



UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

H.246

Annexe E2
(11/2000)

SÉRIE H: SYSTÈMES AUDIOVISUELS ET
MULTIMÉDIAS

Infrastructure des services audiovisuels – Procédures de
communication

Interfonctionnement des terminaux multimédias de
la série H avec d'autres terminaux multimédias de
la série H et des terminaux vocaux ou en bande
vocale sur le RTGC et le RNIS

**Annexe E2: Interfonctionnement entre le sous-
système application mobile ANSI-41
(Amériques) et les terminaux H.225.0**

Recommandation UIT-T H.246 – Annexe E2

RECOMMANDATIONS UIT-T DE LA SÉRIE H
SYSTÈMES AUDIOVISUELS ET MULTIMÉDIAS

CARACTÉRISTIQUES DES SYSTÈMES VISIOPHONIQUES	H.100–H.199
INFRASTRUCTURE DES SERVICES AUDIOVISUELS	
Généralités	H.200–H.219
Multiplexage et synchronisation en transmission	H.220–H.229
Aspects système	H.230–H.239
Procédures de communication	H.240–H.259
Codage des images vidéo animées	H.260–H.279
Aspects liés aux systèmes	H.280–H.299
SYSTÈMES ET ÉQUIPEMENTS TERMINAUX POUR LES SERVICES AUDIOVISUELS	H.300–H.399
SERVICES COMPLÉMENTAIRES EN MULTIMÉDIA	H.450–H.499
PROCÉDURES DE MOBILITÉ ET DE COLLABORATION	
Aperçu général de la mobilité et de la collaboration, définitions, protocoles et procédures	H.500–H.509
Mobilité pour les systèmes et services multimédias de la série H	H.510–H.519
Applications et services de collaboration multimédia mobile	H.520–H.529
Sécurité pour les systèmes et services multimédias mobiles	H.530–H.539
Sécurité pour les applications et services de collaboration multimédia mobile	H.540–H.549
Procédures d'interfonctionnement de la mobilité	H.550–H.559
Procédures d'interfonctionnement de collaboration multimédia mobile	H.560–H.569

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

Interfonctionnement des terminaux multimédias de la série H avec d'autres terminaux multimédias de la série H et des terminaux vocaux ou en bande vocale sur le RTGC et le RNIS

Annexe E2

Interfonctionnement entre le sous-système application mobile ANSI-41 (Amériques) et les terminaux H.225.0

Résumé

La présente annexe décrit l'interfonctionnement du sous-système application mobile (MAP) ANSI-41 (Etats-Unis) du SS7 nord-américain et des protocoles multimédias H.225.0. Elle spécifie les services de mobilité d'utilisateur au moyen du module d'identification d'utilisateur (H323_UIM) et le mappage qu'une fonction d'interfonctionnement devrait s'effectuer pour permettre à des connexions de s'établir entre réseaux H.323 et réseaux mobiles terrestres publics (RMTP) américains et aux fonctionnalités d'opérer.

Les spécifications détaillées des services de mobilité de l'utilisateur entre les réseaux H.323 et les réseaux mobiles terrestres publics ANSI-41 sont traitées dans le cadre des fonctions suivantes:

- portier AnnexE2_GK: spécifications de la fonction d'interfonctionnement entre le sous-système application mobile ANSI-41 (MAP) et les protocoles H.225.0;
- module H323_UIM: spécifications de la capacité du module UIM (module d'identité d'utilisateur) RMTP ANSI-41 sur un terminal H.323.

La présente annexe s'applique aux versions 4 ou ultérieures des Rec. UIT-T H.323 et H.225.0. Les réalisations conformes à la version 4 peuvent être identifiées par des messages H.225.0 contenant un identificateur **protocollIdentif** = {itu-t (0) recommandation (0) h (8) 2250 version (0) 4}.

Source

L'Annexe E2 de la Recommandation H.246 de l'UIT-T, élaborée par la Commission d'études 16 (2001-2004) de l'UIT, a été approuvée le 17 novembre 2000 selon la procédure définie dans la Résolution 1 de l'AMNT.

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 la 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.

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 avait été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

© UIT 2002

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

TABLE DES MATIÈRES

	Page	
E2.1	Domaine d'application.....	1
E2.2	Définitions.....	2
E2.3	Références normatives	2
	E2.3.1 Références à caractère informatif.....	3
E2.4	Abréviations	3
E2.5	Architecture d'interfonctionnement des réseaux H.323 et RMTP.....	6
	E2.5.1 Nouvelles fonctions de l'architecture d'interfonctionnement des réseaux H.323 et RMTP	7
E2.6	Module d'identification d'utilisateur intégré ANSI-41 au terminal UIMH.323	7
	E2.6.1 Clé A-Key	7
	E2.6.2 Données secrètes communes (SSD, <i>shared secret data</i>)	8
	E2.6.3 Authentification.....	8
	E2.6.4 Hypothèses	8
	E2.6.5 Description	9
	E2.6.6 Génération des données de signature d'authentification et des clés de chiffrement	9
	E2.6.7 Validation et stockage des clés A-Key saisies	11
	E2.6.8 Opération demande aléatoire (ask random)	12
	E2.6.9 Mise à jour des données secrètes communes (SSD)	12
	E2.6.10 Confirmation des données secrètes communes (SSD).....	12
	E2.6.11 Cryptage CMEA des chiffres de données d'un canal vocal	13
	E2.6.12 Actualisation de la valeur COUNTsp.....	14
	E2.6.13 Codes d'état H323_UIM.....	14
E2.7	H323_UIM Management Procédures.....	15
	E2.7.1 Initialisation ANSI-41 (noyau central).....	18
	E2.7.2 Initialisation ANSI-41 H323_UIM	18
	E2.7.3 Fin de session par l'UIM	18
	E2.7.4 Procédures relatives aux informations NAM H323_UIM	19
	E2.7.5 Procédures H323_UIM relatives à l'authentification	20
	E2.7.6 Procédures UIM relatives à la sélection de réseau (<i>UIM network selection related procedures</i>)	20
	E2.7.7 Procédures associées à l'interface d'utilisateur H323_UIM	20
	E2.7.8 Procédures relatives au séquençement H323_UIM (<i>H323_UIM timing related procedures</i>)	21
	E2.7.9 Procédures relatives à l'enregistrement H323_UIM (<i>H323_UIM registration related procedures</i>)	21
	E2.7.10 Procédures additionnelles H323_UIM (<i>H323_UIM additional procedures</i>)	21
	E2.7.11 Procédures de gestion de mise à jour du terminal H323_UIM	21

	Page
E2.8 Portier – Annexe E2_GK avec fonction d'interfonctionnement (RMTP) et portier H.323	22
E2.8.1 Mappage des messages MAP du RMTP ANSI-41 en messages H.225.0.....	24
E2.9 Procédures de gestion de mobilité et de gestion des communications relatives au portier AnnexE2_GK	25
E2.9.1 Addition de paramètres de mobilité et de procédures aux messages RAS H.225	25
E2.9.2 Aspect sécurité relatif au module d'identité d'utilisateur de mobile H.323 (UIM)	25
E2.9.3 Mode étranger H.323.....	25
E2.9.4 Données d'abonné.....	25
E2.10 Enregistrement et authentification automatique.....	26
E2.10.1 Adressage	26
E2.10.2 Authentification, cryptage, secret des conversations	26
E2.11 Mobilité fondée sur le module UIM.....	26
E2.11.1 Utilisation des identificateurs d'équipement mobile	27
E2.11.2 Prise en charge du mode ANSI-41	28
E2.11.3 Remise automatique des appels.....	29
E2.11.4 Commande des caractéristiques des services complémentaires.....	29
E2.11.5 Prise en charge du mode H.323 étranger.....	29
E2.11.6 Mappage des codes de fonctionnalité.....	29
E2.11.7 Interdiction d'appel et interdiction d'appel déterminée par l'opérateur	31
E2.11.8 Interdiction des appels sortants (service complémentaire et interdiction déterminée par l'opérateur).....	31
E2.11.9 Interdiction des appels entrants (service complémentaire et interdiction déterminée par l'opérateur).....	31
E2.11.10 Interdiction de la mobilité déterminée par l'opérateur.....	31
E2.11.11 Enregistrement et activation.....	32
E2.11.12 Acheminement optimal dans le cas du renvoi d'appel tardif.....	32
E2.11.13 Prise en charge du téléservice de messagerie brève (SMS)	32
E2.11.14 Notification de message en attente.....	32
E2.11.15 Service d'urgence.....	32
E2.11.16 Services de localisation	33
E2.11.17 Services WAP.....	33
E2.12 Descriptions d'étape 2 de l'interfonctionnement et des fonctionnalités des terminaux H323_UIM du RMTP ANSI-41	33
E2.12.1 Modèle opérationnel et flux de messages	33
E2.12.2 Enregistrement et authentification des flux de messages d'un terminal H323_UIM	35
E2.12.3 Authentification d'un abonné au moyen du numéro PIN pour invoquer les flux de messages associés aux services.....	41

	Page
E2.12.4 Extinction du terminal H323_UIM	43
E2.12.5 Mise sous tension du terminal H323_UIM	43
E2.13 Remise automatique des appels.....	43
E2.13.1 Remise d'un appel à un abonné ANSI-41 se déplaçant dans un réseau H.323	43
E2.13.2 Echec de remise d'appel à un abonné ANSI-41 se déplaçant dans un réseau H.323	44
E2.14 Service de messagerie brève ANSI-136 mappé en message de commande de service de l'Annexe K H.323: réussite.....	46
E2.14.1 Traitement des erreurs à la réception d'un message Forward Short Message dans le portier H.246 AnnexE2_GK	47
E2.14.2 Mappage d'un message de commande de service H.323 Annexe K en un message ANSI-136 SMDPP.....	47
E2.15 Notification de message en attente.....	48
E2.15.1 Terminal H323_UIM en mode ANSI-41	48
E2.15.2 Notification MWN via un message Qualification Directive ANSI-41 mappé en une notification MWN H.450.7.....	49
E2.15.3 Codage de Qualification Directive avec l'information MWN.....	50

Interfonctionnement des terminaux multimédias de la série H avec d'autres terminaux multimédias de la série H et des terminaux vocaux ou en bande vocale sur le RTGC et le RNIS

Annexe E2

Interfonctionnement entre le sous-système application mobile ANSI-41 (Amériques) et les terminaux H.225.0

E2.1 Domaine d'application

La présente annexe a pour objet de spécifier la fonction d'interfonctionnement (IWF, *interworking function*) entre les réseaux mobiles terrestres publics (RMTP) de deuxième génération et les réseaux H.323. La fonction IWF assure le mappage du sous-système application mobile (MAP, *mobile application part*) du RMTP ANSI-41 avec les messages H.323 et aussi avec certains nouveaux messages, procédures et paramètres relatifs aux réseaux H.323. La présente annexe n'exige pas de modification des réseaux mobiles.

La présente annexe a en outre pour objet de préciser comment le module d'identification de l'utilisateur mobile (UIM, *user identification module*) ou l'information d'identification de l'utilisateur peuvent être utilisés dans un terminal H.323. La mise en œuvre du module UIM permet à un terminal H.323 d'apparaître comme un terminal RMTP sur le réseau H.323. La fonction d'interfonctionnement (IWF) du RMTP entre des réseaux H.323 et RMTP ANSI-41 permet à l'utilisateur d'envoyer et de recevoir des appels vocaux et de notification de messages vocaux, ainsi que d'envoyer et de recevoir des messages brefs, etc. Nous nous limiterons ici à étudier les sujets suivants:

- Circuits IMT/RNIS_PRI/CAS G.711 entre réseaux RMTP ANSI-41 et H.323. L'utilisation des codecs de téléphonie mobile de bout en bout (c'est-à-dire EIA/TIA-136-Rév.A, etc.) est à étudier.
- Fonctionnement lorsque le terminal H.323 dispose d'un module UIM ou d'une information d'identification de l'utilisateur. Si le terminal H.323 ne dispose pas de module UIM ou d'information d'identification de l'utilisateur, les principes suivants seront appliqués:
 - un terminal H.323 non équipé d'un module UIM est un terminal H.323 normal. Les appels en provenance d'un terminal H.323 normal à destination de numéros de téléphone sur le RMTP ou le RTPC via une passerelle H.323 associée seront considérés comme des appels H.323 normaux dans le réseau pour données par paquets;
 - les appels en provenance du RMTP ne peuvent pas être remis à un terminal H.323, sauf si le numéro téléphonique mobile est associé au terminal H.323 normal.

Deux fonctions essentielles sont assurées par les réseaux mobiles à savoir la *gestion de la mobilité* et la *gestion des communications*.

La gestion de la mobilité permet aux réseaux mobiles d'actualiser la position et le statut de l'abonné mobile afin d'assurer des services de télécommunications mobiles à l'utilisateur final.

La gestion des communications permet aux réseaux mobiles d'assurer la commande d'appel et d'offrir des services complémentaires, des services de messagerie brève et des services de données. Les systèmes ANSI-41 et PDC offrent des capacités de réseau transparentes entre équipements de réseau provenant de différents constructeurs. En l'absence de normalisation des systèmes ANSI-41 Rév.D, il sera difficile pour un fournisseur de services cellulaires/de communications personnelles (PCS, *personal communication services*) d'assurer la mobilité entre les différents systèmes. La norme ANSI-41 Rév.D spécifie les interfaces et les procédures normalisées permettant d'assurer:

- le départ d'appel, la terminaison d'appel, les services complémentaires, les services de messagerie brève et les services de données en n'importe quel point du réseau hertzien.
- la transparence des abonnements entre réseaux.
- la facilité d'utilisation.
- l'accès sécurisé aux services:
 - prévention des fraudes;
 - authentification et confidentialité.
- capacité de facturation, capacité d'exploitation, de gestion et de maintenance.

E2.2 Définitions

La présente annexe définit les termes suivantes:

E2.2.1 H323_UIM: terminal H.323 avec module d'identification d'utilisateur ou information d'identification d'utilisateur d'un réseau mobile terrestre public ANSI-41 courant.

E2.2.2 AnnexE2_GK: portier H.323 avec fonction d'interfonctionnement RMTP ANSI-41 connu sous l'appellation AnnexE2_GK.

E2.3 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.

Toutes les références normatives indiquées dans la Rec. UIT-T H.323, version 3 (1999), dans la Rec. UIT-T H.225.0, version 2 (1998) et dans la Rec. UIT-T H.245 s'appliquent ici:

- Recommandation UIT-T H.225.0, version 2 (1998), *Protocoles de signalisation d'appel et mise en paquets d'un train multimédia pour des systèmes de communication multimédia en mode paquet.*
- Recommandation UIT-T H.235 (1998), *Sécurité et cryptage des terminaux multimédias de la série H (terminaux H.323 et autres terminaux de type H.245).*
- Recommandation UIT-T H.323, version 2 (1998), *Systèmes de communication multimédia en mode paquet.*
- Recommandation UIT-T H.323, Annexe K (2000), *Voie de transport par protocole HTTP des signaux de commande de services dans les réseaux H.323.*
- Recommandation UIT-T X.680 (1997), *Technologies de l'information – Notation de syntaxe abstraite numéro 1: spécification de la notation de base.*

- Recommandation UIT-T X.691 (1997), *Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage compact*.
- ANSI/TIA/EIA-664-1996, *Cellular Features Description (Description des caractéristiques des systèmes cellulaires)*.
- ETSI GSM 09.02 (1990-1991), *Mobile Application Part (MAP) specifications*.
- ANSI/TIA/EIA-41D-97, *Cellular Radiotelecommunications Intersystem Operations (Interopérabilité des systèmes de radiocommunications cellulaires)*.
- TTC JJ.70.10, *Mobile Application Part (MAP) signalling system of Digital Mobile Communications Network Inter-node Interface (DMNI) for PDC [Système de signalisation du sous-système application mobile (MAP) de l'interface entre nœuds de réseau de communication mobile numérique (DMNI) pour réseaux PDC]*.
- ANSI T1.707-1998, *Requirements for a User Identity Module (Spécification d'un module d'identité d'utilisateur pour les services de communications personnelles)*.
- GSM 11.11 (1995), *Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module – Mobile Equipment (SIM-ME) Interface [Système de communication cellulaire numérique (Phase 2+); Spécification de l'interface module d'identité d'utilisateur – Equipement mobile (SIM-ME)]*.
- TSB50 (1993), *User Interface for Authentication Key Entry [Interface utilisateur pour la saisie de la clé d'authentification]*.
- ANSI TIA/EIA-136-A (currently out for ballot), *TDMA/Cellular/PCS – Radio Interface – Mobile Station – Base Station Compatibility Standard [Interface hertzienne – Station mobile – Norme de compatibilité de station de base (actuellement en procédure de vote)]*.
- TIA/EIA-136-510-A (currently out for ballot), *Authentication, Encryption of Signalling Information/User Data and Privacy [Authentification, cryptage de l'information de signalisation/données d'utilisateur et secret (actuellement en procédure de vote)]*.
- TIA/EIA-136-511, *Messages Subject to Encryption (Messages faisant l'objet d'un cryptage)*.

E2.3.1 Références à caractère informatif

- EIA/TIA/553-A (currently out for ballot), *Mobile Station – Land Station Compatibility Specification [Spécification de la compatibilité station mobile – Station terrestre (soumis au vote)]*.
- *Common Cryptographic Algorithms*, Revision C (1998), An EAR-controlled document subject to restricted distribution. Document EAR à diffusion restreinte. Contacter la Telecommunications Industry Association, Arlington, VA (USA).
- *Interface Specification for Common Cryptographic Algorithms*, Revision C (1998), An EAR-controlled document subject to restricted distribution. Document EAR à diffusion restreinte. Contacter la Telecommunications Industry Association, Arlington, VA (USA).

