UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

# UIT-T H.233

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(07/95)

## TRANSMISSION DE SIGNAUX NON-TÉLÉPHONIQUES

# SYSTÈME DE CONFIDENTIALITÉ POUR LES SERVICES AUDIOVISUELS

## Recommandation UIT-T H.233

(Antérieurement «Recommandation du CCITT»)

## AVANT-PROPOS

L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'Union internationale des télécommunications (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.

La Conférence mondiale de normalisation des télécommunications (CMNT), qui se réunit tous les quatre ans, détermine les thèmes d'études 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 n° 1 de la CMNT (Helsinki, 1er-12 mars 1993).

La Recommandation révisée UIT-T H.233, que l'on doit à la Commission d'études 15 (1993-1996) de l'UIT-T, a été approuvée le 10 juillet 1995 selon la procédure définie dans la Résolution n° 1 de la CMNT.

---

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 de télécommunications.

# TABLE DES MATIÈRES

**Recommandation H.233**

# SYSTÈME DE CONFIDENTIALITÉ POUR LES SERVICES AUDIOVISUELS

*(révisée en 1995)*

## 1 Champ d'application

Un système de protection des données privées comprend deux parties, le mécanisme de confidentialité ou processus de chiffrement des données, et un sous-système de gestion de clés.

La présente Recommandation décrit la partie «mécanisme de confidentialité» d'un système de protection des données privées destiné à être utilisé dans les services audiovisuels à bande étroite conformes aux Recommandations H.221, H.230 et H.242. Bien qu'un tel système de protection des données privées nécessite un algorithme de chiffrement, la spécification de cet algorithme n'est pas incluse ici: le système admet plusieurs algorithmes spécifiques.

Le système de confidentialité est applicable aux liaisons point à point entre terminaux ou entre un terminal et un pont de conférence (MCU) (*multipoint control unit*); son application peut être élargie au fonctionnement multipoint sans chiffrement dans le pont de conférence, mais cette question fera l'objet d'un complément d'étude.

## 2 Références normatives

Les Recommandations et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute Recommandation ou autre référence est sujette à révision; tous les utilisateurs de la présente Recommandation sont donc invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références indiquées ci-après. Une liste des Recommandations UIT-T en vigueur est publiée régulièrement.

[1] Recommandation UIT-T H.221 (1993), *Structure de trame pour un canal à débit de 64 à 1920 kbit/s pour les téléservices audiovisuels.*

[2] Recommandation UIT-T H.242 (1993), *Procédures permettant d'établir des communications entre des terminaux audiovisuels à l'aide de canaux numériques dont le débit peut aller jusqu'à 2 Mbit/s.*

[3] Recommandation UIT-T H.230 (1995), *Signaux de commande et d'indication synchrones de la trame pour les systèmes audiovisuels.*

[4] Recommandation X.208 du CCITT (1988), *Spécification de la syntaxe abstraite numéro un (ASN.1).*

## 3 Abréviations

Pour les besoins de la présente Recommandation, les abréviations suivantes sont utilisées:

| | |
|---|---|
| BAS | Signal d'affectation de débit binaire (*bit-rate allocation signal*) – Voir [1] |
| CRC4 | Contrôle de redondance cyclique à 4 bits (*4-bit cyclic redundancy check*) – Voir [1] |
| ECS | Signal de commande de chiffrement (*encryption control signal*) – Voir [1] |
| FAS | Signal de verrouillage de trame (*frame alignment signal*) – Voir [1] |
| H.221 | «Structure de trame/tramage selon la Recommandation H.221» – Voir [1] |
| ILC | Identificateur, longueur, contenu (*identifier, length, content*) |
| IV | Vecteur d'initialisation (*initialization vector*) |
| LSB | Bit de poids faible (*least significant bit*) |
| MCU | Pont de conférence (*multipoint control unit*) |
| MLP | Canal logique à protocole multicouche (*multi-layer protocol "MLP" logical channel*) – Voir [1] |

MSB Bit de poids fort (*most significant bit*)

SE Echange de session (*session exchange*)

SV Variable initiale (*starting variable*)

AIM Codes de commande et d'indication (*control* & *indication codes*) – Voir [3]

AIA Codes de commande et d'indication (*control* & *indication codes*) – Voir [3]

VIS Codes de commande et d'indication (*control* & *indication codes*) – Voir [3]

# 4 Propriétés du système spécifié

## 4.1 Confidentialité

1) La confidentialité est indépendante des autres services de protection des données privées assurés par le système; les clés sont fournies par d'autres mécanismes tels que celui qui est décrit dans le projet de Recommandation sur l'authentification et la gestion des clés, ou peuvent être introduites manuellement.

2) La confidentialité est applicable aux signaux audiovisuels dont le verrouillage de trame est conforme à la Recommandation H.221, aux débits utiles de $p \times 64$ kbit/s, où $p$ prend une valeur quelconque de 1 à 30. Conformément à la Recommandation H.221, la structure de trame elle-même n'est pas chiffrée.

3) La confidentialité est assurée pour toutes les transmissions audio, vidéo et de données des utilisateurs, ces signaux étant chiffrés ensemble avec la même clé (sont actuellement incluses ici les données MLP, conformément à l'Annexe A/H.221, bien que cet aspect nécessite un complément d'étude).

4) Le système est indépendant de l'algorithme de chiffrement utilisé; certains algorithmes sont actuellement prévus, auxquels d'autres pourront venir s'ajouter.

5) Le mécanisme de confidentialité peut fonctionner dans le cas de communications point à point, mais aussi dans le cas de communications multipoint pour lesquelles le déchiffrement est autorisé dans le pont de conférence (dit «sûr»).

## 4.2 Spécification des algorithmes

La spécification des algorithmes n'est pas incluse dans la présente Recommandation, qui s'applique à un large éventail d'algorithmes de chiffrement. Les spécifications sont à rechercher ailleurs (voir 5.2), avec les précisions suivantes:

– longueurs du vecteur d'initialisation et des clés de session;

– construction de la variable initiale par le vecteur d'initialisation.

# 5 Le mécanisme de confidentialité

## 5.1 Description du fonctionnement

La Figure 1 montre le schéma fonctionnel d'un module de chiffrement, avec ses blocs de chiffrement et de déchiffrement. Le module de chiffrement reçoit les données d'utilisateur, qu'il convertit en données chiffrées. Le module de déchiffrement reçoit les données chiffrées, qu'il déchiffre pour obtenir les données d'utilisateur.

Deux canaux permettent le raccordement du module de chiffrement et du module de déchiffrement. Le premier canal est utilisé pour transmettre les données d'utilisateur chiffrées. Le second est un canal non chiffré appelé «signal de commande de chiffrement» (ECS) (*encryption control signal*) qui est utilisé pour transmettre les informations de commande du module de chiffrement au module de déchiffrement. Bien que ces deux canaux soient représentés séparément sur la figure, dans la pratique ils sont multiplexés en un train de données unique.

Des techniques de chiffrement série sont utilisées (voir 5.2).

Les clés sont fournies par d'autres mécanismes et sont présentées au mécanisme de confidentialité lorsque besoin est. Elles sont utilisées par les unités de chiffrement et de déchiffrement simultanément avec les données, la synchronisation de chargement de clé étant signalée par un drapeau sur le canal de commande [voir L en 5.1.3, point 1), cinquième tiret].

