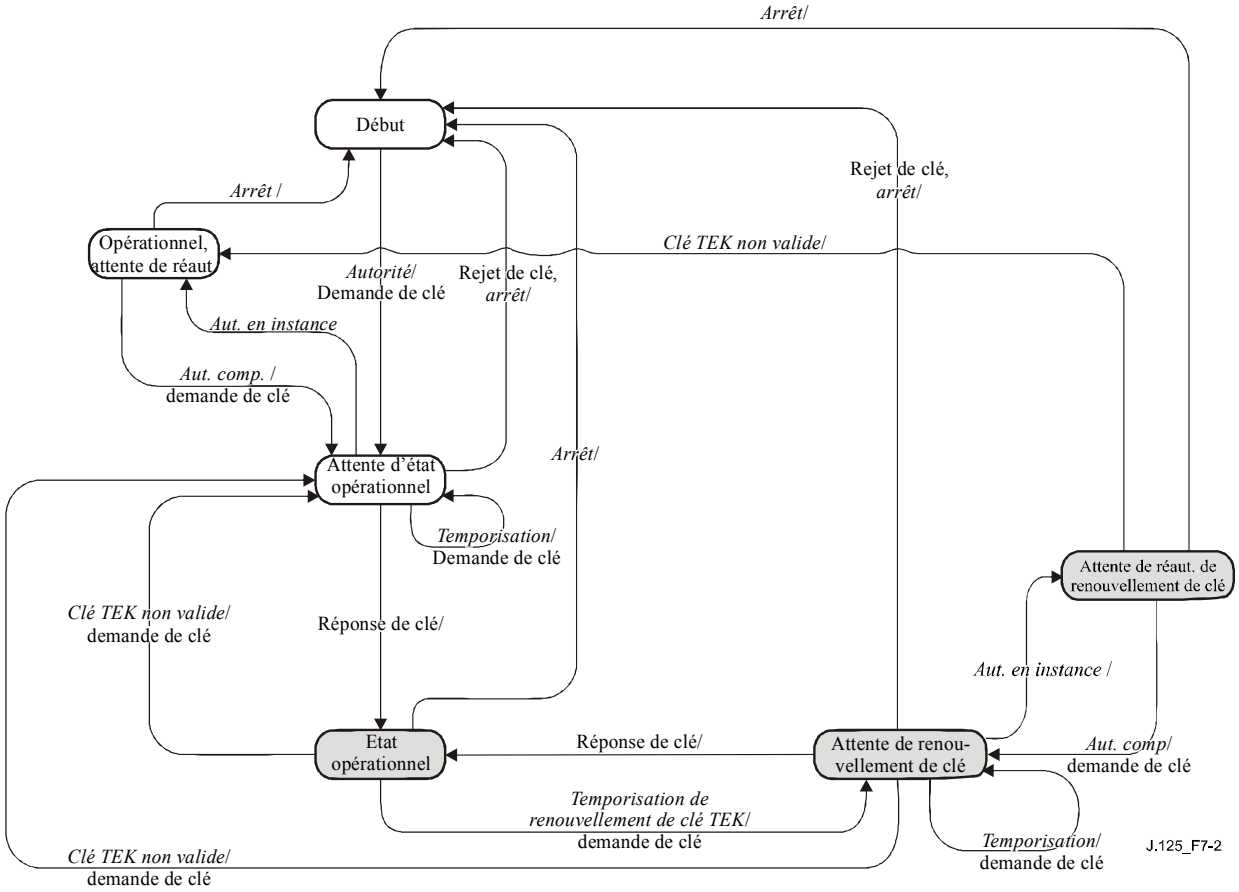


Figure 7-2/J.125 – Organigramme de l'automate à états de clé TEK

Tableau 7-2/J.125 – Matrice de transition de l'automate FSM à états TEK

Etat / ***Evénement ou message reçu***	**(A) Début**	**(B) Attente d'état opér.**	**(C) Opér., Att. de réaut.**	**(D) Opération**	**(E) Attente de renouvel-lement de clé**	**(F) Attente de réaut. de renouv. de clé**
(1) *Arrêt*		Début	Début	Début	Début	Début
(2) *Autorisé*	Attente d'état opér.					
(3) *Aut. en instance*		Opér., Att. de réaut.			Att. de réaut. de renouv. de clé	
(4) *Aut. compl.*			Attente d'état opér.			Attente de renouv. de clé
(5) *Clé TEK non valide*				Attente d'état opér.	Attente d'état opér.	Opér., Att. de réaut.

Tableau 7-2/J.125 – Matrice de transition de l'automate FSM à états TEK

Etat / *Evénement ou message reçu*	**(A) Début**	**(B) Attente d'état opér.**	**(C) Opér., Att. de réaut.**	**(D) Opération**	**(E) Attente de renouvel-lement de clé**	**(F) Attente de réaut. de renouv. de clé**
(6) *Fin de temporisation*		Attente d'état opér.			Attente de renouv. de clé	
(7) *Temporisation de renouv. de clé TEK*				Attente de renouv. de clé		
(8) *Réponse de clé*		Opérationnel			Opérationnel	
(9) *Rejet de clé*		Début			Début	

7.1.3.1 Etats

7.1.3.1.1 Début

C'est l'état initial de l'automate FSM, auquel aucune ressource n'est attribuée et qui n'en utilise aucune: par exemple, tous les temporisateurs sont désarmés et aucun traitement n'est programmé.

7.1.3.1.2 Attente d'état opérationnel (att. d'état op.)

L'automate à états de clé TEK a envoyé sa demande initiale (demande de clé) concernant son matériel de calcul de clés d'identificateur SAID (clé de cryptage de trafic et vecteur d'initialisation CBC). Il attend une réponse du système CMTS.

7.1.3.1.3 Opérationnel, attente de réautorisation (op., att. de réaut.)

Etat d'attente dans lequel l'automate à états de clé TEK est placé s'il ne possède pas de matériel de calcul de clés d'identificateur valide pendant que l'automate à états d'autorisation se trouve au milieu d'un cycle de réautorisation.

7.1.3.1.4 Opérationnel

Le CM possède un matériel de calcul de clés valide pour l'identificateur SAID associé.

7.1.3.1.5 Attente de renouvellement de clé

Le temporisateur de renouvellement de clé TEK a expiré et le CM a demandé une mise à jour de clé pour l'identificateur SAID considéré.

NOTE – La plus récente de ses deux clés TEK n'a pas expiré et peut toujours être utilisée pour le cryptage comme pour le décryptage du trafic de données.

7.1.3.1.6 Attente de réautorisation de renouvellement de clé (att. de réaut. de renouv. de clé)

Etat d'attente dans lequel est placé l'automate à états de clé TEK si celui-ci possède un matériel de calcul de clés de trafic valide ainsi qu'une demande en instance pour le plus récent matériel de calcul de clés, et si l'automate à états d'autorisation lance un cycle de réautorisation.

7.1.3.2 Messages

Les formats des messages sont définis en détail au § 7.2.

7.1.3.2.1 Demande de clé

Ce message demande une clé TEK pour l'identificateur SAID considéré. Il est envoyé par le CM au CMTS et authentifié par un résumé de message chiffré. La clé d'authentification de message est calculée sur la clé d'autorisation.

7.1.3.2.2 Réponse de clé

Réponse du système CMTS acheminant les deux ensembles actifs de matériel de calcul de clés de trafic pour l'identificateur SAID considéré. Ce message est envoyé par le CMTS au CM. Il contient les clés de cryptage du trafic d'un identificateur SAID, à triple cryptage DES avec calcul de clé sur la clé d'autorisation. Le message de réponse de clé est authentifié par un résumé de message chiffré. La clé d'authentification est calculée sur la clé d'autorisation.

7.1.3.2.3 Rejet de clé

Le CMTS DOIT envoyer un message de rejet de clé au CM en réponse au message de demande de clé afin d'indiquer qu'aucune clé ne sera envoyée si l'identificateur SAID du message de demande de clé n'est plus valide. Le message de rejet de clé est authentifié par un résumé de message chiffré. La clé d'authentification est calculée sur la clé d'autorisation.

7.1.3.2.4 Clé TEK non valide

Le CMTS DOIT envoyer ce message au CM s'il détermine que celui-ci a chiffré une unité PDU de données en paquet amont avec une clé TEK non valide, c'est-à-dire qu'un numéro de séquence de clé TEK d'identificateur SAID, contenu dans l'élément d'en-tête étendu de confidentialité de base du paquet reçu, se trouve en dehors de l'étendue des numéros de séquence connus du CMTS et valides pour cet identificateur SAID.

7.1.3.3 Evénements

7.1.3.3.1 Arrêt

Cet événement est envoyé par l'automate FSM d'autorisation à un automate FSM actif (ne se trouvant pas dans l'état de début) afin de mettre fin à un automate FSM de clé TEK et de supprimer le matériel de calcul de clés d'identificateur SAID correspondant dans la table de clés du CM. Voir § 7.1.2.3.8.

7.1.3.3.2 Autorisé

Cet événement est envoyé par l'automate FSM d'autorisation à un automate FSM de clé TEK (dans l'état de début) afin d'indiquer à celui-ci l'attribution de l'autorisation. Voir § 7.1.2.3.9.

7.1.3.3.3 Autorisation en instance (aut. en instance)

Cet événement est envoyé par l'automate FSM d'autorisation à l'automate FSM de clé TEK afin de placer ce dernier en état d'attente pendant que l'automate FSM d'autorisation effectue le renouvellement d'autorisation. Voir § 7.1.2.3.10.

7.1.3.3.4 Autorisation complète (aut. compl.)

Cet événement est envoyé par l'automate FSM d'autorisation à un automate FSM de clé TEK dans les états d'attente de réautorisation opérationnelle ou d'attente de réautorisation de renouvellement de clé afin de libérer l'état d'attente engagé par le précédent événement d'autorisation en instance. Voir § 7.1.2.3.11.

7.1.3.3.5 Clé TEK non valide

Cet événement peut être déclenché soit par une logique de déchiffrage de paquet de données de CM soit par la réception d'un message de clé TEK non valide issu du système CMTS.

Une logique de déchiffrage de paquet de données de CM déclenche un événement de clé TEK non valide si le CM détecte une perte de synchronisme de clé TEK entre lui-même et le système CMTS chiffrant. C'est-à-dire qu'un numéro de séquence de clé TEK d'identificateur SAID, contenu dans l'élément d'en-tête étendu de confidentialité de base d'un paquet aval, est en dehors de l'étendue des numéros de séquence connus du CM pour cet identificateur SAID.

Un CMTS envoie à un CM un message de clé TEK non valide, qui déclenche dans le CM un événement de clé TEK non valide, si la logique de déchiffrage du CMTS détecte une perte du synchronisme de clé TEK entre lui-même et le CM.

7.1.3.3.6 Temporisation

Expiration d'une temporisation de réessai. La demande particulière est généralement réémise.

7.1.3.3.7 Temporisation de renouvellement de clé TEK

Evénement d'expiration de la temporisation de renouvellement de clé TEK, qui signale à l'automate à états de clé TEK qu'il y a lieu d'émettre une nouvelle demande de clé afin de renouveler son matériel de calcul de clés. Le temporisateur de renouvellement est réglé de façon à appliquer une durée configurable (délai de tolérance de clé TEK) avant l'expiration de la clé la plus récente que le CM détient actuellement. Cette durée est configurée au moyen du CMTS de façon à intervenir après l'expiration programmée de la plus ancienne des deux clés TEK.

7.1.3.4 Paramètres

Toutes les valeurs des paramètres de configuration sont spécifiées dans le fichier paramétrique téléchargé par protocole TFTP (voir Annexe A).

7.1.3.4.1 Temporisation d'attente opérationnelle

Période de temporisation entre envois de messages de demande de clé à partir de l'état d'attente opérationnelle. Voir § A.1.1.1.4.

7.1.3.4.2 Temporisation d'attente de renouvellement de clé

Période de temporisation entre envois de messages de demande de clé à partir de l'état d'attente de renouvellement de clé. Voir § A.1.1.1.5.

7.1.3.4.3 Délai de tolérance de clé TEK

Intervalle exprimé en secondes avant l'expiration estimée d'une clé TEK, à l'issue duquel le CM commence à recalculer une nouvelle clé TEK.

Le délai de tolérance de clé TEK est spécifié dans un réglage de configuration contenu dans le fichier paramétrique téléchargé par TFTP. Il est le même pour tous les identificateurs SAID. Voir § A.1.1.1.6.

7.1.3.5 Actions

1-B Attente opérationnelle (*arrêt*) → Début

- réinitialisation du temporisateur de nouvelle demande de clé;
- terminaison de l'automate FSM de clé TEK.

1-C Attente de réautorisation opérationnelle (*Arrêt*) → Début

- terminaison de l'automate FSM de clé TEK.

1-D Opérationnel (*arrêt*) → Début

- réinitialisation du temporisateur de renouvellement de clé TEK, qui est réglé de façon à expirer au bout du "*délai de tolérance de clé Tek*" (en secondes) avant l'instant d'expiration programmé de clé TEK;

- terminaison de l'automate FSM de clé TEK;
- suppression du matériel de calcul de clés SAID dans la table de clés.

1-E Attente de renouvellement de clé (*arrêt*) → Début

- réinitialisation du temporisateur de renouvellement de clé TEK;
- terminaison de l'automate FSM de clé TEK;
- suppression du matériel de calcul de clés SAID dans la table de clés.

1-F Attente de réautorisation de renouvellement de clé (*arrêt*) → Début

- terminaison de l'automate FSM de clé TEK;
- suppression du matériel de calcul de clés SAID dans la table de clés.

2-A Début (*autorisé*) → Attente opérationnelle

- envoi du message de demande de clé au système CMTS;
- réglage du temporisateur de nouvelle demande de clé à la temporisation d'attente opérationnelle.

3-B Attente opérationnelle (*aut. en instance*) → Attente de réaut. opérationnelle

- réinitialisation du temporisateur de nouvelle demande de clé.

3-E Attente de renouv. de clé (*aut. en instance*) → Attente de réaut. de renouv. de clé

- réinitialisation du temporisateur de nouvelle demande de clé.

4-C Attente de réaut. opérationnelle (*aut. compl.*) → Attente opérationnelle

- envoi d'un message de demande de clé au CMTS;
- réglage du temporisateur de nouvelle demande de clé à la temporisation d'attente opérationnelle.

4-F Attente de réaut. de renouv. de clé (*aut. compl.*) → Attente de renouv. de clé

- envoi d'un message de demande de clé au CMTS;
- réglage du temporisateur de nouvelle demande de clé à la temporisation d'attente de renouv. de clé.

5-D Opérationnel (*clé TEK non valide*) → Attente opérationnelle

- réinitialisation du temporisateur de renouvellement de clé TEK;
- envoi du message de demande de clé au CMTS;
- réglage du temporisateur de nouvelle demande de clé à la temporisation d'attente opérationnelle;
- suppression du matériel de calcul de clés SAID dans la table de clés.

5-E Attente de renouv. de clé (*clé TEK non valide*) → Attente opérationnelle

- réinitialisation du temporisateur de renouvellement de clé;
- envoi du message de demande de clé au CMTS;
- réglage du temporisateur de nouvelle demande de clé à la temporisation d'attente opérationnelle;
- suppression du matériel de calcul de clés SAID dans la table de clés.

5-F Attente de réaut. de renouv. de clé (*clé TEK non valide*) → Attente de réaut. opérationnelle

- suppression du matériel de calcul de clés SAID dans la table de clés.

6-B Attente opérationnelle (*temporisation*) → Attente opérationnelle

- envoi du message de demande de clé au CMTS;
- réglage du temporisateur de nouvelle demande de clé à la temporisation d'attente opérationnelle.

6-E Attente de renouv. de clé (*temporisation*) → Attente de renouv. de clé

- envoi du message de demande de clé au CMTS;
- réglage du temporisateur de nouvelle demande de clé à la temporisation d'attente de renouvellement de clé.

7-D Opérationnel (*délai de tolérance de clé TEK*) → Attente de renouv. de clé

- envoi du message de demande de clé au CMTS;
- réglage du temporisateur de nouvelle demande de clé à la temporisation d'attente de renouvellement de clé.

8-B Attente opérationnelle (*réponse de clé*) → Opérationnel

NOTE 1 – La réponse de clé a transmis l'authentification du message.

- réinitialisation du temporisateur de nouvelle demande de clé;
- traitement du contenu du message de réponse de clé et incorporation du nouveau matériel de calcul de clés dans la base de données de clés;
- réglage du temporisateur de renouvellement de clé TEK de façon à expirer au bout du nombre de secondes du "délai de tolérance de clé TEK" avant l'expiration programmée de la clé.

8-E Attente de renouvellement de clé (*réponse de clé*) → Opérationnel

NOTE 2 – La réponse de clé a transmis l'authentification du message.

- réinitialisation du temporisateur de nouvelle demande de clé;
- traitement du contenu du message de réponse de clé et incorporation du nouveau matériel de calcul de clés dans la base de données de clés;
- réglage du temporisateur de renouvellement de clé TEK de façon à expirer au bout du nombre de secondes du "délai de tolérance de clé TEK" avant l'expiration programmée de la clé.

9-B Attente opérationnelle (*rejet de clé*) → Début

NOTE 3– Le rejet de clé a transmis l'authentification du message.

- réinitialisation du temporisateur de nouvelle demande de clé;
- terminaison de l'automate FSM de clé TEK.

9-E Attente de renouvellement de clé (*rejet de clé*) → Début

- réinitialisation du temporisateur de nouvelle demande de clé;
- terminaison de l'automate FSM de clé TEK;
- suppression du matériel de calcul de clés SAID dans la table de clés.

7.2 Formats des messages de gestion de clé[4]

La gestion de clé à confidentialité de base (BPKM, *baseline privacy key management*) fait appel à deux types de messages de commande MAC: BPKM-REQ et BPKM-RSP. [J.112-B] et [J122] définissent les valeurs spécifiques attribuées à chacun de ces types.

Tableau 7-3/J.125 – Messages MAC de gestion de clé à confidentialité de base

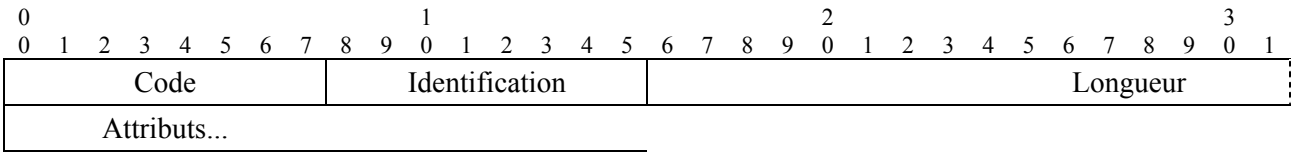
Valeur du type	Nom du message	Description du message
Voir [J.112-B] ou [J.122]	BPKM-REQ	Demande de gestion de clé confidentielle [CM → CMTS]
Voir [J.112-B] ou [J.122]	BPKM-RSP	Réponse de gestion de clé confidentielle [CMTS → CM]

Bien que ces deux types de messages de gestion MAC établissent une distinction entre demandes (de CM à CMTS) et réponses (de CMTS à CM) de gestion BPKM, des informations plus détaillées sur le contenu de ces messages sont codées dans les messages BPKM eux-mêmes, ce qui assure une séparation nette entre fonctions de gestion de confidentialité et d'autre part attribution de largeur de bande amont par commande MAC à l'interface RF, rythme et synchronisation (qui sont les responsabilités principales de la gestion MAC à l'interface RF).

7.2.1 Format des paquets

Exactement un message BPKM est encapsulé dans le champ de charge utile d'un message de gestion MAC.

Un résumé du format de message BPKM est représenté ci-dessous. Les champs sont transmis de gauche à droite.



Code

Le champ de code est d'un octet et désigne le type de paquet BPKM. Lorsqu'un paquet est reçu avec un champ de code non valide, il CONVIENT de l'ignorer sans notification.

Les codes (décimaux) de gestion BPKM sont attribués comme suit:

Tableau 7-4/J.125 – Codes de gestion de clé à confidentialité de base (BPKM)

Code	Type de message BPKM	Nom du message de gestion MAC
0-3	Champ réservé	–
4	Demande d'aut.	BPKM-REQ
5	Réponse d'aut.	BPKM-RSP
6	Rejet d'aut.	BPKM-RSP
7	Demande de clé	BPKM-REQ

[4] Les formats des messages du protocole de base BPKM sont modélisés après ceux du protocole (RADIUS, *remote authentication dial in user service*) [RFC 2868] et un protocole de suivi de normes Internet. Les protocoles BPKM, tels le protocole RADIUS, s'appuient sur un modèle client/serveur. Contrairement au protocole RADIUS, le protocole BPKM ne fonctionnera pas sur le protocole UDP/IP. Les messages BPKM sont encapsulés dans des messages de gestion MAC à l'interface RF.

Tableau 7-4/J.125 – Codes de gestion de clé à confidentialité de base (BPKM)

Code	Type de message BPKM	Nom du message de gestion MAC
8	Réponse de clé	BPKM-RSP
9	Rejet de clé	BPKM-RSP
10	Aut. non valide	BPKM-RSP
11	Clé TEK non valide	BPKM-RSP
12	Inform. d'authentif.	BPKM-REQ
13	Demande de mappage	BPKM-REQ
14	Réponse de mappage	BPKM-RSP
15	Rejet de mappage	BPKM-RSP
16-255	Champ réservé	–

Identificateur

Le champ identificateur est d'un octet. Un CM utilise l'identificateur pour faire correspondre les réponses d'un CMTS avec les demandes de CM.

Le CM DOIT modifier (par exemple, incrémenter ou revenir à 0 après avoir atteint 255) le champ d'identificateur lors de l'émission d'un nouveau message BPKM. Un "nouveau" message est une demande d'autorisation, une demande de clé ou une demande de mappage d'association SA qui n'est pas réexpédiée en réponse à un événement de temporisation. Dans le cas d'une réexpédition, le champ d'identificateur DOIT rester inchangé.

Le champ identificateur PEUT être mis à zéro dans les messages d'information d'authentification, qui sont informatifs et n'appellent aucun message de réponse.

Le champ identificateur d'un message de réponse BPKM d'un CMTS DOIT correspondre au champ identificateur du message de demande BPKM auquel ce CMTS est en train de répondre. Le champ identificateur DOIT être mis à zéro dans les messages de clé TEK non valide, qui ne sont pas envoyés en réponse à des demandes BPKM. Dans les messages d'autorisation non valide non sollicités, le champ identificateur DOIT être mis à zéro.

Dès réception d'un message de réponse BPKM, le CM associe ce message à un automate à états particulier (l'automate d'autorisation dans le cas de réponses d'autorisation, de rejets d'autorisation et d'autorisation non valide; un automate de clé TEK particulier dans le cas de réponses de clé, de rejets de clé et de clé TEK non valide; un automate à états de mappage SA particulier dans le cas de réponses de mappage SA et de rejets de mappage SA).

Un CM PEUT garder trace de l'identificateur, de sa plus récente demande d'autorisation en instance. Le CM PEUT ignorer sans notification des réponses d'autorisation et des rejets d'autorisation dont le champ identificateur ne correspond pas à celui des demandes en instance.

Un CM PEUT garder trace de l'identificateur de sa plus récente demande de clé en instance. Le CM PEUT ignorer sans notification des réponses de clé et des rejets de clé dont le champ identificateur ne correspond pas à celui des demandes en instance.

Un CM PEUT garder trace de l'identificateur de sa plus récente demande de mappage SA en instance. Le CM PEUT ignorer sans notification des réponses de mappage SA et de rejet de mappage SA dont le champ identificateur ne correspond pas à celui des demandes en instance.

Longueur

Le champ de longueur est de 2 octets. Il indique la longueur en octets des champs d'attribut. Le champ de longueur ne comprend pas les champs de code, d'identificateur et de longueur. Les octets

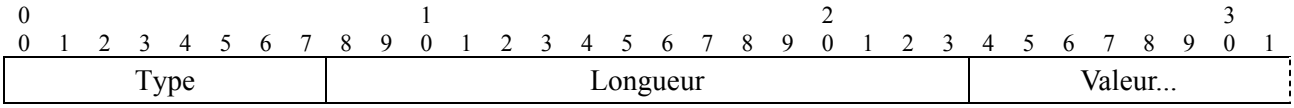
extérieurs à l'étendue du champ de longueur DOIVENT être traités comme un bourrage et être ignorés à la réception. Si le paquet est plus court qu'indiqué par le champ de longueur, il CONVIENT d'ignorer ce paquet sans notification. La longueur minimale est 0 et la longueur maximale est 1490.

Attributs

Les attributs de gestion BPKM acheminent les données spécifiques d'authentification, d'autorisation et de gestion de clés échangées entre client et serveur. Chaque type de paquet BPKM possède son propre ensemble d'attributs requis et facultatifs. Sauf indication explicite, aucune règle ne s'applique à l'ordre des attributs dans un message BPKM.

La fin de la liste d'attributs est indiquée par la longueur du paquet de gestion BPKM.

Les attributs sont codés en type/longueur/valeur (TLV) comme indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Les formats de paquet sont décrits ci-dessous pour chaque message de gestion BPKM. Les descriptions énumèrent les attributs BPKM contenus dans chaque type de message BPKM. Les attributs eux-mêmes sont décrits au § 7.2.2. Les attributs inconnus DOIVENT être ignorés dès réception et omis lors de la recherche d'attributs reconnus.

Le CMTS DOIT ignorer sans notification toutes les demandes qui ne contiennent pas TOUS les attributs requis. Le CM DOIT ignorer sans notification toutes les réponses qui ne contiennent pas TOUS les attributs requis.

7.2.1.1 Demande d'autorisation (demande d'aut.)

Code: 4

Attributs:

Tableau 7-5/J.125 – Attributs de demande d'autorisation

Attributs	Contenu
Identification du CM	Contient des informations utilisées pour identifier le câblo-modem auprès du CMTS
Certificat du CM	Contient le certificat X.509 d'utilisateur du CM
Capacités de sécurité	Décrit les capacités de sécurité du CM demandeur
SAID	SAID primaire du CM, égal au SID primaire

L'attribut "Identification du CM" contient un ensemble de données qui identifie le câblo-modem demandeur auprès du CMTS.

NOTE – Celui-ci n'utilise très vraisemblablement qu'un seul élément de l'attribut "Identification du CM" (par exemple, l'adresse MAC du CM) en tant que pointeur sur le CM. Bien qu'un élément spécifique puisse être sélectionné pour inclusion dans le message de demande d'autorisation, le fait d'insérer l'ensemble de l'attribut "Identification du CM" offre aux vendeurs une plus grande flexibilité de conception du système tête de ligne pour l'identification du CM client.

L'attribut "Certificat du CM" contient un certificat X.509 de CM émis par le fabricant de celui-ci. Il s'agit d'un certificat à clé publique qui associe de façon vérifiable les informations d'identification du CM à sa clé publique codée RSA. Le certificat X.509 comporte une signature numérique du fabricant du CM et cette signature peut être vérifiée par un CMTS qui connaît la clé publique de ce

fabricant, elle-même placée dans un certificat d'autorité de certification (CA, *certification authority*) X.509 signé à son tour par une autorité de certification de niveau supérieur.

L'attribut "Capacités de sécurité" est un élément composite décrivant les capacités du câblo-modem demandeur en termes de sécurité, ce qui inclut l'algorithme (ou les algorithmes) de cryptage de données en paquet pris en charge par un CM ainsi que l'algorithme (ou les algorithmes) d'authentification de données en paquet pris en charge (et qui n'existent pas encore) plus la version du protocole de confidentialité de base pris en charge (la seule existant actuellement étant la version 1 de l'interface BPI+).

L'attribut "SAID" contient un identificateur (ID) d'association de sécurité (SA) à confidentialité de base ou SAID. Dans ce cas, l'identificateur SAID fourni est le SAID primaire d'interface BPI+ du CM, qui est égal à l'identificateur SID primaire qui a été attribué au câblo-modem au cours de l'inscription MAC par interface RF.

7.2.1.2 Réponse d'autorisation (réponse d'aut.)

Le message de réponse d'autorisation, envoyé par le CMTS à un CM client en réponse à une demande d'autorisation, contient une clé d'autorisation, la durée de vie de la clé, le numéro de séquence de la clé, et une liste de descripteurs SA désignant les associations de sécurité primaires et statiques auxquelles le câblo-modem demandeur est autorisé à accéder, avec leurs propriétés particulières (comme le type ou la suite cryptographique). La clé d'autorisation DOIT être chiffrée avec la clé publique du CM. La liste de descripteurs d'association DOIT comprendre un descripteur pour l'identificateur SAID primaire BPI+ indiqué au CMTS dans la demande d'autorisation correspondante. La liste de descripteurs SA PEUT inclure les descripteurs des identificateurs SAID statiques auxquels le CM est autorisé à accéder.

Champ de code: 5

Attributs:

Tableau 7-6/J.125 – Attributs de réponse d'autorisation

Attribut	Contenu
Clé d'autorisation	Clé d'autorisation (AUTH), chiffrée avec la clé publique cible du CM client
Durée de vie de clé	Durée de vie de clé d'autorisation
Numéro de séquence de clé	Numéro de séquence de clé d'autorisation
(Un ou plusieurs) Descripteur(s) SA	Chaque attribut composite "Descripteur(s) SA" spécifie un identificateur SAID et des propriétés additionnelles de l'association SA.

7.2.1.3 Rejet d'autorisation (rejet d'aut.)

Le système CMTS répond à une demande d'autorisation émise par un CM par un message de rejet d'autorisation si le CMTS rejette la demande d'autorisation du CM.

Champ de code: 6

Attributs:

Tableau 7-7/J.125 – Attributs de rejet d'autorisation

Attribut	Contenu
Code d'erreur	Code d'erreur indiquant la raison du rejet de demande d'autorisation
Chaîne d'affichage (facultative)	Chaîne d'affichage indiquant la raison du rejet de demande d'autorisation

Les attributs "Code d'erreur" et "Chaîne d'affichage" donnent au CM demandeur la raison de l'échec d'autorisation.

7.2.1.4 Demande de clé

Code: 7

Attributs:

Tableau 7-8/J.125 – Attributs de demande de clé

Attribut	Contenu
Identification du CM	Contient des informations utilisées pour identifier le câblo-modem auprès du CMTS
Numéro de séquence de clé	Numéro de séquence de clé d'autorisation
SAID	ID d'association de sécurité
Résumé HMAC	Résumé de message à cryptage SHA

L'attribut "Résumé HMAC" est un résumé de message chiffré. Cet attribut DOIT être l'attribut final dans la liste d'attributs contenue dans la demande de clé. Le résumé de message est calculé à partir de l'en-tête de paquet et de tous les attributs de demande de clé autres que "Résumé HMAC", dans l'ordre de leur apparition dans le paquet.

L'insertion du résumé chiffré permet au système CMTS d'authentifier le message de demande de clé. La clé d'authentification du résumé chiffré est calculée sur la clé d'autorisation. Voir le § 10 pour plus de détails.

7.2.1.5 Réponse de clé

Code: 8

Attributs:

Tableau 7-9/J.125 – Attributs de réponse de clé

Attribut	Contenu
Numéro de séquence de clé	Numéro de séquence de clé d'autorisation
SAID	ID d'association de sécurité
Paramètres de clé TEK	"Ancienne" génération de paramètres de clé applicables au SAID
Paramètres de clé TEK	"Nouvelle" génération de paramètres de clé applicables au SAID
Résumé HMAC	Résumé de message à cryptage SHA

L'attribut "Paramètres de clé TEK" est un élément composite contenant tout le matériel de calcul de clés correspondant à une génération particulière de clé d'identificateur SAID. Ce matériel comprendra la clé TEK, la durée de vie restante de la clé TEK, son numéro de séquence de clé et le vecteur d'initialisation CBC. La clé TEK est chiffrée. Voir détails au § 7.2.2.13.

Le système CMTS conserve à tout moment, pour chaque identificateur SAID, deux générations actives formant chacune un ensemble de matériel de calcul de clés (contenant une clé TEK et son vecteur d'initialisation CBC correspondant). Le premier ensemble correspond à "l'ancienne" et le second à la "nouvelle"génération du matériel de calcul de clés. La nouvelle génération possède un numéro de séquence de clé supérieur d'une unité (modulo 16) à celui de l'ancienne génération. Le paragraphe 9.1 spécifie les exigences du système CMTS afin de conserver et d'utiliser les deux générations actives du matériel de calcul de clés d'un identificateur SAID.

Le système CMTS distribue à un CM client les deux générations de matériel de calcul de clés actif. Le message de réponse de clé contient donc deux attributs "Paramètres de clé TEK" contenant chacun le matériel de calcul de clés pour un des deux ensembles actifs de matériel de calcul de clés d'identificateur SAID.

L'attribut "Résumé HMAC" est un résumé de message chiffré qui DOIT être l'attribut final dans la liste d'attributs de la réponse de clé. Le résumé de message est calculé sur l'en-tête du message de gestion BPKM (à partir du champ de code BPKM) et sur tous les attributs de la réponse de clé autres que "Résumé HMAC", dans l'ordre de leur apparition dans le paquet.

L'inclusion du résumé chiffré permet au client récepteur d'authentifier le message de réponse de clé et de vérifier que le CM et le CMTS possèdent des clés d'autorisation synchronisées. La clé d'authentification du résumé HMAC est calculée sur la clé d'autorisation. Voir détails au § 10.

7.2.1.6 Rejet de clé

La réception d'un message de rejet de clé indique que le CM client récepteur n'est plus autorisé pour un identificateur SAID particulier.

Code: 9

Attributs:

Tableau 7-10/J.125 – Attributs de rejet de clé

Attribut	Contenu
Numéro de séquence de clé	Numéro de séquence de clé d'autorisation
SAID	ID d'association de sécurité
Code d'erreur	Code d'erreur indiquant la raison du rejet de la demande de clé
Chaîne d'affichage (facultative)	Chaîne d'affichage indiquant la raison du rejet de clé
Résumé HMAC	Résumé de message à cryptage SHA

L'attribut "Résumé HMAC" est un résumé de message chiffré qui DOIT être l'attribut final dans la liste d'attributs de la réponse de clé. Le résumé de message est calculé sur l'en-tête du message de gestion BPKM (à partir du champ de code BPKM) et sur tous les attributs de la réponse de clé autres que "Résumé HMAC", dans l'ordre de leur apparition dans le paquet.

L'inclusion du résumé chiffré permet au client récepteur d'authentifier le message de réponse de clé et de vérifier que le CM et le CMTS possèdent des clés d'autorisation synchronisées. La clé d'authentification du résumé HMAC est calculée sur la clé d'autorisation. Voir détails au § 10.

7.2.1.7 Autorisation non valide

Le système CMTS peut envoyer un message d'autorisation non valide à un CM client sous la forme:

- d'une indication non sollicitée;
- d'une réponse à un message reçu de ce CM.

Dans un cas comme dans l'autre, le message d'autorisation non valide commande au CM récepteur d'envoyer une demande de réautorisation à son système CMTS.

Le CMTS envoie un message d'autorisation non valide en réponse à une demande de clé si:

1) le CMTS ne reconnaît pas le CM comme étant autorisé (c'est-à-dire qu'aucune clé d'autorisation valide n'est associée au câblo-modem demandeur);
2) la vérification du résumé de message chiffré contenu dans la demande de clé (et dans l'attribut "Résumé HMAC") a échoué, ce qui indique une perte du synchronisme entre les clés d'autorisation du CM et du CMTS.

Code: 10

Attributs:

Tableau 7-11/J.125 – Attributs d'autorisation non valide

Attribut	Contenu
Code d'erreur	Code d'erreur indiquant la raison du message d'autorisation non valide
Chaîne d'affichage (facultative)	Chaîne d'affichage décrivant une situation d'échec

7.2.1.8 Clé TEK non valide

Le système CMTS envoie un message de clé TEK non valide à un CM client si ce CMTS détermine que ce CM a chiffré une unité PDU de données en paquet amont avec une clé TEK non valide; c'est-à-dire que le numéro de séquence de clé TEK d'un identificateur SAID, contenu dans l'élément d'en-tête étendu à confidentialité de base du paquet reçu, se trouve en dehors de l'étendue des numéros de séquence valides et connus du CMTS pour cet identificateur SAID.

Code: 11

Attributs:

Tableau 7-12/J.125 – Attributs de clé TEK non valide

Attribut	Contenu
Numéro de séquence de clé	Numéro de séquence de clé d'autorisation
SAID	ID d'association de sécurité
Code d'erreur	Code d'erreur indiquant la raison du message de clé TEK non valide
Chaîne d'affichage (facultative)	Chaîne d'affichage contenant des informations définies par le vendeur
Résumé HMAC	Résumé de message à cryptage SHA

L'attribut "Résumé HMAC" est un résumé de message chiffré qui DOIT être l'attribut final dans la liste d'attributs de la réponse de clé. Le résumé de message est calculé sur l'en-tête du message de gestion BPKM (à partir du champ de code BPKM) et sur tous les attributs de la réponse de clé autres que "Résumé HMAC", dans l'ordre de leur apparition dans le paquet.

L'inclusion du résumé chiffré permet au client récepteur d'authentifier le message de réponse de clé et de vérifier que le CM et le CMTS possèdent des clés d'autorisation synchronisées. La clé d'authentification du résumé HMAC est calculée sur la clé d'autorisation. Voir détails au § 10.

7.2.1.9 Informations d'authentification (informations d'authentif.)

Le message d'informations d'authentification contient un unique attribut "Certificat CA" contenant un certificat CA X.509 pour le fabricant du CM. Le certificat X.509 d'utilisateur du CM DOIT avoir été émis par l'autorité de certification désignée par le certificat CA X.509. Les certificats CA X.509 DOIVENT être émis par une autorité de certification DOCSIS.

Les messages d'informations d'authentification sont strictement informatifs: alors que le CM DOIT transmettre les messages d'informations d'authentification indiqués par l'automate à états d'authentification (§ 7.1.2), le CMTS PEUT ne pas en tenir compte.

Code: 12

Attributs:

Tableau 7-13/J.125 – Attributs d'informations d'authentification

Attribut	Contenu
Certificat CA	Certificat de l'autorité CA du fabricant qui a émis le certificat du CM

L'attribut "Certificat CA" contient un certificat CA X.509 pour l'autorité CA qui a émis le certificat X.509 de l'utilisateur du CM. L'autorité de certification DOCSIS émet ces certificats CA à l'intention de fabricants de CM certifiés DOCSIS.

7.2.1.10 Demande de mappage SA (demande de mappage)

Un modem CM envoie des demandes de mappage SA à son système CMTS afin d'obtenir le mappage d'un flux de trafic aval particulier sur une association SA de l'interface BPI+. Le paragraphe 8 décrit l'automate à états de mappage SA qui utilise ce message.

Code: 13

Attributs:

Tableau 7-14/J.125 – Attributs de demande de mappage SA

Attribut	Contenu
Identification du CM	Contient des informations utilisées pour identifier le câblo-modem auprès du CMTS
Recherche de SA	Contient des informations d'adressage indiquant le flux de trafic aval pour lequel le CM demande un mappage SA

7.2.1.11 Réponse de mappage SA (réponse de mappage)

Un système CMTS envoie une réponse de mappage SA en réponse favorable à une demande de mappage SA émise par un CM client. Cette réponse de mappage SA informe le CM d'un mappage entre une adresse recherchée et une association SA de l'interface BPI+. Le paragraphe 8 décrit l'automate à états de mappage SA qui utilise ce message.

Code: 14

Attributs:

Tableau 7-15/J.125 – Attributs de réponse de mappage SA

Attribut	Contenu
Recherche de SA	Contient des informations d'adressage indiquant le flux de trafic aval pour lequel un mappage SA est demandé au CM
Descripteur SA	L'attribut composite "Descripteur SA" spécifie l'identificateur SAID de l'association SA mappée ainsi que d'autres propriétés

7.2.1.12 Rejet de mappage SAID (rejet de mappage)

Un système CMTS envoie un rejet de mappage SA en réponse défavorable à une demande de mappage SA émise par un CM client. Ce rejet de mappage SA informe le CM que soit:

1) le flux de trafic aval identifié dans l'attribut "Recherche de SA" n'est pas en cours de cryptage;

2) le CM demandeur n'est pas autorisé à recevoir du trafic.

Le contenu de l'attribut "Code d'erreur" établit une distinction entre ces deux cas. Le paragraphe 8 décrit l'automate à états de mappage qui utilise ce message.

Code: 15

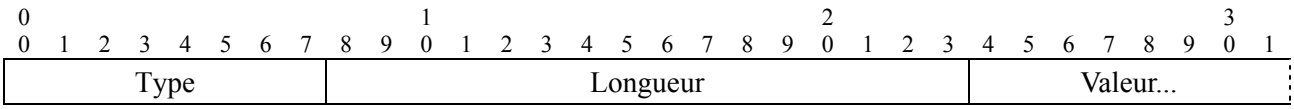
Attributs:

Tableau 7-16/J.125 – Attributs de rejet de mappage SA

Attribut	Contenu
Recherche de SA	Contient des informations d'adressage indiquant le flux de trafic aval pour lequel le CM a demandé un mappage SA
Code d'erreur	Code d'erreur indiquant la raison du rejet de la demande de mappage SA
Chaîne d'affichage (facultative)	Chaîne d'affichage indiquant la raison du rejet de mappage

7.2.2 Attributs de gestion BPKM

Un résumé du format de ces attributs est représenté ci-dessous. Les champs sont transmis de gauche à droite.