E2.4 Abréviations

La présente annexe utilise les abréviations suivantes:

ADN	numéro abrégé (<i>abbreviated dialling number</i>)
ANSI-41	spécifications des réseaux mobiles de l'institut national américain de normalisation – (Spéc 41) (<i>american National Standards Institute Mobile Networks specifications – 41</i>)
AuC/AC	centre d'authentification (<i>authentication centre</i>)

BSC	contrôleur de station de base (<i>base station controller</i>)
BTS	station de base émettrice-réceptrice (<i>base trans-receiver station</i>)
CAVE	authentification et cryptage de la parole pour systèmes cellulaires (<i>cellular authentication and voice encryption</i>)
CDMA-2000	accès multiple par répartition de code – 2000 (<i>Code-division multiple access – 2000</i>)
CHV1	vérification du détenteur de carte 1 (<i>card holder verification 1</i>)
CHV2	vérification du détenteur de carte 2 (<i>card holder verification 2</i>)
EDGE	débits binaires améliorés pour l'évolution des systèmes GSM (<i>enhanced data rates for GSM evolution</i>)
EF	fichiers élémentaires (<i>elementary files</i>)
EIR	registre d'identité d'équipement (<i>equipment identification register</i>)
ESN	numéro de série électronique (<i>electronic serial number</i>)
GMSC	centre de commutation mobile de portier (<i>gateway mobile switching centre</i>)
GPRS	service général de radiocommunication en mode paquet (<i>general packet radio service</i>)
GSM	système mondial de communications mobiles (<i>global system for mobile communications</i>)
H323_UIM	module d'identification d'utilisateur H.323 (<i>H.323 user identification module</i>)
HLPI	indicateur de protocole de couche supérieure (<i>higher layer protocol indicator</i>)
HLR	table de localisation de rattachement (<i>home location register</i>)
HPLMN	RMTP de rattachement (<i>home public land mobile network</i>)
IK	clé d'intégrité (<i>integrity key</i>)
IMEI	identité internationale d'équipement mobile (<i>international mobile equipment identity</i>)
IMSI	identité internationale d'abonné mobile (<i>international mobile subscriber identity</i>)
IMT-2000	télécommunications mobiles internationales (<i>international mobile telecommunications 2000</i>) – appellation donnée au Groupe UIT chargé de la normalisation des systèmes hertziens de troisième génération
IRDB	base de données d'itinérance intelligente (<i>intelligent roaming database</i>)
ISUP	sous-système utilisateur RNIS (<i>ISDN user part</i>)
MAP	sous-système application mobile (<i>mobile application part</i>)
MC	centre de messagerie ANSI-136 (pour le service SMS) (<i>[ANSI-136 message centre (for SMS)]</i>)
MDN	numéro d'annuaire du mobile (<i>mobile directory number</i>)
ME	équipement mobile (<i>mobile equipment</i>)
MGC	contrôleur de passerelle média (<i>media gateway controller</i>)
MGW	passerelle média (<i>media gateway</i>)
MIN	numéro d'identification du mobile (<i>mobile identification number</i>)
MO	au départ du mobile (<i>mobile originated</i>)

MS	station mobile (<i>mobile station</i>)
MSC	centre de commutation de mobile (<i>mobile switching centre</i>)
MSCIN	numéro d'identification de centre MSC (<i>MSC identification number</i>)
MSID	identité de la station mobile (<i>mobile station identity</i>)
MSISDN	numéro RNIS de l'abonné mobile (<i>mobile subscriber ISDN number</i>)
MSRN	numéro de routage de station mobile (<i>mobile station routing number</i>)
MT	se terminant sur un mobile (<i>mobile terminated</i>)
MWN	notification de message en attente (<i>message waiting notification</i>)
NAM	module d'assignation numérique (<i>numeric assignment module</i>)
NNI	interface réseau-réseau (<i>network-to-network interface</i>)
NSDB	base de données de sélection de réseau (<i>network selection database</i>)
ODB	interdiction déterminée par l'opérateur (<i>operator determined barring</i>)
OTA	activation hertzienne (<i>over-the-air activation</i>)
PCS	service de communication personnelle (<i>personal communication service</i>)
PDC	type de réseau numérique essentiellement utilisé au Japon (<i>personal digital cellular</i>)
PDU	unité de données en mode paquet (<i>packet data unit</i>)
PHS	système de téléphonie personnelle – essentiellement utilisé au Japon (<i>personal handy phone system</i>)
PIN	numéro d'identification personnel (<i>personal identification number</i>)
PRI	interface au débit primaire (<i>primary rate interface</i>)
PRN	fournir le numéro d'itinérance (<i>provide roaming number</i>)
PSAP	point d'accès aux services de sécurité publique (<i>public safety access point</i>)
RMTP	réseau mobile terrestre public
RNIS	réseau numérique à intégration de services
RDCP	réseau de données à commutation de paquets
RTPC	réseau téléphonique public à commutation
SESN	numéro de série électronique du module SIM (<i>SIM electronic serial number</i>)
SGW	passerelle de signalisation (<i>signalling gateway</i>)
SID	identité du système (<i>system identity</i>)
SIM	module d'identité d'abonné (<i>subscriber identity module</i>)
SMDPP	remise de message court point à point (<i>short message delivery point-to-point</i>)
SMS	service de message court (<i>short message service</i>)
SMSC	centre de service de messagerie brève (<i>short message service centre</i>)
SOC	code de l'opérateur du système (<i>system operator code</i>)
SS7	système de signalisation n° 7
STP	point de transfert de signalisation (<i>signalling transfer point</i>)

TCAP	sous système de capacités de transaction (<i>transaction capabilities application part</i>)
TDMA	accès multiple par répartition dans le temps (<i>time division multiple access</i>)
TIA	association des industries de télécommunication (<i>telecommunications Industry Association</i>)
TLDN	numéro d'annuaire associé au lieu temporaire (<i>temporary location directory number</i>)
TMSI	identité temporaire de station mobile (<i>temporary mobile station identity</i>)
TP-FCS	cause d'échec TP (<i>TP failure cause</i>)
TS	serveur de téléservice (<i>teleservice server</i>)
TSAR	segmentation et réassemblage pour les téléservices (<i>teleservice segmentation and reassembly</i>)
UDH	en-tête de données universelle (<i>universal data header</i>)
UIM	module d'identité d'utilisateur (<i>user identity module</i>)
UIT	Union internationale des télécommunications
USIM	module d'identité universelle d'abonné (<i>universal subscriber identity module</i>)
UWCC	consortium communication hertzienne universelle (<i>universal wireless communications consortium</i>)
VLR	registre des positions des visiteurs (<i>visited location register</i>)
VMS	système de messagerie vocale (<i>voice mail system</i>)
VPLMN	RMTP visité (<i>visited public land mobile network</i>)
WAP	protocole d'applications hertziennes (<i>wireless application protocol</i>)
W-CDMA	CDMA à large bande (<i>wideband code-division multiple access</i>)

E2.5 Architecture d'interfonctionnement des réseaux H.323 et RMTP

La présente annexe spécifie uniquement les services, procédures, messages de protocole, etc. qui sont obligatoires pour l'implémentation mise en œuvre d'une passerelle mobile H.323 (AnnexE2_GK) et de points d'extrémité mobiles H.323 (H323_uim Terminal) – ce qui correspond à un sous-ensemble de la fonctionnalité optionnelle d'un des systèmes définis dans la version 4 (2000) de la Rec. UIT-T H.323.

Toutes les autres fonctionnalités mobiles (optionnelles) spécifiées dans la version 4 de la Rec. UIT-T H.323 sont, par définition, optionnelles, et leur mise en œuvre dans un équipement mobile H.323 est laissée entièrement à l'appréciation du fabricant.

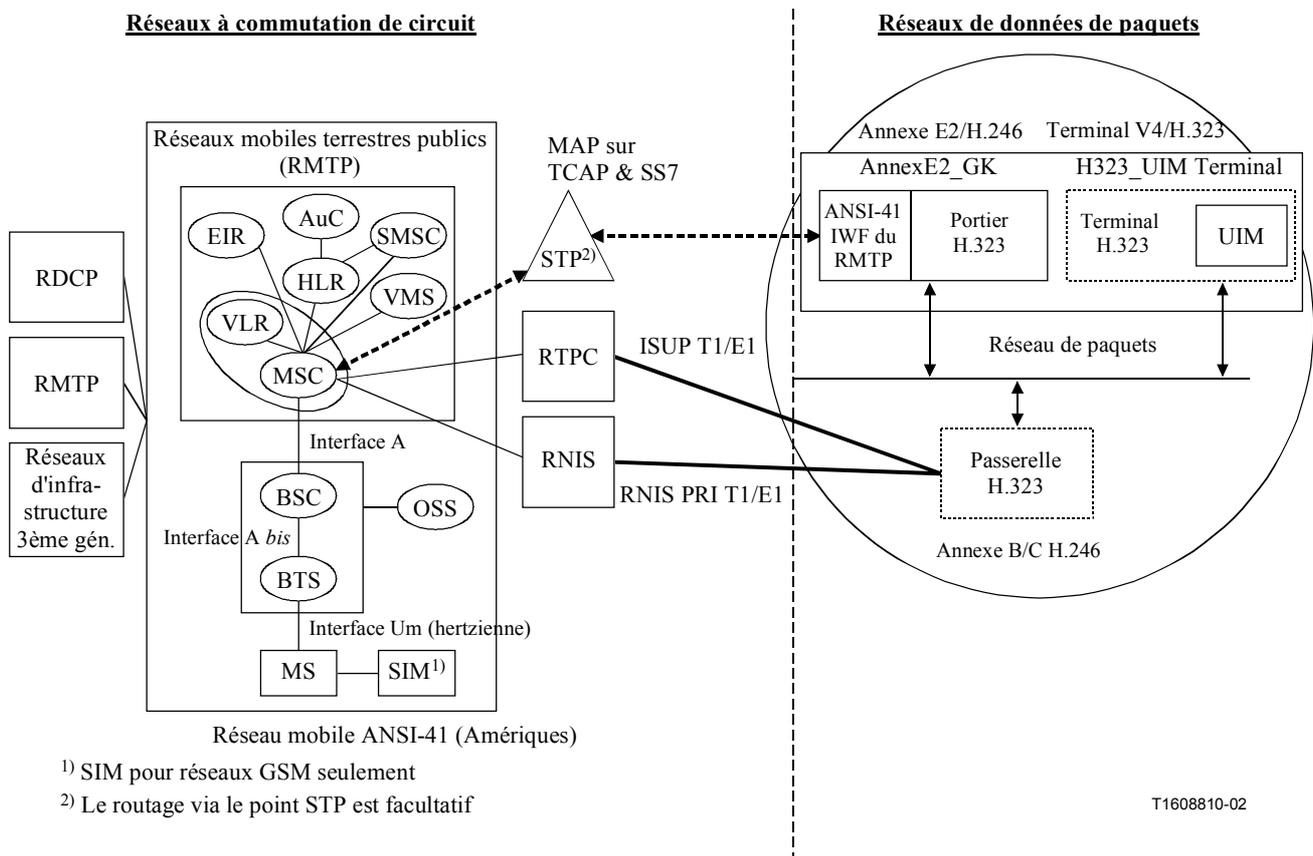


Figure E2.1/H.246 – Architecture d'interfonctionnement des réseaux H.323 et RMTP ANSI-41

E2.5.1 Nouvelles fonctions de l'architecture d'interfonctionnement des réseaux H.323 et RMTP

Les paragraphes qui suivent décrivent les fonctions des diverses composantes d'un réseau E2/H.246 (voir Figure E2.1).

- Un terminal UIM H.323 contient un module d'identification d'utilisateur (UIM) ANSI-41 ou l'information d'identification d'utilisateur prévue dans un réseau mobile ANSI-41.
- Une passerelle AnnexE2_GK est une nouvelle fonction d'interfonctionnement entre réseaux H.323 et RMTP ANSI-41.

E2.6 Module d'identification d'utilisateur intégré ANSI-41 au terminal UIM H.323

Un terminal H.323 doit partager et présenter l'identité de l'abonné utilisée dans le RMTP considéré ANSI-41 avec lequel l'interfonctionnement est souhaité. Ce terminal peut ainsi donner l'identité sous laquelle l'abonné doit s'enregistrer dans le RMTP ANSI-41 et pouvoir accéder aux services de mobilité d'utilisateur.

Il convient de noter que dans le futur, ces identités devront être harmonisées avec le module d'identité universelle d'abonné (USIM, *universal subscriber identity module*) proposé par les groupes chargés de la normalisation des systèmes de la troisième génération.

E2.6.1 Clé A-Key

Seul l'algorithme utilisé pour la génération des clés a accès à la clé A-Key. Cette clé peut être programmée dans le module UIM directement par le fournisseur du service ou au moyen d'une procédure hertzienne spécifique. Cette clé n'est pas accessible à l'équipement mobile; par conséquent la méthode de stockage sur le module UIM n'est pas spécifiée dans la présente annexe.

Une procédure de saisie manuelle de la clé A-Key doit être prévue au moyen du clavier et du dispositif d'affichage de l'équipement mobile. Cette procédure doit utiliser une série normalisée de frappe et, dans les autres cas, être cohérente avec les procédures définies dans la publication TIA/EIA Telecommunications Systems Bulletin TSB-50 User Interface for Authentication Key Entry. La commande UIM "A-KEY_VALIDATION" est utilisée pour mémoriser la clé A-Key dans le module UIM.

Après saisie de la clé d'authentification, celle-ci ne doit pas, en aucun cas et dans aucun mode de fonctionnement, être affichée sur une station mobile ou tout accessoire associé à la station mobile.

E2.6.2 Données secrètes communes (SSD, *shared secret data*)

Les données secrètes communes ne sont accessibles qu'aux fonctions d'authentification et de génération de clé. Les données SSD ne sont pas accessibles à l'équipement mobile et par conséquent la méthode de stockage sur le module UIM n'est pas spécifiée dans la présente annexe.

E2.6.3 Authentification

L'algorithme d'authentification CAVE, selon les références ci-dessous, doit être implémenté sur le module UIM et disposer de l'interface suivante avec le terminal H.323. Toutes ces fonctions ne s'appliquent qu'au EIA/TIA-553 directory 5F40. Ce fichier de données (DF, *data file*) est élargi afin d'inclure des fichiers élémentaires et les procédures permettant au terminal H323_UIM ANSI-41 de fonctionner.

E2.6.4 Hypothèses

- Les structures de données suivantes, toutes les données d'entrée de l'algorithme CAVE, sont dans le terminal H323_UIM:
 - clé A-Key – Uniquement accessible par l'algorithme CAVE. Peut être programmée sur le clavier du terminal H323_UIM ou par voie hertzienne;
 - données secrètes communes (SSD_A, SSD_B) – auxquelles uniquement l'algorithme CAVE a accès;
 - COUNTsp – Accessible au terminal H323_UIM;
 - numéro d'identification du mobile (MIN) – Accessible au terminal H323_UIM;
 - RANDBS – Calculé dans le module UIM, puis transmis au terminal H323_UIM pour transfert vers le système;
 - numéro de série électronique du module SIM (S-ESN, *SIM electronic serial number*).
- Les structures de données suivantes, toutes les données d'entrée vers l'algorithme CAVE, se trouvent dans la mémoire du terminal H323_UIM:
 - numéro de série électronique (ESN);
 - RAND (valeurs combinées de Random Challenge A et B, reçues dans les messages Global Action);
 - les derniers chiffres composés;
 - RANDU;
 - AUTHBS (envoyées par le système);
 - RANDSeed.
- le cryptage des données de signalisation de la signalisation RAS est pris en charge par le module UIM. Cette fonction peut être également exécutée dans le terminal H323_UIM;
- le module UIM déclenche la génération des clés utilisées dans toutes les procédures de chiffrement au niveau du terminal ANSI-41 H323_UIM. Le trafic à chiffrer peut inclure de la voix numérisée, des messages brefs et des données de signalisation;

- le terminal H323_UIM effectuera un certain traitement des clés qui peuvent être nécessaires pour les procédures (EPE, *enhanced privacy and encryption*);
- le terminal H323_UIM acceptera l'introduction manuelle de la clé A-Key dans le terminal H.323, comme cela est fait dans les mobiles ANSI-136;
- on utilisera le protocole de transmission T = 0;
- l'exécution des opérations UIM dépend du contexte de la première sélection de l'annuaire EIA/TIA-553 (5F40).

E2.6.5 Description

Il est nécessaire de disposer de six interfaces avec l'algorithme CAVE et des domaines de données secrètes, comme indiqué ci-dessous:

- génération des données de signature d'authentification et génération des clés de chiffrement;
- validation et mémorisation des clés A-Key introduites;
- demande d'opération aléatoire (génère le RANDBS);
- mise à jour des données secrètes partagées (génère les valeurs SSD_A_NEW, SSD_B_NEW et AUTHBS);
- confirmation des données secrètes communes (mise à jour des valeurs SSD);
- cryptage CMEA des chiffres de données de canal vocal.

En outre, certaines commandes sont définies pour la manipulation de la valeur COUNTsp.

NOTE 1 – Pour chaque opération, le code d'état normal attendu (c'est-à-dire celui qui correspond à une réussite) est listé dans la description du mot d'état. On peut trouver dans les codes d'état UIM une liste des codes possibles qui s'appliquent à toutes les opérations.

NOTE 2 – La phrase "User H323_UIM Terminal ESN (= "00")" dans les opérations ci-dessus est obsolète, mais elle est conservée pour assurer la rétrocompatibilité avec les anciens équipements. Cet octet est mis à "00" dans la présente annexe. Le paramètre de quatre octets qui est utilisé par le module UIM pour les calculs doit être mis à la valeur du champ ESN du terminal H323_UIM si le "usage indicator" (indicateur d'utilisation) impose au module UIM d'utiliser le numéro ESN du terminal H323_UIM. Si "cet indicateur impose au module UIM d'utiliser son numéro S_ESN, le numéro S_ESN stocké de manière interne doit être utilisé. Dans ce dernier cas, le paramètre de quatre octets transmis par le terminal H323_UIM ne doit pas être utilisé comme entrée pour les calculs dans ces paragraphes.

E2.6.6 Génération des données de signature d'authentification et des clés de chiffrement

Cette opération déclenche une réaction d'authentification et doit être utilisée pendant les enregistrements, les émissions et les terminaisons concernant le terminal H323_UIM ainsi que pour la procédure Unique Challenge-Response. Si le bit 1 de l'octet 0 est positionné à une certaine valeur, le module UIM doit également générer les bits de clé après avoir exécuté la fonction d'authentification. Certains de ces octets de chiffrement peuvent être retournés au terminal H323_UIM pour être utilisés avec des mécanismes de cryptage complémentaires, qui sont localisés dans le terminal H323_UIM. Cette opération nécessite l'introduction des paramètres suivants:

Nom de l'opération: Internal_Authenticate

Class = "A0", INS = "88", P1 = "00", P2 = "00", Lc = "0F"

Codage des octets de données:

Octet 0 *Octet de commande de processus*

- bit 0 0 = RAND, 1 = RANDU
- bit 1 Génération du fanion de bits de clé (0 = Non, 1 = Oui)
- bit 2 Fanion de clé interne

0 = transmet tous les octets de clé générés vers le portable
 1 = charger les huit premiers octets des clés générés de manière interne vers l'UIM, transmet tous les bits de clé restants vers le terminal H323_UIM.

• bits 3-7 non utilisés, réservés à une extension future

Octets 1-4 *Octets 1-4*: RAND (pour les enregistrements, les départs et les terminaisons)
 ou

Octets 1-3: RANDU (procédures uniques de demande-réponse)

Octet 4: = 0 (MIN2 sera rempli par le module UIM)

Octet 5 *Longueur des chiffres*

(en bits, = 0, 4, 8, 12, 16, 20 ou 24, = 4 × nombre de chiffres dans les octets 6-8)

Octets 6-8 = 0,0,0 (pour les enregistrements, les terminaisons, les procédures uniques de demande-réponse)

= derniers chiffres composés, les bits non utilisés sont mis à "0" (pour les départs). Lorsque plus de 6 chiffres sont composés, ce sont les 6 derniers chiffres de la chaîne de départ. Lorsque moins de 6 chiffres sont composés, les bits non utilisés du numéro MIN1 seront remplis par le module UIM.

Octet 9 utilisation du numéro ESN du terminal H323_UIM (= "00")

Octets 10-13 ESN (numéro de série électronique)

Octet 14 *Key_size*

= 0 si le bit 1 de l'octet 0 = 0,

= "08"hex ou "49"hex si ce bit = 1)

Lorsque:

"00"hex = pas de génération de clé

"08"hex = génération de la clé CMEA

"49"hex = génération de la clé CMEA key + une clé VPMASK de 520 bits

Le résultat de cette opération sera:

Octets d'état SW1 (= "9F" en cas de réussite)

SW2 (= "nn" en cas de réussite)

"nn" est égal à 03+Key_size si le bit 2 de l'octet 0

ci dessus = 0, 03+Key_size-08 si ce bit = 1

Nom de l'opération: Get_Response

Class = "A0", INS = "C0", P1 = "00", P2 = "00", Le = "nn"

"nn" est égal à 03+Key_size si le bit 2 de l'octet 0

ci dessus = 0, 03+Key_size-08 si ce bit = 1

Le résultat de cette opération sera:

Octets 0-2 la valeur sur 18-bits de la signature d'authentification (AUTHR/AUTHU).

Octets 3-(n+2) Les octets de chiffrement pour les mécanismes de cryptage (n = Key_size or Key_size-8).

Octets d'état SW1 (= "90" en cas de succès)

SW2 (= "00" en cas de succès)

Les valeurs suivantes sont des exemples concernant cette fonction:

Génération des valeurs d'authentification seulement:

Octet 0

- bit 1 = 0 (il n'est pas nécessaire de générer des clés de chiffrement)
- bit 2 = 0 (pas de clé générée, non applicable)

Octet 14 = 0 (aucune clé de chiffrement n'est communiquée au terminal H323_UIM, signifie que les octets 3-(n+2) dans l'opération Get_Response n'existent pas).

Génération des valeurs d'Authentification et les clés de chiffrement à utiliser avec le CMEA dans le module UIM:

Octet 0

- bit 1 = 1 (il est nécessaire de générer des clés de chiffrement)
- bit 2 = 1 (utiliser les 8 premiers octets des clés de chiffrement générée dans le module UIM)

Octet 14 = 8 (8 octets des clés de chiffrement doivent être générés, signifie que les octets 3-(n+2) de l'opération Get_Response n'existent pas étant donné que tous les octets des clés de chiffrement sont utilisés dans le module UIM).