Le chiffrement des données se fait sous la conduite du module de chiffrement: un drapeau de chiffrement EN/HORS SERVICE, envoyé par l'intermédiaire du canal de commande, indique le début du chiffrement des données. Le module de déchiffrement répond à ce drapeau et déchiffre les données lorsque la demande lui en est faite.

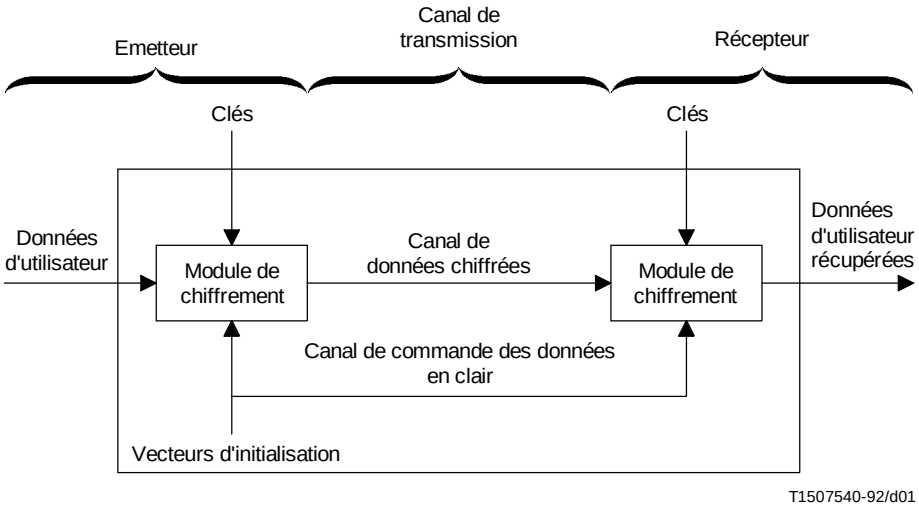



FIGURE 1/H.233

**Schéma fonctionnel d'un module de chiffrement de liaison**

### 5.1.1 Commandes et indication dans la trame H.221

Pour indiquer la présence d'un système de confidentialité dans un terminal, il est nécessaire de transmettre le code «possibilité de chiffrement» du signal BAS. Si cette possibilité est signalée par les deux extrémités d'une liaison, le canal du signal de commande de chiffrement (ECS) peut être ouvert dans chaque sens grâce à l'utilisation de la commande «chiffrement en service» du BAS; le canal ECS peut être fermé à l'aide de la commande «chiffrement hors service», mais cette commande doit être précédée par la transmission du drapeau «chiffrement hors service» dans le canal même (voir ci-dessous). Si un terminal reçoit la commande «chiffrement hors service» du BAS sans avoir reçu préalablement le drapeau «chiffrement hors service», on doit éveiller l'attention de l'utilisateur sur la possibilité d'une intrusion dans le système de confidentialité ou d'un mauvais fonctionnement de celui-ci.

En cas d'utilisation d'un signal dans un seul sens H.221, le canal ECS peut être activé sans que la possibilité de chiffrer soit signalée: le mécanisme qui permet au récepteur de déchiffrer l'algorithme choisi, ou autre possibilité, n'entre pas dans le cadre de la présente Recommandation.

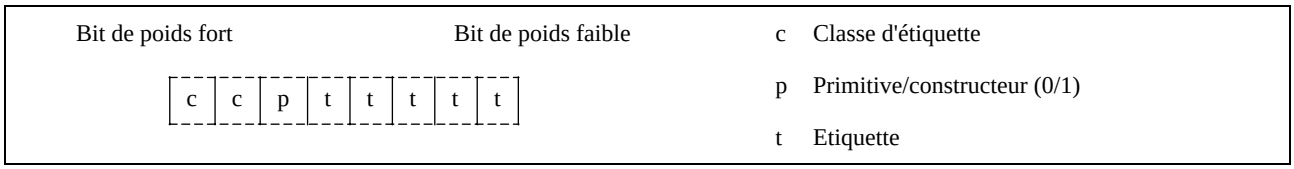
### 5.1.2 Formats des messages

Les messages utilisés par le système de chiffrement pour la distribution des clés et pour l'authentification ont un format de type «identificateur, longueur, contenu» (ILC) (*identifier, length, content*) avec entrelacement, comme indiqué dans la Recommandation X.208 [4]. Le codage de la longueur peut être de forme courte ou de forme longue. La forme indéfinie spécifiée dans la Recommandation X.208 [4] ne sera pas utilisée.

Un bref rappel de quelques-unes des définitions de la Recommandation X.208 [4] utilisées dans le cadre de la présente proposition est présenté ci-dessous.

#### 5.1.2.1 Identificateur

Un identificateur est un octet dont la structure est la suivante:




La classe d'étiquette définit le type d'identificateur qui aura la valeur 10 ou 11 (en fonction du contexte) pour les identificateurs définis dans la présente Recommandation.

Le bit de primitive/constructeur (P) indique si le contenu est une primitive ou s'il est composé d'éléments entrelacés.

L'étiquette de 5 bits définit exceptionnellement l'identificateur (selon sa classe).

Les identificateurs qui figurent dans la présente Recommandation se présentent donc tous sous la forme d'un octet du type: 10 P $t_1$ $t_2$ $t_3$ $t_4$ $t_5$ ou 11 P $t_1$ $t_2$ $t_3$ $t_4$ $t_5$.

#### 5.1.2.2 Longueur

La longueur du contenu, exprimée en nombre d'octets, est elle-même variable.

La forme courte, qui est d'un octet, est à utiliser de préférence à la forme longue lorsque L est inférieur à 128. Le bit 8 a la valeur 0 et les bits 7 à 1 codent L sous forme de nombre binaire sans signe dont le bit de poids fort et le bit de poids faible sont respectivement le bit 7 et le bit 1.

La forme longue, qui varie de 2 à 127 octets, est utilisée lorsque L est supérieur ou égal à 128 et inférieur à 2 à la puissance 1008. Le bit 8 du premier octet a la valeur 1. Les bits 7 à 1 du premier octet servent à coder un nombre inférieur d'une unité à la longueur en octets, sous la forme d'un nombre binaire sans signe dont le bit de poids fort et le bit de poids faible sont respectivement le bit 7 et le bit 1. L lui-même est codé sous la forme d'un nombre binaire sans signe, dont le bit de poids fort et le bit de poids faible sont respectivement le bit 8 du deuxième octet et le bit 1 du dernier octet. Ce nombre binaire doit être codé en un nombre aussi faible que possible d'octets, sans octet de gauche contenant la valeur 0.

#### 5.1.2.3 Chaîne binaire

Une chaîne binaire en forme de primitive compte huit bits par octet, précédés d'un octet qui code le nombre de bits inutilisés du dernier octet du contenu – de zéro à sept – sous la forme d'un nombre binaire sans signe dont le bit de poids fort et le bit de poids faible sont respectivement le bit 8 et le bit 1.

### 5.1.3 Canal ECS non chiffré

Le système de confidentialité nécessite l'utilisation d'un canal de commande non chiffré entre l'unité de chiffrement et l'unité de déchiffrement. Un seul canal de commande par système de chiffrement de liaison suffit. Ce canal de commande sert aussi au chiffrement des signaux audio et vidéo et, le cas échéant, des données.