Type:

le champ de type est d'un octet. Les valeurs du champ de type de gestion BPKM sont spécifiées ci-dessous.

NOTE 1 – Les valeurs de type comprises entre 0 et 127 sont définies dans le cadre de la spécification de la confidentialité de base et que les valeurs comprises entre 128 et 255 sont des types d'attribut attribués par le vendeur.

Un serveur BPKM DOIT ignorer les attributs de type inconnu.

Un client BPKM DOIT ignorer les attributs de type inconnu.

Un client et un serveur BPKM (c'est-à-dire un CM et un CMTS) PEUVENT accuser réception de types d'attribut inconnus.

Tableau 7-17/J.125 – Types d'attribut de gestion BPKM

Type	Attribut BPKM
0	Champ réservé
1	Numéro de série
2	Identificateur de fabricant
3	Adresse de commande MAC
4	Clé publique à codage RSA
5	Identification du CM
6	Chaîne d'affichage
7	CLÉ D'AUT.
8	TEK
9	Durée de vie de clé

Tableau 7-17/J.125 – Types d'attribut de gestion BPKM

Type	Attribut BPKM
10	Numéro de séquence de clé
11	Résumé HMAC
12	SAID
13	Paramètres de clé TEK
14	ANNULÉ
15	Vecteur d'initialisation de concaténation CBC
16	Code d'erreur
17	Certificat CA
18	Certificat du CM
19	Capacités de sécurité
20	Suite cryptographique
21	Liste de suites cryptographiques
22	Version d'interface BPI
23	Descripteur(s) SA
24	Type d'association SA
25	Recherche de SA
26	Recherche de type d'association SA
27	Adresse IP
28	Paramètres de téléchargement
29-126	Champ réservé
127	Défini par le vendeur
128-255	Types d'attribut attribués par le vendeur

Longueur

Le champ de longueur est de 2 octets et indique la longueur, en octets, du champ de valeur de cet attribut. Le champ de longueur *n'inclut pas* les champs de type et de longueur[5]. La longueur minimale d'attribut est de 0 et la longueur maximale est de 1487 octets.

Les paquets contenant des attributs de longueur non valide DEVRAIENT être ignorés sans notification.

Valeur

Le champ de valeur est de zéro, un ou plusieurs octets et il contient des informations propres à l'attribut. Le format et la longueur du champ de valeur sont déterminés par les champs de type et de longueur. Toutes les grandeurs d'entier exprimées par plusieurs octets

[5] Cela est cohérent aussi bien avec le codage TLV employé dans les éléments d'en-tête étendu de commande MAC à l'interface RF qu'avec le codage TLV employé pour les réglages de configuration dans le fichier de configuration du CM, [J.112-B] ou [J.122]. Le codage TLV de la gestion BPKM diffère de celui qui est employé par le protocole RADIUS, sur lequel la structure de message de base de gestion BPKM est fondée, en ce sens que le champ de longueur des attributs RADIUS contient les champs de type et de longueur ainsi qu'un champ de valeur d'attribut.

sont dans l'ordre des octets du réseau, c'est-à-dire que l'octet contenant les bits de plus fort poids est transmis en premier sur la ligne.

NOTE 2 – Une "chaîne" ne nécessite pas de terminaison par le caractère ASCII "néant" parce que l'attribut possède déjà un champ de longueur.

Le format du champ de valeur correspond à un des cinq types de données suivants.

Tableau 7-18/J.125 – Types de données du champ de valeur d'attribut

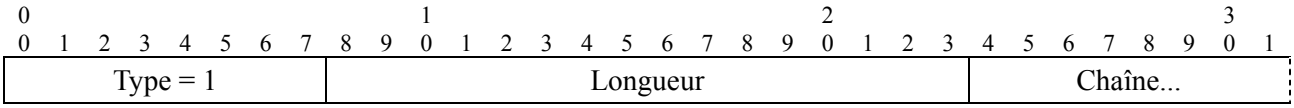
chaîne	0-1487 octets
uint8	Entier non signé de 8 bits
uint16	Entier non signé de 16 bits
uint32	Entier non signé de 32 bits
composite	Ensemble d'attributs

7.2.2.1 Numéro de série

Description

Cet attribut indique le numéro de série attribué par le fabricant à un câblo-modem.

Un résumé du format de l'attribut "Numéro de série" est représenté ci-dessous. Les champs sont transmis de gauche à droite.



Type

1 pour le numéro de série

Longueur

≥ 0 et ≤ 255

Chaîne

Le champ de chaîne est de zéro, un ou plusieurs octets. Il contient un numéro de série attribué par le fabricant.

Le numéro de série attribué par le fabricant DOIT être codé selon le jeu de caractères ISO/CEI 8859-1. Les caractères employés DOIVENT être limités à ce qui suit:

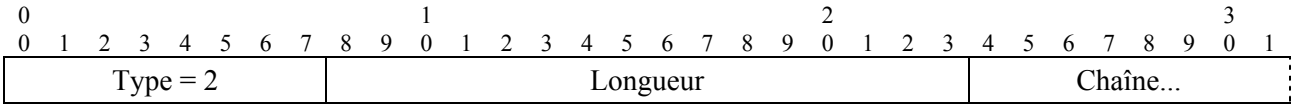
- A-Z (0x41-0x5A)
- a-z (0x61-0x7A)
- 0-9 (0x30-0x39)
- "-" (0xD2)

7.2.2.2 Identificateur de fabricant

Description

Cet attribut identifie le fabricant. L'identificateur a une longueur de 3 octets et contient l'identificateur propre à une organisation (OUI, *organizationally unique identifier*) de 3 octets qui est attribué aux organisations requérantes par l'IEEE [IEEE1]. Les deux premiers bits de la chaîne de 3 octets sont mis à zéro.

Un résumé du format de l'attribut "Identificateur de fabricant" est représenté ci-dessous. Les champs sont transmis de gauche à droite.



Type

2 pour l'identificateur de fabricant

Longueur

3

Chaîne

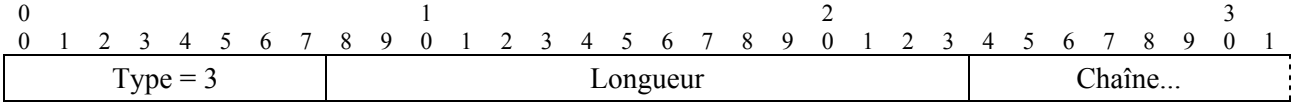
Le champ de chaîne est de trois octets et contient un identificateur OUI attribué par l'IEEE.

7.2.2.3 Adresse de commande MAC

Description

Cet attribut désigne l'adresse de commande MAC IEEE attribuée au CM. Garantie unique, elle est appelée à être utilisée dans le système CMTS comme pointeur/index vers le câblo-modem.

Un résumé du format de l'attribut "Identificateur de fabricant" est représenté ci-dessous. Les champs sont transmis de gauche à droite.



Type

3 pour l'adresse de commande MAC

Longueur

6

Chaîne

Le champ de chaîne contient une adresse MAC de 6 octets.

7.2.2.4 Clé publique à codage RSA

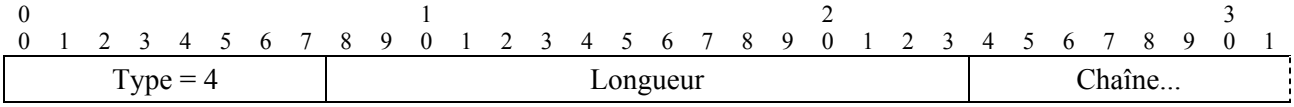
Description

Cet attribut est une chaîne contenant un type ASN.1 RSAPublicKey à codage DER, comme défini dans la norme PKCS #1 v2.0 [RSA3] de codage RSA.

La norme PKCS #1 v2.0 spécifie qu'une clé publique à codage RSA se compose à la fois d'un module public RSA et d'un exposant public RSA. Le type RSAPublicKey comporte ces deux éléments sous forme de types INTEGER à codage DER.

La norme PKCS #1 v2.0 précise que l'exposant public RSA peut être normalisé dans des applications spécifiques. Ce document suggère des valeurs de 3 ou 65537 (F4). L'interface BPI+ normalise sur la base de F4 en tant qu'exposant public et emploie un module de 1024 bits (alors que la confidentialité de base employait un module de 768 bits). Afin de permettre des mises à niveau logicielles du matériel DOCSIS 1.0 conformément à une version préliminaire de la présente Recommandation de l'interface BPI+, les implémentations BPI+ DOIVENT prendre en charge le module de 768 bits.

Un résumé du format de l'attribut de clé publique est représenté ci-dessous. Les champs sont transmis de gauche à droite.



Type

4 pour la clé publique à codage RSA.

Longueur

106, 140, ou 270 (longueur du codage DER en utilisant F4 comme exposant public et, respectivement, un module public de 768 bits, 1024 bits ou 2048 bits).

Chaîne

Type ASN.1 RSAPublicKey à codage DER.

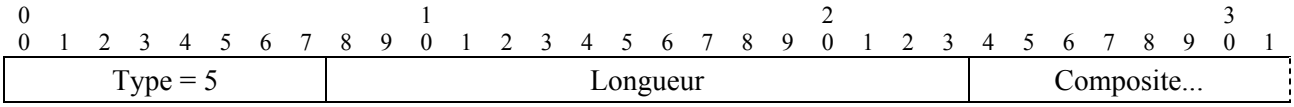
7.2.2.5 Identification du CM

Description

Cet attribut est de type composite car il forme un ensemble de sous-attributs. Ces sous-attributs contiennent des informations qui pourront être utilisées afin d'identifier de façon unique un câblo-modem. Les sous-attributs DOIVENT comprendre:

- un numéro de série;
- un identificateur de fabricant;
- une adresse de commande MAC;
- une clé publique à codage RSA.

L'identification du CM PEUT également contenir des attributs facultatifs, définis par le vendeur.



Type

5

Longueur

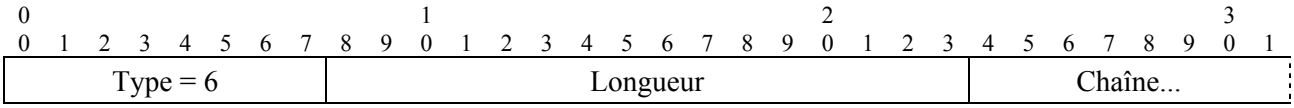
≥ 126

7.2.2.6 Chaîne d'affichage

Description

Cet attribut contient un message alphanumérique. Il est normalement utilisé pour expliquer une réponse d'échec. Il peut être enregistré par le récepteur afin de pouvoir être extrait ultérieurement par un gestionnaire SNMP. Les chaînes d'affichage NE DOIVENT PAS avoir une longueur supérieure à 128 octets.

Un résumé du format de l'attribut "Chaîne d'affichage" est représenté ci-dessous. Les champs sont transmis de gauche à droite.



Type

6 pour une chaîne d'affichage

Longueur

≥ 0 et ≤ 128

Chaîne

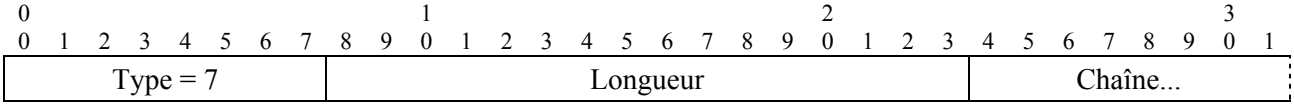
Chaîne de caractères. Il n'est pas obligatoire que la chaîne de caractères se termine par un caractère néant. Le champ de longueur indique toujours la fin de la chaîne.

7.2.2.7 Clé d'autorisation

Description

La clé d'autorisation est une grandeur de 20 octets permettant de calculer une clé de cryptage de clés et deux clés d'authentification de message (l'une pour les demandes amont, l'autre pour les réponses aval).

Cet attribut contient une quantité de 96 ou 128 octets représentant la clé d'autorisation chiffrée par la clé publique RSA à module de 768 ou 1024 bits du CM. Les détails de la procédure de cryptage sont indiqués dans le § 10.5. Le cryptogramme produit par l'algorithme RSA indiquera la longueur du module RSA: 96 ou 128 octets.



Type

7 pour la clé d'autorisation

Longueur

96 ou 128

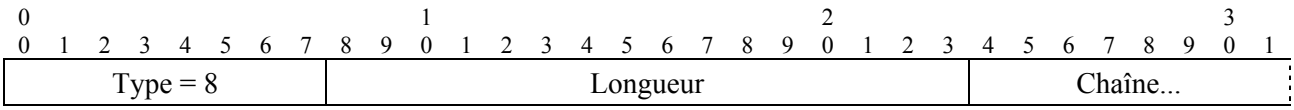
Chaîne

Grandeur de 96 ou 128 octets représentant une clé d'autorisation à cryptage RSA.

7.2.2.8 Clé TEK

Description

Cet attribut contient une grandeur de 8 octets qui est une clé TEK selon la norme DES, cryptée par une clé de cryptage de clés calculée sur la clé d'autorisation. Les clés TEK sont cryptées au moyen du mode cryptage-décryptage-cryptage (EDE, *encrypt-decrypt-encrypt*) du triple algorithme DES à deux clés. Voir détails au § 10.



Type

8 pour clé TEK

Longueur

8

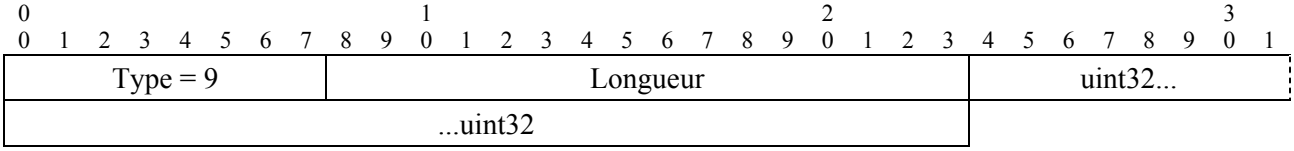
Chaîne

Grandeur de 64 bits représentant une clé de cryptage de trafic cryptée (par mode EDE à triple algorithme DES sur 2 clés).

7.2.2.9 Durée de vie de clé

Description

Cet attribut contient la durée de vie, exprimée en secondes, d'une clé d'autorisation ou d'une clé TEK. Il s'agit d'une grandeur non signée de 32 bits qui représente le nombre de secondes pendant lesquelles la clé associée restera valide.



Type

9 pour durée de vie de clé

Longueur

4

uint32

Grandeur de 32 bits représentant la durée de vie d'une clé

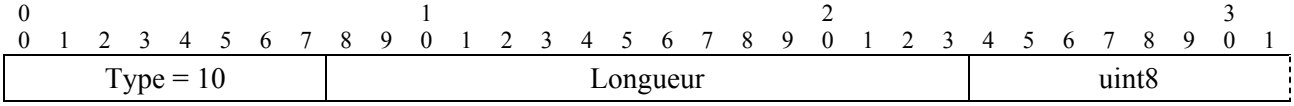
Une valeur zéro de durée de vie de clé indique que la clé d'autorisation ou de cryptage de trafic correspondante n'est pas valide.

7.2.2.10 Numéro de séquence de clé

Description

Cet attribut contient un numéro de séquence de 4 bits destiné à une clé TEK ou d'autorisation. Cette grandeur de 4 bits est cependant mémorisée dans un seul octet, dont les 4 éléments binaires de plus fort poids sont mis à 0.

Un résumé du format de l'attribut "Numéro de séquence de clé" est représenté ci-dessous. Les champs sont transmis de gauche à droite.



Type

10 pour le numéro de séquence de clé

Longueur

1

uint8

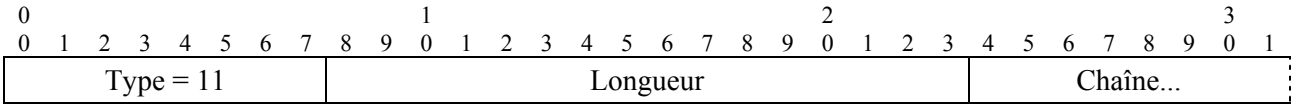
Numéro de séquence de 4 bits

7.2.2.11 Résumé HMAC

Description

Cet attribut contient une dispersion sur clé calculée pour l'authentification des messages. L'algorithme HMAC est défini dans [RFC 2104] qui spécifie l'utilisation d'un algorithme générique de dispersion cryptographique. La confidentialité de base fait appel à une version particulière de l'algorithme HMAC, qui est l'algorithme de dispersion sécurisée (SHA-1) défini dans la référence [FIPS-180-2].

Un résumé du format de l'attribut "Résumé HMAC" est représenté ci-dessous. Les champs sont transmis de gauche à droite.



Type

11 pour résumé HMAC

Longueur

20 octets

Chaîne

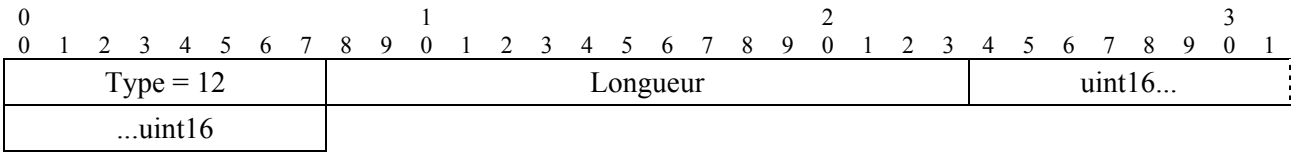
Dispersion SHA calculée sur 160 bits (20 octets)

7.2.2.12 Identificateur SAID

Description

Cet attribut contient un identificateur d'association de sécurité (SAID) de 14 bits qui est utilisé par l'interface BPI+ comme identificateur d'association de sécurité. Les deux bits de plus fort poids seront mis à zéro.

NOTE – Un identificateur SAID primaire d'interface BPI+ de CM est égal à l'identificateur SID primaire de ce CM.



Type

12 pour l'identificateur SAID

Longueur

2

uint16

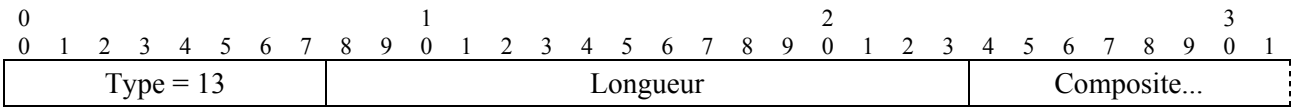
Grandeur de 16 bits représentant un identificateur SAID

7.2.2.13 Paramètres de clé TEK

Description

Cet attribut composite est formé d'un ensemble de sous-attributs qui représentent tous les paramètres de sécurité relatifs à une génération particulière d'une clé TEK d'identificateur SAID.

Un résumé du format de l'attribut "Paramètres de clé TEK" est représenté ci-dessous. Les champs sont transmis de gauche à droite.



Type

13 pour les paramètres de clé TEK

Longueur

33

Composite

Le champ "Composite" contient les sous-attributs suivants:

Tableau 7-19/J.125 – Sous-attributs de l'attribut "Paramètres de clé TEK"

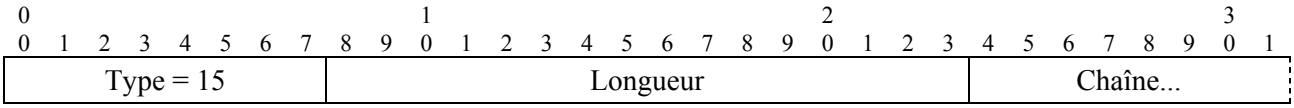
Attribut	Contenu
TEK	Clé TEK chiffrée (en mode EDE à triple algorithme DES sur deux clés) avec la clé KEK
Durée de vie de clé	Durée de vie restante de clé TEK
Numéro de séquence de clé	Numéro de séquence de clé TEK
Vecteur d'initialisation de concaténation CBC	Vecteur d'initialisation de concaténation de blocs chiffrants (CBC, *cipher block chaining*)

7.2.2.14 Vecteur d'initialisation CBC

Description

Cet attribut contient une valeur de 64 bits (8 octets) spécifiant un vecteur d'initialisation de concaténation de blocs chiffrants (CBC).

Un résumé du format de l'attribut "Vecteur d'initialisation CBC" est représenté ci-dessous. Les champs sont transmis de gauche à droite.



Type

15 pour le vecteur d'initialisation de concaténation CBC

Longueur

8 octets

Chaîne

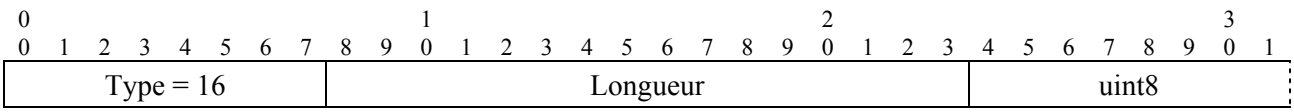
Grandeur de 64 bits représentant un vecteur d'initialisation CBC à codage DES.

7.2.2.15 Code d'erreur

Description

Cet attribut contient un code d'erreur sur un octet donnant des informations complémentaires sur un événement de rejet d'autorisation, de rejet de clé, d'autorisation non valide ou de clé TEK non valide.

Un résumé du format de l'attribut "Code d'erreur" est représenté ci-dessous. Les champs sont transmis de gauche à droite.



Type

16 pour le code d'erreur

Longueur

1

uint8

Code d'erreur sur 1 octet

Un système CMTS DOIT inclure l'attribut "Code d'erreur" dans tous les messages de rejet d'autorisation, d'autorisation non valide, de rejet de clé et de clé TEK non valide et les messages de rejet de mappage SA. Le CMTS PEUT employer les codes d'erreur autres que zéro listés ci-dessous pour les autres types de message BPI+. Le Tableau 7-20 énumère les valeurs de code à utiliser dans cet attribut. Le CMTS PEUT employer les codes d'erreur autres que zéro énumérés ci-dessous pour les messages de rejet de mappage SA; Il PEUT cependant renvoyer une valeur de code égale à zéro (0). Les valeurs de code d'erreur autres que celles qui sont définies dans le Tableau 7-20 DOIVENT être ignorées. Le renvoi d'une valeur de code égale à zéro ne communique au CM aucune information d'échec additionnelle, ce qui peut être utile pour des raisons de sécurité.

Tableau 7-20/J.125 – Valeur de code de l'attribut "Code d'erreur"

Code d'erreur	Messages	Description
0	Tous	Pas d'information
1	Rejet d'aut., aut. non valide	CM non autorisé
2	Rejet d'aut., rejet de clé	SAID non autorisé
3	Aut. non valide	Message non sollicité
4	Aut. non valide, clé TEK non valide	Numéro non valide de séquence de clé
5	Aut. non valide	Echec d'authentification de message (demande de clé)
6	Rejet d'aut.	Rejet d'autorisation permanent
7	Rejet de mappage	Non autorisé pour flux de trafic aval demandé
8	Rejet de mappage	Flux de trafic aval non mappé sur BPI+ SAID
9	Rejet d'aut.	Heure légale non acquise

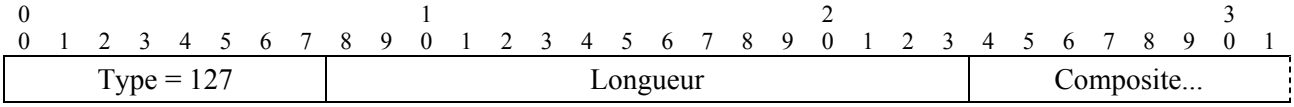
Le code d'erreur 6 (rejet d'autorisation permanent) sert à indiquer un certain nombre de situations d'erreur différentes qui affectent l'échange d'autorisation de la gestion BPKM. Il s'agit des suivantes:

- un fabricant inconnu, à savoir le système CMTS, ne possède pas le certificat CA appartenant à l'émetteur d'un certificat de CM;
- le certificat de CM porte une signature non valide;
- il y a eu un échec d'analyse ASN.1 au cours de la vérification du certificat de CM;
- le certificat CM est sur la "liste rouge";
- il y a des incohérences entre les données du certificat et celles des attributs BPKM qui l'accompagnent;
- le CM et le CMTS ont des capacités de sécurité incompatibles.

Leur caractéristique commune est que la situation d'échec est considérée comme permanente: d'éventuels réessais lors de l'autorisation continueront à se traduire par des rejets d'autorisation. Les détails relatifs à la cause d'un rejet d'autorisation permanent PEUVENT être signalés au CM dans un attribut facultatif de chaîne d'affichage pouvant accompagner l'attribut de code d'erreur dans des messages de rejet d'autorisation. Le CMTS DEVRAIT offrir la capacité de vérifier administrativement si des détails additionnels ont été envoyés au CM. Le CMTS PEUT journaliser ces échecs d'autorisation ou même les envoyer à un gestionnaire SNMP.

7.2.2.16 Défini par le vendeur

L'attribut "Défini par le vendeur" est un composite dont le premier sous-attribut DOIT être l'attribut "Identificateur du fabricant". L'attribut ou les attributs suivants sont définis par l'utilisateur, avec des valeurs de type attribuées par le vendeur désigné par l'attribut "Identificateur du fabricant" précédent.



Type

127 pour "Défini par le vendeur"

Longueur

≥ 6

Composite

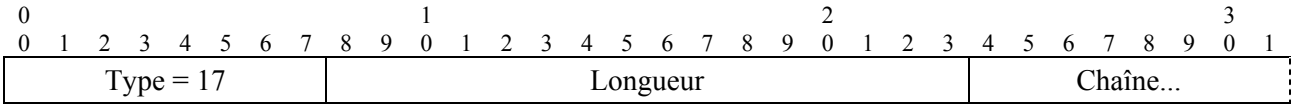
Le premier sous-attribut DOIT être l'identificateur du fabricant. Les attributs suivants peuvent inclure aussi bien des types universels (c'est-à-dire définis dans le cadre de la présente Recommandation) que des types définis par le vendeur, celui-ci étant identifié dans le précédent sous-attribut d'identificateur de fabricant.

7.2.2.17 Certificat CA

Description

Cet attribut est une chaîne contenant un certificat CA X.509 tel que défini dans [X.509].

Un résumé du format de l'attribut "Certificat CA" est représenté ci-dessous. Les champs sont transmis de gauche à droite.



Type

17 pour certificat CA

Longueur

Variable. La longueur NE DOIT PAS provoquer un dépassement de la longueur maximale autorisée d'un message de gestion MAC résultant.

Chaîne

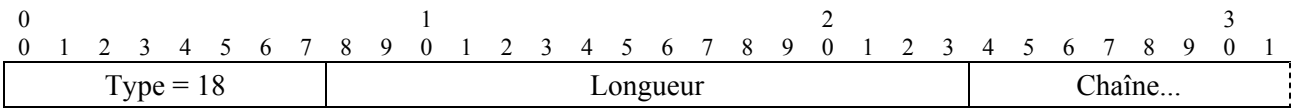
Certificat CA X.509 (en notation ASN.1 codée par les règles DER)

7.2.2.18 Certificat de CM

Description

Cet attribut est une chaîne contenant un certificat X.509 d'utilisateur de câblo-modem, comme défini dans [X.509].

Un résumé du format de l'attribut "Certificat de CM" est représenté ci-dessous. Les champs sont transmis de gauche à droite.



Type

18 pour certificat du CM

Longueur

Variable. La longueur NE DOIT PAS provoquer un dépassement de la longueur maximale autorisée du message de gestion MAC.

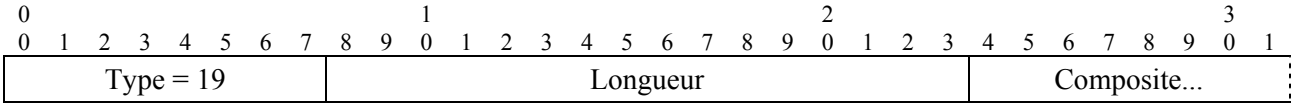
Chaîne

Certificat X.509 d'utilisateur (ASN.1 à codage DER)

7.2.2.19 Capacités de sécurité

Description

L'attribut "Capacités de sécurité" est un composite dont les sous-attributs désignent la version d'interface BPI+ ainsi que la ou les suites cryptographiques qui sont prises en charge par un CM.



Type

19 pour capacités de sécurité

Longueur

≥ 9

Composite

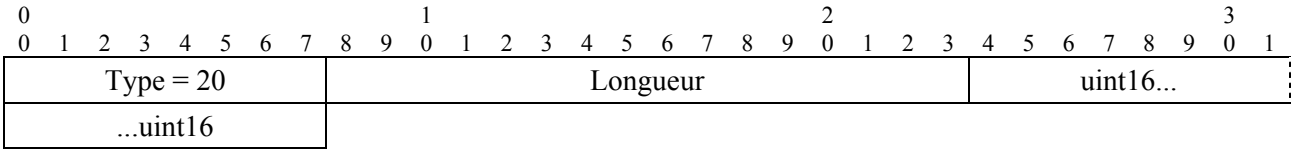
Le champ Composite contient les sous-attributs suivants:

Tableau 7-21/J.125 – Sous-attributs de capacités de sécurité

Attribut	Contenu
Liste de suites cryptographiques	Liste des suites cryptographiques prises en charge
Version d'interface BPI	Version d'interface BPI+ prises en charge

7.2.2.20 Suite cryptographique

Description



Type

20 pour suite cryptographique

Longueur

2

uint16

Entier de 16 bits désignant un appariement d'un algorithme de cryptage de données (codé dans l'octet de plus fort poids situé à gauche) et un algorithme d'authentification de données (codé dans l'octet de plus faible poids situé à droite). Actuellement, les normes DES à

56 bits et à 40 bits sont les seuls algorithmes spécifiés pour utilisation dans le cadre de la sécurité DOCSIS. Aucun d'eux n'est apparié à un algorithme d'authentification de données.

Tableau 7-22/J.125 – Identificateurs d'algorithme de cryptage de données

Valeur	Description
0	Champ réservé
1	Mode CBC, DES à 56 bits
2	Mode CBC, DES à 40 bits
3-255	Champ réservé

Tableau 7-23/J.125 – Identificateurs d'algorithme d'authentification de données

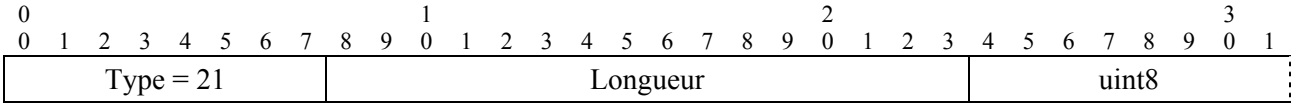
Valeur	Description
0	Pas d'authentification de données
1-255	Champ réservé

Tableau 7-24/J.125 – Valeurs de l'attribut "Suite cryptographique"

Valeur	Description
256 (0x0100 hex)	Mode CBC DES à 56 bits et pas d'authentification de données
512 (0x0200 hex)	Mode CBC DES à 40 bits et pas d'authentification de données
Toutes valeurs restantes	Champ réservé

7.2.2.21 Liste de suites cryptographiques

Description



Type

21 pour Liste de suites cryptographiques

Longueur

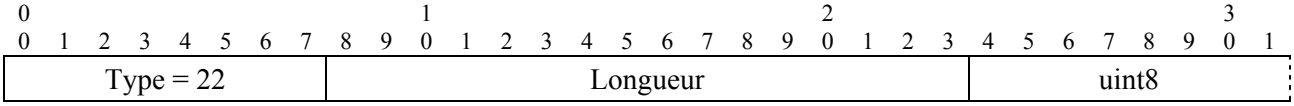
2 × n, où n est le nombre de suites cryptographiques énumérées

uint8

Liste de paires d'octets désignant un ensemble de suites cryptographiques. Chaque paire d'octets représente une suite cryptographique prise en charge, avec un codage identique au champ de valeur de l'attribut "Suite cryptographique" (§ 7.2.2.20). Le système CMTS NE DOIT PAS interpréter l'ordre relatif des paires d'octets dans cette liste comme indiquant des préférences entre les suites cryptographiques que ce système prend en charge.

7.2.2.22 Version d'interface BPI

Description



Type

22 pour Version d'interface BPI

Longueur

1

uint8

Code de 1 octet désignant une version de la sécurité par confidentialité de base.

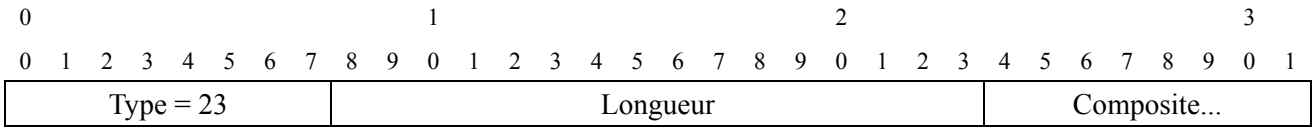
Tableau 7-25/J.125 – Valeurs de l'attribut "Version d'interface BPI"

Valeur	Description
0	Champ réservé
1	BPI+
2-255	Champ réservé

7.2.2.23 Descripteur d'association SA

Description

L'attribut "Descripteur d'association SA" est un composite dont les sous-attributs décrivent les propriétés d'une association de sécurité à l'interface BPI+. Ces propriétés se composent de l'identificateur SAID, du type d'association SA et de la suite cryptographique employée dans l'association SA.



Type

23 pour descripteur(s) SA

Longueur

14

Composite

Le champ Composite contient les sous-attributs suivants:

Tableau 7-26/J.125 – Sous-Attributs "Descripteur d'association SA"

Attribut	Contenu
SAID	Identificateur d'association de sécurité
Type d'association SA	Type de SA

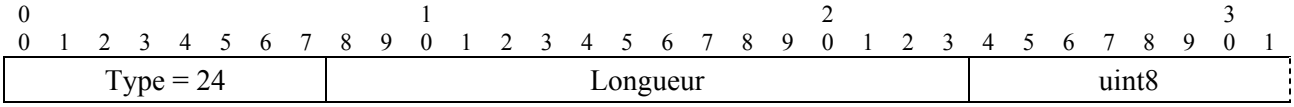
Tableau 7-26/J.125 – Sous-Attributs "Descripteur d'association SA"

Attribut	Contenu
Suite cryptographique	Appariement des algorithmes de cryptage de données et d'authentification de données employés à l'intérieur de l'association SA

7.2.2.24 Type d'association SA

Description

Cet attribut désigne le type d'association SA. L'interface BPI+ définit trois types d'association SA: primaire, statique, dynamique.



Type

24 pour Type d'association SA

Longueur

1

uint8

Code de 1 octet indiquant la valeur du type SA comme défini dans le Tableau 7-27.

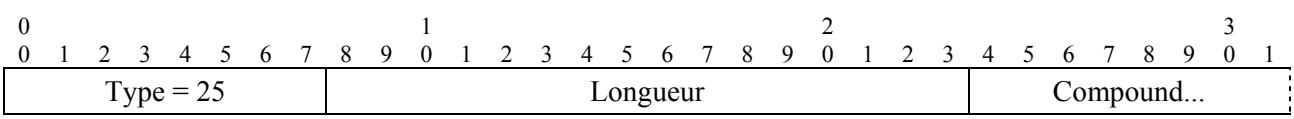
Tableau 7-27/J.125 – Valeurs de l'attribut "Type d'association SA"

Valeur	Description
0	Primaire
1	Statique
2	Dynamique
3-127	Champ réservé
128-255	Propre au vendeur

7.2.2.25 Recherche d'association SA

Description

Attribut composite utilisé dans une demande de mappage SA afin de spécifier des arguments de recherche de mappage. Ces arguments se composent du type de recherche et de tous attributs d'adressage relevant de ce type de recherche. Les attributs d'adressage se rapportent à un flux de trafic aval particulier pour lequel un mappage SA est déjà demandé. Actuellement, le seul type de recherche spécifié est la multidiffusion IP et l'argument associé à ce type est une adresse de groupe IP.



Type

25 pour Recherche d'association SA

Longueur

11

Composite

Le champ Composite contient les sous-attributs suivants:

Tableau 7-28/J.125 – Sous-Attributs "Recherche d'association SA"

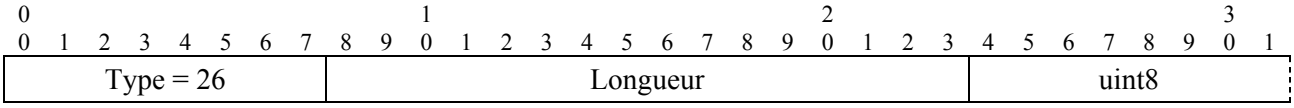
Attribut	Contenu
Recherche de type d'association SA	Type de recherche
Adresse IP	Requis si Recherche de type d'association SA = multidiffusion IP; contient une adresse de groupe IP dont le mappage SA est déjà demandé.

7.2.2.26 Type de recherche SA

Description

Cet attribut désigne une adresse IP servant à identifier un flux de trafic IP crypté. Il est utilisé par exemple afin de spécifier une adresse de groupe multidiffusé IP.

Un résumé du format de l'attribut "Type de recherche SA" est représenté ci-dessous. Les champs sont transmis de gauche à droite.



Type

26 pour Recherche de type d'association SA

Longueur

1

uint8

Code de 1 octet désignant la valeur du type de recherche SA comme défini dans le Tableau 7-29.

Tableau 7-29/J.125 – Valeur de l'attribut "Type de recherche SA"

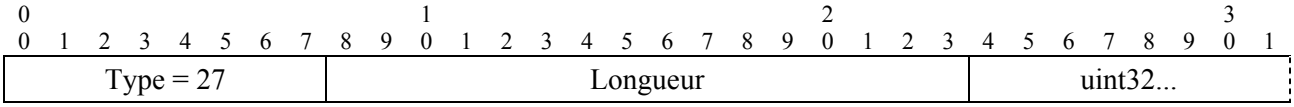
Valeur	Description
0	Champ réservé
1	Multidiffusion IP
2-127	Champ réservé
128-255	Propre au vendeur

7.2.2.27 Adresse IP

Description

Cet attribut désigne une adresse IP utilisée pour identifier un flux de trafic IP crypté. Il est utilisé, par exemple, pour spécifier une adresse de groupe multidiffusé IP.

Un résumé du format de l'attribut "Type de recherche SA" est représenté ci-dessous. Les champs sont transmis de gauche à droite.



Type

27 pour l'adresse IP

Longueur

4

uint32

Contient l'entier non signé de 32 bits (dans l'ordre des octets du réseau) représentant une adresse IP.

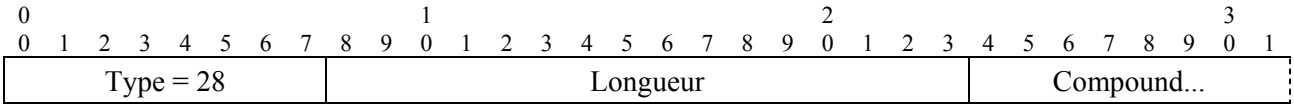
7.2.2.28 Paramètres de téléchargement

Description

Cet attribut est utilisé dans le fichier de code du câblo-modem défini au § B.3.1. Cet attribut est un attribut composé, constitué d'un ensemble de sous-attributs.

Un sous-attribut PEUT inclure l'un des deux ou les deux attributs suivants (dans cet ordre).

- Clé publique RSA (zéro ou un);
- Certificat CA (zéro, un ou plus).



Type

28

Longueur

≥ 0

8 Mappage dynamique d'association SA

8.1 Introduction

Les *associations de sécurité dynamiques (SA dynamiques)* de l'interface BPI+, présentées dans le § 5.1.3, sont les associations de sécurité qu'un système CMTS établit et élimine dynamiquement en réponse à son activation et à sa désactivation de flux de trafic aval spécifiques. Ces flux de trafic peuvent être créés par les mécanismes suivants:

- par un équipement des locaux client (CPE, *customer premises equipment*) rattaché à l'un des CM clients du CMTS;
- par un serveur d'applications contenu dans la tête de réseau;
- par un système OSS;
- ou par d'autres mécanismes non spécifiés.

Quelle que soit l'origine du déclenchement de l'établissement d'une association SA dynamique à l'intérieur du système CMTS, les CM clients ont besoin d'un mécanisme de détection du mappage d'un flux de trafic aval particulier et protégé par interface BPI+ sur l'association de sécurité BPI+ attribuée dynamiquement à ce flux (et sur l'identificateur SAID correspondant à cette association SA).

L'automate à états de mappage SA défini dans le présent paragraphe spécifie la façon dont les câblo-modems consultent un système CMTS au sujet du mappage de flux de trafic aval sur des associations SA dynamiques. L'automate à états commande la transmission à un CMTS de messages de demande de mappage SA.

DOCSIS 1.1 et DOCSIS 2.0 utilisent actuellement des associations SA dynamiques pour un seul type de service: le cryptage, ce qui limite l'accès au trafic multidiffusé IP en aval. Un système CMTS peut établir ou éliminer des associations SA dynamiques en réponse à des modifications dans l'appartenance à des groupes IP dans des équipements CPE aval. Les mécanismes de gestion par protocole IGMP de DOCSIS 1.1 ou 2.0 ([J.112-B], § B.5.3.1 ou [J.122], § 5.3.1), peuvent déclencher l'établissement d'associations SA dynamiques dans le CMTS. Les mécanismes de gestion par protocole IGMP dans le CM DOIVENT déclencher les messages de demande de mappage BPI+ recherchant dans le CMTS le mappage sur une association SA d'une adresse de groupe multidiffusé IP.