Génération des valeurs d'Authentification et les clés de chiffrement pour les algorithmes du terminal H323_UIM:

Octet 0

- bit 1 = 1 (il est nécessaire de générer des clés de chiffrement)
- bit 2 = 0 (transmettre toutes les clés générées au terminal H323_UIM)

Octet 14 = n (n octets des clés de chiffrement doivent être générées, signifie que les octets 3-(n+2) de l'opération Get_Response seront transmis au terminal H323_UIM).

NOTE – Un traitement plus poussé des clés de chiffrement sera peut-être nécessaire de la part du terminal H323_UIM Terminal, en cas d'utilisation de certaines méthodes de chiffrement dans les terminaux H323_UIM.

E2.6.7 Validation et stockage des clés A-Key saisies

Lorsqu'il y a saisie manuelle de la clé A-key, celle-ci doit être validée avant son stockage dans le module UIM. Si l'opération réussit, la clé A-key est sauvegardée dans le module UIM et les COUNTsp et les données secrètes communes (SSD) sont remis à zéro. Cette opération exige les paramètres d'entrée suivants:

Nom de l'opération: AKEY_validation

Class = "A0", INS = "86", P1 = "00", P2 = "00", Lc = "12"

Codage des octets de données:

Octets 0-12 chaîne de chiffres d'authentification (premier chiffre du multiplet de plus fort poids de l'octet 0, dernier chiffre du multiplet de plus faible poids de l'octet 12, pour un total de 26 chiffres)

Octet 13 utilisation du numéro ESN du terminal H323_UIM (= "00")

Octets 14-17 ESN

Le résultat de cette opération est le suivant:

Octets d'état SW1 (= "90" en cas de réussite)
SW2 (= "00" en cas de réussite)

E2.6.8 Opération demande aléatoire (ask random)

Cette opération sert à générer la valeur aléatoire RANDBS. Elle doit être exécutée avant la mise à jour des données SSD. Il faut préalablement à cette opération que le terminal H323_UIM génère la valeur RANDSeed. Cette opération exige les paramètres d'entrée suivants:

Nom de l'opération: Ask_Random

Class = "A0", INS = "8A", P1 = "00", P2 = "00", Lc = "04"

Codage des octets de données:

Octets 0-3 RANDSeed

Le résultat de cette opération doit être le suivant:

Octets d'état: SW1 (= "9F" en cas de réussite)

SW2 (= "04" en cas de réussite)

Nom de l'opération: Get_Response

Class = "A0", INS = "C0", P1 = "00", P2 = "00", Le = "04"

Le résultat de cette opération doit être le suivant:

Octets 0-3 RANDBS

Octets d'état: SW1 (= "90" en cas de réussite)

SW2 (= "00" en cas de réussite)

E2.6.9 Mise à jour des données secrètes communes (SSD)

Cette opération est utilisée pour générer les nouvelles données SSD préliminaires (SSD_A_NEW, SSD_B_NEW) et la valeur AUTHBS. L'opération demande aléatoire (ask random task) (voir ci-dessus) doit être exécutée avant cet utilitaire. Cette opération exige les paramètres d'entrée suivants:

Nom de l'opération: Update_SSD

Class = "A0", INS = "84", P1 = "00", P2 = "00", Lc = "0C"

Codage des octets de données:

Octets 0-6 RANDSSD

Octet 7 Utiliser le numéro ESN du terminal H323_UIM (= "00")

Octets 8-11 ESN

Le résultat de cette opération doit être le suivant:

Octets d'état: SW1 (= "90" en cas de réussite, = "98" en cas d'échec)

SW2 (= "00" en cas de réussite, = "04" en cas d'échec)

E2.6.10 Confirmation des données secrètes communes (SSD)

Cette opération est utilisée pour valider les nouvelles données SSD (SSD_A_NEW, SSD_B_NEW) en comparant les valeurs calculées de manière interne de AUTHBS avec les valeurs AUTHBS fournies par le système. S'il y a concordance, les valeurs SSD_A et SSD_B seront actualisées pour correspondre aux nouvelles valeurs de SSD_A_NEW et SSD_B_NEW respectivement. Cette opération exige les paramètres d'entrée suivants:

Nom de l'opération Confirm_SSD

Class = "A0", INS = "82", P1 = "00", P2 = "00", Lc = "03"

Codage des octets de données:

Octets 0-2 AUTHBS

Le résultat de cette opération doit être le suivant:

Octets d'état: SW1 (= "90" en cas de réussite)

 SW2 (= "00" en cas de réussite)

E2.6.11 Cryptage CMEA des chiffres de données d'un canal vocal

Cette opération est utilisée lorsqu'un terminal H323_UIM se trouve raccordé à un canal vocal, pour crypter et décrypter certaines parties de messages numériques transmis vers le portier AnnexE.1_GK. Cela est le cas du message suivant:

- message d'adresse appelée (en réaction à une manœuvre du crochet, jusqu'à 4 octets par mot, 4 mots, 16 octets au total)

Cette opération exige les paramètres d'entrée suivants:

Nom de l'opération: CMEA_encrypt

Class = "A0", INS = "8C", P1 = "00", P2 = "00", Lc = "nn"

("nn" est la valeur en hexadécimal de la longueur des données n)

Codage des octets de données:

Octets 0-(n-1) Les données de l'octet n à coder, longueur maximale = 32 octets.

Le résultat de cette opération doit être le suivant:

Octets d'état: SW1 (= "9F" en cas de réussite)

 SW2 (= "nn" en cas de réussite) ("nn" est la valeur en hexadécimal de la longueur des données n)

Nom de l'opération: Get_Response

Class = "A0", INS = "C0", P1 = "00", P2 = "00", Le = "nn" ("nn" est la valeur en hexadécimal de la longueur des données n)

Le résultat de cette opération est le suivant:

Octets 0-(n-1) valeur de l'octet n, contenant les bits cryptés, taille maximale = 32 octets.

Octets d'état: SW1 (= "90" en cas de réussite)

 SW2 (= "00" en cas de réussite)

Par exemple, cryptage d'une chaîne de 16 octets de manœuvre du combiné se traduirait par la séquence suivante de données en direction/provenance du module UIM:

en direction de l'UIM:

Class = "A0", INS = "8C", P1 = "00", P2 = "00", Lc = "10", Data: d0, d1, d2, ..., d14, d15

en provenance de l'UIM:

SW1 = "9F", SW2 = "10"

en direction de l'UIM:

Class = "A0", INS = "C0", P1 = "00", P2 = "00", Le = "10"

en provenance de l'UIM:

e0, e1, e2, ..., e14, e15, SW1 = "90", SW2 = "00"

E2.6.12 Actualisation de la valeur COUNTsp

COUNTsp est une unité de données de synchronisation qui est renvoyée au système en coordination avec le processus d'authentification du terminal ANSI-41 H323_UIM. Elle peut être actualisée par le système ANSI-41 et AMPS à tout moment lorsque le terminal H323_UIM est actif. Le terminal H323_UIM doit pouvoir extraire et incrémenter COUNTsp.

Extraire le décompte d'appel

Nom de l'opération: Read_Record (Get Call Count)

Class= "A0", INS = "B2", P1 = "00", P2 = "04", Le = "03"

Le résultat de cette opération doit être le suivant:

Octet 0-2 Returned COUNTsp value

Octets d'état: SW1 (= "90" en cas de réussite)

SW2 (= "00" en cas de réussite)

Initialiser le décompte d'appel

Nom de l'opération: Update Record (Set Call Count)

Class = "A0", INS = "DC", P1 = "00", P2 = "03", Lc = "03"

Codage des octets de données:

Octet 0-2 COUNTsp value

Le résultat de cette opération doit être le suivant:

Octets d'état: SW1 (= "90" en cas de réussite)

SW2 (= "00" en cas de réussite)

Actualiser le décompte d'appel

Nom de l'opération: Increase (Increment Call Count)

Class = "A0", INS = "32", P1 = "00", P2 = "00", Lc = "03"

Codage des octets de données:

Octets 0-2 00, 00, 01 (valeur de l'incrément)

Le résultat de cette opération doit être le suivant:

Octets d'état: SW1 (= "9F" en cas de réussite)

SW2 (= "06" en cas de réussite)

Nom de l'opération: Get_Response

Class = "A0", INS = "C0", P1 = "00", P2 = "00", Le = "06"

Le résultat de cette opération doit être le suivant:

Octet 0-2 COUNTsp

Octets 3-5 Valeur qui a été ajoutée

Octets d'état: SW1 (= "90" en cas de réussite)

SW2 (= "00" en cas de réussite)

E2.6.13 Codes d'état H323_UIM

Les codes d'état suivants renvoyés par le module UIM en réponse à l'exécution d'une des opérations spécifiées dans la présente annexe, sont valides. La première valeur hexadécimale est renvoyée dans le mot d'état 1 (SW1: *status word 1*), la seconde dans le mot d'état 2 (SW2: *status word 2*).

Codes de réussite

- 90, 00 code de réussite générique
- 9F, xx réussite, xx octet sont disponibles en lecture via l'opération "Get_Response".

Codes d'erreur

- 92, 40 erreur, problème de mémoire.
- 94, 08 erreur, fichier incohérent avec la commande
- 98, 04 erreur, échec de vérification CHV1 (cardholder verification 1: vérification du détenteur de carte)
- 98, 34 erreur, ordre de séquence des données de mise à jour des données SSD non respecté (doit être utilisé si les commandes de mise à jour SSD Update sont reçues hors séquence).
- 67, xx erreur, paramètre P3 (code ISO) incorrect
- 6B, xx erreur, paramètre P1 ou P2 (code ISO) incorrect
- 6D, xx erreur, code d'instruction inconnu indiqué dans la commande (code ISO)
- 6E, xx erreur, classe d'instruction erroné indiqué dans la commande (code ISO)
- 6F, xx erreur, problème technique sans indication de diagnostic (code ISO)
- 6A, 80 erreur, paramètres incorrects indiqués dans le champ de données

E2.7 H323_UIM Management Procédures

Après l'activation du terminal H323_UIM (voir GSM 11.11, § 4.3.2.) le terminal H323_UIM Terminal suit les procédures d'initialisation ANSI-41 jusque et y compris la demande IMSI Request. Le terminal H323_UIM Terminal tente alors de sélectionner le fichier spécialisé (DF: Dedicated File) DF_{TIA/EIA-41}. Si le fichier DF_{TIA/EIA-41} est présent, le module UIM est du type H.323/ANSI-136 UIM. Dans le cas contraire, n'est pas l'UIM associé au terminal H323_UIM.

Dans le cas d'un module UIM H.323/ANSI-41, le terminal H323_UIM Terminal doit exécuter l'opération Phase ID Request H.323/ANSI-41. Un module UIM H.323/ANSI-41 doit pouvoir prendre en charge des fichiers et des procédures élémentaires définies pour la phase de l'Annexe E2/H.246 dans la phase ID EF de l'UIM H.323-ANSI-41 et pour toute phase précédente définie dans l'Annexe E2/H.246. Le terminal H323_UIM Terminal doit fonctionner au niveau défini par son propre identificateur inférieur Phase ID H.323-ANSI-41 ou par l'identificateur Phase ID H.323-ANSI-41 de l'UIM.

Dans le cadre également de la phase de gestion, le terminal H323_UIM Terminal doit extraire la valeur de l'indicateur de priorité de protocole (*Protocol Priority Indicator*) en exécutant une demande ANSI-Usage Indicator Request. Le terminal H323_UIM Terminal doit ensuite exécuter la demande de code de l'opérateur de rattachement (*home system operator code*) et de code du pays du système mobile (*Mobile Country Code*), qui est nécessaire à l'exécution de tout test de personnalisation, si nécessaire, afin de déterminer si le module UIM courant sera autorisé à fonctionner ou non.

En cas d'échec du test de personnalisation, le terminal H323_UIM Terminal passe à l'état "limited service state" (service limité) sur la base de la valeur de l'indicateur Protocol Priority Indicator, état dans lequel seuls sont possibles les appels d'urgence (voir l'Annexe A.2 du GSM 02.22 et le TIA/EIA-136-123). En cas de réussite du test de personnalisation, le terminal H323_UIM Terminal passe à la session d'initialisation sur la base du type de module UIM.

Ensuite, le terminal H323_UIM Terminal peut demander toutes les informations de données d'utilisateur dont il peut avoir besoin (voir GSM 11.11, § 11.5). Il convient de noter que la lecture de ces information peut avoir lieu avant ce stade, à savoir après lecture des données d'initialisation (ANSI-41).

Les Figures E2.2 et E2.3 ci-après décrivent le processus et n'ont qu'un caractère informationnel.

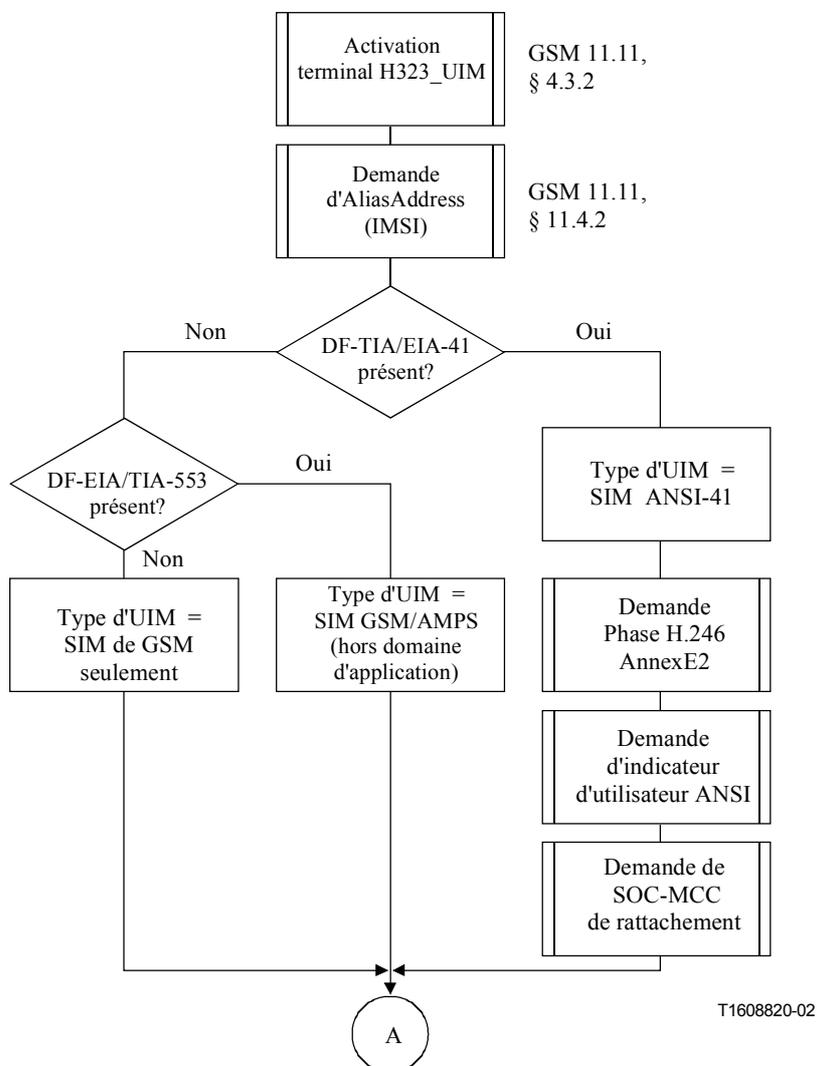
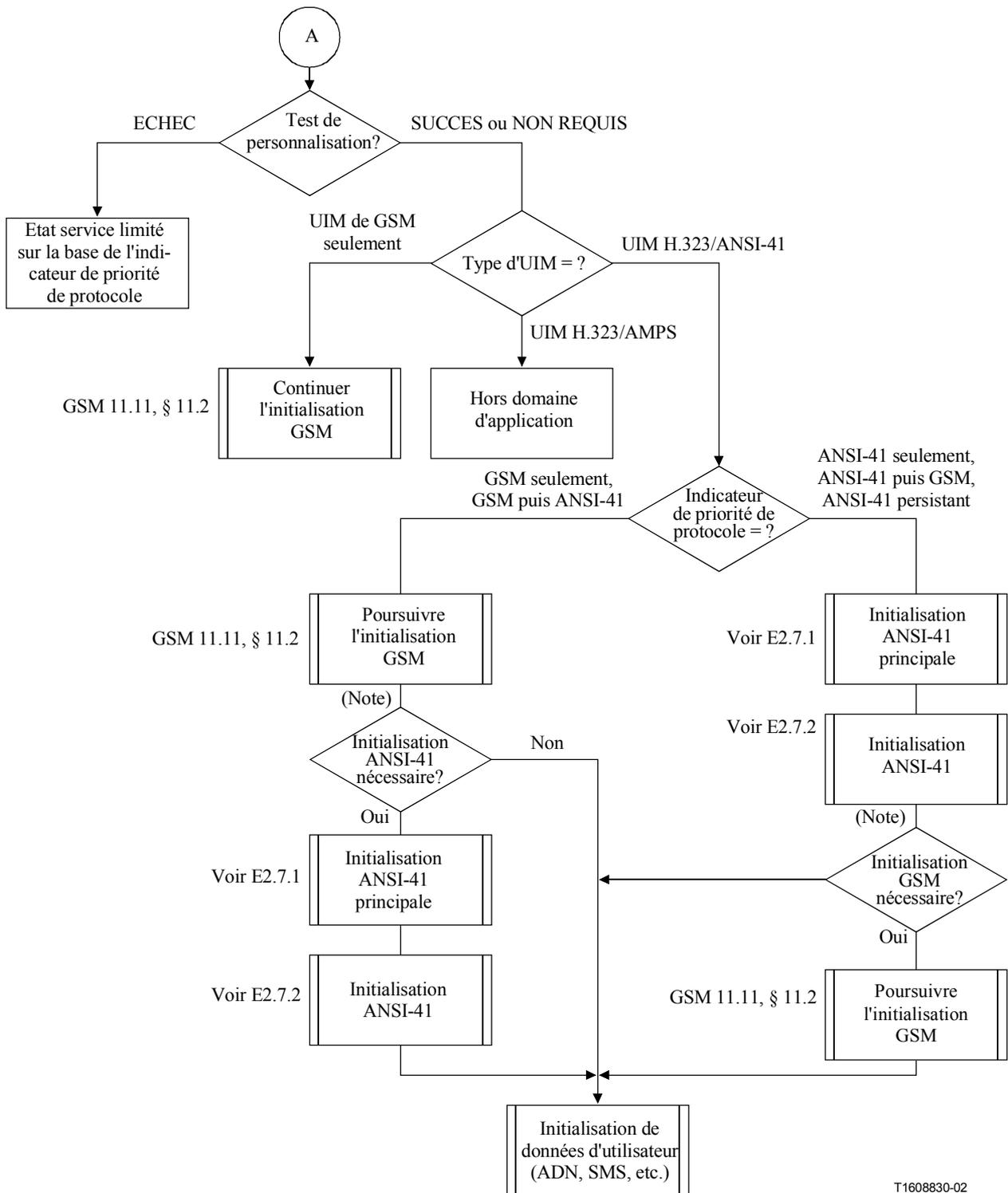


Figure E2.2/H.246 – Procédures de gestion UIM – 1 (pour information)



NOTE – L'initialisation des données d'utilisateur peut avoir lieu à ce stade.

Figure E2.3/H.246 – Procédures de gestion UIM – 2 (pour information)

E2.7.1 Initialisation ANSI-41 (noyau central)

Le terminal H323_UIM Terminal exécute les procédures suivantes:

- MIN Request;
- ACCOLC Request;
- SID request;
- Group ID request;
- S-ESN request;
- COUNTsp request;
- Positive/Favoured SID List request;
- Negative/Forbidden SID List request.

Il existe d'autres fichiers dans le DF_{PCS1900} qui sont exigés pour la station mobile GSM/AMPS; toutefois, la lecture de ces fichiers n'est pas exigée pour un mobile GSM/ANSI-136 et de ce fait sort du cadre de la présente Annexe.