Le contenu du canal ECS est structuré en blocs de 128 bits, inclus dans la multitrame H.221 (voir la Figure 2); le premier bit du bloc est donc le bit 8 de l'octet 17 de la trame numéro 0 de la multitrame. Il existe deux types de blocs: les blocs d'échange de session (SE) (*session exchange*) et les blocs de vecteur d'initialisation (IV) (*initialization vector*). Les informations contenues dans un bloc IV prennent effet dès le début de la multitrame suivante et restent en vigueur jusqu'à ce qu'un autre bloc IV soit envoyé. Le canal ECS doit toujours contenir un bloc IV ou un bloc SE. Il est à noter que la définition des algorithmes prévoit parfois le chargement répété du même bloc IV; cette opération est à utiliser ou à proscrire selon le choix de compromis entre une diminution du temps de reprise en cas d'erreur et une amélioration de la sécurité.

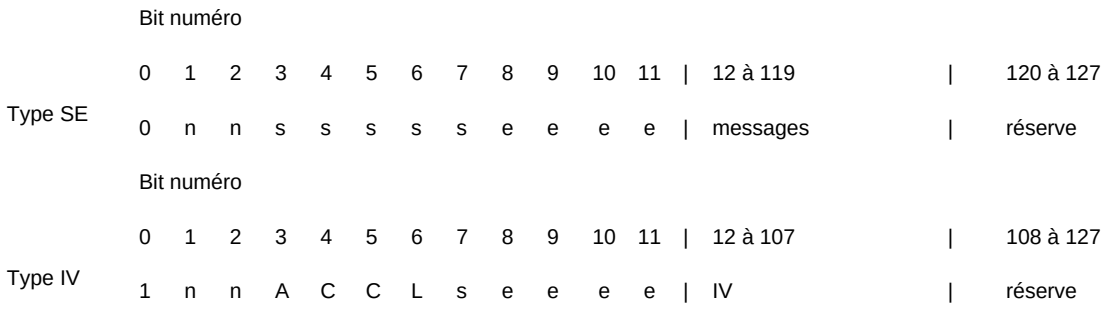



FIGURE 2/H.233

**Blocs du canal de commande**

Le bloc contient les éléments suivants:

1) en-tête (12 bits), comprenant:
   - bit 0 pour sélectionner le type: 0 = SE (échange de session)
     1 = IV (vecteur d'initialisation)
   - bits 1 et 2 pour identifier les blocs d'une séquence de plusieurs blocs:
     00 pour un bloc isolé non suivi de blocs connexes
     01 pour le bloc n° 1 d'une séquence de plusieurs blocs
     10 pour un bloc intermédiaire d'une séquence
     11 sur le dernier bloc d'une séquence
   - bit 3 du bloc de type IV pour indiquer le chiffrement en service/hors service (A):
     1 = EN SERVICE, 0 = HORS SERVICE
   - bits 4 et 5 du bloc de type IV pour indiquer la longueur de IV (CC):
     00 = 64 bits + 32 bits (correction d'erreur)
     01, 10, 11 réservés
   - bit 6 du bloc de type IV: réservé pour la synchronisation de chargement de clé (L)
   - autres bits: réservés mis à «0»
   - bits 8 à 11: correction d'erreur pour les bits 0 à 7,
2) blocs SE: structurés comme suit: 9 × (8 bits d'information + 4 bits de correction d'erreur);

   blocs IV: vecteur d'initialisation de système ou partie de vecteur d'initialisation de système (64 bits), avec protection contre les erreurs (32 bits),
3) blocs SE: 8 bits de réserve;

   blocs IV: 20 bits de réserve – laissent au système un intervalle pour donner suite aux informations reçues; peut aussi permettre une amélioration future.

#### 5.1.3.1 Blocs d'échange de session

Dans les blocs de type SE, les 116 bits qui suivent l'en-tête de 8 + 4 bits sont structurés comme suit: 9 × (8 + 4) + 8, les 8 derniers bits n'étant pas utilisés et les 9 mots comportant chacun 8 bits d'information + 4 bits de correction d'erreur. Dans le récepteur, les bits d'information (dont la provenance sera indiquée dans l'en-tête s'ils proviennent de plusieurs blocs) forment un train constitué des messages sur l'authentification et sur la gestion des clés, ainsi que des messages de possibilité d'algorithme (P8) et de commande d'algorithme (P9) définis ci-dessous.

Les 12 bits des mots inutilisés à la fin du bloc SE doivent être mis à zéro.

**Possibilité d'algorithme (P8)**

Nom du message: présentation de l'information de disponibilité des algorithmes de chiffrement (P8).

Identificateur du message: 1 1 P $t_1$ $t_2$ $t_3$ $t_4$ $t_5$ = 11000000.

Contenu: [numéro 3-255][octets supplémentaires] où le premier octet indique le nombre des octets qui suivent. Chaque ensemble de trois octets indique la disponibilité d'un mécanisme de chiffrement utilisant les valeurs indiquées pour les identificateurs de support d'information, les identificateurs d'algorithme et les identificateurs de paramètre énoncés ci-dessous. Par exemple, un terminal capable de décoder les algorithmes DES et FEAL transmettra le message P8 {[11000000][00000110][00000000][00000010][00000000][00000000][00000001][00000000]}.

**Commande d'algorithme (P9)**

Nom du message: présentation de l'information d'algorithme en service (P9).

Identificateur du message: 1 1 P $t_1$ $t_2$ $t_3$ $t_4$ $t_5$ = 11000001.

Signification: lorsqu'on place ensuite le bit de chiffrement EN SERVICE dans l'en-tête IV, l'algorithme utilisé est celui qui est spécifié ici dans ce message.

Contenu: octets du schéma de chiffrement (mêmes valeurs que dans le message de possibilité P8).

**Identificateurs de support d'information**

Un octet est utilisé pour déterminer ceux des éléments du système audiovisuel qui sont codés. Chaque bit de cet octet correspond au support d'information suivant:

| | |
|---|---|
| Premier bit (bit de poids faible): | Audio 0 = chiffré, 1 = non chiffré |
| Deuxième bit: | Vidéo 0 = chiffré, 1 = non chiffré |
| Troisième bit: | LSD 0 = chiffré, 1 = non chiffré |
| Quatrième bit: | HSD 0 = chiffré, 1 = non chiffré |
| Cinquième bit: | réservé pour MLP, mis à «0» |
| Sixième bit: | réservé pour H-MLP, mis à «0» |
| Septième bit: | réservé pour utilisation future, mis à «0» |
| Huitième bit (bit de poids fort): | réservé pour utilisation future, mis à «0» |

[00000000] indique que le signal multiplexé (sauf FAS, BAS et ECS) est chiffré. Les procédures applicables aux autres cas sont à l'étude.