Le mécanisme de mappage SA de l'interface BPI+ PEUT mapper un groupe multidiffusé IP sur une association SA statique ou même sur une association SA primaire d'un CM particulier. Une réponse de CMTS à une demande de mappage peut renvoyer l'un quelconque des trois types d'association SA. Le mécanisme de mappage SA est cependant le seul qui permette à un CM de connaître l'identité d'associations SA dynamiques.

Le paragraphe 8.4 analysera plus en détail l'usage particulier du mécanisme de mappage SA pour prendre en charge le mappage du trafic multidiffusé IP sur des associations SA dynamiques. Les deux paragraphes suivants seront cependant consacrés au mécanisme plus général de mappage SA.

NOTE – De futures améliorations des spécifications de service DOCSIS pourront définir d'autres applications des associations SA dynamiques.

8.2 Théorie du fonctionnement

L'interface BPI+ définit trois nouveaux messages de gestion BPKM afin de prendre en charge la recherche de mappages SA par un CM: la demande de mappage SA, la réponse de mappage SA et le rejet de mappage SA. Un CM envoie une demande de mappage SA à son système CMTS afin de demander le mappage d'un flux aval connu sur une association de sécurité. Cette demande de mappage transporte les attributs de données BPI+ identifiant le CM demandeur et le flux de trafic aval dont le mappage SA est demandé.

Le CMTS DOIT répondre à une demande de mappage:

- soit par une réponse de mappage fournissant au CM le mappage SA demandé;
- soit par un rejet de mappage signalant au CM que:
    1) le CM n'est pas autorisé à recevoir le flux de trafic indiqué dans la demande de mappage;
    2) le flux de trafic demandé n'est pas mappé sur une association SA d'interface BPI+.

Si le CM ne reçoit ni l'une ni l'autre des réponses ci-dessus au cours d'une période configurable de temporisation avant réessai, il procède à l'envoi d'une nouvelle demande de mappage. Si aucune réponse n'est reçue après un nombre maximal configurable de réessais, le CM abandonne.

Si le CM reçoit un rejet de mappage, il cesse toutes nouvelles tentatives d'obtention du mappage. Si l'accès au flux de trafic aval est mappé sur une association SA d'interface BPI+ et si le CM demandeur n'est pas autorisé à accéder à cette SA, l'accès est refusé à ce CM et à son équipement CPE connexe parce que le CM ne peut pas obtenir le matériel de calcul de clés nécessaire pour déchiffrer les flux de trafic aval cryptés aux termes de cette association de sécurité. Si le flux de trafic demandé n'est pas chiffré (c'est-à-dire s'il n'est pas mappé sur une association de sécurité), le trafic non chiffré sera simplement réexpédié vers l'équipement CPE connexe. Par exemple, un câblo-modem fait une demande SA-MAP pour l'adresse multidiffusée All-Hosts. Comme les

paquets multidiffusés adressés à l'adresse multidiffusée All-Hosts sont nécessaires à l'exploitation correcte du protocole Internet de gestion de groupe (IGMP, *Internet group management protocol*), il n'est pas nécessaire de crypter ces paquets

Si le CM reçoit une réponse de mappage désignant l'association SA d'interface BPI+ correspondant au flux de trafic aval demandé, le CM lance un automate à états de clé TEK pour l'association SA à condition:

1) que le CM n'ait pas déjà lancé un automate à états de clé TEK pour cette association SA;

2) que le CM prenne en charge la suite cryptographique indiquée dans la réponse de mappage ainsi que la valeur d'identificateur d'association de sécurité (SAID).

Le CM peut avoir déjà lancé un automate à états de clé TEK si l'association SA mappée est:

- une association SA dynamique qui a été mappée sur un autre flux de trafic protégé auquel le CM a accès;
- une association SA primaire du CM demandeur;
- une association SA statique dont le CM a été informé dans une réponse d'autorisation reçue précédemment.

Un système CMTS PEUT attribuer plusieurs flux de trafic (par exemple, des adresses IP multicast) à la même association SA. Si plusieurs flux de trafic aval sont cryptés aux termes de la même association SA dynamique, un CM peut déjà avoir lancé un automate à états de clé TEK pour l'association SA désignée dans la réponse de mappage. Le mappage SA renvoyé dans la réponse de mappage peut ne pas concerner une association SA dynamique car le flux de trafic demandé peut être mappé sur une association de sécurité primaire ou statique du CM.

La réponse de mappage contient un attribut "Descripteur d'association SA" qui désigne à la fois un identificateur SAID et la suite cryptographique utilisée dans l'association SA. Comme dans le cas des associations SA statiques, la sélection d'une suite cryptographique est normalement effectuée indépendamment des capacités cryptographiques du CM demandeur. Un CMTS PEUT donc répondre à une demande de mappage par une SA (statique ou dynamique) faisant appel à une suite cryptographique que le CM demandeur ne prend pas en charge. Le CM NE DOIT PAS lancer d'automate à états de clé TEK pour des associations SA statiques ou dynamiques dont les suites cryptographiques ne sont pas prises en charge par le CM. (Une SA primaire doit cependant utiliser une suite cryptographique prise en charge par le CM auquel cette SA appartient.)

L'automate à états de clé TEK commande l'extraction du matériel de calcul de clés de l'association SA mappée. Le CM envoie au sujet de l'association SA des demandes de clé auxquelles le CMTS peut répondre comme suit:

- par une réponse de clé fournissant au CM le matériel de calcul de clés demandé;
- par un rejet de clé signalant au CM qu'il n'est pas autorisé à recevoir l'identificateur SAID dont le mappage a été demandé;
- par un message d'autorisation non valide signalant au CM que l'authentification du message de demande de clé a échoué.

La réception d'un message de rejet de clé force la fermeture de l'automate à états de clé TEK.

Il existe deux mécanismes permettant au CMTS d'informer un CM client qu'il n'est pas autorisé à accéder à un flux de trafic particulier: soit répondre à une demande de mappage par un rejet de mappage, soit répondre à une demande de clé par un rejet de clé. Selon l'implémentation, un CMTS vérifiera l'état d'autorisation d'un CM avant de répondre à une demande de mappage. En effectuant cette vérification au cours de l'échange de mappage, un CM sera empêché de lancer inutilement un automate à états de clé TEK et d'envoyer une demande de clé pour un identificateur SAID auquel il n'est pas autorisé à accéder.

8.3 Automate à états de mappage SA

L'automate à états de mappage SA spécifie le mécanisme permettant à un CM de connaître le mappage d'un flux de service sur une association SA dynamique.

Un automate à états est lancé lorsqu'un événement externe à l'automate à états de mappage SA rend nécessaire un mappage de flux de trafic sur une association SA (par exemple lorsqu'un CM installe les filtres d'autorisation d'un groupe multidiffusé IP en réponse à des mécanismes de gestion IGMP du CM). Cet événement externe produit un événement "de mappage" interne dans l'automate à états de mappage SA.

L'automate à états est fermé si le CM ne reçoit pas de réponse après l'envoi du nombre maximal de nouvelles demandes ou lorsque le CM détermine qu'il n'a plus besoin du matériel de calcul de clés de l'association SA mappée. Dans ce dernier cas, un événement externe produit un événement interne de "démappage" dans l'automate à états de mappage SA, ce qui en force la fermeture. L'automate à états peut donc être utilisé afin non seulement d'obtenir les informations de mappage requises mais aussi de suivre la période pendant laquelle une application externe, utilisant le mécanisme de mappage SA (par exemple, la gestion IGMP), nécessite le mappage. L'association d'un événement de démappage à un événement externe, et donc l'implémentation de cet événement de démappage, est FACULTATIVE.

Comme dans le cas des automates à états d'autorisation et de clé TEK de l'interface BPI+, l'automate à états de mappage SA est présenté sous forme graphique en tant que modèle de fluence d'état (Figure 8-1) et sous forme tabulaire en tant que matrice de transition d'état (Tableau 8-1). Et, comme dans les automates à états déjà définis, la matrice de transition d'état DOIT être utilisée comme spécification définitive des actions protocolaires associées à chaque association d'état.

Si, au moyen du mécanisme de mappage SA, un CM apprend qu'il a besoin d'accéder à un matériel de calcul de clés d'association SA dynamique, ce CM doit établir un automate à états de clé TEK pour cette association SA dynamique. Bien que l'automate à états d'autorisation commande l'établissement et la fermeture des automates à états de clé TEK associés aux identificateurs SAID primaires et éventuellement statiques, il ne commande pas l'établissement et la fermeture des automates à états de clé TEK associés à des associations SA dynamiques. Les CM DOIVENT implémenter la logique nécessaire pour établir et fermer les automates à états de clé TEK pour les associations SA dynamiques détectées au moyen du mécanisme de mappage SA. La spécification BPI+ ne définit cependant pas la façon dont il convient que les CM gèrent leurs automates à états de clé TEK pour associations SA dynamiques.

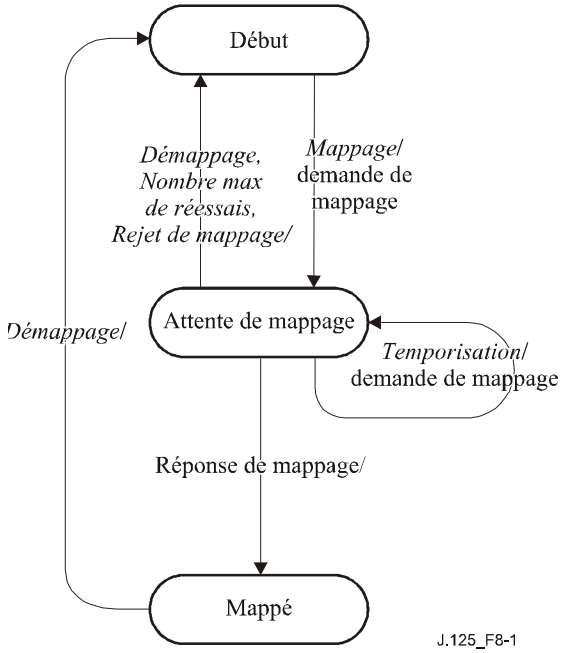


Figure 8-1/J.125 – Organigramme de l'automate à états de mappage SA

Tableau 8-1/J.125 – Matrice de transition d'état d'identificateur SAID dynamique

Etat / ***Evénement ou message reçu***	**(A) Début**	**(B) Attente de mappage**	**(C) Mappé**
(1) Mappage	Attente de mappage		
(2) *Démappage*		Début	Début
(3) *Réponse de mappage*		Mappé	
(4) *Rejet de mappage*		Début	
(5) *Fin de temporisation*		Attente de mappage	
(6) *Nombre max. de réessais*		Début	

8.3.1 Etats

8.3.1.1 Début

Etat initial de l'automate à états finis.

8.3.1.2 Attente de mappage

Le CM a envoyé au CMTS une demande de mappage et en attend la réponse.

8.3.1.3 Mappé

Le CM a reçu une réponse de mappage et a été informé du mappage SA demandé.

8.3.2 Messages

8.3.2.1 Demande de mappage SA (Demande de mappage)

Message envoyé par le CM au CMTS afin de demander un mappage SA.

8.3.2.2 Réponse de mappage SA (Réponse de mappage)

Réponse favorable du CMTS à une demande de mappage contenant le mappage SA demandé.

8.3.2.3 Rejet de mappage SA (Rejet de mappage)

Réponse défavorable du CMTS à une demande de mappage du CM. Ce message signale au CM soit:

1) que celui-ci n'est pas autorisé à accéder au flux de trafic désigné dans la demande de mappage;
2) que le flux de trafic demandé n'est pas mappé sur une association SA à l'interface BPI+.

8.3.3 Evénements

8.3.3.1 Mappage

Cet événement déclenche le début de l'automate à états de mappage SA. L'événement de mappage est lié à un événement de CM externe au protocole BPI+.

8.3.3.2 Démappage

Cet événement déclenche la fermeture de l'automate à états de mappage SA. L'événement de démappage est lié à un événement de CM externe au protocole BPI+. L'implémentation de l'événement de démappage est FACULTATIVE.

8.3.3.3 Réponse de mappage

Le câblo-modem reçoit un message de réponse de mappage SA.

8.3.3.4 Rejet de mappage

Le câblo-modem reçoit un message de rejet de mappage SA.

8.3.3.5 Temporisation

Le câblo-modem a effectué la temporisation d'attente de réponse à un message en instance de demande de mappage SA.

8.3.3.6 Nombre maximal de réessais

Le câblo-modem a envoyé le nombre maximal de réessais et n'a pas reçu de réponse.

8.3.4 Paramètres

Toutes les valeurs paramétriques de configuration sont spécifiées dans le fichier paramétrique téléchargé par protocole TFTP (voir Annexe A).

8.3.4.1 Temporisation d'attente de mappage SA

Période de temporisation qui s'écoule entre les envois de message de demande de mappage SA à partir de l'état d'attente SA. Voir le § A.1.1.1.8.

8.3.4.2 Nombre maximal de réessais de mappage SA

Nombre maximal de fois qu'un CM réessaye une demande de mappage SA avant d'abandonner.

8.3.5 Actions

Les actions effectuées en association avec les transitions d'état sont énumérées ci-dessous par l'expression <événement/message reçu> → <état>:

1-A Début (*mappage*) → Attente de mappage

- envoi d'une demande de mappage SA;
- armement du temporisateur de nouvelle demande de mappage en temporisation d'attente de mappage;
- remise à zéro du compteur de réessais de mappage.

2-B Attente de mappage (*démappage*) → Début

- réinitialisation du temporisateur de réessais de demande de mappage;
- fermeture de l'automate à états de mappage SA.

2-C Mappé (*démappage*) → Début

- fermeture de l'automate à états de mappage SA.

3-B Attente de mappage (*réponse de mappage*) → Mappé

- réinitialisation du temporisateur de nouvelle de demande de mappage.

4-B Attente de mappage (*rejet de mappage*) → Début

- réinitialisation du temporisateur de nouvelle demande de mappage;
- fermeture de l'automate à états de mappage SA.

5-B Attente de mappage (*temporisation*) → Attente de mappage

- envoi d'une demande de mappage SA;
- armement du temporisateur de nouvelle demande de mappage en temporisation d'attente de mappage SA;
- incrémentation du compteur de réessais de mappage;
- si le décompte de réessais de mappage est supérieur au nombre maximal de réessais de mappage SA, l'événement de nombre maximal de réessais est généré.

6-B Attente de mappage (*nombre max. de réessais*) → Début

- fermeture de l'automate à états de mappage SA.

8.4 Trafic multidiffusé IP et associations SA dynamiques

DOCSIS 1.1 [J.112-B] et DOCSIS 2.0 [J.122] spécifient des règles pour la gestion du trafic IGMP dans le CM et dans le CMTS. Ces règles sont conçues afin de commander le flux de trafic multidiffusé IP dans le réseau en câble et de part et d'autre de l'interface CM/CPE, de façon que:

- un CMTS ne réexpédie que le trafic aval associé à un groupe multidiffusé IP si un équipement CPE, rattaché à l'un des CM clients du CMTS, fait partie de ce groupe; *et*
- un CM ne réexpédie de part et d'autre de son interface CPE, que le trafic aval associé à un groupe multidiffusé IP si un équipement CPE rattaché fait partie de ce groupe.

L'interface BPI+, fonctionnant en liaison avec l'interface RFI conforme à DOCSIS 1.1 ou 2.0, commande l'accès aux flux de trafic multidiffusé en les cryptant et en contrôlant la répartition du matériel de calcul de clés multidiffusé qui est requis pour déchiffrer les flux.

Un système CMTS peut mapper des flux multidiffusés aval sur l'une quelconque des trois classes d'association de sécurité à l'interface BPI+: primaire, statique ou dynamique. Si le trafic d'un groupe multidiffusé IP est mappé sur une association SA primaire, seul le CM particulier appartenant à

cette association SA peut accéder à ce groupe. S'il est mappé sur une SA statique ou dynamique, plusieurs CM peuvent accéder à ce groupe, bien qu'un CMTS puisse limiter une SA statique ou dynamique à un CM unique.

Lorsqu'un CM selon DOCSIS 1.1 ou 2.0 active la réexpédition aval d'un groupe multidiffusé IP (en réponse à la réception d'un rapport d'appartenance à son interface avec l'équipement CPE), ce CM DOIT déterminer si le trafic aval de ce groupe multidiffusé IP est crypté et si l'identificateur SAID de l'interface BPI+ est associé au flux multidiffusé aval crypté. Dès que le CM a obtenu l'identificateur SAID associé, il peut lancer un automate à états de clé TEK afin d'extraire le matériel de calcul de clés correspondant à cette association SA.

Le CM utilise le mécanisme de mappage SA de l'interface BPI+ afin de demander à son CMTS le mappage SA pour un groupe multidiffusé IP auquel il vient de se joindre. L'événement "Mappage" de l'automate à états de mappage SA est déclenché par l'activation, dans le CM, de la réexpédition du groupe multidiffusé IP dans le sens interface RF vers équipement CPE (voir le § B.5.3.1.2 et l'Annexe L de [J.112-B] ou le § 5.3.1.2 et l'Appendice V de [J.122]). Une réponse de mappage SA informe le CM que le groupe joint est mappé sur une association SA de l'interface BPI+. Si le groupe est mappé sur l'association SA primaire du CM, celui-ci possède déjà le matériel de calcul de clés nécessaire. Si le groupe est mappé sur une association SA statique ou dynamique, le CM détermine s'il a déjà lancé un automate à états de clé TEK pour cette association. Si ce n'est pas le cas, il en lance un.

L'automate à états de mappage SA définit un événement FACULTATIF de démappage qui ferme l'automate à états de mappage SA et qui PEUT servir à indiquer que le CM n'a plus besoin du matériel de calcul de clés de l'association SA mappée. Dans le cas du mappage d'un trafic multidiffusé IP sur une association SA, l'événement de démappage pourrait indiquer que le CM a supprimé tous les filtres d'autorisation de multidiffusion IP associés aux groupes multidiffusés IP qui ont été mappés sur l'association SA en question. L'automate à états de mappage SA PEUT donc servir à contrôler la nécessité qu'un CM conserve le matériel de calcul de clés pour une SA dynamique mappée sur un ou plusieurs groupes multidiffusés IP.

Les automates à états de clé TEK correspondant à des identificateurs SAID primaires et statiques sont fermés conformément aux conditions de fermeture définies dans les automates à états d'autorisation et de clé TEK.

9 Usage des clés

9.1 CMTS

Après avoir effectué son inscription DOCSIS MAC, un CM lance un échange d'autorisation avec son système CMTS. La première réception par le CMTS d'un message de demande d'autorisation issu du CM non autorisé déclenche l'activation d'une nouvelle clé d'autorisation (AK, *authorization key*) que le CMTS renvoie au CM demandeur dans un message de réponse d'autorisation. Cette clé AK restera active jusqu'à son expiration conformément à sa durée de vie prédéfinie dans le paramètre de configuration de système CMTS, *durée de vie de clé d'autorisation* (voir § A.2).

Le système CMTS DOIT utiliser le matériel de calcul de clés issu de la clé d'autorisation du CM afin:

- de vérifier le résumé HMAC contenu dans les demandes de clé reçues de ce CM;
- de chiffrer (en mode EDE à triple algorithme DES sur 2 clés) la clé TEK dans les réponses de clé qu'il envoie à ce CM (la clé TEK est un sous-attribut de l'attribut "Paramètres de clé TEK" contenu dans une réponse de clé);
- de calculer les résumés HMAC qu'il écrit dans les messages de réponse de clé, de rejet de clé et de clé TEK non valide qu'il envoie à ce CM.

Le système CMTS DOIT être en mesure d'envoyer une clé AK à un CM sur demande. Le CMTS DOIT être en mesure de prendre en charge deux clés AK simultanément actives pour chaque CM client. Le CMTS possède deux clés AK actives pendant une période de transition entre clés d'autorisation. Ces deux clés actives ont des durées de vie en chevauchement.

Une période de transition entre clés d'autorisation commence lorsque le CMTS reçoit une demande d'autorisation issue d'un CM et que ce CMTS possède une seule clé AK active pour ce CM. En réponse à cette demande d'autorisation, le CMTS active une deuxième clé AK qu'il renvoie au CM demandeur dans une réponse d'autorisation. Le CMTS DOIT régler la durée de vie active de cette seconde clé AK de façon qu'elle soit égale à la durée de vie restante de la première clé AK plus la durée prédéfinie dans le paramètre *durée de vie de clé d'autorisation*. La seconde clé "récente" restera donc active pendant une *durée de vie de clé d'autorisation* après l'expiration de la première clé "ancienne". La période de transition de clé se terminera à l'expiration de l'ancienne clé, comme cela est décrit dans la moitié supérieure de la Figure 9-1.

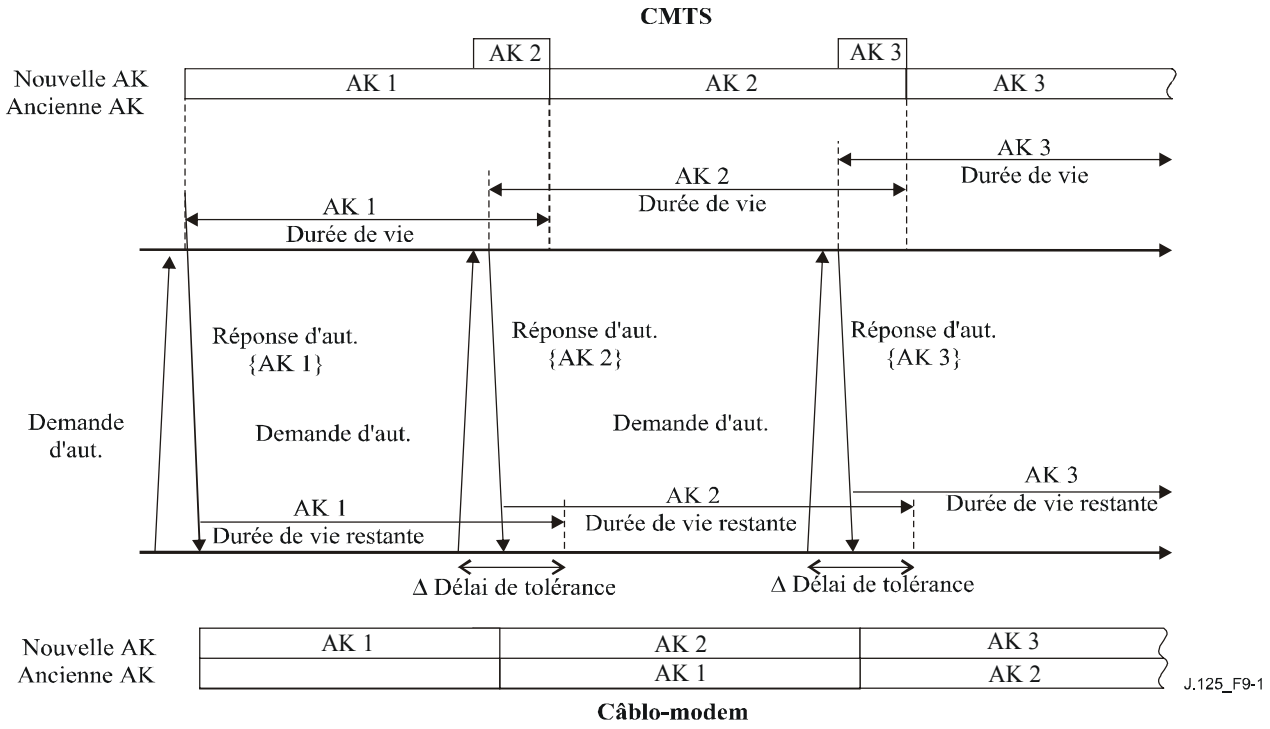


Figure 9-1/J.125 – Gestion de clés d'autorisation dans le CMTS et dans le CM

La durée de vie d'une clé d'autorisation qu'un système CMTS signale dans une réponse d'autorisation DOIT refléter, aussi précisément que l'implémentation le permet, la durée de vie restante des clés AK au moment de l'expédition du message de réponse.

Tant que le CMTS se trouve dans la période de transition entre clés d'autorisation d'un CM et détient donc deux clés d'autorisation actives pour ce CM, il répond aux demandes d'autorisation par la plus récente des deux clés actives. Une fois l'ancienne clé arrivée à expiration, une demande d'autorisation déclenche l'activation d'une nouvelle clé AK ainsi que le début d'une nouvelle période de transition entre clés.

Si un CM ne parvient pas à obtenir une réautorisation avant l'expiration de sa clé AK la plus actuelle, le CMTS ne détiendra plus de clés d'autorisation actives pour ce CM et considérera celui-ci comme *non autorisé*. Un CMTS DOIT supprimer de ses tables de calcul de clé toutes les clés TEK associées à une association SA primaire de CM non autorisé.

Un CMTS DOIT se servir de clé(s) AK active(s) d'un CM afin de vérifier le résumé HMAC contenu dans les demandes de clé reçues de ce CM. Si un CMTS reçoit une demande de clé alors qu'il se trouve dans une période de transition entre clés AK et que le numéro de séquence de clé AK correspondant indique que la demande a été authentifiée avec la plus récente des deux clés AK, le CMTS identifie ce fait comme étant un *acquittement implicite* de l'obtention par le CM de la plus récente des deux clés AK du CM.

Un CMTS DOIT se servir d'une clé AK active lors du calcul de résumés HMAC contenus dans des messages de réponse de clé, de rejet de clé et de clé non valide, ainsi que lors du cryptage de la clé TEK dans des réponses de clé. Lors de l'expédition de messages de réponse de clé, de rejet de clé ou de clé TEK non valide au cours d'une période de transition entre clés (c'est-à-dire lorsque deux clés AK sont actives) et si la clé la plus récente a été implicitement acquittée, le CMTS DOIT utiliser la plus récente des deux clés AK actives; si la clé récente n'a pas été implicitement acquittée, le CMTS DOIT utiliser la plus ancienne des deux clés AK actives.

La moitié supérieure de la Figure 9-1 décrit la politique du CMTS concernant son utilisation de clés AK.

Le CMTS DOIT conserver deux séries de clés actives de cryptage de trafic (avec leurs vecteurs d'initialisation CBC associés) pour chaque identificateur SAID. Ces clés correspondent à deux générations successives de matériel de calcul de clés et possèdent des durées de vie en chevauchement. La clé TEK la plus récente DOIT avoir un numéro de séquence de clé supérieur d'une unité (modulo 16) à celui de la clé TEK la plus ancienne. Chaque clé TEK devient active à mi-parcours de la durée de vie de la clé précédente et expire à mi-parcours de la durée de vie de la clé suivante. Dès que la durée de vie d'une clé TEK arrive à expiration, cette clé devient inactive et ne DOIT plus être utilisée.

Le CMTS effectue une transition différente entre les deux clés TEK actives selon que ces clés sont utilisées pour du trafic aval ou amont. Pour chacun de ses identificateurs SAID, le CMTS DOIT effectuer sa transition entre clés TEK actives conformément aux règles suivantes:

- le CMTS DOIT utiliser la plus ancienne des deux clés TEK actives afin de chiffrer le trafic aval. A l'expiration de l'ancienne clé TEK, le CMTS DOIT effectuer une transition immédiate vers l'utilisation de la nouvelle clé TEK pour le cryptage;
- pour le décryptage du trafic amont, une période de transition est définie à partir du moment où le CMTS a envoyé la nouvelle clé TEK à un CM dans un message de réponse de clé. La période de transition amont commence au moment où le CMTS envoie la nouvelle clé TEK dans un message de réponse de clé et elle se termine au moment où l'ancienne clé TEK arrive à expiration. Pendant la période de transition, le CMTS DOIT être en mesure de déchiffrer les trames amont au moyen de la clé TEK ancienne ou nouvelle.

Le CMTS ne crypte avec une clé TEK donnée que pendant la deuxième moitié de la durée de vie totale de cette clé. Le CMTS est cependant en mesure de déchiffrer avec une clé TEK pendant la durée de vie totale de cette clé.

Le champ KEY_SEQ de l'élément d'en-tête étendu (EH) à confidentialité de base désigne laquelle des deux clés TEK a été utilisée pour le cryptage des données en paquet d'une trame amont. Le bit TOGGLE de l'élément EH de confidentialité, qui est égal au bit de plus faible poids du champ KEY_SEQ, peut être utilisé par le CMTS pour identifier la clé TEK chiffrante.

La moitié supérieure de la Figure 9-2 décrit cette gestion par le CMTS de clés TEK d'une association de sécurité à l'interface BPI+.

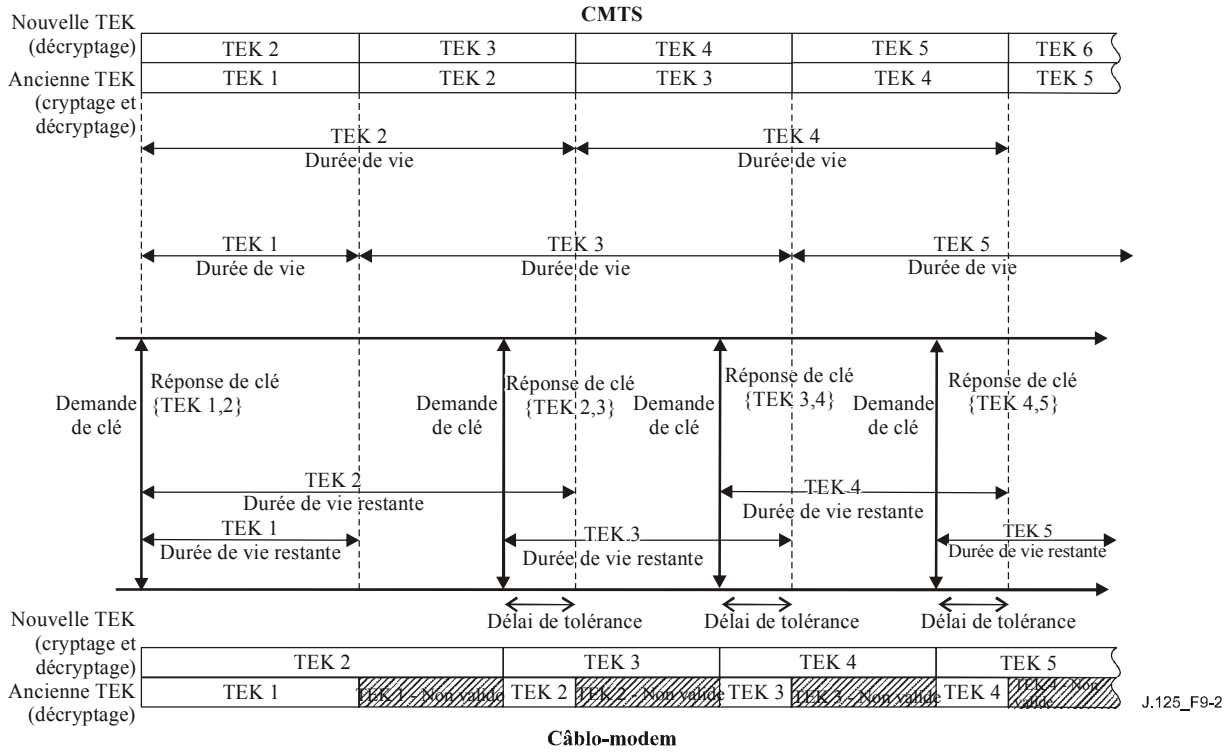


Figure 9-2/J.125 – Gestion de TEK dans le CMTS et le CM

Le CMTS est chargé de conserver comme indiqué ci-dessus les informations de calcul de clés pour les identificateurs SAID aussi bien primaires que multidiffusés. Le protocole de gestion BPKM qui est défini dans la présente Recommandation décrit un mécanisme de synchronisation de ces informations de calcul entre un CMTS et ses CM clients. Il appartient au CM de mettre à jour ses clés opportunément. Le CMTS effectuera sa transition vers une nouvelle clé chiffrante aval sans tenir compte du fait qu'un CM client a extrait une copie de cette clé TEK.

Les messages de réponse de clé envoyés par un CMTS contiennent des paramètres de clé TEK (la clé TEK proprement dite, sa durée de vie, son numéro de séquence et un vecteur d'initialisation de concaténation CBC-IV) pour les deux clés TEK actives. Les durées de vie signalées par un CMTS dans une réponse de clé DOIVENT refléter, aussi précisément que l'implémentation le permet, les durées de vies restantes de ces clés TEK au moment où le message de réponse de clé est envoyé.

9.2 Câblo-modem

Le CM est chargé d'obtenir l'autorisation de son système CMTS et de conserver une clé d'autorisation active. Un CM DOIT utiliser ses deux clés AK obtenues le plus récemment.

Les clés AK ont une durée de vie limitée et doivent être rafraîchies périodiquement. Un CM rafraîchit sa clé d'autorisation en renouvelant une demande d'autorisation auprès du CMTS. L'automate à états d'autorisation (§ 7.1.2) gère la programmation des demandes d'autorisation visant à rafraîchir des clés AK.

Un automate à états d'autorisation de CM programme le début de la réautorisation de façon qu'une période configurable (le *délai de tolérance d'autorisation*) s'écoule avant l'instant d'expiration programmé pour la plus récente clé AK du CM. Le délai de tolérance d'autorisation est configuré de façon à offrir au CM une période de réessais d'autorisation suffisamment longue pour tenir compte des retards du système et de façon à offrir au CM un temps suffisant pour réussir à effectuer un échange d'autorisation avant l'expiration de sa clé AK la plus actuelle.

NOTE – Le CMTS n'a pas besoin de connaître le délai de tolérance d'autorisation. Il s'informe cependant de la durée de vie de ses clés d'autorisation et DOIT désactiver une clé dès qu'elle a expiré.

Un câblo-modem DOIT utiliser la plus récente de ses deux plus récentes clés d'autorisation lors du calcul des résumés HMAC qu'il joint aux demandes de clé. Il DOIT être en mesure d'utiliser l'une ou l'autre de ses deux clés AK les plus récentes afin d'authentifier des messages de réponse de clé, de rejet de clé ou de clé TEK non valide et afin de déchiffrer une clé TEK chiffrée dans une réponse de clé. Le CM utilise le numéro de séquence de clé AK connexe afin de déterminer laquelle des deux clés AK il doit utiliser.

La moitié inférieure de la Figure 9-1 décrit la conservation et l'utilisation par le CM de ses clés d'autorisation.

Un CM DOIT être en mesure de conserver deux ensembles successifs de matériel de calcul de clés de trafic pour chaque identificateur SAID autorisé. Au moyen de ses automates à états de clé TEK, un CM s'efforce de toujours conserver les deux plus récents ensembles de matériel de calcul de clés de trafic pour chaque identificateur SAID.

Pour chacun de ses identificateurs SAID autorisés, le câblo-modem:

- DOIT utiliser la plus récente de ses deux clés TEK afin de chiffrer le trafic amont récemment reçu. Le trafic déjà mis en file d'attente PEUT utiliser l'une ou l'autre clé TEK (sans ordre particulier) pendant une brève période couvrant la transition de l'ancienne à la nouvelle clé.
- DOIT être en mesure de déchiffrer le trafic aval chiffré avec l'une ou l'autre des clés TEK.

Le champ KEY_SEQ dans l'élément EH à confidentialité de base désigne le numéro de séquence de la clé TEK utilisée pour chiffrer les données en paquet de l'unité PDU. Le bit TOGGLE contenu dans l'élément EH de confidentialité, qui est égal au bit de plus faible poids du champ KEY_SEQ, facilite la distinction entre deux générations de clé successives.

9.3 Authentification des demandes de service dynamique en mode DOCSIS v1.1/2.0

Si un CM conforme à DOCSIS 1.1 ou 2.0 est configuré de façon à activer l'interface BPI+, la spécification d'interface RFI de DOCSIS 1.1 [J.112-B] ou 2.0 [J.122] prescrit que le CM et le CMTS doivent inclure des résumés HMAC dans toutes les demandes d'addition de service dynamique (DSA-REQ, *dynamic service addition request*), dans toutes les demandes de modification de service dynamique (DSC-REQ, *dynamic service change request*) et dans toutes les demandes de suppression de service dynamique (DSD-REQ, *dynamic service deletion request*) qu'ils s'envoient l'un à l'autre.

Ces résumés HMAC de service dynamique sont codés au moyen des clés d'authentification de message d'interface BPI+, c'est-à-dire au moyen des clés d'authentification de message calculées sur la base de la clé d'autorisation BPI+. Les CM et les CMTS DOIVENT utiliser les clés actuelles d'authentification de message lors de la production et de la validation des résumés HMAC contenus dans des demandes de service dynamique.

10 Méthodes cryptographiques

Le présent paragraphe spécifie les algorithmes cryptographiques et les longueurs de clé que l'interface BPI+ utilise.

10.1 Cryptage des données en paquet

L'interface BPI+ DOIT utiliser le mode de concaténation de blocs chiffrants (CBC) [FIPS-81] de l'algorithme DES US (DES, *data encryption standard*) norme de cryptage des données aux Etats-Unis d'Amérique [FIPS-46-3] afin de chiffrer le champ de données en paquet dans les trames

d'unité PDU de données en paquet de commande MAC à l'interface RF ainsi que la charge utile de fragmentation et les champs CRC de fragmentation dans les trames de fragmentation MAC.

Les implémentations de l'interface BPI+ implantées dans un matériel conforme à DOCSIS 1.1 ou 2.0 (configuration prédominante du matériel/logiciel) DOIVENT prendre en charge la norme DES à 56 bits et PEUVENT prendre en charge la norme DES à 40 bits.

L'interface BPI+ prend en charge la norme DES à 40 bits afin principalement de permettre l'interfonctionnement avec le matériel à 40 bits conforme à la version initiale de DOCSIS 1.0 puis mis à niveau pour appliquer l'interface BPI+. La norme DES à 40 bits est identique à la norme DES à 56 bits, sauf que 16 bits de la norme DES à 56 bits sont réglés à des valeurs fixes et connues. Un CM ou CMTS exécutant la norme DES à 40 bits DOIT masquer (en les forçant à zéro) les seize bits de gauche de chaque clé DES à 56 bits avant d'exécuter des opérations de cryptage/décryptage.

NOTE – Les bits masqués sont les seize bits de gauche qui seraient présents APRÈS la suppression d'un bit sur huit de la clé TEK à 64 bits (c'est-à-dire des bits dits de parité). Le matériel conforme à DOCSIS 1.1 ou 2.0 et à DOCSIS 1.0 (à 56 bits) PEUT, s'il active l'interface BPI+, implémenter un masquage logiciel de clé DES à 40 bits.

La concaténation CBC DOIT être lancée par un vecteur d'initialisation qui est fourni, ainsi qu'un autre matériel de clé SAID, dans une réponse de clé émise par un CMTS. La concaténation est effectuée de bloc en bloc à l'intérieur d'une trame puis réinitialisée trame par trame afin de rendre le système plus résistant aux éventuelles pertes de trame.

Le traitement des blocs de terminaison résiduels DOIT être effectué afin de chiffrer le bloc alphanumérique final si celui-ci a une longueur inférieure à 64 bits. Si l'on admet un bloc final comptant n bits, avec n inférieur à 64, l'avant-dernier bloc chiffrant est chiffré par norme DES une deuxième fois en mode ECB et les n bits de plus faible poids du résultat sont combinés avec les n derniers bits de la charge utile par un opérateur OUX (ou exclusif) afin de produire la forme courte du bloc chiffrant final. De façon que le récepteur déchiffre ce bloc chiffrant final de forme courte, l'algorithme DES du récepteur chiffre l'avant-dernier bloc chiffrant en mode ECB et combine par opérateur OUX les n bits de gauche avec le bloc chiffrant final de forme courte afin de récupérer le bloc final non chiffré de forme courte. Pour une description de la procédure de cryptage, voir Figure 9-4, (page 195) de [SCHNEIER].

Dans le cas particulier où le bloc alphanumérique à chiffrer dans une trame a une longueur inférieure à 64 bits, le vecteur d'initialisation DOIT être chiffré par algorithme DES et les n bits de gauche du cryptogramme résultant qui correspond au nombre de bits de la charge utile DOIVENT être combinés par opérateur OUX avec les n bits de la charge utile afin de produire le bloc chiffrant de forme courte[6].

[6] Cette méthode de cryptage de charges utiles de courte longueur est vulnérable aux attaques car la combinaison par opérateur OUX de deux ensembles de cryptogrammes chiffrés comme ci-dessus avec le même ensemble de matériel de calcul de clés fournira la combinaison par opérateur OUX des ensembles alphanumériques correspondants. Dans le cas d'une trame d'unité PDU de données en paquet, cela ne pose cependant pas de problème car toutes les trames transportant des données d'utilisateur protégées contiendront au moins 20 octets d'en-tête IP. Dans le cas des trames de fragmentation, une trame courte transportant un cryptogramme de moins de 8 octets (64 bits) est possible. Les quatre derniers octets seront cependant le CRC de fragmentation chiffré et les trois (ou moins de trois) octets précédant le CRC de fragmentation chiffré seront le CRC chiffré des données en paquet.