E2.7.2 Initialisation ANSI-41 H323_UIM

Le terminal H323_UIM Terminal exécute les procédures suivantes:

- IRDB Parameters request;
- Additional User Registration Parameters request;
- Partner SID List request;
- Partner SOC List request;
- Favoured SOC List request;
- Forbidden SOC List request;
- Alpha Tag request;
- Triggered Scan Timers request;
- TeleService Server Address request;
- SS Feature Code Table request;
- IRDB Version Table request;
- User Group ID request;
- Cooperative SOC List request.

E2.7.3 Fin de session par l'UIM

Le terminal H323_UIM Terminal doit exécuter les procédures de fin de session définies au § 11.2.2 du GSM 11.11, dans les cas suivants:

- ANSI-41 H323_UIM avec indicateur de priorité de protocole (*protocol priority indicator*) positionné à ANSI-41 puis à GSM.

Le terminal H323_UIM doit exécuter les mises à jour suivantes:

- paramètres complémentaires d'enregistrement d'utilisateur (*additional user registration parameters*).

Dans les cas suivants:

- module ANSI-41 H323_UIM dont l'indicateur Protocol Priority Indicator est positionné à ANSI-41 seulement.

Dès que le module indique que ces procédures ont été exécutées, la liaison H323_UIM Terminal/UIM peut être libérée. Après libération de cette liaison, le terminal H323_UIM Terminal doit effacer de sa mémoire toutes les informations relatives à l'utilisateur. Si le terminal H323_UIM Terminal a déjà mis à jour une information relative à un abonné pendant la session UIM et que la valeur n'a pas été modifiée jusqu'à la fin de la session UIM, le terminal H323_UIM Terminal peut omettre la procédure de mise à jour applicable.

E2.7.4 Procédures relatives aux informations NAM H323_UIM

E2.7.4.1 Numéro d'identification du mobile (*mobile identification number*)

Obligation: selon la spécification UIM

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{MIN}

Mise à jour: le terminal H323_UIM exécute la procédure de mise à jour avec l'EF_{MIN}

E2.7.4.2 Classe de surcharge d'accès (*access overload class*)

Obligation: selon la spécification UIM

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{ACCOLC}

Mise à jour: le terminal H323_UIM exécute la procédure de mise à jour avec l'EF_{ACCOLC}

E2.7.4.3 Identification par le système du système de rattachement

Obligation: selon la spécification UIM

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{SID}

Mise à jour: le terminal H323_UIM exécute la procédure de mise à jour avec l'EF_{SID}

E2.7.4.4 Code de l'opérateur du système de rattachement et code du pays du mobile

Obligation: selon la spécification UIM

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{HSOC-MCC}

Mise à jour: le terminal H323_UIM exécute la procédure de mise à jour avec l'EF_{HSOC-MCC}

E2.7.4.5 Canal de radiomessagerie initial (*initial paging channel*)

Obligation: selon la spécification UIM

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{IPC}

Mise à jour: le terminal H323_UIM exécute la procédure de mise à jour avec l'EF_{IPC}

E2.7.4.6 ID de groupe (*group ID*)

Obligation: selon la spécification UIM

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{GPI}

Mise à jour: le terminal H323_UIM exécute la procédure de mise à jour avec l'EF_{GPI}

E2.7.4.7 Numéro de série électronique de carte SIM (*SIM electronic serial number*)

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{SESN}

E2.7.4.8 Indicateur d'utilisation AMPS (*AMPS usage indicators*)

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{AMPS-UI}

E2.7.4.9 Indicateurs d'utilisation ANSI-41 (*ANSI-41 usage indicators*)

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{ANSI-UI}

E2.7.4.10 Indicateurs Alpha (*alpha tags*)

Obligation: selon la spécification UIM

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{A-TAG}

Mise à jour: le terminal H323_UIM exécute la procédure de mise à jour avec l'EF_{A-TAG}

E2.7.5 Procédures H323_UIM relatives à l'authentification

E2.7.5.1 Décompte d'appels (*call count*)

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{COUNT-SP}

Mise à jour: le terminal H323_UIM exécute la procédure de mise à jour avec l'EF_{COUNT-SP}

E2.7.6 Procédures UIM relatives à la sélection de réseau (*UIM network selection related procedures*)

E2.7.6.1 Liste des identités SID Positives/Favorisées (*positive/favoured SID list*)

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{PSID}

E2.7.6.2 Liste des identités SID négatives/interdites (*negative/forbidden SID list*)

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{NSID}

E2.7.6.3 Liste des codes SOC coopératifs (*cooperative SOC list*)

Obligation: l'EF_{CNL} est marqué "allocated" et "activated"

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{CSL}

E2.7.6.4 Tableau de la version de la base de données IRDB (*IRDB version table*)

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{IRDB-VER}

E2.7.6.5 Liste des identités SID partenaires (*partner SID list*)

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{PART-SID}

E2.7.6.6 Liste des codes SOC partenaires (*partner SOC list*)

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{PART-SOC}

E2.7.6.7 Liste de codes SOC préférés (*favoured SOC list*)

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{FAV-SOC}

E2.7.6.8 Liste des codes SOC interdits (*forbidden SOC list*)

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{FORB-SOC}

E2.7.6.9 Paramètre IRDB

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{IRDB-PARAM}

E2.7.7 Procédures associées à l'interface d'utilisateur H323_UIM

E2.7.7.1 Tableau des codes de fonctionnalité des services complémentaires (*SS feature code table*)

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{SSFC}

E2.7.8 Procédures relatives au séquençement H323_UIM (*H323_UIM timing related procedures*)

E2.7.8.1 Temporisateurs à balayage déclenché (*triggered scan timers*)

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{TS-TIMER}

E2.7.9 Procédures relatives à l'enregistrement H323_UIM (*H323_UIM registration related procedures*)

E2.7.9.1 Seuil d'enregistrement (*registration threshold*)

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{REG-THRESH}

Mise à jour: le terminal H323_UIM exécute la procédure de mise à jour avec l'EF_{REG-THRESH}

E2.7.10 Procédures additionnelles H323_UIM (*H323_UIM additional procedures*)

E2.7.10.1 Identificateur de phase UIM H.246 Annexe 2 (*H.246 Annex E2 UIM phase ID*)

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{GA-PHASE}

E2.7.10.2 Info d'adresse du serveur de téléservice (*teleservice server address info*)

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{TSAI}

Mise à jour: le terminal H323_UIM exécute la procédure de mise à jour avec l'EF_{TSAI}

E2.7.10.3 Paramètres d'enregistrement d'un utilisateur additionnel (*additional user registration parameters*)

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{AURP}

Mise à jour: le terminal H323_UIM exécute la procédure de mise à jour avec l'EF_{AURP}

E2.7.10.4 Identificateur de groupe d'utilisateurs (*user group ID*)

Obligation: selon la spécification UIM

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{UGIDI}

Mise à jour: le terminal H323_UIM exécute la procédure de mise à jour avec l'EF_{UGIDI}

E2.7.10.5 Clé de commande de dépersonnalisation du code SOC (*SOC de-personalization control key*)

Demande: le terminal H323_UIM exécute la procédure de lecture avec l'EF_{SDCK}

E2.7.11 Procédures de gestion de mise à jour du terminal H323_UIM

Dans certains cas, il peut être nécessaire pour le terminal H323_UIM de notifier au terminal une modification de configuration, c'est-à-dire une mise à jour d'un téléservice de messagerie brève sur un serveur ANSI-41 à la base de données IRBD de l'UIM et ou de l'information associée au module NAM. En tant que tel, il peut être demandé au terminal H323_UIM de mettre à jour des images des fichiers élémentaires qu'il est susceptible de contenir et/ou d'exécuter certaines autres procédures (à savoir une exploration de mise sous tension après la mise à jour du module). Dans ces cas, le module H323_UIM doit utiliser la commande UIM Tool Kit Command REFRESH pour notifier au terminal mobile H.323 les modification de sa configuration. Pour de plus amples détails on se reportera au GSM 11.14.

Le Tableau E2.1 définit les directives à utiliser lorsqu'il y a eu des modification concernant le module UIM. Dès réception d'une commande REFRESH, le terminal mobile H.323 doit exécuter les actions indiquées dans le Tableau E2.1 lorsque le fichier concerné a été modifié.

Tableau E2.1/H.246 – Terminal H323_UIM directives applicables à la modification du module UIM

Fichier mis à jour	Image des mises à jour du terminal H323_UIM	Le terminal H323_UIM exécute une exploration de mise sous tension
MIN		✓ si dans le terminal ANSI-41 H323_UIM
ACCOLC		NA
SID		✓
Group ID		NA
S-ESN	NA	NA
COUNTsp		NA
Positive/Favoured SID List		✓
Negative/Forbidden SID List		✓
Registration Threshold		NA
IRDB Parameters		✓
Additional User Registration Pars.	✓ si dans GSM	NA
Partner SID List		✓
Partner SOC List		✓
Favoured SOC List		✓
Forbidden SOC List		✓
Alpha Tag		NA
Triggered Scan Timers		NA
TeleService Server Address		NA
SS Feature Code Table		NA
IRDB Version Table		NA
User Group ID		NA
SOC De-personalization Control Key	✓	

Si une commande REFRESH est reçue par le terminal mobile H.323 et qu'il en résulte des modifications de certains fichiers de la liste, le terminal doit mettre à jour toutes les images de cette information qu'il peut contenir indépendamment du fait qu'il se trouve dans le mode ANSI-41 ou GSM et que le tableau indique qu'une exploration de mise sous tension peut être requise.

E2.8 Portier – Annexe E2_GK avec fonction d'interfonctionnement (RMTP) et portier H.323

Les réseaux hertziens numériques ANSI-41 actuels comportent principalement:

- des réseaux ANSI-41 dotés d'interfaces hertziennes TDMA et CDMA. Dans toute l'Amérique du Nord et du Sud, dans la plus grande partie de l'Asie et de la Russie, de l'Australie et dans certaines parties de l'Europe.

Le principal rôle du réseau mobile terrestre public ANSI-41 est de gérer les communications entre des utilisateurs mobiles et d'autres utilisateurs (utilisateurs mobiles, utilisateurs H323_UIM, utilisateurs du RNIS, utilisateurs de la téléphonie fixe, etc.). Il comporte également des bases

de données nécessaires au stockage des informations sur les abonnés et à la gestion de leur mobilité. La fonction IWF du RMTP ANSI-41 permet l'interfonctionnement entre le RMTP et un réseau H.323.

Le modèle de base d'une solution du type portier AnnexE2_GK est une fonction d'interfonctionnement logique qui effectue la conversion de protocole nécessaire, le mappage des bases de données et la gestion des transactions permettant de prendre en charge la gestion de la mobilité, le départ d'appel et les fonctions de remise d'appel.

Un portier du type de l'Annexe E2/H.246 entre un réseau H.323 et un réseau RMTP, effectue le mappage des opérations et des messages entre passerelles, le portier et le centre de commutation de mobile (MSC, *mobile switching centre*), le registre de localisation des visiteurs (VLR, *visitor location register*). Les fonctions d'interfonctionnement sont les suivantes:

Zones de gestion de la mobilité

- Enregistrement des terminaux et des utilisateurs H323_UIM;
- Authentification des terminaux et des utilisateurs H323_UIM.

Domaine de gestion de la communication

- Terminaison des appels en direction d'un terminal H323_UIM depuis un RMTP;
- Remise d'une notification de message en attente à un terminal H323_UIM;
- Emission de messages brefs en provenance d'une entité de messagerie brève dans un terminal H323_UIM;
- Terminaison de messages brefs vers une entité de messagerie brève dans un terminal H323_UIM.

Ce portier AnnexE_GK apparaît comme un portier vu du point d'extrémité H.323 et comme un registre de localisation des visiteurs (VLR) et un centre de commutation de mobile (MSC) vu du RMTP.

E2.8.1 Mappage des messages MAP du RMTP ANSI-41 en messages H.225.0

Tableau E2.2/H.246 – Mappage des messages MAP du RMTP ANSI-41 ↔ messages H.225.0

Fonctions	Messages MAP ANSI-41	Messages H.225.0
Enregistrement	RegistrationNotification (REGNOT)	Les opérations GRQ, GCF, GRJ, RRQ, RCF, RRJ sont utilisées pour l'enregistrement et l'authentification du terminal H323_UIM
Authentification	AuthenticationRequest (AUTHREQ) AuthenticationDirective (AUTHDIR) AuthenticationStatusReport (ASREPORT) CountRequest (COUNTREQ) AuthenticationFailureReport (AFREPORT) RandomVariableRequest (RANDREQ)	
Actualisation du profil d'abonné	QualificationRequest (QUALREQ) FeatureRequest (FEATREQ) QualificationDirective (QUALDIR)	ARQ, ACF, ARJ ↑ ↓
Remise d'appel	LocationRequest (LOCREQ) RoutingRequest (ROUTREQ)	
Mappage ISUP ↔ Q.931	RemoteUserInteractionDirective (RUIDIR)	Setup, Connect, Info
Notification de message en attente	Messages d'établissement d'appel, message de libération d'appel (QUALDIR) InformationDirective (INFODIR), indication MWN	Voir les contributions H.248 H.450.7 MWI SS
Service de messagerie brève	SMSRequest (SMSREQ), remise point à point SMS (SMD PP), notification SMS (SMSNOT), SMS vers l'arrière (SMS BACK), SMS vers l'avant (SMS FWD)	H.323 Annexe K (voie de transport HTTP des signaux de commande de service dans les réseaux H.323)
Services de protocole d'application hertzienne (WAP)	Scripts et explorateurs de Web WML	H.323 Annexe K (voie de transport HTTP des signaux de commande de service dans les H.323)
Désenregistrement	RegistrationCancellation (REGCANC) MSInactive (MSINACT) BulkDeregistration (BULKDEREG)	URQ, UCF, URJ, URQ, UCF, URJ URQ, UCF, URJ

E2.9 Procédures de gestion de mobilité et de gestion des communications relatives au portier AnnexE2_GK

E2.9.1 Addition de paramètres de mobilité et de procédures aux messages RAS H.225

Le fait d'étendre le type d'adresse alias par un nouveau type module MobileUIM qui prend en charge les différents formats d'identification des mobiles permet de fournir l'information d'identification de l'utilisateur mobile H.323.

E2.9.2 Aspect sécurité relatif au module d'identité d'utilisateur de mobile H.323 (UIM)

Suivre les procédures définies dans la Rec. UIT-T H.235 pour garantir le secret de l'authentification H323_UIM et de l'authentification ANSI-41 de H.323_UIM.

E2.9.3 Mode étranger H.323

Lorsqu'un abonné ANSI-41 local opère dans le mode étranger H.323, la station mobile doit utiliser l'interface H.323. La fonction d'interfonctionnement de l'Annexe E2/H.246 (AnnexE2_GK) doit assurer à la fois l'émulation du registre HLR H.323 et celle du registre VLR ANSI-41 pour permettre à l'abonné de s'enregistrer automatiquement et d'obtenir le service. Pour le réseau H.323 visité, l'abonné apparaît s'enregistrer depuis un portier AnnexE2_GK, qui émule un enregistreur HLR H.323. Cet enregistreur HLR H.323 se comporte pour le registre HLR ANSI-41 réel, comme une entité dotée d'un pouvoir limité, le registre HLR ANSI-41 conservant le contrôle ultime. Parallèlement, pour le réseau ANSI-41 de rattachement, l'abonné apparaît s'enregistrer depuis un portier AnnexE2_GK, émulant un registre VLR ANSI-41. Le portier AnnexE2_GK fait le lien entre les opérations et les données H.225.0 d'une part et les opérations et données équivalentes du sous-système MAP d'autre part, et inversement, afin d'assurer l'interfonctionnement.

Pour pouvoir opérer en mode H.323 étranger, on peut placer un centre d'authentification H.323 (AuC, *authentication centre*) dans le portier AnnexE2_GK.

En ce qui concerne l'interopérabilité du service de message court (SMS), le portier AnnexE2_GK doit également assurer l'émulation d'un centre SMSC en utilisant le protocole de l'Annexe K/H.323 (Protocole de commande de service), agissant comme ayant une délégation limitée pour le centre de messagerie MC ANSI-41. Dans certains cas, le portier AnnexE2_GK devra pouvoir émettre des messages brefs afin de prendre en charge l'interopérabilité. Afin de prendre en charge le renvoi d'appel différé, le portier AnnexE2_GK and H.246 Annexe B/C assure également l'émulation du centre MSC de la passerelle.

E2.9.4 Données d'abonné

Le portier AnnexE2_GK n'assure pas la duplication du registre HLR existant de l'abonné, mais il offre une passerelle en direction de tout réseau visité qui utilise un protocole MAP étranger. La source d'origine des données d'abonné reste dans le registre HLR du réseau de rattachement. La plupart de ces données ne doivent pas se trouver dans le portier AnnexE2_GK mais être dynamiquement converties et traduites entre message H.323 et message MAP ANSI-41 si nécessaire.

Toutefois, certaines informations de base relatives à l'identité de l'abonné doivent être fournies dans le portier AnnexE2_GK pour pouvoir prendre en charge le processus de mappage, à savoir:

- l'identité d'abonné mobile internationale (IMSI, *international mobile subscriber identity*);
- numéro d'identification du mobile (MIN, *mobile identification number*);
- numéro de série électronique (ESN);
- type de terminal.

Les services d'authentification et de cryptage sont des services essentiels qui peuvent être pris en charge dans le cadre de l'interopérabilité des réseaux. Ces capacités sont gérées dans les réseaux H.323 et ANSI-41 par le centre d'authentification (AuC ou AC), qui peut être physiquement distinct du registre HLR associé. Différents processus et algorithmes d'authentification sont définis pour les réseaux H.323 et ANSI-41. Par conséquent, pour l'implémentation de la phase 1, les données d'authentification propres à l'abonné doivent être fournies et maintenues dans les centres AuC H.323 et AC ANSI-41, afin de pouvoir prendre en charge le service sur l'un des réseaux. Les données d'abonné qui doivent être maintenues sont les suivantes:

- Ki (clé d'authentification d'abonné H.323);
- Les triplets ou groupes de clé de chiffrement (K_c , *cipher key*), numéro de séquence de la clé de chiffrement (CKSN, *cipher key sequence number*) et réponse signée (SRES, *signed response*) pour l'authentification et le chiffrement H.323;
- Clé A-key (clé d'authentification ANSI-41);
- Données SSD-A (données communes secrètes ANSI-41 pour l'authentification);
- Données SSD-B [données secrètes communes ANSI-41 pour le cryptage des messages de signalisation produits (SME) et les masques de secret vocaux (VP)].

Le centre d'authentification en mode étranger peut être intégré au portier AnnexE2_GK ou implémenté dans un élément de réseau distinct.

E2.10 Enregistrement et authentification automatique

La station mobile de l'Annexe E2/H.246 doit utiliser la sélection de réseau pour obtenir automatiquement les meilleurs services possibles dans une zone géographique donnée. Après sélection automatique d'un fournisseur de réseau dans une zone donnée, le réseau doit prendre en charge l'enregistrement automatique depuis cette zone de service dans la table de localisation de rattachement (HLR, *home location register*).

E2.10.1 Adressage

En mode étranger H.323, le portier AnnexE2_GK doit prendre en charge l'enregistrement en utilisant le numéro d'identification du mobile (MIN) telle l'identité de la station mobile (MSID). Lorsque le numéro MIN est utilisé comme identification pour l'enregistrement, le portier AnnexE2_GK doit faire la corrélation de ce numéro MIN avec l'adresse IP associée pour l'abonné H.323 local.

E2.10.2 Authentification, cryptage, secret des conversations

L'authentification, le cryptage et le secret des conversations dans le mode ANSI-41 H323_UIM doivent être pris en charge comme défini dans les documents "Common Cryptographic Algorithms, Revision C", ANSI TIA/EIA-136-510 et ANSI TIA/EIA-136-511, à l'exception que l'entrée du numéro ESN dans l'algorithme CAVE doit dépendre de l'état de l'indicateur ESN Usage Indicator dans le terminal H323_UIM.

E2.11 Mobilité fondée sur le module UIM

La mobilité fondée sur le module H323_UIM identifie la capacité d'un abonné utilisant le module UIM, d'insérer son module dans tout terminal H.323 ou équipement mobile H.323 pouvant le prendre en charge afin d'obtenir le service sans intervention de l'opérateur ou de l'exploitant. L'expression terminal/équipement mobile H.323 de prise en charge renvoie à un terminal/terminal mobile H323_UIM capable de lire l'identification d'abonnement et l'information associée requises sur le terminal H323_UIM.