**Identificateurs d'algorithme**

Un octet est utilisé pour l'identification de l'algorithme. La définition de l'algorithme indique en outre en détail comment procéder pour obtenir la suite chiffrante à partir de la clé et de la valeur IV en vigueur. Plusieurs algorithmes sont actuellement pris en compte; les codes à utiliser sont les suivants:

| Bit de poids fort Bit de poids faible | |
|---|---|
| 0 0 0 0 0 0 0 0 | Non attribué. Réservé pour utilisation ultérieure |
| 0 0 0 0 0 0 0 1 | «FEAL» (voir A.1) – Numéro d'enregistrement d'algorithme selon ISO/CEI 9979: 0010 |
| 0 0 0 0 0 0 1 0 | «DES» (voir A.2), Mode 1 – Numéro d'enregistrement d'algorithme selon ISO/CEI 9979: 0004 |
| 0 0 0 0 0 0 1 1 | Réservé pour «DES» (voir A.2), Mode 2 |
| 0 0 0 0 0 1 0 0 | Réservé pour «DES» (voir A.2), Mode 3 |
| 0 0 0 0 0 1 0 1 | B-CRYPT – Numéro d'enregistrement d'algorithme selon ISO/CEI 9979: 0001 |
| 0 0 0 0 0 1 1 0 | IDEA – Numéro d'enregistrement d'algorithme selon ISO/CEI 9979: 0002 |
| 0 0 0 0 0 1 1 1 | BARAS (ETSI) |
| Autres valeurs | Non attribué. Réservé pour utilisation ultérieure |

**Identificateurs de paramètre**

Un octet est utilisé pour identifier les paramètres des algorithmes de chiffrement définis en 5.2. La valeur par défaut est [00000000]; elle peut être utilisée lorsque l'algorithme ne nécessite pas de valeurs de paramètre. Pour les paramètres opérationnels de chaque méthode de chiffrement, se reporter à l'Annexe A.

L'équipement doit assurer le déchiffrement par au moins un des algorithmes indiqués; si plusieurs possibilités sont indiquées, on peut laisser à l'opérateur du système le soin de choisir l'algorithme nécessaire au chiffrement de l'information transmise.

**Autres messages**

P1 Nom du message: chiffrement impossible

Signification: l'expéditeur de ce message n'utilisera pas de système de chiffrement

Identificateur du message: 1 0 P $t_1$ $t_2$ $t_3$ $t_4$ $t_5$ = 10000001.

Contenu: ce message n'a pas de contenu.

P2 Nom du message: échec du lancement du système de chiffrement

Signification: l'expéditeur de ce message n'a pas réussi à mettre en marche son système de chiffrement. Cet échec peut être dû à une défaillance au stade de l'échange des clés; pour des raisons de sécurité, la cause de l'échec n'est pas indiquée dans le message.

Identificateur du message: 1 0 P $t_1$ $t_2$ $t_3$ $t_4$ $t_5$ = 100000010.

Contenu: ce message n'a pas de contenu.

Si l'on estime qu'il est nécessaire de transmettre P1 ou P2, ou si l'un de ces deux messages est reçu, une indication doit être fournie à l'utilisateur. Il appartient aux responsables de la mise en œuvre de spécifier les moyens à utiliser pour donner cette indication et les opérations qui suivront.

### 5.1.3.2 Vecteurs d'initialisation

La longueur par défaut d'un vecteur d'initialisation (IV) est de 64 bits. Correction d'erreur comprise, la longueur est de 96 bits. On peut transmettre des longueurs de vecteur IV plus grandes en utilisant plusieurs blocs. Le bit de poids fort, c'est-à-dire le bit 12 du (premier) bloc de type IV, est transmis en premier.

### 5.1.3.3 Protection contre les erreurs des informations transmises dans le canal de commande

Les informations transmises dans le canal de commande doivent être protégées contre les erreurs. On utilise à cet effet un code de Hamming [12,8]. Les matrices de générateur et de contrôle de parité sont représentées à la Figure 3.

La même structure est utilisée pour les en-têtes, pour les messages d'échange de session et pour les vecteurs d'initialisation. Dans chaque cas, un octet est suivi de quatre bits de correction d'erreur.

Le vecteur IV est subdivisé en 8 octets, assortis chacun de 4 bits de parité, ce qui porte la longueur totale du vecteur IV, bits de parité compris, à 96 bits, dans le cas par défaut.

| Matrice du générateur | Matrice de contrôle de parité |
|---|---|
| 100000001110<br>010000000111<br>001000001010<br>000100000101<br>000010001011<br>000001001100<br>000000100110<br>000000010011 | 1110<br>0111<br>1010<br>0101<br>1011<br>1100<br>0110<br>0011<br>1000<br>0100<br>0010<br>0001 |

T1507550-92/d02

FIGURE 3/H.233

**Matrices de correction d'erreur**

## 5.2 Méthode de chiffrement de la transmission

Le présent paragraphe traite du chiffrement des signaux audio, des signaux vidéo et, le cas échéant, des données associées. Le chiffrement n'aura lieu qu'en cas de verrouillage de multitrame H.221.

Le système de chiffrement remplit les mêmes fonctions quel que soit le débit utile. Chacun des flux de données d'utilisateur (ou leur ensemble) peut être chiffré. Le système de chiffrement n'a pas besoin d'être informé de la manière dont se répartissent ces diverses formes d'informations d'utilisateur, puisqu'il chiffre les données après le multiplexage et qu'il les déchiffre avant le démultiplexage. Les deux sens de transmission sont indépendants: le chiffrement est unilatéral ou bilatéral et différents algorithmes peuvent être utilisés.

L'ordre temporel de chiffrement suit l'ordre de transmission dans le train série, bit par bit. Il convient de chiffrer les données avant de procéder à un calcul CRC4. Les calculs CRC4 sont ensuite effectués sur des données chiffrées, ce qui garantit la validité du code CRC4 des réseaux associés qui pourront être présents.

Une suite chiffrante est créée dans les deux terminaux à partir des valeurs en cours de la clé et du vecteur d'initialisation; dans le module de chiffrement, cette suite vient s'ajouter en addition modulo 2 aux bits à chiffrer et, dans l'unité de déchiffrement, les bits chiffrés sont ajoutés en addition modulo 2 à la même suite chiffrante pour récupérer les informations d'utilisateur en clair.

Les vecteurs d'initialisation (IV) sont créés de manière aléatoire dans le module de chiffrement et sont envoyés au module de déchiffrement par l'intermédiaire du canal ECS. Ils sont utilisés avec les données à chiffrer ou à déchiffrer. Ils fournissent une méthode de resynchronisation périodique des modules de chiffrement et de déchiffrement.

NOTE – Selon l'algorithme choisi, il convient de prêter attention à l'ordre des bits de vecteur IV chargés dans les unités de chiffrement et de déchiffrement.

En cas de perte de synchronisation, les données seront altérées jusqu'à l'échange d'un nouveau vecteur IV. Le moment auquel le vecteur IV doit être transmis est fonction de la tolérance sur la perte de données jusqu'à resynchronisation.

Chaque bit dans le canal est traité par le système de chiffrement de l'une des trois manières suivantes (voir Appendice I):

a) suite chiffrante construite et appliquée: informations d'utilisateur (audio, vidéo, données);

b) suite chiffrante construite, mais non appliquée: signaux FAS et BAS dans les canaux initiaux, supplémentaires (voir la Recommandation H.221) et ECS; la suite chiffrante n'est ni stockée ni différée en vue d'une utilisation ultérieure, mais perdue; elle n'est pas utilisée pour chiffrer des informations ultérieures;

c) suite chiffrante non construite: si la sortie du terminal vers la ligne inclut des canaux qui ne font pas partie du débit utile spécifié dans la commande BAS pertinente (intervalle(s) TS0 et/ou TS16 d'une liaison à débit primaire, ou autres canaux non transmis de bout en bout, par exemple), aucune suite chiffrante n'est construite pour ces bits.