10.2 Cryptage des clés TEK

Le CMTS chiffre les champs de valeur de clé TEK dans les messages de réponse de clé qu'il envoie aux CM clients. Ce champ est chiffré au moyen du triple algorithme DES à deux clés en mode EDE (cryptage-décryptage-cryptage) [SCHNEIER]:

cryptage: $C = E_{k1}[D_{k2}[E_{k1}[P]]]$

décryptage: $P = D_{k1}[E_{k2}[D_{k1}[C]]]$

P = Clé TEK alphanumérique à 64 bits

C = Clé TEK alphanumérique à 64 bits

k1 = 64 bits de gauche de la clé KEK à 128 bits

k2 = 64 bits de droite de la clé KEK à 128 bits

E[ ] = cryptage DES à 56 bits en mode ECB (répertoire électronique)

D[ ] = décryptage DES à 56 bits en mode ECB

Le § 10.4 décrit comment la clé KEK est calculée à partir de la clé d'autorisation.

10.3 Algorithme de résumé HMAC

La dispersion de clés utilisée par l'attribut "Résumé HMAC" DOIT faire appel à la méthode d'authentification de message HMAC [RFC 2104] avec l'algorithme de dispersion SHA-1 [FIPS-180-2].

Les clés d'authentification de message amont et aval sont calculées d'après la clé d'autorisation (voir détails au § 10.4 ci-dessous).

10.4 Calcul des clés TEK, des clés KEK et des clés d'authentification de message

Le CMTS produit des clés d'autorisation, des clés TEK et des vecteurs d'initialisation (IV). Un générateur de nombres aléatoires ou pseudo-aléatoires DOIT être utilisé afin de produire les clés d'autorisation et les clés TEK. Un générateur de nombres aléatoires ou pseudo-aléatoires PEUT aussi être utilisé afin de produire des vecteurs IV. Quel que soit leur mode de création, les vecteurs IV DOIVENT être imprévisibles. La référence [RFC 1750] propose des pratiques recommandées pour la production de nombres aléatoires à utiliser dans les systèmes cryptographiques.

La référence [FIPS-81] définit les clés DES comme des grandeurs de 8 octets (64 bits) dont les sept éléments binaires de plus fort poids (c'est-à-dire les sept bits de gauche) de chaque octet sont les bits indépendants d'une clé DES et dont le bit de plus faible poids (c'est-à-dire de droite) de chaque octet est un bit de parité calculé d'après les sept bits indépendants qui le précèdent et choisi de façon que l'octet ait une parité impaire.

Le matériel de calcul de clés pour le triple algorithme DES sur deux clés se compose de deux clés distinctes (isolées) à codage DES.

Le protocole de gestion BPKM n'exige pas la parité impaire. Le protocole BPKM produit et distribue des clés DES de 8 octets à parité arbitraire. Il prescrit que les implémentations ne doivent pas tenir compte de la valeur du bit de plus faible poids de chaque octet.

Une clé de cryptage de clé (KEK) et deux clés d'authentification de message sont calculées d'après une clé d'autorisation commune. La façon dont ces clés sont calculées est définie ci-après:

la clé KEK est la clé de cryptage de clé qui sert à crypter les clés de cryptage de trafic.

HMAC_KEY_U est la clé d'authentification de message utilisée dans les demandes de clé amont.

HMAC_KEY_D est la clé d'authentification de message utilisée dans les messages aval de réponse de clé, de rejet de clé et de clé TEK non valide.

SHA(x|y) indique le résultat de l'application de la fonction de dispersion SHA aux chaînes x et y à bits concaténés.

L'expression "Truncate(x,n)" indique le résultat de la troncature de x sur ses n bits de gauche.

```
KEK = Truncate(SHA( K_PAD | AUTH_KEY ), 128)
HMAC_KEY_U = SHA( H_PAD_U | AUTH_KEY )
HMAC_KEY_D = SHA( H_PAD_D | AUTH_KEY )
```

Chaque expression "_PAD_" est une chaîne de 512 bits:

K_PAD = 0x53 répété 64 fois.

H_PAD_U = 0x5C répété 64 fois.

H_PAD_D = 0x3A répété 64 fois.

10.5 Cryptage de clé d'autorisation par clé publique

Les clés d'autorisation contenues dans les messages de réponse d'autorisation DOIVENT être cryptées par clé publique RSA au moyen de la clé publique du câblo-modem. Les clés RSA du CM doivent utiliser l'exposant F4 (65537 en décimal ou, ce qui est équivalent, 010001 en hexadécimal) comme exposant public. L'interface BPI+ utilise un module d'une longueur de 768 bits (96 octets) et 1 024 bits. L'interface BPI+ utilise le modèle de cryptage RSAES-OAEP qui est spécifié dans la version 2.0 de la norme PKCS #1 [RSA3]. Le modèle RSAES-OAEP nécessite la sélection des éléments suivants: une fonction de dispersion; une fonction de création de masques; et une chaîne paramétrique de codage. Les sélections spécifiées par défaut dans [RSA3] DOIVENT être utilisées lors du cryptage de la clé d'autorisation. Ces sélections par défaut sont les suivantes: SHA-1 comme fonction de dispersion; MGF1 avec SHA-1 comme fonction de création de masques; et la chaîne vide comme chaîne paramétrique de codage.

Notons que la confidentialité de base [SCTE22-2] utilisée dans le schéma de cryptage décrit dans la version 1.5 de la norme [RSA1] concernant PKCS #1. Ce schéma est le même que RSAES-PKCS1-v1_5 dans [RSA3]. Afin de garder une compatibilité ascendante, les CM et les CMTS DOIVENT revenir à RSAES-PKCS1-v1_5 [RSA3] pour le cryptage de la clé d'autorisation lors du retour à une interface BPI.

Le protocole de confidentialité de base [SCTE22-2], dont la prise en charge est requise par les câblo-modems DOCSIS, spécifie une longueur module de 768 bits pour ses clés RSA. Afin de permettre les mises à jour logicielles du matériel CM DOCSIS 1.0 vers BPI+, le protocole BPI+ DOIT prendre en charge des longueurs modules de 768 bits ainsi que 1 024 bits. Les câblo-modems DOCSIS 1.1 ou 2.0 originaux développés DOIVENT utiliser des clés RSA d'une longueur module de 1024 bits. Toutefois, les câblo-modem mis à jour de DOCSIS 1.0 vers DOCSIS 1.1 ou 2.0 PEUVENT utiliser des clés RSA d'une longueur module de 768 bits. Pour prendre en charge l'interfonctionnement avec les câblo-modems v1.0 mis à jour, une implémentation d'interface BPI+ d'un CMTS DOCSIS 1.1 ou 2.0 DOIT prendre en charge des longueurs modules de 768 bits ainsi que 1024 bits.

10.6 Signatures numériques

L'interface BPI+ utilise l'algorithme de signature RSA [RSA3] avec la fonction SHA-1 [FIPS-186-2] pour ses trois types de certificat.

Comme dans le cas des clés de cryptage RSA, l'interface BPI+ utilise F4 (65537 en décimal ou 010001 en hexadécimal) comme exposant public pour son opération de signature. L'autorité de certification racine DOCSIS utilisera une longueur de module de 2048 bits (256 octets) pour signer les certificats CA de fabricant qu'elle émet. Les autorités CA de fabricant DOIVENT employer des longueurs de module de clé de signature d'au moins 1024 bits et d'au plus 2048 bits. Notons que

l'autorité CA racine DOCSIS doit être lue comme une autorité CA de fabricant pour les câblo-modems J.122.

10.7 Prise en charge d'autres algorithmes

La spécification actuelle de l'interface BPI+ prescrit l'utilisation de l'algorithme DES à 56 bits pour le cryptage des données en paquet, du triple algorithme DES à deux clés pour le cryptage des clés de cryptage de trafic, de l'algorithme RSA à 1024 bits pour le cryptage des clés d'autorisation et de l'algorithme RSA à 1024-2048 bits pour la signature des certificats X.509 de l'interface BPI+. Ce choix de longueurs et d'algorithmes de clés, bien que convenant aux modèles actuels de menace et aux capacités actuelles des matériels, pourrait un jour ne plus être approprié.

Par exemple, il est généralement admis que l'algorithme DES approche de la fin de son utilité pratique en tant que norme industrielle de cryptage symétrique. Le NIST envisage actuellement la mise au point et l'adoption d'un nouvel algorithme de cryptage normalisé, couramment désigné sous l'appellation de norme de cryptage évoluée, ou (AES, *advanced encryption standard*). Etant donnée la nature des services de sécurité que l'interface BPI+ est appelée à prendre en charge (confidentialité de base à un niveau égal ou supérieur à celui que peuvent offrir des lignes spécialisées et accès conditionnel aux services de transport de données par l'interface RF) ainsi que de la politique de gestion de clés flexible (par réglage de la durée de vie des clés) du protocole, les fournisseurs de services conformes à DOCSIS seront fondés à garder confiance dans l'algorithme DES pendant au moins les cinq prochaines années. Les câblo-modems conformes à DOCSIS devront cependant adopter, un jour ou l'autre, un algorithme de cryptage de trafic plus résistant, qui sera peut-être l'algorithme AES.

L'adoption d'un nouvel algorithme pour le cryptage des données en paquet ne nécessitera pas une refonte de l'interface BPI+. L'utilisation cohérente par le protocole du codage type/longueur/valeur des attributs de gestion BPKM, les éléments d'en-tête étendu de trame MAC et la sélection des capacités de sécurité au cours de l'échange d'autorisation garantissent l'extensibilité de l'interface BPI+. En fait, les changements apportés à l'un quelconque des algorithmes cryptographiques de l'interface BPI+, ou aux longueurs des clés associées, n'auront d'incidence ni sur la structure ni sur le fonctionnement global du protocole.

11 Protection physique des clés dans le CM et dans le CMTS

L'interface BPI+ nécessite que le CM aussi bien que le CMTS conservent en mémoire les clés de cryptage du trafic et les clés d'autorisation de CM. Un CM DOIT conserver également, en mémoire permanente et à écriture unique, une paire de clés RSA. Le CM comme le CMTS DOIVENT empêcher également l'accès physique non autorisé à ce matériel de calcul de clés.

Le niveau de protection physique du matériel de calcul de clés que l'interface BPI+ exige des CM et des CMTS est spécifié en termes de niveaux de sécurité selon la définition donnée dans la norme [FIPS-140-2]. En particulier, les CM et les CMTS DOIVENT répondre aux exigences du niveau de sécurité 1 de la norme FIPS PUBS 140-2.

Le niveau de sécurité 1 de la norme [FIPS-140-2] exige une protection physique minimale au moyen d'enveloppes de classe industrielle. En ce qui concerne les exigences formelles, le lecteur est prié de consulter le document FIPS. Un résumé de ces exigences est cependant présenté ci-après.

Conformément à la classification des "matérialisations physiques" de modules cryptographiques dans la norme [FIPS-140-2], les systèmes CMTS et les CM externes sont des *modules cryptographiques multipuces autonomes*. [FIPS-140-2] spécifie les exigences suivantes pour le niveau de sécurité 1 des modules multipuces autonomes:

- les puces doivent être de classe industrielle, ce qui implique des techniques de passivation normalisées (c'est-à-dire un revêtement d'étanchéité sur les circuits de puce afin de les protéger contre les détériorations dues à l'environnement ou à d'autres facteurs physiques);

- les circuits contenus dans le module doivent être réalisés en tant que matérialisation sur puces multiples de classe industrielle (c'est-à-dire sur une carte imprimée à circuits intégrés, un substrat céramique, etc.);
- le module doit être entièrement contenu dans une enveloppe en métal ou en matière plastique dure de classe industrielle, ce qui peut inclure les portes ou les couvercles amovibles.

Un câblo-modem interne serait classifié comme *module cryptographiqus multipuce autonome* [FIPS-140-2]; les exigences du niveau de sécurité 1 de ces équipements sont les deux premiers de la liste établie ci-dessus.

12 Profil et gestion de certificat X.509 à l'interface BPI+

L'interface DOCSIS BPI+ utilise des certificats numériques [X.509] version 3 pour l'authentification des échanges de clés entre CM et CMTS. [X.509] est à usage général. Le profil de certificat X.509 de l'interface BPI+, ici décrit, spécifie plus précisément le contenu des champs définis dans le certificat. Le profil de certificat définit également la hiérarchie des niveaux de confiance définie pour la gestion et pour la validation des certificats DOCSIS BPI+.

Sauf indication contraire dans les paragraphes suivants, les certificats DOCSIS BPI+ DOIVENT être conformes aux normes PKIX du groupe IETF [RFC 3280]. L'utilisation DOCSIS de certificats X.509 est cependant beaucoup plus circonscrite que celle des normes PKIX. Le profil de certificat X.509 défini par la norme PKIX du groupe IETF vise à prendre en charge, dans le réseau Internet public, un mécanisme de distribution de clés indépendant de l'application et fondé sur des certificats. Le profil de certificat X.509 de la norme PKIX DOIT prendre en charge une large gamme d'environnements de communications, d'applications et de relations de confiance.

En revanche, l'utilisation des certificats numériques à l'interface BPI+ est restreinte à la protection des câblo-opérateurs contre le piratage de services de communication de données grâce à l'application d'un accès conditionnel aux clés de cryptage du trafic. Les services de communication protégés s'inscrivent dans les trois catégories suivantes:

- services de transmission au mieux de données IP à débit élevé;
- services de transmission à débit constant (CBR, *constant bit rate*) de données de kiosque;
- accès à des groupes multidiffusés IP en kiosque.

Ainsi, bien que l'interface BPI+ soit partiellement fondée sur le profil de certificat X.509 proposé par la norme PKIX de l'IETF, le profil X.509 de l'interface BPI+ est prescrit nettement plus souvent.

Le profil de certificat X.509 de l'interface BPI+ utilise également de notables parties de la norme de transaction électronique sécurisée (SET, *secure electronic transaction*) [SET Book 2]. Aussi bien l'organisation générale du présent paragraphe qu'une partie de son contenu reflètent cette norme.

12.1 Aperçu général de l'architecture de gestion des certificats BPI+

L'architecture de gestion des certificats DOCSIS BPI+, décrite dans la Figure 12-1, se compose d'une hiérarchie à trois niveaux de confiance prenant en charge trois types de certificat X.509 version 3:

- un certificat de CA racine, unique et autosigné DOCSIS;
- des certificats de CA de fabricant;
- des certificats de CM.

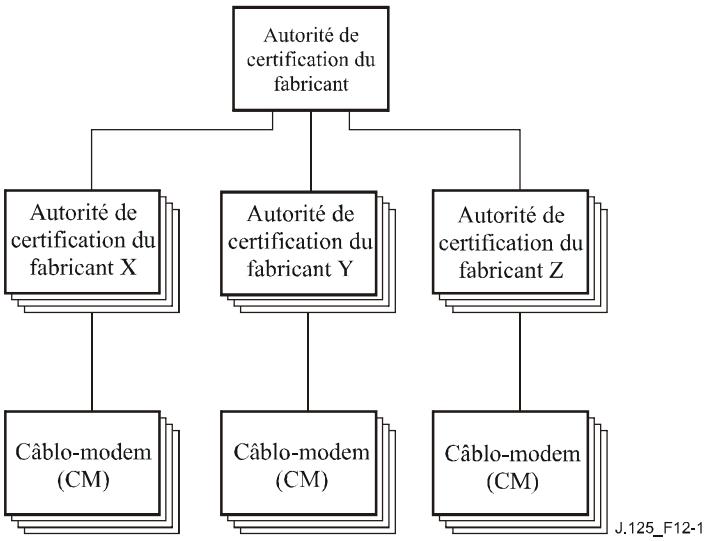


Figure 12-1/J.125 – Architecture de gestion des certificats DOCSIS

L'autorité de certification racine sert de CA racine, qui émet des certificats vers des autorités CA subordonnées, conservées par des fabricants. Les autorités CA de fabricant émettent des certificats vers des entités terminales de câblo-modem.

NOTE – Un même fabricant peut conserver plusieurs autorités CA (par exemple, une autorité CA différente pour chaque usine).

Actuellement, l'autorité de certification racine sert également d'autorité CA racine pour fournir un certificat de vérification de code (CVC, *code verification certificate*) pour le téléchargement logiciel sécurisé, spécifié dans l'Annexe B. Il n'y a cependant pas de raison de sécurité de requérir la même autorité CA racine pour fournir à la fois le certificat CA de fabricant et le certificat CVC. C'est pourquoi, le certificat CVC peut être délivré par les différentes autorités de certification racine à l'avenir.

L'autorité CA racine doit être tenue sous contrôles physiques précis. On y accédera peu fréquemment afin d'émettre de nouveaux certificats CA de fabricant. L'organisation chargée de la certification sera responsable de la maintenance de l'autorité CA racine qui doit créer et distribuer aux câblo-opérateurs une liste de révocation de certificats (CRL, *certificate revocation list*) indiquant les certificats de fabricant qui sont révoqués. La façon dont les listes CRL sont distribuées aux câblo-opérateurs est hors du domaine d'application de la présente Recommandation d'interface BPI+.

L'organisation assurant la maintenance de l'autorité CA racine doit définir un protocole pour les certificats produits par un fabricant à l'intention de l'autorité CA du fabricant demandeur. La spécification de ce protocole est cependant hors du domaine d'application de la présente Recommandation d'interface BPI+.

Les fabricants seront responsables de la maintenance de leur propre CA, à partir de laquelle ils émettront des certificats de CM. Un fabricant donné peut conserver plusieurs CA de fabricant. Les protocoles de demande de certificats auprès d'une autorité CA de fabricant et de distribution de ces certificats aux câblo-modems récepteurs doivent être internes à ce fabricant et sont donc hors du domaine d'application de la présente Recommandation d'interface BPI+. Une autorité CA de fabricant PEUT produire et distribuer des listes CRL à des câblo-opérateurs selon un mode qui est hors du domaine d'application de la présente Recommandation d'interface BPI+.

12.2 Format des certificats

Le présent paragraphe décrit le format des certificats X.509 version 3 et de leurs extensions, utilisés dans l'interface BPI+. Le Tableau 12-1 ci-dessous résume les champs de base d'un certificat X.509 version 3.

Tableau 12-1/J.125 – Champs de base d'un certificat X.509

Champ X.509 v3	Description
tbsCertificate.version	Indique la version du certificat X.509. Ce champ est toujours mis à v3 (valeur de 2).
tbsCertificate.serialNumber	Entier unique que l'autorité CA émettrice attribue au certificat.
tbsCertificate.signature	Identificateur OID et paramètres facultatifs définissant l'algorithme utilisé pour signer le certificat. Ce champ DOIT contenir le même identificateur d'algorithme que le champ signatureAlgorithm ci-dessous.
tbsCertificate.issuer	Nom distinctif de l'autorité CA qui a émis le certificat.
tbsCertificate.validity	Ce champ spécifie le moment où le certificat devient actif et celui où il expire.
tbsCertificate.subject	Nom distinctif indiquant l'entité dont la clé publique est certifiée dans le champ d'information subjectPublicKey.
tbsCertificate .subjectPublicKeyInfo	Champ contenant le matériel de clé publique (clé publique avec ses paramètres) et l'identificateur de l'algorithme avec lequel la clé est utilisée.
tbsCertificate .issuerUniqueID	Champ facultatif permettant de réutiliser dans le temps les noms d'émetteur.
tbsCertificate .subjectUnique ID	Champ facultatif permettant de réutiliser dans le temps les noms de sujet.
tbsCertificate.extensions	Données d'extension.
signatureAlgorithm	Identificateur OID et paramètres facultatifs définissant l'algorithme utilisé pour signer le certificat. Ce champ DOIT contenir le même identificateur d'algorithme que le champ signature de tbsCertificate.
signatureValue	Signature numérique calculée sur la base du champ tbsCertificate codé selon les règles DER de la notation ASN.1.

Tous les certificats et toutes les listes CRL décrits dans la présente Recommandation DOIVENT être signés au moyen de l'algorithme de signature RSA et de l'algorithme SHA-1 comme fonction de dispersion unilatérale. L'algorithme de signature RSA est décrit dans la norme PKCS #1 RSA1; l'algorithme SHA-1 est décrit dans [FIPS-180-2]. Ce n'est là qu'un exemple de la façon dont l'interface BPI+ limite les valeurs des champs de base d'un certificat X.509. Toutes ces restrictions sont décrites ci-dessous:

12.2.1 Champs tbsCertificate.validity.notBefore et tbsCertificate.validity.notAfter

Les certificats de câblo-modem ne seront pas renouvelables. Ils doivent donc avoir une période de validité supérieure à la durée de vie opérationnelle du câblo-modem. Un certificat CA de fabricant DOIT être valide pendant une durée définie dans [SCTE23-3] ou [SCTE79-2] à partir de la date d'émission et être réémis pendant la période définie dans [SCTE23-3] ou [SCTE79-2]. Le certificat CA racine DOCSIS DOIT être valide pendant une période définie dans [SCTE23-3] ou [SCTE79-2] à partir de la date de début de fonctionnement de l'autorité CA racine et être réémis avant une date définie dans [SCTE23-3] ou [SCTE79-2].

La présente Recommandation part du principe que la durée de vie opérationnelle d'un câblo-modem ne dépassera pas vingt ans. La période de validité d'un certificat de câblo-modem DOIT commencer à la date de fabrication du dispositif; cette période de validité DEVRAIT se prolonger au moins 20 ans après cette date de fabrication.

Les périodes de validité DOIVENT être codées en temps UTC. Les valeurs de temps UTC DOIVENT être exprimées en temps moyen de Greenwich (heure Zulu) et DOIVENT inclure les secondes (c'est-à-dire que les temps sont exprimés en format YYMMDDHHMMSSZ), même lorsque le nombre de secondes est égal à zéro. Le champ d'année (YY) DOIT être interprété comme suit:

- lorsque YY est une valeur supérieure ou égale à 50, l'année doit être interprétée comme 19YY;
- lorsque YY est une valeur inférieure à 50, l'année doit être interprétée comme 20YY.

12.2.2 Champ tbsCertificate.serialNumber

Le numéro de série DOIT être un nombre entier positif attribué par l'autorité CA à chaque ecrtificat. Il DOIT être unique pour chaque certificat délivré par une autorité CA donnée (c'est-à-dire que le nom d'émetteur et le numéro de série correspondent à un unique certificat). Les autorités CA DOIVENT obliger le numéro de série à être un entier non négatif. Le fabricant NE DEVRAIT PAS imposer ou supposer qu'il existe une relation entre le numéro de série du certificat et le numéro de série du modem pour lequel le certificat a été délivré.

Etant donné les conditions d'unicité ci-dessus, des numéros de série peuvent être prévus pour contenir de longs nombres entiers. Les utilisateurs de certificats DOIVENT être capables de gérer des valeurs de numéro de série allant jusqu'à 20 octets. Les autorités CA NE DOIVENT PAS utiliser de valeurs de numéro de série de plus de 20 octets.

NOTE – Les utilisateurs de certificats dans les systèmes DOCSIS 1.1 ou 2.0 DOIVENT être préparés à gérer des certificats qui peuvent déjà avoir des numéros de série négatifs, ou nuls, pour assurer une comptabilité ascendante.

12.2.3 Champ tbsCertificate.signature et signatureAlgorithm

Tous les certificats et toutes les listes CRL décrits dans la présente Recommandation DOIVENT être signés au moyen de l'algorithme de signature RSA et de l'algorithme SHA-1 comme fonction de dispersion unilatérale. L'algorithme de signature RSA est décrit dans la norme PKCS #1 [RSA1]; l'algorithme SHA-1 est décrit dans [FIPS-180-2].

L'identificateur OID utilisé en notation ASN.1 pour identifier l'algorithme de signature "SHA-1 avec RSA" est le suivant:

```
sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {
     iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
     pkcs-1(1) 5}
```

Lorsque l'identificateur OID sha-1WithRSAEncryption apparaît dans le type ASN.1 AlgorithmIdentifier, comme c'est le cas avec les deux champs tbsCertificate.signature et signatureAlgorithm, le composant paramétrique de ce type est le type NULL de l'ASN.1.

12.2.4 Champs tbsCertificate.issuer et tbsCertificate.subject

Les noms X.509 sont des SEQUENCES de noms distinctifs relatifs (RelativeDistinguishedNames) qui à leur tour sont des ensembles (SET) de séquences AttributeTypeAndValue. L'élément AttributeTypeAndValue est une SEQUENCE d'un type d'attribut (OBJECT IDENTIFIER) et d'une valeur d'attribut. La valeur de l'attribut countryName DOIT être une chaîne imprimable (PrintableString) de 2 caractères, choisie dans l'ISO 3166. Toutes les autres valeurs d'attribut DOIVENT être codées comme des chaînes de caractères de type soit T.61/télétex soit imprimables.

Le codage d'une chaîne imprimable DOIT être utilisé si la chaîne de caractères ne contient que des caractères issus du jeu de chaîne imprimable. Plus précisément:

abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
0123456789
'()+,-./:=? and space.

La chaîne T.61/télétex DOIT être utilisée si la chaîne de caractères contient d'autres caractères.

Les identificateurs OID suivants sont nécessaires pour définir les noms d'émetteur et de sujet dans les certificats BPI+:

```
id-at OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) ds(5) 4}
id-at-commonName        OBJECT IDENTIFIER ::= {id-at 3}
id-at-countryName       OBJECT IDENTIFIER ::= {id-at 6}
id-at-localityName              OBJECT IDENTIFIER ::= {id-at 7}
id-at-stateOrProvinceName       OBJECT IDENTIFIER ::= {id-at 8}
id-at-organizationName          OBJECT IDENTIFIER ::= {id-at 10}
id-at-organizationalUnitName    OBJECT IDENTIFIER ::= {id-at 11}
```

Les paragraphes suivants décrivent le format du champ de nom de sujet pour chaque type de certificat BPI+. Le champ de nom d'émetteur d'un certificat correspond au champ de nom de sujet du certificat émis. Tout certificat transmis par un CM dans un message d'informations d'autorisation ou de demande d'autorisation DOIT avoir des champs nominatifs conformes au format indiqué. Un CMTS DOIT être capable de traiter les champs nominatifs d'un certificat si ces champs sont conformes au format indiqué. Un CMTS PEUT choisir d'accepter un certificat dont les champs nominatifs ne sont pas conformes au format indiqué.

En général, les certificats X.509 prennent en charge un large ensemble de règles pour déterminer si le nom d'émetteur d'un certificat correspond au nom de sujet d'un autre certificat. Ces règles sont telles que deux champs nominatifs puissent être déclarés concordants même si leur comparaison binaire n'indique pas de concordance. [RFC 3280] recommande que les autorités de certification limitent le codage des champs nominatifs de façon qu'une implémentation puisse déclarer une concordance ou une discordance au moyen d'une simple comparaison binaire. L'interface BPI+ suit la présente Recommandation. En conséquence, le champ tbsCertificate.issuer à codage DER d'un certificat BPI+ DOIT être en concordance exacte avec le champ tbsCertificate.subject à codage DER de l'émetteur de son certificat. Une implémentation PEUT comparer un nom d'émetteur à un nom de sujet en effectuant une comparaison binaire des champs tbsCertificate.issuer et tbsCertificate.subject codés selon les règles DER.

12.2.4.1 Certificat racine DOCSIS

countryName=US

organizationName= Spécifications d'interface du service de données par câble

organizationalUnitName= Câblo-modems

commonName= Autorité de certification racine de câblo-modem selon DOCSIS

Les attributs de nom de pays, de nom d'organisation, de nom d'unité organisationnelle et de nom commun (respectivement countryName, organizationName, organizationalUnitName et commonName) DOIVENT être inclus et DOIVENT avoir les valeurs indiquées. D'autres attributs ne sont pas autorisés et NE DOIVENT PAS être inclus.

12.2.4.2 Certificat de fabricant DOCSIS

countryName=< Pays du fabricant >

[stateOrProvinceName=< état/province >]

[localityName=< Ville >]

organizationName=< Nom de la société >

organizationalUnitName=DOCSIS

[organizationalUnitName=< Lieu de fabrication >]

commonName=< Nom de la société > [<Identifiant de série>] Autorité de certification racine du câblo-modem [<Identifiant de série >]

Les attributs de nom du pays, de nom d'organisation et de nom commun (respectivement countryName, organizationName, et commonName) DOIVENT être inclus et DOIVENT avoir les valeurs indiquées.

Le champ commonName PEUT contenir un identifiant de série (par exemple, 1, 2, UN, DEUX, A, B, I, II, etc.) pour identifier différentes autorités CA de fabricant déployées par le même fabricant avec le même nom de la société.

Le nom d'unité organisationnelle ayant la valeur "DOCSIS" DOIT être inclus.

Le nom d'unité organisationnelle représentant le lieu de fabrication DEVRAIT être inclus. Si c'est le cas, il DOIT être précédé par le nom d'unité organisationnelle ayant la valeur "DOCSIS".

Le nom d'état ou de province et le nom de localité (stateOrProvinceName et localityName) PEUVENT être inclus.

D'autres attributs ne sont pas autorisés et NE DOIVENT PAS être inclus.

12.2.4.3 Certificat de câblo-modem

countryName=<Pays du fabricant>

organizationName=<Nom de la société>

organizationalUnitName=<lieu de fabrication>

commonName=<Numéro de série>

commonName=<Adresse MAC>

Pour établir une distinction entre les deux noms communs, celui qui représente le "numéro de série" DOIT précéder celui qui représente "l'adresse MAC". L'utilisation du champ de numéro de série est déconseillée. S'il est utilisé, le numéro de série DOIT être un identificateur unique de câblo-modem, mais PEUT être différent du numéro de série codé dans les attributs BPKM. L'adresse MAC contenue dans le certificat CM DOIT être la même que celle qui est contenue dans les attributs de gestion BPKM.

Les caractères utilisés dans la représentation par chaîne imprimable des numéros de série de CM DOIVENT être limités au jeu secondaire de caractères suivant:

- A-Z (0x41-0x5A)
- a-z (0x61-0x7A)
- 0-9 (0x30-0x39)
- "–" (0x2D)

L'adresse MAC est exprimée sous la forme de six paires de nombres hexadécimaux séparés par deux points (:), par exemple: "00:60:21:A5:0A:23". Les caractères alphabétiques (A-F) doivent être exprimés en hexadécimal par des majuscules.

Dans un certificat de câblo-modem, le nom d'unité organisationnelle qui décrit le lieu de fabrication du modem DEVRAIT être le même que le nom d'unité organisationnelle indiqué dans le nom d'émetteur pour décrire un lieu de fabrication.

Les attributs de nom de pays, de nom d'organisation, de nom d'unité organisationnelle et de nom commun (adresse MAC) DOIVENT être inclus. L'attribut de nom commun (numéro de série) PEUT être inclus. D'autres attributs ne sont pas autorisés et NE DOIVENT PAS être inclus.

12.2.5 Champ tbsCertificate.subjectPublicKeyInfo

Le champ tbsCertificate.subjectPublicKeyInfo contient la clé publique et l'identificateur d'algorithme de clé publique. La clé publique RSA contenue dans le certificat DOIT être la même que la clé publique RSA contenue dans les attributs de gestion BPKM.

Le champ tbsCertificate.subjectPublicKeyInfo.algorithm est une structure d'identification d'algorithmes. L'algorithme désigné par cet identificateur DOIT être à cryptage RSA, désigné par l'OID suivant:

```
pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) 1}

rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1}
```

Le champ de paramètres de l'identificateur d'algorithme DOIT avoir un type NULL de l'ASN.1.

La clé publique RSA doit être codée au moyen de la clé publique RSA de type ASN.1:

```
RSAPublicKey ::= SEQUENCE {
     modulus            INTEGER, -- n
     publicExponent     INTEGER, -- e -- }
```

où "modulus" désigne le module n et "publicExponent" désigne l'exposant public e. La clé publique RSA codée par règles DER est la valeur de la chaîne binaire BIT STRING tbsCertificate.subjectPublicKeyInfo.subjectPublicKey.

12.2.6 Champs tbsCertificate.issuerUniqueID et tbsCertificate.subjectUniqueID

Les champs issuerUniqueID et subjectUniqueID DOIVENT être omis pour les trois types de certificat d'interface BPI+.

12.2.7 Champ tbsCertificate.extensions

Les certificats des câblo-modems et les certificats d'autorité CA de fabricant DOCSIS ne sont pas tenus de comprendre d'éventuelles extensions. Cela est vrai même pour les extensions prescrites par [RFC 3280]. Les certificats des câblo-modems et les certificats CA de fabricants DOCSIS PEUVENT comprendre des extensions comme décrit dans les § 12.2.7.1 et 12.2.7.2, respectivement. Le § 12.2.7.3 spécifie les exigences des extensions des certificats d'autorité CA racine. Les extensions incluses dans les certificats BPI+ DOIVENT être conformes à [RFC 3280].

12.2.7.1 Certificats de câblo-modem

Les certificats de câblo-modem PEUVENT contenir des extensions non critiques. Ils NE DOIVENT PAS contenir d'extensions critiques. Si l'extension KeyUsage est présente, les bits digitalSignature et keyEncipherment DOIVENT être activés, les bits keyCertSign et cRLSign DOIVENT être désactivés et tous les autres bits DEVRAIENT être désactivés. L'extension Basic Constraints PEUT ne pas être une extension critique des certificates de câblo-modem.

12.2.7.2 Certificats d'autorité CA de fabricant DOCSIS

Les certificats d'autorité CA de fabricant DOCSIS PEUVENT contenir l'extension de contraintes de base et/ou l'extension d'usage de clé. Si elles sont incluses, ces extension PEUVENT apparaître comme étant critiques ou non critiques.

Les certificats d'autorité CA de fabricant DOCSIS PEUVENT contenir des extensions non critiques. Ils NE DOIVENT PAS contenir d'autres extensions critiques que, le cas échéant, l'extension de contraintes de base.

Si l'extension Key Usage est présente dans un certificat d'autorité CA de fabricant DOCSIS, le bit keyCertSign DOIT être activé, le bit cRLSign PEUT être activé et tous les autres bits DEVRAIENT être désactivés.

Si l'extension de contraintes de base est présente, le CA DOIT être mis sur TRUE et le pathLenConstraint doit être mis à 0.

12.2.7.3 Certificats d'autorité CA racine DOCSIS

Les certificats d'autorité CA racine DOCSIS DOIVENT contenir l'extension de contraintes de base et/ou l'extension Key Usage comme extensions critiques.

Les certificats d'autorité CA racine DOCSIS PEUVENT contenir des extensions non critiques. Ils NE DOIVENT PAS contenir d'extensions critiques autres que l'extension de contraintes de base et l'extension d'usage de clé.

Pour l'extension Key Usage, le bit keyCertSign DOIT être activé, le bit cRLSign PEUT être activé et tous les autres bits DEVRAIENT être désactivés.

Si l'extension de contraintes de base est présente, le CA DOIT être mis sur TRUE et le pathLenConstraint doit être mis à 1.

12.2.8 Champ signatureValue

Dans les trois types de certificat BPI+, le champ signatureValue contient la signature RSA (avec fonction SHA-1) calculée sur le certificat tbsCertificate à codage DER de l'ASN.1, qui sert d'entrée dans la fonction de signature RSA. La valeur de signature résultante est codée en ASN.1 sous la forme d'une chaîne binaire puis incluse dans le champ signatureValue du certificat.

12.3 Stockage et gestion dans le CM du certificat de câblo-modem

Les certificats CM émis par les fabricants DOIVENT être stockés dans une mémoire à écriture permanente et unique du CM. Les CM qui possèdent des paires de clés RSA privées/publiques installées à l'usine DOIVENT avoir également des certificats CM préinstallés. Les CM qui se fondent sur des algorithmes internes pour produire une paire de clés RSA DOIVENT prendre en charge un mécanisme d'installation de certificat CM émis par le fabricant après la production des clés.

La clé publique (RSA) de l'autorité CA racine pour la vérification CVC, qu'utilise le CM pour vérifier le certificat de vérification de code (CVC, *code verification certificate*) pour le téléchargement sécurisé de logiciel défini dans l'Annexe B, DOIT être placée en mémoire non volatile du CM. Alors que l'autorité CA racine DOCSIS pour la chaîne de certification du câblo-modem délivre actuellement le certificat CVC, une autorité CA racine différente peut délivrer le certificat CVC à l'avenir. C'est pourquoi, le câblo-modem NE DOIT PAS utiliser la clé publique de l'autorité CA racine pour la vérification du certificat CVC placée dans la mémoire non volatile afin de vérifier la chaîne de certification du câblo-modem.

Le certificat CA de l'autorité CA de fabricant qui a signé le certificat de CM DOIT être mémorisé dans la mémoire non volatile du câblo-modem. Celui-ci DOIT être en mesure de mettre à jour ou de remplacer le certificat CA de fabricant au moyen du fichier de code DOCSIS téléchargé (voir l'Annexe B). Le certificat CA de fabricant PEUT être incorporé dans le logiciel du CM.

Si le certificat CA de fabricant est intégré dans le logiciel du CM et si un fabricant émet des certificats de CM avec de multiples certificats CA, la mémoire du CM doit inclure TOUS les certificats CA de ce fabricant. Le certificat CA de fabricant spécifique qui est installé par le CM (c'est-à-dire annoncé dans les messages d'information d'authentification et renvoyé par l'objet de base MIB) sera celui qui désigne l'émetteur du certificat CM de ce modem.

12.4 Traitement et gestion du certificat dans le système CMTS

La gestion BPKM utilise des certificats numériques pour permettre aux systèmes CMTS de vérifier l'association établie entre une identité de CM (codée dans les noms de sujet d'un certificat X.509 numérique) et sa clé publique. A cette fin, le CMTS valide le chemin ou la chaîne de certification du certificat CM. Ce chemin se composera normalement de trois certificats concaténés: à partir du certificat CM, le chemin conduit au certificat de l'autorité CA de fabricant qui a émis ce certificat CM puis aboutit au certificat DOCSIS autosigné de l'autorité CA racine (Figure 12-2). La validation de cette chaîne implique la vérification de la signature du certificat de l'autorité CA de fabricant au moyen de la clé publique DOCSIS de l'autorité CA racine puis la vérification de la signature du certificat CM au moyen de la clé publique de l'autorité CA de fabricant.

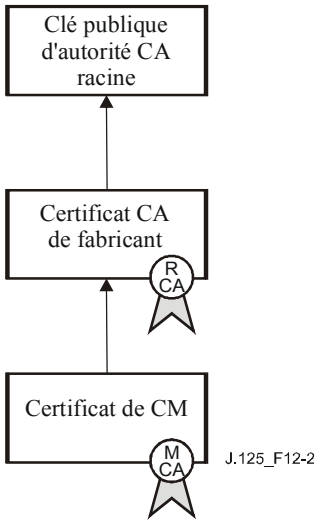


Figure 12-2/J.125 – Chaîne de certification de CM

L'interface BPI+ prescrit que les systèmes CMTS prennent en charge les commandes administratives qui permettent à l'opérateur de neutraliser la validation de chaîne de certification en spécifiant qu'un certificat d'autorité CA de fabricant ou de CM doit être considéré comme fiable ou non fiable. Une description détaillée de ces commandes administratives relatives à la gestion de certificat par les CMTS doit être fournie dans un document de système OSS associé [DOCSIS8]. Le présent paragraphe spécifie le modèle de gestion permettant d'appliquer ces commandes ainsi que le traitement effectué par un système CMTS afin d'évaluer la validité d'un certificat de CM et de vérifier ainsi l'association entre l'identité du CM et sa clé publique.

12.4.1 Modèle de gestion de certificat par un CMTS

Le système CMTS conserve des copies des certificats CA racine, CA fabricant et CM, qu'il obtient soit par préconfiguration soit par messagerie de gestion BPKM. Chaque certificat dont un CMTS est informé DOIT être marqué comme étant dans l'un des quatre états suivants: non sécurisé, sécurisé, concaténé ou racine. Seul le certificat DOCSIS d'autorité CA racine (certificat autosigné qui contient la clé publique sécurisée DOCSIS de l'autorité CA racine) DOIT être marqué comme étant une racine. Un CMTS PEUT cependant prendre en charge plusieurs certificats CA racines. Les certificats racines DOIVENT être préconfigurés dans un système CMTS et celui-ci DOIT prendre en charge la possibilité de montrer tous les certificats racine et/ou son empreinte de façon que l'opérateur puisse vérifier le ou les certificats racine.

Un système CMTS s'informe des certificats CA de fabricant soit par son interface de préconfiguration soit par réception et traitement de messages d'information d'authentification des CM clients. Quelle que soit la façon dont un CMTS obtient ses certificats CA de fabricant, il

DOIT les marquer comme étant non sécurisés, sécurisés ou concaténés. Si un certificat CA fabricant n'est pas autosigné, le CMTS le marque comme étant concaténé. Le CMTS DOIT, cependant, prendre en charge les commandes administratives qui permettent à un opérateur de neutraliser le marquage de concaténation et de spécifier qu'un certificat CA fabricant donné est sécurisé ou non sécurisé.