La mobilité UIM permet aux abonnés de changer de terminal/d'équipement mobile H.323 afin d'accéder à des bandes ou des fonctionnalités spécifiques qui ne peuvent pas être accessibles depuis un terminal/équipement mobile H.323. Elle permet également aux abonnés de changer facilement de terminal/d'équipement mobile H.323 pour mise à niveau ou réparation, sans intervention de l'opérateur ou de l'exploitant.

E2.11.1 Utilisation des identificateurs d'équipement mobile

L'ANSI-41 utilise le numéro de série électronique (ESN, *electronic serial number*) pour identifier de manière univoque la station mobile; actuellement, l'identificateur IMEI n'est pas transmis depuis la station mobile vers le réseau ANSI-41. Dans le réseau ANSI-41, ce numéro est actuellement utilisé pour les opérations d'autorisation et d'authentification des abonnés, le cryptage des messages de signalisation et le secret des conversations et, dans le réseau AMPS, pour les opérations d'autorisation et d'authentification des abonnés. Certains fournisseurs de services ANSI-41 utilisent également le numéro ESN pour suivre les stations mobiles en service. L'association permanente du numéro ESN à l'émetteur mobile est actuellement requis par certains organes de réglementation fédérale afin de diminuer les possibilités de fraude par changement de numéro ESN.

Lorsque toutes les données d'abonné nécessaires aux opérations d'autorisation et d'authentification ont été stockées dans la station H323_UIM, la mobilité UIM peut être facilement prise en charge sans imposer de condition particulière complémentaire au réseau. Toutefois, le stockage de l'identité de la station mobile (MSID) dans la station H323_UIM et du numéro ESN dans l'équipement mobile rend difficile la prise en charge de la mobilité UIM par les réseaux ANSI-41 car l'identificateur MSID et le numéro ESN utilisés pour l'authentification, le cryptage, le secret des conversations peuvent ne pas correspondre aux combinaisons MSID et ESN stockées dans les centres HLR/AC pour l'abonné. Dans le futur, des possibilités de modification d'utilisation actuelle du numéro ESN dans les réseaux ANSI-41 seront peut-être offertes. Parmi ces possibilités, citons:

- 1) modification du rôle du numéro ESN pour l'authentification, le cryptage et le secret des conversations;
- 2) possibilité de faire résider le numéro ESN dans le module UIM avec l'identification de la station mobile;
- 3) adjonction de l'identificateur IMEI à l'ANSI-41. Chaque option présente des avantages et des inconvénients.

Afin d'offrir une certaine souplesse d'implémentation d'une solution permettant d'assurer la mobilité UIM dans les réseaux ANSI-41, le terminal H.246 de l'Annexe E2 H323_UIM doit prendre en charge la méthode suivante utilisant le numéro ESN:

- 1) le terminal H323_UIM doit contenir un numéro ESN;
- 2) le terminal H323_UIM doit contenir un numéro de série électronique SIM (SESN, *SIM electronic serial number*) de même longueur que le numéro ESN. **Le numéro SESN doit être chargé de manière permanente par le constructeur du terminal H323_UIM et impossible à modifier.** Ce numéro SESN ne sera pas nécessairement associé à un constructeur ou attribué par l'UIT/TIA;
- 3) le module SIM doit contenir un indicateur d'utilisation ESN (EUI, *ESN usage indicator*) qui définit la façon dont les numéros ESN et SESN sont utilisés pour l'identification et la sécurité. Par sécurité, on entend les méthodes d'authentification des stations mobiles ainsi que les méthodes de cryptage des données cryptées (d'utilisateur et de signalisation) et des communications vocales. Par identification, on entend la méthode permettant de signaler au réseau la présence de l'équipement mobile H323_UIM. Le champ EUI doit être protégé contre toute intervention non autorisée. Il doit indiquer à la station mobile le mode à utiliser parmi les suivants:
Mode 1 utilisation du numéro ESN de l'équipement mobile aux fins de sécurité et d'identification;

- Mode 2 utilisation du numéro SESN du module H323_UIM aux fins de sécurité et du numéro ESN de l'équipement mobile aux fins d'identification;
- Mode 3 utilisation du numéro SESN du module H323_UIM aux fins de sécurité et d'identification.

Pour éviter toute fraude avec les systèmes plus anciens et dans l'attente de dispositions réglementaires, les premiers équipements mobiles H.246 AnnexE2 ne doivent pas prendre en charge le mode 3. Au cas où l'EUI du terminal H323_UIM serait programmé en mode 3, la station mobile devra utiliser par défaut le mode 1.

E2.11.2 Prise en charge du mode ANSI-41

En ce qui concerne la spécification IS-751, l'identité de la station mobile (MSID, *mobile station identity*) est liée à un numéro ESN spécifique. Cette combinaison fixe MSID-ESN est utilisée pour valider l'abonné qui accède au réseau. Pour les portiers AnnexE2_GK et les terminaux H323_UIM, l'identité de la station mobile dans le mode ANSI-41 doit se trouver dans le module UIM pour permettre la prise en charge de la mobilité UIM d'un abonné H.246 AnnexE2 fonctionnant en mode ANSI-41, lorsque:

- le numéro ESN reste seulement avec l'équipement mobile (ME, *mobile station*);
- l'indicateur d'utilisation de l'ESM (EUI) indique le mode de fonctionnement 1;
- le numéro de série électronique SIM (SESN) n'est pas utilisé.

Pour pouvoir fonctionner en mode ANSI-41, le HLR/AC ANSI-41 et les portiers H.246 AnnexE2_GK doivent prendre en charge les capacités suivantes:

- 1) la mobilité UIM en mode ANSI-41 est une option fournie par le service dans le HLR/AC et le portier AnnexE2_GK pour l'abonné ANSI-41;
- 2) le centre d'authentification (AC, *authentication centre*) pour le réseau de rattachement et le portier AnnexE2_GK pour le fonctionnement en mode ANSI-41 doivent désactiver la fonction de validation initiale de la combinaison MSID-ESN lorsque l'abonné accède pour la première fois au réseau aux fins d'enregistrement. Par contre, le centre AC doit utiliser le numéro ESN dynamique indiqué lorsqu'il effectue le traitement CAVE à l'enregistrement. Si l'authentification CAVE à l'enregistrement est positive sur la base du numéro ESN dynamique indiqué, le centre AC mémorise ce numéro ESN comme étant le numéro validé courant. La validation MSID-ESN pendant les tentatives ultérieures d'accès au réseau doit être exécutée sur la base de l'ESN courant validé;
- 3) lorsqu'un abonné ANSI-41 local s'enregistre en mode étranger H.323, un numéro ESN fixe fourni initialement à cet utilisateur doit toujours être transmis du portier AnnexE2_GK au registre HLR de l'abonné. Le registre HLR doit toujours autoriser l'enregistrement de l'abonné utilisant ce numéro ESN fixe;
- 4) le registre HLR du réseau de rattachement et le registre HLR émulé du portier AnnexE2_GK pour le fonctionnement en mode ANSI-41 doit effectuer la validation MSID-ESN sur la base du résultat de l'authentification de l'abonné obtenu lors de l'enregistrement. Si le résultat de cette authentification à l'enregistrement est positif, sur la base d'un numéro ESN dynamique indiqué, ce numéro est alors stocké comme étant le numéro ESN dynamique validé courant. La validation ultérieure du MSID-ESN au niveau du registre HLR du portier AnnexE2_GK sera effectuée sur la base de ce numéro ESN courant. La validation ultérieure des MSID-ESN dans le registre HLR du réseau de rattachement sera effectuée sur la base du numéro ESN initial fixe fourni ou sur la base du numéro ESN courant validé dynamique. Un numéro ESN validé dynamique reste indéfiniment un numéro ESN autorisé pour cet abonné jusqu'à ce qu'un numéro ESN nouvellement indiqué ait été utilisé avec succès pour l'authentification à l'enregistrement.

E2.11.3 Remise automatique des appels

Après réussite de l'enregistrement en mode ANSI-41 ou H.323 étranger, les appels entrants à destination de l'abonné lui seront automatiquement remis depuis le réseau de rattachement. Le portier AnnexE2_GK doit demander au nœud serveur un numéro d'annuaire local temporaire (TLDN, *temporary local directory number*) ou un numéro de routage vers la station mobile (MSRN, *mobile station routing number*) pour permettre le retour vers la passerelle ou le MSC d'origine afin d'acheminer les appels vers le nœud serveur. Lorsque le numéro TLDN n'est pas fourni sous un format international E.164, le portier AnnexE2_GK doit effectuer la conversion nécessaire du plan de numérotage lorsqu'il procède au mappage vers ou à partir du numéro MSRN.

E2.11.4 Commande des caractéristiques des services complémentaires

Les abonnés doivent activer et utiliser de manière transparente les services complémentaires sans tenir compte ou avoir connaissance du type de réseau auquel cet abonné accède, qu'il s'agisse d'un réseau ANSI-41 ou H.323.

E2.11.5 Prise en charge du mode H.323 étranger

Lorsque l'abonné invoque la commande d'un service complémentaire dans un réseau H.323, la station mobile relaye l'action demandée en émettant une opération REGISTER en direction du commutateur MSC serveur, indiquant l'action requise au niveau du service complémentaire. Le commutateur MSC serveur déclenche l'opération H.225.0 appropriée ou émet une demande au registre HLR de l'abonné.

Si l'abonné local ANSI-41 se déplace en mode étranger H.323, l'opération H.225.0 ou la demande doivent être dirigées vers le portier AnnexE2_GK. Ce portier traduit cette demande en une opération FeatureRequest ANSI-41, contenant la chaîne de chiffres composés *FC et envoie cette demande au registre HLR pour l'abonné ANSI-136. Dès qu'il a reçu un résultat ou un accusé de réception en provenance du registre HLR, le portier AnnexE2_GK émet en retour un accusé de réception approprié vers le centre MSC serveur du portier AnnexE2_GK.

Des flux d'appels types dans le cas d'une commande de service complémentaire en mode étranger H.323 sont présentés dans la description du renvoi d'appel de la Rec. UIT-T H.450.

E2.11.6 Mappage des codes de fonctionnalité

Afin de pouvoir prendre en charge la commande de fonctionnalité des services complémentaires en mode étranger, le portier AnnexE2_GK doit mapper les demandes de commande de fonctionnalité en codes de fonctionnalité spécifiques et inversement. Un ensemble commun de codes de fonctionnalités de services complémentaires n'a pas été implémenté dans tous les réseaux ANSI-41. Dans certains cas, les réseaux cellulaires A-side et B-side ainsi que les réseaux CDMA/ANSI-136 dans l'hyperbande 1 900 MHz (PCS) utilisent des ensembles de codes de fonctionnalité différents.

Afin de mieux assurer l'interopérabilité, l'utilisation de codes de fonctionnalité normalisés ANSI TIA/EIA-660 est recommandée. Les codes de fonctionnalité définis dans le Tableau E2.3 doivent être admis et utilisés dans le réseau pour assurer l'interopérabilité de la commande de fonctionnalité.

Tableau E2.3/H.246 – Codes de fonctionnalité pour la commande de fonctionnalité de service complémentaire

Commande de fonctionnalité de service complémentaire	Code de fonctionnalité ANSI-660 associé (FC)
Désactivation appel en attente (par appel)	700
Activation du renvoi d'appel sans condition	72
Désactivation du renvoi d'appel sans condition	720
Activation du renvoi d'appel sur occupation	90
Désactivation du renvoi d'appel sur occupation	900
Activation du renvoi d'appel sur non-réponse	92
Désactivation du renvoi d'appel sur non-réponse	920

Dans la plupart des cas, ces codes standards de fonctionnalité ne doivent pas entrer en conflit avec les autres ensembles de codes de fonctionnalité existants. Par conséquent, les opérateurs doivent pouvoir prendre en charge ces codes de fonctionnalité en plus des jeux de codes de fonctionnalité existants.

Des services complémentaires doivent être commandés et activés dans les réseaux ANSI-41 en utilisant les codes de fonctionnalité ANSI-660 et les chaînes de chiffres composés comme indiqué dans le Tableau E2.4. Lorsqu'un abonné ANSI-41 invoque ces commandes de fonctionnalité dans le mode étranger H.323, le portier AnnexE2_GK transmet ces chaînes de chiffres composés vers le registre HLR.

Tableau E2.4/H.246 – Chaînes de chiffres composés pour la commande de fonctionnalité de service complémentaire

Demande de commande de service complémentaire	Chaîne de chiffres composés dans FeatureRequest
Activation du renvoi d'appel sans condition – Activation et enregistrement	*72 + numéro de renvoi
Activation du renvoi d'appel sans condition – Activation seulement	*72
Désactivation du renvoi d'appel sans condition	*720
Activation du renvoi d'appel sur occupation – Activation et enregistrement	*90 + numéro de renvoi
Activation du renvoi d'appel sur occupation – Activation seulement	*90
Désactivation du renvoi d'appel sur occupation	*900
Activation du renvoi d'appel sur non-réponse – Activation et enregistrement	*92 + numéro de renvoi
Activation du renvoi d'appel sur non-réponse	*92
Désactivation du renvoi d'appel sur non-réponse	*920

Afin de permettre différentes implémentations de codes de fonctionnalité, le portier AnnexE2_GK doit permettre le stockage d'un tableau de codes de fonctionnalité de service complémentaire consistant dans un ensemble de codes de fonctionnalité constitué par le fournisseur de services de rattachement. Le tableau de codes de fonctionnalité de service complémentaire doit se composer d'entrées prises en charge dans la spécification H.323/ANSI-41 Common H.323 and Mobile

Terminal Specification. Si le tableau de codes de fonctionnalité de service complémentaire est vide, le portier AnnexE2_GK doit par défaut utiliser les codes de fonctionnalité normalisés ANSI TIA/EIA-660.

E2.11.7 Interdiction d'appel et interdiction d'appel déterminée par l'opérateur

Pour un abonné local ANSI-41, le contrôle par l'opérateur des appels entrants et sortants, ainsi que l'autorisation de mobilité, peuvent être assurés au niveau du registre HLR de l'abonné.

E2.11.8 Interdiction des appels sortants (service complémentaire et interdiction déterminée par l'opérateur)

Les capacités d'interdiction des appels sortants suivantes doivent être mappées dans le mode étranger H.323:

- interdiction de tous les appels sortants (BAOC, *barring of all outgoing call*);
- interdiction de tous les appels internationaux sortants (BOIC, *barring of outgoing international call*);
- interdiction de tous les appels sortants internationaux à l'exception de ceux qui sont à destination du pays du RMTP de rattachement (HPLMN) (BOIC-exHC).

Le mappage des conditions d'interdiction des appels sortants ANSI-41 dans le mode étranger H.323 (voir Tableau E2.5) doit être effectué conformément à l'ANSI-41. OriginationIndicator est un paramètre fourni par le registre HLR au registre VLR dans le profil d'abonné pour indiquer les types d'appel sortant autorisés.

Tableau E2.5/H.246 – Mappage en mode étranger H.323 pour l'interdiction des appels sortants

Fonctionnalité d'interdiction des appels H.323	OriginationIndicator ANSI-41 correspondant
Interdiction de tous les appels sortants (BAOC)	Départ interdit
Interdiction de tous les appels internationaux sortants (BOIC)	Appels longue distance nationaux (y compris les appels locaux)
Interdire tous les appels internationaux sortants sauf en direction du RMTP de rattachement (BOIC-exHC)	Appels longue distance nationaux (y compris les appels locaux)

E2.11.9 Interdiction des appels entrants (service complémentaire et interdiction déterminée par l'opérateur)

L'interdiction des appels entrants est contrôlée et invoquée par le registre HLR de l'abonné. L'invocation de l'interdiction de tous les appels entrants (BAIC, *barring of incoming call*) doit être prise en charge dans le mode H.323 étranger. Pour pouvoir prendre en charge l'invocation de l'interdiction de tous les appels entrants lorsqu'il y a mobilité en dehors du pays du RMTP de rattachement (BIC-Roam), le portier AnnexE2_GK doit fournir un système serveur spécifique ou un identificateur de RMTP visité (VPLMN), au registre HLR ANSI-41 lorsque l'abonné s'enregistre en mode H.323 étranger. Chaque système serveur H.246 AnnexE2 doit pouvoir être identifié de manière univoque avec une adresse E.164 appropriée par le registre HLR ANSI-41.

E2.11.10 Interdiction de la mobilité déterminée par l'opérateur

L'interdiction de mobilité déterminée par l'opérateur est commandée par le registre HLR ANSI-41. Pour pouvoir prendre en charge cette caractéristique, le portier AnnexE2_GK doit fournir un système serveur spécifique ou un identificateur de VPLMN, au registre HLR ANSI-41 lorsque l'abonné tente de s'enregistrer en mode H.323 étranger. Dès qu'il y a invocation de cette caractéristique, le registre HLR GSM doit refuser l'enregistrement. Le degré de granularité avec lequel la mobilité peut être refusée (par exemple mobilité en dehors du pays du RMTP de rattachement) sera déterminé par les capacités HLR.

E2.11.11 Enregistrement et activation

Les abonnés locaux ANSI-41 peuvent seulement enregistrer ou activer le renvoi d'appel sur non-réponse dans le mode local de référence aux renvois d'appel sur non-réponse CFNRy et CFNRc individuellement. Par conséquent, l'enregistrement ou l'activation des services complémentaires CFNRc ou CFNRy dans le mode étranger H.323 doit se traduire par l'enregistrement ou l'activation du renvoi d'appel sur non-réponse (CFNR, *call forwarding no reply*). Si l'un des services CFNRc ou CFNRy est enregistré ou activé en mode H.323 étranger, l'autre caractéristique doit aussi être enregistrée ou activée.

Dans le mode H.323 étranger, le portier AnnexE2_GK doit consulter le registre HLR de l'abonné ANSI-41 avec la demande Transfer to Number Request pour vérifier si le renvoi d'appel sur occupation (CFB) ou le renvoi d'appel sur non-réponse a bien été enregistré. Les numéros de renvoi résultant doivent être indiqués au registre VLR du portier AnnexE2_GK pour pouvoir prendre en charge l'invocation anticipée du renvoi CFNRc et l'acheminement non optimal du renvoi d'appel tardif.

E2.11.12 Acheminement optimal dans le cas du renvoi d'appel tardif

Le portier AnnexE2_GK doit prendre en charge l'invocation de l'acheminement optimal pour le renvoi d'appel tardif dans le mode H.323 étranger. Dans le cas de cette capacité, le portier reçoit un message reprise du traitement des appels (resume call handling) provenant du centre MSC serveur AnnexE2 H.246 et générera une demande de réacheminement (*redirection request*) vers le centre serveur MSC ANSI-41. Si une erreur en retour est reçue résultant d'une demande Redirection Request INVOKE, le portier AnnexE2_GK rejette la demande Resume Call Handling émanant du centre serveur MSC H.246 AnnexE2, ce qui déclenche le renvoi par le centre serveur MSC H.246 AnnexE2, de l'appel en utilisant un acheminement non optimal.

E2.11.13 Prise en charge du téléservice de messagerie brève (SMS)

Un portier AnnexE2_GK doté de capacités de l'Annexe K/H.323, doit assurer l'interfonctionnement entre le service SMS ANSI-41 et le terminal H323_UIM pour des messages courts en provenance ou à destination d'une station mobile. Lorsqu'un message bref FSM ANSI-41 (*forward short message*) est remis au portier AnnexE2_GK, ce portier le convertit en un message de commande de service Annexe K/H.323 acheminant des données de message court ANSI-41 et le remet via le réseau H.323. De même, lorsqu'un message court est émis depuis un terminal H323_UIM, un message de commande de service Annexe K/H.323 est remis au portier AnnexE2_GK, ce portier le convertit en message FSM ANSI-41 et le remet via le réseau ANSI-41.

E2.11.14 Notification de message en attente

Le terminal H323_UIM et le portier AnnexE2_GK doit prendre en charge la notification de message en attente (MWN, *message waiting notification*) provenant d'un réseau ANSI-41 par conversion de l'information MWN ANSI_41 en information MWN H.450.7.