Dans le cas de la transmission à 56 kbit/s décrite dans l'Annexe B/H.221, la suite chiffrante est construite pour le huitième sous-canal, mais seuls les sept premiers bits sont utilisés pour l'addition modulo 2 au signal en sept parties.

Dans le cas de la transmission à débit binaire restreint de 128 kbit/s ou supérieur, la suite chiffrante est construite mais pas appliquée au huitième bit inséré par bourrage dans chaque intervalle de temps.

## 5.3 Procédure à suivre pour utiliser le système

Un terminal qui a reçu l'indication que le terminal correspondant dispose du chiffrement (voir Recommandation H.221) et qui souhaite commencer le chiffrement, ouvre le canal ECS et transmet le ou les messages P8. Au reçu du ou des messages P8 provenant du terminal correspondant, il vérifie s'il existe des algorithmes/modes compatibles; s'il n'en existe pas, il envoie le message P1; s'il y a compatibilité, il envoie un message P9 pour identifier l'algorithme/le mode qui sera utilisé, puis commence la transmission des blocs de vecteurs IV. L'Appendice II donne des exemples de procédures complètes pour la session de chiffrement.

Le message P2 peut être utilisé dans les procédures de reprise sur incident (nécessite un complément d'étude).

# 6 Chiffrement du canal MLP

Nécessite un complément d'étude.

# Annexe A

## Algorithmes de chiffrement et paramètres associés

(Cette annexe fait partie intégrante de la présente Recommandation)

### A.1 Algorithme FEAL

Une suite chiffrante est créée dans les deux terminaux à partir des valeurs actuelles de la clé et du vecteur d'initialisation à l'aide de l'algorithme FEAL-8 (FEAL à 8 étages avec clé à 64 bits) dans le mode par rebouclage de la sortie (OFB) (*output feedback*) défini dans ISO 8372. Des précisions sur l'algorithme FEAL sont données dans la référence [A1]. Dans l'unité de chiffrement, cette suite vient s'ajouter en addition modulo 2 aux bits à chiffrer et, dans l'unité de déchiffrement, les bits chiffrés sont ajoutés en addition modulo 2 à la même suite chiffrante pour récupérer l'information d'utilisateur en clair. Voir la Figure A.1.

La variable initiale (SV) (*starting variable*) est identique au vecteur d'initialisation (IV) (*initialization vector*). Le vecteur IV est chargé au début de chaque multitrame.

Sur les 64 bits sortants de l'algorithme de chiffrement, les huit premiers bits en partant du bit de poids fort sont utilisés pour addition bit par bit aux 8 bits du bloc du signal audiovisuel; le premier bit du bloc chiffrant est ajouté modulo 2 au premier bit du bloc du signal et le bit résultant est transmis au premier dans le canal; le deuxième bit du bloc chiffrant est ajouté modulo 2 au deuxième bit du bloc du signal et le bit résultant est transmis dans le canal, et ainsi de suite. Une fois les 8 bits transmis, le cycle suivant de la suite chiffrante est construit et utilisé pour le chiffrement.

### A.2 Algorithme DES

L'algorithme DES et les méthodes permettant d'appliquer la suite chiffrante au train de données sont décrits dans la référence [A2].

Le mode DES n° 1 fait appel à l'une des deux méthodes appelées OFB-8 et OFB-64. La variable initiale SV est identique au vecteur d'initialisation IV. L'identificateur de paramètre est mis aux valeurs suivantes:

| Valeur de champ | | Mode OFB | Nombre de bits |
|---|---|---|---|
| Bit de poids fort | Bit de poids faible | | |
| 0000 | 0000 | OFB-8 | 8 |
| 0000 | 0001 | OFB-64 | 64 |

Toutes les autres valeurs de l'identificateur de paramètre feront l'objet d'un complément d'étude.

Les modes DES n° 2 et 3 sont pour étude ultérieure.

### A.3 Algorithme IDEA

L'algorithme IDEA de chiffrement par blocs fonctionne avec des blocs de 64 bits à l'entrée et à la sortie et est contrôlé par une clé de 128 bits. Il est défini dans la référence [A3].

Pour obtenir la suite chiffrante, on utilise le mode par rebouclage de la sortie OFB-8 (*output feedback OFB*) (le mode OFB est défini dans ISO 8372). La variable initiale SV est identique au vecteur d'initialisation (IV).

Fondamentalement, la méthode qui permet d'appliquer la suite chiffrante au train de données correspond à celle du mode OFB définie dans ISO 8372. Les 8 bits de la suite chiffrante utilisés pour le chiffrement de 8 bits du train de données sont les bits de gauche du bloc de sortie à 64 bits décrit sur la Figure 1 de la référence [A3].

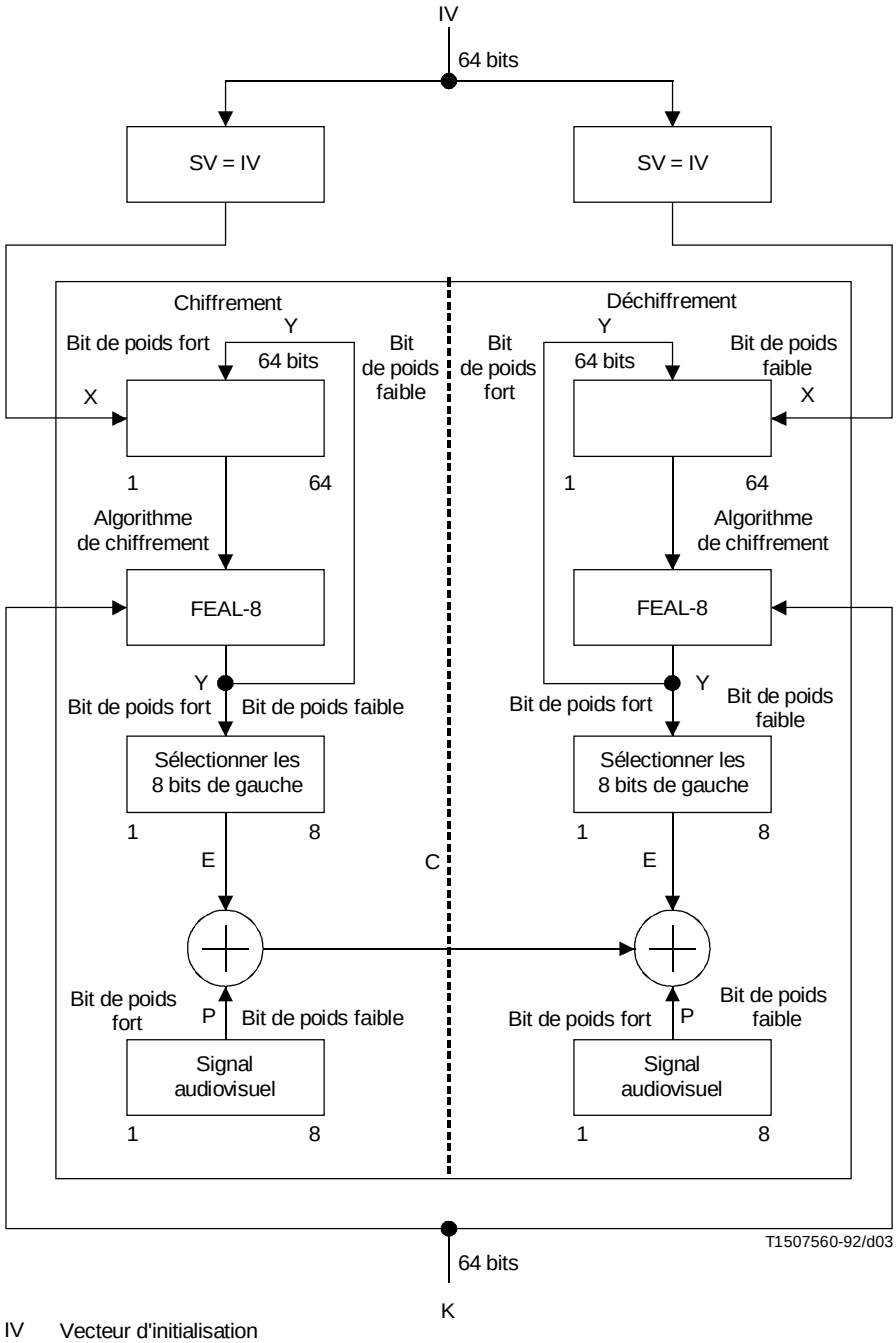
Dans ce mode, l'identificateur de paramètre (voir 5.1.3.1) est mis à la valeur [0000 0000]. D'autres modes de fonctionnement tels que le mode par chaînage de blocs chiffrants ou le mode par rebouclage du cryptogramme, décrits dans ISO 8372, sont pour étude ultérieure.