Si un certificat CA fabricant *est* autosigné, le CMTS le marque comme étant soit sécurisé soit non sécurisé, selon la politique commandée administrativement de ce CMTS. Un certificat CA fabricant autosigné dont la signature ne peut pas être vérifiée DOIT être marqué comme étant non sécurisé. Un CMTS sécurisant des certificats CA fabricant autosignés DOIT être configurable. La sécurisation par défaut des certificats CA fabricant autosignés n'est PAS RECOMMANDEE dans les systèmes opérationnels du marché. La sécurisation par défaut sera principalement utilisée pour prendre en charge la certification et d'autres modes de contrôle. Le CMTS DOIT marquer le certificat CM comme étant concaténé, sauf neutralisation par commande administrative de ce CMTS.

Un système CMTS obtient des copies de certificats CM dans les demandes d'autorisation qu'il reçoit de CM clients. Les certificats CM DOIVENT être émis par une autorité CA de fabricant. Ainsi, sauf s'ils sont neutralisés par commande administrative du CMTS, celui-ci marquera les certificats CM comme étant concaténés. Un opérateur peut, dans le cadre du processus de préconfiguration du modem, spécifier qu'un certificat de CM soit marqué comme étant non sécurisé ou sécurisé.

12.4.2 Validation de certificat

Le système CMTS valide les chemins de certification des certificats CA fabricant et CM au moyen des critères suivants.

NOTE – Ces critères sont itératifs et nécessitent qu'un CMTS valide l'itinéraire de certification d'un certificat CA de fabricant concaténé avant de pouvoir valider l'itinéraire de certification d'un certificat CM émis par cette autorité CA de fabricant.

Le système CMTS DOIT étiquetter les certificats CA fabricant et CM comme étant valides ou non valides selon que leur itinéraire de certificat est, respectivement, valide ou non valide. Les certificats sécurisés DOIVENT être valides. Cela est vrai même si l'heure actuelle n'entre pas dans la période de validité du certificat sécurisé. Les certificats non sécurisés DOIVENT être non valides.

Un certificat concaténé est valide si:

1) le certificat est concaténé avec un certificat racine, sécurisé ou valide;
2) la signature du certificat peut être vérifiée avec la clé publique de l'émetteur;
3) l'heure actuelle entre dans la période de validité de chaque certificat concaténé ou racine contenu dans la chaîne du certificat (noter que l'interface BPI+ n'exige pas l'imbrication des périodes de validité, c'est-à-dire qu'il n'est pas nécessaire que toute la période de validité d'un certificat entre dans la période de validité de son certificat d'émission);
4) le certificat n'est pas inscrit dans une liste d'opposition de certificats de CM et de fabricant (voir § 12.4.4);
5) dans le cas d'un certificat CM, l'adresse MAC du CM, codée dans son champ tbsCertificate.subject et dans sa clé publique RSA codée dans son champ tbsCertificate.subjectPublicKeyInfo correspond à l'adresse MAC du CM et à la clé publique RSA codées dans les attributs de gestion BPKM de demande d'autorisation;
6) dans le cas d'un certificat CM, si l'extension KeyUsage est présente, les bits digitalSignature et/ou keyAgreement et keyEncipherment sont activés, les bits keyCertSign et cRLSign sont désactivés. Dans le cas d'un certificat CA de fabricant, si l'extension KeyUsage est présente, le bit keyCertSign est activé.

La question de savoir si le critère 3) ci-dessus est négligé DOIT faire l'objet d'une commande administrative.

Si la vérification de la période de validité est ACTIVEE et que l'heure légale n'ait pas été acquise par le CMTS, un message de rejet (non permanent) d'autorisation DOIT être renvoyé en réponse à une demande d'autorisation de type BPI+.

Si un certificat concaténé ne satisfait aucun des critères de validité ci-dessus, le CMTS DOIT le considérer comme non valide.

12.4.3 Empreintes de certificat

Les empreintes des certificats sont des fonctions de dispersion unilatérales (comme SHA-1) qui résistent aux collisions. Elles permettent d'identifier les certificats de façon concise. Un CMTS PEUT conserver les empreintes des certificats CM et CA fabricant qu'il détient ou qu'il a validés. Au moyen d'empreintes, un CMTS peut mémoriser en cache les résultats d'une opération de validation antérieure. En comparant l'empreinte d'un certificat récemment offert avec une empreinte mémorisée en cache, il peut déterminer rapidement la validité du certificat offert.

12.4.4 Listes d'opposition de certificats CA fabricant et CM

Lors de la validation de chaînes de certificats, le CMTS n'est pas tenu de vérifier le statut de révocation d'un certificat (c'est-à-dire de vérifier la présence d'une liste CRL mise à jour pour ce certificat). En revanche, le CMTS DOIT être en mesure de conserver des *listes d'opposition* de certificats CA fabricant et CM notoirement non sécurisés. Les certificats inscrits sur ces listes d'opposition peuvent être ceux qui ont été révoqués par leur émetteur. Mais ils peuvent également être des certificats valides que le cablo-opérateur exploitant le CMTS décide de marquer comme étant "non sécurisés".

La définition des procédures et des protocoles de maintenance d'une liste d'opposition de certificats CA de fabricant et de certificats de CM sont hors du domaine d'application de la Recommandation concernant l'interface BPI+.

Annexe A

Extensions du fichier de configuration du protocole de transfert de fichiers simplifié

Toutes les valeurs des paramètres de configuration de la confidentialité de base d'un câblo-modem (CM) sont spécifiées dans le fichier de configuration (TFTP, *trivial file transfert protocol*) protocole de transfert de fichiers simplifié téléchargé par le CM pendant l'initialisation de la commande MAC radiofréquence (RF). Les champs des paramètres de configuration de la confidentialité de base sont inclus dans les calculs MIC du CM comme dans ceux du système CMTS, ainsi que dans les demandes d'enregistrement d'un CM. Se reporter à [J.112-B] pour l'ordre d'insertion des champs de réglage des paramètres de configuration de la confidentialité de base dans le résumé MD5 du circuit MIC du système CMTS.

A.1 Formes de codage

Les formes de codage de type/longueur/valeur suivantes pour les réglages des paramètres de configuration de la confidentialité de base DOIVENT être utilisées à la fois dans le fichier de configuration et dans les demandes d'enregistrement de CM avec commande MAC RF. Toutes les grandeurs de plusieurs octets suivent l'ordre des octets du réseau, c'est-à-dire que l'octet contenant les bits de plus fort poids est transmis en premier.

A.1.1 Réglages de configuration de la confidentialité de base

La combinaison des réglages de configuration d'activité de confidentialité pour la consultation de fichiers distants RFI 1.1 ou 2.0 ([J.112-B] § B.C.1.1.16) ou [J.122] et des réglages de la capacité de modem de prise en charge de la confidentialité ([J.112-B] § B.C.1.3.1.6) ou [J.122] permet de vérifier si la confidentialité de base est activée ou désactivée dans un CM. Si l'opérateur prévoit de préconfigurer un câblo-modem pour fonctionner en mode BPI+ en utilisant les paramètres de configuration BPI par défaut spécifiés dans le Tableau A.1, les réglages de configuration de la confidentialité de base correspondants PEUVENT être omis. Si le fichier de configuration ne contient pas tous les paramètres BPI+ nécessaires, le CM DOIT utiliser les valeurs par défaut spécifiées dans le Tableau A.1 pour les paramètres manquants. D'un autre côté, si l'opérateur prévoit de préconfigurer un câblo-modem pour fonctionner en mode BPI+ en utilisant des paramètres de configuration BPI différents de ceux spécifiés dans le Tableau A.1, les réglages de configuration de la confidentialité de base correspondants DOIVENT être présents. Les réglages de configuration de la confidentialité de base correspondants PEUVENT être présents si la confidentialité de base Plus est désactivée. Le paramètre distinct d'activation de la confidentialité permet à un opérateur de désactiver ou de réactiver la confidentialité de base en modifiant un seul paramètre de de configuration. Il n'est donc pas nécessaire de retirer ou de réinsérer un grand nombre de paramètres de configuration de confidentialité de base.

Ce champ définit les paramètres associés à l'opération de confidentialité de base. Il se compose de plusieurs champs de type/longueur/valeur encapsulés. Les champs de type définis sont valables uniquement dans la chaîne de réglage des paramètres de configuration de la confidentialité de base encapsulée.

type	longueur	valeur
BP_CFG	n	

La valeur spécifique du type BP_CFG est définie dans [J.112-B] ou [J.122].

A.1.1.1 Formes de codage de la confidentialité de base interne

A.1.1.1.1 Temporisation d'attente d'autorisation

La valeur de ce champ spécifie l'intervalle de réexpédition, en secondes, des messages de demande d'autorisation à compter de l'état d'attente d'autorisation.

sous-type	longueur	valeur
1	4	

Fourchette de valeurs admissibles: 1-30

A.1.1.1.2 Temporisation d'attente de réautorisation

La valeur de ce champ spécifie l'intervalle de réexpédition, en secondes, des messages de demande de réautorisation à compter de l'état d'attente d'autorisation.

sous-type	longueur	valeur
2	4	

Fourchette de valeurs admissibles: 1-30

A.1.1.1.3 Délai de tolérance pour l'autorisation

La valeur de ce champ spécifie la période, en secondes, pendant laquelle la réautorisation doit être différée.

sous-type	longueur	valeur
3	4	

Fourchette de valeurs admissibles: 1-6 047 999

A.1.1.1.4 Temporisation d'attente en service

La valeur de ce champ spécifie l'intervalle de réexpédition, en secondes, de demandes de clé à compter de l'état d'attente opérationnel.

sous-type	longueur	valeur
4	4	

Fourchette de valeurs admissibles: 1-10

A.1.1.1.5 Temporisation d'attente de renouvellement de clés

La valeur de ce champ spécifie l'intervalle de réexpédition, en secondes, des demandes de clé à compter de l'état d'attente de renouvellement de clés.

sous-type	longueur	valeur
5	4	

Fourchette de valeurs admissibles: 1-10

A.1.1.1.6 Délai de tolérance pour les clés TEK

La valeur de ce champ spécifie la période, en secondes, pendant laquelle le renouvellement des clés TEK doit être différé.

sous-type	longueur	valeur
6	4	

Fourchette de valeurs admissibles: 1-302399

A.1.1.1.7 Délai d'attente de rejet d'autorisation

La valeur de ce champ indique le temps, en secondes, pendant lequel un CM attend à l'état d'attente de rejet d'autorisation après réception d'un message de rejet d'autorisation.

sous-type	longueur	valeur
7	4	

Fourchette de valeurs admissibles: 1-600

A.1.1.1.8 Temporisation d'attente de mappage d'associations de service

La valeur de ce champ indique l'intervalle de réexpédition, en secondes, des demandes de mappage d'associations de service à compter de l'état d'attente de mappage.

sous-type	longueur	valeur
8	4	

Fourchette de valeurs admissibles: 1-10

A.1.1.1.9 Nombre maximal de nouvelles demandes de mappage d'associations de service

La valeur de ce champ indique le nombre maximal de nouvelles demandes de mappage autorisées.

sous-type	longueur	valeur
9	4	

Fourchette de valeurs admissibles: 0-10

A.2 Principes généraux applicables aux paramètres

Les valeurs extrêmes et les valeurs par défaut recommandées pour les divers paramètres de configuration et d'exploitation de l'interface de confidentialité de base (BPI) sont indiquées dans le tableau ci-dessous. Ces valeurs pourront varier à mesure que les fournisseurs de services se familiariseront avec le fonctionnement de cette interface.

Tableau A.1/J.125 – Fourchette des valeurs en service recommandées pour les paramètres de configuration de l'interface BPI

Système	Nom	Description	Valeur minimale	Valeur par défaut	Valeur maximale
CMTS	Durée de vie de l'autorisation	Durée de vie, en secondes, attribuée par le système CMTS à la nouvelle clé d'autorisation	1 jour (86 400 s)	7 jours (604 800 s)	70 jours (6 048 000 s)
CMTS	Durée de vie des clés TEK	Durée de vie, en secondes, attribuée par le système CMTS aux nouvelles clés TEK	30 min (1800 s)	12 heures (43 200 s)	7 jours (604 800 s)
CM	Temporisation d'attente d'autorisation	Intervalle de retransmission de la demande d'autorisation à compter de l'état d'attente d'autorisation	2 s	10 s	30 s
CM	Temporisation d'attente de réautorisation	Intervalle de retransmission de la demande d'autorisation à compter de l'état d'attente de réautorisation	2 s	10 s	30 s
CM	Délai de tolérance pour l'autorisation	Durée précédant l'expiration de l'autorisation pendant laquelle le CM commence la réautorisation	5 min (300 s)	10 min (600 s)	35 jours (3 024 000 s)
CM	Temporisation d'attente en service	Intervalle de retransmission des demandes de clé à compter de l'état d'attente en service	1 s	10 s	10 s
CM	Temporisation d'attente de renouvellement de clés	Intervalle de retransmission des demandes de clé à compter de l'état d'attente de renouvellement de clés	1 s	10 s	10 s
CM	Délai de tolérance pour les clés TEK	Durée précédant l'expiration des clés TEK pendant laquelle le CM commence à réintroduire celles-ci	5 min (300 s)	1 heure (3600 s)	3,5 jours (302 399 s)
CM	Temporisation d'attente de rejet d'autorisation	Délai d'attente avant renvoi de la demande d'autorisation après réception d'un message de rejet d'autorisation	10 s	60 s	10 min (600 s)

Tableau A.1/J.125 – Fourchette des valeurs en service recommandées pour les paramètres de configuration de l'interface BPI

Système	Nom	Description	Valeur minimale	Valeur par défaut	Valeur maximale
CM	Temporisation d'attente de mappage d'associations de service	Intervalle de retransmission des demandes de mappage à compter de l'état d'attente de mappage	1 s	1 s	10 s
CM	Nombre maximal de nouvelles demandes de mappage d'associations de service	Nombre maximal de fois que le CM procède à de nouvelles demandes de mappage d'associations de service avant de renoncer	0	4	10

La fourchette des valeurs effectives (par opposition à la fourchette des valeurs en service recommandées) pour la durée de vie de l'autorisation et la durée de vie des clés TEK s'établit comme suit:

- valeurs possibles de durée de vie de l'autorisation: 1-6 048 000 secondes;
- valeurs possibles de durée de vie des clés TEK: 1-604 800 secondes.

Les étendues effectives définies pour chacun des paramètres de configuration de l'interface BPI sont inférieures aux valeurs en service recommandées. Aux fins des essais de protocole, il convient d'appliquer au protocole BPI des valeurs de temporisation bien inférieures aux plus basses valeurs en service recommandées. De telles valeurs de temporisation "accélèrent" l'horloge de l'interface BPI, ce qui déclenche l'apparition d'événements de l'automate à états de protocole BPI à des intervalles bien plus rapprochés que dans une configuration "en service". Bien que les implémentations BPI ne doivent pas nécessairement être conçues pour fonctionner de manière efficace à ce rythme BPI accéléré, l'instance de protocole DEVRAIT fonctionner correctement à ces valeurs de temporisation écourtées. Le Tableau A.2 énumère les valeurs écourtées des paramètres qui sont susceptibles d'être employées pour les essais de conformité et de certification de protocole.

Tableau A.2/J.125 – Valeurs écourtées des paramètres de l'interface BPI pour les essais de protocole

Durée de vie de l'autorisation	5 min (300 s)
Durée de vie des clés TEK	3 min (180 s)
Délai de tolérance pour l'autorisation	1 min (60 s)
Délai de tolérance pour les clés TEK	1 min (60 s)

Le délai de tolérance pour les clés TEK DOIT être inférieur à la moitié de la durée de vie des clés TEK.

Annexe B

Vérification d'un logiciel d'exploitation téléchargé

B.1 Introduction

Le système DOCSIS assure le téléchargement du code vers les câblo-modems de son réseau. La provenance et l'intégrité du code téléchargé sont importantes pour la sécurité et le fonctionnement en général du système DOCSIS.

Le module de téléchargement de logiciels est une cible attrayante pour un attaquant. En effet, s'il réussissait à lancer une attaque graduelle contre le module de téléchargement de logiciels, un attaquant serait en mesure d'y installer un code permettant de neutraliser tous les câblo-modems d'un domaine ou de perturber le service à grande échelle. Pour déjouer de telles attaques, il faut mettre l'attaquant en situation d'avoir à surmonter plusieurs barrières de sécurité.

B.2 Aperçu général

Les prescriptions définies dans le présent paragraphe concernent les objectifs de sécurité primaire de la procédure de téléchargement de code:

- le câblo-modem devrait pouvoir certifier que le code de téléchargement qu'il a reçu provient d'un tiers connu et de confiance;
- le câblo-modem devrait pouvoir vérifier que le code téléchargé n'a subi aucune modification par rapport à la forme initiale sous laquelle il a été communiqué par le tiers de confiance;
- la procédure devrait viser à simplifier les modalités de traitement des fichiers de code du câblo-opérateur et à mettre en place à son intention des mécanismes lui permettant d'adapter vers le haut ou vers le bas la version de code des câblo-modems de son réseau;
- la procédure doit également permettre à un câblo-opérateur de déterminer et d'implémenter directement ses propres orientations de politique générale en ce qui concerne:
  a) les fichiers de code qu'accepteront les câblo-modems dans leur domaine de réseau;
  b) les commandes de sécurité définissant la sécurité de la procédure sur leur réseau;
- les câblo-modems doivent pouvoir se déplacer librement entre systèmes relevant de différentes organisations de câblo-opérateurs;
- clé publique d'autorité CA (facultatif): une mise à jour de la clé publique d'autorité CA qui remplace la clé publique d'autorité CA enregistré à ce moment dans le CM;
- le ou les certificats de fabricant (facultatif): un certificat de fabricant, au moins, conforme à X.509 qui remplace les certificats de fabricant enregistré à ce moment dans le CM.

Bien qu'il se limite à ces prescriptions de sécurité primaire, la présente Recommandation reconnaît que, dans certains cas, une sécurité plus poussée sera être souhaitable. Pour les différents câblo-opérateurs ou fabricants de câblo-modems, l'enjeu pourrait être d'accroître la sécurité en ce qui concerne la distribution et l'installation de code dans un câblo-modem ou un autre élément de réseau DOCSIS. La présente Recommandation ne limite en rien l'utilisation d'autres protections, pour autant que celles-ci ne soient pas en contradiction avec son objet et avec ses principes directeurs.

La protection et la vérification efficaces du téléchargement d'un code nécessitent plusieurs niveaux de protection.

- Le fabricant du câblo-modem qui en conçoit le code applique toujours une signature numérique au fichier de code, signature qui est vérifiée par une chaîne de certification remontant jusqu'à la racine DOCSIS. La signature du fabricant authentifie la provenance et

l'intégrité du fichier de code du câblo-modem. D'autres paramètres de commande sont incorporés dans le fichier de code pour assurer la commande d'accès au câblo-modem.

- Bien que le fabricant doive toujours signer son fichier de code, un câblo-opérateur peut ultérieurement joindre sa signature sous forme de code à la signature du fabricant. Le câblo-modem doit vérifier les deux signatures à l'aide d'une chaîne de certification remontant jusqu'à la racine DOCSIS, avant d'accepter un fichier de code.
- Les mécanismes du système d'appui à l'exploitation (OSS) pour la mise en service et la commande du câblo-modem sont importants pour la bonne exécution de cette procédure. La capacité de mise à jour du code d'un câblo-modem est activée pendant la procédure de mise en service et d'enregistrement. Les opérations de téléimportation de code sont lancées pendant la procédure de mise en service et d'enregistrement; elles peuvent aussi être lancées en service normal au moyen d'une commande SNMP (protocole simple de gestion de réseau).

Le fichier de code est créé à l'aide d'une structure conforme au système cryptographique à clés publiques (PKCS #7) qui a été définie dans un format expressément adapté aux câblo-modems DOCSIS. La structure du système DOCSIS PKCS #7 comprend les éléments suivants:

- l'image de code: l'image de code mise à jour;
- la signature de vérification du code (CVS, *code verification signature*): la signature numérique par rapport à l'image de code, et tout autre attribut authentifié tel que défini dans la structure du système DOCSIS PKCS #7;
- le certificat de vérification du code (CVC, *code verification certificate*): un certificat de structure conforme à X.509, qui est utilisé pour remettre et valider la clé publique de vérification de code qui permettra de vérifier la signature par rapport à l'image de code. L'autorité de certification DOCSIS – tiers de confiance, dont la clé publique est déjà enregistrée dans le câblo-modem – signe le certificat. Le certificat X.509 est défini dans un format expressément adapté aux câblo-modems DOCSIS.

La Figure B.1 indique les principales opérations à effectuer aux fins de la signature d'une image de code dans le cas où le fichier de code est signé uniquement par le fabricant du câblo-modem et dans le cas où le fichier de code est signé par le fabricant du câblo-modem et cosigné par un câblo-opérateur.

Chaque câblo-modem faisant partie du système DOCSIS recevra une clé publique sécurisée en provenance de l'autorité de certification racine DOCSIS. Le fabricant qui a conçu le code créera le fichier de code en signant l'image de code suivant une structure de signature numérique du système PKCS #7 au moyen d'un certificat DOCSIS X.509. Le fichier de code est ensuite envoyé au câblo-opérateur, lequel, en possession d'une clé publique racine DOCSIS, DEVRAIT vérifier que le fichier de code provient bien d'un fabricant DOCSIS de confiance et qu'il n'a pas été modifié. A ce stade, le câblo-opérateur peut soit charger le fichier de code tel quel dans le serveur TFTP ou y ajouter sa signature et son certificat CVC de câblo-opérateur. Pendant la procédure de mise à jour du code, le câblo-modem accédera au fichier de code à partir du serveur TFTP et vérifiera l'image de code avant de procéder à l'installation.

Alors que l'autorité CA racine DOCSIS pour la chaîne de certification du câblo-modem sert actuellement d'autorité CA pour le téléchargement de logiciel sécurisé, une autorité CA racine différente peut être utilisée à l'avenir. C'est pourquoi, le câblo-modem NE DOIT PAS supposer que le certificat CVC du fabricant et le certificat CVC du cosignataire proviennent de l'autorité CA racine DOCSIS pour la chaîne de certification du câblo-modem.

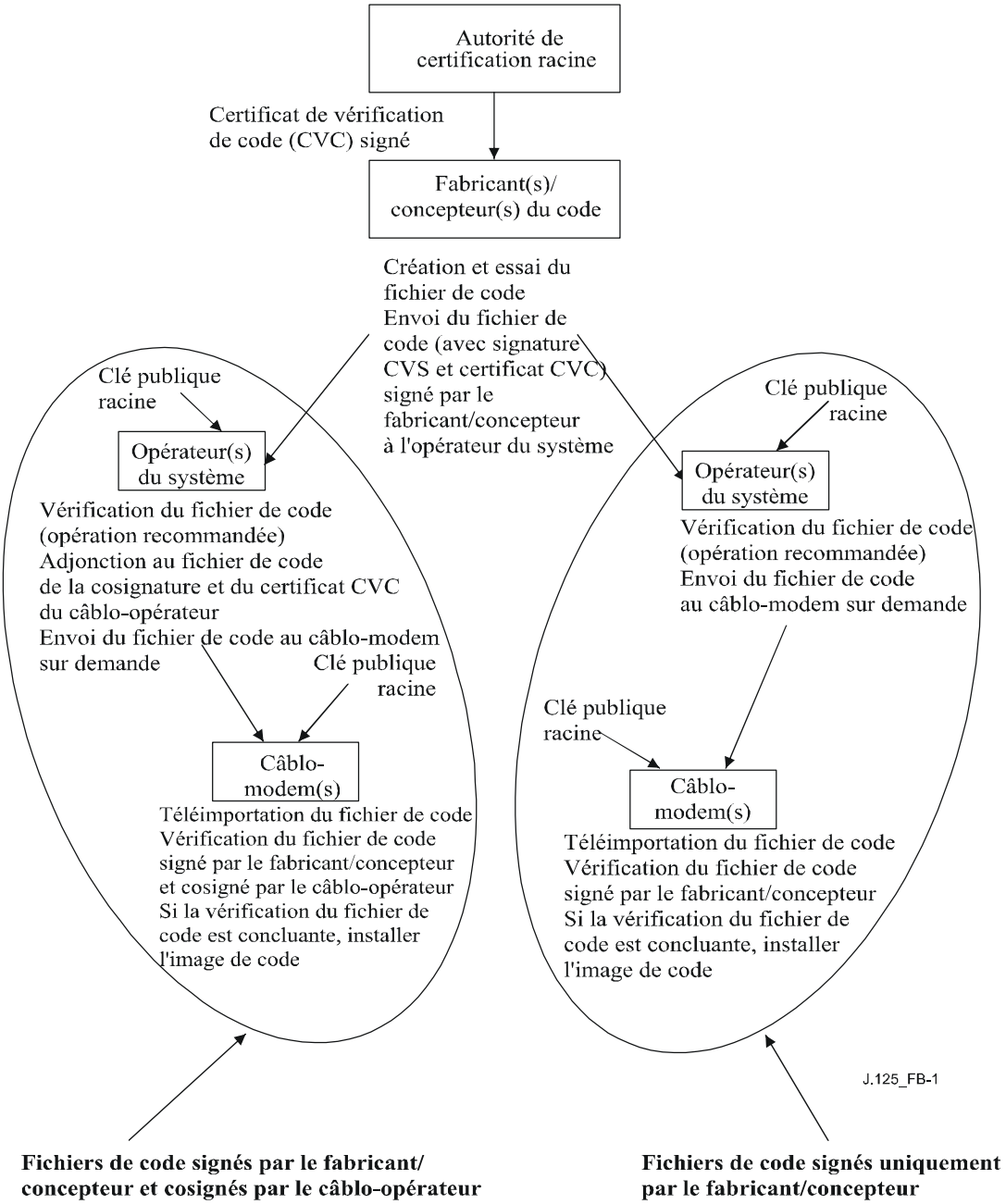


Figure B.1/J.125 – Hiérarchie type de validation de code

B.3 Prescriptions applicables à la mise à jour du code

Les prescriptions régissant la procédure de vérification de mise à jour du code sont définies dans les paragraphes qui suivent. Les mises à jour du code DOCSIS 1.1 ou 2.0 DOIVENT être préparées et vérifiées comme indiqué dans la présente Recommandation. Les câblo-modems certifiés DOCSIS 1.1 ou 2.0 DOIVENT procéder à la vérification des mises à jour du code comme indiqué dans la présente Recommandation, qu'ils fonctionnent ou non dans un mode conforme à DOCSIS 2.0, DOCSIS 1.1, ou DOCSIS 1.0. Les câblo-modems certifiés conformes à DOCSIS 1.1 et DOCSIS 2.0 DOIVENT procéder à la vérification des mises à jour du code comme indiqué dans la présente Recommandation, indépendamment du fait que la confidentialité de base soit activée ou désactivée.

B.3.1 Prescriptions applicables au fichier de code

Un seul fichier est utilisé pour encapsuler le code du câblo-modem. Le fichier de code est constitué d'un message de données signé du système DOCSIS PKCS #7 qui comprend:

1) la signature de vérification du code (CVS) du fabricant;
2) le certificat de vérification du code (CVC) du fabricant, signé par l'autorité de certification racine DOCSIS;
3) l'image de code (compatible avec le câblo-modem de destination) sous forme de contenu signé;
4) à titre facultatif, si le câblo-opérateur cosigne le fichier de code:
   a) la signature CVS du câblo-opérateur;
   b) le certificat CVC du câblo-opérateur, signé par l'autorité de certification racine DOCSIS;
5) clé publique d'autorité CA racine facultative pour la vérification du code CVC;
6) certificat(s) de fabricant facultatif(s).

Le fichier de code DOIT être conforme à la spécification du système [PKCS #7] et DOIT être codé en mode DER (règles de codage distinctives). Le fichier de code DOIT être conforme à la structure indiquée dans le Tableau B.1. Un exemple est donné dans l'Appendice I.

Tableau B.1/J.125 – Structure du fichier de code

Fichier de code	Description
Signature numérique du système PKCS #7 {	
ContentInfo	
contentType	SignedData
SignedData()	Valeur du contenu des données signées EXPLICITES X.509; englobe la signature CVS et le certificat CVC.
}	
SignedContent{	
DownloadParameters {	Format TLV obligatoire (Type 28) défini dans le § 7.2.2.28. (La longueur est de zéro s'il n'y a pas de sous-TLV.)
RootCAPublicKey()	TLV facultatif pour la clé publique d'autorité CA racine pour la vérification du code CVC, formaté en fonction du format TLV de la clé publique RSA (Type 4) défini dans le § 7.2.2.4.
MfgCerts()	TLV facultatif pour un ou plusieurs certificats de fabricant codés en mode DER, chacun formaté en fonction du format TLV du certificat CA (Type 17) défini dans le § 7.2.2.17.
}	
CodeImage()	Image du code mis à jour
}	

Si, au moment où il télécharge la clé publique d'autorité CA racine et/ou son certificat de fabricant en tant qu'éléments du fichier de code du CM, ceux-ci PEUVENT être inclus respectivement dans le champ RootCAPublicKey et/ou le champ MfgCerts comme l'indique le Tableau B.1 et être séparés de l'image de code proprement dite du câblo-modem contenu dans le champ CodeImage.

Cela permet, d'une part, de distinguer clairement l'image de code des autres paramètres figurant dans le fichier de téléchargement du code et, d'autre part, de modifier les clés publiques d'autorité CA racine, les certificats de l'autorité de certification du fabricant ou les paramètres SignedData figurant dans le fichier de téléchar gement du code sans que cela perturbe ou modifie l'image de code que le câblo-modem recevra. On peut ainsi vérifier que l'image de code n'a pas changé bien que le fichier de téléchargement de code ait changé en raison d'une modification dans les clés publiques d'autorité CA racine, les certificats de l'autorité de certification du fabricant ou les paramètres SignedData.

B.3.1.1 Données signées du système DOCSIS PKCS #7

Le fichier de mise à jour du logiciel contiendra dans un type de contenu de données signées du système PKCS #7 les informations indiquées ci-dessous. Bien qu'elle soit conforme au système [PKCS #7], la structure utilisée par DOCSIS a été restreinte dans son format pour faciliter les opérations de traitement qu'un câblo-modem effectue pour valider la signature. Les données signées du système PKCS #7 DOIVENT être codées en mode DER et correspondre exactement avec la structure indiquées dans le Tableau B.2, excepté pour tout changement dans l'ordre requis par codage en mode DER (par exemple, la commande d'attributs SET OF). Le CM DEVRAIT rejeter la signature du système PKCS #7 si les données signées du système PKCS #7 ne correspondent pas à la structure codée en mode DER présentée dans le Tableau B.2.

Tableau B.2/J.125 – Données signées du système DOCSIS PKCS #7

Champ PKCS #7	Description
Signed Data {	
version	version = 1
digestAlgorithmIdentifiers	SHA-1
contentInfo	
contentType	Données (SignedContent est concaténé à la fin de la structure [PKCS #7])
certificates {	Certificat de vérification de code (CVC) DOCSIS
mfgCVC	OBLIGATOIRE pour tous les fichiers de code
msoCVC	FACULTATIF; obligatoire en cas de cosignature de plusieurs câblo-opérateurs
} *end certificates*	
SignerInfo{	
MfgSignerInfo {	OBLIGATOIRE pour tous les fichiers de code
version	version = 1
issuerAndSerialNumber	Figure sur le certificat du signataire
issuerName	Nom distinctif de l'entité émettrice du certificat
CountryName	Etats-Unis d'Amérique
organizationName	Spécifications d'interface de service de données sur câble
organizationalUnitName	Câblo-modems
commonName	Autorité de certification racine du câblo-modem DOCSIS
certificateSerialNumber	Figure sur le certificat CVC, nombre entier, taille comprise entre (1..20) octets
digestAlgorithm	SHA-1

Tableau B.2/J.125 – Données signées du système DOCSIS PKCS #7

Champ PKCS #7	Description
authenticatedAttributes	
contentType	Données; type de contenu du contenu signé
signingTime	Temps UTC (GMT), YYMMDDhhmmssZ
messageDigest	Résumé du contenu tel que défini dans le [PKCS #7]
digestEncryptionAlgorithm	rsaEncryption
encryptedDigest	
} end mfg signer info	
MsoSignerInfo {	FACULTATIF; obligatoire en cas de cosignature de plusieurs câblo-opérateurs
version	version =1
issuerAndSerialNumber	Figure sur le certificat du signataire
issuerName	Nom distintif de l'émetteur du certificate
CountryName	US
organizationName	Spécifications d'interface de service de données sur câble
organizationalUnitName	Câblo-modems
commonName	Autorité de certification racine du câblo-modem DOCSIS
certificateSerialNumber	Figure sur le certificat CVC, nombre entier, taille comprise entre (1..20) octets
digestAlgorithm	SHA-1
authenticatedAttributes	
contentType	Données; type de contenu du contenu signé
signingTime	Temps UTC (GMT), YYMMDDhhmmssZ
messageDigest	Résumé du contenu tel que défini dans le [PKCS #7]
digestEncryptionAlgorithm	rsaEncryption
encryptedDigest	
} end mso signer info (fin des informations concernant le câble-opérateur signataire)	
} end signer info (fin des informations concernant le signataire)	
} end signed data(fin des données signées)	

B.3.1.1.1 Clés de signature de code

La signature numérique du système PKCS #7 utilise l'algorithme de cryptage RSA [RSA3] conjugué à l'algorithme SHA-1 [FIPS-186-2]. Le module de clés RSA pour la signature de code a une longueur de 1024 bits, 1536 bits ou 2048 bits. Le câblo-modem DOIT pouvoir vérifier les signatures de fichiers de code DOCSIS faites selon l'une ou l'autre taille de module. L'exposant public est F4 (65537 sous forme décimale).

B.3.1.1.2 Format du certificat de vérification de code

Le format retenu pour le certificat CVC est conforme à X.509. Toutefois, dans le cas présent, la structure X.509 a été simplifiée pour faciliter les opérations de traitement qu'un câblo-modem effectue pour valider le certificat et extraire la clé publique servant à vérifier la signature CVS. Le certificat CVS DOIT être codé en mode DER et correspondre exactement à la structure décrite dans le Tableau B.3 excepté pour tout changement dans l'ordre requis par codage en mode DER (par exemple, la commande d'attributs SET OF). Le CM DEVRAIT rejeter le certificat CVC s'il ne correspond pas à la structure codée en mode DER présentée dans le Tableau B.3.

Le certificat CVC impose en outre l'obligation d'ajouter l'identificateur de fonction de la clé pour la "signature du code" dans un champ utilisation de clé étendue.

```
-- extended key usage extension OID and syntax
id-ce-exKeyUsage OBJECT IDENTIFIER ::= {id-ce 37}
ExtKeyUsageSyntax ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId
KeyPuposeID ::= OBJECT IDENTIFIER
```

Le certificat CVC DOCSIS DOIT contenir un seul champ d'extension: l'extension d'utilisation de clé étendue. L'extension d'utilisation de clé étendue DOIT être marquée comme étant critique. L'extension d'utilisation de clé DOIT contenir l'identificateur OID de fonction du code aux fins de la signature de celui-ci. Si l'extension d'utilisation de clé étendue n'est pas présente, ou si elle n'est pas marquée comme étant critique, ou si elle comporte un identificateur OID de fonction de clé différent de l'identificateur de fonction de signature du code, ou s'ajoutant à celui-ci, le câblo-modem DOIT arrêter l'opération de validation et ignorer le certificat CVC.

```
-- extended key purpose OIDs
id-kp-codeSigning OBJECT IDENTIFIER::= { id-kp 3 }
```

Tableau B.3/J.125 – Certificat de vérification de code conforme à DOCSIS X.509

Champ de certificat X.509	Description
Certificate {	
tbsCertificate	
version	v3(2)
serialNumber	nombre entier, taile de (1..20) octets
signature	algorithme SHA-1 avec algorithme RSA, paramètres nuls
issuer	
countryName	Etats-Unis d'Amérique
organizationName	Spécifications d'interface de service de données sur câble
organizationalUnitName	Câblo-modems
commonName	Autorité de certification racine du câblo-modem DOCSIS
validity	
notBefore	Temps utc (GMT), YYMMDDhhmmssZ
notAfter	Temps utc (GMT), YYMMDDhhmmssZ
subject	
countryName	< pays de la société concernée >
organizationName	< agent signataire de code concerné >
organizationalUnitName	DOCSIS
commonName	Certificat de vérification du code

Tableau B.3/J.125 – Certificat de vérification de code conforme à DOCSIS X.509

Champ de certificat X.509	Description
subjectPublicKeyInfo	
algorithm	cryptage RSA, paramètres nuls
subjectPublicKey	Module à 1024 bits, 1536 bits, ou 2048 bits
extensions	
extKeyUsage	
critical	Vrai
keypurposeId	id-kp-codeSigning
signatureAlgorithm	algorithme SHA-1 avec algorithme RSA, paramètres nuls
signature Value	
} *end certificate (fin du certificat)*	

B.3.1.1.3 Annulation de certificats

La présente Recommandation n'impose pas et ne définit pas l'utilisation de listes d'annulation de certificats (CRL). La prise en charge de listes CRL par le câblo-modem n'est pas obligatoire. Les câblo-opérateurs pourront souhaiter définir et utiliser des listes CRL en dehors du réseau hybride à fibre optique/câble coaxial DOCSIS pour gérer plus facilement les fichiers de code que leur communiquent les fabricants.

Toutefois, il existe une méthode permettant d'annuler les certificats en fonction de leur date de début de validité (voir le § B.3.2.2). Cette méthode passe par la remise au câblo-modem d'un certificat CVC à jour indiquant l'heure de début de validité la plus récente. Une fois le certificat CVC dûment validé, l'heure de début de validité X.509 permettra de mettre à jour la valeur du champ *cvcAccessStart* du câblo-modem.

Pour activer la remise d'un certificat CVC actualisé sans que le câblo-modem doive procéder à une mise à jour du code, le certificat CVC PEUT être remis dans le fichier de configuration du câblo-modem ou dans une base d'informations de gestion (MIB) utilisant le protocole de transfert de fichiers simplifié (SNMP). Qu'il se trouve dans un fichier de code, dans un fichier de configuration ou dans une base MIB de protocole SNMP, le format d'un certificat CVC est le même.

B.3.1.2 Contenu signé

Le champ de contenu signé du fichier de code contient l'image de code et le champ des paramètres de téléchargement, qui peuvent éventuellement avoir deux éléments facultatifs supplémentaires – une clé publique d'autorité CA racine DOCSIS et un certificat de fabricant.

L'image de code finale est dans un format compatible avec le câblo-modem de destination. Conformément aux prescriptions du système [PKCS #7] en matière de signature, le contenu du code est introduit sous forme de données, c'est-à-dire sous la forme d'une simple chaîne d'octets. Le format de l'image de code finale n'est pas spécifié ici et sera défini par chaque fabricant en fonction de ses exigences.

Chaque fabricant DEVRAIT créer son code en y intégrant des mécanismes supplémentaires permettant de vérifier qu'une image de code mise à jour est compatible avec le câblo-modem de destination. Le câblo-modem NE DEVRAIT PAS installer l'image de code mise à jour avant d'avoir vérifié que celle-ci est compatible avec le CM.

Si elle est incluse dans le champ de contenu signé, il est prévu que la clé publique d'autorité CA racine DOCSIS remplace celle actuellement enregistrée dans le câblo-modem. Si le téléchargement et l'installation du code spécifiés dans le § B.3.5.1 sont réussis, alors le câblo-modem DOIT remplacer sa clé publique d'autorité CA racine DOCSIS actuellement enregistrée par celle reçue dans le champ de contenu signé. Cette nouvelle clé publique d'autorité CA racine DOCSIS sera utilisée pour les vérifications de certificat CVC suivant.

Si il est inclus dans le champ de contenu signé, il est prévu que le certificat de fabricant remplace celui actuellement enregistré dans le câblo-modem. Si le téléchargement et l'installation du code spécifiés dans le § B.3.5.1 sont réussis, alors le câblo-modem DOIT remplacer le certificat de fabricant actuellement enregistré par celui reçu dans le champ de contenu signé. Le nouveau certificat de fabricant sera alors envoyé au CMTS pendant l'initialisation de BPI+ suivant.

B.3.2 Commandes d'accès au fichier de code

Outre les commandes cryptographiques mises en œuvre par la signature numérique et par le certificat X.509, des valeurs de commande spéciales sont intégrées dans le fichier de code qu'il appartiendra au câblo-modem de vérifier avant de valider une image de code. Les valeurs de ces paramètres de commande DOIVENT satisfaire aux conditions requises avant que le câblo-modem valide le certificat CVC ou la signature CVS et accepte l'image de code.

B.3.2.1 Noms des organisations titulaires de certificat

Le câblo-modem reconnaîtra un maximum de deux noms, à un moment quelconque, pour un agent signataire de code qu'il considère comme étant de confiance, dans le champ *entité titulaire de certificat* d'un certificat CVC de fichier de code, à savoir:

- le fabricant du câblo-modem: le nom du fabricant inscrit dans le champ *entité titulaire de certificat* du certificat CVC du fabricant DOIT être rigoureusement identique au nom du fabricant enregistré par celui-ci dans la mémoire rémanente du câblo-modem. Un certificat CVC du fabricant DOIT être incorporé dans le fichier de code;
- un agent cosignataire: DOCSIS et le fabricant autorisent une autre organisation de confiance à cosigner les fichiers de code destinés à leurs câblo-modems. Dans la plupart des cas, il s'agit du câblo-opérateur qui a la haute main sur le domaine d'exploitation utilisé par le câblo-modem à la date considérée. Le nom de l'organisation de l'agent cosignataire est communiqué au câblo-modem via un certificat CVC de cosignataire dans le fichier de configuration lors de l'initialisation de la procédure de vérification du code du câblo-modem. Le nom de l'organisation du cosignataire qui figure dans le champ *entité titulaire de certificat* du certificat CVC du cosignataire DOIT être rigoureusement identique au nom de l'organisation du cosignataire précédemment reçu dans le certificat CVC d'initialisation du cosignataire et enregistré par le câblo-modem.