E2.11.15 Service d'urgence

Le portier AnnexE2_GK n'a pas de rôle direct dans le routage ou l'aboutissement des appels d'urgence depuis des stations mobiles H323_UIM. Toutefois, les réseaux serveurs ANSI-41 et H.323 fournissent une capacité de "transit" pour permettre à l'appel d'être acheminé et présenté en un point de réponse de sécurité publique (PSAP, *public safety answering point*).

Le service d'urgence permet à un abonné de composer un numéro d'urgence et d'être connecté à un point PSAP pour demander une intervention d'urgence de la part de l'organisme concerné (pompiers, police, ambulance, centre antipoison ou centre anti-suicide, etc.).

Un appel d'urgence doit transgresser toute restriction d'autorisation et toute restriction d'émission d'appel.

Lorsque l'appel reçoit une réponse, l'abonné doit pouvoir communiquer le type d'urgence via une connexion vocale normale avec le point PSAP. (Le cryptage doit être désactivé sur la connexion avec le point PSAP.)

Un appel d'urgence a un effet sur la capacité d'un abonné à lancer ou à recevoir des appels pendant un appel d'urgence. Les services complémentaires et les caractéristiques commandées par activation de la clé SEND (appel en attente, conférence à trois, communication conférence ou transfert d'appel) sont suspendus pendant l'appel d'urgence, à l'exception de la reconnexion avec un appel mis en instance pour lancer un appel d'urgence. Lorsque l'appel d'urgence est libéré, les capacités d'appel normales de l'abonné sont rétablies. La libération se produit lorsque l'abonné ou le point PSAP se déconnecte.

Dans le mode ANSI-41, la station mobile doit prendre en charge la procédure d'appel d'urgence telle que décrite dans le Document TIA/EIA-136-123-A. Lorsqu'un appel d'urgence est émis par l'abonné dans le mode ANSI-41, la station mobile doit positionner le fanion Emergency Call dans le message Origination. Si ce fanion est positionné, il indique un appel d'urgence et le Called Party Number (numéro d'un appelé) est ignoré par le réseau.

Les appels d'urgence doivent se conformer aux règles imposées par les organismes publics.

E2.11.16 Services de localisation

Il n'est pas exigé du terminal H323_UIM d'inclure une fonctionnalité GPS. Les services de localisation peuvent être assurés dans les modes H.323 et ANSI-41 au moyen de solutions réseau.

E2.11.17 Services WAP

Les terminaux H323_UIM qui prennent en charge le protocole d'applications hertziennes (WAP, *wireless application protocol*) doivent se conformer aux conditions suivantes via le canal de transport de commande de service décrit dans l'Annexe K/H.323. Le terminal H323_UIM doit prendre en charge le protocole WAP tel que spécifié par le WAP Forum dans la spécification du WAP Wireless Datagram Protocol. Il est recommandé que le terminal H323_UIM prenne en charge au moins le protocole WAP 1.2. Les supports physiques pour le protocole WAP doivent être au minimum le service SMS ANSI-41, le service GPRS Packet Data et l'activation et la programmation à distance par voie hertzienne. Le terminal H323_UIM devra prendre en charge le protocole WAP Over The Air Provisioning (WAP 1.3) lorsque la norme le spécifiant sera finalisée. Le terminal H.323_UIM peut, et cela n'est pas interdit, prendre en charge le protocole WAP via le service GUTS (*general UDP transport service*) alors qu'il se trouve dans le mode ANSI-41.

E2.12 Descriptions d'étape 2 de l'interfonctionnement et des fonctionnalités des terminaux H323_UIM du RMTP ANSI-41

E2.12.1 Modèle opérationnel et flux de messages

Le présent paragraphe décrit certains messages types associés à la fonction d'interfonctionnement du RMTP ANSI-41 (portier AnnexE2_GK) et de la fonction terminal H323_UIM dans un réseau H.323. Dans les figures, les conventions suivantes ont été utilisées:

1) notation:

- ▶ protocole MAP H.323 et ANSI-41;
- ▶ message HTTP;
-▶ primitive donnée en exemple pour information (relève de l'implémentation).

Les messages ANSI-41 du MAP, HTTP et RAS sont en capitales (ANSI-41: REGNOT(invocation), REGNOT(réponse), HTTP:GET, RAS:ARQ), les premières lettres des messages de signalisation d'appel H.225.0 comportent des majuscules (Setup). Les points de code ASN.1 en H.225.0 sont écrits en gras (**ServiceControlAddress**).

Les paramètres des messages indiqués dans les tableaux de flux de messages, qui sont indiqués comme étant requis (R), obligatoirement rétrocompatibles (MBC, *mandatory backward compatible*) et optionnels (O) doivent être traités de la même façon en incluant les paramètres équivalents mobiles UIM H.225.0 dans l'AnnexE2_GK associée aux messages H.225.0.

Les flux de messages suivants indiqués dans la présente annexe ne sont pas limités, ils ne sont donnés qu'à titre d'exemple.

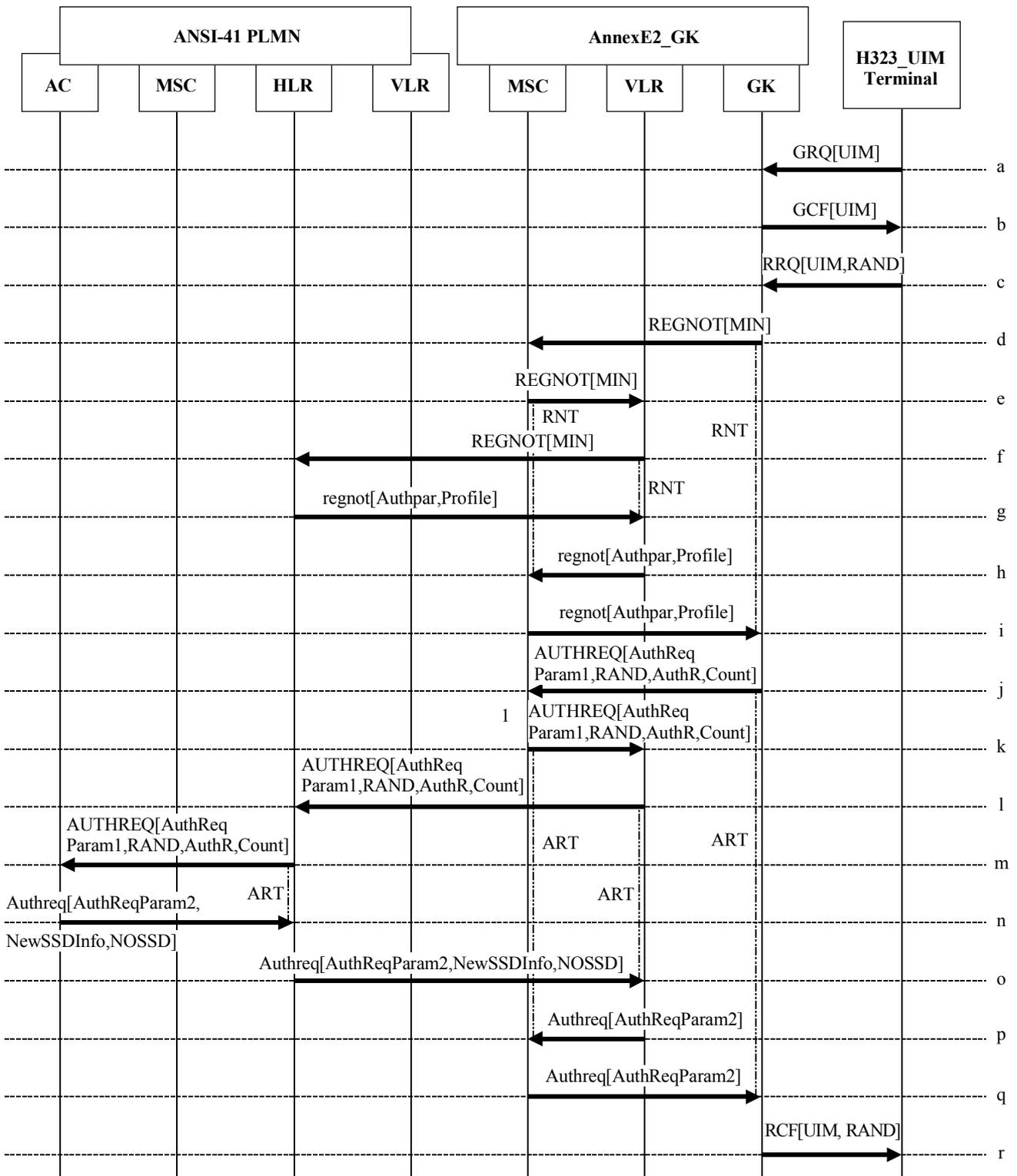
Flux de messages du domaine gestion de la mobilité:

- enregistrement du terminal et d'un utilisateur H323_UIM;
- authentification du terminal et d'un utilisateur H323_UIM.

Flux de messages du domaine gestion de la communication:

- terminaison d'un appel provenant d'un RMTP sur un terminal H323_UIM;
- remise d'une notification de message en attente au terminal H323_UIM;
- émission d'un message bref depuis une entité de message court dans un terminal H323_UIM;
- terminaison d'un message court vers une entité de message court dans un terminal H323_UIM.

E2.12.2 Enregistrement et authentification des flux de messages d'un terminal H323_UIM



T1608840-02

Figure E2.4 – Flux de messages d'enregistrement et d'authentification d'un terminal H323_UIM

Ce scénario opérationnel (Figure E2.4) décrit l'utilisation réussie de l'interfonctionnement des messages GRQ, GCF, RRQ, et RCF avec les opérations RegistrationNotification, AuthenticationRequest du RMTP ANSI-41 destinées à authentifier un terminal H323_UIM (HUT, *H323_UIM Terminal*) qui tente un accès initial. Le terminal HUT sait qu'un enregistrement et qu'une authentification sont requis sur tous les accès au système RMTP. Le résultat de ces opérations est en principe l'autorisation d'accès.

- a) Le terminal H323_UIM avec identité d'utilisation et identité de système mobile crypté (ou qui utilise l'autre méthode comme décrit dans l'Appendice IV/H.225.0) effectue une diffusion multiple d'un message de portier (GRK, *gatekeeper request*), "Qui est mon portier AnnexE_GK?". Ce message est envoyé au portier AnnexE_GK à une adresse bien connue Discovery Multicast Address dans la zone desservant les réseaux dotés d'une fonction IWF du RMTP.
- b) Un ou plusieurs portiers AnnexE_GK peuvent répondre par un message de confirmation de portier (GCF, *gatekeeper confirmation*) indiquant "Je peux être votre portier AnnexE_GK.", et envoyer l'adresse Transport Address en direction du canal RAS du portier AnnexE_GK.
- c) Le terminal H323_UIM (HUT) envoie une demande d'enregistrement (RRQ, *registration request*) avec un module UIM à un portier AnnexE_GK. Cette demande est envoyée vers l'adresse de transport de canal RAS du portier AnnexE_GK. Le terminal HUT a l'adresse de réseau du portier AnnexE_GK obtenue grâce au processus de découverte du portier (Gatekeeper Discovery) et utilise l'identificateur TSAP du canal RAS ou l'identificateur TSAP envoyé dans le message de confirmation GCF. Le portier AnnexE_GK convertit toute l'information relative au terminal H323_UIM en information du RMTP appropriée afin de commencer les transactions en direction du RMTP en qualité de centre MSC serveur et de registre VLR serveur.
- d) La fonction d'interfonctionnement passerelle/portier adresse un message REGNOT (RegistrationNotification) vers le centre MSC serveur situé à l'intérieur du portier AnnexE_GK.
- e) Le centre MSC serveur détecte la présence d'un terminal H323_UIM mobile dans sa zone de service; éventuellement à la suite d'un enregistrement autonome, d'un départ ou d'une terminaison d'appel ou bien d'une commande de service. Le centre MSC serveur envoie un message REGNOT à son registre VLR contenant les informations suivantes comme défini dans les spécifications ANSI-41 du RMTP (voir Rec. UIT-T X.691).

- g) Le registre HLR détermine qu'une autorisation peut être accordée au terminal HUT. Il retourne l'information demandée au registre VLR serveur dans le message REGNOT.

Tableau E2.8/H.246 – Paramètres associés aux messages regnot HLR → VLR

Paramètres	Utilisation	Type
AUTHPER	Indication de confirmation d'autorisation assortie d'une durée d'autorisation.	O
MYTYP	Identification du fournisseur du VLR.	MBC
Profile:	Information relative au profil de l'abonné. A inclure si profil demandé dans QUALCODE:	O
[CallingFeatures-Indicator]	autorisation et états d'activité pour les fonctionnalités.	
[OriginationIndicator]	type d'appel autorisé au départ de la station mobile.	
[Digits(Restriction)]	chiffres de tête choisis ou numéros complets d'annuaire autorisés pour le départ d'appel comme indiqué dans OriginationIndicator. A inclure le cas échéant.	
[Termination-RestrictionCode]	type d'appels que la station mobile est autorisée à terminer.	
HLRID [MSCID]	MSCID du HLR au regard de laquelle la MS doit s'enregistrer pour un UnreliableRoamerDataDirective subséquent.	R
[Digits(Carrier)]	Indique le IC préféré de la MS, le cas échéant.	
[RoutingDigits]	Instructions spéciales d'acheminement, le cas échéant.	
[Geographic-Authorization]	A inclure le cas échéant.	
[Authentication-Capability]	A inclure si l'authentification du terminal HUT est requise.	
[DMH_AccountCode-Digits]	A inclure le cas échéant.	
[DMH_AlternateBillingDigits]	A inclure le cas échéant.	
[DMH_BillingDigits]	A inclure le cas échéant.	
[MobileDirectory-Number]	A inclure si applicable.	
[MessageWaiting-NotificationCount]	A inclure si MessageWaitingNotificationType est <i>Count Indication</i> .	
[MessageWaiting-NotificationType]	Inclure si la fonctionnalité notification de message en attente est active et qu'une action est requise.	
[OriginationTriggers]	Points de déclenchement d'origine actuellement active pour l'abonné. A inclure le cas échéant.	
[PACAIndicator]	Indique l'état d'activation permanente PACA et le niveau de priorité assigné à l'abonné, le cas échéant.	
[PreferredLanguage-Indicator]	Indique le langage préféré associé à l'abonné, le cas échéant.	
[SMS_Origination-Restrictions]	Définit le type de messages que la MS est autorisée à émettre, le cas échéant.	
[SPINIPIN]	Indique le PIN de l'abonné, le cas échéant.	
[SPINITriggers]	Points de déclenchement SPINI actuellement actifs pour l'abonné. A inclure le cas échéant.	
[SMS_Termination-Restrictions]	Définit le type de messages que la MS est autorisée à recevoir, le cas échéant.	
[TerminationTriggers]	Points de déclenchement de terminaison actuellement actifs pour l'abonné. A inclure le cas échéant.	

- h) Le registre VLR transmet le message regnot au centre MSC serveur.

**Tableau E2.9/H.246 – Paramètres associés au message regnot du portier
AnnexE2_GK (VLR → MSC)**

Même paramètres que dans l'étape c), sauf que le paramètre HLRID n'est pas inclus et, avec les modifications suivantes:		
Paramètre	Utilisation	Type
MYTYP	Identification du fournisseur de VLR	MBC

- i) Le centre MSC serveur retransmet à son tour le message regnot avec l'information relative au profil de l'abonné, dans la fonction d'interfonctionnement de la passerelle/portier.
- j) Lors de cette tentative d'accès initial par un terminal HUT disposant de la capacité d'authentification, la fonction d'interfonctionnement de la passerelle/portier envoie un paramètre AUTHREQ au centre MSC serveur.

**Tableau E2.10/H.246 – Paramètres associés au message AUTHREQ du portier
AnnexE2_GK (GK→MSC)**

Paramètres	Utilisation	Type
AuthReqParameters1:	Ensemble de paramètres dans AUTHREQ:	
[MIN]	MIN de la MS servie.	R
[ESN]	ESN de la MS servie.	R
[MSCID]	MSCID du MSC serveur.	R
[PC_SSN]	PC_SSN du MSC serveur. A inclure si les services de transport SS7 sont utilisés	O
[SystemCapabilities]	capacités d'authentification du MSC serveur	R
[SystemAccessType]	type d'accès au système = enregistrement	R
[TerminalType]	identifie la norme de l'interface radiofréquence prise en charge par la MS associée.	R
RAND	Numéro aléatoire obtenu par le MSC serveur à partir du RANDC fourni par l'HUT.	R
AUTHR	Résultat d'authentification fourni par l'HUT.	R
COUNT	Valeur de CallHistoryCount fournie par l'HUT.	R

- k) Le MSC serveur envoie une demande AUTHREQ au registre VLR serveur avec tous les paramètres indiqués dans l'étape j).
- l) Le registre VLR envoie une demande AUTHREQ au registre HLR associé avec l'HUT.

**Tableau E2.11/H.246 – Paramètres associés au message AUTHREQ du portier
AnnexE2_GK (VLR → HLR)**

Mêmes paramètres que dans l'étape a, avec les modifications suivantes:		
Paramètres	Utilisation	Type
[SystemCapabilities]	Capacité d'authentification du VLR serveur.	R
[PC_SSN]	PC_SNN du VLR serveur. A inclure si les services d'acheminement SS7 sont utilisés.	O

- m) Le registre HLR transmet la demande AUTHREQ à l'AC. Les paramètres se trouvent dans l'étape k).

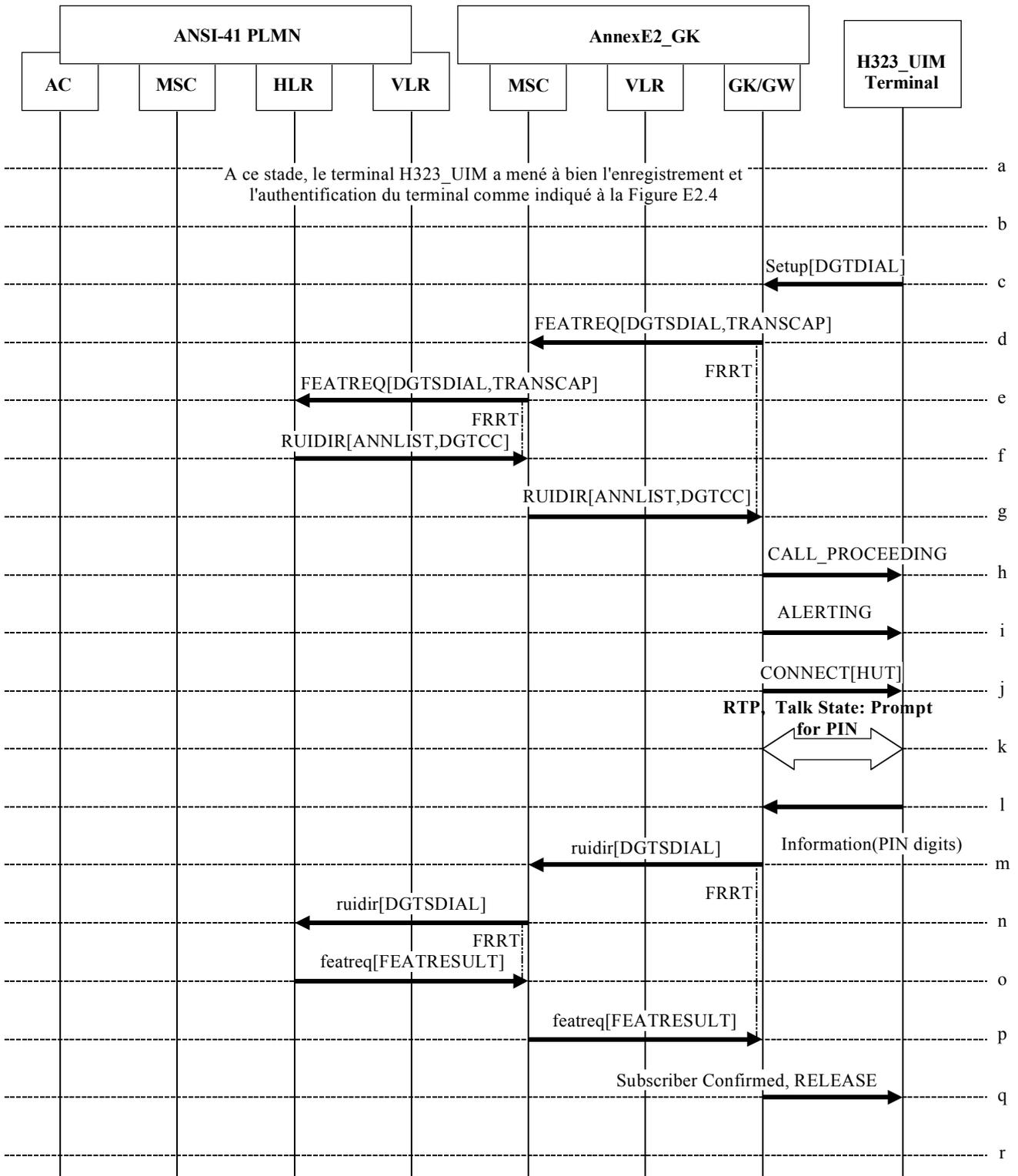
- n) L'AC détermine que l'accès doit être accordé au terminal HUT. L'AC envoie un authreq au registre HLR.