## Références


[A1] Algorithme FEAL: Numéro d'enregistrement 0010 selon ISO/CEI 9979.

[A2] Algorithme DES (*data encryption standard*, Norme relative au chiffrement des données): Numéro d'enregistrement 0004 selon ISO/CEI 9979.

[A3] Algorithme IDEA: Numéro d'enregistrement 0002 selon ISO/CEI 9979 (Techniques cryptographiques – Procédures pour l'enregistrement des algorithmes cryptographiques).


IV Vecteur d'initialisation
K Clé (*key*)
SV Vecteur initial

FIGURE A.1/H.233

**Mode par rebouclage de la sortie pour l'algorithme FEAL**

# Appendice I

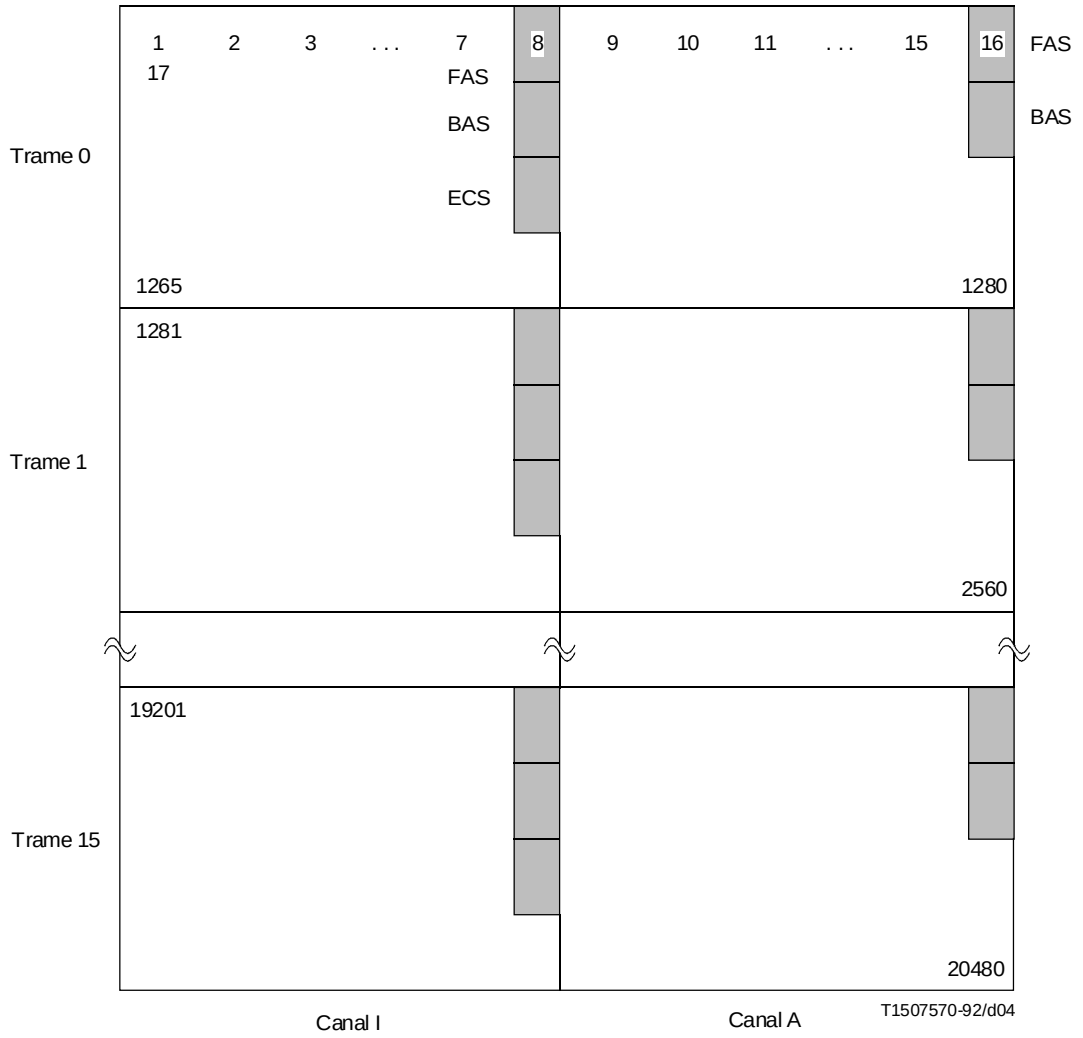
## Chiffrement et déchiffrement de 2 × canaux B

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

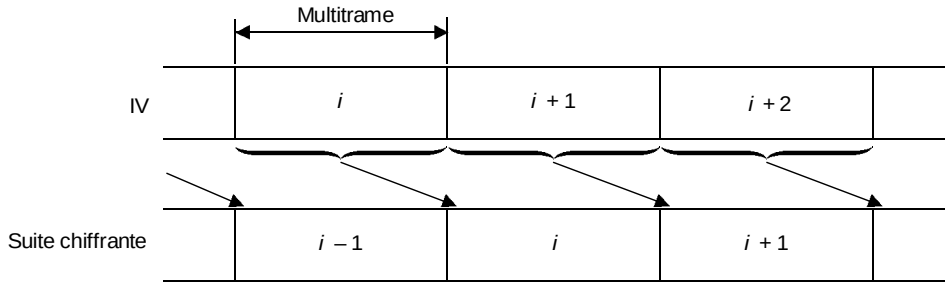
Le présent appendice donne un exemple du mode de fonctionnement du chiffrement/déchiffrement selon la Recommandation H.233.

– La suite chiffrante est construite pour tous les bits;

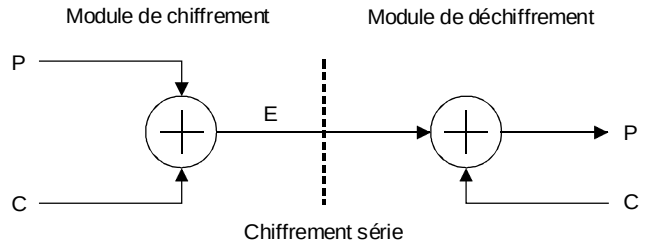
– la suite chiffrante est ajoutée à tous les bits sauf ceux de la partie ombrée.



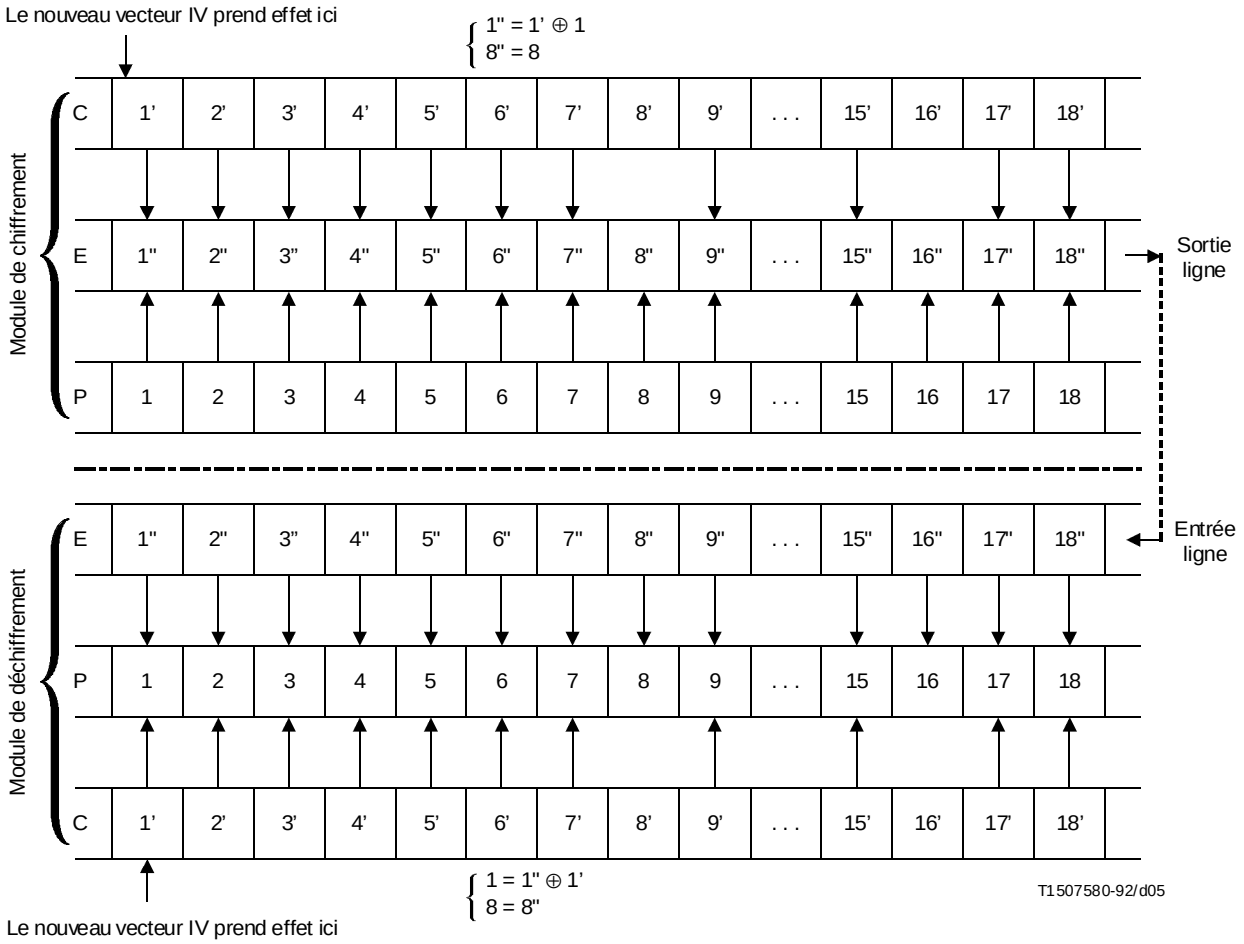

**Numérotation des bits et bits non chiffrés d'une multitrame sur 2 canaux B**




Production d'une suite chiffrante à partir d'un nouveau vecteur IV




Chiffrement série




P Texte clair
C Train chiffré
E Texte chiffré

# Appendice II

## Procédure relative à l'établissement d'une communication audiovisuelle protégée

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

La mise en œuvre des Recommandations de la série H (H.233, H.234, etc.) permet de protéger une communication audiovisuelle. Etant donné que les éléments des procédures de communication sont définis dans plusieurs Recommandations, cet appendice regroupe différents exemples de procédures et indique les Recommandations auxquelles il est fait référence.

On peut envisager les deux scénarios suivants pour protéger une communication audiovisuelle:

1) la communication est déjà en cours lorsque les participants décident de commencer le chiffrement;

2) les participants décident de commencer le chiffrement avant d'établir la communication et se transmettent cette décision par des moyens externes si bien qu'aucune communication audiovisuelle ne débute avant la mise en œuvre effective du processus de confidentialité.

Les Tableaux II.1 et II.2 ci-après décrivent le processus de protection dans chacun des deux cas. L'ordre chronologique dans lequel apparaissent les procédures correspond à l'utilisation de la structure de Diffie-Hellman étendue pour la distribution des clés.

Lorsque une communication protégée est invoquée, il convient d'accorder une attention particulière à la synchronisation du chiffrement réel des signaux audiovisuels. Bien qu'il n'existe aucune méthode normalisée, la conception des terminaux doit permettre de prévoir la marge de plusieurs secondes nécessaire à l'établissement d'une communication protégée.

Cela peut consister à autoriser le chiffrement de la communication jusqu'au moment où les signaux chiffrés sont disponibles (scénario 1 ci-dessus), ou bien à prévoir la suppression des signaux audiovisuels tant que les signaux chiffrés ne sont pas disponibles (scénario 2 ci-dessus). Dans les deux cas, l'état du chiffrement doit être indiqué clairement aux utilisateurs à l'aide d'un voyant lumineux ou d'un autre dispositif.

TABLEAU II.1/H.233

**Décision relative au chiffrement prise après l'établissement de la communication**

| Ordre chrono-logique | Procédure | Message | Canal utilisé | Référence et Notes |
|---|---|---|---|---|
| 1 | Etablissement de la communication | BC/LLC/HLC | Canal D | Rec. Q.939 |
| 2 | Pas de codage des signaux audio; envoyer un message AIM en cas de suppression audio; indiquer à l'utilisateur la suppression des signaux audio à l'entrée; indiquer l'absence de chiffrement des signaux audio à la sortie s'il n'y a pas de suppression | AIM | BAS | Rec. H.230 |
| 3 | Echange de codes de possibilité ECS (Note 1) | Possibilité de chiffrement | BAS | Rec. H.242 |
| 4 | Activation du canal ECS (Note 1) | Chiffrement en service | BAS | Rec. H.242 |
| 5 | Identification des algorithmes de chiffrement disponibles | P8 | Rec. H.233 | |
| 6 | Identification des méthodes de gestion de clés communes | P0 | ECS(SE) | Rec. H.234 |
| 7 | Une fois connue la méthode de gestion des clés, choisir l'algorithme de chiffrement | – | (Canal local) | |
| 8 | Transmettre l'algorithme choisi à la fois pour l'échange des clés de session et la communication audiovisuelle | P9 | | Rec. H.233 (Note 2) |

TABLEAU II.1/H.233 *(fin)*

**Décision relative au chiffrement prise après l'établissement de la communication**

| Ordre chrono-logique | Procédure | Message | Canal utilisé | Référence et Notes |
|---|---|---|---|---|
| 9 | Echange des éléments suivants: nombre premier, racine primitive et résultat intermédiaire | P3, P4 | ECS(SE) | Rec. H.234 |
| 10 | Détermination de la *clé*; r1, r2 et R12 | – | (Canal local) | Rec. H.234 |
| 11 | Présentation du code de vérification à 64 bits sous la forme de chiffres hexadécimaux | (Canal local) | (Canal local) | Rec. H.234 |
| 12 | Effectuer la présentation directe (point à point) ou l'envoi par le pont MCU (multipoint) des informations codées correspondant au code de vérification à 64 bits – en cas de suppression audio, la vérification directe peut se faire après le début du chiffrement | 16 chiffres hexadécimaux | Canal principal (point à point) ou ECS (multipoint) | Rec. H.234 |
| 13 | Transmission du vecteur d'initialisation IV et d'un nombre aléatoire chiffré sur 4N bits | P6 | ECS(SE) | Rec. H.234 (Note 3) |
| 14 | Début du chiffrement et transmission du vecteur d'initialisation IV | A et IV sur le canal ECS | ECS(IV) | Rec. H.233 |
| 15 | Indiquer le chiffrement à la sortie; désactiver la suppression audio si le mode n'est pas automatique; procéder à la vérification directe, le cas échéant, si elle n'a pas encore été effectuée | AIA, 16 chiffres hexadécimaux | (Canal local) BAS Canal principal | Rec. H.230, Rec. H.234 |
| 16 | Chiffrement de la communication audiovisuelle | Audio, vidéo, etc. | Canal principal | |
| 17 | Suppression des signaux audio et vidéo | AIM, VIS | BAS | Rec. H.230 |
| 18 | Arrêt du chiffrement | A sur le canal ECS | ECS(IV) | Rec. H.233 |
| 19 | Désactivation du canal ECS (Note 4) | Chiffrement hors service | BAS | Rec. H.242 |
| 20 | Libération de la communication | – | Canal D | Rec. Q.939 |

NOTES

1 Conformément aux procédures d'initialisation de mode et de phase d'établissement de modes compatibles définies dans la Recommandation H.242.

2 L'algorithme et le mode de chiffrement décrits dans l'Annexe A sont communément utilisés pour l'échange des clés de session et pour les communications audiovisuelles.

3 Le numéro aléatoire à 4N bits est chiffré à l'aide de l'algorithme de chiffrement choisi dans le cadre de la procédure 8; la procédure 10 et la procédure 13 fournissent respectivement la *clé* et le vecteur IV.

4 Conformément aux procédures définies dans la Recommandation H.242 pour la phase de terminaison de la communication.

TABLEAU II.2/H.233

**Décision relative au chiffrement prise avant l'établissement de la communication**

| Ordre chrono-logique | Procédure | Message | Canal utilisé | Référence et Notes |
|---|---|---|---|---|
| 0 | Les deux participants décident de protéger la communication | | Moyens externes | (Note 1) |
| 1 | Etablissement de la communication | BC/LLC/HLC | Canal D | Rec. Q.939 |
| 2 | Suppression des signaux audio et vidéo; indiquer à l'utilisateur si les signaux audio ou vidéo sont supprimés à l'entrée | AIM, VIS | BAS | Rec. H.230 |

TABLEAU II.2/H.233 *(fin)*

**Décision relative au chiffrement prise avant l'établissement de la communication**

| Ordre chrono-logique | Procédure | Message | Canal utilisé | Référence et Notes |
|---|---|---|---|---|
| 3 | Echange de codes de possibilité ECS (Note 2) | Possibilité de chiffrement | BAS | Rec. H.242 |
| 4 | Activation du canal ECS (Note 2) | Chiffrement en service | BAS | Rec. H.242 |
| 5 | Identification des algorithmes de chiffrement disponibles | P8 | ECS(SE) | Rec. H.233 |
| 6 | Identification des méthodes de gestion de clés communes | P0 | ECS(SE) | Rec. H.234 |
| 7 | Une fois connue la méthode de gestion des clés, choisir l'algorithme de chiffrement | – | (Canal local) | |
| 8 | Transmettre l'algorithme choisi à la fois pour l'échange des clés de session et la communication audiovisuelle | P9 | | Rec. H.233 (Note 3) |
| 9 | Echange des éléments suivants: nombre premier, racine primitive et résultat intermédiaire | P3, P4 | ECS(SE) | Rec. H.234 |
| 10 | Détermination de la *clé*; re1, r2 et R12 | – | (Canal local) | Rec. H.234 |
| 11 | Présentation du code de vérification à 64 bits sous la forme de chiffres hexadécimaux | (Canal local) | (Canal local) | Rec. H.234 |
| 12 | (En mode multipoint), envoi par le pont MCU des informations codées correspondant au code de vérification à 64 bits | 16 chiffres hexadécimaux | ECS | Rec. H.234 |
| 13 | Transmission du vecteur d'initialisation IV et d'un nombre aléatoire chiffré sur 4N bits | P6 | ECS(SE) | Rec. H.234 (Note 4) |
| 14 | Début du chiffrement et transmission du vecteur d'initialisation IV | A et IV sur le canal ECS | ECS(IV) | Rec. H.233 |
| 15 | Indiquer le chiffrement à la sortie; désactiver la suppression audio si le mode n'est pas automatique; désactiver la suppression des signaux audio et vidéo; (en mode point à point) présentation directe du code de vérification à 64 bits | AIA, VIA 16 chiffres hexadécimaux | (Canal local) BAS canal principal | Rec. H.230 |
| 16 | Chiffrement de la communication audiovisuelle | Audio, vidéo, etc. | Canal principal | |
| 17 | Suppression des signaux audio et vidéo | AIM, VIS | BAS | Rec. H.230 |
| 18 | Arrêt du chiffrement | A sur le canal ECS | ECS(IV) | Rec. H.233 |
| 19 | Désactivation du canal ECS (Note 5) | Chiffrement hors service | BAS | Rec. H.242 |
| 20 | Libération de la communication | – | Canal D | Rec. Q.939 |

NOTES

1 Hors du champ d'application de la présente Recommandation.

2 Conformément aux procédures d'initialisation de mode et de phase d'établissement de modes compatibles définies dans la Recommandation H.242.

3 L'algorithme et le mode de chiffrement décrits dans l'Annexe A sont communément utilisés pour l'échange des clés de session et pour les communications audiovisuelles.

4 Le numéro aléatoire à 4N bits est chiffré à l'aide de l'algorithme de chiffrement choisi dans le cadre de la procédure 8; la procédure 10 fournit respectivement la *clé* et le vecteur IV.

5 Conformément aux procédures définies dans la Recommandation H.242 pour la phase de terminaison de la communication.