Le câblo-modem PEUT comparer les noms des organisations selon une méthode de comparaison binaire.

B.3.2.2 Commandes variables dans le temps

Conformément à la procédure de mise à jour du code, le câblo-modem DOIT conserver deux séries de valeurs temporelles UTC associées à chaque agent signataire du code. Une série DOIT toujours être enregistrée et tenue à jour pour le fabricant du câblo-modem. Au moment où il se voit affecter un agent cosignataire de code, le câblo-modem DOIT aussi enregistrer et tenir à jour une série distincte de valeurs temporelles pour l'agent cosignataire.

Ces valeurs sont utilisées pour assurer la commande d'accès du fichier de code au câblo-modem par un contrôle individuel de la validité de la signature CVS et du certificat CVC. Il s'agit des valeurs suivantes:

codeAccessStart: valeur temporelle UTC de 12 octets par référence au temps moyen de Greenwich (GMT, *Greenwich mean time*).

cvcAccessStart: valeur temporelle UTC de 12 octets par référence au temps GMT.

Les valeurs temporelles UTC figurant dans le certificat CVC DOIVENT être exprimées dans le temps moyen de Greenwich (GMT) et inclure les secondes. Autrement dit, elles DOIVENT être exprimées sous la forme suivante: YYMMDDhhmmssZ. Le champ année (YY) DOIT être interprété comme suit:

- pour les valeurs de YY égales ou supérieures à 50, il s'entend qu'il s'agit de l'année 19YY;
- pour les valeurs de YY inférieures à 50, il s'entend qu'il s'agira de l'année 20YY.

Etant donné que ces valeurs seront toujours établies par rapport au temps moyen de Greenwich (GMT), le dernier caractère ASCII (Z) peut être supprimé lorsqu'il est enregistré par le câblo-modem sous la forme des valeurs codeAccessStart ou cvcAccessStart. Le câblo-modem DOIT conserver chacune de ces valeurs temporelles dans un format équivalent, en termes d'informations de temps et de précision, au format UTC de 12 caractères (c'est-à-dire, YYMMDDhhmmss). Le câblo-modem DOIT comparer avec précision ces valeurs enregistrées aux valeurs temporelles UTC qui lui sont communiquées dans un certificat CVC. Ces prescriptions sont examinées plus loin dans la présente Recommandation.

Les valeurs codeAccessStart et cvcAccessStart correspondant au fabricant du câblo-modem NE DOIVENT PAS diminuer. Les valeurs codeAccessStart et cvcAccessStart correspondant à l'agent cosignataire NE DOIVENT PAS diminuer tant que le cosignataire ne change pas et que le câblo-modem tient à jour les valeurs de commande variables dans le temps de l'agent cosignataire.

B.3.3 Initialisation du câblo-modem aux fins de la mise à jour du code

Avant qu'il puisse procéder à la mise à jour du code, le câblo-modem doit être dûment initialisé. Le fabricant du câblo-modem s'attache donc en premier lieu à cette opération d'initialisation. Chaque fois qu'un câblo-modem est enregistré auprès d'un réseau DOCSIS, l'état d'initialisation dans lequel il se trouve DOIT être vérifié en fonction des besoins opérationnels du réseau en question. Il pourra s'avérer nécessaire de réinitialiser le câblo-modem lors de son enregistrement, surtout s'il s'est déplacé d'un réseau à un autre.

B.3.3.1 Initialisation par le fabricant

Il incombe au fabricant d'installer comme il se doit la version de code initiale dans le câblo-modem.

Aux fins de la vérification de la mise à jour du code, les valeurs des paramètres suivants DOIVENT être enregistrées dans la mémoire rémanente du câblo-modem:

1) le nom de l'organisation du fabricant du câblo-modem;
2) les valeurs de commande variables dans le temps du fabricant:
   a) la valeur d'initialisation codeAccessStart;
   b) la valeur d'initialisation cvcAccessStart.

Le nom de l'organisation du fabricant du câblo-modem DOIT toujours figurer dans le câblo-modem. Ce nom (paramètre organizationName) PEUT être enregistré dans l'image de code des câblo-modems. Dans des conditions normales, le paramètre organizationName du fabricant NE DEVRAIT PAS changer, mais la présente Recommandation n'interdit pas à un fabricant de modifier le mode d'enregistrement de ce paramètre dans le câblo-modem. Le nom du fabricant utilisé pour la mise à jour du code n'est pas nécessairement le même que celui qui est utilisé dans le certificat du fabricant DOCSIS.

Les valeurs de commande variables dans le temps codeAccessStart et cvcAccessStart DOIVENT être initialisées à une valeur temporelle UTC compatible avec l'heure de début de validité du dernier

certificat CVC du fabricant. Ces valeurs variables dans le temps seront mises à jour périodiquement en service normal au moyen des certificats CVC des fabricants reçus et vérifiés par le câblo-modem.

Au départ, le câblo-modem ne reconnaîtra aucun agent cosignataire.

B.3.3.2 Initialisation par le réseau

La méthode d'ouverture et d'obtention de fichiers de téléchargement de code de câblo-modem est définie dans [J.112-B] ou [J.122]. Aux fins de la vérification du code, le fichier de configuration est utilisé comme un moyen authentifié d'initialiser la procédure de vérification du code. Dans son fichier de configuration, le câblo-modem reçoit les réglages des paramètres de configuration se rapportant à la vérification de la mise à jour du code. Ces réglages NE DOIVENT PAS être utilisés avant que le système CMTS ait dûment enregistré le câblo-modem.

Le fichier de configuration DEVRAIT toujours comporter le plus récent certificat CVC applicable au câblo-modem de destination. Toutefois, lorsqu'il est utilisé pour lancer la procédure de mise à jour du code, le fichier de configuration DOIT comporter un certificat de vérification de code (CVC) pour initialiser le câblo-modem aux fins de l'acceptation des fichiers de code conformément à la présente Recommandation. Qu'il soit ou non nécessaire de procéder à la mise à jour du code, un certificat CVC figurant dans le fichier de configuration DOIT être traité par le câblo-modem.

Un fichier de configuration PEUT contenir:

- aucun certificat CVC;
- un certificat CVC de fabricant seulement;
- un certificat CVC de cosignataire (câblo-opérateur) seulement;
- un certificat CVC de fabricant et un certificat CVC de cosignataire.

Avant qu'il n'active sa capacité à mettre à jour les fichiers de code sur le réseau, le câblo-modem DOIT recevoir un certificat CVC valide dans un fichier de configuration et être dûment enregistré auprès du système CMTS. En outre, lorsque son fichier de configuration ne contient pas de certificat CVC valide et que sa capacité à mettre à jour les fichiers de code a été désactivée, le câblo-modem DOIT ignorer les informations contenues dans un certificat CVC qui lui sera remis ultérieurement via le protocole SNMP.

Lorsque son fichier de configuration ne contient qu'un certificat CVC valide émanant du fabricant, le câblo-modem devra uniquement faire signer les fichiers de code par le fabricant. Dans ce cas, le câblo-modem NE DOIT PAS accepter de fichiers de code qui ont été cosignés.

Lorsque le fichier de configuration du câblo-modem contient un certificat CVC de cosignataire, celui-ci est utilisé pour initialiser le câblo-modem par l'intermédiaire d'un agent cosignataire. Une fois validé, le nom de l'organisation titulaire du certificat CVC sera attribué à l'agent cosignataire de code affecté au câblo-modem. Afin qu'un câblo-modem puisse ultérieurement accepter une image de code, le cosignataire et le fabricant du câblo-modem DEVRONT avoir signé le fichier de code.

Le nom de l'organisation du fabricant du câblo-modem et les valeurs de commande variables dans le temps du fabricant DOIVENT figurer dans le câblo-modem. Si celui-ci est initialisé de manière à accepter le code cosigné par un autre agent signataire du code, le nom de l'organisation et ses valeurs de commande variables dans le temps correspondantes DOIVENT être enregistrés et conservés tant qu'ils sont utilisés. De la place DOIT être réservée dans la mémoire du câblo-modem pour les valeurs de commande de cosignataire suivantes:

1) nom de l'organisation de l'agent cosignataire;
2) valeurs de commande variables dans le temps du cosignataire:
   a) cvcAccessStart;
   b) codeAccessStart.

La série de valeurs ainsi fournies par le fabricant DOIT être enregistrée dans la mémoire rémanente du câblo-modem pour ne pas se perdre en cas de coupure de la source d'alimentation principale ou en cas de réinitialisation de celui-ci. En cas d'affectation au câblo-modem d'un cosignataire, la série de valeurs fournies par le cosignataire DOIT être enregistrée dans la mémoire du câblo-modem. Le câblo-modem PEUT garder ces valeurs dans une mémoire rémanente, qui ne sera pas perdue en cas de coupure de la source d'alimentation principale ou en cas de réinitialisation de celui-ci. Toutefois, si un cosignataire est affecté au câblo-modem, le certificat CVC se trouve toujours dans le fichier de configuration. En conséquence, le câblo-modem recevra toujours les valeurs de commande de cosignataire pendant la phase d'initialisation, et il n'est pas nécessaire d'enregistrer les valeurs de commande variables dans le temps du cosignataire dans la mémoire rémanente du câblo-modem en cas de coupure de l'alimentation principale du câblo-modem ou en cas de réinitialisation de celui-ci.

B.3.3.2.1 Traitement du certificat CVC du fichier de configuration

Lorsqu'un certificat CVC est incorporé dans le fichier de configuration DOCSIS 1.1 ou 2.0, le câblo-modem DOIT vérifier ce certificat avant d'accepter les éventuels réglages de mise à jour de code qu'il contient. Dès réception du certificat CVC dans le fichier de configuration, le câblo-modem DOIT exécuter les opérations de validation et de procédure suivantes. Si l'une quelconque des opérations de vérification suivantes échoue, le câblo-modem DOIT arrêter immédiatement la procédure de vérification du certificat CVC et consigner l'erreur, s'il y a lieu. Si son fichier de configuration ne contient pas de certificat CVC dûment validé, le câblo-modem NE DOIT PAS télécharger la mise à jour des fichiers de code, que cette opération soit déclenchée par son fichier de configuration ou via une base MIB utilisant le protocole SNMP. En outre, si les fichiers de configuration ne contiennent pas de certificat CVC dûment validé, le câblo-modem n'aura pas à traiter les certificats CVC qu'il recevra ultérieurement via une base MIB utilisant le protocole SNMP et NE DOIT PAS accepter d'informations extraites d'un certificat CVC qu'il recevra ultérieurement via une telle base.

Lorsqu'il reçoit le certificat CVC dans son fichier de configuration, et après s'être dûment enregistré auprès du système CMTS, le câblo-modem DOIT:

1) vérifier que l'extension d'utilisation de clé étendue figure bien dans le certificat CVC comme indiqué dans le § B.3.1.1.2.

2) vérifier le nom de l'organisation titulaire du certificat CVC.

   Si le certificat CVC est un certificat CVC de fabricant (type 32), alors:

   a) SI le nom de l'organisation est identique au nom du fabricant du câblo-modem, ALORS il s'agit du certificat CVC du fabricant. Dans ce cas, le câblo-modem DOIT vérifier que la valeur de l'heure de début de validité du certificat CVC du fabricant est supérieure ou égale à la valeur cvcAccessStart du fabricant alors en mémoire dans le câblo-modem.

   b) SI le nom de l'organisation n'est pas identique au nom du fabricant du câblo-modem, ALORS le certificat CVC DOIT être rejeté et l'erreur consignée.

   Si le certificat CVC est un certificat CVC de cosignataire (type 33), alors:

   a) SI le nom de l'organisation est identique au nom de l'agent qui a cosigné le code à la date considérée, ALORS il s'agit du certificat CVC de l'agent cosignataire et le câblo-modem DOIT vérifier que la valeur de l'heure de début de validité du certificat CVC du fabricant est supérieure ou égale à la valeur cvcAccessStart du cosignataire alors en mémoire dans le câblo-modem.

   b) SI le nom de l'organisation n'est pas identique au nom de l'agent qui a cosigné le code à la date considérée, ALORS, une fois que le certificat CVC aura été dûment validé (et que l'enregistrement aura été réalisé), le nom de l'organisation titulaire du certificat deviendra celui du nouvel agent cosignataire du code du câblo-modem. Le câblo-modem NE DOIT PAS accepter un fichier de code si celui-ci n'a pas été signé par le fabricant et cosigné par ledit agent cosignataire.

3) Valider la signature du certificat à l'aide de la clé racine DOCSIS en mémoire dans le câblo-modem. La vérification de la signature du certificat CVC permettra d'authentifier la provenance et de valider la fiabilité des paramètres du certificat CVC.

4) Actualiser la valeur attribuée dans le câblo-modem aux valeurs cvcAccessStart et codeAccesStart correspondant au nom de l'organisation titulaire du certificat CVC (c'est-à-dire le fabricant ou l'agent cosignataire du code) par rapport à la valeur de début de validité figurant dans le certificat CVC validé. Si la valeur de l'heure de début de validité du certificat CVC du fabricant est supérieure à la valeur cvcAccessStart alors en mémoire dans le câblo-modem, il faut mettre à jour le paramètre codeAccessStart du câblo-modem avec la valeur de l'heure de début de validité. Le câblo-modem DEVRAIT ignorer tous les éléments restants du certificat CVC.

B.3.3.2.2 Traitement du certificat CVC remis via le protocole SNMP

Le câblo-modem DOIT traiter les certificats CVC remis via le protocole SNMP lorsqu'ils sont activés aux fins de la mise à jour des fichiers de code; dans le cas contraire, tous les certificats CVC remis via le protocole SNMP DOIVENT être rejetés. Lorsqu'il valide le certificat CVC remis via le protocole SNMP, le câblo-modem DOIT exécuter les opérations de validation et de procédure suivantes. Si l'une quelconque des opérations de vérification suivantes échoue, le câblo-modem DOIT arrêter immédiatement la procédure de vérification du certificat CVC, consigner l'erreur s'il y a lieu, et supprimer tous les éléments qui pourraient subsister à l'issue de cette opération.

Le câblo-modem DOIT:

1) vérifier que l'extension d'utilisation de clé étendue figure dans le certificat CVC comme indiqué dans le § B.3.1.1.2;

2) vérifier le nom de l'organisation titulaire du certificat CVC.

   a) SI le nom de l'organisation est identique au nom du fabricant du câblo-modem, ALORS il s'agit du certificat CVC du fabricant. Dans ce cas, le câblo-modem DOIT vérifier que la valeur de l'heure de début de validité du certificat CVC du fabricant est supérieure à la valeur cvcAccessStart du fabricant alors en mémoire dans le câblo-modem.

   b) SI le nom de l'organisation est identique au nom de l'agent qui a cosigné le code à la date considérée, ALORS il s'agit du certificat CVC de l'agent cosignataire et le câblo-modem DOIT vérifier que la valeur de l'heure de début de validité du certificat CVC du fabricant est supérieure à la valeur codeAccessStart du cosignataire alors en mémoire dans le câblo-modem.

   c) SI le nom de l'organisation n'est pas identique au nom du fabricant du câblo-modem ou au nom de l'agent qui a cosigné le code à la date considérée, ALORS le certificat CVC DOIT être rejeté immédiatement.

3) Valider la signature du certificat à l'aide de la clé racine DOCSIS en mémoire dans le câblo-modem. La vérification de la signature du certificat CVC permettra d'authentifier la provenance et de valider la fiabilité des paramètres du certificat CVC.

4) Actualiser la valeur attribuée à cvcAccessStart, par rapport à la valeur de l'heure de début de validité du certificat CVC validé. Si la valeur de l'heure de début de validité du certificat CVC du fabricant est supérieure à la valeur codeAccessStart alors en mémoire dans le câblo-modem, il faut mettre à jour le paramètre codeAccessStart du câblo-modem avec la valeur de l'heure de début de validité. N'étant plus nécessaires, EXCEPTE l'heure de début de validité, tous les paramètres du certificat DEVRAIENT être ignorés.

B.3.4 Prescriptions applicables à la signature du code

Les procédures suivantes DOIVENT être appliquées pour la signature des fichiers de code.

B.3.4.1 Prescriptions auxquelles doit se conformer l'autorité de certification DOCSIS

Outre les certificats de fabricant DOCSIS qu'elle délivre aux fabricants selon les modalités décrites précédemment dans la présente Recommandation, l'autorité de certification racine DOCSIS délivrera des certificats de signature de code appelés certificats de vérification de code (CVC).

Le certificat de vérification de code (CVC) est fourni par l'autorité de certification DOCSIS et signé par la clé racine (DRK) DOCSIS. Les certificats CVC signés par l'autorité de certification DOCSIS DOIVENT se présenter exactement sous la forme spécifiée dans le § B.3.1.1.2 et ne doivent être utilisés que pour valider les signatures de code des câblo-modems DOCSIS. L'autorité de certification DOCSIS NE DOIT PAS signer de certificat CVC non conforme au format spécifié dans ledit paragraphe. Avant de signer un certificat CVC DOCSIS, l'autorité de certification DOIT vérifier que l'agent signataire de code est dûment agréé et habilité à agir en tant que tel.

L'autorité de certification sera chargée de tenir un registre des noms des agents signataires de code agréés. Comptent parmi les agents signataires de code les fabricants de câblo-modems et les câblo-opérateurs qui cosigneront les images de code des câblo-modems. Il incombe à l'autorité de certification DOCSIS de garantir que le nom de l'organisation de chaque agent signataire de code soit différent. Les principes suivants DOIVENT être appliqués afin d'attribuer des noms d'organisations des cosignataires de code:

- le nom d'organisation utilisé par un agent cosignataire de code pour s'identifier dans un certificat CVC DOIT être attribué par DOCSIS;
- ce nom DOIT être une chaîne imprimable de huit chiffres hexadécimaux permettant d'identifier de manière unique un agent signataire de code parmi tous les autres agents;
- chaque chiffre hexadécimal composant le nom DOIT être choisi dans la série de caractères 0-9 (0x30-0x39) ou A-F (0x41-0x46);
- la chaîne constituée de huit chiffres 0 n'est pas autorisée et NE DOIT PAS être utilisée dans un certificat CVC.

B.3.4.2 Prescriptions de fabrication

Pour signer ses fichiers de code, le fabricant DOIT se procurer un certificat CVC en bonne et due forme auprès de l'autorité de certification DOCSIS. Toutes les images de code du fabricant communiquées à un câblo-opérateur aux fins de la mise à jour à distance d'un câblo-modem faisant partie d'un réseau hybride à fibre optique/câble coaxial DOCSIS DOIVENT être signées conformément aux prescriptions définies dans la présente Recommandation.

Au moment où il signe un fichier de code, un fabricant PEUT décider de ne pas actualiser la valeur signingTime (heure de signature) du système [PKCS #7] figurant dans les informations de signature du fabricant. La présente Recommandation exige que la valeur signingTime du système [PKCS #7] soit égale ou supérieure à celle de l'heure de début de validité du certificat CVC. Si le fabricant utilise une valeur signingTime égale à celle de l'heure de début de validité du certificat CVC au moment où il signe une série de fichiers de code, ceux-ci pourront être utilisés et réutilisés, notamment par un câblo-opérateur pour mettre à jour la version de code des câblo-modems de ce fabricant ou revenir à une version antérieure. Ces fichiers de code conserveront leur validité jusqu'à ce qu'un nouveau certificat CVC soit établi et reçu par le câblo-modem. Il est recommandé à tout fabricant de procéder de cette manière pour signer ses fichiers de code lorsque DOCSIS et sa politique générale en matière de sécurité le lui permettent (voir § B.4).

Pour sauvegarder la capacité de stockage, le câblo-modem PEUT enregistrer dans sa mémoire interne le nom de l'agent cosignataire de code dans un autre format, à condition que toutes les informations soient conservées et que le format initial puisse être reproduit; par exemple, sous la forme d'un nombre entier non nul de 32 bits, avec une valeur entière de 0 représentant l'absence d'agent signataire de code.

B.3.4.3 Prescriptions imposées aux câblo-opérateurs

Le fabricant communiquera aux câblo-opérateurs DOCSIS les fichiers de code dont ils ont besoin pour mettre à jour leurs logiciels. A l'aide de la clé publique racine DOCSIS, le câblo-opérateur devrait vérifier que l'image de code se présente bien telle qu'elle a été constituée par le fabricant de confiance. Le câblo-opérateur peut procéder à tout moment à une nouvelle vérification du fichier de code en relançant la procédure.

Le câblo-opérateur a la possibilité de cosigner l'image de code destinée à un câblo-modem de son réseau. Pour ce faire, il cosigne le contenu des fichiers conformément aux normes de signature du système [PKCS #7] et y joint son certificat CVC DOCSIS signé. DOCSIS n'oblige pas le câblo-opérateur à cosigner les fichiers de code; toutefois, lorsque le câblo-opérateur se conforme à toutes les règles définies dans la présente Recommandation pour établir un fichier de code, le câblo-modem DOIT accepter ce fichier.

Toutes les images de code téléchargées dans un câblo-modem par l'intermédiaire du réseau hybride à fibre optique coaxial DOCSIS DOIVENT être signées conformément aux prescriptions définies dans la présente Recommandation.

B.3.5 Prescriptions de vérification de code

La nouvelle version d'un code NE DOIT PAS être installée si sa fiabilité n'a pas été établie selon la procédure de vérification décrite dans la présente Recommandation.

Le câblo-modem DOIT pouvoir traiter une signature numérique [PKCS #7] et un certificat X.509 comme indiqué dans la présente Recommandation. Il n'a pas à satisfaire à la totalité des spécifications [PKCS #7] et X.509.

B.3.5.1 Opérations de vérification du code d'un câblo-modem

Pour télécharger son code, le câblo-modem DOIT procéder en suivant les opérations de vérification décrites dans le présent paragraphe. Si l'une quelconque des opérations de vérification échoue, le câblo-modem DOIT arrêter immédiatement la procédure de téléchargement, consigner l'erreur s'il y a lieu, supprimer tous les éléments qui pourraient subsister à l'issue de cette opération, et continuer à utiliser son code existant. Les opérations de vérification peuvent être réalisées dans n'importe quel ordre si toutes les opérations applicables présentées dans ce paragraphe sont effectuées.

1) Le câblo-modem DOIT valider les informations de signature du fabricant en vérifiant:
   a) que la valeur signingTime (heure de signature) du système [PKCS #7] est égale ou supérieure à la valeur codeAccessStart du fabricant en mémoire dans le câblo-modem au moment considéré;
   b) que la valeur signingTime du système [PKCS #7] est égale ou supérieure à la valeur de l'heure de début de validité du certificat CVC du fabricant;
   c) que la valeur signingTime du système [PKCS #7] est inférieure ou égale à la valeur de l'heure de fin de validité du certificat CVC du fabricant.
2) Le câblo-modem DOIT valider le certificat CVC du fabricant en vérifiant:
   a) que le nom de l'organisation titulaire du certificat CVC est identique au nom du fabricant enregistré dans la mémoire du câblo-modem au moment considéré;
   b) que la valeur de l'heure de début de validité du certificat CVC est égale ou supérieure à la valeur cvcAccessStart du fabricant en mémoire dans le câblo-modem au moment considéré;
   c) que l'extension d'utilisation de clé étendue figure bien dans le certificat CVC comme indiqué dans le § B.3.1.1.2.
3) Le câblo-modem doit valider la signature du certificat à l'aide de la clé racine DOCSIS en mémoire dans le câblo-modem. La vérification de la signature du certificat CVC permettra

d'authentifier la provenance et de valider la fiabilité de la clé de vérification de code (CVK, *code verification key*). Une fois que la fiabilité de la clé CVK a été établie, tous les paramètres du certificat, EXCEPTE l'heure de début de validité, ne sont plus nécessaires et DEVRAIENT être ignorés.

4) Le câblo-modem DOIT vérifier la signature du fichier de code du fabricant.

   a) Le câblo-modem DOIT réaliser une nouvelle dispersion SHA-1 concernant le contenu signé. Si la valeur du messageDigest ne correspond pas à la nouvelle dispersion, le câblo-modem doit considérer la signature sur le fichier de code comme n'étant pas valide.

   b) Si la signature n'est pas authentifiée, tous les éléments du fichier de code (y compris l'image de code) ainsi que les valeurs découlant éventuellement de la procédure de vérification DOIVENT être rejetés et DEVRAIENT être immédiatement ignorés.

5) Si la signature du fabricant est authentifiée et si la signature d'un agent cosignataire est nécessaire:

   a) le câblo-modem DOIT valider les informations de signature du cosignataire en vérifiant:

      1) que celles-ci figurent bien dans le fichier de code;

      2) que la valeur signingTime [PKCS #7] est égale ou supérieure à la valeur codeAccessStart correspondante en mémoire dans le câblo-modem au moment considéré;

      3) que la valeur signingTime [PKCS #7] est égale ou supérieure à la valeur de l'heure de début de validité du CVC correspondante;

      4) que la valeur signingTime [PKCS #7] est inférieure ou égale à la valeur de l'heure de fin de validité du certificat CVC correspondante;

   b) le câblo-modem DOIT valider le certificat CVC du cosignataire en vérifiant:

      1) que le nom de l'organisation titulaire du certificat CVC est identique au nom de l'organisation du cosignataire en mémoire dans le câblo-modem au moment considéré;

      2) que la valeur de l'heure de début de validité du certificat CVC est égale ou supérieure à la valeur cvcAccessStart en mémoire dans le câblo-modem au moment considéré pour le nom de l'organisation titulaire correspondante;

      3) que l'extension d'utilisation de clé étendue figure bien dans le certificat CVC comme indiqué dans le § B.3.1.1.2;

   c) le câblo-modem DOIT valider la signature du certificat au moyen de la clé racine DOCSIS qu'il a en mémoire. La vérification de la signature permettra d'authentifier la provenance de la clé de vérification de code (CVK) publique du cosignataire et de confirmer la fiabilité de la clé. Dés l'instant où la fiabilité de la clé CVK du cosignataire a été établie, les paramètres qui restent dans le certificat, EXCEPTE l'heure de début de validité, ne sont plus d'aucune utilité et DEVRAIENT être supprimés;

   d) le câblo-modem DOIT vérifier la signature du fichier de code du cosignataire;

   e) le câblo-modem DOIT réaliser une nouvelle opération de dispersion d'algorithme SHA-1 concernant le contenu signé. Si la valeur du résumé du message ne correspond pas à la nouvelle dispersion, le CM DOIT considérer que la signature du fichier de code n'est pas valide;

   f) si la signature n'est pas authentifiée, tous les éléments du fichier de code (y compris l'image de code) ainsi que les valeurs découlant éventuellement de la procédure de vérification DOIVENT être rejetés et DEVRAIENT être immédiatement ignorés.

6) Si la signature du fabricant, et éventuellement celle du cosignataire, a été authentifiée, l'image de code est sécurisée et peut être installée. Avant de procéder à cette opération, tous les autres éléments du fichier de code ainsi que les valeurs éventuelles découlant de la procédure de vérification, à l'exception des valeurs signingTime [PKCS #7] et des valeurs de début de validité du certificat CVC, DEVRAIENT être immédiatement ignorés.

7) Le câblo-modem peut mettre à jour son logiciel en installant le fichier de code conformément à [J.112-B].

8) Si l'installation du code est infructueuse, le câblo-modem DOIT ignorer les valeurs signingTime [PKCS #7] et les valeurs de début de validité du certificat CVC qu'il vient de recevoir dans le fichier de code. Exécuter successivement les opérations indiquées dans [J.112-B] pour remédier à cet état de dérangement.

9) Lorsque l'installation du code est fructueuse, le câblo-modem DOIT mettre à jour les commandes variables dans le temps du fabricant par rapport aux valeurs figurant dans les informations de signature et dans le certificat CVC du fabricant:

   a) mettre à jour la valeur codeAccessStart considérée par rapport à la valeur recommandée signingTime [PKCS #7];

   b) mettre à jour la valeur cvcAccessStart considérée par rapport à la valeur de début de validité du certificat CVC.

10) Lorsque l'installation du code est fructueuse et SI le fichier de code a été cosigné, le câblo-modem DOIT mettre à jour les commandes variables dans le temps du cosignataire par rapport aux valeurs figurant dans les informations de signature et dans le certificat CVC du cosignataire:

   a) mettre à jour la valeur codeAccessStart considérée par rapport à la valeur signingTime [PKCS #7];

   b) mettre à jour la valeur cvcAccessStart considérée par rapport à la valeur de début de validité du certificat CVC.

B.3.6 Interopérabilité DOCSIS 1.0

Les câblo-modems conformes à DOCSIS 1.1 ou 2.0 DOIVENT vérifier les versions de code actualisées conformément à la présente Recommandation, même lorsqu'ils fonctionnent dans un environnement utilisant DOCSIS 1.0.

Les fichiers de configuration conformes à DOCSIS 1.0 conçus pour des câblo-modems conformes à DOCSIS 1.1 ou 2.0 DOIVENT satisfaire aux caractéristiques des fichiers de configuration définies dans la présente Recommandation.

Les câblo-modems conformes à DOCSIS 1.1 ou 2.0 DOIVENT être munis de fichiers de code conformes à DOCSIS 1.1 ou 2.0. La mise à jour des fichiers s'effectue via le système DOCSIS 1.0 tel quel, et n'exigera aucune modification des caractéristiques de traitement des fichiers de code de DOCSIS 1.0.

Dans un environnement conforme à DOCSIS 1.0 dans lequel des câblo-modems conformes à DOCSIS 1.1 ou 2.0 sont munis de fichiers de code actualisés, le gestionnaire SNMP DEVRAIT pouvoir accéder aux bases MIB définies pour la procédure de vérification de code spécifiée dans DOCSIS 1.1 ou 2.0. La possibilité d'utiliser cette capacité MIB est importante pour assurer le fonctionnement convenable et sécurisé de la procédure de mise à jour de code spécifiée dans DOCSIS 1.1 ou 2.0.

B.3.7 Codes d'erreur

Des codes d'erreur sont définis pour signaler les états de dérangement possibles pendant la procédure de vérification du code. Les directives de description et d'utilisation de ces codes d'erreur se trouvent en Appendice H de [SCTE23-3] ou en Annexe D de [SCTE79-2].

1) Erreurs de commande des fichiers de code:
   a) Le nom de l'organisation du titulaire du certificat CVC du fabricant n'est pas le même que le nom du fabricant enregistré dans la mémoire du câblo-modem.
   b) Le nom de l'organisation titulaire du certificat CVC de l'agent cosignataire du code n'est pas le même que le nom de l'agent cosignataire du code en mémoire dans le câblo-modem.
   c) La valeur signingTime PKCS #7 du fabricant est inférieure à la valeur codeAccessStart en mémoire dans le câblo-modem.
   d) La valeur de l'heure de début de validité PKCS #7 du fabricant est inférieure à la valeur cvcAccessStart en mémoire dans le câblo-modem.
   e) La valeur de l'heure de début de validité du certificat CVC du fabricant est inférieure à la valeur cvcAccessStart en mémoire dans le câblo-modem.
   f) La valeur signingTime PKCS #7 du fabricant est inférieure à la valeur de l'heure de début de validité du certificat CVC.
   g) Absence ou erreur de l'extension de l'utilisation de clé étendue dans le certificat CVC du fabricant.
   h) La valeur signingTime PKCS #7 du cosignataire est inférieure à la valeur codeAccessStart en mémoire dans le câblo-modem.
   i) La valeur de l'heure de début de validité PKCS #7 du cosignataire est inférieure à la valeur cvcAccessStart en mémoire dans le câblo-modem.
   j) La valeur de l'heure de début de validité du certificat CVC du cosignataire est inférieure à la valeur cvcAccessStart en mémoire dans le câblo-modem.
   k) La valeur signingTime PKCS #7 du cosignataire est inférieure à la valeur de l'heure de début de validité du certificat CVC.
   l) Absence ou erreur de l'extension d'utilisation de clé étendue dans le certificat CVC du cosignataire.
2) Echec de la validation du certificat CVC du fabricant dans le fichier de code.
3) Echec de la validation de la signature CVS du fabricant dans le fichier de code.
4) Echec de la validation du certificat CVC du cosignataire dans le fichier de code.
5) Echec de la validation de la signature CVS du cosignataire dans le fichier de code.
6) Erreur de format du certificat CVC dans le fichier de configuration:
   a) absence ou erreur de l'attribut d'utilisation de clé.
7) Echec de la validation du certificat CVC dans le fichier de configuration.
8) erreur de format du certificat CVC utilisant le protocole SNMP.
   a) Le nom de l'organisation titulaire du certificat CVC du fabricant n'est pas le même que le nom du fabricant du câblo-modem.
   b) Le nom de l'organisation titulaire du certificat CVC de l'agent cosignataire du code n'est pas le même que le nom de l'agent cosignataire du code du câblo-modem considéré.
   c) La valeur de l'heure de début de validité du certificat CVC est inférieure ou égale à la valeur cvcAccessStart correspondante de l'organisation titulaire du certificat en mémoire dans le câblo-modem.
   d) Absence ou erreur de l'attribut d'utilisation de clé.
9) Echec de la validation du certificat CVC utilisant le protocole SNMP.

B.4 Considérations sur la sécurité (Informatif)

La protection des clés privées est un élément essentiel pour assurer la sécurité. Les utilisateurs autorisés à signer des codes, c'est-à-dire les fabricants et les opérateurs auxquels des certificats de vérification de signatures de code (CVC) ont été délivrés par l'autorité de certification DOCSIS racine, doivent protéger leurs clés privées. Un attaquant ayant accès à la clé privée d'un utilisateur signataire de code agréé peut créer, à sa guise, des fichiers de code qui pourraient être utilisés sur un grand nombre de câblo-modems.

La parade contre une telle attaque consiste, pour l'opérateur, à annuler le certificat dont l'attaquant a eu connaissance de la clé privée de signature de code. Pour annuler un certificat, l'opérateur doit remettre à chaque câblo-modem concerné un nouveau certificat CVC portant une heure de début de validité postérieure à celle qui figure sur le certificat à annuler. Le nouveau certificat CVC peut être remis par l'un quelconque des mécanismes autorisés: fichier de confirmation, fichier de code ou base MIB utilisant le protocole SNMP. Le nouveau certificat CVC annule implicitement tous les certificats dont l'heure de début de validité est antérieure à celle qui figure sur le nouveau certificat CVC.

Pour moins s'exposer à ce genre d'attaque, un opérateur doit impérativement mettre à jour régulièrement le certificat CVC en mémoire dans chaque câblo-modem, à un rythme comparable à celui auquel il procéderait à la mise à jour d'une liste d'annulations de certificats (CRL) s'il disposait d'une telle liste. Des mises à jour régulières permettent de limiter l'intervalle de temps pendant lequel une clé de signature de code connue de l'attaquant lui est utile. Quel que soit le stade où il en est dans le cycle de mise à jour des certificats CVC, l'opérateur devrait aussi les remettre à jour s'il y a lieu de penser qu'une clé de signature de code a été violée. Pour mettre à jour son certificat, l'utilisateur doit se faire délivrer par l'autorité de certification DOCSIS un certificat CVC dont l'heure de début de validité est postérieure à celle du certificat CVC en mémoire dans le câblo-modem. Cela signifie que l'autorité de certification DOCSIS racine doit délivrer régulièrement des nouveaux certificats CVC à tous les fabricants et opérateurs signataires de code agréés, pour leur permettre de mettre à jour leurs certificats. Il est à prévoir que la spécification DOCSIS décidera de la politique de implémentée de son calendrier d'émission de nouveaux certificats CVC, calendrier sur lequel les opérateurs souhaiteront vraisemblablement coordonner leur politique de mise à jour.

Lorsqu'un câblo-modem tente de s'inscrire auprès du réseau pour la première fois ou après être resté déconnecté pendant un certain temps, un certificat CVC sécurisé doit impérativement lui être communiqué dans les meilleurs délais. Il pourra ainsi recevoir le plus récent certificat CVC disponible et refuser l'accès aux certificats CVC qui devaient être annulés depuis la dernière initialisation du câblo-modem. La première opportunité pour un câblo-modem de recevoir un certificat CVC sécurisé se trouve dans son fichier de configuration. Si ce fichier ne contient pas de certificat CVC valide, le câblo-modem ne demandera pas la mise à jour à distance des fichiers de code ou ne sera pas en mesure d'assurer cette mise à jour. En outre, le câblo-modem n'acceptera pas les certificats CVC qui lui seront remis ultérieurement via une base MIB utilisant le protocole SNMP.

Pour réduire le risque qu'un câblo-modem reçoive un fichier de code antérieur en raison d'une attaque par réexécution, les fichiers de code comportent une valeur d'heure de signature dans la structure [PKCS #7] qui peut être utilisée pour indiquer l'heure à laquelle l'image de code a été signée. Lorsqu'il reçoit un fichier de code dont l'heure de signature est postérieure à la dernière qu'il a reçue, le câblo-modem mettra à jour sa mémoire interne compte tenu de cette nouvelle heure. Il n'acceptera aucun fichier de code dont l'heure de signature est antérieure à cette valeur enregistrée dans sa mémoire interne. Pour mettre à jour un câblo-modem avec un nouveau fichier de code sans refuser l'accès aux fichiers de code antérieurs, le signataire peut décider de ne pas mettre à jour l'heure de signature. Ainsi, l'existence de plusieurs fichiers de code portant la même heure de signature du code permet à un opérateur de passer librement d'une image de code de câblo-modem à une version antérieure (c'est-à-dire jusqu'à ce que le certificat CVC soit mis jour). Cette manière de

procéder présente un certain nombre d'avantages pour l'opérateur, encore qu'il faille mettre en balance ces avantages avec les risques d'une attaque par réexécution d'un fichier de code.

A défaut d'un mécanisme fiable permettant de revenir à une version de code satisfaisante connue, tout système de mise à jour du code y compris celui qui est décrit dans la présente Recommandation, présente un point faible en ceci qu'une seule mise à jour forcée fructueuse d'une image de code non valide par un câblo-modem risque de rendre celui-ci inopérant. Pire encore, l'image de code non valide peut déclencher un comportement du câblo-modem dommageable au réseau. Un tel câblo-modem peut ne pas pouvoir être réparé par une mise à jour à distance, du fait que l'image de code non valide peut ne pas prendre en charge le système de mise à jour.

Annexe C

Interopérabilité des interfaces BPI/BPI+

La "confidentialité de base Plus" est une version améliorée de la "confidentialité de base". La spécification a ajouté, lorsque cela était nécessaire, des améliorations concernant la sécurité du système et a répondu à certaines préoccupations en matière de performance formulées dans la spécification originale. L'architecture et la conception originale de la confidentialité de base ont été maintenues lorsque cela était possible.

L'évolution vers les fonctionnalités de DOCSIS 1.1 ou 2.0 et la confidentialité de base "Plus" n'a pas pour objet de rendre obsolètes les systèmes conformes à DOCSIS 1.0 et l'utilisation de la confidentialité de base. La mise en conformité des systèmes DOCSIS avec DOCSIS 1.1 ou 2.0 peut se faire progressivement. Dans l'intervalle et par la suite, les unités de confidentialité de base conformes à DOCSIS 1.0 et les unités de confidentialité de base Plus conformes à DOCSIS 1.1 or 2.0 peuvent coexister dans un système DOCSIS.

C.1 Interopérabilité entre systèmes conformes à DOCSIS v1.0/v1.1/v2.0

Les conditions d'interopérabilité entre les interfaces BPI et BPI+ forment un sous-ensemble des conditions d'interopérabilité des systèmes conformes à DOCSIS v1.0/v1.1/v2.0 définies dans l'Annexe G de [J.112-B] ou [J.122]. Les conditions d'interopérabilité définies par [J.112-B] ou [J.122] pour la fourniture et l'enregistrement doivent être respectées.

C.2 Conditions d'interopérabilité entre interfaces BPI et BPI+

Les conditions d'interopérabilité BPI/BPI+ sont résumées dans le Tableau C.1. Un système de confidentialité de base Plus DOIT être rétrocompatible avec la confidentialité de base conformément à ce tableau. Il existe quatre capacités d'unité définies ici à partir de la spécification de la confidentialité de base et dont il est tenu compte dans ces conditions d'interopérabilité.

1) Système de terminaison de câblo-modem:
   a) CMTS BPI: confidentialité de base avec utilisation de la norme DES à 56 bits, et qui acceptera les modules de clé publique à 768 et à 1024 bits.
   b) CMTS BPI – 40 bits: confidentialité de base avec utilisation de la norme DES à 40 bits, et qui acceptera les modules de clé publique à 768 et à 1024 bits. La norme DES ne peut opérer que dans le mode à 40 bits.
2) Câblo-modem:
   a) CM BPI: confidentialité de base avec utilisation de la norme DES à 56 bits, et module de clé publique à 768 ou 1024 bits.

b) CM BPI – 40 bits: confidentialité de base avec utilisation de la norme DES à 40 bits, et module de clé publique à 768 ou 1024 bits. La norme DES ne peut opérer que dans le mode 40 bits.