Tableau E2.12/H.246 – Paramètres associés au message authreq (AuC→HLR)

Paramètres	Utilisation	Type
AuthReqParameters2: [CallHistoryCount] [RANDSSD] [RANDU] [AUTHU] [UpdateCount]	Ensemble de paramètres dans authreq: compteur d'événements utilisé pour la détection de clones. A inclure si les SSD sont communes. nombre aléatoire pour la génération de SSD. A inclure si une mise à jour des SSD et un Unique Challenge au HUT doivent être initiés par le système serveur. nombre aléatoire généré par l'AC pour produire AUTHU. A inclure si un Unique Challenge de l'HUT doit être déclenché par le système serveur. réponse de l'HUT attendue à un Unique Challenge Order tel que calculé par l'AC. A inclure si un Unique Challenge de l'HUT doit être déclenché par le système serveur. indique que la procédure COUNT update doit être déclenchée par le système serveur.	O O O O O
NewSSDInfo: [Authentication AlgorithmVersion] [SSD]	Nouvelle information SSD: à inclure si SSD incluses pour choisir un algorithme d'authentification autre que l'algorithme par défaut. nouvelle valeur du VLR et des SSD AC. Peut être inclus dans les SystemCapabilities du VLR inclus "CAVE execution" et des politiques d'administration AC permettant la distribution des SSD.	O O
NOSSD	Indique que les SSD précédemment fournies ne sont plus valables et doivent être ignorées.	O

- o) Le registre HLR transmet l'authreq vers le registre VLR serveur. Mêmes paramètres que dans l'étape n).
- p) Le registre VLR serveur retransmet le message authreq vers le centre MSC serveur. Mêmes paramètres que dans l'étape n), sauf que les paramètres SSD, AAV et NOSSD ne sont pas inclus.
- q) Le centre MSC serveur envoie le message authreq vers la passerelle/le portier de la fonction d'interfonctionnement pour permettre l'exécution de l'authentification du terminal H323_UIM.
- r) Le portier AnnexE_GK doit envoyer une confirmation d'enregistrement (RCF, *registration confirmation*) avec l'ensemble de paramètres AuthReqParam2 au terminal H323_UIM indiquant la réussite de l'enregistrement et de l'authentification du terminal H323_UIM dans la zone du RMTP AnnexE_GK. Cette étape étant exécutée, le terminal HUT est prêt à accéder aux services mobiles depuis les RMTP et les réseaux H.323 des fournisseurs de services préférés.

E2.12.3 Authentification d'un abonné au moyen du numéro PIN pour invoquer les flux de messages associés aux services



T1608850-02

Figure E2.5/H.246 – Authentification d'un abonné au moyen de flux de messages PIN

Ces flux de messages relatifs à cette opération (dans la Figure E2.5) décrivent l'utilisation réussie des messages Q.931 (Setup, Call_proceed, Alerting, Connect, Release Complete et Information) interfonctionnant avec les opérations du RMTP ANSI-41 FeatureRequest (FEATREQ), RemoteUserInteractionDirective (RUIDIR) afin d'authentifier un abonné H323_UIM, qui tente d'accéder à un premier accès au service mobile. L'abonné au service mobile sait que l'authentification au moyen du PIN est requise sur tous les accès au service RMTP. Le résultat de ces opérations vise à permettre l'accès aux utilisateurs abonnés et actifs mobiles.

- a) Trouver la passerelle mobile au moyen des opérations GRQ, GCF.
- b) Enregistrement et authentification du terminal H323_UIM au moyen des opérations RRQ, RCF. Les fonctions des étapes a) et b), qui sont représentées à la Figure E2.1 sont menées à bien à ce stade du scénario.
- c) Le terminal H323_UIM avec Encrypted Mobile User Identity and System Identity compose (identité de l'utilisateur mobile et identité du système crypté) compose les chiffres de code de fonctionnalité (par exemple,*1234), un message Setup (établissement) avec Digits Dialed (chiffres composés) est envoyé du terminal HUT vers le portier mobile Annexe_GK.
- d) La fonction d'interfonctionnement passerelle/portier mobile dans l'Annexe_GK détecte le code de fonctionnalité dans le message SETUP en provenance du terminal H323_UIM et envoie une RMTP FeatureRequest avec Dialed Digits pour déclencher l'authentification de l'abonné sur le RMTP.
- e) Le centre MSC serveur envoie l'opération FEATREQ vers le registre HLR associé à l'abonné H323_UIM. Le paramètre TransactionCapability est également inclus dans l'opération FEATREQ, indiquant que le centre MSC serveur prend en charge les RUIDIR.
- f) Le registre HLR constate que les chiffres composés sont un enregistrement de fonctionnalités avec une adresse de terminaison de renvoi ou de déviation qui correspond à un déclencheur SPINI Trigger. Le registre HLR envoie une opération RUIDIR vers le centre MSC serveur.
- g) Dès réception de l'opération RUIDIR, le centre MSC serveur désactive le temporisateur FEATREQ (FRRT, *FEATREQ timer*) et transmet le message FEATREQ vers la fonction d'interfonctionnement de la passerelle/portier H.323 afin de permettre le traitement de l'appel comme indiqué dans le message reçu. Dans ce cas, le traitement consiste à répondre à l'appel (c'est-à-dire à connecter l'appelant au sous-système capable d'interaction d'utilisateur), et inviter l'utilisateur sur la base de l'information contenue dans l'opération RUIDIR reçue (dans le paramètre DigitCollectionControl) et d'attendre des chiffres.
- h) Le portier AnnexeE_GK envoie le message CallProceeding message vers le terminal H323_UIM (HUT).
- i) Le portier AnnexeE_GK envoie le message Alerting au terminal HUT.
- j) Le portier AnnexeE_GK envoie également le message Connect message au terminal HUT.
- k) Le terminal HUT et le portier AnnexeE_GK sont dans l'état Talk (conversation) avec le support RTP, l'IVR du portier AnnexeE_GK invite l'utilisateur à saisir son numéro PIN.
- l) L'utilisateur répond avec le numéro PIN d'authentification, qui est envoyé dans le message **Information (collected digits)** du terminal HUT au portier AnnexeE_GK.
- m) La fonction passerelle/portier H.323, après les avoir recueillis, transmet les chiffres à la fonction MSC serveur dans l'opération ruidir.
- n) Le centre MSC serveur envoie une opération ruidir en direction du registre HLR et inclut les chiffres composés par l'utilisateur. Le centre MSC serveur redémarre le temporisateur FRRT.

- o) Le registre HLR met à jour l'information d'enregistrement de fonctionnalité de la station mobile et envoie une opération featreq incluant le paramètre FeatureResult indiquant la réussite de l'opération fonctionnalité, au centre MSC serveur.
- p) Le centre MSC serveur désactive le temporisateur FEATREQ (FRRT) et assure le traitement pour le terminal HUT servi comme indiqué dans l'opération featreq reçues. Dans ce cas, le traitement consiste à confirmer la fonctionnalité et à libérer l'appel.
- q) Le portier AnnexE_GK actualise le profil confirmé par l'utilisateur et envoie le message Release Complete au terminal HUT pour libérer l'appel.
- r) L'abonné du terminal HUT est maintenant prêt à utiliser les services mobiles jusqu'au désenregistrement du terminal et de l'utilisateur.

E2.12.4 Extinction du terminal H323_UIM

En cas d'extinction d'un terminal H323_UIM alors qu'il fonctionne en mode étranger ANSI-41 (réseau H.323), le portier AnnexE2_GK reçoit un message MS INACTIVE de la part du registre VLR serveur. Le portier positionne alors le fanion "IMSI Detached". Si un terminal H323_UIM reste inactif pendant un certain temps (déterminé par l'opérateur), le portier peut alors effacer l'inscription de l'abonné associée à ce terminal H323_UIM et envoyer un message MS Purge (élimination de la station mobile) au registre HLR.

E2.12.5 Mise sous tension du terminal H323_UIM

Lorsque le terminal H323_UIM est mis sous tension et s'enregistre auprès d'un portier AnnexE2_GK (MSC/VLR serveur), alors qu'il fonctionne dans le mode étranger ANSI-41, ce sont les procédures d'enregistrement normales qui s'appliquent.

E2.13 Remise automatique des appels

La remise automatique des appels est demandée lorsque arrive une tentative d'appel entrant pour un abonné en déplacement. Les scénarios de remise des appels pour le cas où un abonné ANSI-41 se déplace dans un réseau H.323 sont indiqués ici.

E2.13.1 Remise d'un appel à un abonné ANSI-41 se déplaçant dans un réseau H.323

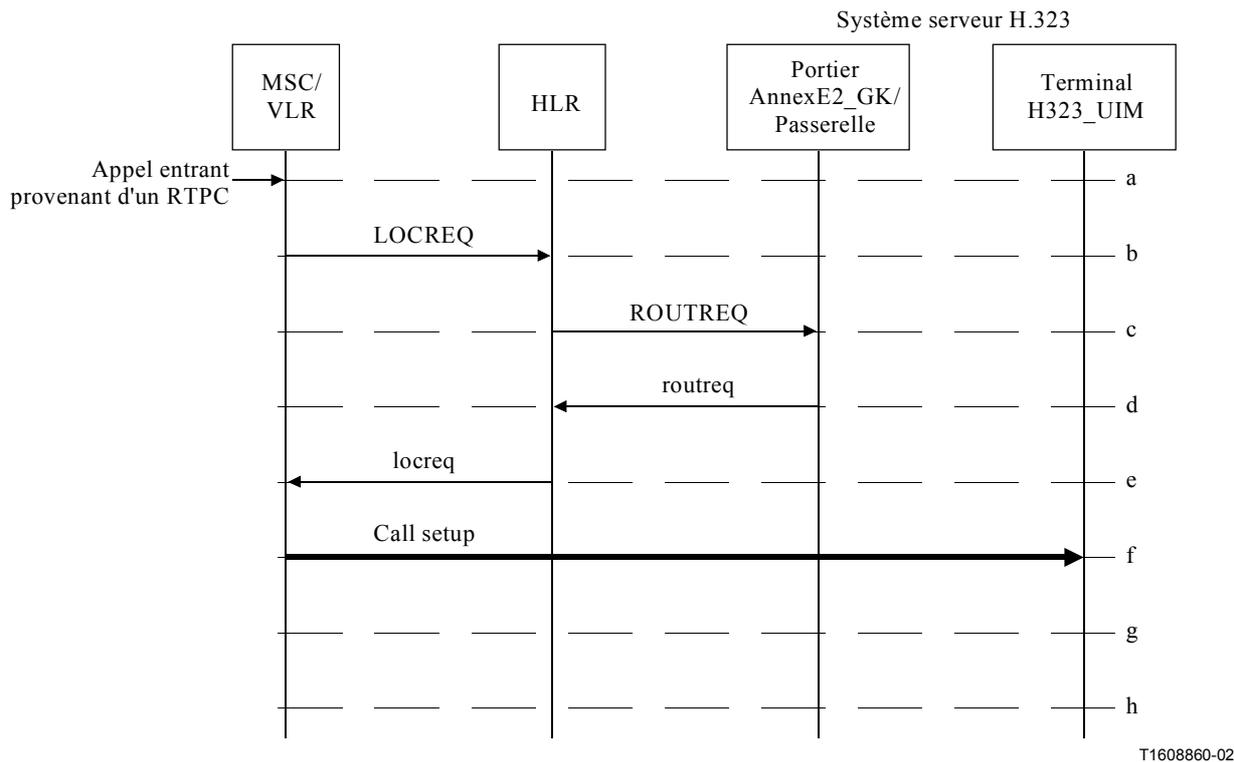


Figure E2.6/H.246 – Remise de l'appel à un abonné ANSI-41 se déplaçant dans un réseau H.323

- a) Une indication de départ d'appel et des chiffres d'adresse (numéro d'annuaire) sont reçus par le centre MSC de départ en provenance du RTPC pour un appel vers un abonné à un réseau ANSI-41.
- b) Le centre MSC de départ envoie un message LOCREQ au registre HLR associé à l'abonné appelé, cette association est faite au moyen des chiffres MS composés.
- c) Le registre HLR envoie un message ROUTREQ au portier AnnexE2_GK émulant le registre VLR où le H323_UIM associé à la station mobile MS est enregistré.
- d) Le portier AnnexE2_GK renvoie un message routreq au registre HLR qui inclut un numéro d'annuaire local temporaire TLDN, *temporary local directory number*), qui est rendu égal au numéro MSRN reçu dans le paramètre Digits (Destination). Il faut noter que le numéro MSRN est toujours au format international. On suppose que le centre MSC de la passerelle côté ANSI-41 est capable de prendre en charge des numéros TLDN au format international.
- e) Lorsque le message routreq est reçu par le registre HLR, il renvoie un message locreq vers le centre MSC de départ. Le message locreq inclut l'information d'acheminement sous la forme du paramètre TerminationList, ainsi qu'une indication du motif de prolongement de l'appel entrant (c'est-à-dire, pour remise d'appel dans le cas présent) dans le paramètre DMH_RedirectionIndicator.
- f) A la réception du message locreq, le centre MSC de départ établit un trajet vocal vers le portier AnnexE2_GK H.323 du réseau H.323 serveur (au moyen d'un protocole tel que celui de l'ISUP SS7 et des messages de commande d'appel H.225.0).

E2.13.2 Echec de remise d'appel à un abonné ANSI-41 se déplaçant dans un réseau H.323

Dans le scénario ci-après, la remise d'un appel à un abonné ANSI-41 se déplaçant dans un réseau H.323 échoue car l'utilisateur ne répond pas à un message envoyé par le système serveur pendant le traitement du message Provide Roaming Number, et que le renvoi d'appel n'est pas actif pour ledit abonné.

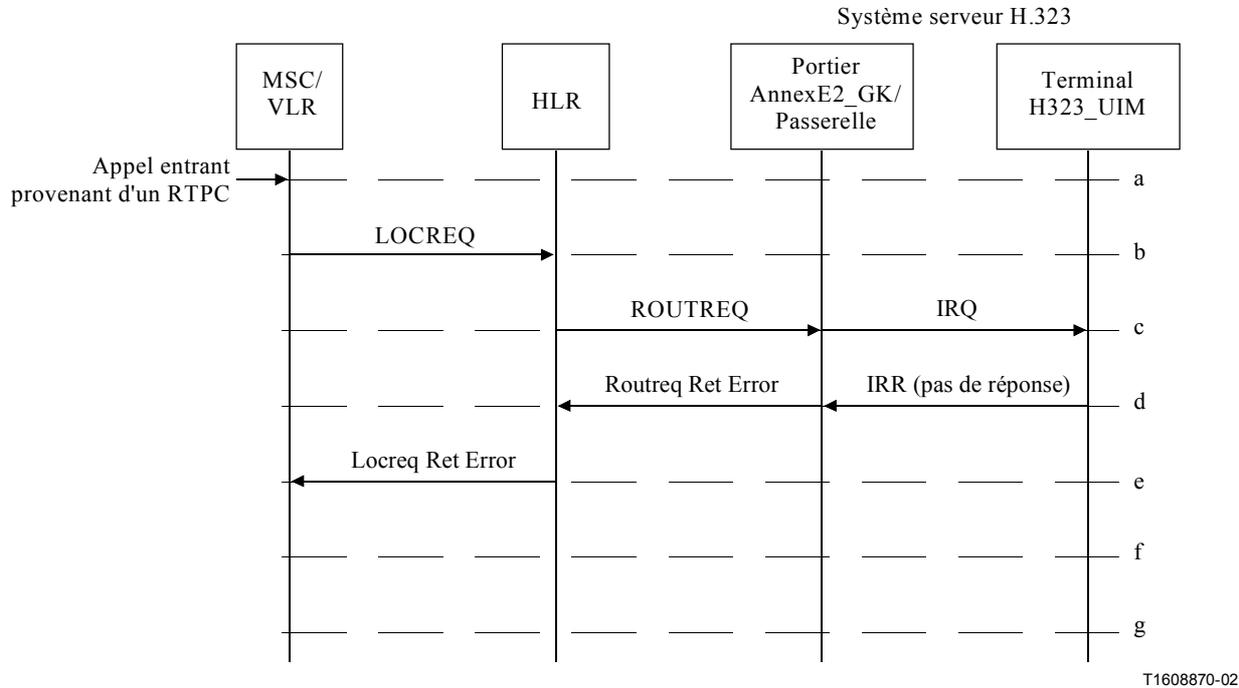


Figure E2.7/H.246 – Echec de remise à un abonné ANSI-41 se déplaçant dans un réseau H.323

- a) Une émission d'appel et les chiffres d'adresse MS composés (numéro d'annuaire) sont reçus par le centre MSC ANSI-41 depuis le RTPC à destination d'un abonné à un réseau ANSI-41.
- b) Le centre MSC ANSI-41 de départ envoie un message LOCREQ au registre HLR ANSI-41 associé à l'abonné appelé; cette association s'effectue au moyen des chiffres d'adresse du MS composés.
- c) Le registre HLR ANSI-41 envoie un message ROUTREQ au portier AnnexE2_GK émulant le registre VLR dans lequel la station mobile MS associée au H323_UIM est enregistrée. Un mappage de l'identité IMSI avec le numéro MIN est effectué si nécessaire avant traitement par le portier AnnexE2_G K. Egalement, le portier AnnexE2_G K envoie un message IRQ (Demande d'information) au terminal H323_UIM pour obtenir l'état du terminal en vue de la remise de l'appel.
- d) Le portier AnnexE2_GK envoie un message RoutingRequest RETURN ERROR dont le code d'erreur est mis à *ResourceShortage* vers le registre HLR ANSI-41 de l'abonné après avoir obtenu un IRR (pas de réponse) de la part du terminal H323_UIM.
- e) Le registre HLR ANSI-136 envoie un message LocationRequest RETURN ERROR au centre MSC ANSI-136 de départ avec un code d'erreur *SystemFailure*.

Pour les autres cas d'échec de remise d'appel, le Tableau E2.13 décrit les mappages préférés entre le H.323 et l'ANSI-41. Il convient de noter que la réponse que le portier AnnexE2_GK envoie au registre HLR ANSI-41 peut différer sur la base du code d'erreur reçu en provenance du portier AnnexE2_GK H.323 (VLR/MSC).