Comme cela est défini dans la présente Recommandation, la Confidentialité de base "Plus" introduit deux types additionnels d'unités.

1) CMTS BPI+: confidentialité de base "Plus" avec utilisation de la norme DES à 56 bits, acceptera à la fois les modules de clé publique à 768 et à 1024 bits.

2) CM BPI+: confidentialité de base "Plus" avec utilisation de la norme DES à 56 bits, accepte un module de clé publique à 1024 bits.

Le CMTS et le CM négocient les mode compatibles avec les interfaces BPI/BPI+ en utilisant les capacités de modem pour la prise en charge de la confidentialité TLV (type 5.6) dans les messages REG-REQ et REG-RSP. Les prescriptions d'interopérabilité BPI/BPI+ sont les suivantes:

a) un système CMTS DOIT accepter des clés publiques ayant un module de 768 ou 1024 bits provenant d'un câblo-modem pendant la phase d'autorisation;

b) lorsqu'un système CM avec confidentialité de base "Plus" (CM BPI+) fonctionne avec un fichier de configuration de type DOCSIS 1.0, le câblo-modem place les capacités de modem pour la prise en charge de la confidentialité TLV (type 5.6) soit sur BPI Support (0), soit sur BPI+ Support (1) en fonction de ses capacités dans cette situation (cf. [J.112-B], § B.G.2.1, ou [J.122], § G.1.1);

c) lorsqu'un CMTS avec confidentialité de base "Plus" (CMTS BPI+) reçoit l'ensemble de capacités de modem pour la prise en charge de la confidentialité TLV pour la prise en charge de la confidentialité de base (type 5.6, valeur 0) ou aucun TLV de type 5.6 dans le message REG-REQ envoyé par le câblo-modem, le CMTS DOIT revenir dans un mode d'exploitation [SCTE22-2] compatible avec la confidentialité de base pour les communications avec ce CM;

d) lorsqu'un système CMTS avec confidentialité de base "Plus" fonctionne dans un système qui prend en charge à la fois les câblo-modems BPI et BPI+, le serveur TFTP DOIT inclure à la fois les deux types de fichiers de configuration suivants:

- fichier de configuration avec tous les paramètres d'interface BPI (type 17.1 à 17.7) des câblo-modems configurés pour fonctionner en mode BPI;
- fichier de configuration avec tous les paramètres d'interface BPI+ des câblo-modems configurés pour fonctionner en mode BPI+;

e) lorsqu'un CM avec confidentialité de base "Plus" (CM BPI+) reçoit l'ensemble de capacités de modem pour la prise en charge de la confidentialité TLV pour la prise en charge de la confidentialité de base (type 5.6, valeur 0) ou aucun TLV de type 5.6 dans le message REG-RSP envoyé par le CMTS, le CM DOIT revenir dans un mode d'exploitation [SCTE22-2] compatible avec la confidentialité de base pour les communications avec le CMTS.

NOTE – Comme l'indique l'Annexe B, les câblo-modems DOCSIS 1.1 ou 2.0 vérifient toujours les logiciels opérationnels téléchargés, indépendamment des réglages de prise en charge de la confidentialité (type 5.6) dans le message REG-RSP et des réglages d'activation de la confidentialité (type 4.7 ou 29) dans le fichier de configuration du câblo-modem.

Tableau C.1/J.125 – Matrice d'interopérabilité BPI/BPI+

	CM BPI	CM BPI – 40 bits	CM BPI+
CMTS BPI	Configuration nationale BPI. Module RSA à 768 ou 1024 bits	Module RSA à 768 ou 1024 bits. Le CMTS met à zéro certains bits TEK pour se conformer à la norme 40 bits.	Le CM revient au mode BPI avec module RSA à 1024 bits.
CMTS BPI – 40 bits	Module RSA à 768 ou 1024 bits. Le CMTS met à zéro certains des bits TEK pour se conformer à la norme 40 bits.	Module RSA 768 ou 1024 bits. Toute la compatibilité 40 bits traitée par des microcircuits MAC.	CM en mode BPI mode avec module RSA à 1024 bits. Le CMTS met à zéro certains bits TEK pour se conformer à la norme 40 bits.
CMTS BPI+	Le CMTS revient au mode DPI avec module RSA 768 ou 1024 bits	Module RSA à 768 ou 1024 bits. Le CMTS met à zéro certains bits TEK pour se conformer à la norme 40 bits.	Configuration BPI+ complet dépendant du fichier de configuration et des paramètres du CMTS. Module RAS à 1 024 bits.

C.3 Considérations relatives au mode d'exportation DES 40 bits BPI

La spécification confidentialité de base Plus est rétrocompatible avec le mode d'exportation DES à 40 bits de la confidentialité de base. Cette conformité doit être assurée au niveau du système CMTS. Tous les fournisseurs d'équipements DOCSIS n'auront pas un jour besoin de s'accommoder d'un système doté d'unités BPI capables de fonctionner selon la norme DES à 40 bits. Par conséquent, la conformité relève de la décision de chaque fabricant de système CMTS. Un système CMTS DEVRAIT être rétrocompatible avec la confidentialité de base DES à 40 bits. Si tel est le cas, il DOIT le faire conformément à la présente Recommandation.

a) Lorsqu'il envoie ou reçoit des données cryptées entre lui-même et un câblo-modem qui utilise un DES à 40 bits, le système CMTS DOIT mettre à zéro les bits appropriés de sa clé TEK avant de crypter ou de décrypter les données de trafic correspondantes. Les bits appropriés de la clé TEK DOIVENT être mis à zéro conformément aux prescriptions de la clé TEK à 40 bits de la confidentialité de base.

b) Lorsque le trafic crypté est transmis entre un système CMTS qui dispose uniquement de la capacité DES à 40 bits et un câblo-modem qui dispose de la capacité DES à 56 bits, le système CMTS DOIT fournir une clé compatible avec la norme 40 bits dans le message de réponse de clé adressé au câblo-modem.

La méthode utilisée par le système CMTS pour reconnaître si les câblo-modems d'un système disposent de la capacité DES 56 bits ou uniquement de la capacité DES 40 bits, dépend des choix de l'opérateur d'un système donné et du fournisseur de système CMTS, pour répondre au mieux à la situation. Il sera aussi possible d'obtenir cette information auprès du fournisseur de câblo-modems, basée sur le numéro de série, l'adresse MAC, la date de fabrication ou certains mécanismes de traçage du dispositif. Une fois collectée, cette information sera incorporée dans la base de données d'informations CMTS stockées sur chaque câblo-modem.

Une autre méthode permettant d'obtenir cette information est la BPI MIB DOCSIS définie à cette fin.

C.4 Fonctionnement du système

C.4.1 Système CMTS doté de la capacité BPI

Un système CMTS doté de la capacité BPI fournira toujours aux câblo-modems des informations nécessaires en utilisant des fichiers de configuration TFTP du type DOCSIS 1.0 et les réglages de

configuration TFTP. Les câblo-modems BPI et BPI+ recevront les réglages d'interface BPI et chaque cablô-modem tentera uniquement de s'enregistrer comme câblo-modem DOCSIS 1.0 doté de la capacité BPI. Si un câblo-modem renvoie une capacité de modem BPI+ dans la demande d'enregistrement, le système CMTS répondra en supprimant cette capacité et en obligeant le CM à être compatible BPI.

C.4.2 Système CMTS doté de la capacité BPI+

Un système doté de la capacité DOCSIS 1.1 ou 2.0 d'interface BPI+ DOIT pouvoir fonctionner en mode compatible BPI et BPI+ et se caler sur la capacité de chaque câblo-modem client. Lorsque le système CMTS dispose de la capacité BPI+ et que le système prend en charge simultanément les câblo-modems BPI et BPI+, les fichiers de configuration DOCSIS 1.0 et DOCSIS 1.1 ou 2.0 DOIVENT être disponibles pour fournir les réglages de configuration BPI+ et BPI au câblo-modem approprié. Un câblo-modem disposant de la capacité BPI recevra un fichier de configuration DOCSIS 1.0 avec des réglages BPI. Il s'enregistrera alors avec la capacité de modem BPI.

Annexe D

Mise à jour de BPI à BPI+

D.1 Câblo-modem hybride avec interface BPI+

Certains modèles de CM selon DOCSIS 1.0 peuvent prendre en charge des caractéristiques de BPI+ au moyen d'une mise à jour logicielle. Afin de faciliter la prise en charge de ces "Câblo-modems hybrides DOCSIS 1.0", [J.112-B] ou [J.122] fournit les formes de codage des capacités de modem que les câblo-modems hybrides peuvent mettre dans le message de demande d'enregistrement afin de négocier ses fonctionnalités DOCSIS 1.1 ou 2.0 avec le CMTS.

Un câblo-modem hybride DOCSIS 1.0 PEUT régler les paramètres de capacités de modem pour la prise en charge de la confidentialité à 1 (BPI Plus Support) si le câblo-modem est entièrement conforme à l'interface BPI+, excepté pour les points suivants:

- prise en charge de DES à 56 bits si le câblo-modem ne prend en charge que les DES à 40 bits;
- prise en charge de clé RSA à 1 024 bits si le câblo-modem prend en charge les clés RSA à 768 bits;
- la mémoire permanente, à écriture unique, pour les certificats de câblo-modem délivrés par le fabricant;
- cryptage des paquets concaténés si les formes de codages des capacités de modem prenant en charge la concaténation est mis à 0 (éteint);
- cryptage des paquets de fragmentation si les formes de codages des capacités de modem prenant en charge la fragmentation est mis à 0 (éteint);
- cryptage des paquets de (PHS, *payload header suppression*) si les formes de codages des capacités de modem prenant en charge la suppression d'en-tête de charge utile est mis à 0 (éteint).

Le câblo-modem hybride avec interface BPI+ interfonctionnera avec le CMTS BPI+ et le CMTS BPI avec DES à 56 bits et 40 bits. L'exigence pour l'interopérabilité BPI/BPI+, en plus de l'Annexe C, est la suivante:

a) si un câblo-modem hybride avec interface BPI+ prend en charge uniquement le DES à 40 bits et qu'il fonctionne en mode BPI+, il DOIT envoyer le message de demande d'autorisation avec l'attribut de capacités de sécurité pour spécifier le DES à 40 bits et le

CMTS DOIT fonctionner avec le câblo-modem en mode DES à 40 bits spécifié dans le § 10.1.

D.2 Procédure de mise à jour

Les fonctionnalités de l'interface BPI+ PEUVENT être téléchargées dans le câblo-modem DOCSIS 1.0 grâce aux procédures suivantes.

1) Télécharger l'image du code logiciel avec les fonctionnalités BPI+ et MIB BPI+ dans le câblo-modem en utilisant la fonction de téléchargement de logiciel définie par la spécification DOCSIS 1.0. Le certificat CA de fabricant signé par la clé privée racine DOCSIS est inclus dans cette image de code logiciel.
2) Mettre le certificat du câblo-modem signé par la clé privée du fabricant et la clé publique de l'autorité CA racine DOCSIS au câblo-modem utilisant les MIB BPI+ si le câblo-modem n'a pas déjà ces informations. Le détail de ces objects MIB BPI+ pour cette operation sera défini par [DOCSIS8].

NOTE – Le câblo-modem ne peut ni fonctionner en mode BPI+, ni régler les paramètres de capacités de modem pour la prise en charge de la confidentialité à 1 (prise en charge de BPI Plus), avant que le certificat du câblo-modem et la clé publique de l'autorité CA racine DOCSIS soient mis dans le câblo-modem.

Appendice I

Exemples de messages, de certificats et d'unités PDU

Le présent appendice présente des exemples numériques susceptibles d'intéresser les utilisateurs de la présente Recommandation. Ces exemples portent sur un échange type de clés, à savoir: information d'autorisation, demande d'autorisation, réponse d'autorisation, demande de clé et réponse de clé. Le détail des calculs cryptographiques est donné pour chaque étape ainsi que des exemples de certificats. Les exemples concernent également plusieurs unités PDU en mode paquet, cryptées selon les informations relatives aux clés qui découlent de l'échange de clés dans cet exemple.

Le présent appendice a uniquement un caractère informatif et ne fait pas partie de la présente Recommandation.

I.1 Notation

Dans les exemples ici, les paquets sont représentés par un flux d'octets, chaque octet figurant en notation hexadécimale, accompagné parfois d'une annotation textuelle. L'ordre de transmission des octets est de gauche à droite et de haut en bas. Prenons comme exemple la représentation suivante d'un paquet:

00 01 02 03	Description #1
04 05	
06 07 08	Description #2

Le paquet se compose de 9 octets, représentés en notation hexadécimale par "00", "01", ... , "08". L'octet représenté par "00"est transmis en premier et celui représenté par "08" en dernier.

Dans la discussion relative aux exemples, les valeurs entières sont représentées en notation hexadécimale au moyen d'un préfixe "0x" ou en notation décimale sans préfixe. Ainsi, la notation hexadécimale 0x12345 et la notation décimale 74565 représentent la même valeur entière. Toutes

les valeurs entières sont non négatives. Ainsi, 0xff représente un entier ayant la valeur de 255 et non pas une valeur négative.

Le protocole BPKM produit et distribue des clés DES à 8 octets et des clés triple DES à 16 octets, sans faire de correction de parité sur le dernier bit de plus fort poids de chaque octet. Dans les applications, une clé de 56 bits est extraite d'une clé de 8 octets et une clé de 112 bits d'une clé à 16 octets en ignorant la valeur du bit de plus fort poids de chaque octet. Dans les exemples ici, les clés sont représentées sans correction de parité.

I.2 Message information d'authentification *(authentication info)*

Le câblo-modem envoie le message (information d'authentification) suivant:

0c 01 02 94	En-tête d'info. d'authentification
11 02 91	En-tête Certificat CA
30 82 02 8d 30 82 01 f6 . . . 81 87 19 61 72 20 19 1e	Certificat CA

Le champ code a la valeur 0x0c, qui identifie un message information d'authentification. Le champ longueur a la valeur 0x294 (660), qui est le nombre d'octets qui suit le champ longueur.

Le seul attribut est le certificat de CA. Les détails concernant le certificat sont donnés ci-dessous.

I.2.1 Détails concernant le certificat de CA

Les champs de l'attribut certificat de CA dans le message information d'autorisation ci-dessus se subdivisent comme suit:

30 82 02 8d	En-tête du certificat
30 82 01 f6	En-tête du certificat tbs
a0 03 02 01 02	Version
02 08 01 02 03 04 05 06 07 08	Numéro de série
30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00	Signature
30 81 88	En-tête de l'émetteur
31 0b 30 09 06 03 55 04 06 13 02 55 53	Nom du pays
31 0f 30 0d 06 03 55 04 0a 13 06 4e 6f 72 74 65 6c	Nom de l'organisation
31 0f 30 0d 06 03 55 04 0b 13 06 44 4f 43 53 49 53	Nom de l'unité organisationnelle
31 1f 30 1d 06 03 55 04 0b 13 16 42 75 69 6c 64 69 6e 67 20 31 2c 20 41 6e 64 6f 76 65 72 20 4d 41	Nom de l'unité organisationnelle
31 36 30 34 06 03 55 04 03 13 2d 4e 6f 72 74 65 6c 20 43 61 62 6c 65 20 4d 6f 64 65 6d 20 52 6f 6f 74 20 43 65 72 74 69 66 69 63 61 74 65 20 41 75 74 68 6f 72 69 74 79	Nom commun
30 1e	En-tête validité
17 0d 39 39 30 31 32 30 31 36 30 35 30 30 5a	Pas avant
17 0d 34 39 31 32 33 31 32 33 35 39 35 35 5a	Pas après
30 81 88	En-tête sujet
31 0b 30 09 06 03 55 04 06 13 02 55 53	Nom de pays
31 0f 30 0d 06 03 55 04 0a 13 06 4e 6f 72 74 65 6c	Nom de l'organisation

31 0f 30 0d 06 03 55 04 0b 13 06 44 4f 43 53 49 53	Nom de l'unité organisationnelle
31 1f 30 1d 06 03 55 04 0b 13 16 42 75 69 6c 64 69 6e 67 20 31 2c 20 41 6e 64 6f 76 65 72 20 4d 41	Nom de l'unité organisationnelle
31 36 30 34 06 03 55 04 03 13 2d 4e 6f 72 74 65 6c 20 43 61 62 6c 65 20 4d 6f 64 65 6d 20 52 6f 6f 74 20 43 65 72 74 69 66 69 63 61 74 65 20 41 75 74 68 6f 72 69 74 79	Nom commun
30 81 9f	En-tête informations relatives à la clé publique du titulaire
30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00	Type d'algorithme de clé publique
03 81 8d 00 30 81 89	En-tête de clé publique
02 81 81 00 af d1 86 c8 17 45 02 bc e5 59 b4 15 ac 95 87 7b 89 f5 8b f8 3b 8a 8b ef 67 cf 9e 00 47 d5 f1 06 42 55 36 a1 d1 8c dc cb 81 bb 31 8d 35 f7 6d 11 a0 91 9b 31 3d b9 71 38 46 15 c8 81 c4 51 06 7b d7 8a 70 be c1 28 0d 78 80 3c 44 a6 5e 35 5f 6e 46 2f 80 41 28 78 63 6c 86 cc d0 b3 58 ca bc 07 d5 19 3e 8a a2 1c 7e ff 0d 16 2b 0f bd a5 5e 60 93 64 09 80 24 76 ed e4 a9 e3 81 26 0c de 8a 89	Module de clé publique
02 03 01 00 01	Exposant de clé publique
30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00	Algorithme de signature
03 81 81 00 81 4d db 31 e2 31 d2 6c f5 21 29 93 4a ce cb 6c fb 8b fc 3d ef 4b e8 4a 8a db f7 d8 e3 70 1d 3c ff ba 71 70 c4 82 24 9f 12 b5 d4 3e 3a 4d 20 64 2f ab 8b 05 27 9a 34 24 33 24 d4 7e bc 41 07 34 7a a6 51 12 29 55 e7 9b 5b e5 6b 79 bb 31 04 2f d1 c6 d3 7f 32 a2 b5 cc 99 23 09 97 1a 21 44 fa 25 3b f4 4b d6 00 cf e9 1b a9 be 9b 88 f8 90 fd 59 77 80 41 7d cb ca bf 81 87 19 61 72 20 19 1e	Valeur de signature

Dans cet exemple, certains champs sont les mêmes dans tous les certificats de l'autorité de certification (CA). Ces champs sont les suivants:

- version: v3;
- signature: SHA-1 avec RSA, paramètres nuls;
- nom de la première unité organisationnelle: "DOCSIS";
- type d'algorithme de clé publique: cryptage RSA, paramètres nuls;
- exposant clé publique: entier sur 3 octets, valeur 0x10001;
- algorithme de signature: SHA-1 avec RSA, paramètres nuls.

Il s'agit d'un exemple d'un certificat CA autosigné. Les noms de l'émetteur et du titulaire sont identiques. Dans cet exemple, les champs de nom correspondants sont:

- nom de pays: "US";
- nom de l'organisation: "Nortel" ;
- nom de la première unité organisationnelle: "DOCSIS";
- nom de la deuxième unité organisationnelle: "Building 1, Andover MA";
- nom commun: "Nortel Cable Modem Root Certificate Authority".

Les autres champs contiennent des valeurs données en exemple, parmi celles-ci citons les suivantes:

- numéro de série: entier de 8 octets, valeur 0x0102030405060708. (D'autres certificats CA peuvent utiliser une longueur différente);
- pas avant: 1999-01-20 16:05:00 GMT;
- pas après: 2049-12-31 23:59:55 GMT;
- module de clé publique: entier de 1 024 bits, valeur 0x00afd1...8a89 (D'autres certificats CA peuvent utiliser un entier de longueur comprise entre 1 024 et 2 048 bits, valeurs incluses);
- valeur de signature: chaîne binaire occupant 1 024 bits, représentant la valeur entière 0x00814d...191e. (D'autres certificats CA peuvent utiliser une chaîne binaire de longueur comprise entre 1024 et 2048 bits, valeurs incluses; la longueur correspond à celle du module de l'émetteur. La signature est calculée sur la partie du certificat qui commence par l'en-tête Certificat tbs et se termine avec l'exposant clé publique, valeurs incluses.)

I.3 Demande d'autorisation

Le câblo-modem envoie la demande d'autorisation suivante:

04 72 03 40	En-tête demande d'autorisation
05 00 ad	En-tête Identification de CM
01 00 0c 30 30 30 30 30 30 31 32 33 34 35 36	Numéro de série
02 00 03 00 00 ca	ID de fabricant
03 00 06 00 00 ca 01 04 01	Adresse MAC
04 00 8c 30 81 89 02 81 81 00 e0 e0 6c 8d be b2 8b c9 f3 a6 3d a1 12 ea f7 99 f7 3d 3e fa a3 b1 e2 42 95 71 b5 71 d2 32 7a da 10 40 e2 5b 09 74 69 08 78 46 37 71 34 3e 69 a7 37 6d f8 70 1d aa a5 34 b0 33 a3 43 ac 4d eb 41 5e 0a 8a fd a6 0a 4b 09 7f 5a 18 f2 9e c2 22 a6 6b 9a 69 73 22 d5 37 c9 63 b0 88 f5 60 5d 99 16 33 54 53 30 ed 35 de 0c 87 3b 54 ba 59 22 3e b2 79 90 96 61 db f3 4a 37 18 4c 7f a8 ca ee d6 31 02 03 01 00 01	Clé publique RSA
12 02 7a	En-tête de certificat CM
30 82 02 76 30 82 01 df . . . 19 c9 f1 dc 30 b8 d3 d5	Certificat CM
13 00 0b	En-tête capacité de sécurité
15 00 04 01 00 02 00	Liste de la suite cryptographique
16 00 01 01	Version BPI
0c 00 02 22 60	SAID

Le champ code a la valeur 0x04, indiquant qu'il s'agit d'un paquet demande d'autorisation. La valeur du champ identificateur est 0x72; cette valeur n'est donnée qu'à titre d'exemple. Le champ longueur a la valeur 0x0340 (832), qui est le nombre d'octets qui suit le champ longueur.

Le premier attribut est l'identificateur de cablô-modem (CM). Il s'agit d'un attribut composé qui comprend les sous-attributs suivants: numéro de série, ID de fabricant, adresse MAC et clé publique RSA. Des exemples de valeurs sont donnés pour ces sous-attributs.

La clé publique RSA est codée en DER et est analogue à l'exemple donné au § 2.2 de [RSA2]. Le module est un entier de 1024 bits représenté au moyen de 0x81 (129) octets. Dans cet exemple la valeur du module est:

```
0x00e0e06c8d ... caeed631.
```

Il convient de noter que 0x00 est l'octet de plus fort poids du module et 0x31 l'octet de plus faible poids. L'exposant est un entier constitué de trois octets et dont la valeur est 0x010001.

L'attribut suivant est le certificat du CM. Les détails concernant le certificat sont donnés ci-dessous.

NOTE – Certains champs du certificat du CM doivent correspondre aux sous-attributs de l'identification CM; ces attributs sont l'adresse MAC et la clé publique RSA.

L'attribut suivant est l'attribut capacité de sécurité. Il s'agit d'un attribut composite constitué de la liste de la suite cryptographique et la version BPI. Dans le présent exemple, deux suites cryptographiques sont indiquées: la DES à 56 bits sans authentification, et la DES à 40 bits sans authentification. La version BPI est BPI+.

L'attribut final est l'identificateur SAID primaire du câblo-modem, dont la valeur est égale à son identificateur SID primaire. Dans cet exemple, l'identificateur SAID primaire a la valeur 0x2260.

I.3.1 Détails du certificat de câblo-modem (CM)

Les champs du certificat CM dans le message information d'autorisation ci-dessus se ventilent comme suit:

30 82 02 76	En-tête de certificat
30 82 01 df	En-tête du certificat tbs
a0 03 02 01 02	Version
02 08 01 01 01 01 01 01 01 01	Numéro de série
30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00	Signature
30 81 88	En-tête de l'émetteur
31 0b 30 09 06 03 55 04 06 13 02 55 53	Nom du pays
31 0f 30 0d 06 03 55 04 0a 13 06 4e 6f 72 74 65 6c	Nom de l'organisation
31 0f 30 0d 06 03 55 04 0b 13 06 44 4f 43 53 49 53	Nom de l'unité organisationnelle
31 1f 30 1d 06 03 55 04 0b 13 16 42 75 69 6c 64 69 6e 67 20 31 2c 20 41 6e 64 6f 76 65 72 20 4d 41	Nom de l'unité organisationnelle
31 36 30 34 06 03 55 04 03 13 2d 4e 6f 72 74 65 6c 20 43 61 62 6c 65 20 4d 6f 64 65 6d 20 52 6f 6f 74 20 43 65 72 74 69 66 69 63 61 74 65 20 41 75 74 68 6f 72 69 74 79	Nom commun
30 1e	En-tête de validité
17 0d 39 39 30 33 32 33 31 36 35 38 33 34 5a	Pas avant
17 0d 34 39 31 32 33 31 32 33 35 39 35 30 5a	Pas après
30 72	En-tête titulaire
31 0b 30 09 06 03 55 04 06 13 02 55 53	Nom de pays
31 0f 30 0d 06 03 55 04 0a 13 06 4e 6f 72 74 65 6c	Nom de l'organisation
31 1f 30 1d 06 03 55 04 0b 13 16 42 75 69 6c 64 69 6e 67 20 31 2c 20 41 6e 64 6f 76 65 72 20 4d 41	Nom de l'unité organisationnelle

31 15 30 13 06 03 55 04 03 13 0c 30 30 30 30 30 30 31 32 33 34 35 36	Nom commun (numéro de série)
31 1a 30 18 06 03 55 04 03 13 11 30 30 3a 30 30 3a 43 41 3a 30 31 3a 30 34 3a 30 31	Nom commun (adresse MAC)
30 81 9f	En-tête d'info de clé publique du titulaire
30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00	Type d'algorithme de clé publique
03 81 8d 00 30 81 89	En-tête clé publique
02 81 81 00 e0 e0 6c 8d be b2 8b c9 f3 a6 3d a1 12 ea f7 99 f7 3d 3e fa a3 b1 e2 42 95 71 b5 71 d2 32 7a da 10 40 e2 5b 09 74 69 08 78 46 37 71 34 3e 69 a7 37 6d f8 70 1d aa a5 34 b0 33 a3 43 ac 4d eb 41 5e 0a 8a fd a6 0a 4b 09 7f 5a 18 f2 9e c2 22 a6 6b 9a 69 73 22 d5 37 c9 63 b0 88 f5 60 5d 99 16 33 54 53 30 ed 35 de 0c 87 3b 54 ba 59 22 3e b2 79 90 96 61 db f3 4a 37 18 4c 7f a8 ca ee d6 31	Module clé publique
02 03 01 00 01	Exposant clé publique
30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00	Algorithme de signature
03 81 81 00 19 b0 2b e5 2c 37 4a af 34 cb c9 59 62 68 88 05 8a 91 5b d4 c6 fa 2e 19 ab 98 42 33 68 9d fc e4 76 23 84 8d 4a be ff bf 34 cf e0 fb 93 96 01 8b 89 d9 86 42 5e cf 6d e6 68 2e 44 99 56 6a cc f1 2c b9 5b 30 21 08 22 f5 11 b1 38 ba 6e b5 62 f0 3a dc f1 2e c4 61 95 2f 16 c8 27 63 b6 e8 69 a6 1c e1 4f 1a 8c 65 cb 57 5e 13 ce db 7f 27 f9 c1 6e bf 2f 75 77 9e a9 87 19 c9 f1 dc 30 b8 d3 d5	Valeur de la signature

Certains champs donnés dans cet exemple sont les mêmes pour tous les certificats de CM. Il s'agit des champs suivants:

- version: v3;
- signature: SHA-1 avec RSA, paramètres nuls;
- nom de l'émetteur de l'unité organisationnelle première: "DOCSIS";
- type d'algorithme de clé publique: cryptage RSA, paramètres nuls;
- exposant de la clé publique: entier sur 3 octets, valeur 0x10001;
- algorithme de signature: SHA-1 avec RSA, paramètres nuls.

Le nom de l'émetteur du certificat CM correspond au nom du titulaire du certificat délivré par le CA. Dans cet exemple, les champs de nom d'émetteur correspondants sont les suivants:

- nom de pays: "US";
- nom de l'organisation: "Nortel";
- nom de la première unité organisationnelle: "DOCSIS";
- nom de la deuxième unité organisationnelle: "Building 1, Andover MA";
- nom commun: "Nortel Cable Modem Root Certificate Authority".

Les autres champs contiennent des exemples de valeurs dont certaines sont les suivantes:

- numéro de série: entier de huit octets, valeur 0x0101010101010101. (D'autres certificats CM peuvent utiliser une longueur différente);
- pas avant: 1999-03-23 16:58:34 GMT;
- pas après: 2049-12-31 23:59:50 GMT;
- nom de pays titulaire: "US";

- nom de l'organisation titulaire: "Nortel";
- nom de l'unité organisationnelle titulaire: "Building 1, Andover MA";
- premier nom commun du titulaire (numéro de série): "000000123456". (D'autres certificats CM peuvent utiliser une chaîne de longueur différente. La valeur correspond à l'attribut numéro de série du message de demande d'autorisation (*authorization request*));
- deuxième nom commun du titulaire (adresse MAC): "00:00:CA:01:04:01". (Tous les certificats CM utilisent une chaîne de cette longueur dont la valeur correspond à l'attribut d'adresse MAC du message de demande d'autorisation);
- module de clé publique: entier de 1024 bits de longueur, de valeur 0x00e0e0...d631. (D'autres certificats CM peuvent utiliser un entier de longueur égale à 768 ou 1024 bits);
- valeur de signature: chaîne binaire de longueur 1024 bits, représentant la valeur d'entier 0x0019b0...d3d5. (D'autres certificats CM peuvent utiliser une chaîne binaire d'une longueur comprise entre 1024 et 2048 bits inclus; la longueur correspond à celle du module de l'émetteur. La signature est calculée sur une partie du certificat qui commence par l'en-tête tbsCertificate et se termine avec l'exposant clé publique inclus.)

I.4 Réponse d'autorisation *(authorization reply)*

Le système de terminaison de câblo-modem (CMTS) envoie la réponse d'autorisation suivante:

05 72 00 9f	En-tête de réponse d'autorisation
07 00 80 a2 cb ad c8 34 27 71 47 06 d5 10 0c 07 94 90 bf e6 44 1b 0c 90 0d b4 ed 9c 39 aa 05 a0 c1 ef 54 4b cc fb 3a 7a 22 81 c0 dc c6 6e 39 a4 91 1c ba bf b0 ed 47 10 f2 f4 13 f9 09 33 c6 ae a3 45 67 c8 38 0f c3 9a 12 be d5 27 27 39 77 fb 98 03 39 50 39 99 f5 b6 ad b5 85 f9 16 d0 ff c6 2a ff 9f 38 73 6f 35 44 21 ad 9e e1 a5 91 4d 34 06 1d bb c9 b6 8f 8a 17 9e be c6 c9 40 eb 81 f0 62 d8 18	Clé d'autorisation
09 00 04 00 09 3a 80	Durée de vie de la clé
0a 00 01 07	Numéro de séquence de la clé
17 00 0e	En-tête du descripteur SA
0c 00 02 22 60	SAID
18 00 01 00	Type de SA
14 00 02 01 00	Suite cryptographique

Le champ code a la valeur 0x05, indiquant qu'il s'agit d'un paquet de réponse d'autorisation. Le champ identificateur a la valeur 0x72, correspondant au champ d'identificateur de la demande d'autorisation. Le champ longueur a la valeur 0x009f (159), qui est le nombre d'octets qui suit le champ longueur.

Le premier attribut est la clé d'autorisation. Cet attribut contient une clé d'autorisation qui a été cryptée selon le code RSA en utilisant la clé publique se trouvant dans le message de demande d'autorisation. La clé d'autorisation cryptée RSA est un entier constitué de 0x80 (128) octets. Dans cet exemple, la valeur de cette clé est:

0xa2cbadc8 ... f062d818.

Il convient de noter que 0xa2 est l'octet de plus fort poids de la clé d'autorisation cryptée RSA et 0x18 est l'octet de plus faible poids. Les détails concernant le calcul du cryptage RSA sont donnés ci-dessous.

Le deuxième attribut est la durée de vie de la clé (Key Lifetime). Dans cet exemple, sa valeur est égale à 0x00093a80 (604800) secondes, ou sept jours.

Le troisième attribut est le numéro de séquence de la clé. Dans cet exemple sa valeur est 0x07.

Les attributs restants sont des descripteurs SA. Chaque descripteur SA est un attribut composite constitué des sous-attributs suivants: SAID, SA Type et Cryptographic Suite. Dans cet exemple, un seul descripteur SA est inclus, correspondant à l'identificateur SAID dans la demande d'autorisation. Le type SA est primaire, et la suite cryptographique conforme à la norme DES à 56 bits sans authentification.

Le câblo-modem (CM) et le système de terminaison de câblo-modem (CMTS) calculent la clé de cryptage et deux clés d'identification de message à partir de la clé d'autorisation, en utilisation la dispersion. Le détail des calculs de dispersion est donné ci-après. Nous donnons ci-après les valeurs de ces clés dans l'exemple considéré:

Clé d'autorisation	`4e 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc 0b 75`
Clé de cryptage de clé	`76 b4 d4 2f 14 98 59 6a ab fe 72 94 15 7c 7d 62`
Clé d'authentification de message, flux amont	`fe b9 f1 e2 46 a7 6d 7c a7 7b 5e b0 98 25 fd 0b 57 ca 90 c7`
Clé d'authentification de message, flux aval	`93 d3 9d 70 c3 b6 f5 92 c4 6b d3 92 76 46 f4 f1 90 3a 52 fd`

I.4.1 Détails du cryptage RSA

Le système CMTS produit une clé d'autorisation aléatoire de 20 octets. Dans le présent exemple, la valeur de cette clé est:

```
4e 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc 0b 75
```

La clé d'autorisation est cryptée en utilisant le système RSAES-OAEP (RSA, *encryption scheme – optimal asymmetric encryption padding*) décrit dans [RSA3]. Le présent paragraphe donne des détails relatifs au schéma appliqué pour cet exemple. Le schéma utilise une fonction de production de masque (MGF, *mask-generating function*) qui est fondée sur la dispersion; les détails sont donnés dans un prochain paragraphe.

La clé d'autorisation est introduite dans un bloc de 107 octets DB:

```
DB =
da 39 a3 ee 5e 6b 4b 0d 32 55 bf ef 95 60 18 90 af d8 07 09 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01 42 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc ob 75
```

Pour former DB, la clé d'autorisation est préfacée par un octet de valeur 1, et le résultat est inséré dans les 21 derniers octets du bloc. Les 20 premiers octets du bloc sont le résultat de l'exécution de l'opération de dispersion sur une chaîne de longueur nulle; ces 20 octets ont la même valeur dans chaque réponse d'autorisation (*authorization reply*) et ne sont pas propres à cet exemple. Les 66 octets restants du bloc sont mis à zéro.

Le système CMTS produit une chaîne aléatoire de 20 octets appelée SEED. Cette chaîne est générée de manière indépendante pour chaque réponse d'autorisation. Dans cet exemple, la chaîne SEED a la valeur suivante:

```
SEED =
ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d
```

La chaîne SEED est appliquée à la fonction MGF pour générer le DB_MASK, qui est un bloc de 107 octets:

```
DB_MASK =
de 10 c9 59 41 c9 ea 72 a4 35 68 79 d2 53 85 db 13 7b a6 3b 37 ac 86 06 7c b5 ec
97 d2 d0 9e 01 30 2b 10 91 3a ec 3f d9 a1 2f c4 e9 8d 18 88 95 f6 9c ea 17 23 9f
5d d5 f1 4d 25 8e 9e 6d 7d 3c ca 55 fe 0e ee 2d 0d 7e 5b 64 b6 79 44 76 c 3f 6e
ac 99 3a ae 14 3e 9a 8e df 3c 36 79 58 b2 fa 13 72 58 4c ca 04 a1 af c7 c4 62
```

On applique à DB et DB_MASK un OU exclusif pour produire le MASKED_DB, qui comporte 107 octets:

```
MASKED_DB =
04 29 6a b7 1f a2 a1 7f 96 60 d7 96 47 33 9d 2d bc a3 a1 32 37 ac 86 06 7c b5 ec
97 d2 d0 9e 01 30 2b 10 91 3a ec 3f d9 a1 2f c4 e9 8d 18 88 95 f6 9c ea 17 23 9f
5d d5 f1 4d 25 8e 9e 6d 7d 3c ca 55 fe 0e ee 2d 0d 7e 5b 64 b6 79 44 76 cc 3f 6e
ac 99 3a ae 14 3f d4 0b f8 c3 f2 6b 2a 3c 9b 97 ac 91 6c 7c e4 c5 5f 7b cf 17
```

MASKED_DB est appliquée à la fonction MGF afin de générer SEED_MASK, qui est un bloc de 20 octets:

```
SEED_MASK =
b4 b6 f1 bf a6 b3 a1 7e 95 82 d3 b8 93 71 b6 7f 45 31 9e 82
```

On applique aux chaînes SEED et SEED_MASK un ou exclusif pour produire une chaîne MASKED_SEED, comportant 20 octets:

```
MASKED_SEED =
19 2a 5e 32 5e 95 5f d1 20 5d 2e 2d 4d 0f 21 b3 ac 7a f3 ef
```

Les chaînes MASKED_SEED et MASKED_DB sont concaténées et le résultat est précédé par un seul octet de valeur zéro. Cela se traduit par la création d'un bloc de 128 octets appelé EM:

```
EM =
00 19 2a 5e 32 5e 95 5f d1 20 5d 2e 2d 4d 0f 21 b3 ac 7a f3 ef 04 29 6a b7 1f a2
a1 7f 96 60 d7 96 47 33 9d 2d bc a3 a1 32 37 ac 86 06 7c b5 ec 97 d2 d0 9e 01 30
2b 10 91 3a ec 3f d9 a1 2f c4 e9 8d 18 88 95 f6 9c ea 17 23 9f 5d d5 f1 4d 25 8e
9e 6d 7d 3c ca 55 fe 0e ee 2d 0d 7e 5b 64 b6 79 44 76 cc 3f 6e ac 99 3a ae 14 3f
d4 0b f8 c3 f2 6b 2a 3c 9b 97 ac 91 6c 7c e4 c5 5f 7b cf 17
```

Pour réaliser le cryptage RSA, le bloc EM est interprété comme étant l'entier:

0x00192a5e32 ... 5f7bcf17.

A noter que 0x00 est l'octet de plus fort poids et 0x17 l'octet de plus faible poids.

Le cryptage RSA est exécuté comme étant l'opération $Y = M^E \bmod N$, dans laquelle:

M est la valeur entière du bloc EM (0x00192a5e32 ... 5f7bcf17); E est la valeur entière de l'exposant de la clé publique RSA (0x010001); N est la valeur entière du module de la clé publique RSA (oxe0e06c8d ...caeed631); Y est la valeur de la clé d'autorisation cryptée en RSA (0xa2cbadc8 ... f062d818).

I.4.2 Détails du décryptage RSA

Le Tableau I.1 donne la liste des paramètres de clés privées qui correspondent à la clé publique RSA dans l'exemple de message de demande d'autorisation:

Tableau I.1/J.125 – Paramètres de clés privées

Paramètres	Propriété	Valeur
D (exposant privé)	M^{DE} mod N = M	6b 1f 1d 36 ec 77 7b 15 a9 c6 30 27 71 ae 92 62 3a 9f 67 47 d8 00 9d ca a0 0b f9 a6 0d be 54 3d 5a 6e be 25 25 bc d9 67 da 7b 80 5f a1 c6 75 67 dd 84 ba 4b 16 26 ba e9 fd 61 ab cd 49 e0 18 47 37 9f 56 08 2d d9 16 81 ff 7d d0 7e 01 8f d4 84 d3 e8 eb 27 48 c3 6c dc a9 01 b7 e5 24 28 d1 6c 67 03 a7 63 fb fa 79 d8 08 6a e1 de 3d 12 7a 36 20 25 01 d1 08 11 0c cd 80 44 3c fd c5 c4 db d1
P (facteur principal)	N = PQ	f1 6b dd 2f dd d8 df 80 30 e6 9c d3 4e 46 5e 9f 42 62 b1 66 86 57 1b ca 87 9c cf fd 1c b6 26 76 95 35 bf 0b fb 51 af 0f 46 1c 5e cb 82 a0 83 bf 46 c9 3b d6 4e 7a 5d bf 03 05 69 27 31 6d 65 bd
Q (facteur principal)	N = PQ	ee 74 cb a3 d0 90 2d 8a e9 e7 10 dd b4 65 2e 91 22 09 52 72 ab bd 32 31 4e d7 d0 2b 4b 13 57 20 6b f9 a4 57 b1 47 59 67 86 a6 8c 2c c1 f3 8b ba 8a 6b b1 62 5d 43 5a 71 db d0 33 43 97 99 17 85
D_p (exposant CRT)	D_p = D mod (P – 1)	a6 35 dc d2 57 aa 38 35 c9 74 fc 03 7e a0 74 04 b1 6f c1 33 14 ca 64 17 cb c5 ea 6c 18 98 4f 62 d4 d7 6b f0 93 d6 68 ef db 15 2d 2e 6f 80 93 33 dd 48 2e 2a 1d 5d a1 ad 20 27 59 7d e2 49 af 01
D_q (exposant CRT)	D_q = D mod (Q – 1)	cf f1 9c 30 33 cd b7 59 7f 96 57 f7 ee bb 99 bb 48 a2 36 7a f7 57 1a f1 32 df 32 92 be 7a 94 2d 1a db ed bb e7 45 e0 2a 4e 9a e8 7c 93 7a 4e 2c 93 4f 4c b6 09 bc 95 9f da df 9a 04 e4 ab c5 7d
U_p (constante CRT)	PU_p mod Q = 1	08 17 0c 11 bc aa 2f 96 80 8b 31 95 6d 2e b8 3c ee 2e 05 88 ab 9e fc 53 24 c4 04 b8 7e 1d 01 db 2d f2 2c 06 b0 cd 04 6b 1c 14 d8 d0 4f c9 a0 ae 1b c9 80 88 be 42 0a 52 4a ef 62 3c 8b dd c5 37

Chaque valeur du Tableau I.1 représente les octets d'un entier, dont l'octet de plus fort poids est représenté en premier. Par exemple, l'exposant privé D a la valeur entière:

0x6b1f1d36 ... c5c4dbd1.

Le câblo-modem peut décrypter la clé d'autorisation en utilisant ou non le théorème du reste chinois (CRT, *chinese remainder theorem*). Le décryptage utilisant le théorème CRT est plus compliqué, mais il peut s'avérer plus rapide.

Pour effectuer le décryptage sans utiliser le théorème CRT, le câblo-modem exécute l'opération $M = Y^D \bmod N$. D est l'exposant privé dans le tableau, et Y et N sont tels que décrits dans le paragraphe précédent. La valeur résultante correspond à la valeur de M du paragraphe précédent, c'est-à-dire qu'elle est la valeur entière du bloc EM formé par le CMTS. Le câblo-modem décode la

clé d'autorisation à partir du bloc EM en inversant la procédure utilisée par le CMTS pour former le bloc EM, tel que décrit dans [RSA3].

Pour procéder au décryptage en utilisant le théorème CRT, le câblo-modem calcule d'abord deux quantités intermédiaires:

$$A = Y^{Dp} \bmod P;$$

$$B = Y^{Dq} \bmod Q.$$

P et Q sont des facteurs principaux du module et D_p et D_q sont des exposants privés associés à ces facteurs, ayant les valeurs indiquées dans le tableau. Le câblo-modem calcule la valeur de M au moyen de l'équation:

$$M = A + ((B – A)U_p \bmod Q)P;$$

U_p est une constante issue des facteurs principaux, dont la valeur est indiquée dans le tableau. La valeur résultante de M correspond à la valeur qui aurait été calculé en utilisant l'opération $M = Y^D \bmod N$.

I.4.3 Détails de l'opération de dispersion

La clé d'autorisation est dispersée au moyen de l'algorithme SHA-1 [FIPS-180-2] pour produire la clé de cryptage (KEK, *key encryption key*), la clé d'authentification de message pour le flux amont et la clé d'authentification de message pour le flux aval.

Pour le calcul de dispersion présenté ici on utilise un tableau qui montre les données d'entrée de la fonction de dispersion et la valeur résultante de la dispersion. Pour référence, nous donnons ici un tableau qui décrit l'exemple donné dans l'Appendice B de [FIPS-180-2]:

Donnée d'entrée de dispersion	61 62 63 64 62 63 64 65 63 64 65 66 64 65 66 67 65 66 67 68 66 67 68 69 67 68 69 6a 68 69 6a 6b 69 6a 6b 6c 6a 6b 6c 6d 6b 6c 6d 6e 6c 6d 6e 6f 6d 6e 6f 70 6e 6f 70 71
Valeur de dispersion	84 98 3e 44 1c 3b d2 6e ba ae 4a a1 f9 51 29 e5 e5 46 70 f1

I.4.3.1 Clé de cryptage de clé (KEK)

La clé KEK est calculée en utilisant les calculs de dispersion suivants:

Donnée d'entrée de dispersion	53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 4e 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc 0b 75
Valeur de dispersion	76 b4 d4 2f 14 98 59 6a ab fe 72 94 15 7c 7d 62 b0 df e6 3b

La donnée d'entrée est l'octet 0x53, répété 64 fois, suivi des 20 octets de la clé d'autorisation. L'ordre dans lequel les octets de la clé d'autorisation sont résumés est le même que l'ordre avec lequel ils apparaissent dans le bloc de cryptage EM.

La valeur de dispersion occupe 20 octets. Les 16 premiers octets sont la clé KEK.

I.4.3.2 Clés d'authentification de message

La clé d'authentification du message amont est calculée par dispersion comme suit:

Donnée d'entrée de dispersion	5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 4e 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc 0b 75
Valeur de dispersion	fe b9 f1 e2 46 a7 6d 7c a7 7b 5e b0 98 25 fd 0b 57 ca 90 c7

La donnée d'entrée est l'octet 0x5c, répété 64 fois, suivi des 20 octets de la clé d'autorisation. L'ordre dans lequel les octets de la clé d'autorisation sont absorbés est le même que dans le calcul de la clé KEK.

La valeur de dispersion occupe 20 octets. Ces 20 octets constituent la clé d'authentification du message amont.

La clé d'authentification du message aval est calculée par dispersion comme suit:

Donnée d'entrée de dispersion	3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 4e 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc 0b 75
Valeur de dispersion	93 d3 9d 70 c3 b6 f5 92 c4 6b d3 92 76 46 f4 f1 90 3a 52 fd

Ce calcul est analogue à celui du cas du message amont, sauf que la valeur 0x3a remplace la valeur 0x5c.

I.4.3.3 Fonction de production de masque

La fonction de production de masque (MGF, *mask-generation function*) est constituée d'opérations de dispersion SHA-1. Chaque opération de dispersion produit 20 octets de données de masque. Le nombre d'opérations de dispersion exécutées dépend de la taille du masque nécessaire.

La quantité SEED_MASK est formée en appliquant la fonction MGF à MASKED_DB. Puisque SEED_MASK occupe 20 octets, une seule opération de dispersion est nécessaire:

Donnée d'entrée de dispersion	04 29 6a b7 1f a2 a1 7f 96 60 d7 96 47 33 9d 2d bc a3 a1 32 37 ac 86 06 7c b5 ec 97 d2 d0 9e 01 30 2b 10 91 3a ec 3f d9 a1 2f c4 e9 8d 18 88 95 f6 9c ea 17 23 9f 5d d5 f1 4d 25 8e 9e 6d 7d 3c ca 55 fe 0e ee 2d 0d 7e 5b 64 b6 79 44 76 cc 3f 6e ac 99 3a ae 14 3f d4 0b f8 c3 f2 6b 2a 3c 9b 97 ac 91 6c 7c e4 c5 5f 7b cf 17 00 00 00 00
Valeur de dispersion	b4 b6 f1 bf a6 b3 a1 7e 95 82 d3 b8 93 71 b6 7f 45 31 9e 82

Les données d'entrée pour l'opération de dispersion sont MASKED_DB qui occupe 107 octets suivis de quatre octets de valeur zéro. Le résultat de l'opération de dispersion est la valeur de SEED_MASK.

La quantité DB_MASK est formée en appliquant la fonction MGF à SEED. Etant donné que DB_MASK occupe 107 octets, il faut six opérations de dispersion:

Donnée d'entrée de dispersion	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 00
Valeur d'entrée de dispersion	de 10 c9 59 41 c9 ea 72 a4 35 68 79 d2 53 85 bd 13 7b a6 3b

Donnée d'entrée de dispersion	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 01
Valeur d'entrée de dispersion	37 ac 86 06 7c b5 ec 97 d2 d0 9e 01 30 2b 10 91 3a ec 3f d9

Donnée d'entrée de dispersion	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 02
Valeur d'entrée de dispersion	a1 2f c4 e9 8d 18 88 95 f6 9c ea 17 23 9f 5d d5 f1 4d 25 8e

Donnée d'entrée de dispersion	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 03
Valeur d'entrée de dispersion	9e 6d 7d 3c ca 55 fe 0e ee 2d 0d 7e 5b 64 b6 79 44 76 cc 3f

Donnée d'entrée de dispersion	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 04
Valeur d'entrée de dispersion	6e ac 99 3a ae 14 3e 9a 8e df 3c 36 79 58 b2 fa 13 72 58 4c

Donnée d'entrée de dispersion	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 05
Valeur d'entrée de dispersion	ca 04 a1 af c7 c4 62 3a df 6f 33 ec e2 cd 2c 7f b7 7e 48 19

Les données d'entrée à chaque opération de dispersion sont les 20 octets de SEED suivis d'une valeur occupant quatre octets. La valeur occupant quatre octets compte les valeurs entières 0, 1, 2, 3, 4, 5 sur les opérations de dispersion successives. Les données de sortie des six opérations de dispersion sont concaténées en un résultat de 120 octets et des 107 premiers octets du résultat constitué par DB_MASK.

I.5 Demande de clé

Le câblo-modem envoie la demande de clé suivante:

07 73 00 d0	En-tête de demande de clé
05 00 ad	En-tête d'identification de CM
01 00 0c 30 30 30 30 30 30 31 32 33 34 35 36	Numéro de série
02 00 03 25 53 41	ID de fabricant
03 00 06 00 00 ca 01 04 01	Adresse MAC

04 00 8c 30 81 89 02 81 81 00 e0 e0 6c 8d be b2 8b c9 f3 a6 3d a1 12 ea f7 99 f7 3d 3e fa a3 b1 e2 42 95 71 b5 71 d2 32 7a da 10 40 e2 5b 09 74 69 08 78 46 37 71 34 3e 69 a7 37 6d f8 70 1d aa a5 34 b0 33 a3 43 ac 4d eb 41 5e 0a 8a fd a6 0a 4b 09 7f 5a 18 f2 9e c2 22 a6 6b 9a 69 73 22 d5 37 c9 63 b0 88 f5 60 5d 99 16 33 54 53 30 ed 35 de 0c 87 3b 54 ba 59 22 3e b2 79 90 96 61 db f3 4a 37 18 4c 7f a8 ca ee d6 31 02 03 01 00 01	Clé publique RSA
0a 00 01 07	Numéro de séquence de clé
0c 00 02 22 60	SAID
0b 00 14 86 b8 33 b7 48 9c 4b a1 51 67 44 d7 a6 e6 ca 21 33 f5 22 9e	Résumé HMAC

Le champ code a la valeur 0x07, qui identifie celle-ci comme étant un paquet de demande de clés. Le champ identificateur a la valeur 0x73; il s'agit d'une valeur donnée en exemple, obtenue en incrémentant la valeur de l'identificateur contenu dans la demande d'autorisation. Le champ longueur a la valeur 0x00d0 (208), qui est le nombre d'octets qui suit le champ longueur.

Le premier attribut est l'identification CM. Il s'agit d'un attribut composite, identique à celui qui se trouve dans la demande d'autorisation.

Le deuxième attribut est le numéro de séquence de clé qui identifie la clé d'autorisation. La valeur est identique à celle qui se trouve dans la réponse d'autorisation.

Le troisième attribut est l'identificateur SAID pour lequel une clé est demandée. Cette valeur de l'identificateur SAID était contenue dans la demande d'autorisation.

Le dernier attribut est le résumé HMAC. Ce résumé se compose de 20 octets. Il est calculé en utilisant la clé d'authentification de message. L'opération de résumé est effectuée sur tous les octets du paquet de demandes de clés, à l'exclusion des 23 octets de l'attribut résumé HMAC lui-même. Les détails de l'opération de résumé sont donnés ci-après.

I.5.1 Détails relatifs au résumé HMAC

Le résumé MAC est calculé en utilisant la méthode d'authentification HMAC définie dans [RFC 2104], la fonction de dispersion étant la fonction SHA-1. Des exemples de calculs de HMAC utilisant le SHA-1 sont présentés dans [RFC 2202].

La présente discussion porte sur le calcul de HMAC en utilisant le tableau qui montre la clé, les données d'entrée pour la fonction HMAC et le résumé HMAC résultant. Pour référence, nous donnons ci-après un tableau qui décrit le cas de test #2 des exemples HMAC-SHA-1 dans [RFC 2202]:

Clé	4a 65 66 65
Données d'entrée HMAC	77 68 61 74 20 64 6f 20 79 61 20 77 61 6e 74 20 66 6f 72 20 6e 6f 74 68 69 6e 67 3f
Résumé HMAC	ef fc df 6a e5 eb 2f a2 d2 74 16 d5 f1 84 df 9c 25 9a 7c 79

Le résumé HMAC du paquet de demande de clés est calculé en utilisant le calcul HMAC suivant:

Clé	fe b9 f1 e2 46 a7 6d 7c a7 7b 5e b0 98 25 fd 0b 57 ca 90 c7
Données d'entrée HMAC	07 73 00 d0 05 00 ad 01 00 0c 30 30 30 30 30 30 31 32 33 34 35 36 02 00 03 25 53 41 03 00 06 00 00 ca 01 04 01 04 00 8c 30 81 89 02 81 81 00 e0 e0 6c 8d be b2 8b c9 f3 a6 3d a1 12 ea f7 99 f7 3d 3e fa a3 b1 e2 42 95 71 b5 71 d2 32 7a da 10 40 e2 5b 09 74 69 08 78 46 37 71 34 3e 69 a7 37 6d f8 70 1d aa a5 34 b0 33 a3 43 ac 4d eb 41 5e 0a 8a fd a6 0a 4b 09 7f 5a 18 f2 9e c2 22 a6 6b 9a 69 73 22 d5 37 c9 63 b0 88 f5 60 5d 99 16 33 54 53 30 ed 35 de 0c 87 3b 54 ba 59 22 3e b2 79 90 96 61 db f3 4a 37 18 4c 7f a8 ca ee d6 31 02 03 01 00 01 0a 00 01 07 0c 00 02 22 60
Résumé HMAC	86 b8 33 b7 48 9c 4b a1 51 67 44 d7 a6 e6 ca 21 33 f5 22 9e

La clé est la clé d'authentification de message aval. Les données d'entrée se composent de tous les octets du paquet de demande de clés, à l'exclusion de l'attribut résumé HMAC. Les octets du résumé sont le contenu de l'attribut résumé HMAC.

I.6 Réponse de clé

Le CMTS envoie la réponse de clé suivante:

08 73 00 68	En-tête de réponse de clé
0a 00 01 07	Numéro de séquence de clé (clé d'autorisation)
0c 00 02 22 60	SAID
0d 00 21	En-tête de paramètre clé TEK
08 00 08 b6 4d 54 8c 3f 6b 25 69	Clé TEK
09 00 04 00 00 a8 c0	Durée de vie de la clé
0a 00 01 02	Numéro de séquence de la clé (TEK)
0f 00 08 81 0e 52 8e 1c 5f da 1a	DES CBC-IV
0d 00 21	En-tête paramètres TEK
08 00 08 5e bd 03 aa 5e d5 e2 94	Clé TEK
09 00 04 00 01 51 80	Durée de vie de la clé
0a 00 01 03	Numéro de séquence de la clé (TEK)
0f 00 08 25 35 67 c3 09 21 8c 2c	DES CBC-IV
0b 00 14 a5 e3 33 25 ea 72 f8 50 1c 2a b6 65 45 6b cc de 8b 4f 22 02	Résumé HMAC

Le champ code a la valeur 0x08, laquelle indique qu'il s'agit d'un paquet de réponse de clés. L'identificateur a la valeur 0x73, correspondant à la valeur figurant dans la demande de clé. Le champ longueur a la valeur 0x68 (104), qui est le nombre d'octets qui suit le champ longueur.

L'attribut numéro de séquence de clé identifie la clé d'autorisation. Elle correspond à la valeur figurant dans la demande de clé.

L'attribut SAID identifie l'identificateur SAID pour lequel une clé TEK doit être fournie. Il correspond à la valeur figurant dans la demande de clé.

Deux attributs de paramètre TEK sont inclus, le premier pour l'ancienne génération de paramètres d'octet, le second pour la nouvelle. Chaque attribut paramètre de clé est un attribut composite

constitué des attributs suivants: clé TEK, durée de vie de clé, numéro de séquence de clé et DES CBC-IV.

La clé TEK comporte 8 octets. La clé TEK, est cryptée en utilisant le cryptage triple DES-ECB avec la clé KEK dérivée de la clé d'autorisation. Des détails concernant le calcul du cryptage triple DES-ECB sont donnés ci-dessous.

Le sous-attribut de durée de vie de clé se réfère à la clé TEK. Dans cet exemple, la valeur pour l'ancienne clé TEK est 0x0000a8c0 (43200) secondes, ou 12 heures, et la valeur pour la nouvelle TEK est 0x00015180 (86400) secondes, ou 24 heures.

Le sous-attribut numéro de séquence de clé identifie la clé TEK. Dans cet exemple, la valeur pour les anciennes clés TEK est 0x02 et 0x03 pour les nouvelles.

Le sous-attribut DES CBC-IV se compose de 8 octets. Il spécifie le vecteur d'initialisation (IV, *initialization vector*) à utiliser avec la clé TEK.

L'attribut final est le résumé HMAC. Il se compose de 20 octets. Il est calculé de manière analogue à la réponse de clé, à l'exception de la clé d'authentification de message aval qui est utilisée au lieu de la clé amont. Des détails du calcul HMAC sont donnés ci-dessous.

Après que le câblo-modem ait traité le paquet réponses de clés, le câblo-modem et le système CMTS partagent chacun deux générations de clés et de vecteurs d'initialisation (IV). Les valeurs de ces paramètres correspondant à cet exemple sont données ci-après:

Ancienne clé TEK	`e6 60 0f d8 85 2e f5 ab`
Ancien vecteur IV	`81 0e 52 8e 1c 5f da 1a`
Nouvelle clé TEK	`b1 d7 4f c9 64 68 f7 58`
Nouveau vecteur IV	`25 35 67 c3 09 21 8c 2c`

I.6.1 Détails de cryptage de la clé TEK

Le système CMTS produit une clé TEK aléatoire de 8 octets. Dans cet exemple la valeur de TEK est la suivante:

```
e6 60 0f d8 85 2e f5 ab.
```

Il s'agit de la première clé TEK du message réponse de clé.

La clé TEK est cryptée en utilisant le cryptage triple DES-ECB. La clé de cryptage est la clé KEK:

```
76 b4 d4 2f 14 98 59 6a ab fe 72 94 15 7c 7d 62.
```

Le cryptage triple DES-ECB est décrit ici en termes d'itérations de cryptage ou de décryptage DES-ECB. Le cryptage DES-ECB est défini dans [FIPS-81].

La discussion ici porte sur une opération de cryptage ou de décryptage DES-ECB utilisant un tableau montrant la clé, l'entrée et le résultat. Pour référence, les tableaux qui décrivent l'exemple du Tableau B1 de [FIPS-81] sont donnés ci-après:

Mode	Cryptage ECB
Clé	`01 23 45 67 89 ab cd ef`
Entrée DES	`4e 6f 77 20 69 73 20 74`
Résultat DES	`3f a4 0e 8a 98 4d 48 15`

Mode	Décryptage ECB
Clé	01 23 45 67 89 ab cd ef
Entrée DES	3f a4 0e 8a 98 4d 48 15
Résultat DES	4e 6f 77 20 69 73 20 74

NOTE – Dans la norme [FIPS-81], le bit de plus faible poids de chaque octet de la clé doit être ajusté afin que l'octet ait une parité paire. Cela est évident dans la clé de l'exemple ci-dessus. Dans le protocole BPKM, on n'exige pas une parité paire. Ce protocole produit et distribue des clés DES à 8 octets de parité arbitraire et demande à ce que dans les implémentations soit ignorée la valeur du bit de plus faible poids de chaque octet.

La clé TEK est cryptée en triple DES-ECB au moyen des trois opérations DES-ECB suivantes:

Mode	Cryptage ECB
Clé	76 b4 d4 2f 14 98 59 6a
Entrée DES	e6 60 0f d8 85 2e f5 ab
Résultat DES	c3 94 31 f5 8d f9 1d bf

Mode	Décryptage ECB
Clé	ab fe 72 94 15 7c 7d 62
Entrée DES	c3 94 31 f5 8d f9 1d bf
Résultat DES	44 b0 94 4e ab 04 4c 23

Mode	Cryptage ECB
Clé	76 b4 d4 2f 14 98 59 6a
Entrée DES	44 b0 94 4e ab 04 4c 23
Résultat DES	b6 4d 54 8c 3f 6b 25 69

La première et la troisième opération sont le cryptage DES-ECB; la clé pour chacune de ces opérations est constituée par les huit premiers octets de la clé KEK. La deuxième opération est le décryptage DES-ECB; la clé est constituée par les huit derniers octets de la clé KEK. L'entrée de la première opération est la clé TEK à crypter. L'entrée de la deuxième opération est le seul résultat de la première, et l'entrée de la troisième opération est le résultat de la deuxième opération. Le résultat de la troisième opération est la TEK cryptée; elle est acheminée dans le sous-attribut clé TEK du message de réponse de clé.

I.6.2 Détails concernant HMAC

Le résumé HMAC du paquet réponse de clé est calculé par une méthode analogue à celle utilisée pour le paquet demande de clé. La clé est la clé d'authentification de message aval. Voici les détails du calcul HMAC:

Clé	93 d3 9d 70 c3 b6 f5 92 c4 6b d3 92 76 46 f4 f1 90 3a 52 fd
Données d'entrée HMAC	08 73 00 68 0a 00 01 07 0c 00 02 22 60 0d 00 21 08 00 08 b6 4d 54 8c 3f 6b 25 69 09 00 04 00 00 a8 c0 0a 00 01 02 0f 00 08 81 0e 52 8e 1c 5f da 1a 0d 00 21 08 00 08 5e bd 03 aa 5e d5 e2 94 09 00 04 00 01 51 80 0a 00 01 03 0f 00 08 25 35 67 c3 09 21 8c 2c
Résumé HMAC	a5 e3 33 25 ea 72 f8 50 1c 2a b6 65 45 6b cc de 8b 4f 22 02

I.7 Cryptage de l'unité PDU en mode paquet

Les douze premiers octets de l'unité PDU en mode paquet, contenant les adresses de destination et d'origine Ethernet/802.3 (DA/SA, *destination and source adresses*) ne sont pas cryptés. Les octets restants du PDU paquet sont cryptés au moyen du mode DES-CBC avec traitement spécial des blocs de terminaison résiduels dont la longueur est inférieure à 64 bits. La combinaison du mode DES-CBC et du traitement des blocs résiduels garantit que la longueur du paquet n'est pas modifiée par le cryptage. La clé de cryptage est la clé TEK correspondant au numéro de séquence de clé de l'en-tête élargi de confidentialité du paquet.

La spécification décrit le traitement des blocs résiduels comme suit:

"étant donné un bloc final de longueur n bits, n étant inférieur à 64, le bloc du texte du cryptogramme immédiatement après le dernier est crypté en DES une seconde fois, en utilisant le mode ECB et l'on applique un OU exclusif pour n bits de plus faible poids avec les n bits finals de la charge utile, afin de générer le bloc de chiffrement final court. ... Dans le cas particulier où la charge utile PDU de données en mode paquet occupe moins de 64 bits, le vecteur initialisation est crypté en DES et on applique un OU exclusif aux n bits les plus à gauche du cryptogramme résultant correspondant au nombre de bits de la charge utile avec les n bits de la charge utile pour générer le bloc de cryptage court."

Une autre description de cette procédure, qui est équivalente à la description figurant dans la spécification, est la suivante:

"étant donné un bloc final occupant n bits, n étant inférieur à 64, on ajoute 64 n bits de valeur arbitraire à la droite des n bits de charge utile pour former un bloc de 64 bits. Le bloc résultant est crypté en DES en utilisant le mode CFB64, le bloc de cryptogramme suivant servant de vecteur d'initialisation pour l'opération CFB64. Les n bits les plus à gauche du cryptogramme résultant sont utilisés comme bloc de chiffrement court. ... Dans le cas spécial où la charge utile PDU de données en mode paquet occupe moins de 64 bits, la procédure est la même que celle appliquée à un bloc final court, pour lequel le vecteur initialisation fourni sert de vecteur initialisation pour l'opération de cryptage DES-CFB64."

La deuxième description donne le même cryptogramme que la description contenue dans la spécification. Dans cette deuxième description, cependant, aucune mention n'est faite de l'application d'un opérateur OU exclusif au cryptage ECB. Ces opérations sont internes au mode CFB64, tout comme elles sont internes au mode CBC. L'autre description est pratique ici car elle permet d'illustrer le traitement du bloc résiduel en utilisant les exemples de mode CFB64 figurant dans [FIPS-81].

L'unité PDU en mode paquet inclut les champs DA, SA, et Type/Longueur. Dans les exemples ici, on n'essaie pas d'utiliser des valeurs correctes pour ces champs. Par conséquent, les exemples ici ne portent pas sur des paquets valables pour la transmission. Ces exemples servent uniquement à illustrer les détails du cryptage.

Dans ces exemples, les clés TEK et le vecteur d'initialisation (IV) proviennent du paquet réponse de clé utilisé pour l'exemple décrit ci-dessus.

I.7.1 Mode CBC uniquement

Lorsque le nombre d'octets à crypter est un multiple de 8, le mode de cryptage est le DES-CBC défini dans [FIPS-81]. La clé de cryptage et le vecteur d'initialisation (IV) sont acheminés dans le paquet réponse de clé.

L'analyse porte ici sur un cryptage DES-CBC avec un tableau qui montre la clé, le vecteur d'initialisation (IV), l'entrée en texte en clair et le cryptogramme résultant. Pour information, nous donnons ci-après un tableau qui reprend l'exemple du Tableau C1 de [FIPS-81]:

Mode	CBC
Clé	01 23 45 67 89 ab cd ef
IV	12 34 56 78 90 ab cd ef
Texte en clair	4e 6f 77 20 69 73 20 74 68 65 20 74 69 6d 65 20
Cryptogramme	e5 c7 cd de 87 2b f2 7c 43 e9 34 00 8c 38 9c 0f

Supposons que l'unité PDU en mode paquet, avant cryptage soit la suivante:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Type/Longueur	00 01
Données utilisateur	02 03 04 05 06 07 08 09 0a 0b
CRC	88 41 65 06

Le cryptage DES-CBC est effectué comme suit:

Mode	CBC
Clé	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texte en clair	00 01 02 03 04 05 06 07 08 09 0a 0b 88 41 65 06
Cryptogramme	0d da 5a cb d0 5e 55 67 9f 04 d1 b6 41 3d 4e ed

L'unité PDU en mode paquet, après cryptage se présente comme suit:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Type/Longueur	0d da
Données utilisateur	5a cb d0 5e 55 67 9f 04 d1 b6
CRC	41 3d 4e ed

I.7.2 Mode CBC avec traitement des blocs résiduels

Lorsque le nombre d'octets à crypter est supérieur à 8 sans être un multiple de 8, le mode de cryptage est une combinaison des deux modes DES-CBC et DES-CFB64.

Le cryptage commence en mode DES-CBC. Ce mode est utilisé pour traiter tous les blocs DES complets présents. La clé de cryptage et le vecteur d'initialisation (IV) sont acheminés dans le paquet réponse de clé.

Après cryptage DES-CBC, il reste 1 à 7 octets non cryptés. Ces octets sont cryptés en utilisant le mode DES-CFB64. Ce mode est un "mode de chiffrage à 64 bits avec réaction" défini dans la publication [FIPS-81]. La clé de cryptage est celle qui est contenue dans le paquet réponse de clé. Le vecteur d'initialisation (IV) est constitué des derniers 8 octets du cryptogramme produit par le traitement DES-CBC.

La discussion ici porte sur un cryptage DES-CFB64 avec un tableau montrant la clé, le vecteur d'initialisation (IV), l'entrée texte en clair et le cryptogramme résultant. Pour information, nous donnons ici un tableau qui reprend l'exemple du Tableau D3 de la publication [FIPS-81]:

Mode	CFB64
Clé	01 23 45 67 89 ab cd ef
IV	12 34 56 78 90 ab cd ef
Texte en clair	4e 6f 77 20 69 73 20 74 68 65 20 74 69 6d 65 20
Cryptogramme	f3 09 62 49 c7 f4 6e 51 a6 9e 83 9b 1a 92 f7 84

Supposons que le paquet PDU avant cryptage soit le suivant:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Type/Longueur	00 01
Données utilisateur	02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
CRC	91 d2 d1 9f

Le nombre total d'octets à crypter est de 19. Les 16 premiers octets sont traités par cryptage DES-CBC et les 3 derniers par cryptage DES-CFB64.

Le cryptage DES-CBC est effectué comme suit:

Mode	CBC
Clé	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texte en clair	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 91
Cryptogramme	0d da 5a cb d0 5e 55 67 51 47 46 86 8a 71 e5 77

Le cryptage DES-CFB64 est effectué comme suit:

Mode	CFB64
Clé	e6 60 0f d8 85 2e f5 ab
IV	51 47 46 86 8a 71 e5 77
Texte en clair	d2 d1 9f 00 00 00 00 00
Cryptogramme	ef ac 88 e8 ee 80 33 14

La clé est la même que celle utilisée pour l'opération de cryptage DES-CBC. Le vecteur IV est constitué des 8 octets du cryptogramme généré par l'opération DES-CBC.

Il convient de noter que 5 octets de valeur 0 ont été adjoints aux 3 octets du texte en clair. Les valeurs de ces 5 octets n'ont aucun effet sur les 3 octets du texte en clair qui sont les seuls octets intéressants du cryptogramme. Il est possible d'utiliser pour les octets adjoints des valeurs autres que 0.

Après cryptage l'unité PDU paquet se présente comme suit:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Type/Longueur	0d da
Données d'utilisateur	5a cb d0 5e 55 67 51 47 46 86 8a 71 e5
CRC	77 ef ac 88

I.7.3 Trames incomplètes

Lorsque le nombre d'octets à crypter est inférieur à 8, le mode de cryptage est le DES-CFB64. La clé de cryptage et le vecteur IV sont acheminés dans le paquet réponse de clé.

Supposons que l'unité PDU en mode paquet, avant cryptage, soit la suivante:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Type/Longueur	00 01
Données d'utilisateur	02
CRC	88 ee 59 7e

Le cryptage DES-CFB64 est effectué comme suit:

Mode	CFB64
Clé	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texte en clair	00 01 02 88 ee 59 7e 00
Cryptogramme	17 86 a8 03 a0 85 75 01

A noter qu'un octet de valeur 0 a été adjoint aux 7 octets du texte en clair. La valeur de cet octet adjoint en texte clair n'a aucune incidence sur les 7 premiers octets du cryptogramme, qui sont les seuls octets du cryptogramme intéressants. Il est possible d'utiliser pour l'octet adjoint en texte clair une valeur arbitraire autre que 0.

Après cryptage, l'unité PDU en mode paquet se présente comme suit:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Type/Longueur	17 86
Données d'utilisateur	a8
CRC	03 a0 85 75

I.7.4 Clé de 40 bits

Le protocole BPKM produit et distribue toujours des clés DES de 56 bits. Lorsqu'on demande un cryptage à 40 bits, la clé DES de 56 bits est convertie dans une implémentation en une clé de 40 bits en remplaçant 16 des 56 bits de la clé TEK par des 0.

Une clé TEK comporte 8 octets, chaque octet contenant 7 bits de clé et un bit de parité. La conversion d'une clé TEK en une clé de 40 bits s'effectue comme suit:

- les deux premiers octets de la clé TEK sont mis à 0;
- les deux bits de plus fort poids du troisième octet de la clé TEK sont mis à 0;
- les 5 octets restants de la clé TEK ne sont pas modifiés.

Par exemple, si la clé TEK distribuée par le protocole BPKM est:

```
ff ff ff ff ff ff ff ff,
```

alors, la conversion à 40 bits donne la clé TEK:

```
00 00 3f ff ff ff ff ff.
```

A l'exception de cette conversion de la valeur de la clé, la procédure de cryptage sur 40 bits d'une unité PDU en mode paquet est identique au cas du cryptage sur 40 bits.

Afin d'illustrer le cryptage sur 40 bits, nous reprenons un exemple précédent d'unité PDU en mode paquet, avec conversion sur 40 bits de la clé TEK.

Supposons que l'unité PDU en mode paquet, avant cryptage, soit la suivante:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Type/Longueur	00 01
Données utilisateur	02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
CRC	91 d2 d1 9f

Le nombre total d'octets à crypter est 19. Les 16 premiers octets sont traités par cryptage DES-CBC et les 3 derniers par cryptage DES-CFB64.

Le cryptage DES-CBC est effectué comme suit:

Mode	CBC
Clé	00 00 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texte en clair	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 91
Cryptogramme	44 c8 4a 41 14 67 56 a2 dc 64 8f b0 dc 1e 1e 86

La clé est la clé TEK acheminée dans le message réponse de clé et convertie en une clé de 40 bits. Le vecteur IV est celui acheminé dans le message réponse de clé.

Le cryptage DES-CFB64 est effectué comme suit:

Mode	CFB64
Clé	00 00 0f d8 85 2e f5 ab
IV	dc 64 8f b0 dc 1e 1e 86
Texte en clair	d2 d1 9f 00 00 00 00 00
Cryptogramme	f1 42 aa a3 e4 9b eb 29

La clé est la même que celle utilisée pour le cryptage DES-CBC. Le vecteur IV est constitué des 8 derniers octets du cryptogramme généré par le cryptage DES-CBC.

L'unité PDU en mode paquet, après cryptage, se présente comme suit:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Type/Longueur	44 c8
Données utilisateur	4a 41 14 67 56 a2 dc 64 8f b0 dc 1e 1e
CRC	86 f1 42 aa

I.8 Cryptage des unités PDU en mode paquet avec suppression de l'en-tête de charge utile

Ces exemples décrivent le cryptage d'unités PDU en mode paquet en cas de suppression de l'en-tête de charge utile (PHS, *payload header suppression*). On utilise pour ces exemples une charge utile voix sur IP RTP sans essayer d'utiliser les valeurs correctes pour les champs de l'unité PDU en mode paquet. Par conséquent, ces exemples ne portent pas sur des paquets valables pour la transmission. Il s'agit uniquement d'illustrer les détails du cryptage.

I.8.1 Sens aval

Supposons une unité PDU en mode paquet, après suppression de l'en-tête de charge utile et avant cryptage, suivante:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
En-tête RTP	21 22 23 24 25 26 27 28 29 2a 2b 2c
Données vocales	31 32 33 34 35 36 37 38 39 3a
CRC	93 86 b3 b9

La suppression d'en-tête de charge utile a également entraîné la suppression du champ Type/Longueur qui autrement aurait été inclus dans l'en-tête Ethernet/802.3. Les données d'utilisateur se composent de l'en-tête RTP et des données vocales. Le cryptage commence avec le premier octet de l'en-tête RTP et se termine avec le dernier octet du contrôle CRC comme suit:

Mode	CBC
Clé	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texte en clair	21 22 23 24 25 26 27 28 29 2a 2b 2c 31 32 33 34 35 36 37 38 39 3a 93 86

Cryptogramme	b4 55 da c8 39 1e 0c ed 15 cf b5 79 0a c3 24 5e cf 0f 52 c0 69 f5 f6 6e

Mode	CFB64
Clé	e6 60 0f d8 85 2e f5 ab
IV	cf 0f 52 c0 69 f5 f6 6e
Texte en clair	b3 b9 00 00 00 00 00 00
Cryptogramme	3e 31 de ea 96 6a 88 6b

L'unité PDU en mode paquet, après cryptage se présente comme suit:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
En-tête RTP	b4 55 da c8 39 1e 0c ed 15 cf b5 79
Données vocales	0a c3 24 5e cf 0f 52 c0 69 f5
CRC	f6 6e 3e 31

I.8.2 Sens amont

Supposons que l'unité PDU en mode paquet, après application de la suppression de l'en-tête de paquet et avant le cryptage soit la suivante:

En-tête RTP	21 22 23 24 25 26 27 28 29 2a 2b 2c
Données vocales	31 32 33 34 35 36 37 38 39 3a
CRC	65 cf fe 89

La suppression d'en-tête de paquet a entraîné la suppression des champs DA, SA, et type/longueur qui autrement auraient été inclus dans l'en-tête Ethernet/802.3. Les données d'utilisateur se composent de l'en-tête RTP et des données vocales. Les douze premiers octets des données d'utilisateur ne sont pas cryptés. Le cryptage commence au premier octet des données vocales et se termine avec le dernier octet du contrôle CRC comme suit:

Mode	CBC
Clé	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texte en clair	31 32 33 34 35 36 37 38
Cryptogramme	d6 88 87 66 1f 66 04 79

Mode	CFB64
Clé	e6 60 0f d8 85 2e f5 ab
IV	d6 88 87 66 1f 66 04 79
Texte en clair	39 3a 65 cf fe 89 00 00
Cryptogramme	c0 07 20 8e 3b 0b b1 b9

L'unité PDU en mode paquet après cryptage se présente comme suit:

En-tête RTP	21 22 23 24 25 26 27 28 29 2a 2b 2c
Données vocales	d6 88 87 66 1f 66 04 79 c0 07
CRC	20 8e 3b 0b

I.9 Cryptage de paquets fragmentés

Lorsqu'un paquet est fragmenté, chaque fragment est indépendamment crypté en mode DES-CBC avec traitement de bloc résiduel. Les clés TEK et le vecteur IV de chaque fragment sont les mêmes que la clé TEK et le vecteur IV utilisés pour le cryptage d'une unité PDU en mode paquet non fragmentée. Tous les octets d'un fragment sont cryptés, y compris les 12 octets acheminant les adresses de destination et d'origine Ethernet/802.3 (DA/SA) de l'unité PDU en mode paquet.

Dans l'exemple ici, on n'a pas essayé d'utiliser des valeurs significatives pour les champs du paquet; par conséquent, le paquet n'est pas valable pour la transmission. Cet exemple a uniquement pour but d'illustrer les détails du cryptage.

Dans cet exemple, la clé TEK et le vecteur IV sont extraits de l'exemple de paquet réponse de clé précédemment décrit.

Supposons que le paquet soit divisé en deux fragments comme suit:

Fragment 1 de la charge utile	01 02 03 04 05 06 f1 f2 f3 f4 f5 f6 00 01 02 03 04 05
CRC du fragment 1	b4 2b 6d d4

Fragment 2 de la charge utile	06 07 08 09 0a 0b 0c 0d
CRC du fragment 2	48 34 45 36

Le premier fragment est crypté en utilisant les modes DES-CBC et DES-CFB64, comme suit:

Mode	CBC
Clé	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texte en clair	01 02 03 04 05 06 f1 f2 f3 f4 f5 f6 00 01 02 03
Cryptogramme	47 41 0f 4f fd 78 47 6e c8 1a 67 4e 26 0c 20 c5

Mode	CFB64
Clé	e6 60 0f d8 85 2e f5 ab
IV	c8 1a 67 4e 26 0c 20 c5
Texte en clair	04 05 b4 2b 6d d4 00 00
Cryptogramme	56 6d 5c 58 2f 56 dc 39

Le premier fragment après cryptage se présente comme suit:

Fragment 1 de la charge utile	47 41 0f 4f fd 78 47 6e c8 1a 67 4e 26 0c 20 c5 56 6d
CRC du fragment 1	5c 58 2f 56

Le deuxième fragment est crypté en utilisant les modes DES-CBC et DES-CFB64, comme suit:

Mode	CBC
Clé	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texte en clair	06 07 08 09 0a 0b 0c 0d
Cryptogramme	d8 55 0f 59 9d 19 d9 c6

Mode	CFB64
Clé	e6 60 0f d8 85 2e f5 ab
IV	d8 55 0f 59 9d 19 d9 c6
Texte en clair	48 34 45 36 00 00 00 00
Cryptogramme	b4 5f 3e 95 0e e4 d7 df

Le deuxième fragment après cryptage, se présente comme suit:

Fragment 2 de la charge utile	d8 55 0f 59 9d 19 d9 c6
CRC du fragment 2	b4 5f 3e 95

BIBLIOGRAPHIE

[IEEE1] IEEE Standard 802-1990, *IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture*, décembre 1990.

[RFC1750] EASTLAKE (D.), CROCKER (S.), SCHILLER (J.), *Randomness Recommendations for Security*, *IETF RFC 1750*, décembre 1994.

[RFC2202] CHENG (P.), GLENN (R.), *Test Cases for HMAC-MD5 and HMAC-SHA-1*, *IETF RFC 2202*, septembre 1997.

[SCHNEIER] SCHNEIER (B.), *Applied Cryptography*, Second Edition, John Wiley, New York, 1996.

[SET Book 2] *SET, Secure Electronic Transaction Specification* – Book 2: Programmer's Guide, Version 1.0, 31 mai 1997.

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	RGT et maintenance des réseaux: systèmes de transmission, circuits téléphoniques, télégraphie, télécopie et circuits loués internationaux
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 et communication entre systèmes ouverts
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de nouvelle génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2005