Tableau E2.13/H.246 – Traitement des erreurs dans le cas de remise d'un appel à un utilisateur itinérant dans les réseaux RMTP ANSI-41 et H.323

Erreur envoyée par le portier AnnexE2_GK H.246 Erreur concernant l'utilisateur	Réponse du portier AnnexE2_GK au message ROUTREQ HLR ANSI-41
Abonné absent	routreq avec AccessDeniedReason mis à <i>Unavailable</i>
Pas de numéro d'acheminement disponible	RETURN ERROR avec code d'erreur mis à <i>ResourceShortage</i>
OR non autorisé	<i>(N'entre pas dans le domaine d'application de la fonctionnalité de remise d'appel pour le GAIT Phase 1.)</i>
Fonctionnalité non prise en charge	RETURN ERROR avec code d'erreur mis à <i>SystemFailure</i>
Panne du système	RETURN ERROR avec code d'erreur mis à <i>SystemFailure</i>
Données manquantes	RETURN ERROR avec code d'erreur mis à <i>SystemFailure</i>
Unexpected Data Value	RETURN ERROR avec code d'erreur mis à <i>SystemFailure</i>

E2.14 Service de messagerie brève ANSI-136 mappé en message de commande de service de l'Annexe K H.323: réussite

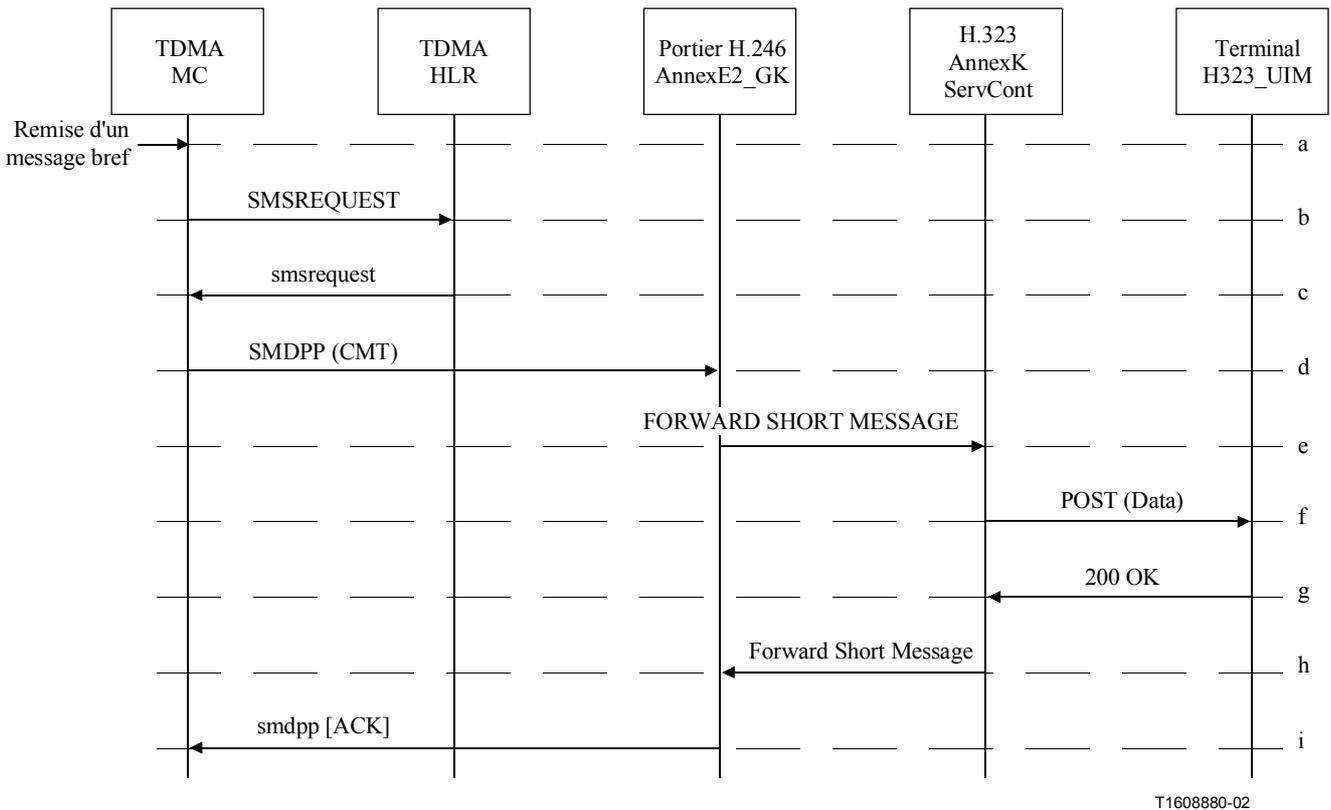


Figure E2.8/H.246 – Remise d'un message bref à un terminal H323_UIM d'abonné en déplacement dans un réseau H.323

- a) Le centre de messagerie (MC, *messsage centre*) ANSI-41 reçoit un message court destiné à un abonné particulier.

NOTE – Cette étape est indiquée uniquement dans un souci d'exhaustivité et n'est pas répétée dans les flux d'appel subséquents.

- b) Le centre de messagerie envoie un message de demande de SMS au registre HLR ANSI-41 du destinataire du message court pour demander l'adresse d'acheminement pour remettre le message court à l'abonné en question.
- c) Etant donné que l'abonné a des coordonnées valides actuelles stockées dans le registre HLR, ce registre renvoie au centre de messagerie dans le message SMS Request Return Result.
- d) Le centre de messagerie envoie alors un message point à point de remise de message court au portier H.246 AnnexE2_GK, qui est considéré comme le MSC/VLR ANSI-41 courant serveur pour l'abonné. Il convient de noter que dans ce cas le format utilisé par le centre de messagerie est au format (CMT, *cellular messaging transport*).
- e) A la réception du message point à point remise de message court en provenance du centre de messagerie ANSI-41 MC, le portier AnnexE2_GK émet un message FORWARD SHORT MESSAGE au serveur du centre de service après avoir mis le message court dans le format de commande de service Annexe K H.323.
- f) Le serveur de commande de service envoie le message POST (Données) au terminal H323_UIM Terminal.
- g) Le terminal H323_UIM accuse réception de la remise du message bref avec un message de réponse 200 OK.
- h) Le serveur du centre de service envoie le résultat dans le message Forward Short Message au portier AnnexE2_GK.
- i) Le portier AnnexE2_GK envoie le résultat du Short Message Delivery Point-to-Point au centre de messagerie ANSI-41.

E2.14.1 Traitement des erreurs à la réception d'un message Forward Short Message dans le portier H.246 AnnexE2_GK

- 1) Si un paramètre obligatoire manque (MAP V2), une erreur **Forward Short Message Return Error** avec l'indication "Data Missing" (données manquantes) au centre SMS-GMSC.
- 2) Si un paramètre obligatoire manque (MAP V1), un réjet **Forward Short Message Return Reject** avec le code d'erreur "Mistyped Parameter" (paramètre mal introduit) est envoyé au centre SMS-GMSC.
- 3) Un message **Forward Short Message Return Reject** avec le code de problème "Mistyped Parameter" (paramètre mal introduit) est envoyé dans les cas suivants:
 - a) un indicateur de paramètre n'est pas l'un de ceux associés à l'opération;
 - b) la valeur reçue n'est pas une valeur du type associé à l'opération;
 - c) étiquette et information de longueur erronées;
 - d) dépassement de la taille définie d'un module ASN.1.
- 4) Si le paramètre *SM-RP-DA* n'a pas de numéro IMSI, une erreur **Forward Short Message Return Error** avec l'indication "Unexpected Data Value" (valeur de données inattendue) est renvoyée au centre SMS-GMSC.
- 5) Si le paramètre *SM-RP-OA* n'a pas de SC, une erreur **Forward Short Message Return Error** avec indication "Unexpected Data Value" (valeur de données non attendue) est retournée au centre SMS-GMSC.
- 6) Si l'abonné n'est pas connecté dans le IIF ou si le profil n'est pas disponible, une erreur **Forward Short Message Return Error** avec l'indication "Unidentified Subscriber" (abonné non identifié) est retournée au centre SMS-GMSC.

- 7) Si un emplacement n'est pas connu ou inactif, il est renvoyé au SMS-GMSC un message **Forward Short Message Return Error** avec l'indication "Absent Subscriber" (abonné absent).
- 8) Si l'abonné a une restriction de terminaison de messagerie ANSI SMS, un message **Forward Short Message Return Error** avec l'indication "Facility Not Supported" (facilité non prise en charge) est retourné au centre SMS-GMSC.
- 9) Si le contenu du message court ne peut pas être extrait du paramètre SM-RP-UI, il est renvoyé au centre SMS-GMSC un message **Forward Short Message Return Error** avec l'indication "System Failure" (panne de système).

E2.14.2 Mappage d'un message de commande de service H.323 Annexe K en un message ANSI-136 SMDPP

Le CMT ANSI-41, transmis au VLR/MSC ANSI-41 comme étant un message **SMS Delivery Point-to-Point** (ce message contiendra les paramètres suivants):

- 1) *Numéro MIN*;
- 2) *Numéro ESN*;
- 3) *SMS Bearer Data* (données support SMS) (voir les détails ci-dessous);
- 4) *SMS Teleservice Identifier* (Identificateur du téléservice SMS) (avec la valeur CMT ou GSM Hosted SMS Teleservice);
- 5) *SMS Original Originating Address* (adresse originale de départ SMS) (avec la valeur reçue dans le paramètre *Originating Address* du message GSM SMS-DELIVER);

Le paramètre *SMS Bearer Data* envoyé dans le message **SMS Delivery Point to Point** est structuré sous forme d'un message SMS-DELIVER ANSI-136 et comporte les paramètres suivants:

- 1) *Message Type Indicator* (obligatoire): mis à la valeur "SMS-DELIVER";
- 2) *Message Reference* (obligatoire): numéro créé par le IIF et incrémenté à chaque envoi de message;
- 3) *Privacy Indicator* (obligatoire): mis à la valeur "Not restricted";
- 4) *Urgency Indicator* (obligatoire): mis à la valeur "Very Urgent" si le paramètre *Data Coding Scheme* indique "class 0 message", mis à la valeur "Normal" dans les autres cas;
- 5) *Delivery Acknowledgement Request* (obligatoire): mis à la valeur fournie;
- 6) *Manual Acknowledgement Request* (obligatoire): mis à la valeur fournie;
- 7) *Message Updating* (obligatoire): mis à la valeur "New (do not overwrite)";
- 8) *Validity* (obligatoire): mis à la valeur "Indefinite";
- 9) *Display Time* (obligatoire): mis à la valeur "Default";
- 10) *User Data Unit* (obligatoire): il contient le message lui-même et est structuré comme suit:
 - 10.1) Least Significant Byte of Length (Octet de poids le plus faible de longueur): longueur du message.
 - 10.2) Encoding Identifier (Identificateur de codage): mis à la valeur "IRA" si le message reçu utilise l'alphabet par défaut GSM, mis à la valeur "User Specific" dans les autres cas.
 - 10.3) Length Modifier (Modificateur de longueur): mis à la valeur "0".
 - 10.4) User Data Structure (Type de structure de données d'utilisateur): mis à la valeur "00".
 - 10.5) User Data (Données d'utilisateur): message SMS ANSI-41 (paramètre User Data). Si l'identificateur de codage a la valeur "IRA", convertir le message court en alphabet IRA ANSI-136.

E2.15 Notification de message en attente

E2.15.1 Terminal H323_UIM en mode ANSI-41

Pour un abonné ANSI-41 local se déplaçant dans un environnement H.323, il peut y avoir deux événements susceptibles de provoquer l'envoi par le portier H.246 AnnexE2_GK d'une notification Message Waiting Notification (MWN) utilisant la notification Message Waiting Notification H.450.7 (MWN) vers le terminal H323_UIM. Dans le premier cas, il s'agit d'un enregistrement (mise à jour de l'emplacement) s'il y a une indication dans le registre HLR ANSI-41 que les messages ont été remis à la boîte aux lettres vocale de l'abonné, le registre HLR ANSI-41 indiquera ce fait dans le message Registration Notification Return Result. Cela déclenche l'envoi par le portier H.246 AnnexE2_GK d'une information MWN H.450.7. Le deuxième événement se produit lorsque le registre HLR reçoit une notification Message Waiting Notification pour un abonné qui est déjà enregistré. Dans ce cas, le registre HLR ANSI-41 envoie un message Qualification Directive vers le portier H.246 AnnexE2_GK qui le convertira en une indication MWN H.450.7.

E2.15.2 Notification MWN via un message Qualification Directive ANSI-41 mappé en une notification MWN H.450.7

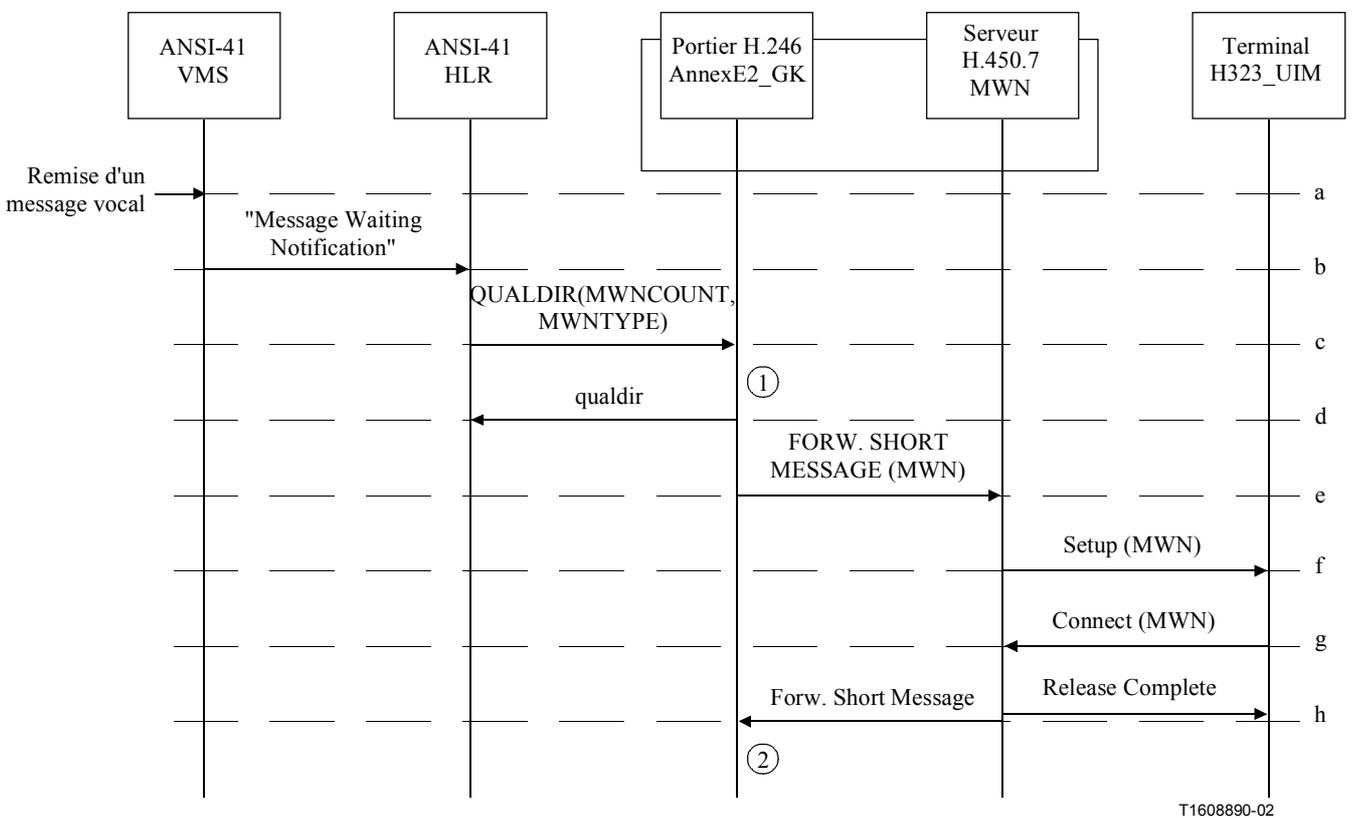


Figure E2.9/H.246 – Notification d'attente de message pour un abonné ANSI-41 se déplaçant dans des réseaux H.323: flux de messages

- Le système de messagerie vocale (VMS, *voice mail system*) ANSI-41 reçoit un message vocal pour un abonné.
- Le système VMS ANSI-41 envoie la notification "Message Waiting Notification" (MWN) au registre HLR ANSI-41 du destinataire du courrier vocal. Il convient de noter que l'interface entre le système VMS ANSI-41 VMS et le registre HLR ANSI-41 n'est pas normalisée dans la norme ANSI-41-D.

- c) Etant donné que l'abonné a un emplacement valide courant stocké dans le registre HLR, le registre HLR déclenche l'envoi d'un message Qualification Directive avec l'information MWN vers le portier AnnexE2_GK/serveur H.450.7 agissant comme MSC/VLR ANSI-41 serveur. L'information MWN se compose de deux paramètres: MessageWaitingNotificationCount (MWNCOUNT) et MessageWaitingNotificationType (MWNTYPE). On trouvera une description de ces paramètres dans les spécifications ANSI-41-D (EIA/TIA-41-5-D), Chapitre 5 (Protocoles de signalisation), Sections 6.5.2.78 et 6.5.2.79.
- ① A ce stade, le portier AnnexE2_GK/serveur H.450.7 positionne le fanion MWN. Il s'agit d'une indication que la notification MWN doit être remise au terminal H323_UIM.
- d) Le portier AnnexE2_GK/serveur H.450.7 envoie le résultat du message Qualification Directive au registre HLR ANSI-41.
- e) Le portier AnnexE2_GK/serveur H.450.7 convertit l'information MWN ANSI-41 au format MWN H.450.7.
- f) Le portier AnnexE2_GK/serveur H.450.7 envoie le message Setup avec l'information au terminal H323_UIM.
- g) Le terminal H323_UIM accuse réception de la remise de l'information MWN et efface le fanion MWN et répond par un message Connected (MWN).
- h) Le portier AnnexE2_GK/serveur H.450.7 efface le fanion MWN dans le profil d'abonné terminal H323_UIM. Il envoie également un message Release Complete au terminal H323_UIM.

La réception du Connected Message Result sans erreur et l'envoi d'un message Release complète au terminal indiquent que l'information MWN a bien été remise au terminal H323_UIM.

E2.15.3 Codage de Qualification Directive avec l'information MWN

L'information MWN est codée dans l'opération Qualification Directive (QUALDIR) au moyen des paramètres MessageWaitingNotificationCount (MWNCOUNT) et MessageWaitingNotificationType (MWNTYPE).

La Qualification Directive (ANSI-41) avec l'information MWN envoyée depuis le portier H.246 AnnexE2_GK au MSC/VLR ANSI-41 contient les paramètres suivants:

- 1) *SystemMyTypeCode* (obligatoire) (utiliser la valeur pour le fournisseur de l'IIF).
- 2) *QualificationInformationCode* (obligatoire) (mis à la valeur "Profile only").
- 3) *ElectronicSerialNumber* (obligatoire) (utiliser le numéro ESN de la station mobile).
- 4) *MobileIdentificationNumber* (obligatoire) (utiliser le numéro MIN de la station mobile).

Profile (inclus la liste des messages attendant l'information ci-dessous).

- 5) *MessageWaitingNotificationCount*
 - Octet 1: type de message (mis à 0 "Voice Messages").
 - Octet 2: nombre de messages en attente. Mis au nombre de messages vocaux en attente (valeur de 1 à 253). Si le nombre de messages vocaux est égal à 254 ou plus, indiquer la valeur 254. Si le nombre de messages vocaux est nul, le paramètre doit être mis à la valeur "no message waiting" (valeur 0). Si le nombre de messages vocaux n'est pas reçu mais que le Data Coding Scheme a la valeur "disable indication" (c'est-à-dire que le bit numéro 3 a la valeur 0) ou que Originating Address a la valeur "clear indicator" (c'est-à-dire que le bit 0 de l'octet 3 a la valeur 0) il faut positionner le nombre de messages en attente à "no message waiting" (valeur 0). Si le nombre de messages n'est pas disponible, le paramètre doit être mis à la valeur "Unknown" (valeur 255).

6) *MessageWaitingNotificationType*

- Bit 0 (A) mis à la valeur "Pip Tone notification not required" (valeur 0).
- Bit 1 (B) mis à la valeur "Alert Pip Tone notification not required" (valeur 0).
- Bit 32 (DC) mis à la valeur "MWI on" (valeur 2) si le nombre de messages est > 0 et si le nombre de messages a changé. Mis à la valeur "MWI off" (valeur 3) si le nombre de messages est nul et si le nombre de messages a changé. Si le nombre de messages n'a pas changé, mettre la valeur "No MWI" (valeur 0).

NOTE – Pour de plus amples détails, voir EIA/TIA-41-5-D § 6.4.2.31.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
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 et protocole Internet
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication