UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T Q.1721

(06/2000)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

SÉRIE Q: COMMUTATION ET SIGNALISATION

Prescriptions et protocoles de signalisation pour les IMT-2000

Flux d'informations pour l'ensemble de capacités 1 des IMT-2000

Recommandation UIT-T Q.1721

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE Q

COMMUTATION ET SIGNALISATION

SIGNALISATION DANS LE SERVICE MANUEL INTERNATIONAL	Q.1–Q.3
EXPLOITATION INTERNATIONALE AUTOMATIQUE ET SEMI-AUTOMATIQUE	Q.4–Q.59
FONCTIONS ET FLUX D'INFORMATION DES SERVICES DU RNIS	Q.60–Q.99
CLAUSES APPLICABLES AUX SYSTÈMES NORMALISÉS DE L'UIT-T	Q.100–Q.119
SPÉCIFICATIONS DES SYSTÈMES DE SIGNALISATION N° 4 ET N° 5	Q.120–Q.249
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION N° 6	Q.250–Q.309
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION R1	Q.310–Q.399
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION R2	Q.400–Q.499
COMMUTATEURS NUMÉRIQUES	Q.500–Q.599
INTERFONCTIONNEMENT DES SYSTÈMES DE SIGNALISATION	Q.600–Q.699
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION N° 7	Q.700–Q.849
SYSTÈME DE SIGNALISATION D'ABONNÉ NUMÉRIQUE N° 1	Q.850–Q.999
RÉSEAUX MOBILES TERRESTRES PUBLICS	Q.1000–Q.1099
INTERFONCTIONNEMENT AVEC LES SYSTÈMES MOBILES À SATELLITES	Q.1100–Q.1199
RÉSEAU INTELLIGENT	Q.1200–Q.1699
PRESCRIPTIONS ET PROTOCOLES DE SIGNALISATION POUR LES IMT-2000	**Q.1700–Q.1799**
RNIS À LARGE BANDE	Q.2000–Q.2999

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

RECOMMANDATION UIT-T Q.1721

FLUX D'INFORMATIONS POUR L'ENSEMBLE DE CAPACITÉS 1 DES IMT-2000

Résumé

La présente Recommandation spécifie les procédures de flux d'informations d'étape 2 pour la prise en charge de services et de capacités de réseau de l'ensemble des capacités 1 (CS-1, *capability set 1*) des IMT-2000 entre familles et entre systèmes de bout en bout. Les domaines couverts sont la gestion de la mobilité, la commande d'appel et de support, la commande de services et les services d'autorisation par voie hertzienne.

Source

La Recommandation UIT-T Q.1721, élaborée par la Commission d'études 11 (1997-2000) de l'UIT-T, a été approuvée le 15 juin 2000 selon la procédure définie dans la Résolution 1 de la CMNT.

Mots clés

CN, CS-1, IMT-2000, LMFh, LMFv, MT, NNI, RAN, UIM, VHE.

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.

La Conférence mondiale de normalisation des télécommunications (CMNT), qui se réunit tous les quatre ans, détermine les thèmes d'études à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de la CMNT.

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

TABLE DES MATIÈRES

Recommandation Q.1721

FLUX D'INFORMATIONS POUR L'ENSEMBLE DE CAPACITÉS 1 DES IMT-2000

1 Domaine d'application

La présente Recommandation fournit les flux d'informations d'étape 2 entre familles de bout en bout pour les capacités de réseau et les services de l'ensemble de capacités 1 (CS-1) des IMT-2000. Les spécifications sont conformes à la méthodologie d'étape 2 décrite dans la Recommandation UIT-T Q.65 [1]. Les Recommandations UIT-T connexes Q.1701 [2] et Q.1711 [3], forment la base de la présente Recommandation. L'utilisation conjointe de ces Recommandations forme une description de l'étape 2 qui identifie la capacité fonctionnelle et le flux d'informations nécessaires pour prendre en charge des services et des capacités réseaux de l'étape 1 des IMT-2000.

La présente Recommandation couvre les flux d'informations pour l'interface UIM-MT, l'interface MT-RAN+CN et l'interface CN-CN interface (également connue sous le nom de NNI). Les flux d'informations décrits couvrent uniquement les cas de succès. Les cas restés infructueux sortent du domaine d'application de la présente Recommandation et sont mieux traités comme partie du développement de l'étape 3. Les Recommandations connexes de la série Q, Q.1731, Q.1741 et Q.1751 complètent le point de vue bout en bout de la Recommandation Q.1721 en traitant les aspects spécifiques de ces interfaces.

La présente Recommandation n'inclut pas la gestion des ressources radio (RRM, *radio ressource management*), la gestion des stations de base (BSM, *base station management*) ou les flux d'informations. La gestion des ressources radio est traitée dans d'autres documents et les flux d'informations RAN-CN sortent du domaine d'application du CS-1 des IMT-2000 conformément au paragraphe 8.1/Q.1701.

Les alinéas qui suivent résument succinctement le contenu de chacun des paragraphes de la présente Recommandation.

Les paragraphes 2, 3 et 4 fournissent les références, les définitions et une liste d'abréviations et acronymes propres au contenu de la présente Recommandation.

Le paragraphe 5, "Introduction", apporte le contexte du reste de la présente Recommandation. Il inclut l'architecture du protocole général, l'identification des modèles fonctionnels utilisés à partir de la Recommandation Q.1711, un modèle de réseau de bout en bout, des types de séquences de flux d'informations et le modèle de flux d'informations.

Le paragraphe 6, "Gestion de la mobilité", décrit les flux d'informations pour la gestion de l'authentification, y compris la vérification du détenteur de l'UIM, l'authentification de l'utilisateur et du réseau ainsi que l'authentification du terminal. Il traite ensuite de la gestion de l'emplacement, y compris la position géographique, la gestion des données de l'abonné, l'interrogation du profil utilisateur, l'extraction de l'identité, la gestion de l'enregistrement et la reprise sur défaut de données d'emplacement.

Le paragraphe 7, "Commande d'appel et commande de support", décrit les appels de mobiles entrants et sortants, y compris la radiorecherche de terminal, le routage, les appels d'urgence et les appels prioritaires.

Le paragraphe 8, "Appel multimédia et commande de support", décrit le flux d'informations et les procédures permettant de modifier un téléservice pendant un appel (commutation entre les communications voix et données), ajouter et retirer un support dans un appel existant et changer les configurations de la communication en ajoutant et supprimant un correspondant dans un appel de données. Ce paragraphe couvre également l'accès à Internet.

Le paragraphe 9, "Environnement de rattachement virtuel", fournit le flux d'informations pour les méthodes commande directe de rattachement (DHC, *direct home command*) et commande de service de relais (RSC, *relay service control*). (L'utilisation d'un réseau intelligent (RI) pour supporter les services complémentaires dans un réseau sort du domaine d'application de la présente Recommandation.)

Le paragraphe 10, "Applications du service de messagerie", décrit les flux d'informations et les procédures pour la diffusion des messages de téléservice et la notification de message en attente.

Le paragraphe 11, "Procédure des services complémentaires", fournit les flux d'informations pour une série de procédures à usage général qui peuvent être utilisées par différents services complémentaires.

Le paragraphe 12, "Fourniture de service par voie hertzienne", décrit les flux d'informations pour la fourniture de services par voie hertzienne.

Le paragraphe 13, "Définitions des éléments d'information", définit la signification des éléments d'information dans la présente Recommandation.

L'Annexe A fournit une liste de tous les modules de procédure communs utilisés dans la présente Recommandation et le numéro du paragraphe où ils sont décrits.

L'Appendice I, "Q.1721 Couverture du Tableau 1/Q.1701, Exigences de l'ensemble de capacités 1", établit le lien entre le Tableau 1/Q.1701, les capacités requises de l'ensemble de capacités 1 des IMT-2000 et le contenu de la présente Recommandation.

L'Appendice II, "Génération de la clé A" fournit un aperçu général succinct du sujet en incluant l'algorithme Diffie-Hellman.

L'Appendice III, "Bibliographie", fournit une liste des références supplémentaires pour compléter les références spécifiques indiquées au paragraphe 2.

2 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.

[1] Recommandation UIT-T Q.65 (2000), *Méthode fonctionnelle unifiée de caractérisation des services et des capacités des réseaux avec utilisation des techniques alternatives orientées objet*.

[2] Recommandation UIT-T Q.1701 (1999), *Cadre général des réseaux IMT-2000*.

[3] Recommandation UIT-T Q.1711 (1999), *Modèle fonctionnel réseau pour les IMT-2000*.

[4] Recommandation UIT-T A.3 (1996), *Elaboration et présentation des textes et mise au point de la terminologie et des autres moyens d'expression pour les Recommandations du Secteur de la normalisation des télécommunications de l'UIT*.

[5] Recommandations UIT-T de la série Q.1200, *Réseaux intelligents*.

[6] Recommandation UIT-T E.164 (1997), *Plan de numérotage des télécommunications publiques internationales*.

[7] Recommandation UIT-T E.212 (1988), *Plan d'identification pour les stations mobiles terrestres*.

[8] Recommandation UIT-T E.213 (1988), *Plan de numérotage du réseau téléphonique et du réseau numérique avec intégration des services (RNIS) pour les stations mobiles terrestres dans les réseaux mobiles terrestres publics (RMTP)*.

[9] Recommandation UIT-T X.121 (1996), *Plan de numérotage international pour les réseaux publics pour données*.

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

[11] Recommandation UIT-T Q.762 (1997) *Système de signalisation n° 7 – Fonctions générales des messages et des signaux du sous-système utilisateur du RNIS.*

3 Définitions

La présente Recommandation définit les termes suivants:

3.1 réseau central d'ancrage: dans un environnement d'itinérance de session de données, réseau où la session de données est initiée et une passerelle de service par paquets attribuée au mobile. Le réseau central d'ancrage peut être le réseau de rattachement ou le réseau visité.

3.2 interface homme-machine: interaction de l'usager et du réseau via un dispositif d'abonné.

3.3 demande-indication: flux d'informations envoyé d'une entité fonctionnelle à une autre entité demandant une action spécifique. Il est désigné sous la forme dem. ind.

3.4 réponse-confirmation: flux d'informations envoyé par l'unité fonctionnelle demandée confirmant que l'action demandée a été effectuée avec succès. Il est désigné sous la forme rep. conf.

3.5 application de service: fourniture de services par des capacités à usage général, telles que les capacités de réseau intelligent appliquées au lieu de rattachement ou à un lieu visité, en tant que partie d'un environnement de rattachement virtuel.

3.6 commande de service: fonctions qui établissent ou modifient le contexte dans lequel les appels de base et les supports sont établis, modifiés et libérés.

3.7 abonné: utilisateur d'un terminal mobile qui a souscrit au service.

3.8 application de service complémentaire: fourniture d'un service complémentaire spécifique, normalement en utilisant des capacités spécifiques de service, du lieu de rattachement ou à un lieu visité, en tant que partie d'un environnement de rattachement virtuel.

3.9 utilisateur: utilisateur d'un terminal mobile.

3.10 environnement de rattachement virtuel (VHE, *virtual home environment*): fourniture de services à l'abonné, identiques ou simulant au mieux les services offerts à l'abonné par son lieu de rattachement.

NOTE 1 – Les termes "utilisateur" et "abonné" sont utilisés de façon interchangeable dans la présente Recommandation.

NOTE 2 – Réseau de rattachement est synonyme de réseau central de rattachement (CNh).

NOTE 3 – Réseau visité est synonyme de réseau central visité (CNv).

Le paragraphe 13, "Définitions des éléments d'information", définit la signification des différents éléments d'information dans la présente Recommandation.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations suivantes:

A-key clé d'authentification (*authentication key*)

AC centre d'authentification (*authentication centre*)

ACSM modèle d'états de contrôle d'authentification (*authentication control state model*)

ADDS service de livraison de données d'application (*application data delivery service*)

AMF fonction de gestion d'authentification (*authentication management function*)

AMSC centre d'ancrage de commutation mobile (*anchor mobile switching centre*)

AMSM modèle d'état de gestion de l'authentification (*authentication management state model*)

ARF fonction de relais de liaison d'accès (*access link relay function*)

AUTH réponse d'authentification (*authentication response*)

BCSM modèle d'états d'appel de base (*basic call state model*)

BS station de base (*base station*)

CC commande d'appel (*call control*)

CCAF' fonction agent de commande d'appel (améliorée) [*call control agent function (enhanced)*]

CCF fonction de commande d'appel (*call control function*)

CCF' fonction de commande d'appel (améliorée) [*call control function (enhanced)*]

CHCNT historique de comptage des appels (*call history count*)

CN réseau central (*core network*)

CNa réseau central (ancré) [*core network (anchored)*]

CnCAF fonction d'agent de commande de connexion (*connection control agent function*)

CnCF fonction de commande de connexion (*connection control function*)

CNdest réseau central (destination) [*core network (destination)*]

CNh réseau central (de rattachement) [*core network (home)*]

CNpv réseau central (précédemment visité) [*core network (previous visited)*]

CNs réseau central (de support) [*core network (supporting)*]

CNv réseau central (visité) [*core network (visited)*]

conf. confirmation

CS ensemble de capacités (*capability set*)

DFP plan fonctionnel réparti (*distributed functional plane*)

DHC commande directe de rattachement (*direct home command*)

FE entité fonctionnelle (*functional entity*)

FEA action d'entité fonctionnelle (*functional entity action*)

FT terminal fixe (*fixed terminal*)

GC mécanisme mise à l'épreuve globale/réponse (*global challenge/response mechanism*)

GPCF fonction de commande de position géographique (*geographic position control function*)

GPF fonction de position géographique (*geographic position function*)

ID identité

IF flux d'informations (*information flow*)

IMT-2000 Telécommunications mobiles internationales-2000 *(international mobile telecommunications-2000)*

IMUI identité internationale d'utilisateur mobile (*international mobile user identity*)

ind. indication

IP protocole Internet (*Internet protocol*)

ISP fournisseur de services Internet (*Internet service provider*)

ITDN numéro de répertoire temporaire international (*international temporary directory number*)

LMF fonction de gestion de l'emplacement (*location management function*)

LMFh fonction de gestion de l'emplacement (rattachement) [*location management function (home)*]

LMFp fonction de gestion de l'emplacement (paquet) [*location management function (packet)*]

LMFv fonction de gestion de l'emplacement (visité) [*location management function (visited)*]

LMSM modèle d'état de gestion de l'emplacement (*location management state model*)

MCF fonction de commande mobile (*mobile control function*)

MGPF fonction de position géographique mobile (*mobile geographic position function*)

MMI interface homme-machine (*man machine interface*)

MRTR réception et émission de radio mobile (*mobile radio transmission and reception*)

MSC centre de commutation de mobile (*mobile switching centre*)

MT terminal mobile (*mobile terminal*)

MWN notification de message en attente (*message waiting notification*)

NAI identificateur d'accès au réseau (*network access identifier*)

NNI interface réseau-réseau (*network-to-network interface*)

OTASP fourniture de service sur voie hertzienne (*over-the-air service provisioning*)

PDGN nœud de passerelle de données en paquets (*packet data gateway node*)

PDSN nœud serveur de données en paquets (*packet data serving node*)

PIN numéro d'identification personnel (*personal identification number*)

PSCAF fonction d'agent de commande de service par paquets (*packet service control agent function*)

PSCF fonction de commande de service par paquets (*packet service control function*)

PSGCF fonction de commande de passerelle de service par paquets (*packet service gateway control function*)

QS qualité de service

RACAF fonction d'agent de commande d'accès radio (*radio access control agent function*)

RAN réseau d'accès radio (*radio access network*)

RAND nombre aléatoire (*random number*)

RANDC nombre aléatoire (mise à l'épreuve) [*random number (challenge)*]

RANDG nombre aléatoire (global) [*random number (global)*]

req. demande (*request*)

resp. réponse (*response*)

RF radiofréquence (*radio frequency*)

RFTR réception et émission par radiofréquence (*radio frequency transmission and reception*)

RNC contrôleur de réseau radio (*radio network controller*)

RSC commande de service relais (*relay service control*)

SACF fonction de commande d'accès au service (*service access control function*)

SCF fonction de commande du service (*service control function*)

SCP point de commande de services (*service control point*)

SDF fonction de données du service (*service data function*)

SDP point de données de service (*service data point*)

SIBF fonction de diffusion d'information de système d'accès (*system access information broadcast function*)

SLP programme de logique de service (*service logic program*)

SMF fonction de gestion de service (*service management function*)

SMS service de message court (*short message service*)

SNCF fonction de commande de réseau par satellite (*satellite network control function*)

SPI indice de paramètre de sécurité (*security parameter index*)

SRES résultat de signature (*signature result*)

SRF fonction de ressource spécialisée (*specialized resource function*)

SSD données secrètes partagées (*shared secret data*)

SSF fonction de commutation de service (*service switching function*)

TMB diffusion de message de téléservice (*teleservice message broadcast*)

TMUI identificateur d'utilisateur mobile temporaire (*temporary mobile user identifier*)

TPU télécommunications personnelles universelles

UC mécanisme mise à l'épreuve unique/réponse (*unique challenge/response mechanism*)

UIM module d'identité d'utilisateur (*user identity module*)

UIMF fonction de gestion de l'identification d'utilisateur (*user identification management function*)

USSD données de service complémentaire non structuré (*unstructured supplementary service data*)

VHE environnement de rattachement virtuel (*virtual home environment*)

5 Introduction

La présente Recommandation décrit les flux d'informations pour les procédures de bout en bout entre familles des IMT-2000, qui sont nécessaires pour prendre en charge les services CS-1 IMT-2000 et les services et les capacités de réseau. La description des flux d'informations contient la liste des éléments d'information qui sont échangés entre les entités fonctionnelles. De plus, les actions des entités fonctionnelles (FEA, *functional entity action*) effectuées par l'entité réceptrice sont également décrites.

Les techniques de modélisation utilisées dans la description des flux d'informations pour les procédures IMT-2000 sont présentées ci-dessous.

Les flux d'informations spécifiés dans la présente Recommandation, pour les différents services et capacités de réseau, commandent plusieurs aspects du réseau IMT-2000 pour lequel les exigences de signalisation et de protocole doivent être spécifiées. Les prescriptions concernées sont les suivantes:

- commande de service, y compris:
  - services multimédia;
  - environnement de rattachement virtuel (VHE);
  - services de messagerie;
  - services complémentaires;
- gestion de la mobilité et contrôle d'authentification;
- contrôle d'appel;
- commande de support.

La présente Recommandation ne traite pas de la gestion des ressources radio.

L'annexe A fournit la liste des modules de procédure communs. Ces modules de base sont réutilisés dans différentes tâches qui sont composites de ces procédures de base et d'autres procédures spécifiques à ces tâches.

L'un des principes fondamentaux appliqué dans toute la présente Recommandation est la "séparation des questions". Cette séparation stricte permet une indépendance des fonctions et des protocoles pour chacun des secteurs traités en garantissant ainsi que chacun puisse évoluer et fournir des capacités plus importantes sans nécessiter que les autres secteurs soient remaniés simultanément.

Dans le cadre des réseaux IMT-2000, tels qu'ils sont spécifiés dans la Recommandation Q.1701, la Figure 5.1 reprend les limites d'application de ces séparations pour guider le développement des exigences de protocole et de signalisation des IMT-2000.

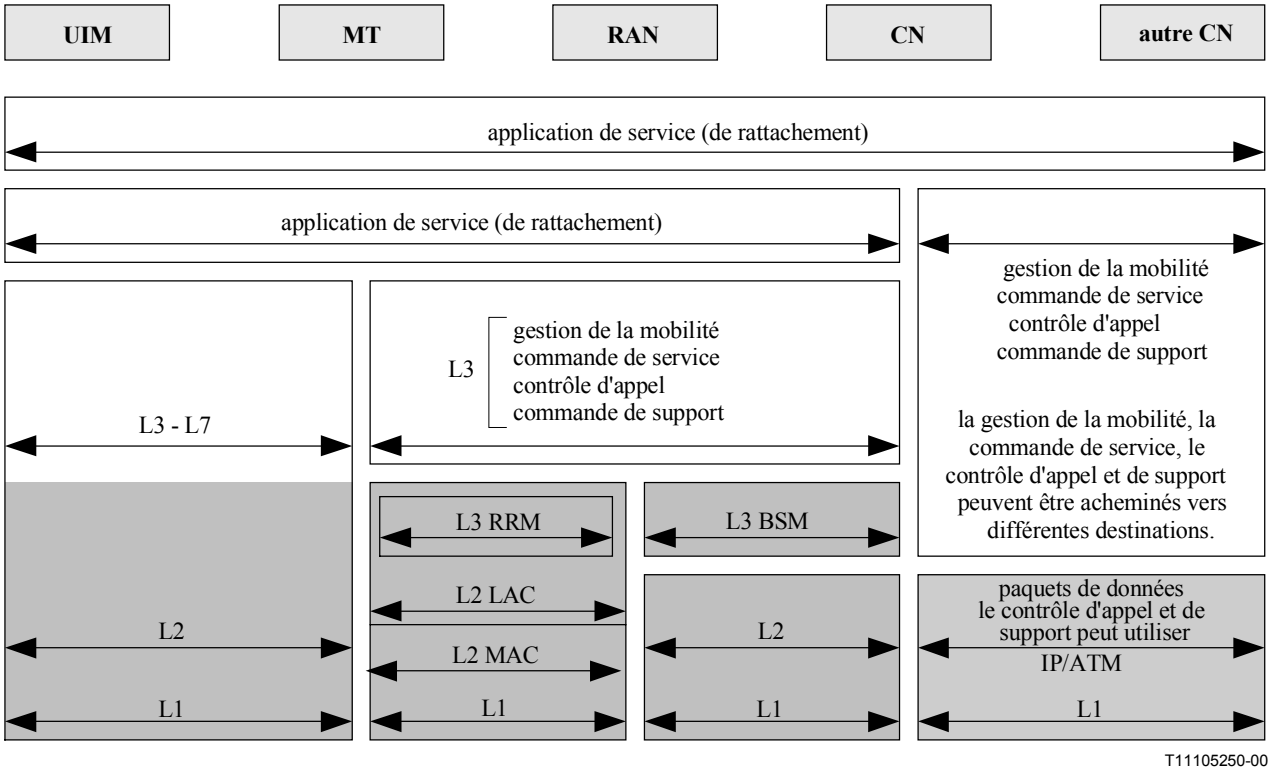


Figure 5-1/Q.1721 – Architecture générale des flux d'informations

5.1 Description des techniques de modélisation des flux d'informations

Le présent sous-paragraphe fournit deux modèles fonctionnels spécifiés dans la Recommandation UIT-T Q.1711 [3], notamment, "modèle de contrôle d'appel et de commande de connexion intégrées" et "modèle de contrôle d'appel et de commande de connexion séparées". De plus, le présent sous-paragraphe définit un modèle de relations de sous-systèmes de bout en bout.

5.1.1 Modèles fonctionnels

La Figure 5.1.1-1 est identique à la Figure 5-1a/Q.1711. Elle représente un modèle fonctionnel IMT-2000 illustrant un FE de commande d'appel et de commande de connexion intégré. Se reporter au paragraphe 6/Q.1711, pour plus de détails.

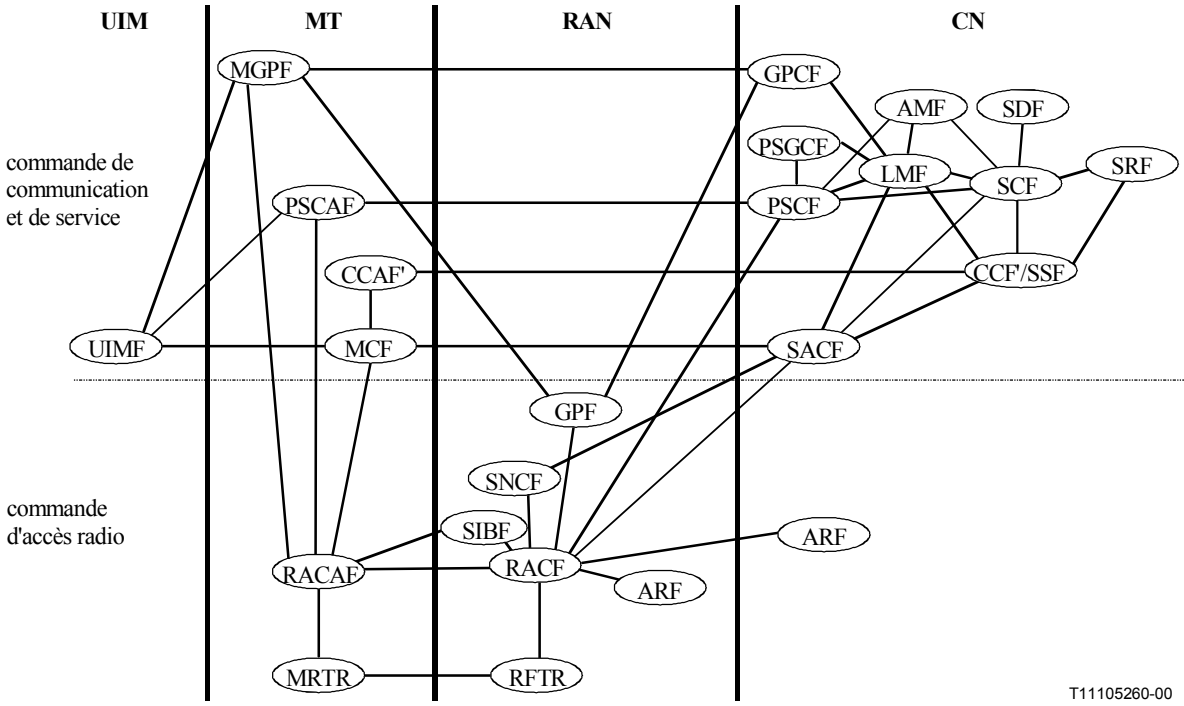


Figure 5.1.1-1/Q.1721 – Modèle fonctionnel IMT-2000 (contrôle d'appel intégré et commande de connexion)

La Figure 5.1.1-2 est identique à la Figure 5-1b/Q.1711. Elle représente un modèle fonctionnel IMT-2000 illustrant des FE de commande de connexion et de contrôle d'appel séparés. Se reporter au paragraphe 6/Q.1711, pour plus de détails.

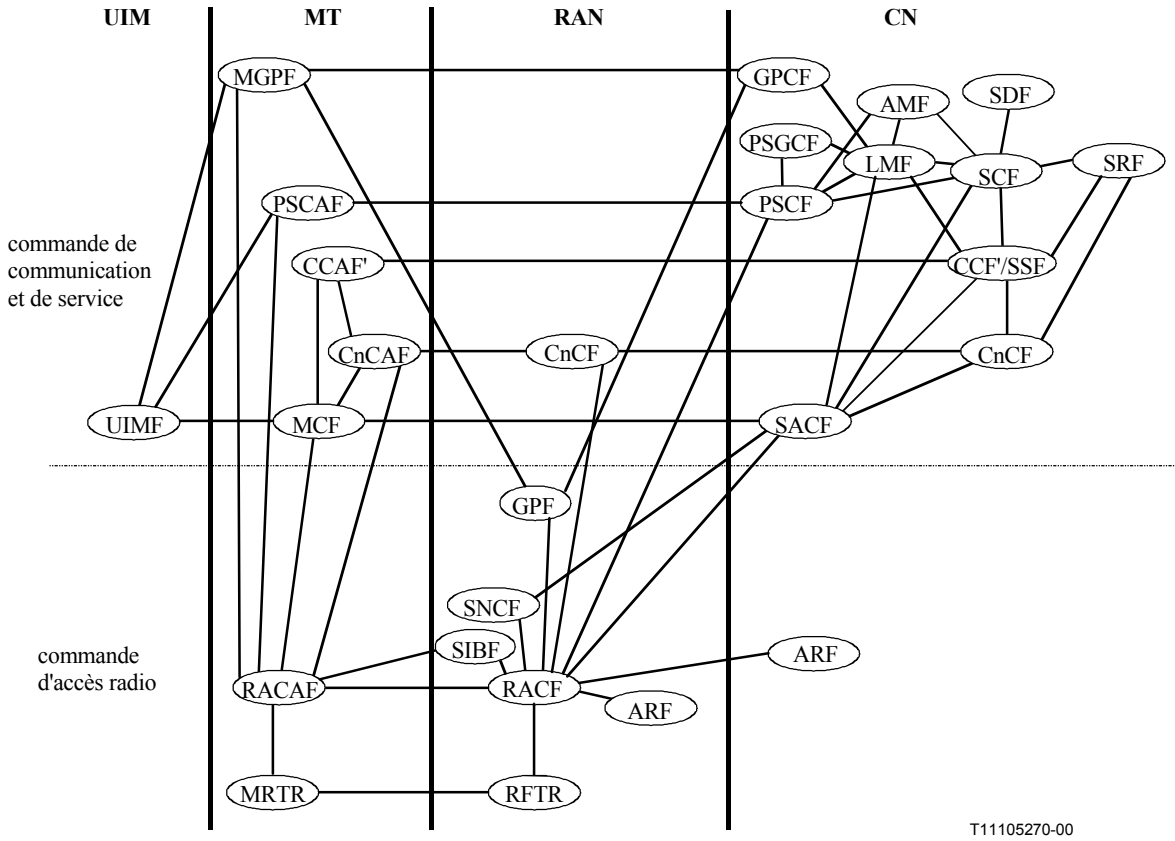
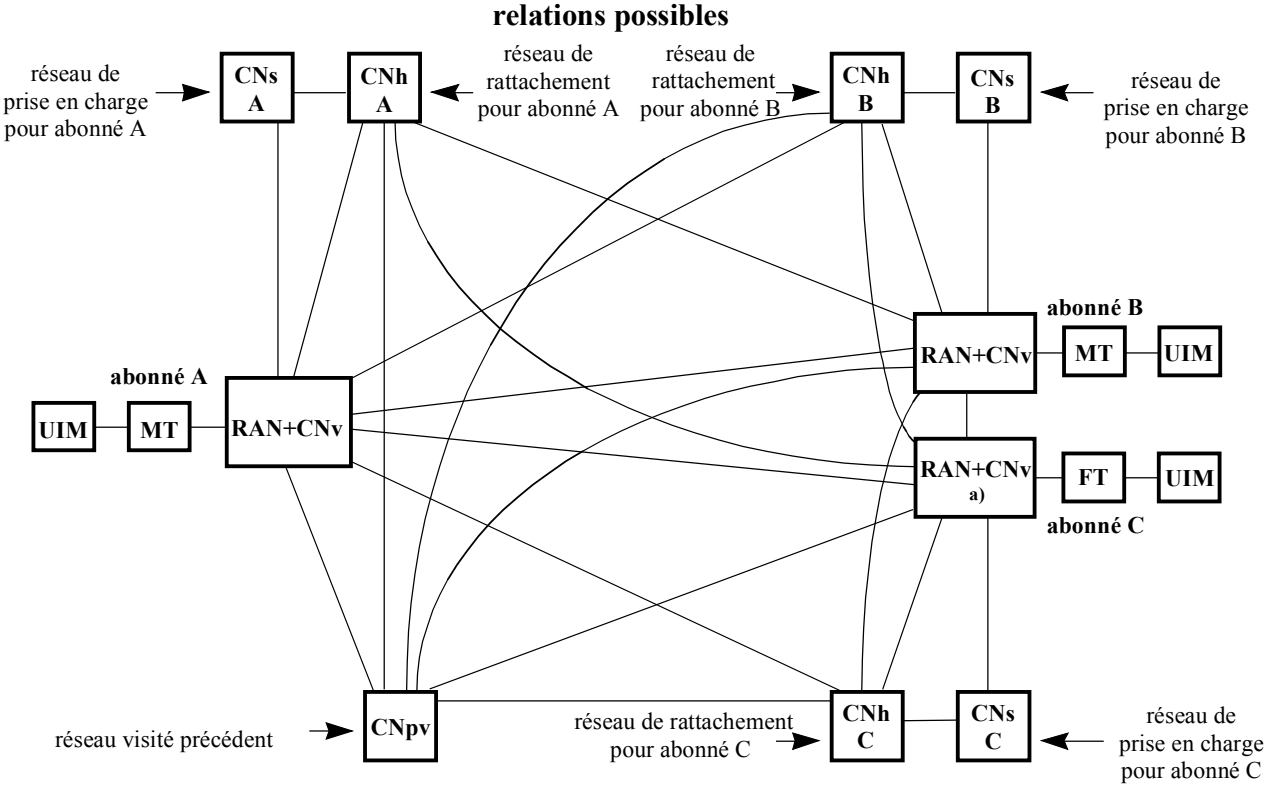


Figure 5.1.1-2/Q.1721 – Modèle fonctionnel IMT-2000 (contrôle d'appel et commande de connexion séparées)

Il convient de noter qu'un mappage des FE aux sous-systèmes UIM, MT, RAN et CN, tel que défini dans la Recommandation Q.1701, est également connu dans les modèles pour refléter l'applicabilité du concept de famille de systèmes des IMT-2000. Il convient également de noter que l'allocation des FE aux sous-systèmes RAN et CN est préliminaire (se reporter à la Recommandation Q.1711 pour plus de détails).

5.1.2 Modèle de relations entre sous-systèmes de bout en bout

Le modèle de relations de réseau fonctionnel de bout en bout illustre une optique de réseau via les sous-systèmes fonctionnels (FS, *functional subsystems*) définis dans la Recommandation Q.1701 et Q.1711 (c'est-à-dire, UIM, MT, RAN et CN) et leurs associations avec plusieurs utilisateurs. Comme l'illustre la Figure 5.1.2-1, le modèle de réseau de bout en bout contient trois points finaux d'utilisateur. Ces derniers sont utilisés pour illustrer des services plus avancés, tels que les communications conférences ou des services de support point à multipoint.



RAN+CN	réseau d'accès radio visité + réseau central
UIM	module d'identité d'utilisateur
MT	terminal mobile
CNpv	réseau central visité précédent
CNh	réseau central de rattachement
CNs	réseau central de prise en charge
FT	terminal fixe

a) Ce sous-système fonctionnel principal pourrait être remplacé par un autre sous-système réseau pour illustrer l'interfonctionnement avec d'autres réseaux tels que RTPC, RNIS, etc.

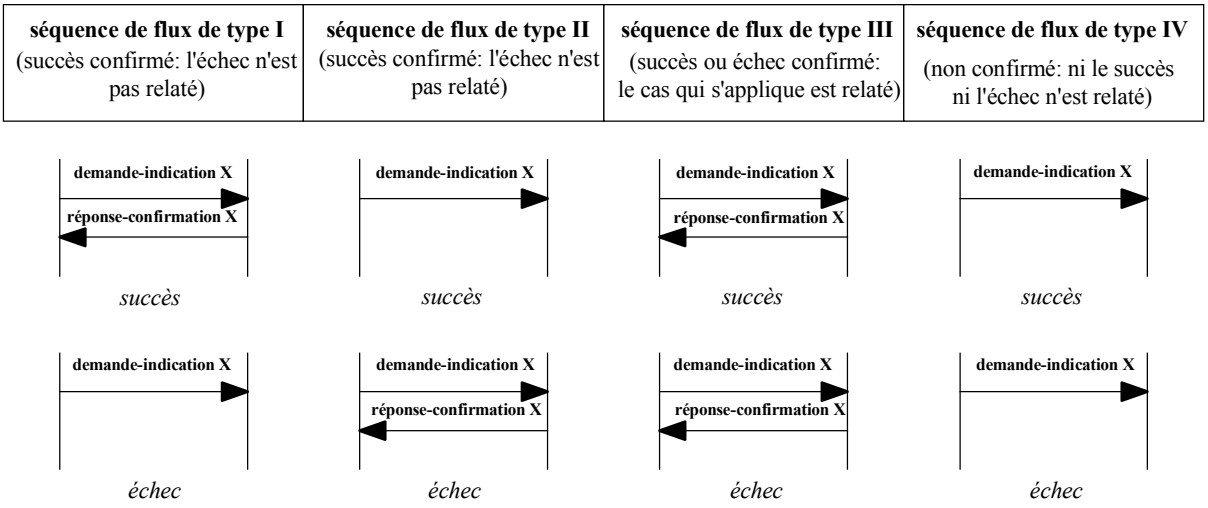
Figure 5.1.2-1/Q.1721 – Modèle de relation entre les sous-systèmes IMT-2000 de bout en bout

Le réseau central peut assumer différents rôles:

- CNpv = réseau central (précédemment visité): l'entité réseau qui a été précédemment associée au terminal mobile visité.
- CNh = réseau central (de rattachement): où la fonction de gestion de l'emplacement de rattachement (LMFh, *home location management function*) et la fonction de gestion de l'authentification (AMFh, *home authentication management function*) sont situées.
- CNs = réseau central (réseau de prise en charge): où la fonction de commande de service de rattachement (SCFh, *home service control function*), la fonction de données de service de rattachement (SDFh, *home service data function*), et la fonction de ressources spécialisées de rattachement (SRFh, *home specialized resource function*) sont situées.

5.1.3 Type de séquence de flux d'informations

Un flux d'informations se compose de deux parties: nom de la fonction du flux d'informations et type de séquence de flux. La Figure 5.1.3-1 ci-dessous illustre les types d'actions possibles.



NOTE – "X" représente le nom de la fonction de flux d'information, alors que la demande-indication est un exemple de type qui pourrait être associé au nom de la fonction de flux d'information.

T11105290-00

Figure 5.1.3-1/Q.1721 – Type de séquence de flux d'informations

La figure ci-dessus illustre quatre types de séquences de flux d'informations. Chaque type décrit le flux d'informations spécifique qui constitue ce type. Le premier type est la séquence de flux d'informations client-serveur et le résultat est un succès confirmé, avec échec non confirmé. Le second type est également une séquence de flux d'informations client-serveur mais le résultat est un échec confirmé avec succès non confirmé. Le troisième type est une notification confirmée de succès ou d'échec selon le cas. Le quatrième type est une notification non confirmée.

Le flux de "réponse-confirmation" vient en réponse à un flux "demande-indication" et transporte à ce titre une "identification de transaction" qui lui est associée. Cette "identification de transaction" est utilisée pour lier chaque paire de flux "demande-indication" et "réponse-confirmation". Par conséquent, il n'est pas nécessaire de répéter une identification d'utilisateur telle qu'une identité internationale d'utilisateur mobile IMT-2000 (IMUI, *international mobile user identity*) ou un numéro de répertoire mobile international IMT-2000 (IMDN, *international mobile directory number*) dans le flux "réponse-indication".

5.2 Modèle de flux d'informations

Le présent sous-paragraphe décrit le modèle utilisé dans le développement des procédures de flux d'informations (IF, *information flow*).

X.Y.Z "Nom de la procédure (par exemple, enregistrement d'emplacement de terminal)"

Dans le présent sous-paragraphe, donner une description succincte du service ou de la capacité réseau. "X.Y.Z" est le numéro d'en-tête du sous-paragraphe dans la Recommandation Q.1721. Le présent sous-paragraphe contient un schéma fonctionnel détaillé des flux d'informations pour le service ou la capacité de réseau utilisant le modèle fourni ci-dessous. Voir Figure 5.2-1.

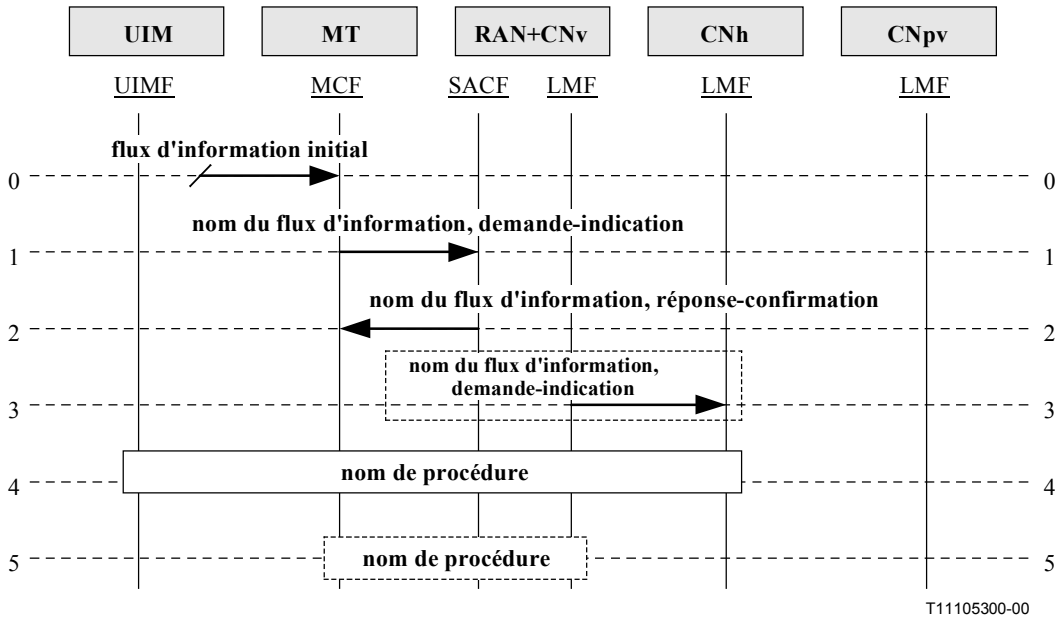


Figure 5.2-1/Q.1721 – Modèle de diagramme de flux d'informations IMT-2000

Le présent sous-paragraphe comprend des alinéas consacrés chacun à un flux d'informations du schéma des flux d'informations. Pour chaque flux d'informations, une description détaillée est fournie sur le nom du flux d'informations, son type (par exemple, demande-indication ou réponse-confirmation, les éléments d'information dans le flux d'informations, si chaque IE est obligatoire ou facultatif (M/O), dans la séquence indiquée conformément au schéma des flux d'informations. Les actions FE (FEA) sont également fournies dans le présent sous-paragraphe. Les actions communes telles que la "réception et l'analyse d'un flux" et la "génération du flux suivant" sont supposées pour chaque entité qui reçoit un flux et par conséquent ne sont pas incluses dans la description des FEA. Le format du présent sous-paragraphe se divise comme suit:

0. **Flux d'informations initial**: *décrit l'initiation de l'action de l'entité fonctionnelle (FEA) amenant au premier flux d'informations (Flux n° 1).*

FEA0	– Décrit l'action du FE à l'extrémité réceptrice de ce flux.

1. **Flux d'informations n° 1, nom du flux, type de séquence du flux**: *une description succincte du flux ainsi que son début et sa fin suivie par le contenu des éléments d'information du flux, comme l'indique le tableau ci-dessous. Lorsqu'un élément d'information (IE) est "O", les conditions de son inclusion doivent être spécifiées et la réponse à sa présence, lorsqu'elle est reçue, doit également être spécifiée. Par exemple: inclure IE n° 2 lorsque la condition xyz se produit. Pour les flux d'informations qui sont du type demande-indication, indiquer si une réponse est requise à partir d'un résultat de succès au flux d'informations reçu, un résultat d'échec, les deux ou aucun des deux, par exemple, "réponse: succès ou échec".*

Nom du flux d'informations (réponse: succès/échec/succès ou échec/aucun)	**demande-indication**
IE n°1 (par exemple, identité de l'abonné appelé)	M/O
IE n°2	M/O
IE n°3	M/O

FEA1	– Description de la/des actions des entités fonctionnelles à l'extrémité réceptrice de ce flux.
NOTE – Décrire les conditions facultatives pour les IE qui sont facultatifs.	

2. **Flux d'informations n° 2, nom du flux, type de flux**: *une description succincte du flux ainsi que son début et sa fin suivie par le contenu des éléments d'information du flux, comme l'indique le tableau ci-dessous. Lorsqu'un élément d'information (IE) est "O", les conditions de son inclusion doivent être spécifiées et la réponse à sa présence, lorsqu'elle est reçue, doit également être spécifiée. Par exemple: lorsque IE n°6 est reçu, faire wxy. Pour la réponse-confirmation, l'indication de réponse n'est pas applicable.*

Nom de l'IF	réponse-confirmation
IE n°4	M/O
IE n°5	M/O
IE n°6	M/O

FEA2	– Description de la/des actions des entités fonctionnelles à l'extrémité réceptrice de ce flux.
NOTE – Décrire les conditions facultatives pour les IE qui sont facultatifs.	

3. **Flux d'informations n° 3, nom du flux, type de séquence du flux**: *une description succincte du flux ainsi que son début et sa fin suivie par le contenu des éléments d'information du flux, comme l'indique le tableau ci-dessous. Lorsqu'un élément d'information (IE) est "O", les conditions de son inclusion doivent être spécifiées et la réponse à sa présence, lorsqu'elle est reçue, doit également être spécifiée. Par exemple: inclure IE n° 2 lorsque la condition xyz se produit. Pour les flux d'informations qui sont du type demande-indication, indiquer si une réponse est requise à partir d'un résultat de succès au flux d'informations reçu, un résultat d'échec, les deux ou aucun des deux, par exemple, "réponse: succès ou échec".*

Nom de l'IF (réponse: succès/échec/succès ou échec/néant)	demande-indication
IE n°1	M/O
IE n°2	M/O
IE n°3	M/O

FEA3	Description de la/des actions des entités fonctionnelles à l'extrémité réceptrice de ce flux.
NOTE – Décrire les conditions facultatives pour les IE qui sont facultatifs.	

4. **Flux d'informations n° 4, nom de la procédure**: *une définition brève de la procédure commune qui est suivie à cet endroit de la séquence.*

FEA4	– Description de la/des actions des entités fonctionnelles à la fin de cette procédure au niveau de l'entité fonctionnelle définie par la spécificité de la procédure proprement dite. – Si la procédure suivante est en option, comme dans ce modèle, inclure les conditions indiquant quand elle doit ou ne doit pas être effectuée.

5. **Flux d'informations n° 5, nom de la procédure**: *une définition brève de la procédure commune qui est suivie à cet endroit de la séquence.*

FEA5	– Description de la/des actions des entités fonctionnelles à la fin de cette procédure au niveau de l'entité fonctionnelle définie par la spécificité de la procédure proprement dite. – Etant donné que cette étape conclut la procédure illustrée dans ce modèle, la mention "Aucune action supplémentaire" peut être indiquée.

6 Gestion de la mobilité

Le présent paragraphe fournit les flux d'informations pour la gestion de la mobilité liée aux services et aux capacités réseau IMT-2000.

6.1 Gestion de l'authentification

6.1.1 Autorisation du détenteur d'un UIM

Il s'agit d'une fonctionnalité par laquelle l'extraction de l'UIM par l'utilisateur est autorisée. Cette fonctionnalité ne s'applique que lorsque l'UIM est utilisé pour l'association des utilisateurs aux terminaux mobiles IMT-2000. Elle est distincte de la fonctionnalité de "verrouillage" fournie par certains vendeurs de stations mobiles. Voir Figure 6.1.1-1.

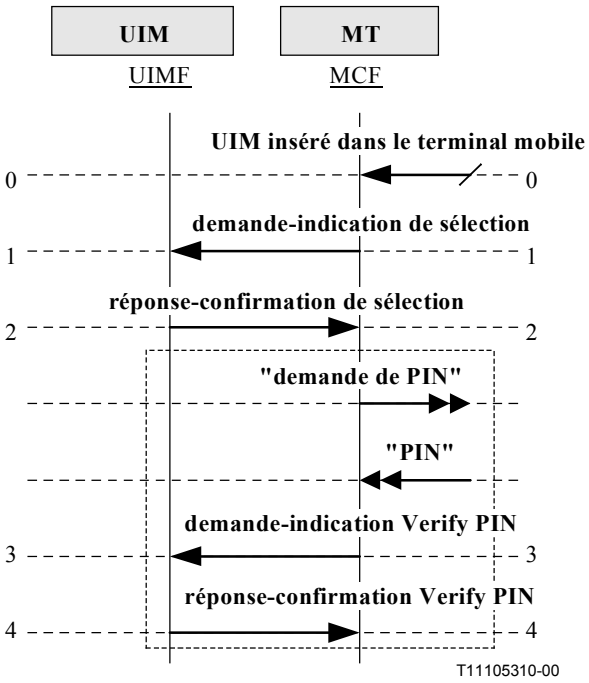


Figure 6.1.1-1/Q.1721 – Autorisation du détenteur de l'UIM

0. **UIM inséré dans le terminal mobile**: le terminal mobile avec l'UIM inséré est mis sous tension.

FEA0	– Initie la procédure de vérification du détenteur d'un UIM.

1. **Demande-indication de sélection**: est utilisée pour sélectionner le ou les fichiers appropriés dans un UIMF.

Sélection (réponse: succès ou échec)	demande-indication
Identification du fichier	M

FEA1	– Sélectionne le ou les fichiers appropriés dans l'entité UIMF.

2. **Réponse-confirmation de sélection**: constitue la réponse à la demande.

Selection	réponse-confirmation
Identification du fichier	M (Note)
Format du numéro PIN	M

FEA2	– Interagit avec l'utilisateur pour obtenir le numéro PIN.
NOTE – Système effectuant la confirmation ou système effectuant la demande s'il est différent.	

3. **Demande-indication Verify PIN**: est utilisée pour vérifier le numéro PIN.

Vérification du numéro PIN (réponse: succès ou échec)	demande-indication
PIN	M

FEA3	– Comparer le numéro PIN entré par l'utilisateur avec le numéro PIN stocké dans l'UIM.

4. **Réponse-confirmation Verify PIN**: constitue la réponse à la demande.

Verify PIN	réponse-confirmation
Résultat	M

FEA4	– Si une réponse de succès est retournée alors l'utilisateur de l'UIM est valide et le terminal est autorisé.

6.1.2 Authentification des utilisateurs

Le processus d'authentification de l'identité internationale d'utilisateur mobile (IMUI, *international mobile user identity*) est la vérification par le réseau central que l'identité IMT-2000 MT/UIM (IMUI ou TMUI) est celle revendiquée. L'authentification se compose d'un protocole de mise à l'épreuve/réponse montrant la connaissance d'une clé secrète, appelée clé d'authentification (A-key, *authentication key*), qui est partagée entre l'IMT-2000 MT/UIM et le centre d'authentification (AC, *authentication center*) dans le réseau de rattachement de l'abonné et n'est disponible qu'auprès de ces entités. L'objet de cette procédure de sécurité de l'authentification est de protéger le réseau contre les usages non autorisés.

Le réseau peut déclencher le processus d'authentification IMT-2000 dans les cas suivants:

- l'abonné s'enregistre dans un système serveur (y compris mise à jour d'emplacement, directives attachées/détachées);
- l'abonné effectue un appel;
- l'abonné répond à une radiorecherche;
- l'abonné répond à une recherche SMS;

- en fonction de la politique d'un exploitant, y compris la gestion des services complémentaires, les essais, les mises à l'épreuve périodiques d'une authentification d'utilisateur, mises à jour de données secrètes partagées (SSD, *shared secrete data*), etc.

Si une procédure d'authentification de terminal mobile échoue, l'accès au réseau IMT-2000 doit être refusé, sauf pour les appels d'urgence. Il convient de noter qu'un fournisseur de services peut en option permettre cet accès de terminal mobile au réseau lorsque l'authentification ne peut pas être effectuée par le système serveur et le LMFh/AMF de rattachement ne peut pas être atteint en raison d'une surcharge de réseau ou d'un échec.

Trois procédures d'authentification différentes sont définies pour un réseau IMT-2000: deux "mécanismes de mise à l'épreuve unique/réponse (UC, *unique challenge/response mechanism*)" et le "mécanisme de mise à l'épreuve global, (GC, *global challenge mechanism*)" conformément à la description ci-dessous. Dans le cas d'une exploitation intersystème entre différents membres de la famille des IMT-2000, le système visité initie le mécanisme d'authentification en fonction de ses capacités. Ceci implique qu'un système de rattachement prenne en charge la demande d'authentification provenant du système visité pour prendre en charge l'itinérance dans les membres de la famille des IMT-2000.

Deux procédures supplémentaires associées à la sécurité sont exécutées lorsque les procédures d'authentification de l'utilisateur ont abouti avec succès. La première est la procédure permettant de "démarrer le chiffrement", la deuxième est la procédure "d'affectation de la TMUI".

6.1.2.1 Clé d'authentification

La clé d'authentification de l'abonné (A-key, *authentication key*) doit être connue et uniquement stockée dans le terminal mobile dans le centre d'authentification de rattachement (AC). La clé d'authentification ne doit jamais être transmise par voie hertzienne ou sur le réseau et son intégrité est essentielle pour un processus d'authentification effectif.

6.1.2.2 Mécanisme d'authentification mise à l'épreuve unique/réponse basé sur des vecteurs d'authentification de triplet

Le mécanisme d'authentification de l'utilisateur mise à l'épreuve unique/réponse se compose de l'échange suivant entre le réseau visité et l'UIM.

- Le réseau visité transmet un nombre aléatoire imprévisible RAND à l'UIM.
- L'UIM calcule la signature de RAND en utilisant l'algorithme d'authentification de l'utilisateur et la clé d'authentification secrète de l'utilisateur puis transmet le résultat de la signature (SRES, *signature result*) au réseau visité.
- Le réseau visité vérifie le résultat de la signature.

Voir Figure 6.1.2.2-1.

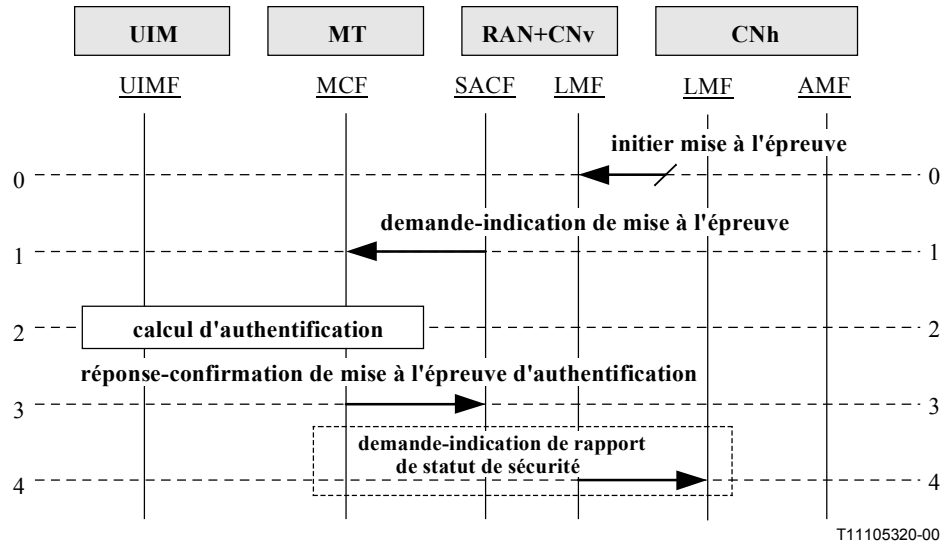


Figure 6.1.2.2-1/Q.1721 – Authentification de l'utilisateur par mise à l'épreuve unique/réponse

0. **Demande initier mise à l'épreuve**: la SACF reçoit une demande initier mise à l'épreuve. Cette demande se produit lorsque l'entité LMFv détermine que l'authentification de l'utilisateur est nécessaire.

FEA0	– Initier mise à l'épreuve d'authentification.
NOTE – La procédure de gestion facultative de la clé d'authentification est exécutée pour obtenir des triplets d'authentification si ces derniers ne sont pas disponibles. Se reporter à la procédure de gestion de la clé d'authentification pour plus de détails.	

1. **Demande-indication de mise à l'épreuve**: utilisée pour vérifier l'identité de l'utilisateur.

Mise à l'épreuve d'authentification (réponse: succès ou échec)	demande-indication
Mise à l'épreuve	M

FEA1	– Initier calcul d'authentification.

2. **Authentification**: la procédure est effectuée.

3. **Réponse-confirmation de mise à l'épreuve d'authentification**: envoyée par le MCF à la SACF pour transporter le résultat du calcul d'authentification.

Mise à l'épreuve d'authentification	réponse-confirmation
Réponse de la mise à l'épreuve	M

FEA3	– Détermine si un rapport de statut de sécurité est nécessaire.

4. **Demande-indication de rapport de statut de sécurité**: est utilisée pour envoyer un rapport de statut de sécurité au réseau de rattachement (option).

Rapport de statut de sécurité (réponse: aucune)	demande-indication
Résultat	M
IMUI	O (Note)

FEA4	– Analyse le rapport de statut de sécurité.
NOTE – L'IMUI doit être incluse lorsqu'elle est disponible.	

6.1.2.2.1 Gestion de la clé d'authentification

La clé d'authentification de l'abonné (A-key) est allouée avec l'IMUI au moment de la souscription d'un abonnement.

La clé A-key est stockée côté réseau dans le réseau de rattachement (AMFh, *home network*), dans un centre d'authentification (AC).

Un réseau IMT-2000 peut contenir un ou plusieurs AC. Un AC peut être physiquement intégré à d'autres fonctions, par exemple à un registre de l'emplacement de rattachement (LMFh, *home location register*). Un abonné peut être associé à un seul AC.

Chaque fois que nécessaire pour un MT, l'entité LMFv demande des informations associées à la sécurité à l'entité AMFh correspondant au terminal mobile. Ces informations comprennent un tableau de paires de RAND et SRES correspondants. Ces paires sont obtenues en appliquant l'algorithme d'authentification à chaque RAND et A-key. Les paires sont stockées dans l'entité LMFv en tant que partie des informations liées à la sécurité.

Pour le mécanisme unique de mise à l'épreuve, les triplets d'authentification peuvent être générés en lots par l'AMFh dans le centre d'authentification et envoyés via la LMFh à l'entité LMFv.

Voir Figure 6.1.2.2-2.

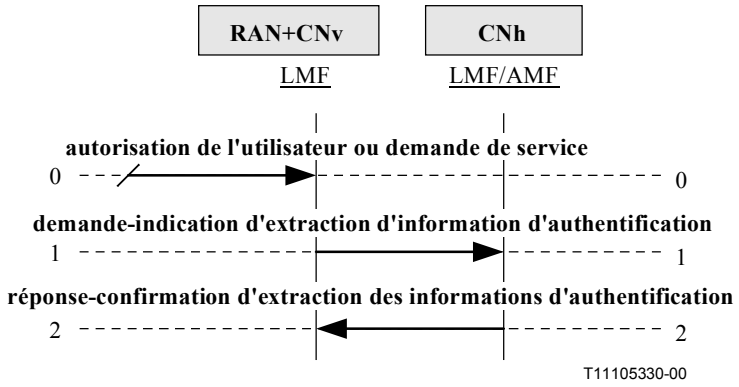


Figure 6.1.2.2-2/Q.1721 – Gestion de la clé d'authentification

0. **Autorisation de l'utilisateur ou demande de service**: l'identité de l'abonné est reçue, l'entité LMFv vérifie si une authentification de l'utilisateur est nécessaire.

FEA0	– Si les informations d'authentification dans l'entité LMFv ne sont pas suffisantes pour effectuer l'authentification, une demande d'extraction d'informations d'authentification est envoyée à la LMFh.

1. **Demande-indication d'extraction d'information d'authentification**: est utilisée pour demander les informations de sécurité à la LMFh pour l'authentification de l'utilisateur.

Extraction des informations d'authentification (réponse: succès ou échec)	demande-indication
IMUI	M

FEA1	– Extraire informations de sécurité. – Extraire mise à l'épreuve et informations de réponse pour l'authentification.

2. **Réponse-confirmation d'extraction des informations d'authentification**: contient le résultat de la demande-indication d'extraction des informations d'authentification

Information d'authentification	réponse-confirmation
Mise(s) à l'épreuve	M
Réponse(s) de mise à l'épreuve	M
Résultat	M
Clé de chiffrement	O (Note)

FEA2	– Stocke les informations d'authentification.
NOTE – Pour le mécanisme d'authentification basé sur des triplets, la clé de chiffrement doit être disponible pour certains accès réseau, par exemple, mises à jour de l'emplacement, réponses de radiorecherche, lancement d'appel, etc.	

6.1.2.2.2 Transfert de triplets d'authentification inutilisés pendant la mise à jour de l'emplacement

Lorsqu'un utilisateur se déplace dans une autre entité LMFv, les triplets inutilisés de l'entité LMFv précédente peuvent être transférés à la nouvelle entité LMFv. Cette capacité est uniquement utilisée lorsque l'authentification est effectuée en utilisant la TMUI (voir Figure 6.2.2).

6.1.2.2.3 Calcul de l'authentification

Cette procédure est initiée par le terminal mobile vers l'UIM demandant l'exécution de l'algorithme de calcul de l'authentification pour les besoins d'authentification d'une signature d'utilisateur.

NOTE – L'entité UIMF conserve la clé d'authentification qui est utilisée pour calculer le résultat de l'authentification. D'un point de vue sécurité, la clé d'authentification ne doit pas être extraite à partir de l'extérieur de cette entité fonctionnelle. Par conséquent, une procédure de demande à l'entité UIMF d'exécuter un calcul d'authentification est nécessaire. Cette procédure est une procédure commune pour les mécanismes de mise à l'épreuve unique/réponse et mise à l'épreuve globale servant à l'authentification de l'utilisateur.

Voir Figure 6.1.2.2-3.

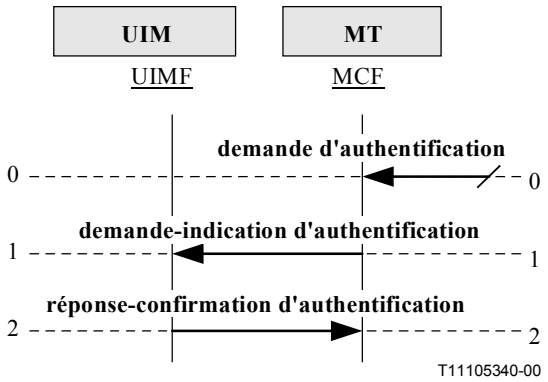


Figure 6.1.2.2-3/Q.1721 – Calcul d'authentification

0. **Demande d'authentification**: l'entité MCF reçoit une demande d'authentification.

FEA0	– Initie le calcul d'authentification.

1. **Demande-indication d'authentification**: utilisée pour demander que le calcul d'authentification soit effectué en utilisant le nombre aléatoire et la clé d'authentification.

Authentification (réponse: succès ou échec)	demande-indication
RAND	M

FEA1	– L'entité UIMF calcule la signature d'authentification en utilisant le nombre aléatoire fourni par l'entité MCF et la clé d'authentification de l'utilisateur stockée dans l'entité UIMF.

2. **Réponse-confirmation d'authentification**: est utilisée pour retourner le résultat de calcul de l'authentification.

Authentification	réponse-confirmation
Résultat de signature	M
Clé(s) de chiffrement	M

FEA 2	– Reçoit une réponse de calcul d'authentification.

6.1.2.3 Mise à l'épreuve globale

Une mise à l'épreuve globale est le message des interfaces radio (RAND) diffusé sur un canal d'information commun à l'échelle du système. Sa fréquence de génération et de mise à jour sont placées sous le contrôle de l'exploitant réseau et devront par conséquent se conformer à des pratiques d'authentification correctes.

Lors d'une tentative d'accès au réseau ou une réponse à une radiorecherche SMS, la station mobile doit inclure sa signature d'authentification. La signature d'authentification calculée repose sur les secrets qui ont été répartis pendant le processus d'abonnement. Les éléments d'information de réponse de mise à l'épreuve globale incluent, sans toutefois s'y limiter, une identification d'abonnement, une confirmation de la mise à l'épreuve globale reçue [RANDC, *random number (challenge)*], une réponse d'authentification (AUTH, *authentication response*), une valeur pour le paramètre CHCNT. Les éléments d'information qui comprennent la réponse à la mise à l'épreuve du réseau sont généralement incorporés dans les messages de demande d'accès au réseau, tels que les

enregistrements, l'origine des appels, les terminaisons d'appel ou les réponses de radiorecherche SMS. Ainsi, le mécanisme de mise à l'épreuve globale n'est pas utilisé en tant que mécanisme autonome mais accompagne d'autres protocoles d'accès au réseau afin de réduire les échanges de messages sur les canaux de l'interface air. La procédure de mise à l'épreuve globale déclenche également le calcul de clés de chiffrement qui sont ensuite utilisées pour encrypter le trafic des utilisateurs. Voir Figure 6.1.2.3-1.

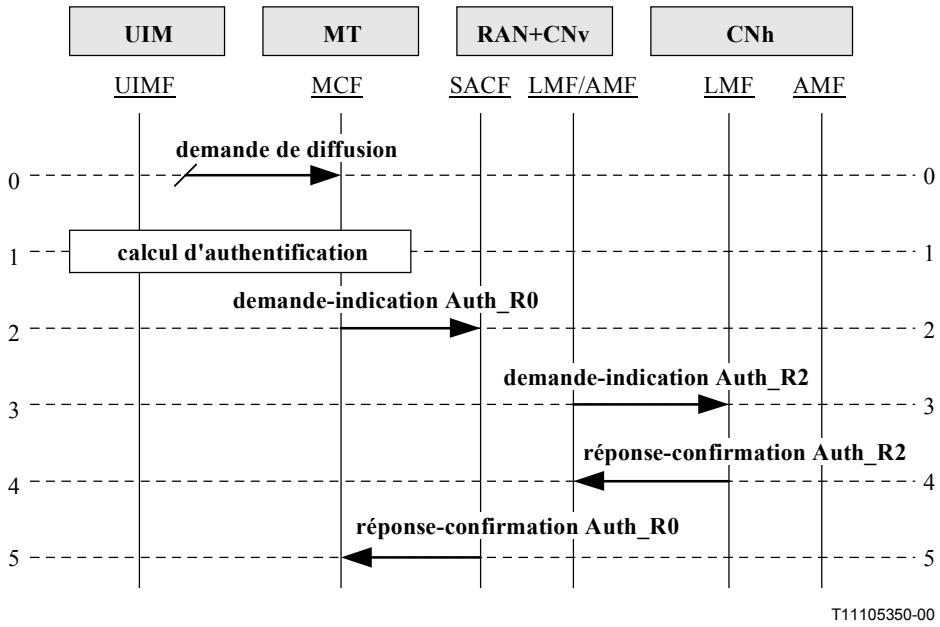


Figure 6.1.2.3-1/Q.1721 – Authentification de l'utilisateur par mise à l'épreuve globale

0. **Demande de diffusion**: lors de la tentative d'accès au système par le terminal mobile, la "mise à l'épreuve globale" est lue à partir du canal de diffusion des informations système.

FEA0	– La "mise à l'épreuve" globale de diffusion est obtenue par la station mobile à partir d'un canal sémaphore commun puis appliquée à l'algorithme d'authentification dans l'entité UIMF, avec les informations secrètes de l'utilisateur pour calculer la signature d'authentification de l'entité UIMF (AUTH_R). – Initie le calcul d'authentification.

1. **Calcul d'authentification**: ce calcul est effectué.

2. **Demande-indication Auth_R0**: utilisée en tant que composant d'une procédure d'enregistrement ou de demande de service.

Auth_R0	**demande-indication**
TMUI	M
Confirmation de RAND (RANDC)	M
AUTH_R	M
CHCNT	M

FEA2	– Vérifie que la Confirmation de RAND (c'est-à-dire, RANDC) est cohérente avec le RAND global reçu sur le canal d'information du système. – Obtention du SSD utilisateur de l'entité LMFv du système serveur. – Si la clé SSD n'est pas disponible dans le réseau visité, envoie la réponse d'authentification à l'entité LMFh, y compris le RAND global complet au lieu du RANDC. – Effectue la procédure d'authentification de l'utilisateur. – Calcule les clés de chiffrement applicables.
NOTE – L'entité LMFv prend en charge le mécanisme de mise à l'épreuve globale en participant à la génération et à la distribution du RAND global qui est diffusé par le réseau serveur sur un canal d'information à l'échelle du système. Les mises à jour du RAND global sont contrôlées par le système serveur.	

3. **Demande-indication Auth_R2**: utilisée pour transmettre la demande d'authentification au réseau de rattachement.

Auth_R2 (réponse: succès ou échec)	**demande-indication**
IMUI	M
RANDG	M
AUTH_R	M
CHCNT	M

FEA3	– Calcule la ou les clés de chiffrement applicables. – Effectue la procédure d'authentification de l'utilisateur. – Envoie la confirmation de la validité de l'utilisateur avec la ou les clés de chiffrement applicables, et dans certains cas la clé SSD, à l'entité LMFv.

4. **Auth_R2 réponse-confirmation**: constitue la réponse fournissant l'information de sécurité demandée.

Auth_R2	**réponse-confirmation**
Résultat	M
SSD	O (Note 1)
Clé(s) de chiffrement	O (Note 2)

FEA4	– Envoie la confirmation de la validité de l'utilisateur avec la ou les clés de chiffrement applicables et, dans certains cas, la clé SSD, à l'entité MCF.
NOTE 1 – Si le partage de SSD est activé par l'entité LMFh/AMF, le paramètre SSD peut être inclus dans ce message. NOTE 2 – Retourné si disponible.	

5. **Réponse-confirmation Auth_R0**: transporte la réponse à la demande-indication Auth_R0 à l'entité MCF.

Auth_R0	Réponse-confirmation
Résultat	M

FEA 5	– Reçoit une confirmation de statut du réseau en tant que composant de tentative d'accès au système.

6.1.2.4 Gestion de la clé SSD

6.1.2.4.1 Mise à jour des données secrètes partagées de l'utilisateur (mise à jour de la clé SSD)

Afin de réduire le trafic réseau entre le système serveur et l'AMF de rattachement, tout en fournissant une protection supplémentaire à la clé A-key, une deuxième d'authentification appelée données secrètes partagées (SSD, *shared secret data*), est dérivée de la clé d'authentification de l'abonné. La procédure de mise à jour de la clé SSD, par laquelle la clé SSD du terminal mobile est partagée avec un système serveur peut être exécutée à tout moment à la discrétion du fournisseur de service "de rattachement". Le processus de mise à jour de la clé SSD sera uniquement initié après une authentification réussie du terminal mobile. Voir Figure 6.1.2.4.1-1.

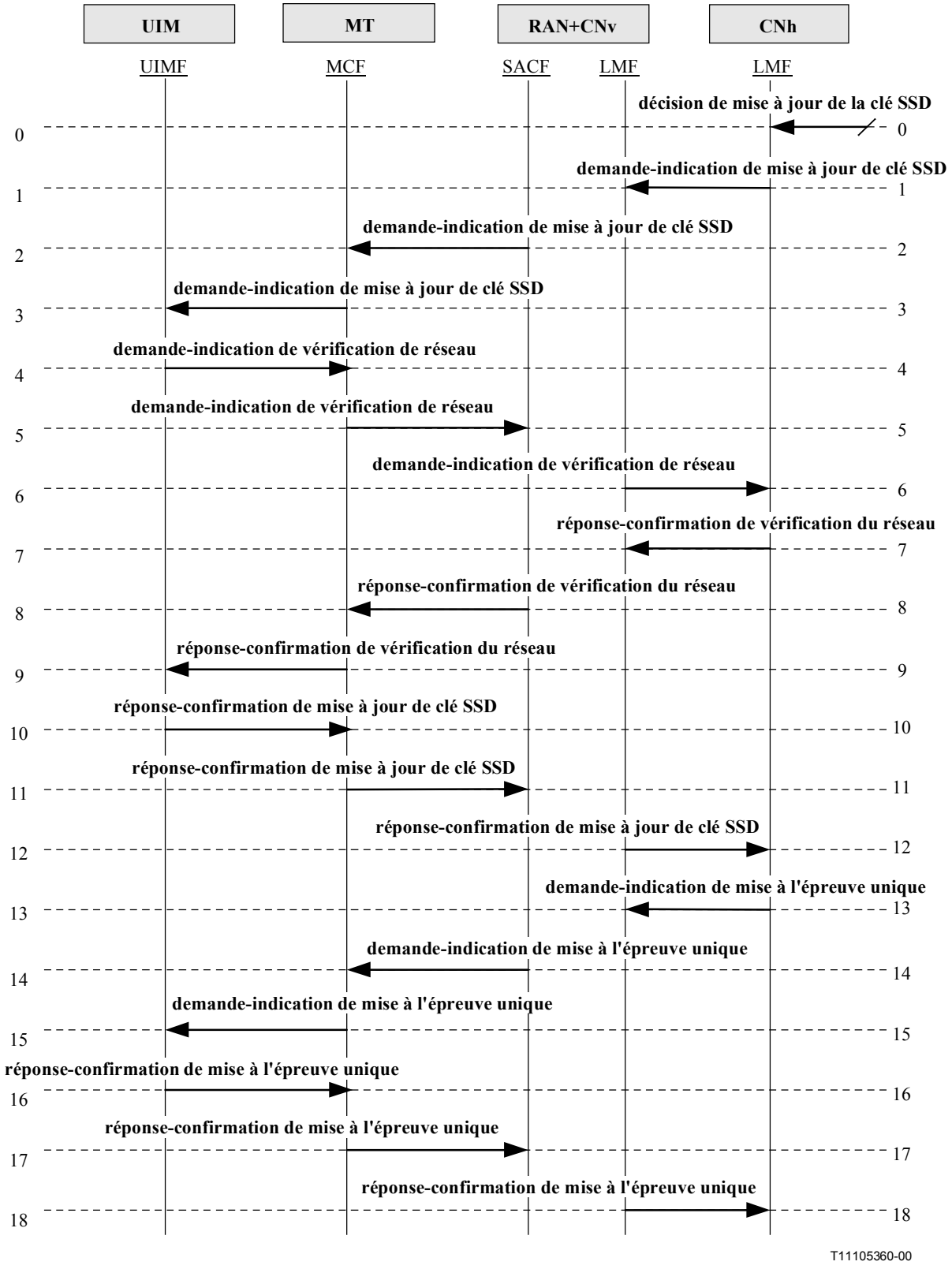


Figure 6.1.2.4.1-1/Q.1721 – Mise à jour de clé SSD (la clé SSD n'est pas partagée)

0. **Décision de mise à jour de la clé SSD**: lance l'exécution de la procédure de mise à jour de la clé SSD pour un utilisateur mobile sélectionné dans le réseau visité.

FEA0	– Génère un nombre aléatoire RANDSSD. – Calcule la nouvelle clé SSD pour l'utilisateur mobile. – Génère un nombre aléatoire RANDU et calcule AUTH_U en utilisant la nouvelle clé SSD. – Envoie la demande-indication de mise à jour de la clé SSD à l'entité LMFv en demandant que l'utilisateur mobile sélectionné effectue une mise à jour immédiate de sa clé SSD.

1. **Demande-indication de mise à jour de clé SSD**: ordonne à l'UIMF de mettre à jour sa valeur de clé SSD. Cette demande-indication est envoyée depuis le système de rattachement vers le système visité où l'utilisateur mobile est situé. Pour que cette procédure soit exécutée, il est nécessaire que l'UIM (extractible ou permanent) soit présent dans le terminal mobile.

Mise à jour de clé SSD (réponse: succès ou échec)	**demande-indication**
IMUI	M
RANDSSD	M
RANDU	M
AUTH_U	M
Clé(s) de chiffrement	O (Note)

FEA1	– Reçoit une demande-indication de mise à jour de clé SSD de l'entité LMFh, effectue une traduction IMUI/TMUI et l'envoie à l'entité MCF.
NOTE – Les clés de chiffrement sont envoyées si elles sont disponibles.	

2. **Demande-indication de mise à jour de clé SSD**: ordonne à l'utilisateur mobile de mettre à jour sa valeur de clé SSD. Elle est envoyée du système de rattachement vers le système visité où l'utilisateur mobile est situé. Pour que cette procédure soit exécutée, il est nécessaire que l'UIM (extractible ou permanent) soit présent dans le terminal mobile afin d'interagir avec le réseau.

Mise à jour de clé SSD (réponse: succès ou échec)	**demande-indication**
IMUI	M
RANDSSD	M

FEA2	– Relaie la demande-indication de mise à jour de clé SSD provenant du réseau visité.

3. **Demande-indication de mise à jour de clé SSD**: ordonne à l'utilisateur mobile de mettre à jour sa valeur de SSD. Cette demande-indication est relayée par le système visité.

Mise à jour de clé SSD (réponse: succès ou échec)	**demande-indication**
IMUI	M
RANDSSD	M

FEA3	– Calcule une nouvelle valeur SSD (provisoire). – Génère un nombre aléatoire RANDBS qui sera utilisé dans le flux d'informations de vérification du réseau. – Calcule l'AUTHBS attendu en utilisant la nouvelle valeur SSD (provisoire). – Envoie la demande-indication de vérification de réseau à l'entité MCF (pour authentifier et vérifier le réseau).

4. **Demande-indication de vérification de réseau**: amène le réseau à s'authentifier et se vérifier auprès du mobile. Cette demande-indication provient de l'UIM.

Vérification du réseau (réponse: succès ou échec)	demande-indication
TMUI	M
RANDBS	M

FEA4	– Relaie la demande-indication de vérification du réseau de l'entité UIMF.

5. **Demande-indication de vérification de réseau**: relayée au réseau visité par l'entité MCF.

Vérification du réseau (réponse: succès ou échec)	demande-indication
TMUI	M
RANDBS	M

FEA5	– Effectue la traduction IMUI/TMUI.

6. **Demande-indication de vérification de réseau**: relayée par le système visité au système de rattachement pour les besoins d'authentification du réseau.

Vérification du réseau (réponse: succès ou échec)	demande-indication
IMUI	M
RANDBS	M

FEA6	– Génère l'AUTHBS en utilisant la nouvelle clé SSD.

7. **Réponse-confirmation de vérification de réseau**: la réponse du réseau de rattachement au flux d'informations de la demande-indication de vérification du réseau.

Vérification du réseau	réponse-confirmation
AUTHBS	M

FEA7	– Effectue la traduction IMUI/TMUI.

8. **Réponse-confirmation de vérification de réseau**: est relayée par le système visité.

Vérification du réseau	réponse-confirmation
AUTHBS	M

FEA8	– Relaie la réponse-confirmation de vérification du réseau.

9. **Réponse-confirmation de vérification de réseau**: est relayée par le système mobile à l'UIM.

Vérification du réseau	réponse-confirmation
AUTHBS	M

FEA9	– Compare l'AUTHBS reçu à l'AUTHBS attendu. – Prépare une confirmation satisfaisant/non satisfaisant. – Met à jour la mémoire avec la nouvelle clé SSD si la procédure a réussi.

10. **Réponse-confirmation de mise à jour de clé SSD**: la réponse de l'UIM à la demande-indication de mise à jour de clé SSD.

Mise à jour de clé SSD	réponse-confirmation
Résultat	M

FEA10	– Relaie la réponse-confirmation de mise à jour de clé SSD.

11. **Réponse-confirmation de mise à jour de clé SSD**: la réponse au flux d'informations de la demande-indication de mise à jour de clé SSD.

Mise à jour de clé SSD	réponse-confirmation
Résultat	M

FEA11	– Confirmation du processus

12. **Réponse-confirmation de mise à jour de clé SSD**: la réponse au flux d'informations de la demande-indication de mise à jour de clé SSD.

Mise à jour de clé SSD	réponse-confirmation
Résultat	M

FEA12	– Prépare à envoyer une demande-indication de mise à l'épreuve unique à l'utilisateur mobile dans le réseau visité.

13. **Demande-indication de mise à l'épreuve unique**: active le réseau pour déterminer si le mobile sélectionné peut ou non mettre à jour avec succès sa clé SSD.

Mise à l'épreuve unique (réponse: succès ou échec)	demande-indication
IMUI	M
RANDU	M
AUTH_U	M

FEA13	– Effectue la traduction IMUI/TMUI.

14. **Demande-indication de mise à l'épreuve unique**: est envoyée de l'UIMF au terminal mobile.

Mise à l'épreuve unique (réponse: succès ou échec)	demande-indication
TMUI	M
RANDU	M
AUTH_U	M

FEA14	– Relaie la demande-indication de mise à l'épreuve unique.

15. **Demande-indication de mise à l'épreuve unique**: est envoyée à l'entité UIMF.

Mise à l'épreuve unique (réponse: succès ou échec)	demande-indication
TMUI	M
RANDU	M
AUTH_U	M

FEA15	– Calcule la réponse d'authentification AUTH_U en utilisant la nouvelle clé SSD.

16. **Réponse-confirmation de mise à l'épreuve unique**: constitue la réponse à la demande-indication de mise à l'épreuve unique et contient la réponse d'authentification.

Mise à l'épreuve unique	réponse-confirmation
AUTH_U	M

FEA16	– Relaie la réponse-confirmation de mise à l'épreuve unique.

17. **Réponse-confirmation de mise à l'épreuve unique**: est envoyée à RAN+CNv.

Mise à l'épreuve unique	réponse-confirmation
AUTH_U	M

FEA17	– Effectue la traduction IMUI/TMUI.

18. **Réponse-confirmation de mise à l'épreuve unique**: est envoyée au réseau de rattachement.

Mise à l'épreuve unique	réponse-confirmation
AUTH_U	M

FEA18	– Met à jour les données de l'utilisateur mobile à partir des informations de statut reçues. – Si le statut est satisfaisant, stocke la nouvelle valeur SSD pour être utilisée dans les exécutions ultérieures de la procédure d'authentification et permet à l'abonné mobile de continuer avec l'origine de l'appel et la terminaison d'appel. La clé SSD peut être éventuellement partagée avec une entité LMFv, si ce partage est permis par des accords entre fournisseurs de services.
NOTE – L'entité LMFh met à jour les données de l'utilisateur mobile à partir des informations reçues. Si l'authentification n'a pas échoué, elle permet ensuite à l'utilisateur mobile de continuer avec l'origine de l'appel et la terminaison de l'appel. De plus, elle transfère la clé SSD à l'identité LMFv lorsque des accords entre fournisseurs de services le permettent. Si le statut est satisfaisant, elle met à jour la clé SSD courante et essaye à nouveau de mettre à jour la clé SSD de l'utilisateur mobile lors d'une transaction ultérieure.	

6.1.2.4.2 Invocation du partage de la sécurité

L'invocation de partage de la sécurité est utilisée pour invoquer le partage des informations de sécurité associées à un utilisateur IMT-2000 particulier.

Scénario:

a) le système de rattachement d'un abonné détermine que le partage de la sécurité doit être activé et étend (partage) les informations de sécurité au système visité;

b) le système visité active le partage de la sécurité et répond au système de rattachement en indiquant le succès ou l'échec.

Voir Figure 6.1.2.4.2-1.

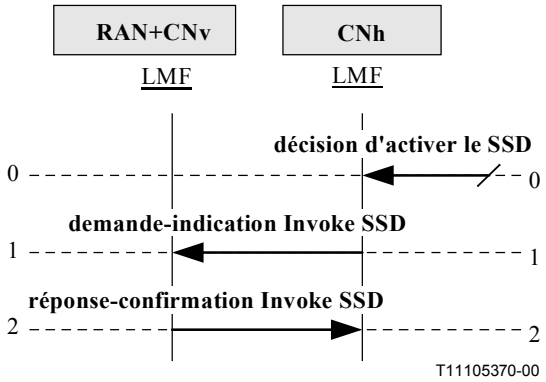


Figure 6.1.2.4.2-1/Q.1721 – Schéma des flux d'informations d'invocation de partage de la sécurité

0. **Décision d'activer le SSD**: décide d'activer le partage de données secrètes entre le système de rattachement et visité.

FEA0	– L'entité LMFh détermine que le partage de la sécurité doit être activé et envoie une demande Invoke_security_sharing *(invocation de partage de la sécurité)* à l'entité LMFv avec l'information de sécurité à partager.

1. **Demande-indication Invoke_security_sharing**: cette demande-indication est utilisée pour invoquer le partage des informations de sécurité au niveau du système visité.

Invoke_security_sharing (réponse: succès ou échec)	demande-indication
IMUI	M
SSD	M

FEA1	– L'entité LMFv reçoit la demande, active le partage de la sécurité et indique en retour le succès ou l'échec.

2. **Réponse-confirmation Invoke_security_sharing**: la réponse au flux d'informations de la demande-indication Invoke_security_sharing.

Invoke_security_sharing	réponse-confirmation
Résultat	M

6.1.2.4.3 Révocation du partage de la sécurité

La révocation du partage de la sécurité est utilisée pour révoquer les informations de partage de la sécurité au niveau du système visité.

Scénario:

a) le système de rattachement d'un abonné détermine que le partage de la sécurité doit être désactivé et informe le système visité;

b) le système visité désactive le partage de la sécurité et répond au système de rattachement avec l'historique de comptage d'appel s'il est disponible en indiquant le succès ou l'échec.

Voir Figure 6.1.2.4.3-1.

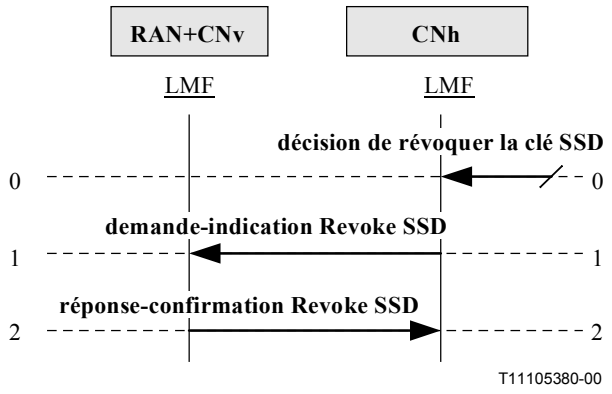


Figure 6.1.2.4.3-1/Q.1721 – Schéma des flux d'informations de révocation de partage de la sécurité

0. **Décision de révoquer la clé SSD**: décide d'activer le partage de données secrètes entre le système de rattachement et visité.

FEA0	– L'entité LMFh détermine que le partage de la sécurité doit être désactivé et envoie une demande Revoke_security_sharing à l'entité LMFv.

1. **Demande-indication Revoke_security_sharing**: cette demande-indication est utilisée pour révoquer le partage des informations de sécurité au niveau du système visité.

Revoke_security_sharing (réponse: succès ou échec)	demande-indication
IMUI	M

FEA1	– L'entité LMFv reçoit la demande, désactive le partage de la sécurité et indique en retour le succès ou l'échec.

2. **Réponse-confirmation Revoke_security_sharing**: constitue la réponse au flux d'informations de demande-indication Revoke_security_sharing.

Revoke_security_sharing	réponse-confirmation
Résultat	M
CHCNT	O (Note)
NOTE – Le CHCNT est renvoyé s'il est disponible.	

6.1.2.5 Activer chiffrement

Cette procédure fournit le cryptage des flux de données sur l'interface radio pour empêcher un accès non autorisé aux informations. Le chiffrement est initié dans le terminal mobile (et l'entité LMFv) uniquement après un processus d'authentification réussi. Voir Figure 6.1.2.5-1.

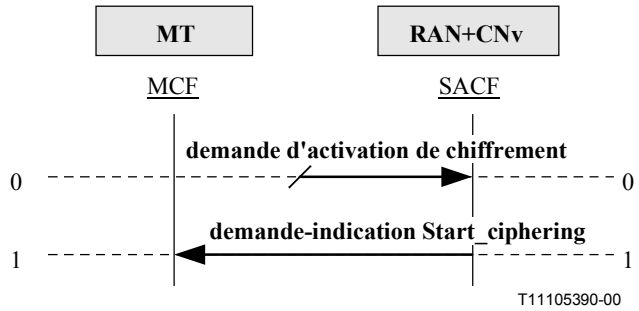


Figure 6.1.2.5-1/Q.1721 – Schéma des flux d'informations d'activation du chiffrement

0. **Demande d'activation de chiffrement**: la demande d'activation de chiffrement est reçue.

1. **Demande-indication Start_ciphering**: est utilisée pour activer la commande de chiffrement sur l'interface radio.

Activation du chiffrement (réponse: néant)	demande-indication
Néant	N/A

FEA1	– Active la commande de chiffrement sur l'interface radio.

6.1.2.6 Attribution de la TMUI

Une TMUI possède une signification locale uniquement dans la zone d'emplacement dans laquelle l'utilisateur est enregistré. En dehors de cette zone, il convient que la TMUI soit accompagnée par

une identification de zone d'emplacement appropriée (LAI, *location area identification*) afin d'éviter les ambiguïtés. L'association entre les identités d'utilisateur permanentes et temporaires est conservée par l'entité LMFv dans laquelle l'utilisateur est enregistré.

La TMUI, lorsqu'elle est disponible, est normalement utilisée pour identifier l'utilisateur sur la voie d'accès radio, par exemple dans les demandes de radiofréquence, les demandes de mise à jour d'emplacement, les demandes d'attachement, les demandes de service, les demandes de rétablissement de connexion et les demandes de détachement.

Cette procédure est utilisée pour attribuer et transférer la TMUI à l'UIM après que le réseau a vérifié l'identité de l'utilisateur. Il convient de l'effectuer après l'initiation du chiffrement. Voir Figure 6.1.2.6-1.

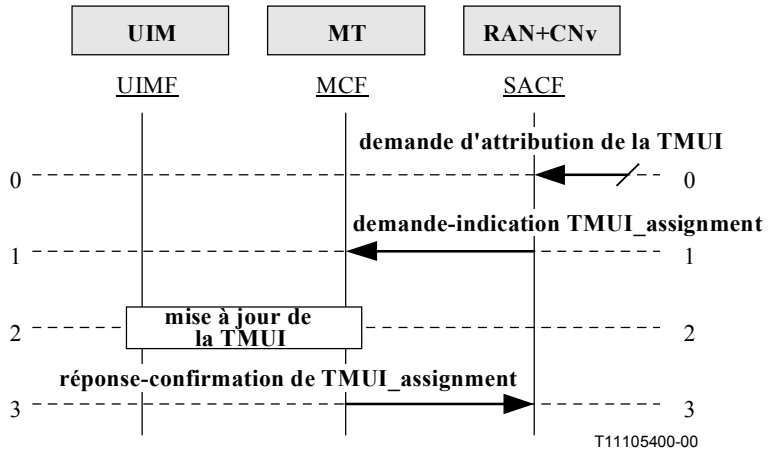


Figure 6.1.2.6-1/Q.1721 – Schéma des flux d'informations d'attribution de la TMUI

0. **Demande d'attribution de la TMUI**: est reçue.

FEA0	– Extrait l'identité de la source d'attribution de la TMUI et facultativement le temporisateur d'expiration de la TMUI. – Envoie demande-indication d'attribution de la TMUI.

1. **Demande-indication TMUI_assignment**: cette demande-indication est utilisée pour attribuer et transférer la TMUI à l'utilisateur après que le réseau a vérifié l'identité de l'utilisateur.

TMUI_assignment (réponse: succès ou échec)	**demande-indication**
TMUI	M
Identité de la source d'attribution de la TMUI	M
Temporisateur d'expiration de la TMUI	O (Note)

FEA1	– Initie le module de procédure de mise à jour de la TMUI.
NOTE – Inclus si une valeur autre qu'une valeur d'expiration par défaut fixée par le réseau doit être utilisée.	

2. **Réponse-confirmation de TMUI_assignment**: indique que la procédure de mise à jour de la TMUI a été exécutée.

FEA2	– Analyse le résultat de mise à jour de la TMUI et le rapporte au réseau visité.

3. **Réponse-confirmation de TMUI_assignment**: constitue la réponse à la demande-indication TMUI_assignment.

TMUI_assignment	**réponse-confirmation**
Résultat	M

FEA3	Remarquer la réponse. Aucune action supplémentaire n'est requise.

6.1.2.7 Historique de comptage des appels

6.1.2.7.1 Mise à jour de l'historique de comptage d'appels

La procédure de mise à jour de l'historique de comptage d'appels est utilisée pour mettre à jour l'historique de comptage d'appels (CHCNT, *call history count*) dans le système visité, le terminal mobile et l'UIM. Voir Figure 6.1.2.7.1-1.

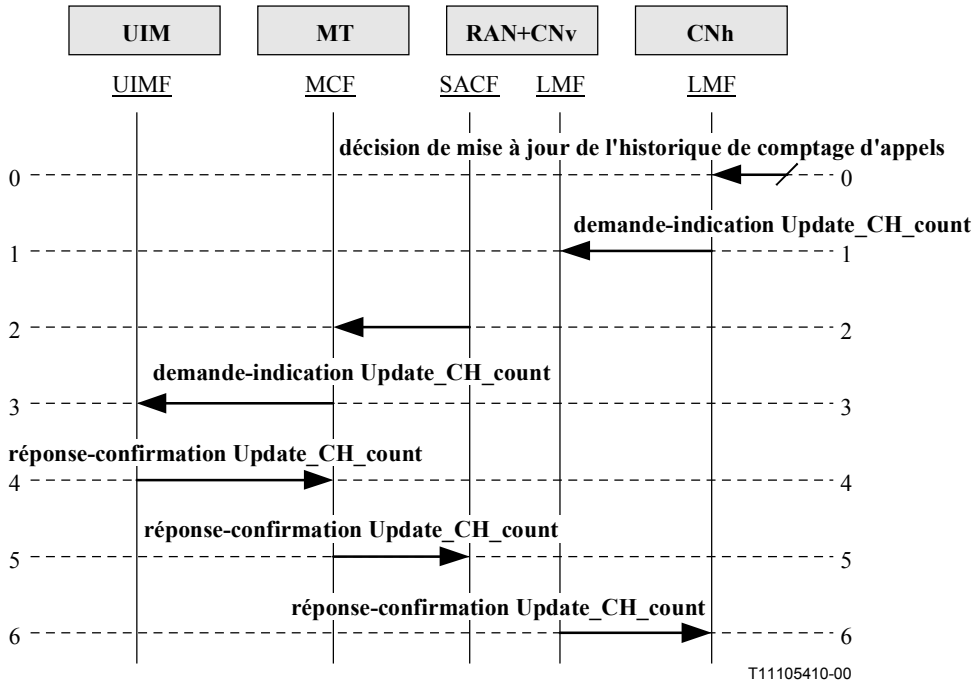


Figure 6.1.2.7.1-1/Q.1721 – Schéma des flux d'informations de mise à jour de l'historique de comptage d'appels

0. **Décision de mise à jour de l'historique de comptage d'appels**: le système de rattachement détecte la nécessité de mettre à jour l'historique de comptage des données et envoie une demande au système visité pour mettre à jour l'historique de comptage d'appels.

FEA0	– Extrait les paramètres appropriés et initie la procédure de mise à jour de l'historique de comptage d'appels.

1. **Demande-indication Update_CH_count**: est utilisée pour demander la mise à jour de l'historique de comptage d'appels dans le système visité.

Update_CH_count (réponse: succès ou échec)	demande-indication
IMUI	M
Update_CH_count	M

FEA1	– Mise à jour des données de l'historique de comptage d'appels.

2. **Demande-indication Update_CH_count**: est envoyée à l'entité MCF.

Update_CH_count (réponse: succès ou échec)	demande-indication
IMUI	M
Update_CH_count	M

FEA2	– Mise à jour de données de l'historique de comptage d'appels dans le terminal mobile.

3. **Demande-indication Update_CH_count**: est envoyée à l'UIMF.

Update_CH_count (réponse: succès ou échec)	demande-indication
IMUI	M
Update_CH_count	M

FEA3	– Mise à jour des données de l'historique de comptage d'appels dans l'UIM.

4. **Réponse-confirmation Update_CH_count**: constitue la réponse à la demande de l'UIMF.

Update_CH_count	réponse-confirmation
CHCNT	M
Résultat	M

FEA4	– Relaie le résultat à l'entité MCF.

5. **Update_CH_count réponse-confirmation**: constitue la réponse à la demande de l'entité MCF.

Update_CH_count	réponse-confirmation
CHCNT	M
Résultat	M

FEA5	– Relaie le résultat à l'entité SACF dans le système visité.

6. **Réponse-confirmation Update_CH_count**: constitue la réponse à la demande du système visité.

Update_CH_count	réponse-confirmation
CHCNT	O (Note 1)
Résultat	M

FEA6	– Relaie le résultat au système de rattachement.
NOTE – Envoie le CHCNT au système de rattachement si nécessaire.	

6.1.2.7.2 Procédure de demande de l'historique de comptage d'appels

Lorsque le paramètre CHCNT est utilisé, le réseau de "rattachement" a besoin d'interroger le réseau visité pour obtenir la valeur courante de CHCNT afin que le réseau serveur courant puisse l'utiliser. Le réseau serveur courant peut être le réseau de "rattachement" ou un autre réseau "visité". Voir Figure 6.1.2.7.2-1

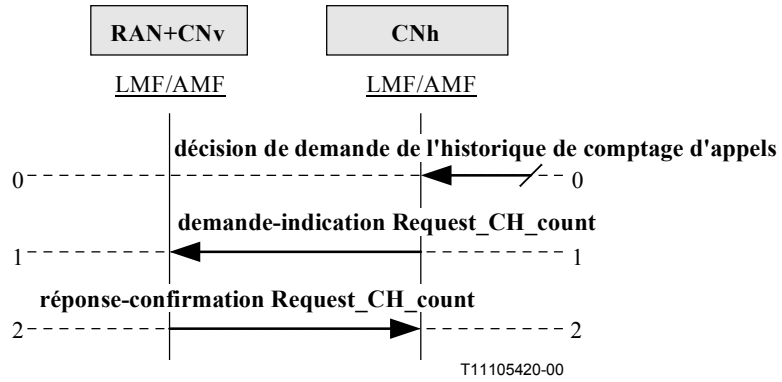


Figure 6.1.2.7.2-1/Q.1721 – Schéma des flux d'informations de l'historique de comptage d'appels

0. **Décision de demande de l'historique de comptage d'appels**: le système de rattachement détecte le besoin d'interroger le réseau précédemment visité pour obtenir la valeur courante de CHCNT afin que le réseau serveur courant puisse l'utiliser.

FEA0	– Initie la procédure de demande de CHCNT.

1. **Demande-indication Request_CH_count**: est utilisée pour demander la valeur courante de CHCNT au réseau précédemment visité.

Request_CH_count (réponse: succès ou échec)	demande-indication
IMUI	M

FEA1	– Accède à la valeur courante de CHCNT pour l'utilisateur et l'envoie au système de rattachement.

2. **Réponse-confirmation Request_CH_count**: constitue la réponse à la demande.

Request_CH_count	réponse-confirmation
CHCNT	M

FEA2	– Reçoit le CHCNT pour l'utilisateur du système précédemment visité et le stocke pour une utilisation ultérieure.

6.1.2.8 Authentification de mise à l'épreuve unique – Basée RANDU

Le HLR/AC de rattachement ainsi que le système serveur peut déclencher ce type de processus UC (si le SSD est partagé). Un nombre aléatoire est sélectionné par le système serveur (RANDU) et une réponse d'authentification attendue, basée sur le SSD du mobile, est produite par l'algorithme d'authentification. A la réception de la mise à l'épreuve (c'est-à-dire, RANDU), le terminal mobile calcule à son tour sa propre signature d'authentification en utilisant son SSD et le même algorithme d'authentification. La signature d'authentification est renvoyée au système serveur (ou l'AC) où elle est vérifiée en la comparant à celle attendue. Si les deux signatures correspondent, l'authentification est réussie.

Le processus d'UC peut être en option utilisé pour (ré)authentifier un terminal mobile, pour authentifier des services complémentaires ou en tant que partie du processus de mise à jour de la clé SSD. Voir Figure 6.1.2.8-1.

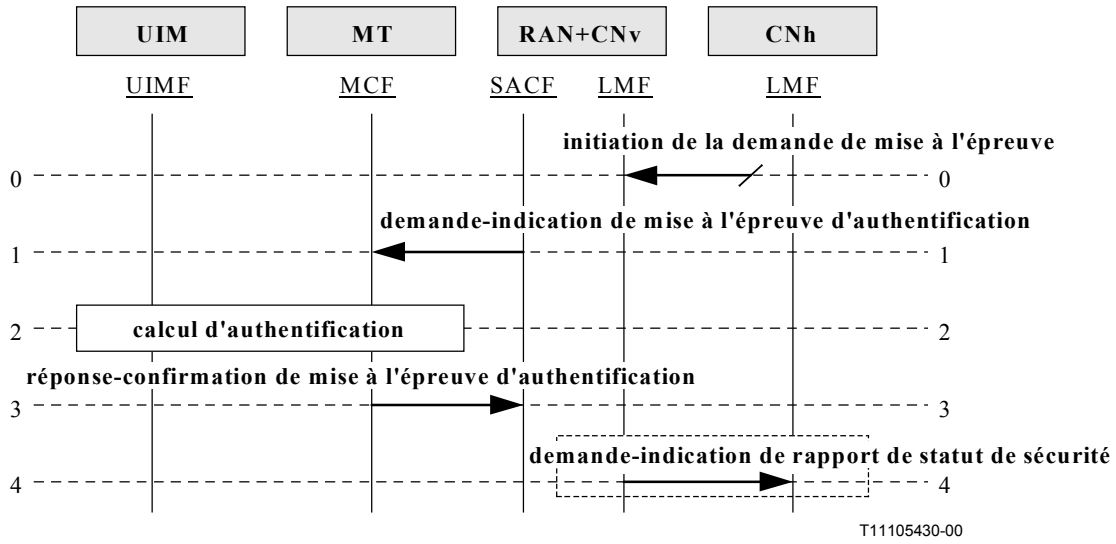


Figure 6.1.2.8-1/Q.1721 – Authentification de l'utilisateur par mise à l'épreuve unique/réponse (clé SSD partagée)

0. **Initiation de la demande de mise à l'épreuve**: l'entité SACF reçoit une demande d'initiation de mise à l'épreuve après que l'entité LMFv soit déclenchée pour initier un processus d'authentification UC.

FEA0	– Initie la mise à l'épreuve d'authentification. – Génère la mise à l'épreuve – RANDU et l'envoie à l'utilisateur.

1. **Demande-indication de mise à l'épreuve d'authentification**: est envoyée pour vérifier l'identité de l'utilisateur.

Mise à l'épreuve d'authentification (réponse: succès ou échec)	demande-indication
RANDU	M

FEA1	– Calcule la signature d'authentification attendue AUTHU.

2. **Calcul d'authentification**: est exécutée.

3. **Réponse-confirmation de mise à l'épreuve d'authentification**: envoie la signature d'authentification basée sur RANDU.

FEA2	– Reçoit AUTHU. – Vérifie la validité d'AUTHU.

4. **Demande-indication de rapport de statut de sécurité**: est utilisée pour envoyer un rapport de sécurité au réseau de rattachement (facultatif).

Rapport de statut de sécurité (réponse: néant)	demande-indication
Résultat	M
IMUI	O (Note)

FEA5	– Analyse le rapport de statut de sécurité.
NOTE – L'IMUI doit être incluse si elle est disponible.	

6.2 Gestion de l'emplacement

6.2.1 Gestion des données de l'abonné

Les procédures de gestion des données de l'abonné sont utilisées par l'entité LMFh pour changer ou supprimer certaines données de l'abonné du profil de l'abonné dans l'entité LMFv si la souscription d'un ou plusieurs services de base ou complémentaires a été modifiée ou retirée. On peut donc l'envisager comme une modification "autonome" du profil de l'abonné dans le système visité, c'est-à-dire, qui n'est pas en conjonction avec une mise à jour de l'emplacement.

NOTE – Les termes "utilisateur" et "abonné" utilisés dans le présent sous-paragraphe sont interchangeables.

On supposera dans tout le présent paragraphe que les informations suivantes sont stockées dans le réseau de rattachement de l'abonné/le réseau de prise en charge et sont le sujet des activités de gestion de profil et d'information de l'abonné:

- numéro de répertoire mobile IMT-2000 (IMDN), par exemple un numéro composable;
- identification de l'utilisateur mobile IMT-2000 (IMUI);
- identité internationale d'équipement mobile (IMEI, *international mobile equipment ID*);
- information d'emplacement de l'utilisateur;
- données de service de base (par exemple, services support souscrits);
- téléservices (par exemple, données de diffusion et de souscription d'appels de groupe);
- données de sécurité;
- données de services complémentaires;
- fonctionnalités/services déterminés par l'exploitant (par exemple, données d'interdiction d'appel);
- fonctionnalités/services déterminés par l'abonné (par exemple, données de filtrage d'appel);

- données de restriction d'itinérance;
- données d'abonnement régional;
- données d'abonnement VHE.

6.2.1.1 Modification du profil de l'abonné

6.2.1.1.1 Modification du profil de l'abonné, Cas 1: copie du profil de l'abonné

Les données de profil de l'abonné ont été modifiées et les modifications ont été reflétées dans l'entité LMFv. Dans ce cas, la procédure de "Copie de profil de l'abonné " peut être utilisée. Cette procédure écrase toutes les valeurs existantes des paramètres par leurs nouvelles valeurs correspondantes. Voir Figure 6.2.1.1-1.

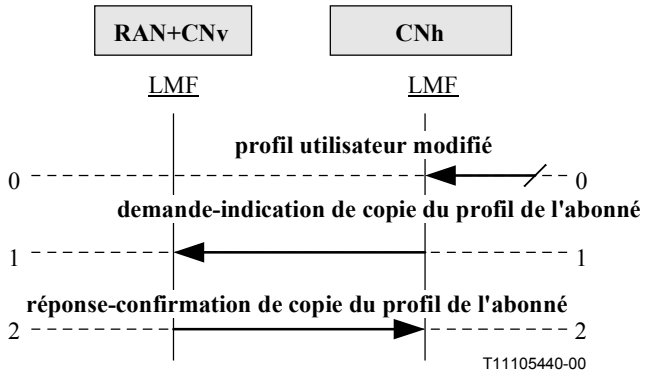


Figure 6.2.1.1-1/Q.1721 – Modification du profil de l'abonné, Cas 1: Copie du profil de l'abonné

0. **Profil utilisateur modifié**: initie la copie du profil de l'abonné dans l'entité LMFv.

FEA0	– Détermine la nécessité de mettre à jour le profil de l'utilisateur résidant dans l'entité LMF du réseau visité.

1. **Demande-indication de copie du profil de l'abonné**: est envoyée de l'entité LMFh à l'entité LMFv dans le réseau serveur indiquant les exigences pour mettre à jour un ou plusieurs éléments du profil de l'abonné.

Copie du profil de l'abonné (réponse: succès)	demande-indication
IMUI	M
Profil d'abonné	M

FEA1	– Identifie l'utilisateur IMT-2000 en question. – Met à jour le profil de l'abonné.

2. **Réponse-confirmation de copie du profil de l'abonné**: est envoyée de l'entité LMFv dans le réseau serveur à l'entité LMFh dans le réseau de rattachement de l'utilisateur. Sert à informer l'entité LMFh des résultats de mise à jour du profil.

Copie du profil de l'abonné	réponse-confirmation
Résultat	M

FEA2	NOTE – Fin de la procédure de mise à jour du profil de l'abonné.

6.2.1.1.2 Modification du profil de l'abonné, Cas 2: supprimer les données utilisateur

L'abonnement d'un ou de plusieurs services de base ou complémentaires a été supprimé. Cette procédure est utilisée pour indiquer les services spécifiques qui ont été retirés et les données spécifiques à supprimer. Voir Figure 6.2.1.1-2.

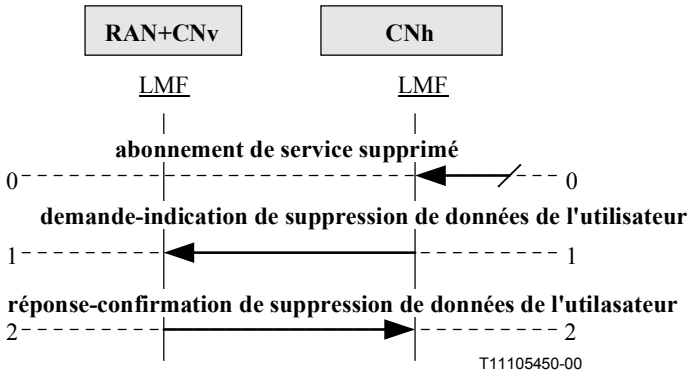


Figure 6.2.1.1-2/Q.1721 – Modification du profil de l'abonné, Cas 2: suppression des données de l'utilisateur

0. **Abonnement de service supprimé**: demande de supprimer un abonnement de services spécifique de la liste des services souscrits.

FEA0	– Détermine la nécessité de supprimer un ou plusieurs services de base ou complémentaires du profil de l'utilisateur résidant dans l'entité LMF du réseau visité.

1. **Demande-indication de suppression de données de l'utilisateur**: est utilisée pour supprimer des données utilisateur spécifiques.

Supprimer données de l'utilisateur (réponse: succès)	demande-indication
IMUI	M
Données de l'utilisateur supprimées	M

FEA1	– Identifie l'utilisateur IMT-2000 concerné. – Supprimer les données de l'utilisateur indiquées dans la demande-indication supprimer les données de l'utilisateur.

2. **Réponse-confirmation de suppression de données de l'utilisateur**: confirme la demande.

Supprimer données de l'utilisateur	réponse-confirmation
Résultat	M

FEA2	– Fin de la procédure de suppression de données de l'utilisateur.

6.2.1.1.3 Modification du profil de l'abonné, Cas 3: suppression du profil de l'abonné

L'algorithme d'authentification ou la clé d'authentification de l'abonné a été changée ou la modification du profil de l'abonné affecte la permission de l'abonné de se déplacer dans sa zone courante. Dans ce cas, il convient de retirer complètement le profil de l'abonné du réseau visité, par conséquent la procédure "suppression du profil abonné" est utilisée. Voir Figure 6.2.1.1-3.

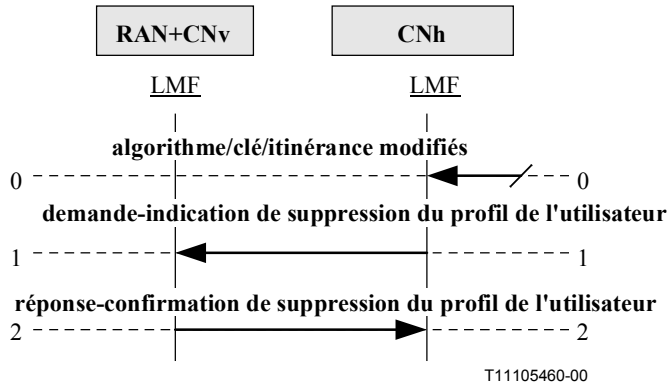


Figure 6.2.1.1-3/Q.1721 – Modification du profil de l'abonné, Cas 3: suppression du profil de l'abonné

0. **Algorithme/clé/itinérance modifiés**: initie la suppression du profil de l'abonné de l'entité LMFv.

FEA0	– Initie la suppression du profil de l'utilisateur.

1. **Demande-indication de suppression du profil de l'utilisateur**: est utilisée pour demander la suppression du profil de l'abonné.

Suppression du profil de l'abonné (réponse: succès)	demande-indication
IMUI	M

FEA1	– Identifie l'utilisateur IMT-2000 concerné. – Supprime le profil de l'utilisateur identifié.

2. **Réponse-confirmation de suppression du profil de l'utilisateur**: est renvoyé pour confirmer les actions prises par l'entité LMFv.

Suppression du profil de l'utilisateur	réponse-confirmation
Résultat	M

FEA2	NOTE – Fin de la procédure de suppression du profil de l'utilisateur.

6.2.1.2 Interrogation sur l'information d'emplacement

La procédure d'interrogation d'information d'emplacement peut être invoquée dans les cas suivants:

cas 1: la version la plus courante de l'information d'emplacement de l'utilisateur résidant dans l'entité LMFv constitue l'objet de l'interrogation par l'entité LMFh;

cas 2: un réseau de prise en charge interroge le réseau de rattachement pour obtenir l'information d'emplacement. Le cas 1 peut être implémenté indépendamment ou en tant que procédure intégrée au cas 2.

6.2.1.2.1 Interrogation pour l'information d'emplacement par l'entité LMF

Cette procédure prévoit que l'entité LMFh interroge l'entité LMFv pour l'information sur l'utilisateur. En recevant une demande relative à l'information d'emplacement de l'utilisateur, l'entité LMFh peut demander la dernière information d'emplacement ou l'information d'emplacement la plus récente (c'est-à-dire, le statut et l'emplacement de l'utilisateur) au réseau serveur. Voir Figure 6.2.1.2-1.

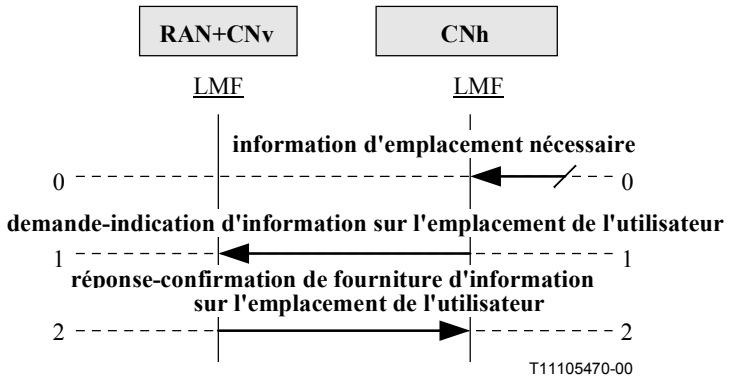


Figure 6.2.1.2-1/Q.1721 – Interrogation d'information sur l'utilisateur par l'entité LMFh

0. **Information d'emplacement nécessaire**: initie la demande pour l'interrogation d'information sur l'emplacement de l'utilisateur (pour l'interrogation de l'information d'emplacement de l'utilisateur).

FEA0	– Détermine la nécessité d'acquérir une information sur l'utilisateur, afin d'effectuer une procédure de gestion de la mobilité (par exemple, enregistrement de terminal) ou simplement dans un mode de mise à jour/relayage, pour répondre à une demande d'information.

1. **Demande-indication d'information sur l'emplacement de l'utilisateur**: est envoyé de l'entité LMFh à l'entité LMFv pour demander que l'information sur l'utilisateur (par exemple, information sur l'état et l'emplacement) soit fournie.

Fourniture de l'information d'emplacement de l'utilisateur (réponse: succès ou échec)	**demande-indication**
Information demandée	M
IMUI	O (Note)
IMDN	O (Note)

FEA1	– Identifie l'utilisateur IMT-2000 concerné. – Extrait l'information sur l'utilisateur requise.
NOTE – L'IMUI ou l'IMDN doivent être fournies.	

2. **Réponse-confirmation de fourniture d'information sur l'emplacement de l'utilisateur**: est envoyée de l'entité LMFv à l'entité LMFh en fournissant l'information sur l'utilisateur demandée (par exemple, information sur l'état et l'emplacement)

Fourniture de l'information sur l'utilisateur	réponse-confirmation
Information d'emplacement	O (Note)
Etat de l'utilisateur	O (Note)

FEA2	NOTE – Fin de la procédure de fourniture d'information sur l'utilisateur.
NOTE – Cet IE doit être fourni s'il est demandé et disponible.	

6.2.1.2.2 Interrogation d'information sur l'utilisateur par l'entité SCF

Cette procédure active le SCF pour obtenir l'information sur l'utilisateur (par exemple, information sur l'état du terminal et son emplacement) résidant dans l'entité LMFh. L'information est utilisée pour prendre en charge les services basés RI à l'utilisateur. Voir la Figure 6.2.1.2-1.

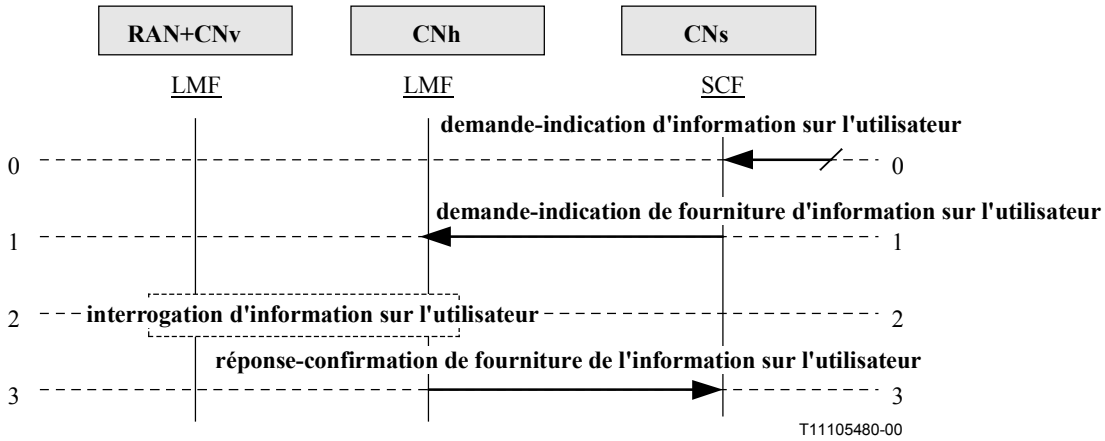


Figure 6.2.1.2-2/Q.1721 – Interrogation d'information sur l'emplacement de l'utilisateur par le SCF

0. **Demande-indication d'information sur l'utilisateur**: initie la demande pour l'interrogation d'information sur l'utilisateur.

FEA0	– Détermine le besoin d'acquérir une information sur l'utilisateur pour fournir un service basé RI.

1. **Demande-indication de fourniture d'information sur l'utilisateur**: est envoyée de l'entité SCF dans le réseau de prise en charge à l'entité LMFh pour demander l'information sur l'utilisateur.

Fourniture de l'information sur l'utilisateur (réponse: succès ou échec)	demande-indication
Information demandée	M
IMUI	O (Note)
IMDN	O (Note)

FEA1	– Identifie l'utilisateur IMT-2000 concerné. – Extrait l'information sur l'utilisateur demandée. Si l'information sur l'utilisateur n'est pas disponible, demande l'information à l'entité LMFv en effectuant la procédure d'interrogation d'information sur l'utilisateur.
NOTE – L'IMUI ou l'IMDN doivent être fournies.	

2. **Interrogation d'information sur l'utilisateur**: est effectuée, si nécessaire.

3. **Réponse-confirmation de fourniture de d'information sur l'utilisateur**: la réponse de l'entité LMFh à l'entité SCF fournissant l'information sur l'utilisateur demandée.

Fourniture de l'information sur l'utilisateur	réponse-confirmation
Information d'emplacement	M
Statut de terminal	M

FEA3	– Utilise l'information reçue dans le SLP qui a été exécutée.

6.2.1.3 Transfert de profil d'abonné

Cette procédure est invoquée quand un utilisateur IMT-2000 tente un enregistrement dans un réseau visité. Cette procédure est exigée dans un module commun pour transférer le profil d'abonné de l'entité LMFh à l'entité LMFv lorsqu'un utilisateur se déplace dans un réseau serveur en dehors de son réseau de rattachement. Voir Figure 6.2.1.3-1.

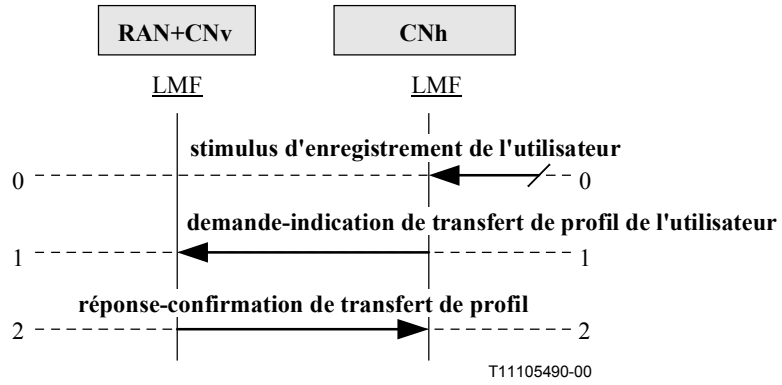


Figure 6.2.1.3-1/Q.1721 – Transfert de profil d'abonné

0. **Stimulus d'enregistrement de l'utilisateur**: initie cette procédure.

FEA0	– Détermine que le profil utilisateur est nécessaire pour prendre en charge un utilisateur itinérant.

1. **Demande-indication de transfert de profil de l'utilisateur**: est envoyé de l'entité LMFh à l'entité LMFv pour fournir le profil de l'utilisateur itinérant.

Transfert de profil (réponse: succès)	demande-indication
IMUI	M
Profil abonné	M

FEA1	– Identifie l'utilisateur IMT-2000 en question et stocke le profil.

2. **Réponse-confirmation de transfert de profil**: la réponse de l'entité LMFv à l'entité LMFh, confirmant la mise à jour du profil de services de l'utilisateur avec des données fournies par l'entité LMFh.

Transfert de profil	réponse-confirmation
Résultat	M

FEA2	– Noter le transfert de profil réussi

6.2.2 Extraction d'identité – Utilisateur

6.2.2.1 Extraction d'identité et mise à jour

L'UIMF contient la TMUI, la LAI et les IMUI des utilisateurs IMT-2000. En ce qui concerne l'origine de l'appel, la fin de l'appel, la mise à jour d'emplacement de terminal, etc., il est nécessaire que le terminal mobile extraie les informations IMUI, TMUI et LAI. Pour la mise à jour de l'emplacement du terminal, le terminal mobile doit mettre à jour la TMUI et la LAI.

Cinq schémas de flux d'informations pour l'extraction d'identité et la mise à jour sont décrits, soit:

- demande d'IMUI;
- demande de TMUI;
- demande de LAI;
- mise à jour de TMUI;
- mise à jour de LAI.

6.2.2.1.1 Demande d'IMUI

Voir Figure 6.2.2.1-1.

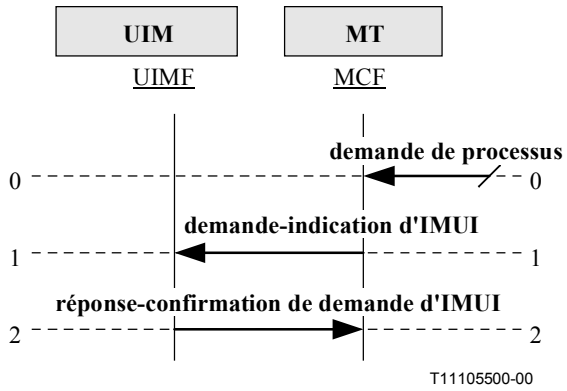


Figure 6.2.2.1-1/Q.1721 – Demande d'IMUI

0. **Demande de processus**: le stimulus pour que la demande d'IMUI soit reçue par le MCF.

FEA0	– Initie la procédure de demande IMUI.

1. **Demande-indication d'IMUI**: est envoyée du MCF à l'UIMF pour extraire l'IMUI de l'abonné.

Demande d'IMUI (réponse: succès ou échec)	demande-indication
Néant	N/A

FEA1	– Extrait l'IMUI de l'abonné.

2. **Réponse-confirmation de demande d'IMUI**: constitue la réponse à la demande.

Demande d'IMUI	réponse-confirmation
IMUI	M

FEA2	– Enregistre l'IMUI.

6.2.2.1.2 Demande de TMUI

Voir Figure 6.2.2.1-2.

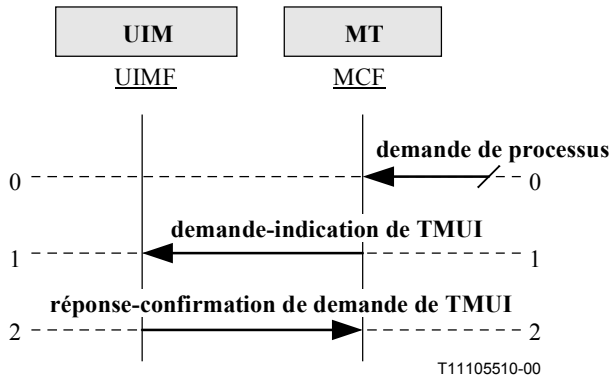


Figure 6.2.2.1-2/Q.1721 – Demande de TMUI

0. **Demande de processus**: reçue par l'entité MCF qui initie la demande de TMUI.

FEA0	– Initie la procédure de demande de TMUI.

1. **Demande-indication de TMUI**: envoyée de l'entité MCF à l'UIMF pour extraire la TMUI de l'abonné.

Demande de TMUI (réponse: succès ou échec)	demande-indication
Néant	N/A

FEA1	– Extrait la TMUI de l'abonné.

2. **Réponse-confirmation de demande de TMUI**: la réponse à la demande.

Demande d'IMUI	réponse-confirmation
TMUI	M
Identité de la source d'attribution de la TMUI	M

FEA2	– Enregistre la TMUI et l'identité de la source d'attribution de la TMUI.

6.2.2.1.3 Demande de LAI

Voir Figure 6.2.2.1-3.

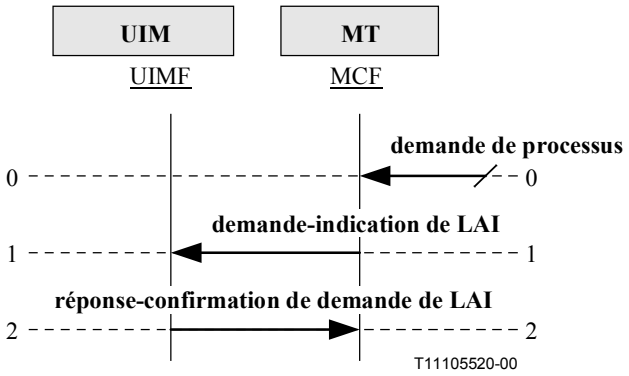


Figure 6.2.2.1-3/Q.1721 – Demande de LAI

0. **Demande de processus**: reçue par l'entité MCF qui est le stimulus pour la demande de LAI.

FEA0	– Initie la procédure de demande de LAI.

1. **Demande-indication de LAI**: est envoyée de l'entité MCF à l'UIMF pour extraire la LAI de l'abonné.

Demande de LAI (réponse: succès ou échec)	demande-indication
Néant	N/A

FEA1	– Extrait la LAI de l'abonné.

2. **Réponse-confirmation de demande de LAI**: constitue la réponse à la demande.

Demande de LAI	réponse-confirmation
LAI	M

FEA2	– Enregistre la LAI.

6.2.2.1.4 Mise à jour de la TMUI

Voir Figure 6.2.2.1-4.

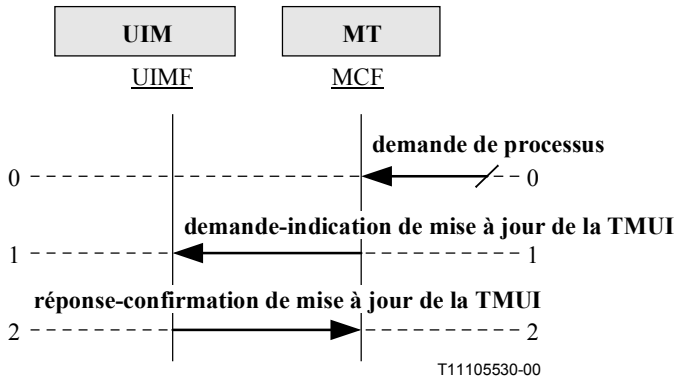


Figure 6.2.2.1-4/Q.1721 – Mise à jour de la TMUI

0. Demande de processus: le stimulus pour la mise à jour la TMUI est reçu par l'entité MCF.

FEA0	– Initie la procédure de mise à jour de la TMUI.

1. **Demande-indication de mise à jour de la TMUI**: est envoyée de l'entité MCF à l'UIMF pour mettre à jour la TMUI de l'abonné.

Mise à jour de la TMUI (réponse: succès ou échec)	demande-indication
TMUI	M
Identité de la source d'attribution de la TMUI	M

FEA1	– Met à jour la TMUI pour l'abonné et enregistre l'identité de la source d'attribution de la TMUI.

2. **Réponse-confirmation de mise à jour de la TMUI**: constitue la réponse à la demande.

Mise à jour de la TMUI	réponse-confirmation
Néant	N/A

FEA2	– Noter l'achèvement réussi.

6.2.2.1.5 Mise à jour de la LAI

Voir Figure 6.2.2.1-5.

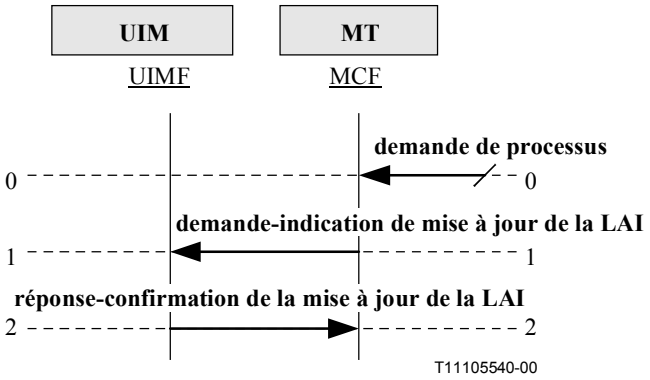


Figure 6.2.2.1-5/Q.1721 – Mise à jour de la LAI

0. **Demande de processus**: le stimulus pour la mise à jour de la LAI est reçu par l'entité MCF.

FEA0	– Envoie la demande de mise à jour de la LAI à l'UIMF.

1. **Demande-indication de mise à jour de la LAI**: est envoyée de l'entité MCF à l'UIMF pour mettre à jour la LAI de l'abonné.

Mise à jour de la LAI (réponse: succès ou échec)	demande-indication
LAI	M

FEA1	– Met à jour la LAI de l'abonné.

2. **Réponse-confirmation de la mise à jour de la LAI**: constitue la réponse à la demande

Mise à jour de la LAI	réponse-confirmation
Néant	N/A

FEA2	– Noter l'achèvement réussi.

6.2.2.2 Extraction de l'identité de l'utilisateur

Cette procédure est utilisée pour convertir la TMUI à l'IMUI de l'utilisateur. Le nouveau réseau visité initie cette procédure lorsque le réseau reçoit la TMUI ou un ensemble de la TMUI et l'identité de la source d'attribution de la TMUI en tant qu'identité de l'utilisateur côté mobile.

Pour l'enregistrement d'emplacement du terminal et la mise à jour, deux cas se présentent:

– cas 1: la TMUI a été attribuée par la nouvelle entité LMF visitée (voir 6.2.2.1.2);

– cas 2: la TMUI a été attribuée par une autre entité LMF, différente de la nouvelle entité LMF visitée (le présent sous-paragraphe).

Si le nouveau réseau visité ne peut pas extraire avec succès l'IMUI (par exemple, perte de la TMUI), il tente d'extraire l'IMUI de l'utilisateur IMT-2000 à partir de l'UIMF (voir 6.2.2.1.1). Voir Figure 6.2.2.2-1.

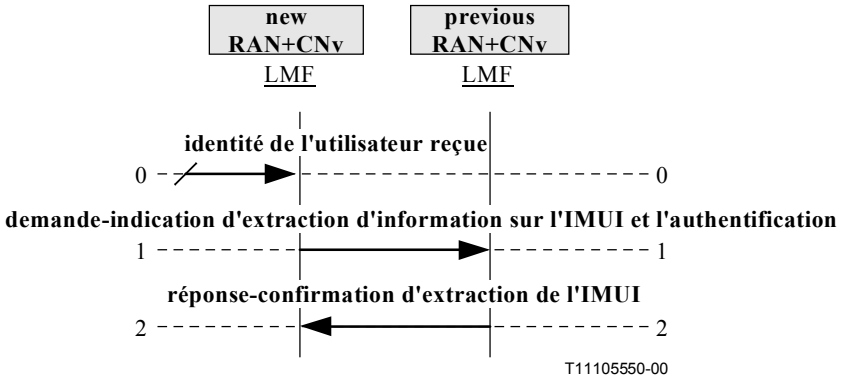


Figure 6.2.2.2-1/Q.1721 – Schéma des flux d'informations d'extraction d'information sur l'authentification et l'IMUI

0. **Identité de l'utilisateur reçue**: reçue par la nouvelle entité LMF visitée, initie cette procédure.

FEA0	Pour le cas 1: – extrait l'IMUI de l'utilisateur IMT-2000 effectuant la demande avec la TMUI. Pour le cas 2: – identifie l'entité LMF par laquelle la TMUI est affectée avec l'identité de la source d'attribution de la TMUI.

1. **Demande-indication d'extraction d'information sur l'IMUI et l'authentification**: est utilisée pour extraire l'IMUI avec la TMUI. Ce flux d'informations est envoyé à l'entité LMF dans le réseau précédemment visité.

Extraction d'information sur l'IMUI et l'authentification (réponse: succès ou échec)	**demande-indication**
TMUI	M
Identité de la source d'attribution de la TMUI	M

FEA1	– Extrait l'IMUI et les triplets d'authentification non utilisés de l'utilisateur IMT-2000 effectuant la demande avec la TMUI.

2. **Réponse-confirmation d'extraction de l'IMUI**: constitue la réponse à la demande.

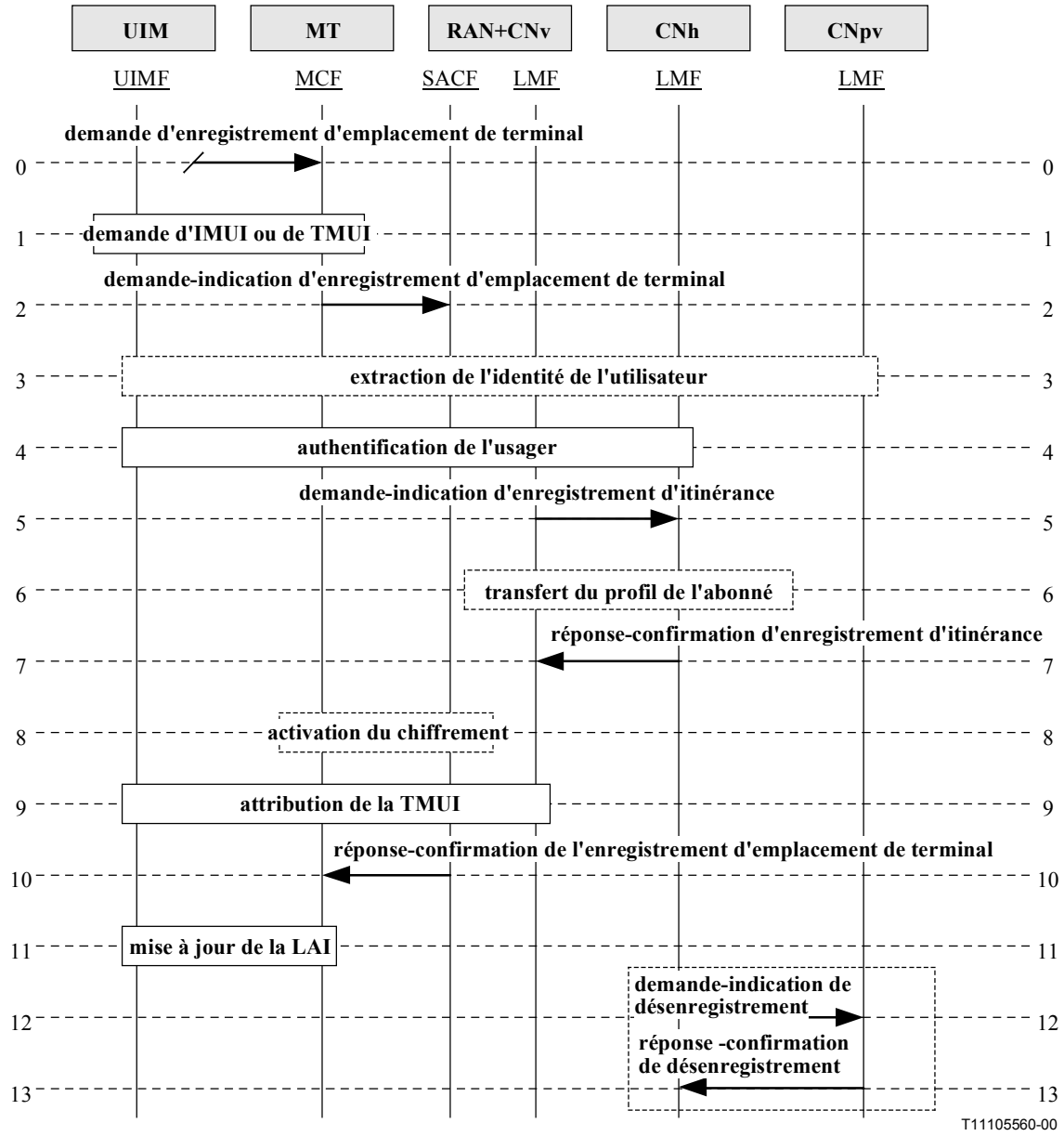
Extraction d'information sur l'IMUI et l'authentification	**réponse-confirmation**
IMUI	M
Résultat	M
Mise(s) à l'épreuve	O (Note 1)
Réponse(s) de mise à l'épreuve	O (Note 1)
Clé(s) de chiffrement	O (Note 2)

FEA2	– Confirme l'achèvement de l'extraction de l'IMUI
NOTE 1 – Inclus si l'authentification doit être exécutée. NOTE 2 – Retourné, si disponible.	

6.2.3 Gestion de l'enregistrement

6.2.3.1 Enregistrement de l'emplacement du terminal

Cette fonctionnalité est utilisée lorsqu'un utilisateur IMT-2000 notifie au système son emplacement. Cette procédure permet d'enregistrer les informations de zone d'emplacement dans le réseau visité. Une procédure d'enregistrement de terminal est effectuée lorsque aucun détail d'emplacement précédent n'est connu sur l'utilisateur lorsqu'il apparaît pour la première fois dans un domaine de réseau. Pendant cette procédure, toutes les informations de l'utilisateur sont supprimées dans le réseau précédemment visité. La mise à jour des informations de zone d'emplacement peut se produire après une panne de réseau ou de terminal. Voir Figure 6.2.3.1-1.



NOTE – Les IF 12 et 13 peuvent se produire à tout moment après IF 5 et sont indépendants des IF 8 à 11 inclus.

Figure 6.2.3.1-1/Q.1721 – Enregistrement d'emplacement de terminal

0. **Demande d'enregistrement d'emplacement de terminal**: elle est lancée lorsque le terminal mobile est mis sous tension et tente de s'enregistrer dans le réseau en utilisant les informations diffusées par ce réseau.

FEA0	– Obtient l'identité de l'utilisateur.

1. **Demande d'IMUI ou de TMUI**: est utilisée pour obtenir l'IMUI ou la TMUI suivant le cas.

2. **Demande-indication d'enregistrement d'emplacement de terminal**: utilisée pour enregistrer les informations de zone d'emplacement du terminal mobile dans le réseau.

Enregistrement d'emplacement de terminal (réponse: succès ou échec)	demande-indication
Identification de l'utilisateur	M (Note1)
Informations du TC	O (Note 2)
AUTH_R	O (Note 3)
Confirmation de RANDG	O (Note 3)
CHCNT	O (Note 3)

FEA2	– Initie la procédure d'extraction d'identité de l'utilisateur pour extraire l'IMUI, si la TMUI est utilisée.
NOTE 1 – L'IMUI ou la TMUI selon l'identité disponible. NOTE 2 – Envoyée si elle est disponible pour indiquer les services que le terminal peut prendre en charge. NOTE 3 – Si la mise à l'épreuve globale (numéro aléatoire) est utilisée dans les informations diffusées pour les besoins de l'authentification, les données d'authentification sont envoyées.	

3. **Extraction de l'identité de l'utilisateur**: est exécutée si nécessaire.

4. **Authentification de l'utilisateur**: est exécutée.

5. **Demande-indication d'enregistrement d'itinérance**: est utilisée pour mettre à jour l'adresse LMFV dans le réseau de rattachement.

Enregistrement de l'itinérance (réponse: succès ou échec)	demande-indication
IMUI	M
adresse LMFv	M

FEA5	– Identifie l'utilisateur IMT-2000 demandeur. – Met à jour l'adresse LMFv. – Identifie, le cas échéant, l'adresse LMFv du réseau précédemment visité. – Lance la mise à jour du profil utilisateur si nécessaire.

6. **Transfert du profil de l'abonné**: est exécuté si nécessaire.

7. **Réponse-confirmation d'enregistrement d'itinérance**: constitue la confirmation à la demande-indication d'enregistrement d'itinérance.

Enregistrement d'itinérance	réponse-confirmation
Résultat	M

FEA7	– Confirme l'exécution de l'enregistrement d'itinérance pour l'utilisateur IMT-2000. – Identifie la zone d'emplacement et les informations du TC. – Stocke la zone d'emplacement et les informations du TC pour l'utilisateur IMT-2000. – Invoque la procédure de mise à jour de la TMUI pour l'utilisateur IMT-2000.

8. **Activation du chiffrement**: est exécuté le cas échéant.

9. **Attribution de la TMUI**: est exécutée.

FEA9	– Analyse le résultat de la procédure de mise à jour de la TMUI.
NOTE – Le module de procédure de mise à jour ce la TMUI est séparé du module de la procédure d'authentification de l'utilisateur afin d'attribuer la TMUI après que le profil utilisateur soit créé dans le nouveau réseau visité.	

10. **Réponse-confirmation de l'enregistrement d'emplacement de terminal**: constitue la confirmation de la demande-indication d'enregistrement d'emplacement de terminal.

Enregistrement d'emplacement de terminal	réponse-confirmation
Résultat	M

FEA10	– Mémorise l'identifiant de la zone d'emplacement en cours dans la station mobile.

11. **Mise à jour de la LAI**: est exécutée pour mettre à jour l'identification de la zone d'emplacement (LAI) dans l'UIM.

12. **Demande-indication de désenregistrement**: est utilisée facultativement pour désenregistrer l'utilisateur du réseau précédemment visité.

Désenregistrement (réponse: succès ou échec)	demande-indication
IMUI	M

FEA12	– Identifie l'utilisateur IMT-2000 demandeur. – Supprime le profil de l'utilisateur de l'utilisateur IMT-2000 demandeur. – Formule et envoie une réponse-confirmation de désenregistrement.

13. **Réponse-confirmation de désenregistrement**: constitue la confirmation de la demande-indication de désenregistrement.

Désenregistrement	réponse-confirmation
Résultat	M

FEA8	– Identifie le nouveau réseau visité.

6.2.3.2 Mise à jour de l'emplacement du terminal

Cette fonctionnalité est utilisée lorsqu'un utilisateur IMT-2000 qui se déplace dans le même domaine de réseau notifie au système sa nouvelle zone d'emplacement. Les informations sur cette nouvelle zone d'emplacement sont ensuite enregistrées dans le réseau visité. La mise à jour de ces informations sur la zone d'emplacement peut également se produire après une panne du réseau du terminal. Voir Figure 6.2.3.2-1.

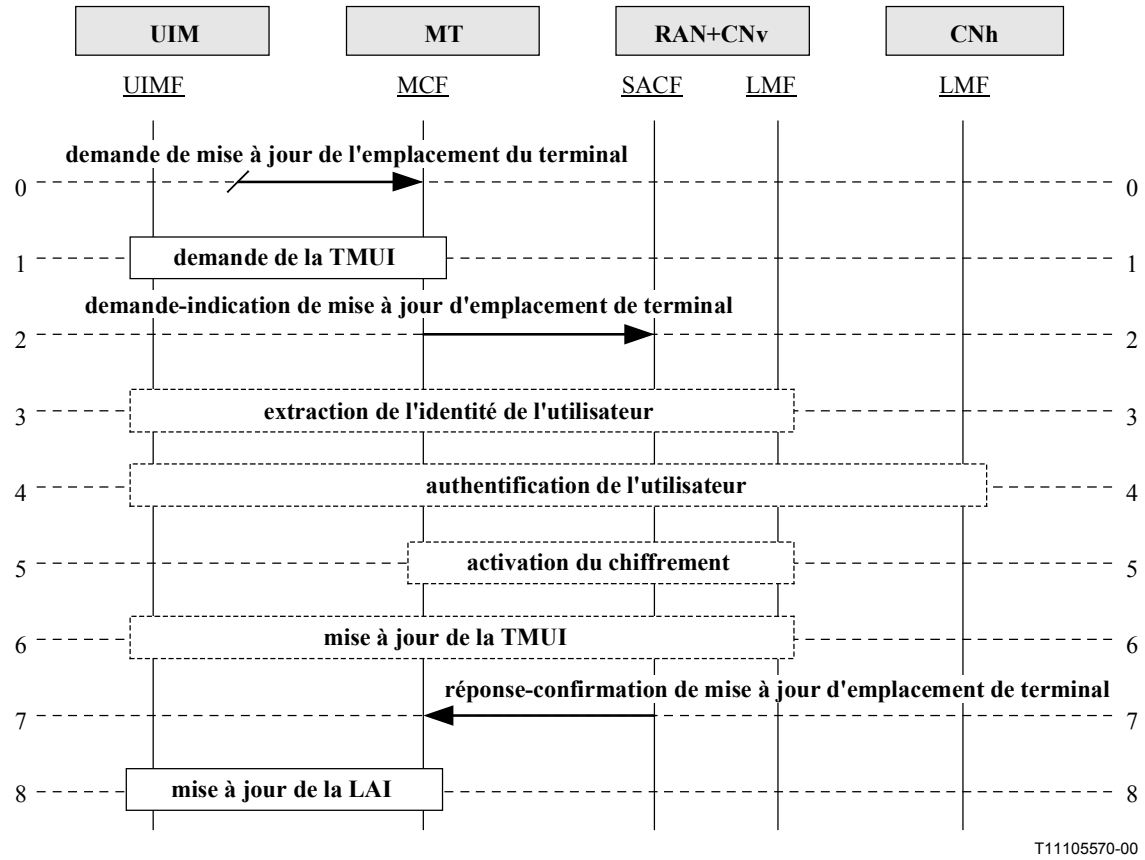


Figure 6.2.3.2-1/Q.1721 – Mise à jour de l'emplacement du terminal

0. **Demande de mise à jour de l'emplacement du terminal**: cette demande est effectuée par le réseau visité.

FEA0	– Initie la procédure de demande de la TMUI pour extraire la TMUI.

1. **Demande de la TMUI**: est exécutée.

2. **Demande-indication de mise à jour d'emplacement de terminal**: est envoyée de la MCF à l'entité LMFv.

Mise à jour d'emplacement de terminal (réponse: succès ou échec)	demande-indication
TMUI	M
Identification de la source de la TMUI	M
AUTH_R	O (Note 1)
Confirmation de RANDG	O (Note 1)
CHCNT	O (Note 2)
Statut du terminal	O (Note 3)
Informations du TC	O (Note 3)

FEA2	– Initie la procédure d'extraction de l'identité de l'utilisateur, si les identités de la source d'attribution de la TMUI et de la TMUI sont utilisées comme identités de l'utilisateur IMT-2000 dans la demande de mise d'emplacement du terminal.
NOTE 1 – Inclus si l'authentification doit être effectuée. NOTE 2 – Inclus si l'historique de comptage d'appels est disponible. NOTE 3 – Fournies si elles sont disponibles.	

3. **Extraction de l'identité de l'utilisateur**: est exécutée si nécessaire pour identifier l'utilisateur IMT-2000 demandeur.

4. **Authentification de l'utilisateur**: est exécutée si la procédure d'extraction de l'identité de l'utilisateur a été exécutée.

5. **Activation du chiffrement**: est exécutée si la procédure d'authentification de l'utilisateur a été exécutée.

6. **Mise à jour de la TMUI**: est exécutée à la suite de deux procédures ci-dessus, si ces dernières sont exécutées.

7. **Réponse-confirmation de mise à jour d'emplacement de terminal**: constitue la confirmation à la demande-indication de mise à jour d'emplacement de terminal.

Mise à jour d'emplacement du terminal	réponse-confirmation
Résultat	M

FEA7	– Enregistre la LAI. – Initie la procédure de mise à jour de la LAI.

8. **Mise à jour de la LAI**: la procédure est exécutée.

6.2.3.3 Détachement

Le terminal notifie explicitement au réseau serveur qu'il ne pourra être joint (par exemple, mise hors tension ou ne pas déranger) en utilisant cette procédure.

Dans certaines situations (par exemple, après une période d'inactivité), le réseau visité peut décider de notifier à l'entité LMFh que l'utilisateur ne peut pas être joint, de façon à ce que, par exemple, toute demande d'information de routage pour les appels à destination du mobile soit traitée en conséquence.

Cette capacité peut également être utilisée dans d'autres cas implicites (par exemple, décharge de la batterie ou détérioration du signal radio). Voir Figure 6.2.3.3-1.

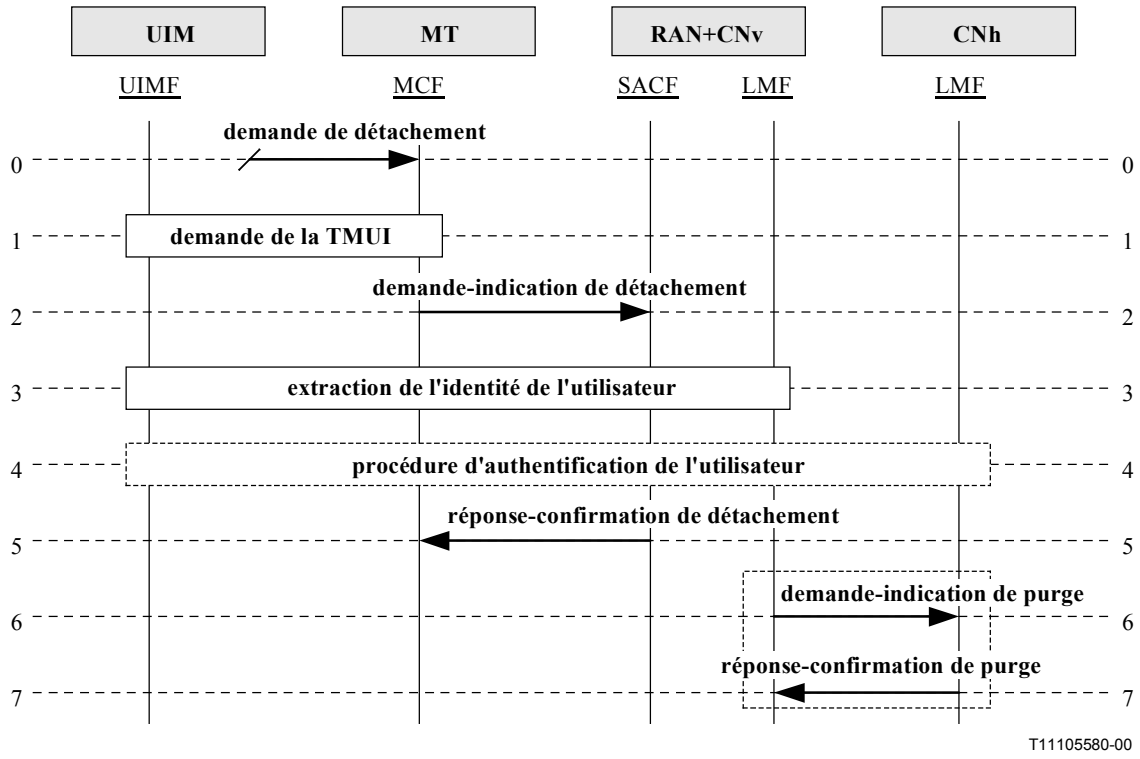


Figure 6.2.3.3-1/Q.1721 – Détachement

0. **Demande de détachement**: le stimulus qui initie la procédure de détachement.

FEA0	– Initie la procédure de demande de la TMUI pour extraire la TMUI.

1. **Demande de la TMUI**: la procédure est exécutée.

2. **Demande-indication de détachement**: est utilisée par le terminal pour notifier au réseau serveur qu'il ne pourra être joint.

Détachement (réponse: succès ou échec)	**demande-indication**
Identification de l'utilisateur	M (Note)

FEA2	– Initie la procédure d'extraction de l'identité de l'utilisateur si l'identité des sources d'attribution de la TMUI et la TMUI sont utilisées comme identité de l'utilisateur IMT-2000 dans la demande de détachement.
NOTE – Il convient que la TMUI soit utilisée à la place de l'IMUI comme identité de l'utilisateur IMT-2000 pour conserver confidentielle l'identité de l'utilisateur.	

3. **Extraction de l'identité de l'utilisateur**: la procédure est exécutée.

4. **Procédure d'authentification de l'utilisateur**: est exécutée si nécessaire.

5. **Réponse-confirmation de détachement**: la confirmation de la demande-indication de détachement.

Détachement	réponse-confirmation
Résultat	M

FEA5	NOTE – Fin de la procédure de détachement.

6. **Demande-indication de purge**: est utilisée par le réseau serveur pour notifier le réseau de rattachement que le terminal ne peut pas être joint.

Purge (réponse: succès ou échec)	demande-indication
IMUI	M
Adresse LMFv	O

FEA6	– Marque l'utilisateur IMT-2000 comme ne pouvant être joint dans le réseau qui effectue la notification.

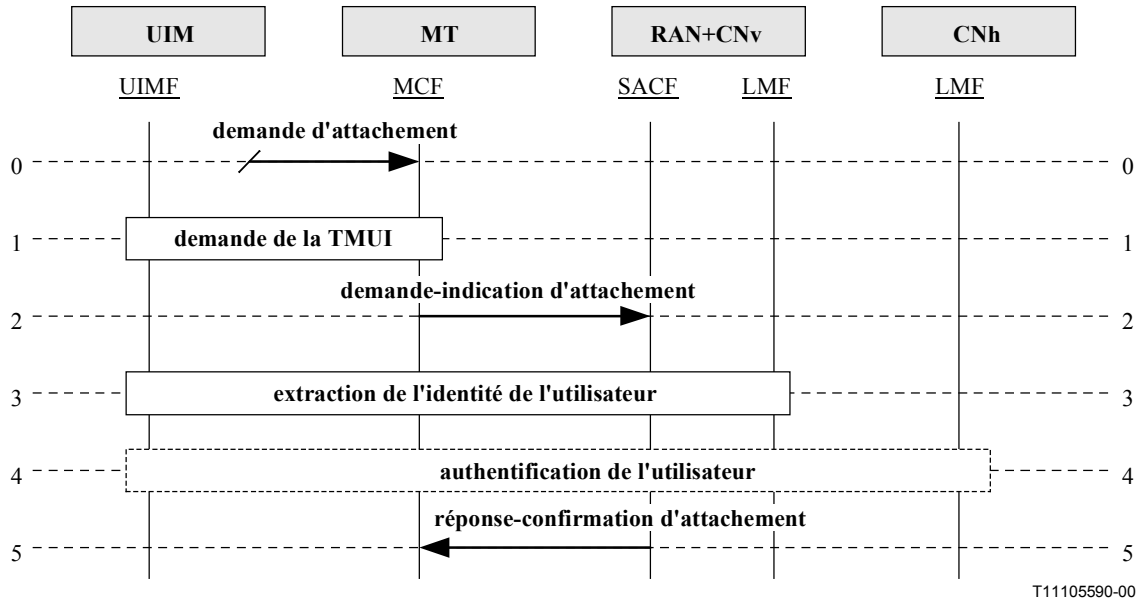
7. **Réponse-confirmation de purge**: la confirmation à la demande-indication de purge.

Purge	réponse-confirmation
Résultat	M

FEA7	– Décide si l'enregistrement de l'abonné doit être supprimé de l'entité LMFv.

6.2.3.4 Attachement

Voir Figure 6.2.3.4-1.



NOTE – Si la procédure d'attachement échoue, il convient que le terminal mobile interprète cet échec comme le besoin d'effectuer la procédure d'enregistrement d'emplacement de terminal.

Figure 6.2.3.4-1/Q.1721 – Attachement

0. **Demande d'attachement**: initie la procédure d'attachement.

FEA0	– Initie la procédure de demande de la TMUI pour extraire la TMUI.

1. **Demande de la TMUI**: est exécutée.

2. **Demande-indication d'attachement**: est utilisée par le terminal pour notifier le réseau serveur que le terminal mobile peut être joint.

Attachement (réponse: succès ou échec)	demande-indication
TMUI	M

FEA0	– Initie la procédure d'extraction de l'identité de l'utilisateur.

3. **Extraction de l'identité de l'utilisateur**: est exécutée.

4. **Authentification de l'utilisateur**: est exécutée si nécessaire comme résultat de la procédure indiquée ci-dessous.

FEA4	– Basée sur les informations d'état de message court dans l'entité LMFv (par exemple, échec de transfert de message court parce que le terminal ne peut pas être joint), la procédure de message court va commencer (non indiqué dans la figure). – Si l'entité LMFv a un drapeau réglé pour indiquer que les données d'itinérance du système de rattachement ne sont pas fiables, la mise à jour de l'emplacement sera exécutée (non indiqué dans la figure). – Accuse réception de la demande-indication d'attachement

5. **Réponse-confirmation d'attachement**: la confirmation de la demande-indication d'attachement.

Attachement	réponse-confirmation
Résultat	M

FEA5	– Le terminal mobile continue à fonctionner normalement.

6.2.4 Reprise sur défaut de données d'emplacement

Cette catégorie de procédure traite de la reprise après une situation de défaut. L'objet est de s'assurer que les données stockées dans les différents nœuds sont cohérentes. Dans cette catégorie trois procédures s'appliquent:

– données de l'abonné itinérant non fiables;

– indication de vérification de données de services complémentaires;

– restauration de données LMF.

6.2.4.1 Données de l'abonné itinérant non fiables

Les données de l'abonné itinérant non fiables sont utilisées pour informer un système visité que les données du terminal mobile itinérant du système de rattachement ne sont pas fiables (par exemple, en raison d'une panne du système). Voir Figure 6.2.4.1-1.

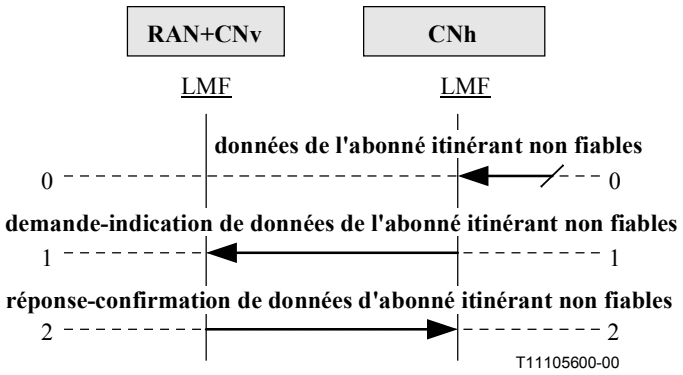


Figure 6.2.4.1-1/Q.1721 – Données de l'abonné itinérant non fiables

0. **Données de l'abonné itinérant non fiables**: indique que les données de l'abonné itinérant ne sont pas fiables et initient la notification des autres systèmes.

FEA0	– La LMFh se prépare à informer le ou les autres systèmes qu'ils ont subi une panne rendant les données de l'abonné itinérant non fiables.

1. **Demande-indication de données de l'abonné itinérant non fiables**: est envoyée de l'entité LMFh aux LMF des autres systèmes.

Données de l'abonné itinérant non fiables (réponse: succès ou échec)	demande-indication
Identification du réseau de rattachement	M

FEA1	– L'entité LMFv supprime tous les enregistrements des abonnés associés à la LMFh envoyant le message.

2. **Réponse-confirmation de données d'abonné itinérant non fiables**: apporte la réponse à la demande.

Abonné itinérant non fiable	réponse-confirmation
Résultat	M

FEA2	– Accusé de réception.

6.2.4.2 Indication de vérification de données de services complémentaires

La fonctionnalité indication de vérification de données de services complémentaires est utilisée par la LMFh pour indiquer à l'utilisateur mobile qu'il est possible que les données de services complémentaires soient altérées en raison du redémarrage. A la réception de la LMFh, l'entité LMFv envoie cette indication à la SACF qui à son tour envoie cette indication à la MCF. Voir Figure 6.2.4.2-1.

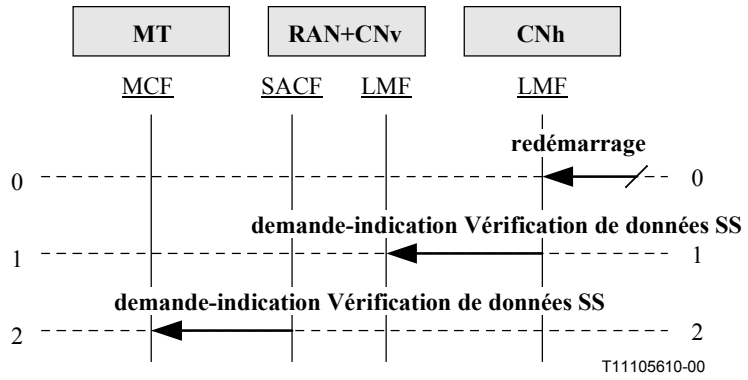


Figure 6.2.4.2-1/Q.1721 – Indication de vérification de données de services complémentaires

0. **Redémarrage**: le stimulus qui initie la procédure Vérification de données SS.

FEA0	– Détermine qu'un redémarrage s'est produit et qu'il convient que le mobile soit informé des changements possibles aux données SS.

1. **Demande-indication Vérification de données SS**: est envoyée de la LMFh à l'entité LMFv.

Vérification de données SS (réponse: néant)	**demande-indication**
Néant	N/A

FEA1	– Demande-indication Envoyer vérification de données SS.

2. **Demande-indication Vérification de données SS**: est envoyée de la SACF à la MCF.

Vérification de données SS (réponse: néant)	**demande-indication**
Néant	N/A

FEA2	– Le terminal doit indiquer à l'utilisateur que les informations SS sont vérifiées.

6.2.4.3 Restauration de données LMF

La fonctionnalité de restauration de données LMF est utilisée pour indiquer à la LMFh qu'elle a reçu une opération de fourniture d'un numéro itinérant pour une IMUI inconnue ou pour une IMUI connue avec l'indicateur "confirmé par le HLR" réglé à "non confirmé". Le service est utilisé pour mettre à jour le numéro d'emplacement (c'est-à-dire l'adresse LAI et LMFv) dans la LMFh, si elle est fournie, et pour demander à la LMFh d'envoyer toutes les données de profil d'abonné à l'entité LMFv. Voir Figure 6.2.4.3-1.

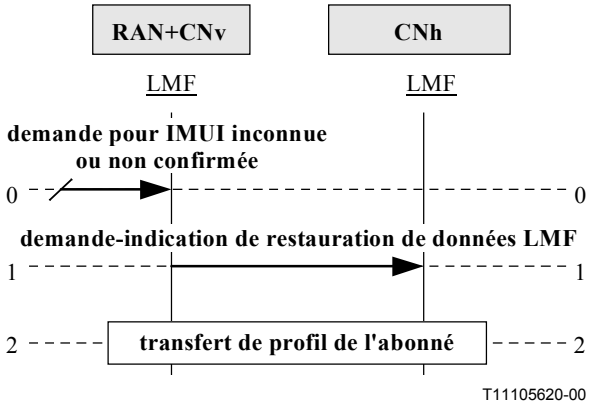


Figure 6.2.4.3-1/Q.1721 – Restaure les données LMF

0. **Demande pour IMUI inconnue ou non confirmée**: initie la procédure de restauration de données LMF.

FEA0	– Détermine qu'un numéro itinérant a été demandé pour une IMUI inconnue ou pour une IMUI qui a besoin d'une confirmation de la LMFh.

1. **Demande-indication de restauration de données LMF**: est envoyée de l'entité LMFv à la LMFh.

Restaure les données LMF (réponse: succès ou échec)	demande-indication
IMUI	M
LAI	M

FEA1	– Exécute la procédure de transfert de profil d'abonné.

2. **Transfert de profil de l'abonné**: est exécuté pour terminer le processus de restauration.

7 Commande d'appel de base et commande de support

Le présent paragraphe fournit le flux d'informations pour l'appel de base et la commande de support pour les systèmes IMT-2000 pour établir et libérer des communications vocales en utilisant des supports à commutation de paquets ou à commutation de circuits.

La commande d'appel de base et de support comprend des flux d'informations pour:

- l'appel mobile sortant;
- la radiorecherche de terminal;
- le routage d'appel;
- l'appel mobile entrant;
- la libération d'appel mobile;
- l'appel d'urgence;
- l'appel prioritaire.

7.1 Appel mobile sortant

La procédure d'appel mobile sortant implique qu'un abonné mobile effectue un appel dans l'état de repos (appel initial) ou dans l'état occupé (appel supplémentaire). Avant que l'appel soit établi, le réseau visité valide l'appelant et peut invoquer des services basés sur la tentative d'origine. Cette procédure est locale vers le réseau serveur ou utilise la capacité de réseau VHE.

7.1.1 Appel mobile sortant initial

La procédure d'appel mobile sortant initial est utilisée lorsque l'utilisateur effectue un appel dans l'état de repos. Voir Figure 7.1.1-1.

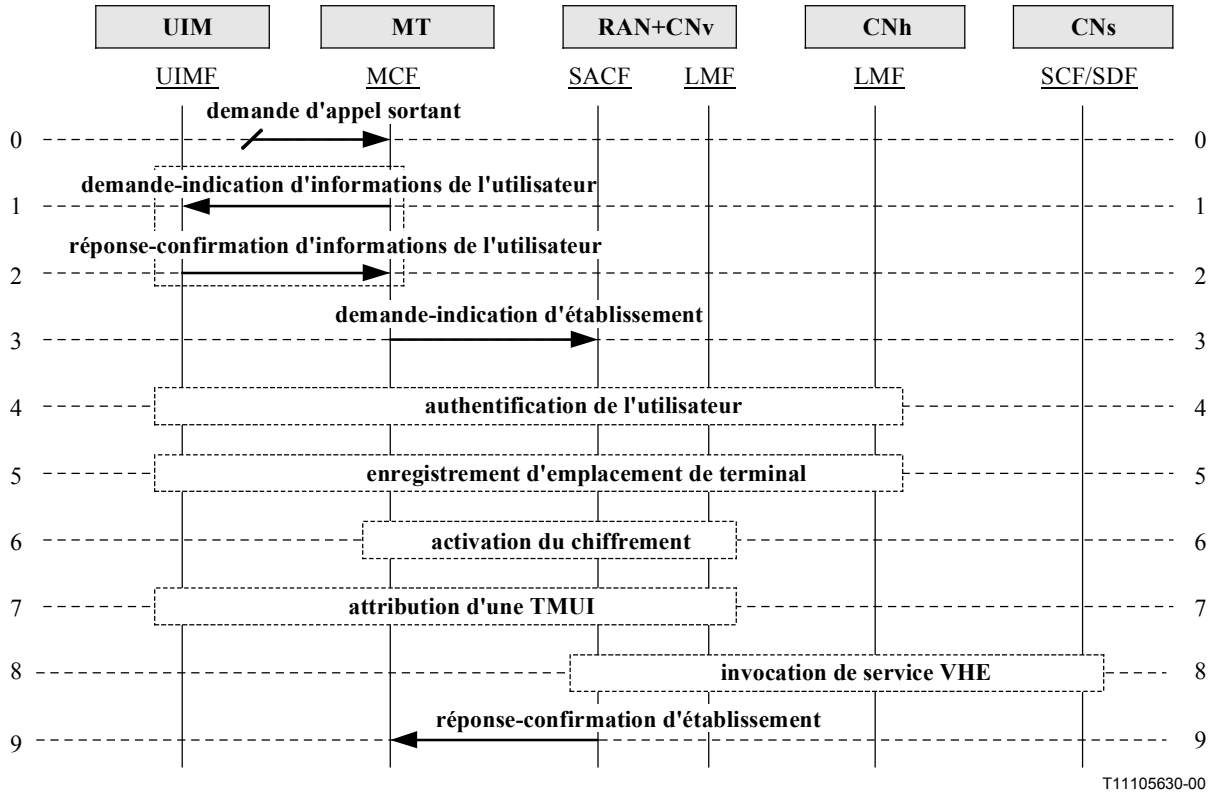


Figure 7.1.1-1/Q.1721 – Schéma du flux d'informations d'appel mobile sortant initial

0. **Demande d'appel sortant:** l'abonné mobile effectue un appel sortant (appel d'origine mobile) dans l'état de repos.

FEA0	– Le terminal mobile peut interagir avec l'abonné pour accumuler les informations. Il peut invoquer la logique de service (par exemple, liste de numérotation abrégée).

1. **Demande-indication d'informations de l'utilisateur**: la MCF demande en option à l'entité UIMF des informations/instructions supplémentaires.

Informations de l'utilisateur (réponse: succès ou échec)	demande-indication
Demande d'informations UIM	M

FEA1	– En option, invoque une logique de service local (par exemple, basée UIM). – Collecte les informations demandées.

2. **Réponse-confirmation d'informations de l'utilisateur**: L'entité UIMF retourne à la MCF les informations de l'utilisateur demandées.

Information de l'utilisateur	réponse-confirmation
Réponse des informations de l'UIM	M

FEA2	– Initie l'établissement d'appel et la demande de support.

3. **Demande-indication d'établissement**: le MCF commence à établir l'appel et demande au SACF dans le réseau serveur d'allouer un canal support.

Etablissement (réponse: succès ou échec)	demande-indication
Identification de l'utilisateur	M (Note 1)
Numéro appelé	M
Numéro appelant	M
Identifiant de service	M
Identifiant de facturation	O (Note 2)
Capacité support	O (Note 3)
QoS	O (Note 4)
AUTH_R	O (Note 5)
RANDC	O (Note 5)
CHCNT	O (Note 5)
IMEI	O (Note 5)
AUTHKEYS	O (Note 6)
SRES	O (Note 7)

FEA3	– En option, invoque et attend l'exécution de l'authentification de l'utilisateur. – En option, invoque et attend l'exécution de l'enregistrement d'emplacement du terminal. – En option, invoque et attend l'exécution de l'activation du chiffrement. – Etablit le canal d'appel et le canal support.

NOTE 1 – Inclut l'IMUI ou la TMUI selon l'identité disponible. La TMUI est recommandée pour la sécurité sur la voie hertzienne.

NOTE 2 – Inclus si elle est demandée par le fournisseur de service de rattachement.

NOTE 3 – Inclus pour indiquer la capacité du canal support.

NOTE 4 – Inclus pour indiquer la qualité de service désirée.

NOTE 5 – Inclus pour fournir les informations liées à l'authentification uniquement pour les systèmes basés SSD.

NOTE 6 – Inclus pour fournir les informations liées à l'authentification uniquement pour les systèmes non basés SSD.

NOTE 7 – Inclus pour fournir le résultat de la signature.

4. **Authentification de l'utilisateur**: si l'authentification est nécessaire pour cette tentative d'appel, elle est effectuée.

5. **Enregistrement d'emplacement de terminal**: si le terminal mobile n'est pas enregistré dans le réseau visité, l'enregistrement d'emplacement du terminal est effectué.

6. **Activation du chiffrement**: le chiffrement est lancé s'il est nécessaire pour cette tentative d'appel.

7. **Attribution d'une TMUI**: l'attribution d'une TMUI, si elle est nécessaire, peut être effectuée à tout moment après que le chiffrement a été lancé.

8. **Invocation de service VHE**: basée sur le profil de l'abonné, le réseau visité peut appeler une logique de service de réseau intelligent. Cela peut se produire à tout point de détection de déclenchement défini et actif.

9. **Réponse-confirmation d'établissement**: le SACF du réseau visité rapporte l'exécution réussie de l'établissement de l'appel et du canal support.

Etablissement	réponse-confirmation
Identité du support	M

FEA9	– Exécute l'établissement de l'appel sur le support sélectionné.

7.1.2 Appel mobile sortant supplémentaire

L'appel mobile sortant supplémentaire implique qu'un abonné mobile lance un deuxième appel alors qu'il est déjà sur un appel, c'est-à-dire un appel trois voies. La procédure suivie est similaire aux appels de mobile sortants.

7.2 Radiorecherche de terminal

La procédure de radiorecherche de terminal est utilisée pour localiser un terminal mobile. Voir Figure 7.2.1.

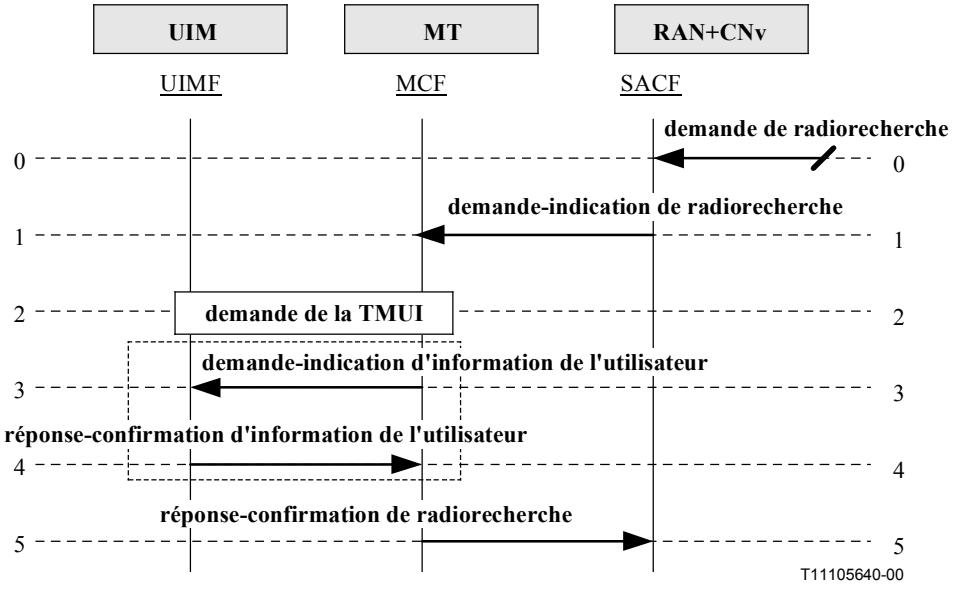


Figure 7.2-1/Q.1721 – Radiorecherche de terminal

0. **Demande de radiorecherche**: un appel mobile entrant provoque une demande de radiorecherche sur le réseau visité.

FEA0	– Le réseau visité envoie la demande de radiorecherche à la MCF.

1. **Demande-indication de radiorecherche**: le réseau visité essayer de localiser le terminal mobile.

Radiorecherche (réponse: succès ou échec)	demande-indication
TMUI	M

FEA1	– Se prépare à effectuer une demande de la TMUI.

2. **Demande de la TMUI**: la MCF extrait la TMUI de l'entité UIMF, la compare à la TMUI reçue du réseau visité et détermine que la demande de radiorecherche est adressée à ce terminal mobile.

3. **Demande-indication d'information de l'utilisateur**: en option la MCF demande à l'entité UIMF des informations/instructions supplémentaires.

Informations de l'utilisateur (réponse: succès ou échec)	demande-indication
Demande de traitement de terminaison	O (Note)

FEA3	– Donne à la MCF l'ordre de répondre à la radiorecherche.
NOTE – Inclut pour demander les instructions de traitement d'appel de l'entité UIMF.	

4. **Réponse-confirmation d'information de l'utilisateur**: l'entité UIMF renvoie les informations demandées à la MCF.

Informations de l'utilisateur	réponse-confirmation
Informations de traitement de la terminaison	O (Note)

FEA4	– Se prépare à répondre à la demande de radiorecherche.
NOTE – Inclut pour indiquer le type de traitement de terminaison d'appel à appliquer.	

5. **Réponse-confirmation de radiorecherche**: l'entité MCF répond à la radiorecherche.

Radiorecherche	réponse-confirmation
Néant	(Note)

FEA5	– Néant
NOTE – La réponse-confirmation est vide. Simplement, sa présence est suffisante pour indiquer le succès.	

7.3 Acheminement d'appel sur le réseau

Le présent sous-paragraphe traite du flux d'informations de bout en bout pour les opérations de routage d'appel IMT-2000 entre familles (ou entre réseaux). Le routage d'appel dans un système

membre de la famille des IMT-2000 est considéré comme une opération à l'intérieur de la famille est n'est pas traité ici.

La procédure de routage d'appel est utilisée pour obtenir une adresse (par exemple, numéro itinérant) de l'élément de réseau du réseau visité où l'utilisateur est situé afin de router un appel d'arrivée. L'adresse est liée dynamiquement à l'identité de l'utilisateur.

Le routage des données d'informations est nécessaire au réseau effectuant l'interrogation pour demander un "établissement d'appel" au réseau visité de l'abonné appelé. L'expression "information de routage" est utilisée pour représenter toutes les données informatives nécessaires à l'identification du réseau visité et à l'emplacement du terminal de l'utilisateur.

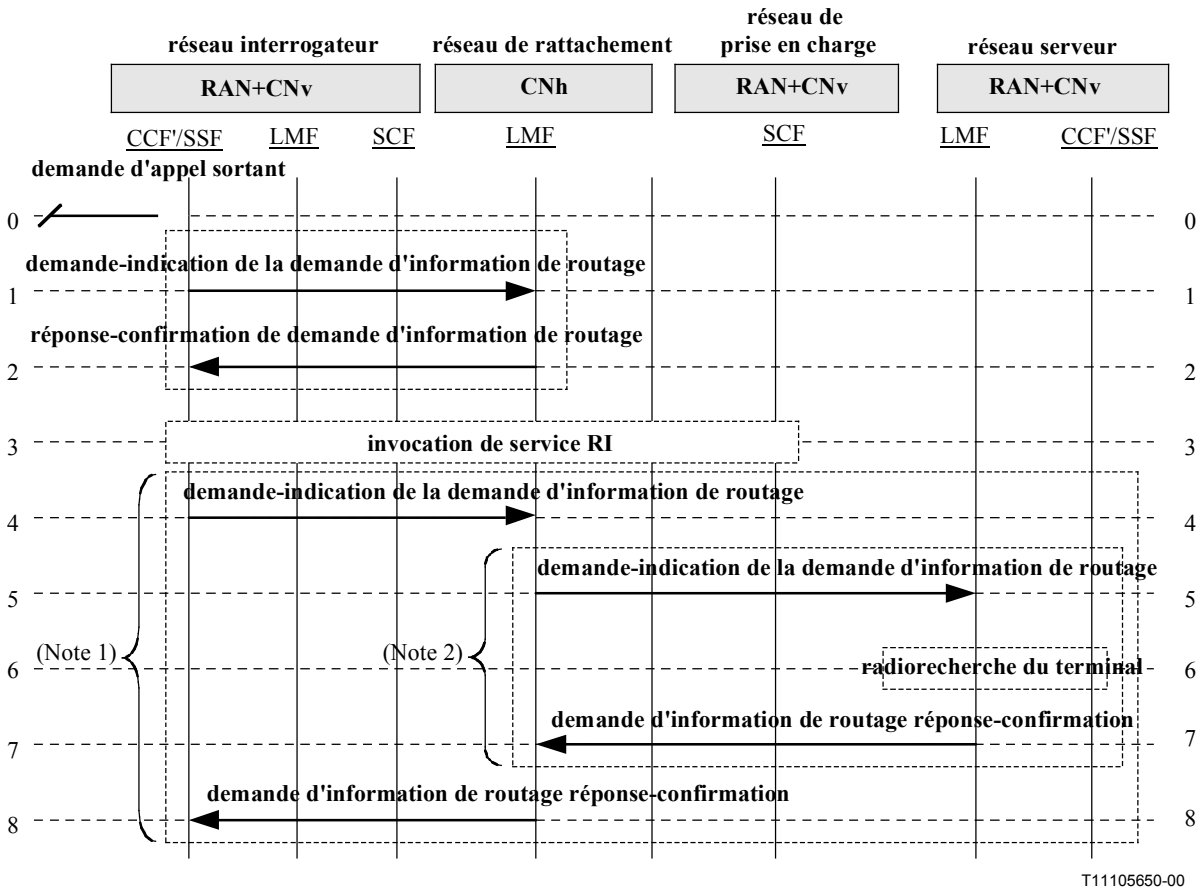
La demande d'information de routage peut être exécutée directement entre réseaux. Lorsque le réseau d'origine ou le réseau intermédiaire est le réseau effectuant l'interrogation, la demande d'information de routage est envoyée directement au réseau de rattachement sans router l'appel (demande d'établissement d'appel) vers le réseau de rattachement. Toutefois, l'exécution dépend de l'accord bilatéral entre les réseaux. Lorsque ni le réseau d'origine ni le réseau intermédiaire ne sont capables d'effectuer une interrogation, l'appel est routé au réseau de rattachement et la première demande est invoquée ici. Dans tous ces cas, il n'existe qu'un seul "réseau effectuant l'interrogation": le réseau d'origine, le réseau intermédiaire ou le réseau de rattachement.

La procédure de routage d'appel utilise un schéma d'interrogation en chaîne par lequel le réseau d'interrogation obtient des informations de routage mises à jour (par exemple, DN, adresse IP) directement du réseau de rattachement de la partie appelée. De plus, le schéma de demande en chaîne est défini comme la procédure selon laquelle le réseau effectuant l'interrogation demande des informations de routage au réseau de rattachement de l'abonné appelé puis le réseau de rattachement demande au réseau visité des informations de routage de l'abonné appelé mises à jour.

Les suppositions suivantes sont faites relativement à ce flux d'informations de routage d'appel:

- Le "réseau effectuant l'interrogation" peut être soit le réseau d'origine, intermédiaire ou de support.
- La demande "d'information de routage" est envoyée dans un schéma en chaîne du réseau effectuant l'interrogation au réseau de rattachement de l'abonné appelé et après réception des informations, la demande d'établissement d'appel est envoyée au réseau visité de l'abonné appelé.
- L'exécution de la radiorecherche dans le réseau visité de l'abonné appelé peut être effectuée à tout moment après la réception d'une demande d'information de routage.

Voir Figure 7.3.1.



NOTE 1 – Cette relation de commande de service peut être invoquée à divers instants.
NOTE 2 – Ces fonctions d'interfonctionnement peuvent ne pas être requises si la LMF dispose déjà d'informations de routage.

Figure 7.3-1/Q.1721 – Routage d'appel

0. **Demande d'appel sortant**: une demande d'appel sortant est reçue.

FEA0	– Le réseau effectuant l'interrogation lance les procédures de demande de routage.

1. **Demande-indication de la demande d'information de routage**: invoquée en option par la CCF'/SSF du réseau effectuant l'interrogation, ce flux est utilisé pour obtenir de la LMFh, l'adresse de routage du réseau de prise en charge si la commande de service doit être effectuée.

Demande d'information de routage (réponse: succès ou échec)	demande-indication
Numéro appelé	M

FEA1	– Extrait l'adresse de routage du réseau de prise en charge du correspondant appelé.

2. **Réponse-confirmation de demande d'information de routage**: ce flux est utilisé pour informer le réseau effectuant l'interrogation de l'adresse de routage du réseau de prise en charge de l'abonné appelé. L'adresse de routage du réseau de prise en charge peut (facultatif) être utilisée pour invoquer les fonctionnalités de service RI de l'abonné appelé (par exemple, filtrage d'appel, interdiction d'appel).

Demande d'information de routage	réponse-confirmation
Adresse de routage (pour le réseau de prise en charge de l'abonné appelé)	

FEA2	– Effectue en option une procédure d'invocation de service RI.
NOTE 1 – Il peut se produire des interactions supplémentaires de commande de service dans la "relation de commande de service" (indiquée schématiquement par le carré en gris) englobant le flux d'informations "d'invocation de logique de service". La relation de commande de service peut se terminer après la première interaction de logique de service ou peut continuer jusqu'à ce que l'appel soit routé. NOTE 2 – L'invocation de service peut émaner de la SSF dans le réseau effectuant l'interrogation à la SCF du réseau de rattachement (éventuellement relayée via la SCF du réseau effectuant l'interrogation), ou de la LMF du réseau de rattachement. NOTE 3 – Si l'invocation de service est invoquée depuis le réseau effectuant l'interrogation, les informations obtenues du réseau de rattachement en réponse à la demande d'information de routage contiendront les instructions destinées au réseau serveur pour l'invocation de service. NOTE 4 – L'invocation de service peut aboutir à différents scénarios, tels que le détournement d'appel vers une ligne fixe par exemple, l'interaction de l'utilisateur avec une SRF ou d'autres scénarios. Cette figure représente uniquement la terminaison d'appel simple vers l'abonné mobile.	

3. **Invocation de service RI**: cette procédure peut être invoquée en option.

4. **Demande-indication de la demande d'information de routage**[1]: invoqué par la CCF'/SSF du réseau effectuant l'interrogation ce flux est utilisé pour demander les informations de routage (par exemple, ITDN pour l'abonné appelé) à la LMF du réseau de rattachement de la partie appelée.

Demande d'information de routage (réponse: succès ou échec)	demande-indication
Numéro appelé	M

FEA4	– Identifie l'abonné appelé. – Envoie la demande au réseau serveur/visité pour obtenir un numéro de routage (par exemple, ITDN).

5. **Demande-indication de la demande d'information de routage**: ce flux est utilisé pour envoyer la demande à la LMF du réseau serveur pour obtenir le numéro de routage (par exemple, ITDN) de l'utilisateur. Il peut (facultatif) être utilisé pour invoquer la logique de service pour localiser le terminal.

Demande d'information de routage (réponse: succès ou échec)	demande-indication
IMUI	M
Numéro appelé	O

FEA5	– Identifie l'abonné appelé. – Procédure de radiorecherche (flux facultatifs). – Attribue un numéro de routage (par exemple, ITDN) pour l'abonné appelé.

[1] Conditionnel, si l'invocation de service provient du réseau effectuant l'interrogation.

6. **Radiorecherche du terminal**: cette procédure est effectuée en option, si nécessaire.

7. **Réponse-confirmation de demande d'information de routage**: ce flux est utilisé pour transférer le numéro de routage (par exemple, ITDN) de l'abonné appelé à la LMF du réseau de rattachement de l'utilisateur.

Demande d'information de routage	réponse-confirmation
Numéro de routage de l'abonné appelé (par exemple, ITDN)	M

FEA7	– Envoie le numéro de routage (par exemple, ITDN).

8. **Réponse-confirmation de demande d'information de routage**: ce flux est utilisé pour transférer l'adresse/le numéro de routage de l'utilisateur appelé et peut être également utilisé pour transférer le résultat de la radiorecherche (si elle est exécutée).

Demande d'information de routage	réponse-confirmation
Numéro de routage de l'abonné appelé (par exemple, ITDN)	M

FEA8	– Utilise le numéro de routage (par exemple, ITDN) pour router l'appel (par exemple, via le RTPC) vers le réseau serveur.

7.4 Appel mobile entrant

La procédure d'appel mobile entrant est utilisée pour terminer un appel vers un terminal mobile dans l'état de repos.

En supposant que l'appel soit routé dans des conditions optimales (le réseau d'interrogation n'est pas le réseau de rattachement):

- pour les services de base l'appel est routé depuis le réseau de service jusqu'à sa destination par l'intermédiaire de la signalisation de commande d'appel en utilisant le numéro itinérant précédemment extrait;
- pour les services avancés, les VHE s'appliquent.

7.4.1 Appel entrant initial de mobile

Voir Figure 7.4.1-1.

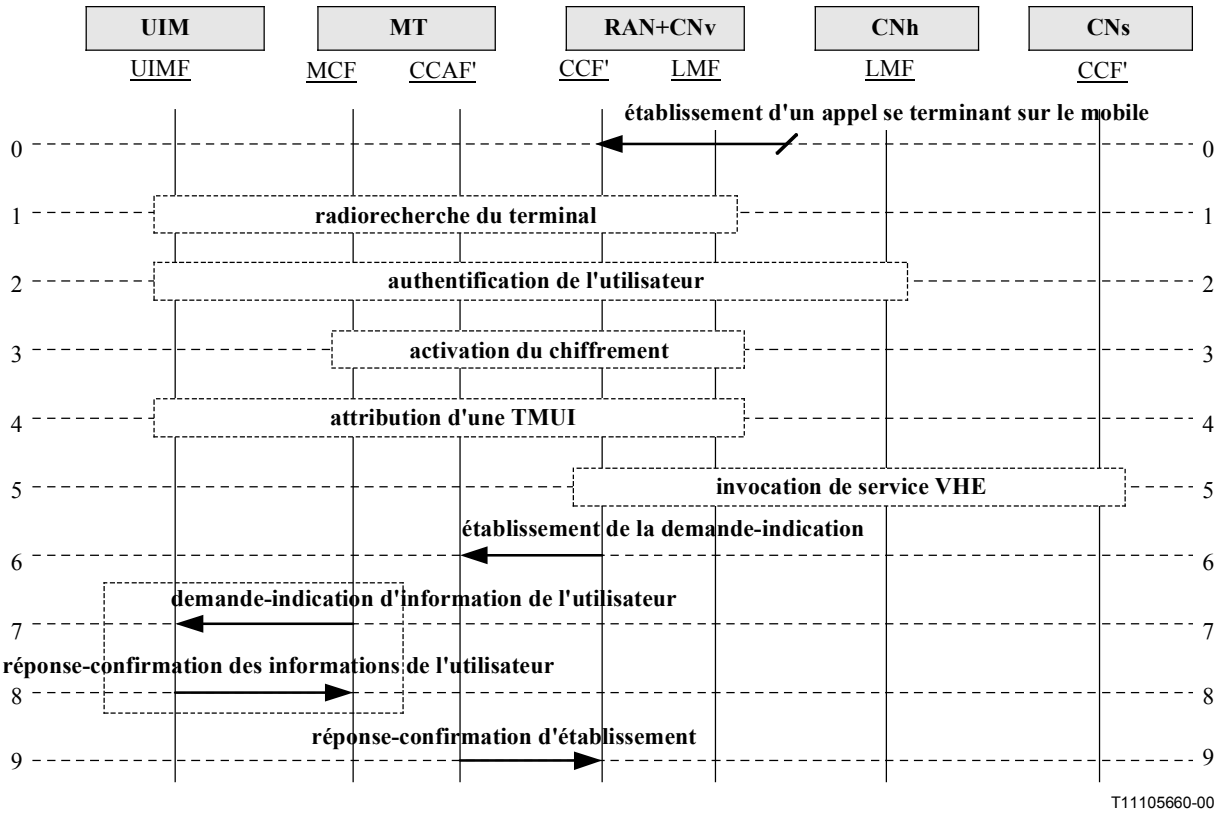


Figure 7.4.1-1/Q.1721 – Appel mobile entrant

0. **Etablissement d'un appel se terminant sur le mobile**: un appel arrive au système serveur pour un abonné mobile dans l'état de repos.

FEA0	– Avant d'établir l'appel, le réseau visité valide le correspondant appelé et peut invoquer des services basés sur la tentative de terminaison.

1. **Radiorecherche du terminal**: le système serveur peut essayer à ce moment d'effectuer une radiorecherche du terminal mobile. Il est possible que la radiorecherche ait été effectuée plus tôt pendant l'étape de routage ou qu'elle ne soit pas nécessaire si le terminal mobile est déjà occupé à un autre appel.

2. **Authentification de l'utilisateur**: l'authentification est effectuée si elle est nécessaire pour cette tentative d'appel.

3. **Activation du chiffrement**: le chiffrement est lancé s'il est nécessaire pour cette tentative d'appel.

4. **Attribution d'une TMUI**: l'attribution d'une TMUI, si elle est nécessaire, peut être effectuée à tout moment après que le chiffrement a été lancé.

5. **Invocation de service VHE**: en fonction du profil de l'abonné, le réseau visité peut invoquer une logique de service de réseau intelligent. Cela peut se produire à tout point de détection de déclenchement défini et actif.

6. **Etablissement de la demande-indication**: la CCF' continue pour établir l'appel.

Etablissement (réponse: succès ou échec)	demande-indication
ID utilisateur	M (Note)
Numéro de l'appelant (IMDN)	M

FEA6	– En option, invoque et attend l'exécution de la procédure d'information de l'utilisateur. – Etablit le canal d'appel et le canal support.
NOTE – Inclut soit l'IMUI ou la TMUI disponible. La TMUI est recommandée pour la sécurité sur la voie hertzienne.	

7. **Demande-indication d'information de l'utilisateur**: en option, le MCF demande l'entité UIMF pour de plus amples informations/instructions.

Informations de l'utilisateur (réponse: succès ou échec)	demande-indication
Demande de traitement de la terminaison	O (Note)

FEA7	– Donne à la MCF l'ordre d'accepter l'appel.
NOTE – Inclut pour demander les instructions de traitement d'appel de l'entité UIMF.	

8. **Réponse-confirmation des informations de l'utilisateur**: l'entité UIMF retourne les informations demandées à l'entité MCF.

Informations de l'utilisateur	réponse-confirmation
Informations de traitement de la terminaison	O (Note)

FEA8	– Appliquer le traitement de la terminaison d'appel indiquée.
NOTE – Inclut pour indiquer le type de traitement de terminaison d'appel à appliquer.	

9. **Réponse-confirmation d'établissement**: le CCAF' rapporte l'exécution réussie de l'établissement de l'appel et du canal support.

Etablissement	réponse-confirmation
Néant	(Note)

FEA9	– Néant.
NOTE – La réponse-confirmation est vide. Simplement, sa présence est suffisante pour indiquer le succès.	

7.4.2 Appel mobile entrant supplémentaire

L'appel entrant de mobile supplémentaire implique qu'un abonné mobile reçoive un deuxième appel alors qu'il est déjà sur un appel, c'est-à-dire un appel trois voies. La procédure suivie est similaire aux appels de mobile entrants, sauf que la radiorecherche ne sera pas nécessaire pour l'ajout du troisième correspondant.

7.5 Libération de l'appel mobile

7.5.1 Libération normale: à l'initiative du mobile

Voir Figure 7.5.1-1.

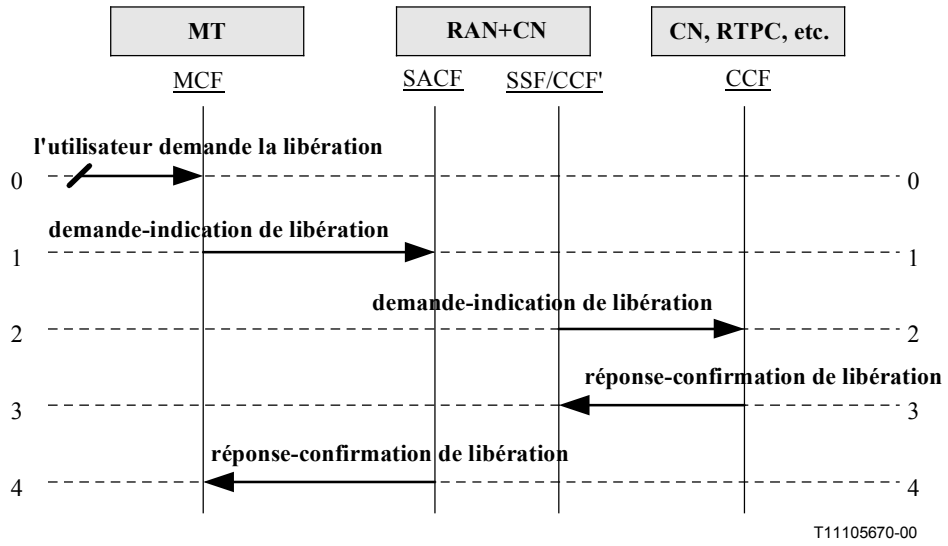


Figure 7.5.1-1/Q.1721 – Libération normale à l'initiative du mobile

0. **L'utilisateur demande la libération**: l'abonné mobile libère l'appel.

FEA0	– Le terminal mobile effectue une demande de libération.

1. **Demande-indication de libération**: la MCF envoie une demande de libération à la SACF.

Libération (réponse: succès ou échec)	demande-indication
TMUI	M

FEA1	– Prépare à envoyer la demande au réseau d'origine.

2. **Demande-indication de libération**: la SSF/CCF' du réseau visité envoie la demande de libération à la CCF dans le réseau d'origine.

Libération (réponse: succès ou échec)	demande-indication
TMUI	M

FEA2	– Libère les ressources associées à cet appel.

3. **Réponse-confirmation de libération**: la CCF dans le réseau d'origine retourne un accusé de réception de libération d'appel réussie à la SSF/CCF' du réseau visité.

Libération	réponse-confirmation
Néant	(Note)

FEA3	– Prépare à envoyer la réponse de libération au réseau visité.
NOTE – La réponse-confirmation est vide. Simplement sa présence est suffisante pour indiquer le succès.	

4. **Réponse-confirmation de libération**: la SACF du réseau visité envoie l'accusé de réception de la libération d'appel réussie à l'entité MCF.

Libération	réponse-confirmation
Néant	(Note)

FEA4	– Libère les ressources associées à cet appel.
NOTE – La réponse-confirmation est vide. Sa simple présence suffit à indiquer le succès.	

7.5.2 Libération normale: à l'initiative du réseau

Voir Figure 7.5.2-1.

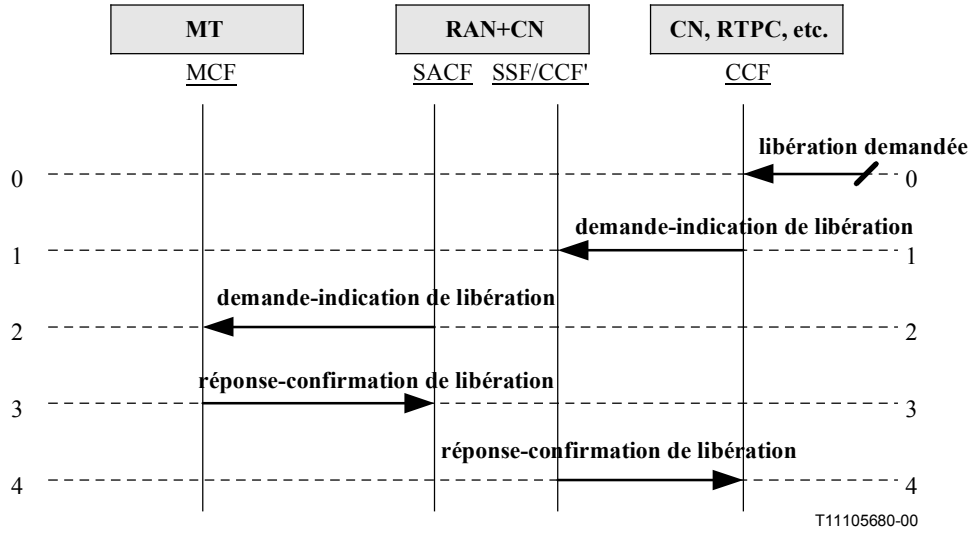


Figure 7.5.2-1/Q.1721 – Libération normale à l'initiative du réseau: diagramme des flux d'informations d'appel

0. **Libération demandée**: le réseau demande automatiquement la libération ou reçoit une demande de libération de la part de l'abonné du réseau (par exemple ligne filaire/abonné autre que mobile).

FEA0	– Le réseau se prépare à effectuer une demande de libération au réseau visité.

1. **Demande-indication de libération**: la CCF envoie une demande de libération à la SSF/CCF'.

Libération (réponse: succès ou échec)	demande-indication
TMUI	M

FEA1	– Prépare à envoyer la demande de libération au terminal mobile.

2. **Demande-indication de libération**: la SACF du réseau visité envoie la demande de libération à la MCF.

Libération (réponse: succès ou échec)	demande-indication
TMUI	M

FEA2	– Libère les ressources associées à cet appel.

3. **Réponse-confirmation de libération**: la MCF retourne un accusé de réception de libération d'appel réussi à la SACF du réseau visité.

Libération	réponse-confirmation
Néant	(Note)

FEA3	– Prépare à envoyer la réponse de libération au réseau d'origine.
NOTE – La réponse-confirmation est vide. Simplement, sa présence est suffisante pour indiquer le succès.	

4. **Réponse-confirmation de libération**: la SACF du réseau visité envoie l'accusé de réception de la libération d'appel réussie au réseau d'origine.

Libération	réponse-confirmation
Néant	(Note)

FEA4	– Libère les ressources associées à cet appel.
NOTE – La réponse-confirmation est vide. Simplement, sa présence est suffisante pour indiquer le succès.	

7.6 Appels d'urgence

7.6.1 Origine des appels d'urgence

Il convient que les appels d'urgence contournent les procédures d'authentification normale et d'enregistrement d'emplacement. Les appels d'urgence peuvent ne pas demander la présence d'un UIM dans le terminal mobile.

La procédure d'origine de l'appel d'urgence est similaire à un appel mobile sortant, sauf que les procédures d'authentification de l'utilisateur, d'enregistrement de l'emplacement de l'utilisateur, d'activation du chiffrement, d'affectation de la TMUI n'auront pas à être effectuées. De plus, le réseau serveur reçoit la demande d'appel et tente d'établir l'appel une fois que le numéro de routage est disponible. Le réseau serveur peut demander le service VHE à tout point de détection de déclenchement défini et actif. Pour un appel d'urgence, cela peut inclure la traduction d'un numéro d'urgence en un numéro local ou régional. La position géographique du terminal mobile peut être également déterminée à tout moment après que le réseau serveur reçoive la demande d'établissement. La détermination de la position géographique peut se produire avant l'invocation des services VHE.

7.6.2 Libération d'appel d'urgence: à l'initiative du réseau

La procédure de libération d'appel d'urgence à l'initiative du réseau est similaire à celle de libération d'appel à l'initiative du réseau. Dans un appel d'urgence, lorsque le point de réponse de sécurité publique (PSAP, *public safety answering point*) libère l'appel, la voie complète jusqu'à l'utilisateur sera libérée.

7.6.3 Libération d'appel d'urgence: à l'initiative du mobile

La procédure de libération d'appel d'urgence à l'initiative du mobile est similaire à celle de libération d'appel à l'initiative du mobile. Les ressources peuvent être conservées lorsque l'utilisateur demande la libération d'appel et la communication de l'appel d'urgence est suspendue. Cette procédure est en option et la procédure de libération normale d'appel (c'est-à-dire libération de la voie complète jusqu'à l'utilisateur) peut également être appliquée. Si les ressources sont conservées et que l'utilisateur demande ensuite l'établissement de l'appel, l'appel d'urgence suspendu est repris.

7.7 Appels de priorité

Les appels de priorité permettent à un abonné d'avoir un accès prioritaire à des canaux de voie ou de trafic au moment de la création de l'appel. Cette fonctionnalité permet d'obtenir un accès prioritaire à des canaux de voix ou de trafic en mettant en file d'attente ces appels de départ d'abonnés lorsque les canaux ne sont pas disponibles. Lorsqu'un canal devient disponible, l'abonné mis en file d'attente est servi selon le principe du premier arrivé premier servi et une base de priorité. L'abonné se voit attribuer un des niveaux de priorité *n* au moment où il souscrit son abonnement (où *n* a un minimum et un maximum). Les niveaux de priorité sont définis comme étant 1, 2, 3, …, *n*, 1 étant le niveau de priorité le plus élevé et *n* le niveau de priorité le plus bas. Le niveau de priorité, transporté dans le profil de l'abonné, est utilisé dans le RAN+CN pour affecter des canaux radio.

8 Commande de support et d'appels multimédias

Le présent paragraphe explique les flux d'informations pour l'établissement et la commande des appels multimédias, d'appels entre plusieurs participants et les services de données par paquets dont l'établissement de l'accès aux services Internet. Le présent paragraphe contient deux groupes de services: les téléservices et l'accès aux services Internet.

8.1 Changement de téléservice

La procédure de changement de téléservice permet à un utilisateur de IMT-2000 de modifier le service au cours d'un appel (exemple, passer d'une communication vocale à numérique et vice versa) qui peut entraîner une modification de la liaison d'accès à utiliser. A partir de la perspective d'interface réseau-réseau, le changement de téléservice doit permettre de modifier le support pour permettre à la capacité de ce dernier de prendre en charge le changement dans le type de service. Les changements dans les téléservices peuvent être à l'initiative soit de l'utilisateur d'origine soit de l'utilisateur de terminaison. Cependant, le flux d'informations de bout en bout (de mobile à mobile) pour le changement de téléservice traite des deux cas comme il est illustré dans la Figure 8.1-1.

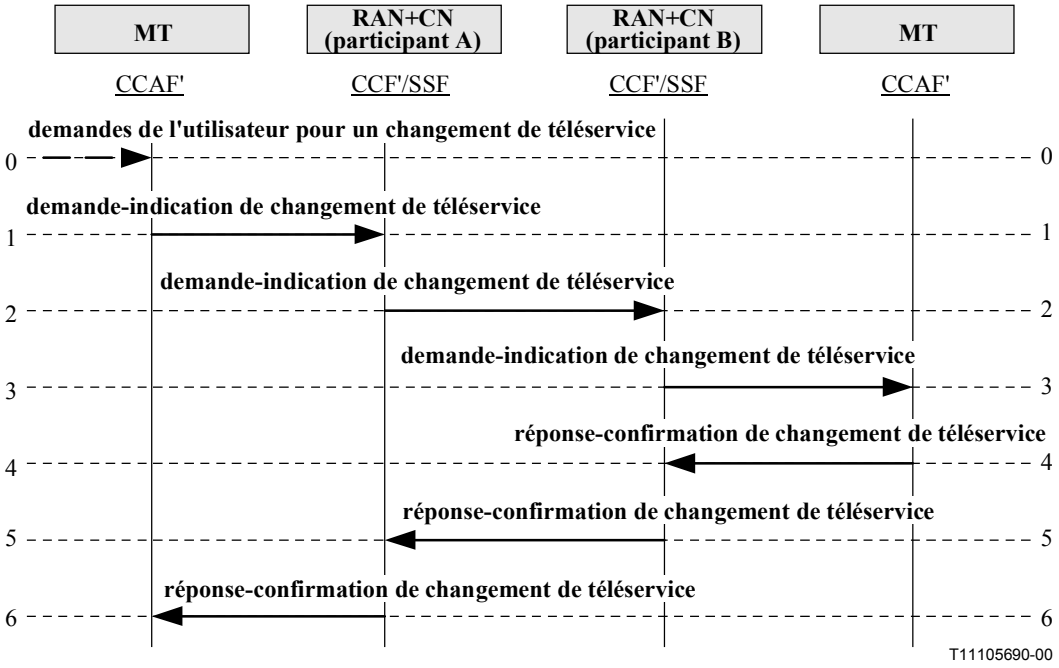


Figure 8.1-1/Q.1721 – Changement de téléservice

0. Demandes de l'utilisateur pour un changement de téléservice: l'utilisateur demande le changement de téléservice (liaison d'accès).

FEA0	– Demander un changement dans la connexion.

1. **Demande-indication de changement de téléservice**: s'utilise pour demander l'établissement d'une connexion.

Changement de téléservice (rapport: succès/échec)	demande-indication
Identité (ID) de l'appel	M
Type de téléservice	M

FEA1	– Dialoguer avec la gestion des ressources radio pour modifier la liaison d'accès selon la demande. – Envoyer la demande pour un changement de téléservice pour informer le ou les autres participants.

2. **Demande-indication de changement de téléservice**: est transmis par la CCF', fonction de commande d'appel CCF (CCF, *call control function*); fonction de commutation de service SSF (SSF, *service switching function*) pour effectuer la demande de changement de téléservice.

Changement de téléservice (rapport: succès/échec)	demande-indication
Identité (ID) de l'appel	M
Type de téléservice	M

FEA2	– Envoyer la demande de changement de téléservice.

3. **Demande-indication de changement de téléservice**: sert à demander au réseau du participant B pour un changement de téléservice.

Changement de téléservice (réponse: succès ou échec)	demande-indication
Identité (ID) de l'appel	M
Type de téléservice	M

FEA3	– Dialoguer avec la gestion des ressources radio pour la modification de la liaison d'accès. – Répondre pour confirmer le changement de téléservice (liaison d'accès).

4. **Réponse-confirmation de changement de téléservice**: est transmise par la CCAF', fonction d'agent de commande d'appel (CCAF', *call control agent function*) pour répondre à la demande de changement de téléservice.

Changement de téléservice	réponse-confirmation
Résultat	M

FEA4	– Répondre au réseau du participant A pour confirmer l'établissement de la connexion pour le changement de téléservice.

5. **Réponse-confirmation de changement de téléservice**: s'utilise pour confirmer que la connexion a été établie.

Changement de téléservice	réponse-confirmation
Résultat	M

FEA5	– Se connecter avec la nouvelle liaison d'accès.

6. **Réponse-confirmation de changement de téléservice**: s'utilise pour confirmer que la connexion a été établie.

Changement de téléservice	réponse-confirmation
Résultat	M

FEA6	– Aucun

8.2 Ajouter un média au cours d'un appel (utilisateur du mobile d'origine)

L'objectif de cette procédure est d'ajouter un média composant à un appel actif. On suppose que l'ajout d'un média composant est lié à une attribution dans l'appel d'un nouveau support dédié pour le prendre en charge. Voir Figure 8.2-1.

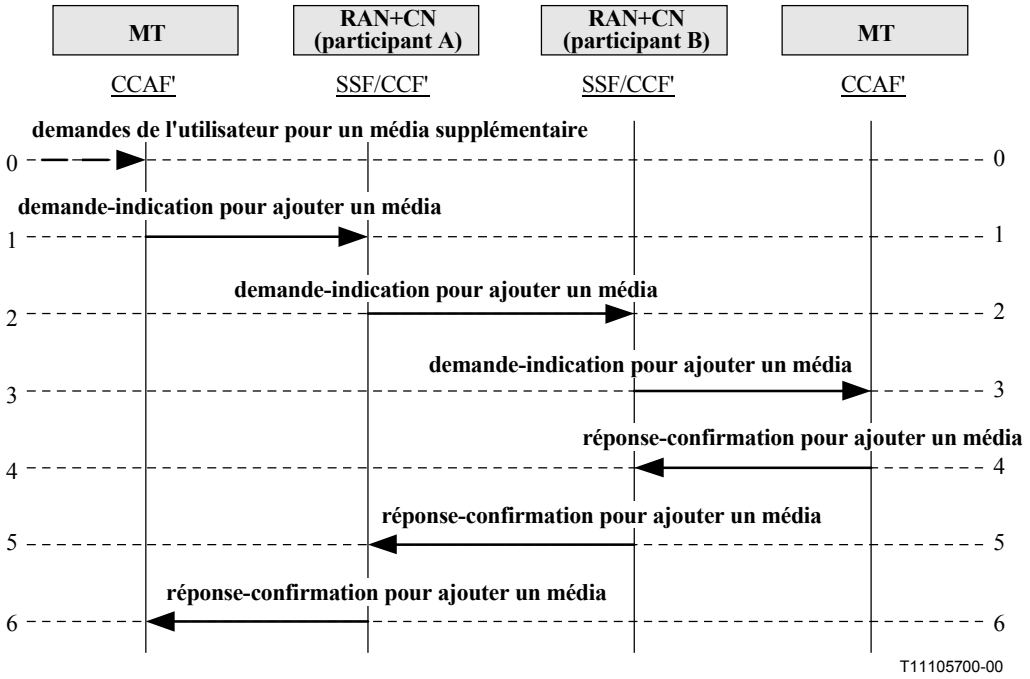


Figure 8.2-1/Q.1721 – Ajouter un média à un appel (utilisateur du mobile d'origine)

0. **Demandes de l'utilisateur pour un média supplémentaire**: l'utilisateur du mobile souhaite ajouter un média composant. Ceci indique le service supplémentaire désiré.

FEA0	– Demander un média supplémentaire. – Envoyer la demande pour la connexion de la liaison d'accès.

1. **Demande-indication pour ajouter un média**: sert à envoyer les informations que l'utilisateur souhaite pour ajouter un média composant à l'appel actif. Ceci indique le téléservice supplémentaire désiré.

Ajouter un média (réponse: succès ou échec)	demande-indication
Identité (ID) de l'appel	M
Type de média	M

FEA1	– Vérifier l'autorisation du service du participant A (opération interne). Demander en aval "Ajouter un média".

2. **Demande-indication pour ajouter un média**: sert à demander un média composant supplémentaire vers l'appel actif.

Ajouter un média (réponse: succès ou échec)	demande-indication
Identité (ID) de l'appel	M
Type de média	M

FEA2	– Vérifier l'autorisation du service du participant B (interne). – Envoyer la demande pour la connexion de la liaison d'accès.

3. **Demande-indication pour ajouter un média**: sert à envoyer les informations que l'utilisateur souhaite pour ajouter un média composant à l'appel actif. Ceci indique le téléservice supplémentaire désiré.

Ajouter un média (réponse: succès ou échec)	demande-indication
Identité (ID) de l'appel	M
Type de média	M

FEA3	– Vérifier l'autorisation du service. – Envoyer la demande pour la connexion de la liaison d'accès.

4. **Réponse-confirmation pour ajouter un média**: sert à informer que les mesures ont été prises pour ajouter la demande de média.

Ajouter un média	réponse-confirmation
Résultat	M

FEA4	– Relayer la réponse.

5. **Réponse-confirmation pour ajouter un média**: sert à informer que les mesures ont été prises pour ajouter la demande de média.

Ajouter un média	réponse-confirmation
Résultat	M

FEA5	– Relayer la réponse.

6. **Réponse-confirmation pour ajouter un média**: sert à informer que les mesures ont été prises pour ajouter la demande de média.

Ajouter un média	réponse-confirmation
Résultat	M

FEA6	– Demander l'établissement d'un canal support.

8.3 Supprimer un média d'un appel actif

Cette procédure vise à supprimer un média composant d'un appel actif. Ceci peut être soit décidé par l'utilisateur soit par le réseau (si les ressources nécessaires ne sont plus disponibles et si cela concerne un appel "de basse classe"). Le premier cas est illustré ici. Voir Figure 8.3-1.

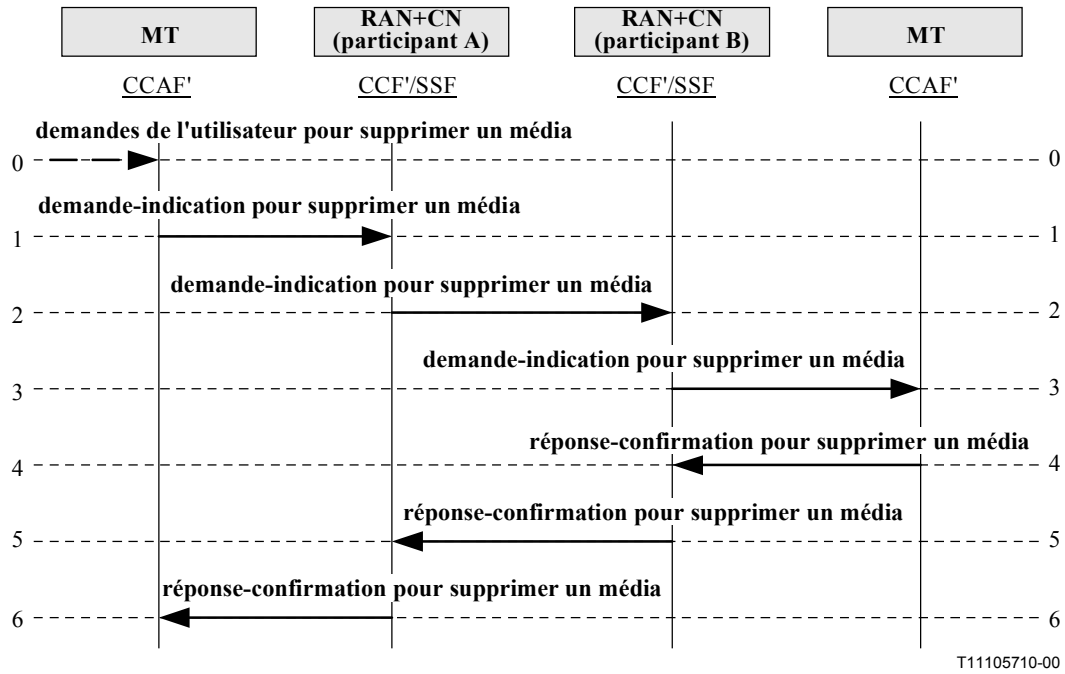


Figure 8.3-1/Q.1721 – Supprimer un média d'un appel multimédias (mobile d'origine)

0. **Demandes de l'utilisateur pour supprimer un média**: constitue la demande de l'utilisateur pour supprimer un média composant.

FEA0	– Envoyer une demande pour supprimer le média composant à partir de l'entité de contrôle des appels correspondante du réseau.

1. **Demande-indication pour supprimer un média**: s'utilise pour demander l'opération "supprimer un média".

Supprimer un média (réponse: succès ou échec)	demande-indication
Identité (ID) de l'appel	M
Identité (ID) du média	M

FEA1	– Identifie l'appel et le média correspondant à supprimer. – Envoyer la demande "supprimer un média" à l'entité de commande des appels distants, le réseau serveur du participant B.

2. **Demande-indication pour supprimer un média**: sert à envoyer la demande "supprimer un média" au réseau central de l'autre participant pour modifier l'appel (suppression du support concerné) dans la région sous leur responsabilité.

Supprimer un média (réponse: succès ou échec)	demande-indication
Identité (ID) de l'appel	M
Identité (ID) du média	M

FEA2	– Identifie l'appel et le média correspondant à supprimer. – Envoyer une demande pour supprimer le média vers le réseau d'accès. – Supprimer le média composant correspondant.

3. **Demande-indication pour supprimer un média**: sert à envoyer la demande "supprimer un média" au réseau d'accès pour modifier l'appel en supprimant le média sous son contrôle.

Supprimer un média (réponse: succès ou échec)	demande-indication
Identité (ID) de l'appel	M
Identité (ID) du média	M

FEA3	– Identifie l'appel et le média correspondant à supprimer. – Dialoguer avec les éléments de gestion des ressources radio. – Supprimer le média composant correspondant.

4. **Réponse-confirmation pour supprimer un média**: sert à confirmer que le réseau d'accès distant et le réseau central ont supprimé correctement le média composant et son ou ses supports connexes.

Supprimer un média	réponse-confirmation
Résultat	M

FEA4	– Supprimer le média composant et son support associé.

5. **Réponse-confirmation pour supprimer un média**: sert à confirmer que le réseau d'accès distant et le réseau central ont supprimé correctement le média composant et son ou ses supports connexes.

Supprimer un média	réponse-confirmation
Résultat	M

FEA5	– Supprimer le média composant et son support associé.

6. **Réponse-confirmation pour supprimer un média**: sert à envoyer le résultat à l'entité fonctionnelle (FE, *functional entity*) de commande des appels d'origine.

Supprimer un média	réponse-confirmation
Résultat	M

FEA6	– Demander libération des médias associés aux supports.

8.4 Appel de point à multipoint

8.4.1 Ajout de participants (de mobile à mobile)

Dans un appel à deux participants, chacun peut demander l'ajout d'un autre participant à la communication. Le participant A devient la racine de la connexion réseau de type 1 (c'est-à-dire,

la connexion point à point) demandant qu'un nouveau participant C de mobile soit ajouté à la communication. L'ancienne connexion réseau de type 1 devient une connexion réseau de type 2 (c'est-à-dire connexion point à multipoint) avec les participants racines et feuilles présents dans la configuration. La demande pour l'opération "ajouter participant" requiert aussi qu'une procédure de "changement de téléservice" ou "de notification" soit effectuée pour la communication en cours entre les différents participants. Le présent sous-paragraphe traite à la fois des procédures d'ajouts des participants à l'initiative de la racine et des feuilles.

8.4.1.1 Ajout de participants (à l'initiative de la racine)

La Figure 8.4.1-1 illustre le diagramme des flux des informations pour l'ajout de participants à l'initiative de la racine. Participant C est ajouté à la communication déjà en cours entre participant A et participant B. Pour le nouveau participant, participant C, dans le réseau visité de destination, une procédure d'appel entrant du mobile est appliquée dans le cadre de la procédure courante "établissement de la connexion".

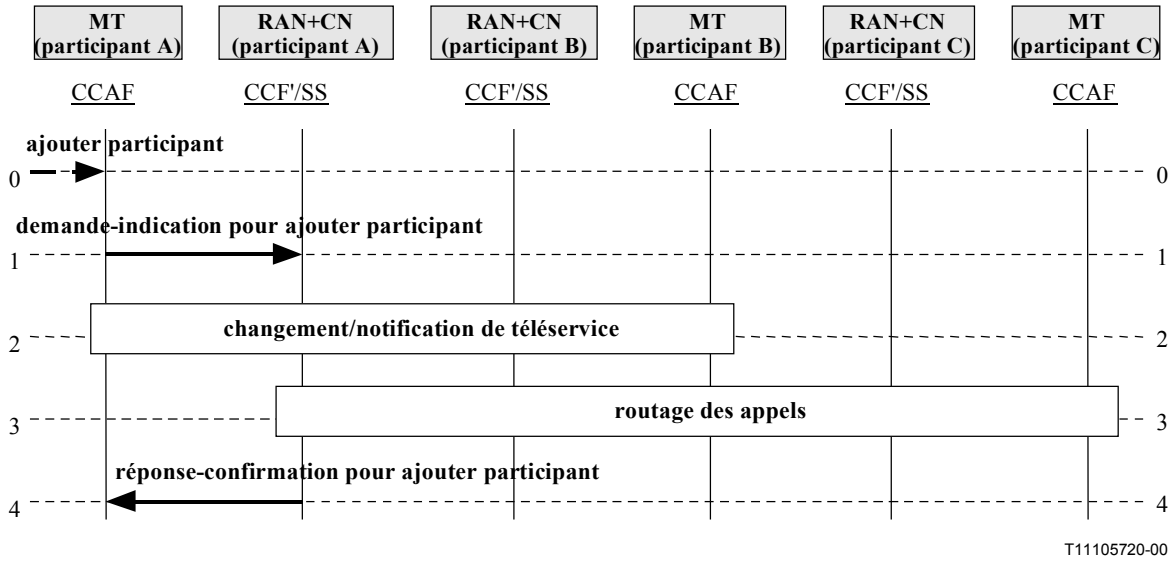


Figure 8.4.1-1/Q.1721 – Ajout de participants (à l'initiative de la racine)

0. Ajouter participant: est exécutée par l'utilisateur participant A pour ajouter un autre participant, participant C à un appel en cours avec participant B.

FEA0	– Envoyer demande ajouter participant. – Une demande de changement de téléservice est effectuée pour les participants prenant part à la communication.

1. **Demande-indication pour ajouter participant**: sert à exécuter l'ajout d'un participant à une connexion en cours.

Ajouter participant (rapport: succès ou échec)	demande-indication
Identité (ID) de l'appel	M
Numéro appelé	M
Référence des extrémités	M

FEA1	– Identifier l'utilisateur à ajouter. – Sélectionner et réserver les ressources sortantes. – Envoyer une demande de configuration pour lancer l'établissement des appels et des connexions.

2. **Changement/notification de téléservice**: sert à demander le changement du service (exemple, de point à point à point-multipoint) et traiter l'ajout de la liaison d'accès (si nécessaire).

FEA2	– Demander le changement du service (exemple, de point-multipoint à point à point).

3. **Routage des appels**: s'utilise pour demander l'établissement d'un appel devant être suivi par une connexion support.

4. **Réponse-confirmation pour ajouter participant**: s'utilise pour accuser réception du succès de la demande ajouter participant.

Ajouter participant	**réponse-confirmation**
Identité (ID) de l'appel	M
Référence des extrémités	M

FEA4	– Envoyer la confirmation ajouter participant. – Demander l'établissement du canal ou des canaux supports.

8.4.1.2 Ajout de participants (à l'initiative d'une feuille)

La Figure 8.4.1-2 illustre le diagramme des flux des informations pour un ajout de participants à l'initiative d'une feuille. Participant D doit être ajouté par participant C à la communication qui est déjà en cours entre participant A, participant B et participant C. Le participant C informe le participant racine, le participant A de l'ajout du participant D à la communication. A partir de ce moment, le réseau central (CN, *core network*) du participant racine reprend et effectue une procédure "ajout de participant (à l'initiative de la racine)".

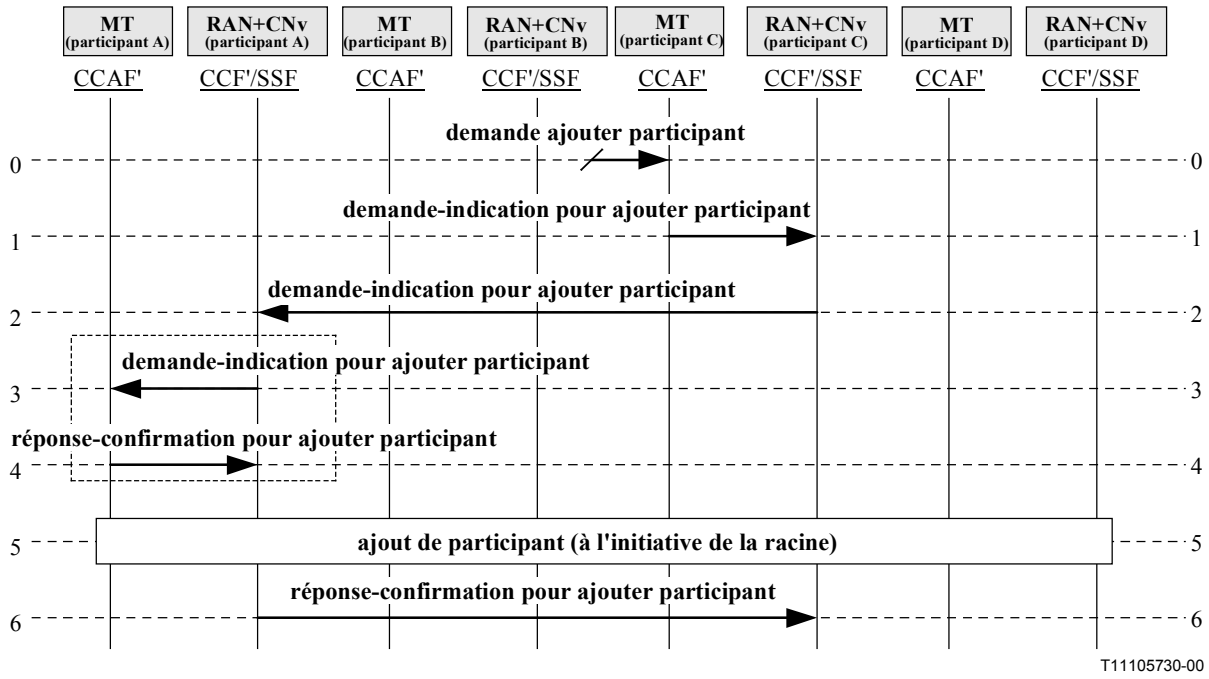


Figure 8.4.1-2/Q.1721 – Ajout de participants (à l'initiative de la feuille)

Les flux d'informations, les éléments d'informations et les actions des entités fonctionnelles associés à cette procédure, sont décrits dans le même ordre que les flux illustrés dans la Figure 8.4.1-2.

0. **Demande ajouter participant**: est exécutée par l'utilisateur participant C pour ajouter un autre participant, participant D, à un appel actif avec les participants A et B.

1. **Demande-indication pour ajouter participant**: sert à exécuter l'ajout d'un participant à une connexion en cours.

Ajouter participant (rapport: succès ou échec)	demande-indication
Identité (ID) de l'appel	M
Numéro appelé	M

FEA1	– Envoyer une demande ajouter participant au participant racine. – Sélectionner et réserver les ressources sortantes.

2. **Demande-indication pour ajouter participant**: sert à lancer l'ajout d'un participant à une connexion en cours.

Ajouter participant (rapport: succès ou échec)	demande-indication
Identité (ID) de l'appel	M
Numéro appelé	M
Référence des extrémités	M

FEA2	– Identifier le nouveau participant à ajouter. – Informer tous les participants en ligne (sauf le demandeur) de l'ajout du participant. – Sélectionner et réserver les ressources sortantes. – Envoyer la demande de configuration pour exécuter l'établissement des connexions et des appels. – Fournir la référence des extrémités.

3. **Demande-indication pour ajouter participant**: (en option) sert à exécuter l'ajout d'un participant à une connexion en cours.

Ajouter participant (réponse: ni succès ni échec)	demande-indication
Identité (ID) de l'appel	M
Numéro appelé	M
Référence des extrémités	M

FEA3	– Identifier le nouveau participant à ajouter. – Accuser réception de la demande pour ajouter participant. – Exécuter la procédure ajouter participant.

4. **Réponse-confirmation pour ajouter participant**: s'utilise pour accuser réception de la demande ajouter participant.

Ajouter participant	réponse-confirmation
Résultat	M

FEA4	– Aucun.

5. **Ajout de participant (à l'initiative de la racine)**: s'utilise pour demander l'ajout d'un participant par le participant racine d'un appel en cours.

6. **Réponse-confirmation pour ajouter participant**: s'utilise pour accuser réception du succès de la demande ajouter participant.

Ajouter participant	réponse-confirmation
Résultat	M

FEA6	– Aucun.

8.4.2 Suppression de participants

Un participant feuille peut être supprimé d'une connexion point à multipoint par une demande soit du participant racine soit du participant feuille lui-même.

8.4.2.1 Suppression de participants (à l'initiative du participant racine)

Le participant racine (participant A) peut demander qu'un participant feuille (participant C) soit supprimé de la connexion. Dans cette procédure, les ressources entre le participant C et le réseau central sont normalement libérées par le déclenchement du réseau central. Voir Figure 8.4.2-1.

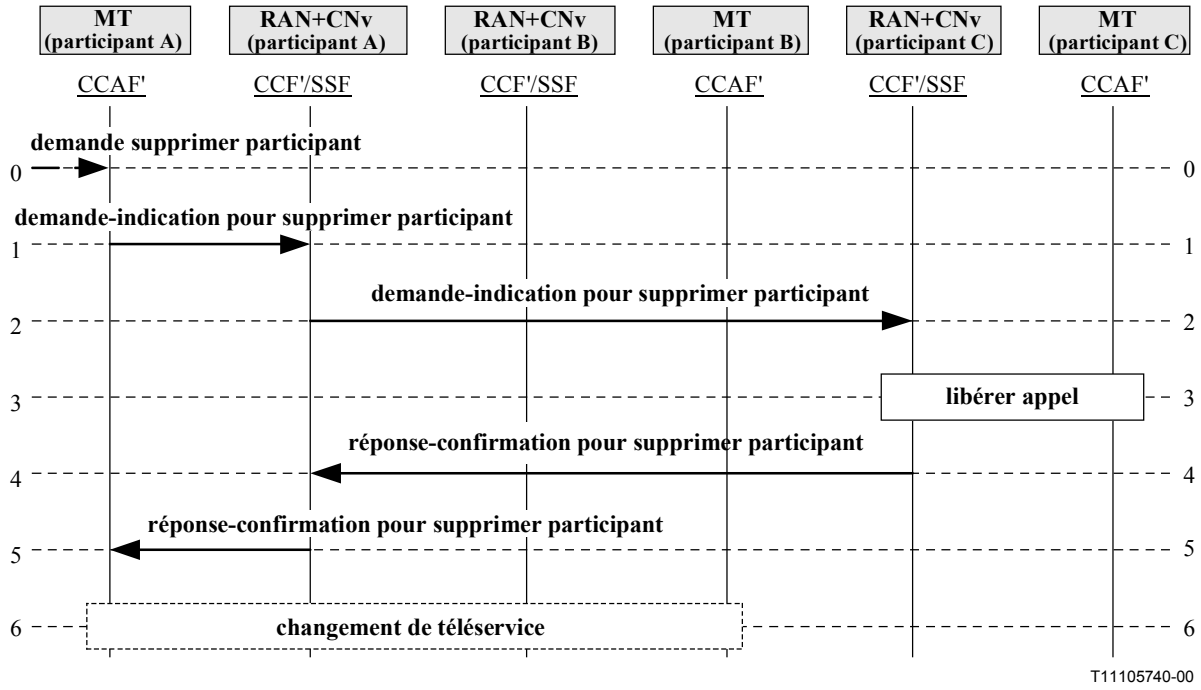


Figure 8.4.2-1/Q.1721 – Suppression de participants (à l'initiative du participant racine)

0. **Demande supprimer participant**: constitue la demande de l'utilisateur pour supprimer un participant en ligne.

FEA0	– Identifier le participant à supprimer. – Vérifier l'état de tous les autres participants feuilles associés à la connexion le cas échéant.

1. **Demande-indication pour supprimer participant**: sert à lancer l'abandon d'un participant d'une connexion en cours.

Supprimer participant (réponse: succès ou échec)	**demande-indication**
Identité (ID) de l'appel	M
Référence des extrémités	M
Cause	M

FEA1	– Identifier l'utilisateur demandeur. – Accuser réception que l'utilisateur demandeur est racine. – Identifier le participant à supprimer. – Vérifier l'état de tous les autres participants feuilles associés à cette connexion.

2. **Demande-indication pour supprimer participant**: sert à exécuter l'abandon d'un participant d'une connexion en cours.

Supprimer participant (réponse: succès ou échec)	demande-indication
Identité (ID) de l'appel	M
Référence des extrémités	M
Cause	M

FEA1	– Identifier l'utilisateur demandeur. – Accuser réception que l'utilisateur demandeur est racine. – Identifier le participant à supprimer. – Vérifier l'état de tous les autres participants feuilles associés à cette connexion. – Exécuter la procédure libérer appel.

3. **Libérer appel**: procédure (à l'initiative du réseau) pour demander la suppression d'un participant de la communication.

FEA3	– Envoyer réponse supprimer participant/libérer appel.

4. **Réponse-confirmation pour supprimer participant**: s'utilise pour informer que la demande supprimer participant a réussi.

Supprimer participant	réponse-confirmation
Cause	O (Note)

FEA4	– Relayer la réponse-confirmation supprimer participant.
NOTE – Envoyer les informations sur la cause de la libération du participant si disponibles.	

5. **Réponse-confirmation pour supprimer participant**: s'utilise pour informer que la demande supprimer participant a réussi.

Supprimer participant	réponse-confirmation
Cause	O (Note)

FEA5	– Relayer la réponse-confirmation supprimer participant.
NOTE – Envoyer les informations sur la cause de la libération du participant si disponibles.	

6. **Changement de téléservice**: la procédure est une demande pour l'éventuel changement de téléservice pour le participant A et le participant B, passant de point à multipoint à point à point.

FEA6	– Demander le changement de service (exemple, de point-multipoint à point à point).

8.4.2.2 Suppression de participant (à l'initiative du participant feuille)

Sur reçu de la demande de libération d'un participant feuille à supprimer (participant C), le réseau central informe le participant racine (participant A) que le participant feuille s'est retiré en envoyant une demande supprimer participant. Voir Figure 8.4.2-2.

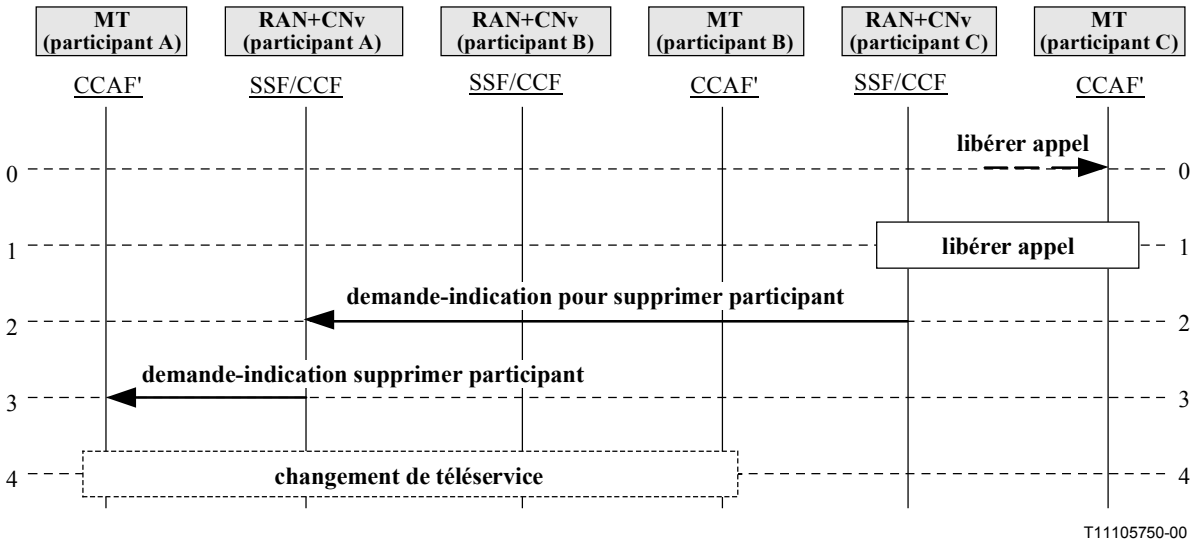


Figure 8.4.2-2/Q.1721 – Suppression de participant (à l'initiative d'un participant feuille)

0. **Libérer appel**: est lancé par un participant feuille demandant d'être supprimé de la communication/connexion.

FEA0	– Démarrer la procédure de libération de l'appel du mobile. – Identifier le participant feuille (participant demandeur) à supprimer. – Envoyer une demande supprimer participant au réseau du participant racine.

1. **Libération de l'appel**: procédure qui doit libérer l'appel entre le participant feuille supprimé et les participants restant en communication.

FEA1	– Envoyer une demande supprimer participant au terminal mobile du participant racine.

2. **Demande-indication pour supprimer participant**: est envoyée pour informer l'abandon d'un participant feuille d'une connexion en cours.

Supprimer participant (réponse: ni succès ni échec)	**demande-indication**
Identité (ID) de l'appel	M
Référence des terminaisons	M
Cause	M

FEA2	– Identifier le participant feuille supprimé en fonction de la référence des extrémités. – Vérifier l'état de tous les autres participants feuilles associés à la connexion le cas échéant. – Envoyer l'indication supprimer participant.

3. **Demande-indication supprimer participant**: est envoyée pour informer l'abandon d'un participant feuille d'une connexion en cours.

Supprimer participant (réponse: ni succès ni échec)	demande-indication
Identité (ID) de l'appel	M
Référence des terminaisons	M
Cause	M

FEA3	– Identifier le participant feuille supprimé en fonction de la référence des extrémités. – Vérifier l'état de tous les autres participants feuilles associés à la connexion le cas échéant. – Envoyer l'indication supprimer participant.

4. **Changement de téléservice**: (en option) sert à traiter un changement de téléservices pour les participants restant dans la communication.

FEA4	– Demander changement de service (exemple: de point à multipoint à point à point).

8.5 Accès aux services Internet

L'accès aux services Internet permet à un abonné itinérant de l'IMT-2000 de lancer une session de service de données dans un réseau central (CN) visité. Une fois la session de service de données établie, l'abonné est itinérant dans le CN visité suivant sans interruption dans la session de service de données. Lors du démarrage d'une session de service de données, le terminal mobile de l'abonné peut posséder une ou plusieurs adresses IP qui lui a été attribué définitivement par le CN de rattachement ou une adresse IP publique (une ou plusieurs) peut lui être attribuée(s) dynamiquement par le CN de rattachement ou par le CN visité. Le contexte du routage dans le réseau IMT-2000 est établi lorsque la session est lancée et il est mis à jour chaque fois que le terminal mobile est itinérant dans le CN visité suivant.

Les procédures décrites dans le présent sous-paragraphe sont obligatoires lors de l'itinérance entre des réseaux IMT-2000 avec différentes architectures de réseaux centraux (c'est-à-dire, de membres différents de la famille IMT-2000). L'itinérance entre les réseaux implémentés avec le même membre de la famille peut utiliser des procédures spécifiques aux membres de la famille.

8.5.1 Etablissement des sessions de services de données par paquets

Pour accéder aux services de données en paquets, le terminal mobile itinérant est enregistré avec le réseau visiteur IMT-2000 en utilisant des procédures d'authentification courante et d'enregistrement du terminal et en demandant l'accès aux installations de données en paquets. Le terminal mobile est enregistré pour l'usage des ressources de données en paquets en accédant aux installations de données en paquets. L'architecture de l'IMT-2000 permet une séparation des capacités de la fonction de gestion de l'emplacement (LMF, *location management function*) et de la fonction de gestion d'authentification associée (AMF, *authentication management function*) qui se rapportent à l'accès aux installations et aux capacités du LMFp (et AMFp associé) qui se rapportent aux services de données en paquets.

La Figure 8.5.1-1 illustre le diagramme des flux des informations pour cette procédure. Les étapes 4-7 peuvent être répétées afin de prendre en charge plusieurs sessions de données à partir du même terminal mobile.

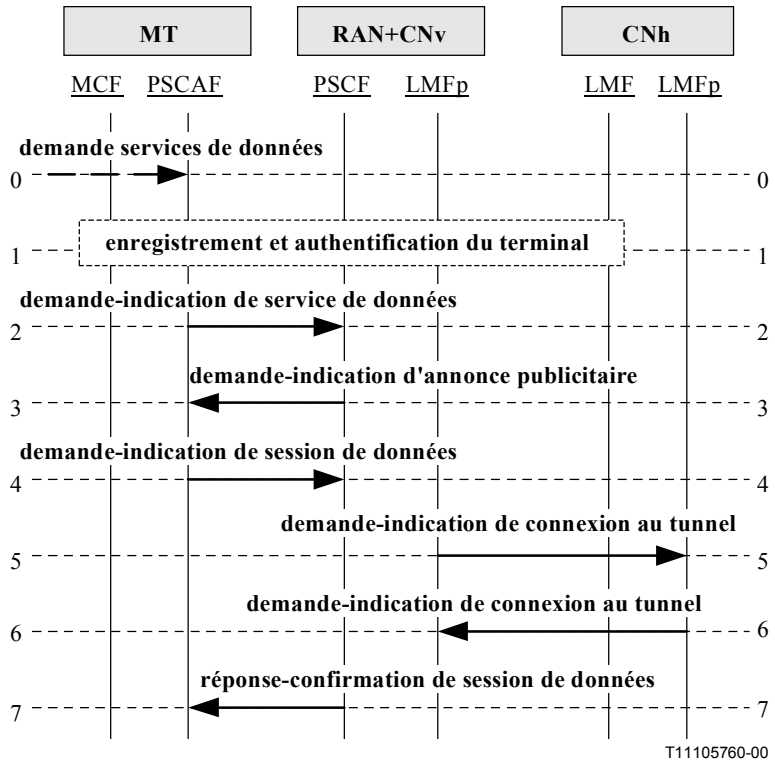


Figure 8.5.1-1/Q.1721 – Etablissement des sessions de données en paquets

0. **Demande services de données**: l'utilisateur exécute une session de services de données en paquets.

FEA0	– Demander l'établissement d'une session de services de données précédée par l'enregistrement et l'authentification du terminal.

1. **Enregistrement et authentification du terminal**: est requis si ce n'est déjà fait.

2. **Demande-indication de service de données**: sert à lancer une session de services de données dans le réseau visité en demandant le service.

Service de données (réponse: ni succès ni échec)	demande-indication
Identité (ID) de l'utilisateur	M
Type de services (données)	M

FEA2	– Utilise la procédure de couches de liaison pour établir une liaison d'accès suivie par la demande "annonce publicitaire".

3. **Demande-indication d'annonce publicitaire**: sert au flux vers le terminal pour demander l'établissement d'une session de données lorsqu'un nouvel identificateur d'accès au réseau (NAI, *network access identifier*) est détecté.

Annonce publicitaire (réponse: ni succès ni échec)	demande-indication
Adresse IP (PSCF)	M
Adresse IP (PSCF-Public)	M (Note)
Valeur de mise à l'épreuve	M
NAI (PSCF)	M

FEA3	– Répondre à l'annonce publicitaire avec une demande session de données si elle détecte un nouveau NAI de fonction de commande de service par paquet (PSCF, *packet service control function*). – Spécifier un port UDP bien connu et l'adresse IP du PSCF comme destination pour ces informations.
NOTE – Cette adresse IP est l'adresse de l'agent étranger (exemple, elle est utilisée comme point de terminaison du tunnel vu à partir de la fonction de commande de passerelle de service par paquet (PSGCF, *packet service gateway control function*).	

4. **Demande-indication de session de données**: est envoyée de PSCAF au PSCF dans le réseau visité sur la liaison d'accès établie pour demander l'établissement d'une nouvelle session[2] de données.

Session de données (réponse: succès ou échec)	demande-indication
Identité (ID) de la session	O (Note 1)
NAI (MT)	M
NAI (PSCFpv)	M
Adresse IP (MT)	O (Note 2)
Adresse IP (PSCF Public)	M
Discriminateur du service	O (Note 3)
Valeur de mise à l'épreuve (à partir de PSCF)	M
Réponse à la mise à l'épreuve	M
Méthode d'encapsulage	M
Durée de vie de la session de données	M

FEA4	– Déterminer l'adresse de LMFp en fonction du discriminateur du service. – Demander l'établissement d'une connexion au tunnel pour cette session de données. – Peut réduire la durée de vie de la session de données proposée avant d'envoyer ces informations à son LMFp.
NOTE 1 – Si c'est un cas de session multiple. NOTE 2 – Attribution statique si l'adresse IP est statique et permanente autre qu'attribution dynamique. NOTE 3 – La LMFp peut avoir besoin du discriminateur du service à des fins d'autorisation.	

5. **Demande-indication connexion au tunnel**: est établie du LMFp visitée au LMFp de rattachement du terminal mobile pour authentifier et autoriser le terminal mobile visiteur à utiliser les services de données en paquets dans le réseau visité.

---

[2] Ne pas confondre la procédure "d'enregistrement" du terminal mobile avec l'enregistrement pour établir une session de données, le nom "session de données" a été choisi pour ce flux.

Connexion au tunnel (réponse: succès ou échec)	demande-indication
NAI (MT)	M
NAI (PSCFpv)	M
NAI (PSCFv)	M
Adresse IP (MT)	O (Note 1)
Adresse IP (PSCF Public)	M
Discriminateur du service	O (Note 2)
Valeur de mise à l'épreuve (à partir de PSCF)	M
Réponse à la mise à l'épreuve	M
Méthode d'encapsulage	M
Durée de vie de la session de données	M

FEA5	– Déterminer la PSGCF en fonction du discriminateur du service. – Authentifier le terminal mobile en utilisant la valeur de mise à l'épreuve, la réponse à la mise à l'épreuve et le secret qu'il partage avec son terminal mobile. – Peut attribuer une adresse IP au terminal mobile ou il peut décider que le PSGCF doit attribuer cette adresse. Comme requis par la demande-indication de connexion au tunnel, le PSGCF peut être dynamiquement attribué ou il peut avoir été déjà préattribué statiquement au terminal mobile. – Si le PSGCF est attribué dynamiquement, alors le LMFp de rattachement peut soit l'attribuer dans le réseau de rattachement ou le LMFp de rattachement peut décider que le réseau visité doit attribuer le PSGCF. – Peut aussi générer un ensemble de clés de sécurité et des indices de paramètres de sécurité (SPI, *security parameter indices*) qui seront distribués au terminal mobile, le PSCF visité et PSGCF pour prendre en charge le cryptage et les associations de sécurité entre ces entités. – Utiliser les secrets partagés avec le PSCAF, PSGCF de rattachement, et le LMFp visité. – Peut aussi réduire la durée de vie de la session de données proposée avant d'envoyer ces informations au PSGCF ou au LMFp visité. – Renvoyer la réponse de connexion au tunnel au LMFp visité indiquant que le PSGCF dans le réseau visité doit être attribué.
NOTE 1 – Attribution de l'adresse IP statique si l'adresse IP est statique ou permanente autre qu'attribution dynamique. NOTE 2 – Le LMFp peut avoir besoin du discriminateur du service à des fins d'autorisation.	

6. **Réponse-confirmation de connexion au tunnel**: est envoyée par le LMFp de rattachement du terminal mobile vers le LMFp visité pour autoriser le terminal mobile à utiliser les services de données en paquets dans le réseau visité.

Eléments d'informations	réponse-confirmation
Résultat (indication d'attribution de PSGCF)	M
Adresse IP (PSGCF public)	M
Adresse IP (MT) incluse si attribuée par le réseau de rattachement	O (Note)
Durée de vie de la session de données	M
Informations sur la sécurité	M

FEA6	– Répondre pour confirmer l'établissement d'une connexion au tunnel. – Envoyer le résultat pour l'établissement de la session de données.
NOTE – L'adresse IP ne peut pas être demandée si aucune nouvelle attribution par le réseau de rattachement n'a eu lieu.	

7. **Réponse-confirmation de session de données**: est une réponse à une demande pour l'établissement d'une nouvelle session de données.

Enregistrement	réponse-confirmation
Identité (ID) de la session	O (Note)
Résultat (succès ou échec)	M
Adresse IP (PSGCF public)	M
Adresse IP (MT)	M
Informations sur la sécurité	M
Durée de vie de la session	M

FEA7	– Continue la session de données, aucune action supplémentaire requise.
NOTE – Si fourni par PSCAF dans flux 4.	

8.5.2 Itinérance durant une session de données par paquets établie

Lors de l'itinérance dans le réseau suivant visité, un PSGCF dans le réseau d'ancrage a déjà été attribué au terminal mobile. Le réseau d'ancrage peut soit être le réseau de rattachement soit le réseau visité où la session de données a été exécutée. Le terminal mobile peut être enregistré avec le réseau visiteur suivant en utilisant les procédures courantes d'authentification et d'enregistrement du terminal. En invoquant la procédure gestion des ressources radio (RRM, *radio resource management*), le terminal mobile établit une liaison d'accès avec le PSCF dans le réseau suivant visité. Puisque l'adresse annoncée NAI PSCF est différente de celle existante, le PSCAF démarre une nouvelle procédure "établissement d'une session de services de données en paquets" comme illustré dans la Figure 8.5.2-1.

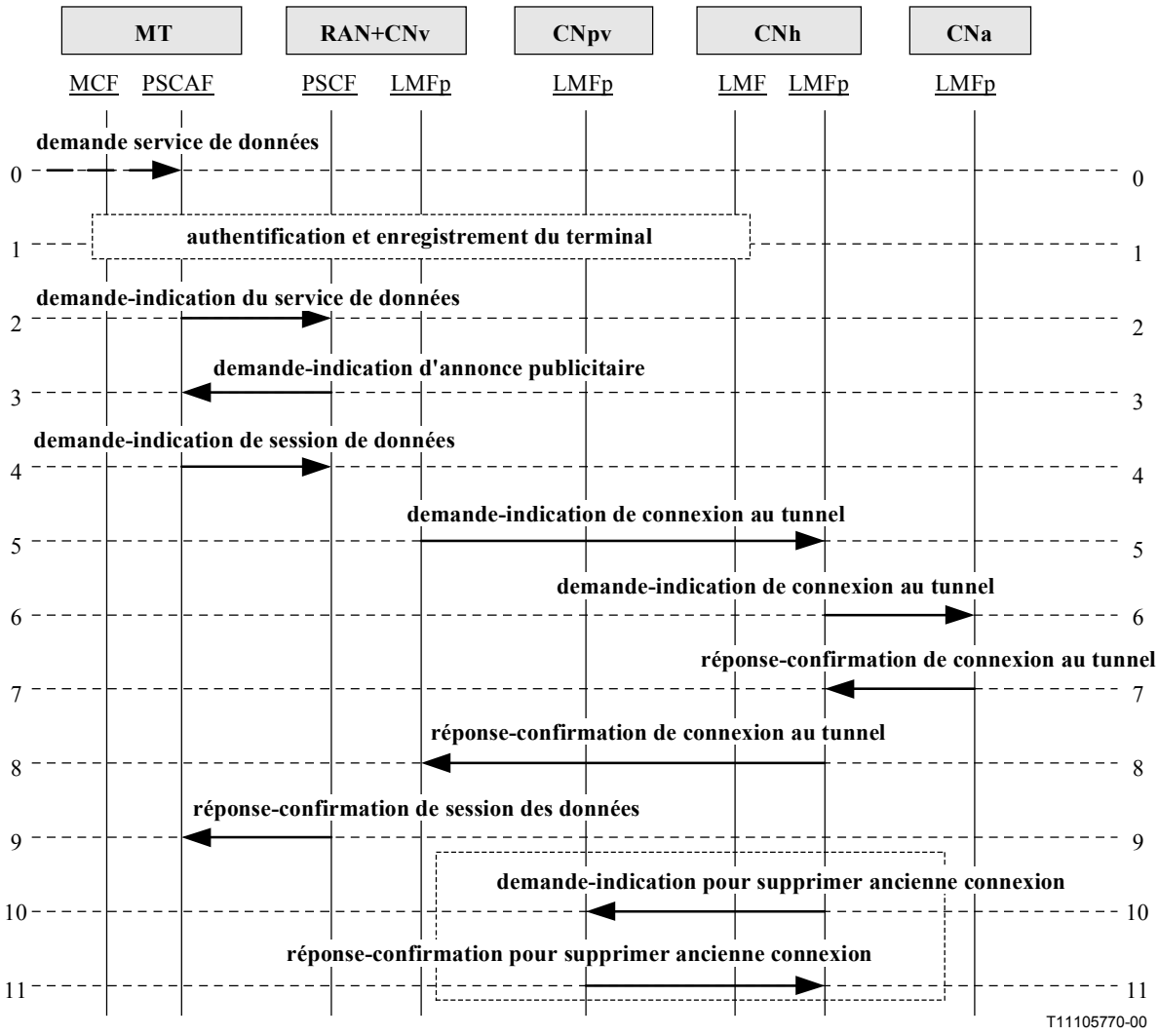


Figure 8.5.2-1/Q.1721 – Itinérance durant une session de données établie

Ce diagramme de flux des informations est semblable au diagramme de flux des informations du 8.5.1 jusqu'à l'opération "connexion au tunnel" où le flux est transmis (du réseau de rattachement) au réseau d'ancrage. En outre, l'opération "annuler ancienne connexion" doit être effectuée une fois la nouvelle connexion établie.

0. **Demande service de données**: est le déclenchement de l'enregistrement du terminal mobile durant une session de données en paquets établie.

FEA0	– Exécuter l'authentification et l'enregistrement du terminal si nécessaire.

1. **Authentification et enregistrement du terminal**: sert à l'enregistrement du terminal mobile auprès du réseau visité avant de demander le service de données en paquets.

FEA1	– Demander l'établissement d'une session de services de données.

2. **Demande-indication du service de données**: le terminal mobile lance une session de services de données dans le réseau visité.

Service de données (réponse: ni succès ni échec)	demande-indication
Identité (ID) de l'utilisateur	M
Type de services (données)	M

FEA2	– Demander que la configuration de la liaison d'accès soit suivie par la demande de l'opération "Annonce publicitaire" au terminal.

3. **Demande-indication d'annonce publicitaire**: est envoyée au terminal pour demander l'établissement d'une session de données lorsqu'un nouveau NAI est détecté.

Annonce publicitaire (rapport: ni succès ni échec)	demande-indication
Adresse IP (PSCFv)	M
Adresse IP (PSCFv-Public)	M
Valeur de mise à l'épreuve (PSCFv)	M
NAI (PSCFv)	M

FEA3	– Répondre à l'annonce publicitaire par un enregistrement s'il détecte un nouveau NAI PSCF. – Indiquer un port UDP bien connu et l'adresse IP du PSCF visité comme destination pour ces informations. – Indiquer un port UDP qui doit être utilisé par le PSCF visité lors du renvoi des informations sur la réponse au PSCAF.

4. **Demande-indication de session de données**: est envoyée du PSCAF au PSCF dans le réseau visité sur la liaison d'accès établie pour demander l'établissement d'une nouvelle connexion au tunnel pour la session de données existante.

Enregistrement (réponse: succès ou échec)	demande-indication
Identité (ID) de la session	O (Note 1)
NAI (MT)	M
NAI (PSCFpv)	M
Adresse IP (MT)	M
Adresse IP (PSCFv Public)	M
Discriminateur du service	M (Note 2)
Adresse IP (PSGCF Public)	M
Valeur de mise à l'épreuve (PSCFv)	M
Réponse à la mise à l'épreuve	M
Méthode d'encapsulage	M
Durée de vie de la session de données	M

FEA4	– Communiquer avec son LMFp pour demander l'établissement d'une nouvelle connexion au tunnel avec le PSGCF d'ancrage pour la session de données existante. – Stocker localement toutes les informations qui lui ont été fournies par le PSCAF dans la demande-indication enregistrement et relier ces informations à la liaison d'accès et le IMSI si elles ont été fournies durant l'établissement de la liaison d'accès. – Peut réduire la durée de vie de la session de données proposée avant d'envoyer ces informations à son LMFp. – Attribuer un identificateur de transaction à cette transaction. Ensuite, il envoie les informations obtenues à partir de la demande-indication enregistrement à son LMFp. Une association de sécurité entre le PSCF visiteur suivant et son LMFp aura été arrangée au préalable. – Stocker le ID de la session.
NOTE 1 – Si cet élément est fourni dans le flux 4 par le PSCAF. NOTE 2 – Le discriminateur de service tel qu'il est utilisé au 8.4.1, n'est pas utilisé ici car la session est déjà active dans le PSGCF. Le LMFp ne sélectionne donc pas le PSGCF. Toutefois, le LMFp peut avoir besoin du discriminateur de service à des fins d'autorisation.	

5. **Demande-indication de connexion au tunnel**: est envoyée du LMFp visité au LMFp de rattachement du terminal mobile pour authentifier et autoriser le terminal mobile visiteur et établir une nouvelle connexion au tunnel entre le PSCF visité et le PSGCF. En fonction des informations précédentes du NAI, le LMFp visité détermine que le PSCF précédent se situe dans un réseau différent. Les NAI du terminal mobile sont utilisés pour localiser son LMFp de rattachement. Une association de sécurité entre le LMFp visité et le LMFp de rattachement doit exister avant que toute information puisse être échangée entre ces deux entités. Le LMFp visité envoie ces informations avec celles qui ont été incluses dans la demande-indication d'enregistrement initiale vers le LMFp de rattachement.

Connexion au tunnel (rapport: succès ou échec)	**demande-indication**
NAI (MT)	M
NAI (PSCFpv)	M
NAI (PSCFv)	M
Adresse IP (MT)	M
Adresse IP (PSCFv Public)	M
Discriminateur du service	M
Adresse IP (PSGCF Public)	M
Valeur de mise à l'épreuve (à partir de PSCFv)	M
Réponse à la mise à l'épreuve	M
Méthode d'encapsulage	M
Durée de vie de la session de données	M

FEA5	– Authentifier le terminal mobile en utilisant valeur de mise à l'épreuve, réponse à la mise à l'épreuve et le secret qu'il partage avec son terminal mobile. – Détecter que ceci est une session de données en paquets établie et il saura si le réseau d'ancrage se trouve dans le réseau de rattachement ou le réseau visité où la session a été lancée. – Peut décider d'utiliser les clés de sécurité existantes et les indices des paramètres de sécurité (SPI) qui ont été attribués au PSCF précédent ou il peut générer de nouvelles valeurs pour ces paramètres. – Lorsqu'il transmet les clés de sécurité et les SPI au PSCAF, PSGCF d'ancrage, LMFp d'ancrage, et le LMFp visité, le LMFp de rattachement utilise les secrets partagés avec ces entités. – Lorsque le réseau d'ancrage n'est pas le réseau de rattachement, le LMFp de rattachement envoie la demande-indication connexion au tunnel au LMFp d'ancrage dans le réseau visité où la session a été lancée. – Dans le cas où le PSGCF se trouve dans le réseau de rattachement, une demande est envoyée par le LMFp de rattachement à son PSGCF dans le réseau de rattachement pour demander l'établissement d'une nouvelle connexion au tunnel entre le PSCF visité et le PSGCF de rattachement.

6. **Demande-indication de connexion au tunnel**: est envoyée par le LMFp de rattachement au LMFp d'ancrage pour demander l'établissement d'une nouvelle connexion au tunnel entre le PSGCF d'ancrage et le PSCF visité. Le LMFp de rattachement a enregistré le NAI du LMFp d'ancrage lorsque la session de données a été lancée.

Connexion au tunnel (réponse: succès ou échec)	**demande-indication**
NAI (MT)	M
Adresse IP (MT)	M
Adresse IP (PSCFv Public)	M
Adresse IP (PSGCF Public)	M
Méthode d'encapsulage	M
Durée de vie de la session de données restante	M
Clés de sécurité et SPI	M
Durée de vie de la session de données	M

FEA6	– Détecter que ceci est une session de données établie. – Envoyer une demande à son PSGCF pour demander l'établissement d'une nouvelle connexion au tunnel entre le PSCF visité et le PSGCF d'ancrage.

7. **Réponse-confirmation de connexion au tunnel**: est envoyée par le LMFp d'ancrage au LMFp de rattachement pour indiquer si la demande pour établir une nouvelle connexion au tunnel entre le PSCF visité et le PSGCF d'ancrage a été acceptée ou refusée.

Connexion au tunnel	**réponse-confirmation**
Résultat (indication de l'attribution PSGCF)	M
Adresse IP (PSGCF Public)	M
Adresse IP (MT)	M
Durée de vie de la session de données	M

FEA7	– Répondre pour confirmer l'autorisation pour établir la nouvelle session de données. – En option, demander que le réseau précédemment visité supprime l'ancienne connexion, opération "supprimer ancienne connexion".

8. **Réponse-confirmation de connexion au tunnel**: est envoyée par le LMFp de rattachement du terminal mobile au LMFp visité pour autoriser le service de données en paquets pour le terminal mobile dans le réseau visité et indiquer qu'une nouvelle connexion au tunnel avec le PSGCF d'ancrage a été établie.

Connexion au tunnel	réponse-confirmation
Résultat (indication de l'attribution PSGCF)	M
Adresse IP (PSGCF – Public)	M
Adresse IP (MT)	M
Durée de vie de la session de données	M
Clés de sécurité et SPI	M

FEA8	– Informe le PSCF visité si une nouvelle connexion au tunnel a été établie.

9. **Réponse-confirmation de session des données**: est envoyée par le PSCF visité au PSCAF en réponse à la demande-indication enregistrement demandant l'établissement d'une nouvelle connexion au tunnel. Ces informations sont envoyées à la liaison d'accès établie.

Session des données	réponse-confirmation
Résultat (indication de l'attribution PSGCF)	M
Adresse IP (PSGCF – Public)	M
Adresse IP (MT)	M
Clés de sécurité et SPI	M
Durée de vie de la session de données	M
Identité (ID) de la session	O (Note)

FEA9	– Aucune action requise.
NOTE – Si fournie par PSCAF.	

10. **Demande-indication pour supprimer ancienne connexion**: (en option) s'adresse au LMFp de rattachement pour informer le LMFp auparavant visité de supprimer toutes les informations locales qui se rapportent à l'ancienne connexion au tunnel avec le PSGCF d'ancrage. Cet IF est indépendant de IF 9.

Supprimer ancienne connexion (réponse: ni succès ni échec)	demande-indication
NAI (MT)	M
Adresse IP (MT)	M
NAI (PSCFpv)	M
Adresse IP (PSGCF – Public)	M

FEA11	– Répondre pour confirmer la suppression de l'ancienne connexion.

11. **Réponse-confirmation pour supprimer ancienne connexion**: (en option) s'adresse au LMFp précédemment visité pour envoyer les informations sur la confirmation au LMFp de rattachement indiquant que l'ancienne connexion au tunnel a été supprimée.

Supprimer ancienne connexion	réponse-confirmation
Résultat	M

FEA11	– Aucune action requise.

8.5.3 Terminaison des sessions de services de données en paquets

8.5.3.1 Terminaison des sessions lancée par le terminal mobile

Soit le terminal soit le réseau peut décider de terminer une session de données en paquets active. Le présent sous-paragraphe décrit la procédure de flux d'informations sur la suppression de l'enregistrement lancée par le terminal. La Figure 8.5.3-1 illustre le diagramme de flux d'informations pour cette procédure. Les étapes 2-4 peuvent être répétées afin de prendre en charge plusieurs sessions de données à partir du même terminal mobile.

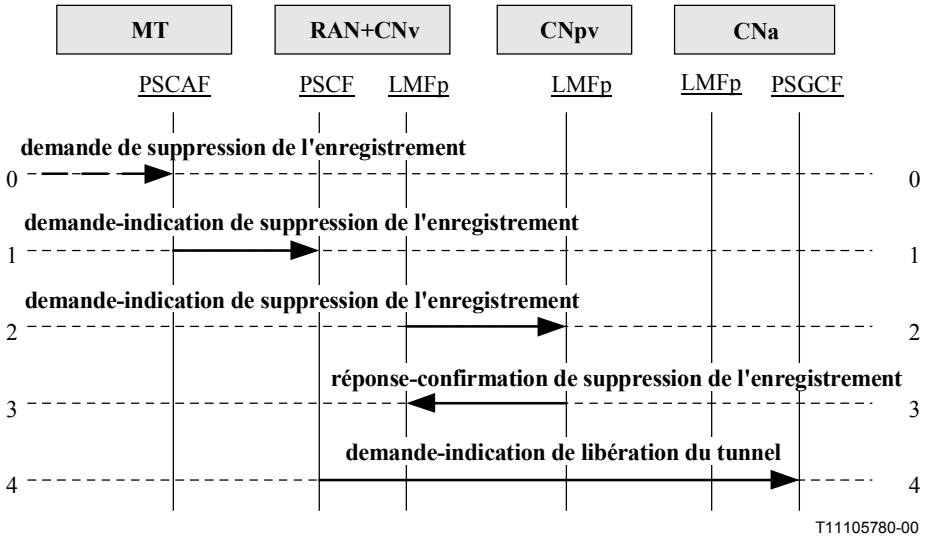


Figure 8.5.3-1/Q.1721 – Terminaison des sessions de données en paquets lancée par le terminal

0. **Demande de suppression de l'enregistrement**: sert à exécuter une suppression de l'enregistrement des services de données en paquets.

FEA0	– Demander la terminaison de la session de données en paquets active.

1. **Demande-indication de suppression de l'enregistrement**: est envoyée par le terminal mobile pour informer le réseau IMT-2000 de sa demande de suppression de l'enregistrement de la session des services de données en paquets active.

Suppression de l'enregistrement (aucune réponse prévue)	demande-indication
Identification de l'utilisateur (IMUI ou TMUI)	M
Adresse IP (PSGCF – Public)	M
Adresse IP (PSCFv – Public)	M
NAI (PSCFv)	M
Adresse IP (MT)	M
NAI (MT)	M
Durée de vie de la session de données	M

FEA1	– Le LMFp visité met à jour sa base de données comme approprié. – Le LMFp visité informe le LMFp de rattachement.

2. **Demande-indication de suppression de l'enregistrement**: provient du LMFp visité envoyant la demande-indication de suppression de l'enregistrement au LMFp de rattachement pour indiquer que le terminal n'est plus accessible dans le système visité.

Suppression de l'enregistrement (réponse: succès/échec)	demande-indication
Adresse IP (PSGCF – Public)	M
Adresse IP (PSCFv – Public)	M
NAI (PSCFv)	M
Adresse IP (MT)	M
NAI (MT)	M
Durée de vie de la session de données	M
Adresse source de la session	O (Note)

FEA2	– Le LMFp de rattachement met à jour sa base de données comme approprié. – Le LMFp de rattachement répond au LMFp visité.
NOTE – Dans le cas de sessions multiples, le PSCFv doit associer le signal de réponse-confirmation avec le signal demande-indication correspondant avec les informations sur l'adresse source.	

3. **Réponse-confirmation de suppression de l'enregistrement**: est envoyée par le LMFp de rattachement accusant réception de la demande de supprimer l'enregistrement du terminal.

Suppression de l'enregistrement	réponse-confirmation
Adresse IP (MT)	M
NAI (MT)	M
Adresse source de la session	O (Note)

FEA3	– Le système visité exécute la libération du tunnel vers le PSCF de passerelle.
NOTE – Dans le cas de sessions multiples, le PSCFv doit associer le signal de réponse-confirmation avec le signal demande-indication correspondant avec les informations sur l'adresse source.	

4. **Demande-indication de libération du tunnel**: est envoyée par le PSCF serveur informant le PSGCF d'ancrage de libérer le tunnel vers le réseau visité.

Libération du tunnel (réponse: ni succès ni échec)	demande-indication
Adresse IP (PSGCF – Public)	M
Adresse IP (PSCFv – Public)	M
NAI (PSCFv)	M
Adresse IP (MT)	M
NAI (MT)	M
Durée de vie de la session de données	M

FEA4	– Le PSGCF dans le réseau d'ancrage informe son LMFp local qu'il ne sert plus de passerelle vers le terminal dont l'enregistrement est supprimé. – Le LMFp d'ancrage met à jour sa base de données comme approprié.

8.5.3.2 Terminaison des sessions à l'initiative du réseau

Soit le terminal soit le réseau peut décider de terminer une session de données en paquets active. Le présent sous-paragraphe décrit la procédure de flux d'informations sur la suppression de l'enregistrement à l'initiative du réseau. La Figure 8.5.3-2 illustre le diagramme de flux d'informations pour cette procédure. Les étapes 2-4 peuvent être répétées afin de prendre en charge plusieurs sessions de données à partir du même terminal mobile.

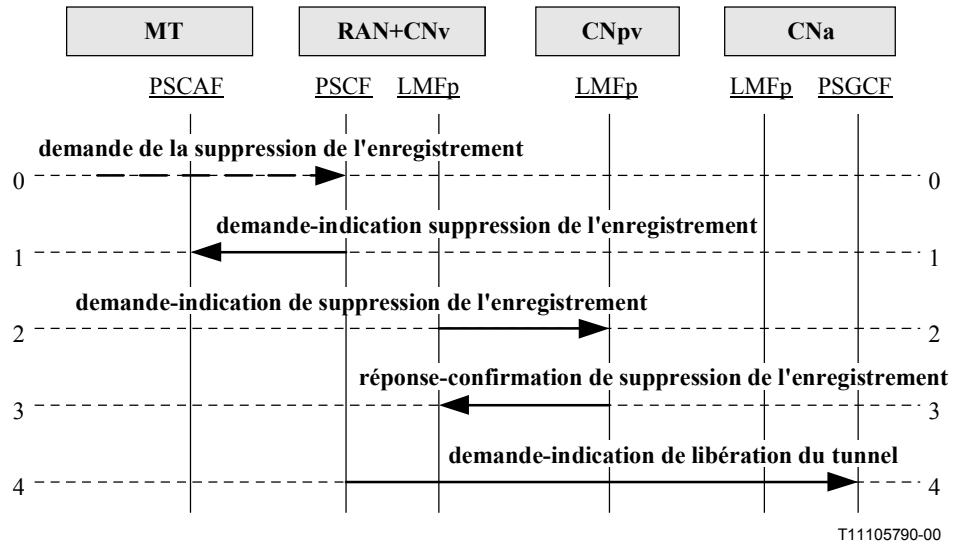


Figure 8.5.3-2/Q.1721 – Terminaison des sessions de données en paquets à l'initiative du réseau

0. **Demande de la suppression de l'enregistrement**: le réseau exécute une suppression de l'enregistrement des services de données en paquets.

FEA0	– Informer le terminal (PSCAF) pour la suppression de l'enregistrement.

1. **Demande-indication suppression de l'enregistrement**: sert à informer le terminal de l'intention du réseau de supprimer l'enregistrement du terminal de la session des services de données en paquets active.

Suppression de l'enregistrement (réponse: ni succès ni échec)	demande-indication
Identification de l'utilisateur (IMUI ou TMUI)	M

FEA1	– Le terminal se prépare à libérer la liaison d'accès.

2. **Demande-indication de suppression de l'enregistrement**: envoie la demande de suppression de l'enregistrement au LMFp de rattachement pour indiquer que le terminal n'est plus accessible dans le système visité.

Suppression de l'enregistrement (rapport succès/échec)	demande-indication
Adresse IP (PSGCFv – Public)	M
Adresse IP (PSCFv – Public)	M
NAI (PSCFv)	M
Adresse IP (MT)	M
NAI (MT)	M
Durée de vie de la session de données	M
Adresse source de la session	O (Note)

FEA2	– Le LMFp de rattachement met à jour sa base de données comme approprié. – Le LMFp de rattachement répond au LMFp visité.
NOTE – Dans le cas de sessions multiples, le PSCFv doit associer le signal de réponse au signal demande-indication correspondant avec les informations sur l'adresse source.	

3. **Réponse-confirmation de suppression de l'enregistrement**: s'adresse au LMFp de rattachement pour accuser réception de la demande de supprimer l'enregistrement du terminal.

Suppression de l'enregistrement	réponse-confirmation
Adresse IP (MT)	M
NAI (MT)	M
Adresse source de la session	O (Note)

FEA3	– Le système visité exécute la libération du tunnel vers le PSCF de passerelle.
NOTE – Dans le cas de sessions multiples, le PSCFv doit associer le signal de réponse au signal de demande correspondant avec les informations sur l'adresse source.	

4. **Demande de libération du tunnel**: le PSCF serveur informe le PSGCF d'ancrage de libérer le tunnel vers le réseau visité.

Libération du tunnel (aucune réponse prévue)	demande-indication
Adresse IP (PSGCFv – Public)	M
Adresse IP (PSCFv – Public)	M
NAI (PSCFv)	M
Adresse IP (MT)	M
NAI (MT)	M
Durée de vie de la session de données	M

FEA4	– Le PSGCF dans le réseau d'ancrage informe son LMFp local qu'il ne sert plus de passerelle vers le terminal dont l'enregistrement est supprimé. – Le LMFp d'ancrage met à jour sa base de données comme approprié.

9 Environnement de rattachement virtuel

L'invocation des services dans le système IMT-2000 peut survenir à tout moment durant le traitement des appels. Il peut également survenir, soit conjointement avec ou indépendamment d'un appel, par rapport au traitement de la gestion de la mobilité ou pour le traitement de l'authentification. Les services sont offerts selon les informations contenues dans le profil des services de l'abonné. Ce dernier répertorie les services d'abonnements standard de base ou complémentaires ainsi que les déclencheurs et les informations connexes (exemple: critères de déclenchements, adresse logique de services associés, etc.) pour les services personnalisés basés sur le VHE. Il n'est pas prévu que les réseaux IMT-2000 visités offrent des services personnalisés (c'est-à-dire, des services personnalisés offerts par des exploitants de réseaux de rattachement/fournisseurs de services). Cependant, la capacité et les procédures du VHE permettent au réseau serveur de mettre ces services à la disposition des utilisateurs visiteurs.

Dans le concept du VHE, l'approvisionnement des services et le fonctionnement du réseau peuvent être distincts, permettant aux services d'être offerts par des réseaux autres que ceux offrant les capacités de traitement des appels du réseau de rattachement. Dans certains cas, le réseau de rattachement offre la logique de service et agit donc comme réseau de prise en charge.

Dans la description suivante (sous-paragraphes 9.1 et 9.2), le réseau de prise en charge est le réseau où la logique de service est localisée et exécutée (indiqué par CNs). Le réseau serveur ou visité est le réseau où l'utilisateur est itinérant lorsque l'exécution du service est demandée (indiqué par CNv). Le réseau de rattachement (indiqué par CNh) est celui où la fonction de gestion de l'emplacement (LMFh) de rattachement et la fonction de gestion d'authentification (AMFh) de rattachement se trouvent. Le CNs et le CNh peuvent être le même réseau.

Les Recommandations Q.1701 et Q.1711 identifient deux scénarios de réalisation du VHE pour IMT-2000 CS-1. Ils constituent le scénario "commande directe de rattachement" décrit au 9.1 et le scénario "contrôle des services de relais" décrit au 9.2.

9.1 "Commande directe du rattachement"

Dans le scénario du VHE "commande directe du rattachement", le réseau de prise en charge offre une logique de service à un réseau visité servant l'abonné itinérant pour prendre en charge les services basés sur le VHE de cet abonné. La logique de service dans le réseau de prise en charge est invoquée via la capacité de déclenchement du réseau intelligent RI du réseau visité. Le pré-arrangement entre les réseaux de prise en charge et visités peut être nécessaire pour filtrer les invocations de déclenchement.

9.1.1 Procédure de service de haut niveau de "commande directe du rattachement"

Dans le cadre du schéma des flux d'informations de bout en bout, cette procédure se divise en quatre étapes: création de l'appel, invocation d'une logique de service VHE, acheminement/routage de l'appel et connexion de l'appel (dans le cas de services liés à un appel, des procédures identiques de service VHE s'appliquent aux scénarios non-liés à un appel). Le présent sous-paragraphe traite des flux d'informations en ce qui concerne le sous-système d'invocation d'une logique de service VHE, et considère les flux d'informations pour les trois autres sous-systèmes, comme étant des procédures ordinaires dans le contexte des flux d'informations de bout en bout.

Les suppositions suivantes sont établies en fonction des flux d'informations d'invocation d'une logique de services VHE:

- dans ce scénario, un accord préalable entre le réseau de prise en charge et les réseaux de rattachement, ou entre le réseau de prise en charge et les réseaux visités, est indispensable pour le filtrage d'invocation de déclenchement;
- le réseau serveur/visité a une capacité de réseau intelligent pour déclencher la logique de service requise.

La Figure 9.1.1-1 représente un diagramme de synthèse du flux d'informations (IF, *information flow*) de haut niveau en ce qui concerne le scénario d'environnement VHE "commande directe de rattachement". A propos de la figure ci-dessous, les remarques suivantes devraient être prises en compte:

- dans le cas des services liés à un appel, la figure inclut seulement le côté création de l'appel des flux en provenance d'un participant demandeur. Une interaction similaire pourrait avoir lieu entre un appel d'arrivée et un participant demandé;
- d'autres moyens de lancement d'une logique de services non liés à des appels, tels que la gestion de la mobilité ou la gestion d'authentification, se comportent de la même façon, bien que la messagerie provienne d'une entité fonctionnelle différente dans le "RAN+CNh ou v" (voir 9.1.3 et 9.1.4);
- le cas d'une notification à une logique de service est un sous-ensemble de la Figure 9.1.1-1 (c'est à dire que le flux 2 ne serait pas requis);
- la figure est très simplifiée étant donné qu'elle n'illustre pas l'étendue totale de l'interaction de logique de service prise en charge par un réseau intelligent, par exemple, elle ne reflète pas l'interaction étendue avec une logique de service (qui peut se prolonger jusqu'à la libération de l'appel), l'interaction entre les utilisateurs prise en charge par une logique de service, etc.

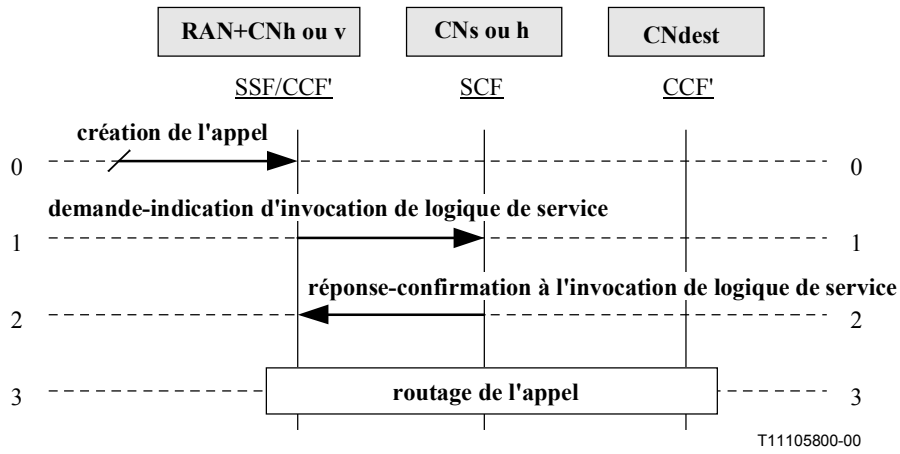


Figure 9.1.1-1/Q.1721 – "Commande directe de rattachement" de haut- niveau liée à un appel

0. **Création de l'appel**: un abonné crée un appel. Les données obtenues en provenance du réseau de rattachement lors de la souscription, contiendront les informations pour permettre au réseau serveur de prendre en charge l'invocation de services VHE[3].

FEA0	– Poursuit le traitement de l'appel jusqu'à ce qu'un déclencheur armé soit rencontré à un TDP, et que les critères pour le déclencheur armé soient satisfaits.

1. **Demande-indication d'invocation de logique de service**: s'utilise pour invoquer une logique de service à l'entité SCF associée au déclencheur dont les critères sont satisfaits. Cette demande achemine des informations sur l'abonné, sur l'état de l'appel ainsi que sur les conditions de déclenchement advenues.

Invocation de logique de service (réponse: succès ou échec)	**demande-indication**
Eléments d'information dans le flux d'informations initiateur de logique de service	Par [5]
IMUI	M

FEA1	– Effectue une logique de service.

2. **Réponse-confirmation à l'invocation de logique de service**: fournit des instructions sur le traitement de l'appel qui doivent être effectuées par l'entité invocatrice à la demande de la logique de service.

Invocation de logique de service	**réponse-confirmation**
Eléments d'information dans le flux d'informations répondant à la logique de service.	Par [5]

FEA2	– Si possible, effectue les instructions du traitement de l'appel.

3. **Routage de l'appel**: s'utilise pour poursuivre le traitement de l'appel et le connecter à un réseau de destination, si ceci est l'action appropriée selon les informations contenues dans la réponse-confirmation de l'appel de logique de service.

La logique de services en ce qui concerne les services personnalisés basés dans un environnement VHE et utilisant la "commande directe de rattachement" est fournie par le réseau de rattachement de l'utilisateur ou le réseau de prise en charge (qui peut être le réseau de rattachement). Pour le scénario généralisé d'environnement VHE, les services sont supposés être fournis par un réseau de prise en charge.

Le présent sous-paragraphe ci-dessus, décrit un flux d'informations de haut niveau, de bout en bout, simplifié pour la procédure de "commande directe de rattachement" (DHC, *direct home command*). L'invocation de la capacité de déclenchement de service basé dans un environnement VHE peut avoir lieu pour deux classes de services:

- **l'invocation de services liés à un appel** a lieu lors du traitement de l'appel (par exemple, la création de l'appel, la fin de l'appel ou l'appel en cours). Au niveau de l'entité fonctionnelle, ce scénario fait appel à la logique de service dans l'entité SCF du réseau de prise en charge grâce à la capacité de déclenchement de l'entité CCF'/SSF dans le réseau visité;

[3] Cette information est incluse dans les informations de profil de l'abonné pendant l'enregistrement du terminal mobile. Ceci évite de devoir obtenir cette information en tant que partie de l'origine de l'appel.

- **l'invocation de services non liés à un appel** a lieu pour les événements de gestion[4] de la mobilité ou pour les événements d'authentification. Au niveau de l'entité fonctionnelle, ce scénario fait appel à une logique de service dans l'entité SCF du réseau de prise en charge grâce à une requête de l'entité LMF ou une requête de l'entité AMF.

9.1.2 Services reliés à un appel – "Commande directe de rattachement"

Cette partie développe l'idée du composant "invocation de services VHE" pour l'interface NNI, et traite des spécifications de signalisation dans le scénario de DHC pour les services invoqués par une entité SSF/CCF' dans le réseau visité. L'entité SSF/CCF' est supposée avoir la capacité de déclencher la logique de service de l'entité SCF requise, résidant dans le réseau de prise en charge.

Le sous-paragraphe 7.2.2.5/Q.1711 décrit un mode fonctionnel IMT-2000 pour les interconnexions sur une interface NNI entre le réseau de rattachement, le réseau de prise en charge et le réseau visité. Ces interconnexions sont requises pour l'invocation de logique de service dans un réseau de prise en charge.

La Figure 9.1.2-1 représente un scénario de DHC du diagramme de flux d'informations VHE. La figure est simplifiée étant donné qu'elle n'illustre pas l'étendue totale de l'interaction de logique de service prise en charge par un réseau intelligent (comme il a été mentionné dans le 9.1.1 ci-dessus). La procédure "d'invocation de service VHE" peut s'achever après la première "aide en ressources spécialisées" ou peut se poursuivre jusqu'à ce que le service lié à un appel soit complet.

Le présent sous-paragraphe décrit le processus de déclenchement en rapport avec une création d'appel. Les déclenchements peuvent avoir lieu à la fin de l'appel ou pendant l'appel.

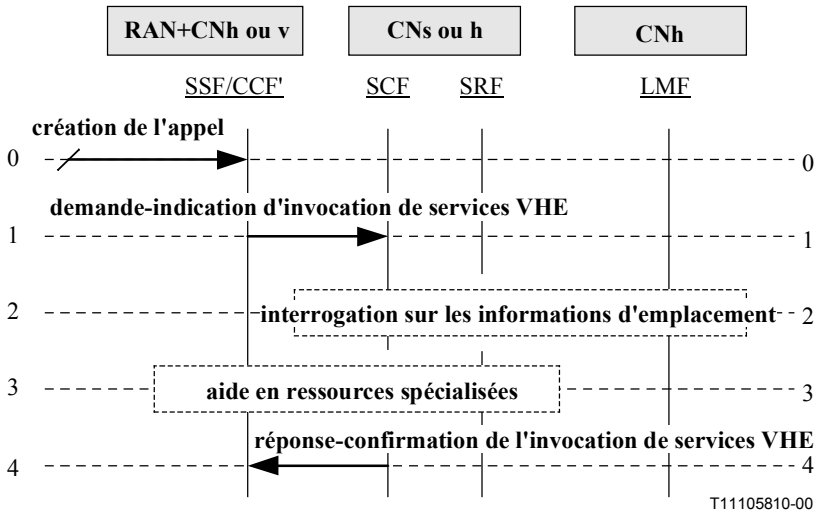


Figure 9.1.2-1/Q.1721 – "Commande directe de rattachement" détaillée, liée à un appel

0. **Création de l'appel**: le participant demandeur crée un appel dans le réseau visité. Les informations obtenues incluent les déclencheurs et critères associés ainsi que d'autres paramètres pour la prise en charge des services basés dans l'environnement VHE par le réseau visité.

FEA0	– Un déclencheur armé dans le modèle BCSM de l'entité SSF/CCF' est rencontré et ses critères sont satisfaits.

[4] La procédure de gestion de la mobilité peut se produire en conjonction avec un appel ou séparée de tout événement d'appel.

1. **Demande-indication d'invocation de services VHE**: s'utilise pour invoquer une logique de service basée dans un VHE de l'entité SCF de prise en charge.

Invocation de services VHE (réponse: succès ou échec)	demande-indication
Eléments d'information dans l'IF de logique de service	Par [5]
IMUI	M
Capacité du MS	O (Note 1)
Informations sur l'emplacement du MS	O (Note 2)

FEA1	– Identification de l'utilisateur. – Récupération des données de service de l'utilisateur à partir du profil de service VHE de l'abonné (par exemple, entité SDF). – Si nécessaire, formulation et envoi d'une demande auprès de l'entité LMF, d'informations sur l'emplacement et l'état du MS dans le réseau de rattachement.
NOTE 1 – La capacité du MS est incluse en fonction des critères du déclencheur. NOTE 2 – Les informations sur l'emplacement du MS sont incluses suivant leur disponibilité.	

2. **Interrogation sur les informations d'emplacement**: s'utilise pour demander des informations sur l'emplacement de l'utilisateur demandé, si elles sont requises par la logique de service et si elles n'ont pas été incluses dans le premier flux d'informations.

3. **Aide en ressources spécialisées**: si nécessaire, est lancée par la logique de service au niveau de l'entité SCF pour obtenir l'accès aux ressources spécialisées de SRF' (par exemple annonce enregistrée ou collecte de chiffres) en relation avec le SSF/CCF'. Cette procédure utilise les procédures de INAP définies dans la Recommandation Q.1238.

4. **Réponse-confirmation de l'invocation de services VHE**: transfère les instructions de service basé dans un VHE vers l'entité initiatrice d'invocation de service basé dans un VHE.

Invocation de services VHE	réponse-confirmation
Eléments d'information dans un IF de logique de service	Par [5]

FEA4	– Si possible, poursuit le traitement de l'appel selon les instructions reçues par l'entité SCF.

9.1.3 "Commande directe de rattachement" – Services invoqués par l'entité LMF

Le sous-paragraphe 7.2.2.5/Q.1711 décrit un modèle fonctionnel IMT-2000 pour les interconnexions sur une interface NNI entre un réseau de rattachement ou un réseau visité, et un réseau de prise en charge. Ces interconnexions sont requises pour le processus d'invocation de logique de service dans le réseau de prise en charge, déclenchées à partir de l'entité LMF.

La Figure 9.1.3-1 représente le diagramme du flux d'informations du scénario VHE DHC invoqué par l'entité LMF.

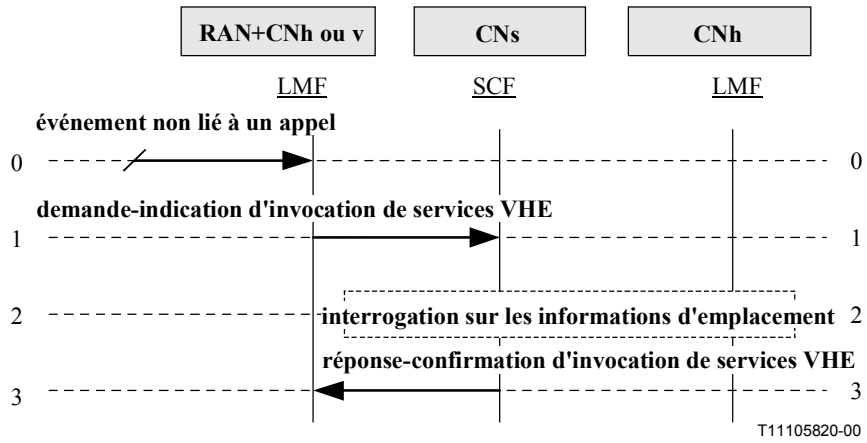


Figure 9.1.3-1/Q.1721 – "Commande directe de rattachement" de l'entité LMF

0. **Evénement non lié à un appel**: le processus de gestion de la mobilité utilise des informations obtenues en provenance du réseau de rattachement lors de la souscription. Ces informations incluent les déclencheurs et critères correspondants ainsi que d'autres paramètres pour la prise en charge, par le réseau visité, des services basés en VHE invoqués par l'entité LMF.

FEA0	– Un déclencheur armé est rencontré au point TDP dans le modèle d'état de l'entité LMF, et les critères du déclencheur armé sont satisfaits.

1. **Demande-indication d'invocation de services VHE**: s'utilise pour invoquer une logique de service basé en VHE auprès de l'entité de prise en charge SCF.

Invocation de services VHE (réponse: succès ou échec)	demande-indication
Identificateur de service	M
Type d'événement	M
IMUI	M
Capacité du MS	O (Note 1)
Informations sur l'emplacement du MS	O (Note 2)

FEA1	– Identification de l'utilisateur. – Récupération des données de service de l'utilisateur à partir du profil de service VHE de l'abonné (par exemple, entité SDF). – Si nécessaire, formulation et envoi d'une demande auprès de l'entité LMF, d'informations sur l'emplacement et l'état du MS dans le réseau de rattachement.
NOTE 1 – La capacité du MS est incluse en fonction des critères du déclencheur. NOTE 2 – Les informations sur l'emplacement du MS sont incluses suivant leur disponibilité.	

2. **Interrogation sur les informations d'emplacement**: s'utilise pour demander des informations sur l'emplacement de l'utilisateur demandé, si elles sont requises par la logique de service et si elles n'ont pas été incluses dans le premier flux d'informations.

3. **Réponse-confirmation d'invocation de services VHE**: transfère les instructions de service basé en VHE vers l'entité initiatrice d'invocation de services basé en VHE.

Invocation de services VHE	réponse-confirmation
Instructions de services VHE	M

FEA2	– Poursuit, si possible, le traitement de l'appel selon les instructions reçues par l'entité SCF.

9.1.4 "Commande directe de rattachement" – Services invoqués par l'entité AMF

Le sous-paragraphe 7.2.2.5/Q.1711 décrit un modèle fonctionnel IMT-2000 pour les interconnexions sur une interface NNI entre un réseau de rattachement ou un réseau visité et un réseau de prise en charge. Ces interconnexions sont requises pour le processus d'invocation de logique de service dans le réseau de prise en charge, déclenchée à partir de l'entité AMF.

La Figure 9.1.4-1 représente le diagramme du flux d'informations du scénario VHE DHC invoqué par l'entité AMF.

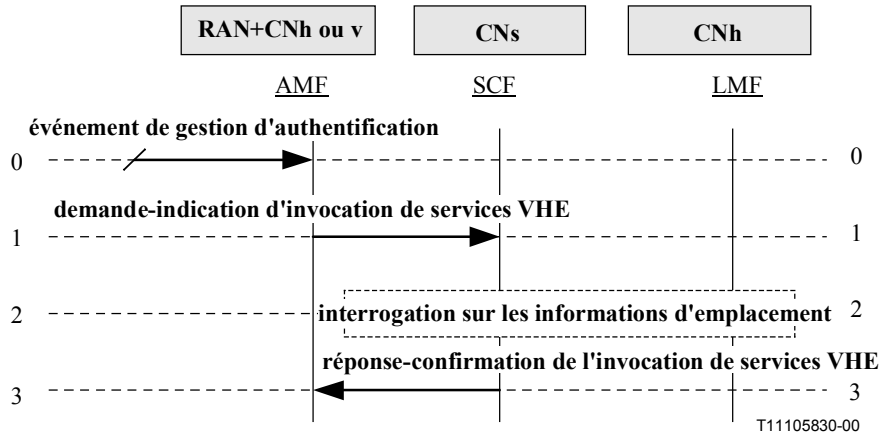


Figure 9.1.4-1/Q.1721 – "Commande directe de rattachement" de l'entité AMF

0. **Evénement de gestion d'authentification**: lance le processus de gestion d'authentification. Les informations disponibles incluent les déclencheurs et critères correspondants ainsi que d'autres paramètres pour la prise en charge de services basés en VHE invoqués par l'entité AMF.

FEA0	– Un déclencheur armé est rencontré au point TDP dans le modèle d'état de l'entité AMF, et les critères du déclencheur armé sont satisfaits.

1. **Demande-indication d'invocation de services VHE**: s'utilise pour invoquer une logique de service basé en VHE auprès de l'entité de prise en charge SCF .

Invocation de services VHE (réponse: succès ou échec)	demande-indication
IMUI	M
Identificateur de service	M
Modèle BMSM de type d'événement	M
Informations sur l'emplacement du MS	O (Note)

FEA1	– Identification de l'utilisateur. – Récupération des données de service de l'utilisateur à partir du profil de service VHE de l'abonné (par exemple, entité SDF). – Si nécessaire, formulation et envoi d'une demande auprès de l'entité LMF, d'informations sur l'emplacement et l'état du MS dans le réseau de rattachement.
NOTE – Les informations sur l'emplacement du MS sont incluses suivant leur disponibilité.	

2. **Interrogation sur les informations d'emplacement**: s'utilise pour demander des informations sur l'emplacement de l'utilisateur demandé, si elles sont requises par la logique de service et si elles n'ont pas été incluses dans le premier flux d'informations.

3. **Réponse-confirmation de l'invocation de services VHE**: est utilisée pour envoyer des services d'instructions VHE en provenance de l'entité SFC dans le réseau de prise en charge vers l'entité demandeuse AMF.

Invocation de services VHE	**réponse-confirmation**
Instructions de services VHE	M

FEA2	– Poursuit la procédure d'authentification selon l'instruction reçue par l'entité SCF.

9.2 "Commande de service relais"

Le scénario de "commande de service relais" (RSC, *relay service control*) VHE est une invocation de logique de service résidant dans l'entité SCF d'un réseau de prise en charge (ou réseau de rattachement) par l'entité SCF d'un réseau serveur (soit réseau de rattachement ou un réseau visité).

Dans VHE-RSC, la logique de service est répartie entre le réseau de prise en charge et le réseau visité afin de prendre en charge les services basés en VHE de l'abonné itinérant.

Lorsque le réseau serveur est le même que le réseau de prise en charge, VHE RSC est une invocation de service basé sur un réseau intelligent pour laquelle il existe des procédures bien définies. Lorsque le réseau serveur n'est pas un réseau de prise en charge, le VHE RSC peut alors s'appliquer. Pour VHE RSC, les réseaux serveurs et le réseau de prise en charge sont supposés être deux réseaux différents en interfonctionnement dans un protocole d'interface NNI.

Dans le réseau serveur, les événements pertinents peuvent faire l'objet d'un compte rendu effectué par les entités CCF'/SSF, LMF ou AMF vers l'entité SCF. Les déclencheurs dans les entités fonctionnelles invocatrices peuvent être armés par le biais des informations du profil de l'abonné ou par un processus de fourniture de service simultané. L'entité SCFv invoquée (du réseau serveur) fera une requête auprès de l'entité SCF (du réseau de prise en charge) pour la prise en charge de commande de service[5].

La logique de service pour des services basés en VHE utilisant le RSC est fournie par le réseau de rattachement de l'utilisateur ou par le réseau de prise en charge. Dans le scénario d'environnement VHE généralisé, les services sont supposés être fournis par le réseau de prise en charge.

[5] Les Figures 7-7/Q.1711 et 7-8/Q.1711 représentent les interconnexions sur l'interface NNI qui peuvent être utilisées pour le compte rendu de cet événement.

Des accords préalables devraient être réalisés pour la coopération et coordination entre les réseaux serveurs et le réseau de prise en charge pour le VHE RSC. L'étendue de cette coopération peut aller d'un programme de commande de service relais partiel jusqu'à un programme de commande de service relais complet[6].

De la même manière que dans le cas de la "commande directe de rattachement" VHE, les services pour le scénario de RSC peuvent être liés ou non liés à l'appel.

9.2.1 Procédure de service de "commande de service relais"

Cette procédure fait appel à l'invocation de logique de service par le biais d'entité SCFv vers SCFs pour la prise en charge de la commande du service. Un accord préalable entre les réseaux de prise en charge et le réseau visité peut porter sur les capacités de sécurité/filtrage par relais, les sous-routines de programme d'exécution de logique de service ou des programmes entièrement exécutables.

Le sous-paragraphe 7.2.2.5/Q.1711 décrit un modèle fonctionnel IMT-2000 pour les interconnexions sur une interface NNI entre un réseau de rattachement ou un réseau de prise en charge, et un réseau visité. Ces interconnexions sont requises pour l'invocation de la logique ou de la commande de service dans le réseau support.

Dans le cadre d'un schéma de flux d'informations de bout en bout, cette procédure se divise en quatre étapes: stimulus initial, invocation de services VHE, informations de traitement VHE, et achèvement de la procédure initiale. Le présent sous-paragraphe traite des flux d'informations en ce qui concerne l'invocation de logique de services et les parties de l'information de traitement VHE, et considère les flux d'informations pour les trois autres parties, comme étant des procédures ordinaires dans le contexte de flux d'informations de bout en bout.

La Figure 9.2.1-1 représente le diagramme du flux d'informations pour le scénario de "commande de service relais" VHE. Une fois que le rapprochement des critères a été effectué, l'entité SSF/CCF', LMF ou AMF, est supposée avoir la capacité d'envoyer un message vers l'entité SCF requise au sein du réseau serveur. De même, l'entité SCF serveuse est supposée avoir la capacité de demander de l'assistance auprès d'une SCF de prise en charge. Les remarques suivantes concernant la figure ci-dessous, devraient être prises en compte:

- le cas d'une notification vers une logique de service est un sous-ensemble de la Figure 9.2.1-1 (c'est-à-dire que les flux 2 et 3 ne seraient pas requis);
- la figure est simplifiée étant donné qu'elle n'illustre pas l'étendue totale de l'interaction de logique de service pris en charge par un réseau intelligent. Par exemple, elle ne reflète pas l'interaction étendue avec la logique de service (qui pourra se poursuivre jusqu'à libération de l'appel), ni l'interaction de l'utilisateur, prise en charge par une logique de service, etc.

---

[6] La capacité de sécurité/de filtrage par relais pour les procédure de contrôle de fraude/abus peut également être exécutée par un Programme de Logique de Service (SLP) au niveau d'une SCF.

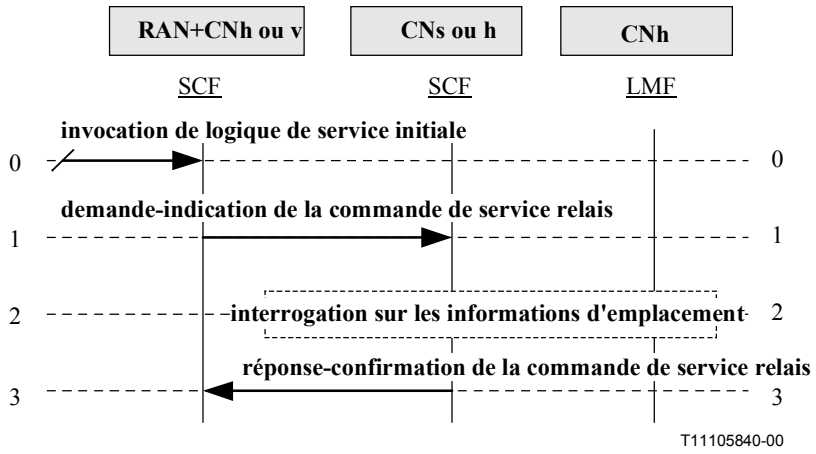


Figure 9.2.1-1/Q.1721 – "Commande de service relais" de haut niveau

0. **Invocation de logique de service initiale**: invoque une logique de service auprès de l'entité SCF associée au déclencheur dont les critères ont été satisfaits. Cette invocation achemine des informations sur l'abonné, sur l'état du traitement de l'appel (invoqué par l'entité SSF/CCF') ou sur l'état de la gestion de la mobilité (invoqué par l'entité LMF) ou sur l'état de gestion d'authentification (invoqué par l'entité AMF) et enfin sur les conditions de déclenchement rencontrées.

FEA0	– Identification du réseau de prise en charge de l'utilisateur. – Vérification de l'accord bilatéral pour le processus de RSC. – Invocation des entités SCFs (ou du réseau de prise en charge) pour le programme de logique de service (SLP, *service logic program*) de l'utilisateur.

1. **Demande-indication de la commande de service relais**: est utilisée par l'entité SCF de commande pour envoyer une demande auprès de l'entité SCF de prise en charge, ou pour demander à l'entité SCF de prise en charge, d'effectuer les actions prédéfinies.

Commande de service relais (réponse: succès ou échec)	**demande-indication**
Identificateur de service	M
Modèle BCSM, LMSM ou AMSM de type d'événement (dans l'entité LMFv ou LMFh)	M
IMUI	M
Capacité du MS	O (Note 1)
Informations sur l'emplacement du MS	O (Note 2)

FEA1	– Identification de l'utilisateur et de son ID de services. – Identification du programme SLP requis. – Si nécessaire, formulation et envoi d'une demande d'informations sur l'emplacement et l'état du MS auprès de l'entité LMF dans le réseau de rattachement. – Vérification des restrictions (à l'aide de IMUI, emplacement de MS, etc.)
NOTE 1 – La capacité de MS est inclue en fonction des critères du déclencheur. NOTE 2 – Les informations d'emplacement du terminal mobile sont envoyées suivant disponibilité.	

2. **Interrogation sur les informations d'emplacement**: s'utilise pour demander des informations sur l'emplacement de l'utilisateur demandé, si elles sont requises par la logique de service et si elles n'ont pas été incluses dans le premier flux d'informations.

3. **Réponse-confirmation de la commande de service relais**: est utilisée pour retransmettre les informations requises, au SCF de commande pour permettre d'établir l'appel.

Commande de service relais	demande-indication
Logique de service effectuée par relais	M

FEA2	– Exécute la logique de service relais.

10 Applications de services de messagerie

Le service de messages courts (SMS, *short message service*) point à point est une méthode d'envoi de messages texte vers et à partir de terminaux mobiles IMT-2000. La fourniture de SMS utilise un centre de messagerie (MC, *message centre*), qui fait office de centre de stockage et de retransmission de messages courts.

Deux services point à point ont été définis: celui en provenance de terminaux mobiles et celui à destination de terminaux mobiles. Les messages en provenance de terminaux mobiles seront transportés à partir d'un terminal mobile vers un centre de messagerie. Ces messages seront destinés à d'autres utilisateurs de mobiles, ou à des abonnés dans un réseau fixe. Les messages à destination de terminaux mobiles seront transportés à partir d'un centre de messagerie vers un terminal mobile. Ces messages pourront être entrés dans le centre de messagerie par d'autres utilisateurs de mobiles (par le biais de messages courts en provenance de terminaux mobiles) ou par d'autres sources variées, par exemple la parole, le télex ou le fac-similé.

La diffusion de message de téléservice point à multipoint (TMB, *teleservice message broadcast*) est une méthode de gestion et de livraison des messages de téléservice pour diffusion sur une interface radio vers des terminaux mobiles IMT-2000. Les messages de TMB sont diffusés vers des zones géographiques connues sous le nom de zones de diffusion à cellule. Ces zones peuvent être constituées d'une ou plusieurs cellules, ou de tout un réseau pour certains fournisseurs de services. Des zones spécifiques de couverture géographique seront attribuées aux messages de TMB, sur accord mutuel entre le fournisseur d'informations et l'exploitant réseau.

10.1 Le service de messages courts (SMS)

10.1.1 Transfert de notification de SMS

La procédure de notification de SMS est utilisée pour alerter le centre de messagerie. La procédure démarre lorsque le terminal mobile est actif (à la suite de l'échec d'un transfert de message car le terminal mobile était inaccessible) ou lorsque le terminal mobile indique qu'il a désormais une capacité de mémoire suffisante pour accepter un message court.

10.1.1.1 Le terminal mobile est actif

Voir Figure 10.1.1.1-1.

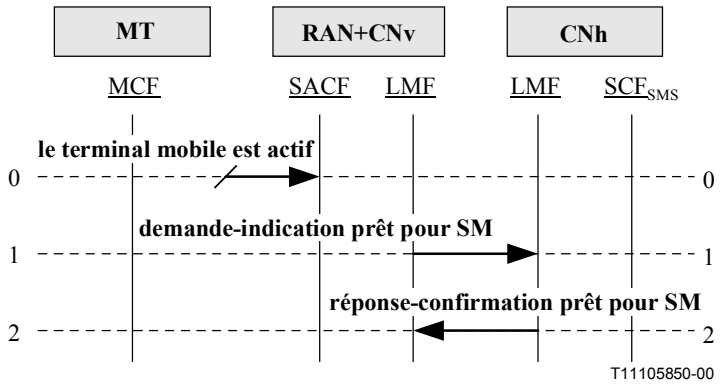


Figure 10.1.1.1-1/Q.1721– Transfert de notification de SMS (terminal mobile est actif)

0. **Le terminal mobile est actif**: lorsque le terminal mobile est actif, par exemple lorsque le terminal mobile a effectué une demande de service, a eu une création d'appel ou une réponse à la radiorecherche. De façon optionnelle, l'authentification de l'utilisateur peut avoir eu lieu.

FEA0	– Lorsque le terminal mobile est présent, LMFv modifiera la base de données appropriée et en informera l'entité LMFh.

1. **Demande-indication pour SM**: informe l'entité LMFh que le terminal mobile est prêt à accepter des messages courts.

Prêt pour SM (réponse: succès)	**demande-indication**
IMUI	M
Raison de l'alerte	M

FEA1	– Informe le réseau visité que la demande prêt pour SM a été reçue.

2. **Réponse-confirmation pour SM**: accuse réception de la demande de message court.

Prêt pour SM	**réponse-confirmation**
Erreur de l'utilisateur	O (Note)
Erreur du fournisseur	O (Note)

FEA2	– Achève le transfert de notification du SMS.
NOTE – Nécessaire seulement si une situation d'erreur a eu lieu.	

10.1.1.2 Capacité de mémoire disponible

Voir Figure 10.1.1.2-1.

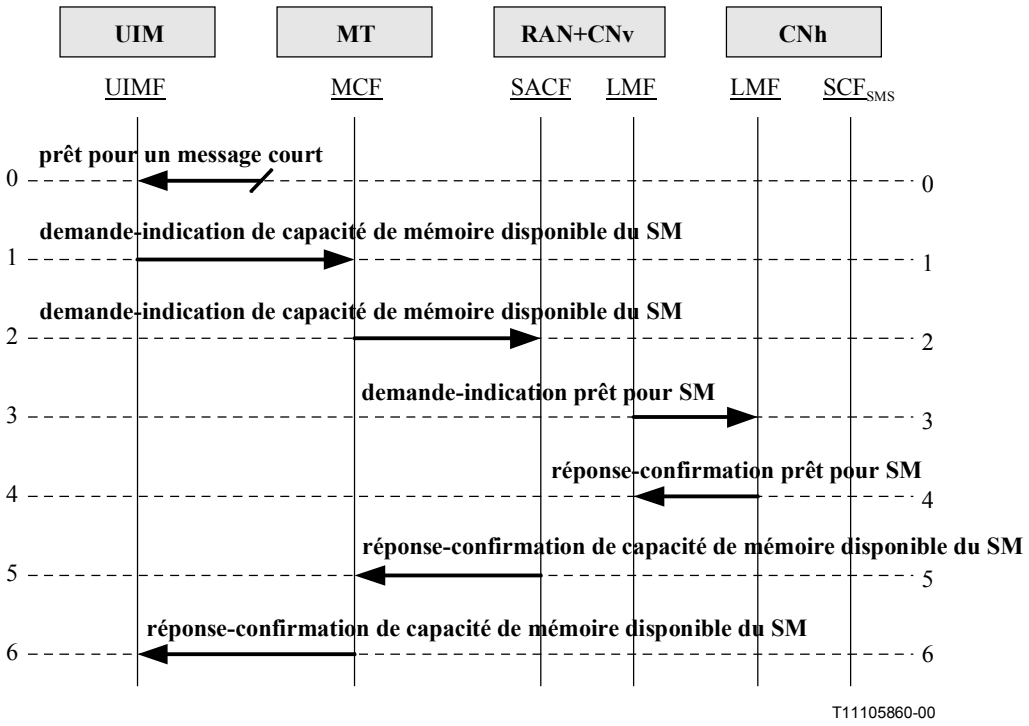


Figure 10.1.1.2-1/Q.1721 – Transfert de notification du SMS (capacité de mémoire disponible)

0. **Prêt pour un message court**: est le stimulus initial par lequel le terminal mobile a effectué une demande de service. De façon optionnelle, l'authentification de l'utilisateur aura pu avoir lieu.

FEA0	– Lorsque l'entité UIMF a la possibilité de traiter les messages courts, et a rendu la capacité de mémoire disponible, elle informe l'entité MCF.

1. **Demande-indication de capacité de mémoire disponible du SM**: informe l'entité MCF dans le terminal mobile qu'il a une mémoire disponible pour recevoir des messages courts.

Capacité de mémoire disponible du SM (réponse: succès)	demande-indication
TMUI ou IMUI	M (Note)

FEA1	– Effectue le relais de la demande vers le réseau serveur.
NOTE – TMUI devrait être utilisé suivant sa disponibilité.	

2. **Demande-indication de capacité de mémoire disponible du SM**: informe le réseau visité que le terminal mobile est prêt à accepter des messages courts.

Capacité de mémoire disponible du SM (réponse: succès)	demande-indication
TMUI ou IMUI	M (Note)

FEA2	– S'apprête à informer le réseau de rattachement que l'abonné demandeur est prêt à accepter des messages courts.
NOTE – TMUI devrait être utilisé suivant sa disponibilité.	

3. **Demande-indication prêt pour SM**: informe l'entité LMFh que le terminal mobile est prêt à accepter des messages courts.

Prêt pour SM (réponse: succès)	demande-indication
IMUI	M
Raison de l'alerte	M

FEA3	– Informe le réseau visité que la demande prêt pour SM a été reçue.

4. **Réponse-confirmation prêt pour SM**: accuse réception de la demande de message court.

Prêt pour SM	réponse-confirmation
Erreur de l'utilisateur	O (Note)
Erreur du fournisseur	O (Note)

FEA4	– Effectue le relais de l'accusé de réception vers l'entité MCF.
NOTE – Nécessaire seulement si une situation d'erreur a eu lieu.	

5. **Réponse-confirmation de capacité de mémoire disponible du SM**: envoie une confirmation du réseau visité au terminal mobile.

Capacité de mémoire disponible du SM	réponse-confirmation
Aucune	(Note)

FEA5	– Effectue le relais de l'accusé vers l'entité UIMF.
NOTE – La réponse-confirmation est vide. Sa seule présence suffit à indiquer un succès.	

6. **Réponse-confirmation de capacité de mémoire disponible du SM**: envoie une confirmation à l'entité UIMF.

Capacité de mémoire disponible du SM	réponse-confirmation
Aucune	(Note)

FEA6	– Aucune action requise.
NOTE – La réponse-confirmation est vide. Sa seule présence suffit à indiquer un succès.	

10.1.2 Message court en provenance de terminaux mobiles

Le terminal mobile envoie un message court à l'entité CCF'/SACF dans le réseau visité. L'entité CCF'/SACF interroge l'entité LMFv pour récupérer l'adresse de MS RNIS et retransmettre le message vers le nœud CCF'/SSF en interfonctionnement, dans le réseau de destination. Les nœuds CCF'/SSF envoient le message court vers le centre de messagerie. Un numéro E.164 dans le plan de

numérotage du réseau de destination auquel le centre de messagerie est connecté, adresse le centre de messagerie à partir du mobile. Le numéro E.164 est stocké dans le module UIM.

10.1.2.1 Message court en provenance de terminaux mobiles (sur un canal de trafic)

Cette procédure est invoquée lorsqu'un utilisateur de IMT-2000 envoie un message court de point à point alors qu'un appel est déjà en cours. Voir Figure 10.1.2.1-1.

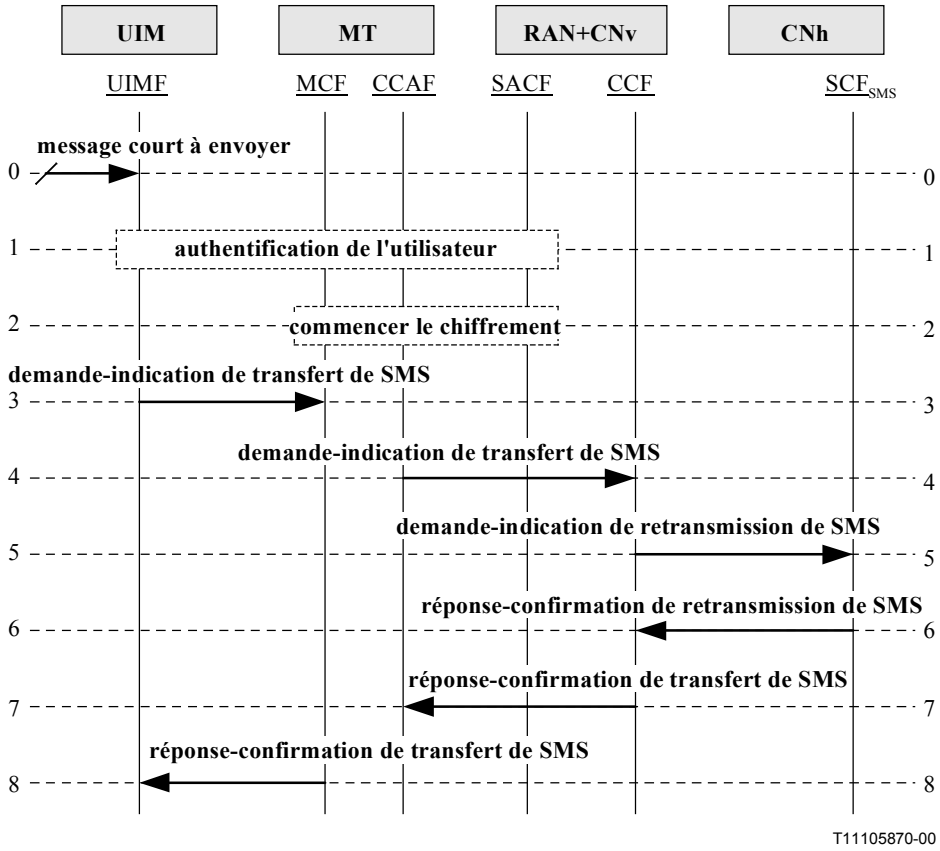


Figure 10.1.2.1-1/Q.1721 – Message court en provenance de terminaux mobiles (sur un canal de trafic)

0. Message court à envoyer: il s'agit du stimulus initial par lequel l'abonné soumet un message court à un terminal mobile pour l'envoyer à un receveur/destinataire.

FEA0	– Le terminal mobile effectue une demande de message court.

1. **Authentification de l'utilisateur**: de façon optionnelle, la procédure d'authentification de l'utilisateur peut être invoquée.

2. **Commencer le chiffrement**: de façon optionnelle**,** la procédure de chiffrement peut être lancée.

3. **Demande-indication de transfert de SMS**: transfère le message court vers l'entité MCF.

Transfert de SMS (réponse: succès)	demande-indication
TMUI ou IMUI	M (Note)
Numéro demandé	M
Adresse de centre de messagerie	M
Message	M

FEA3	– Retransmission des informations vers l'entité CCAF.
NOTE – L'identité TMUI peut être utilisée si elle est disponible.	

4. **Demande-indication de transfert de SMS**: est utilisée pour envoyer un message vers l'entité CNv.

Transfert du SMS (réponse: succès)	demande-indication
<Eléments d'information identiques à ceux trouvés dans le flux d'informations 3>	<Voir IF 3>

FEA4	– Retransmission des informations vers un centre de messagerie dans l'entité CNh.

5. **Demande-indication de retransmission de SMS**: transfère le message vers un centre de messages courts dans l'entité CNh.

Retransmission de SMS (réponse: succès)	demande-indication
<Eléments d'information identiques à ceux trouvés dans le flux d'informations 3>	<Voir IF 3>

FEA5	– Etablit un compte rendu de livraison à renvoyer à l'entité CNv.

6. **Réponse-confirmation de retransmission de SMS**: accusé de réception reçu vers le message.

Retransmission de SMS	réponse-confirmation
Aucune	(Note)

FEA6	– Retransmission du compte rendu de livraison vers l'entité CCAF.
NOTE – La réponse-confirmation est vide. Sa seule présence suffit à indiquer un succès.	

7. **Réponse-confirmation de transfert de SMS**: accusé de réception reçu vers le message.

Transfert du SMS	réponse-confirmation
Aucun	(Note)

FEA7	– Retransmission du compte rendu de livraison vers l'entité MCF.
NOTE – La réponse-confirmation est vide. Sa seule présence suffit à indiquer un succès.	

8. **Réponse-confirmation de transfert de SMS**: accusé de réception reçu vers le message.

Transfert du SMS	réponse-confirmation
Aucun	(Note)

FEA8	– Informe l'abonné du succès ou de l'échec de la livraison du message.
NOTE – La réponse-confirmation est vide. Sa seule présence suffit à indiquer un succès.	

10.1.2.2 Message court en provenance de terminaux mobiles (sur un canal de commande)

Voir Figure 10.1.2.2-1.

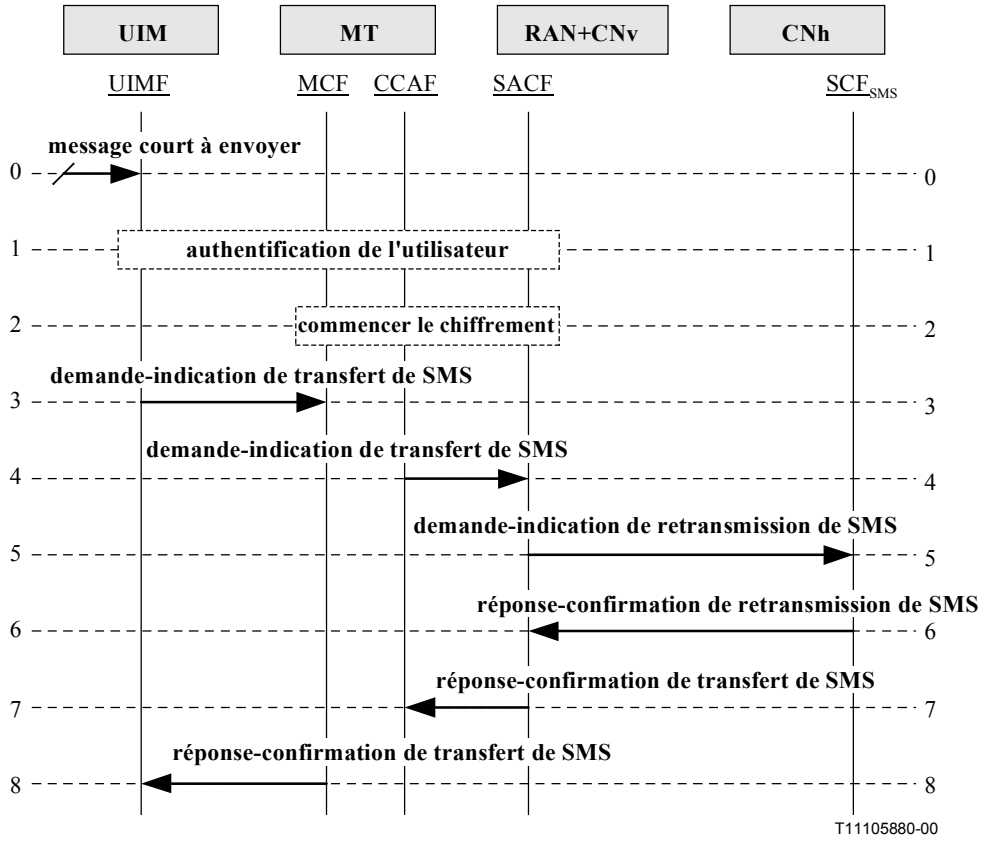


Figure 10.1.2.2-1/Q.1721 – Message court en provenance de terminaux mobiles (sur un canal de commande)

0. **Message court à envoyer**: il s'agit du stimulus initial par lequel l'abonné soumet un message court à un terminal mobile pour l'envoyer à un receveur/destinataire.

FEA0	– Le terminal mobile effectue une demande de message court.

1. **Authentification de l'utilisateur**: de façon optionnelle, la procédure d'authentification de l'utilisateur peut être invoquée.

2. **Commencer le chiffrement**: de façon optionnelle**,** la procédure de chiffrement peut être lancée.

3. **Demande-indication de transfert de SMS**: transfère le message court vers l'entité MCF.

Transfert de SMS (réponse: succès)	demande-indication
TMUI ou IMUI	M (Note)
Numéro demandé	M
Adresse du centre de messagerie	M
Message	M

FEA3	– Retransmission des informations vers un centre de messagerie dans l'entité CCAF.
NOTE – L'identité TMUI peut être utilisée si elle est disponible.	

4. **Demande-indication de transfert de SMS**: est utilisée pour envoyer un message vers l'entité CNv.

Transfert de SMS (réponse: succès)	demande-indication
<Eléments d'information identiques à ceux trouvés dans le flux d'informations 3>	<Voir IF 3>

FEA4	– Retransmission des informations vers un centre de messagerie dans l'entité CNh.

5. **Demande-indication de retransmission de SMS**: transfère le message ver l'entité SCF dans CNh.

Retransmet le SMS (réponse: succès)	demande-indication
<Eléments d'information identiques à ceux trouvés dans le flux d'informations 3>	<Voir IF 3>

FEA5	– Etablit un compte rendu de livraison à renvoyer à l'entité CNv.

6. **Réponse-confirmation de retransmission de SMS**: accuse réception du message.

Retransmet le SMS	réponse-confirmation
Aucun	(Note)

FEA6	– Retransmet le compte rendu de livraison à l'entité CCAF.
NOTE – La réponse-confirmation est vide. Sa seule présence suffit à indiquer un succès.	

7. **Réponse-confirmation de transfert de SMS**: accusé de réception reçu vers le message.

Transfert de SMS	réponse-confirmation
Aucun	(Note)

FEA7	– Retransmet le compte rendu de livraison à l'entité MCF.
NOTE – La réponse-confirmation est vide. Sa seule présence suffit à indiquer un succès.	

8. **Réponse-confirmation de transfert de SMS**: accusé de réception reçu vers le message.

Transfert de SMS	réponse-confirmation
Aucun	(Note)

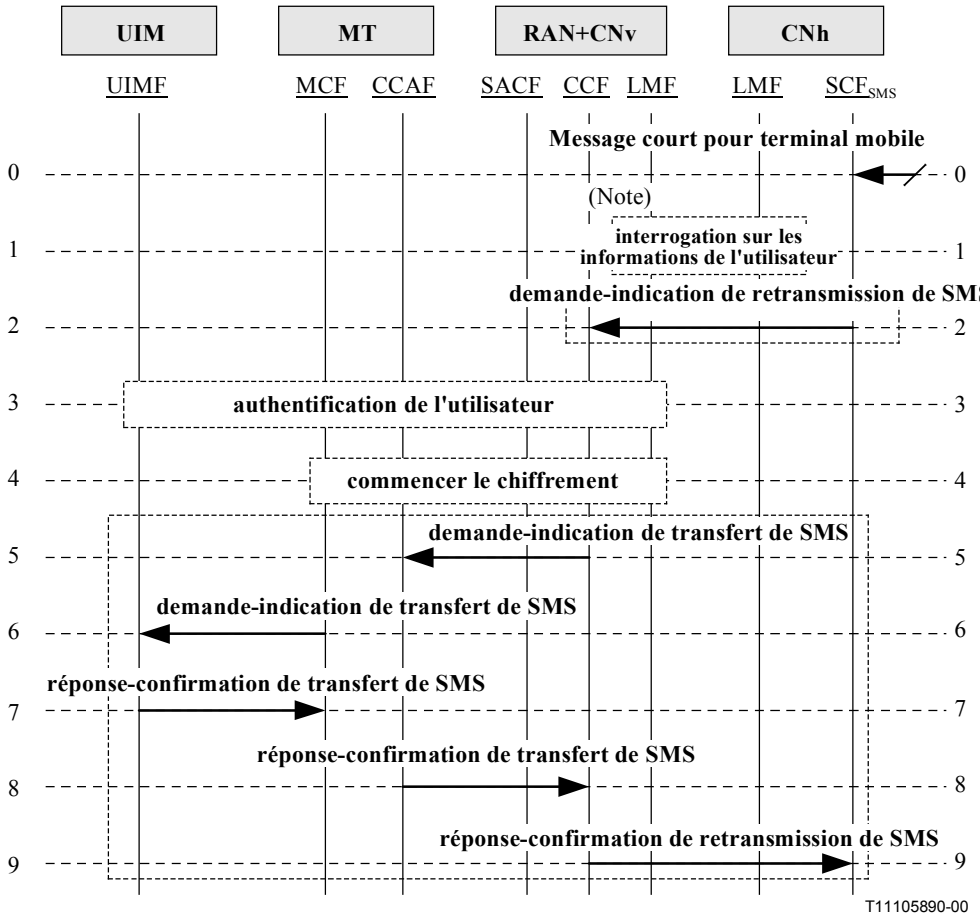
FEA8	– Informe l'abonné du succès ou de l'échec de la livraison du message.
NOTE – La réponse-confirmation est vide. Sa seule présence suffit à indiquer un succès.	

10.1.3 Message court à destination de terminaux mobiles

Le centre de messagerie envoie un message court à l'entité CCF'/SACF dans le réseau de rattachement de l'abonné. L'entité CCF'/SACF interroge le LMFh afin de récupérer les informations de routage nécessaires pour la retransmission du message court. Par la suite, elle envoie le message vers les entités CCF'/SACF appropriées, dans le réseau visité, en transit dans d'autres réseaux le cas échéant. L'entité CCF'/SACF envoie ensuite un message court au terminal mobile.

10.1.3.1 Message court à destination de terminaux mobiles sur un canal de trafic

Voir Figure 10.1.3.1-1.



NOTE – Le SCF_{SMS} peut facultativement demander à l'entité LMFh des informations d'emplacement si le mobile est déclaré comme pouvant être joint et possède une capacité de mémoire disponible. "L'interrogation des informations de l'utilisateur" étant facultative, les flux d'information postérieurs sont facultatifs.

Figure 10.1.3.1-1/Q.1721 – Message court à destination de terminaux mobiles (sur un canal de trafic)

0. **Message court pour terminal mobile**: un message court est soumis au centre de messagerie du réseau de rattachement de l'abonné, pour livraison à l'abonné du terminal mobile.

FEA0	– Initie la procédure d'interrogation des informations de l'utilisateur pour obtenir les données requises pour la livraison du message.

1. **Interrogation sur les informations de l'utilisateur**: l'entité LMFh effectue une requête auprès de l'entité LMFv sur l'état et l'emplacement actuel de l'abonné à qui le message est destiné. L'entité LMFv détermine l'emplacement actuel et l'état du terminal mobile et répond au LMFh.

2. **Demande-indication de retransmission de SMS**: transfère le message court vers l'entité CCF identifiée lors de la 1ère étape.

Retransmet le SMS (réponse: succès)	demande-indication
IMUI	M
Numéro du demandeur	M
Adresse de centre de messagerie	M
Message	M

FEA2	– Transfère le message vers l'entité CCAF dans le terminal mobile.

3. **Authentification de l'utilisateur**: de façon optionnelle, la procédure d'authentification de l'utilisateur peut être invoquée.

4. **Commencer le chiffrement**: de façon optionnelle, la procédure de chiffrement pourra être lancée.

5. **Demande-indication de transfert de SMS**: transfère le message vers le terminal mobile.

Transfert de SMS (réponse: succès)	demande-indication
<Eléments d'information identiques à ceux trouvés dans le flux d'informations 2>	<Voir IF 2>

FEA5	– Retransmission des informations vers l'entité MCF.

6. **Demande-indication de transfert de SMS**: transfère le message vers le module UIM.

Transfert du SMS (réponse: succès)	demande-indication
<Eléments d'information identiques à ceux trouvés dans le flux d'informations 2>	<Voir IF 2>

FEA6	– Affiche le message court ou notifie à l'utilisateur la présence d'un tel message. – Lance le compte rendu de la livraison et le renvoie vers l'entité CNh.

7. **Réponse-confirmation de transfert de SMS**: accuse réception du message.

Transfert du SMS	réponse-confirmation
Aucun	(Note)

FEA7	– Retransmission de l'accusé de réception vers le CCAF.
NOTE – La réponse-confirmation est vide. Sa seule présence suffit à indiquer un succès.	

8. **Réponse-confirmation de transfert de SMS**: accusé de réception reçu vers le message.

Transfert du SMS	réponse-confirmation
Aucun	(Note)

FEA8	– Transfère l'accusé de réception vers l'entité SCF dans CNh.
NOTE – La réponse-confirmation est vide. Sa seule présence suffit à indiquer un succès.	

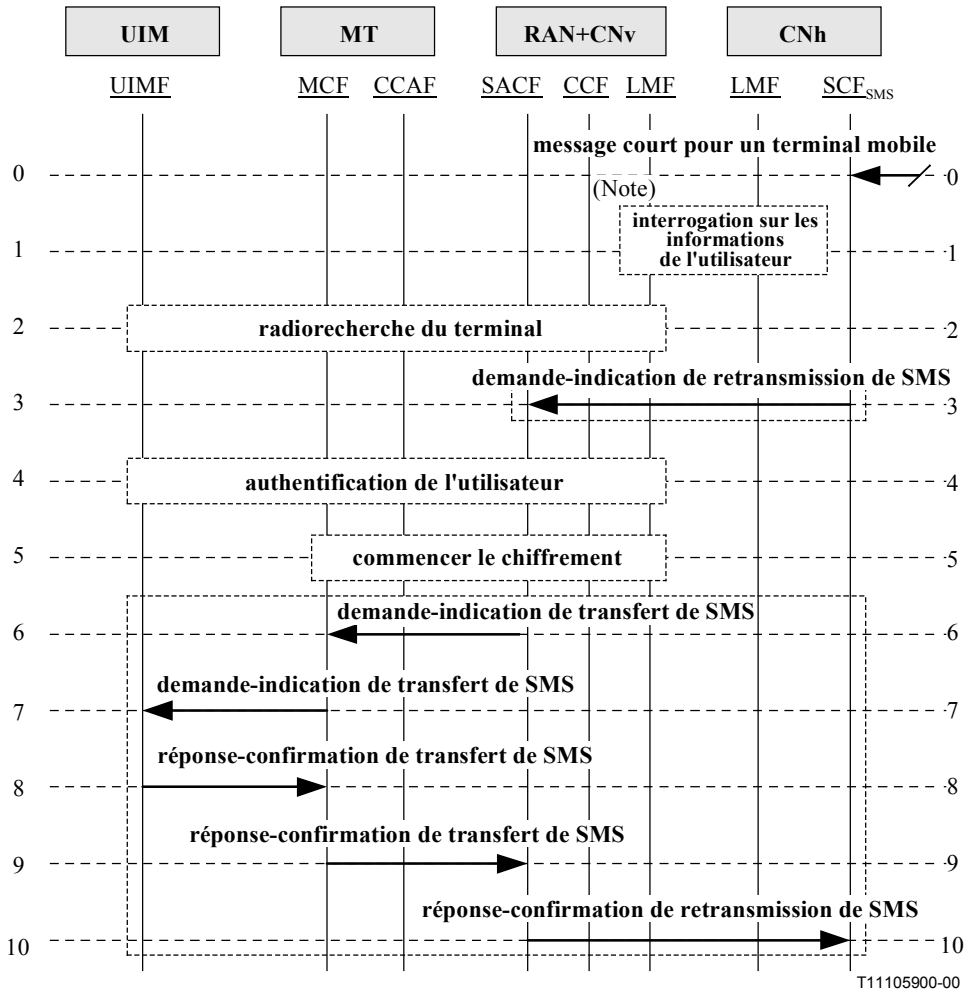
9. **Réponse-confirmation de retransmission de SMS**: accuse réception du message.

Retransmet le SMS	réponse-confirmation
Aucun	(Note)

FEA9	– Marque le message comme étant délivré avec succès.
NOTE – La réponse-confirmation est vide. Sa seule présence suffit à indiquer un succès.	

10.1.3.2 Message court à destination de terminaux mobiles sur un canal de commande

Voir Figure 10.1.3.2-1.



NOTE – Le SCF$_{SMS}$ peut facultativement demander à l'entité LMFh des informations d'emplacement si le mobile est déclaré comme pouvant être joint et possède une capacité de mémoire disponible. "L'interrogation des informations de l'utilisateur" étant facultative, les flux d'informations postérieurs sont facultatifs.

Figure 10.1.3.2-1/Q.1721 – Message court à destination de terminaux mobiles (sur un canal de commande)

0. **Message court pour un terminal mobile**: un message court est soumis au centre de messagerie du réseau de rattachement de l'abonné pour livraison, à l'abonné du terminal mobile.

FEA0	– Initie la procédure d'interrogation des informations sur l'utilisateur afin d'obtenir les données requises pour la livraison du message.

1. **Interrogation sur les informations de l'utilisateur**: l'entité LMFh effectue une requête auprès de l'entité LMFv sur l'état et l'emplacement actuel de l'abonné à qui le message est destiné. L'entité LMFv détermine l'emplacement actuel et l'état du terminal mobile et répond au LMFh.

2. **Radiorecherche du terminal**: de façon optionnelle, la procédure de radiorecherche peut s'effectuer pour déterminer, de façon plus approfondie, l'emplacement du terminal mobile**.**

3. **Demande-indication de retransmission de SMS**: transfère le message court vers l'entité SACF dans le CNv.

Retransmet le SMS (réponse: succès)	demande-indication
IMUI	M
Numéro du demandeur	M
Adresse du centre de messagerie	M
Message	M

FEA3	– Transfère le message vers l'entité MCF dans le terminal mobile.

4. **Authentification de l'utilisateur**: de façon optionnelle, la procédure d'authentification de l'utilisateur peut être invoquée.

5. **Commencer le chiffrement**: de façon optionnelle, la procédure de chiffrement pourra être lancée.

6. **Demande-indication de transfert de SMS**: transfère le message vers le terminal mobile.

Transfert de SMS (réponse: succès)	demande-indication
<Eléments d'information identiques à ceux trouvés dans le flux d'informations 3>	<Voir IF 3>

FEA6	– Transfère le message vers l'entité UIMF.

7. **Demande-indication de transfert de SMS**: transfère le message vers le module UIM.

Transfert de SMS (réponse: succès)	demande-indication
<Eléments d'information identiques à ceux trouvés dans le flux d'informations 3>	<Voir IF 3>

FEA7	– Affiche le message court ou notifie à l'utilisateur la présence d'un tel message. – Lance le compte rendu de la livraison et le renvoie vers l'entité CNh.

8. **Réponse-confirmation de transfert de SMS**: accuse réception du message.

Transfert de SMS	réponse-confirmation
Aucun	(Note)

FEA8	– Retransmet l'accusé de réception vers le SACF.
NOTE – La réponse-confirmation est vide. Sa seule présence suffit à indiquer un succès.	

9. **Réponse-confirmation de transfert de SMS**: accuse réception du message.

Transfert de SMS	réponse-confirmation
Aucun	(Note)

FEA9	– Transfère l'accusé de réception vers l'entité SCF dans le CNh.
NOTE – La réponse-confirmation est vide. Sa seule présence suffit à indiquer un succès.	

10. **Réponse-confirmation de retransmission de SMS**: accuse réception du message.

Retransmission de SMS	réponse-confirmation
Aucun	(Note)

FEA10	– Marque le message comme étant délivré avec succès.
NOTE – La réponse-confirmation est vide. Sa seule présence suffit à indiquer un succès.	

10.2 Diffusion de messages de téléservice (TMB)

Le présent sous-paragraphe traite des flux d'informations pour la diffusion de messages de téléservice (TMB) qui constitue une méthode de gestion et de livraison de messages texte de téléservice sur une interface radio vers des terminaux mobiles ITM-2000. Les messages texte peuvent s'utiliser entre autres pour les urgences, annonces administratives, publicités et services souscrits. La diffusion peut se faire sur une zone prescrite (c'est-à-dire sur tout ou partie d'un SACF ou CN). La diffusion peut se faire grâce à la prise en charge de la périodicité basée sur un réseau de rattachement ou grâce à la prise en charge de la périodicité basée sur un réseau visité. D'autres attributs tels que la langue de la diffusion, sa priorité caractérisent également la diffusion. Les diffusions de messages de téléservice ne font pas l'objet d'un accusé de réception (c'est-à-dire que le mobile n'est pas supposé répondre lorsqu'il reçoit un message de diffusion).

TMB a lieu de façon périodique selon les options suivantes:

NOTE – La **périodicité** consiste en une **heure de début**, un **taux de répétition** et une **durée**.

Option A: prise en charge de la périodicité basée sur un réseau visité – La périodicité de la diffusion des messages de téléservice est prise en charge par un réseau visité. Le message de téléservice devant être diffusé est déposé par un "client" dans le centre de messagerie, (le SCF_{SMS} du réseau de rattachement) qui le transfère ensuite vers une ou plusieurs entités CNv. Les SACF dans les CNv stockent alors le message et démarrent la diffusion du message à intervalles de temps réguliers et pour la durée prescrite, selon la périodicité spécifiée. Les SACF dans les CNv stockent le message jusqu'à achèvement de la diffusion (c'est-à-dire jusqu'à la fin de la période de diffusion). Le SACF peut réduire de façon prématurée, le temps de diffusion du message selon les directives du SCF_{SMS}.

Option B: prise en charge de la périodicité basée sur un réseau de rattachement – La périodicité de la diffusion des messages de téléservice est prise en charge par un réseau de rattachement. Le message de téléservice devant être diffusé, est déposé par un "client" dans le centre de messagerie (le SCF du réseau de rattachement), qui le transfère ensuite vers une ou plusieurs entités CNv. Les SACF dans les CNv diffusent alors immédiatement le message. Dans ce cas, les SACF n'ont pas besoin de stocker le message. Cependant, si le client avait souhaité la rediffusion à intervalles de temps réguliers et sur une durée donnée, le rattachement (SCF_{SMS}) peut envoyer à nouveau le message vers les CNv pour rediffusion. Dans ce scénario, le SCF_{SMS} dans le CNh a la charge de retenir le message jusqu'à achèvement de la diffusion (c'est-à-dire jusqu'à la fin de la période de diffusion).

Ces deux options sont illustrées dans la Figure 10.2-1.

De plus, l'entité SCF envoie la charge utile de la diffusion de messages de téléservice et les éléments d'information associés à tous les SACF dans les CNv qui font partie de la zone de diffusion prescrite. Cependant, la Figure 10.2-1 a été simplifiée.

En général, l'option A est utilisée pour des diffusions à taux de répétition élevé (par exemple, toutes les deux minutes) sur une courte durée (par exemple, pendant trois heures).

En général, l'option B est utilisée pour des diffusions à taux de répétition faible (par exemple, toutes les six heures) sur une durée importante (par exemple, pendant sept jours).

Il en est de la décision de l'exploitant: l'option A a tendance à utiliser des ressources système (mémoire) plus important alors que l'option B a tendance à utiliser des ressources en lien de signalisation plus important (niveau d'utilisation plus élevé).

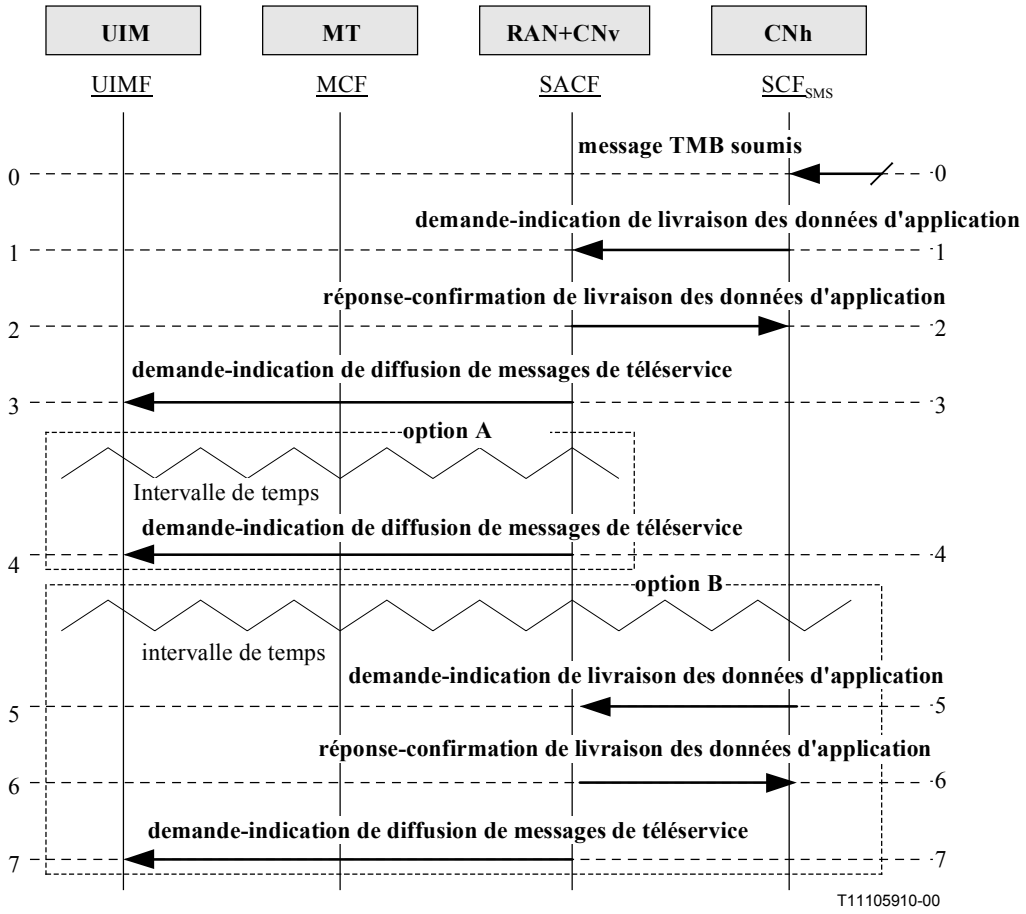


Figure 10.2-1/Q.1721 – Diffusion de messages de téléservice

0. **Message TMB soumis**: il s'agit du stimulus initial par lequel le "client" soumet un message en vue de le diffuser, par le biais de la diffusion de messages de téléservice. La demande inclut la charge utile de la diffusion actuelle, l'adresse de l'auteur, la catégorie de la diffusion, l'état du message diffusé, la priorité du message diffusé, la périodicité de la diffusion, le groupe de service de diffusion, l'identificateur de zone de diffusion et enfin la langue choisie pour la diffusion.

FEA0	– Lance l'option A (prise en charge de la périodicité basée sur un réseau visité) ou l'option B (prise en charge de la périodicité basée sur un réseau de rattachement) selon les demandes du TMB.

1. **demande-indication de livraison des données d'application**: en provenance de l'entité SCF dans le réseau de rattachement vers toutes les SACF qui prennent en charge la zone de diffusion.

Livraison de données d'application (réponse: succès)	demande-indication
Adresse de l'auteur	M
Charge utile	M
Catégorie	M
Type de message	M
Etat du message	M
Identificateur de zone	O (Note 1)
Périodicité	O (Note 2)
Priorité du message	O (Note 3)
Groupe de services	O (Note 4)
Langue choisie	O (Note 5)

FEA1	– Accuse réception de la demande de livraison des données d'application. – S'initialise pour envoyer la diffusion de messages de téléservice vers le réseau visité.
NOTE 1 – Inclut pour spécifier les zones de diffusion. L'absence d'éléments d'information implique une diffusion sur tout le SACF. NOTE 2 – Inclut pour la prise en charge de la périodicité basée sur un réseau visité si l'absence envoie un message une fois seulement. NOTE 3 – Inclut pour indiquer si la diffusion est normale (par défaut), interactive, pressante ou d'urgence. NOTE 4 – Inclut pour indiquer l'audience cible du terminal mobile (définie par l'exploitant). NOTE 5 – Inclut pour indiquer la langue dans laquelle le message est élaboré pour le filtrage.	

2. **Réponse-confirmation de livraison des données d'application**: accuse réception des demandes de livraison des données.

Livraison des données d'application	réponse-confirmation
Aucune	(Note)

FEA2	– Aucune action requise si l'option A est choisie. – Attendre l'expiration du timer si l'option B est choisie.
NOTE – La réponse-confirmation est vide. Sa seule présence suffit à indiquer un succès.	

3. **Demande-indication de diffusion de messages de téléservice**: transmet le message au UIMF.

Diffusion de messages de téléservice (réponse: aucune)	demande-indication
Adresse de l'auteur	M
Charge utile	M
Catégorie	M
Type de message	M
Etat du message	M
Priorité du message	O (Note 1)
Groupe de service	O (Note 2)
Langue choisie	O (Note 3)

FEA3	– Affiche le message pour l'utilisateur selon les paramètres reçus.
NOTE 1 – Inclut pour indiquer si la diffusion est normale (par défaut), interactive, pressante ou d'urgence. NOTE 2 – Inclut pour indiquer l'audience cible du terminal mobile (définie par l'opérateur). NOTE 3 – Inclut pour indiquer la langue dans laquelle le message est élaboré pour le filtrage.	

La 4e étape répète le flux d'informations 3 et n'est valable que dans le cas de l'option A, pour laquelle le réseau visité prend en charge la périodicité. Les éléments d'information et les actions d'entité fonctionnelle sont identiques à celles du flux d'informations 3. Cette étape se répète suivant la périodicité prescrite.

Les étapes 5, 6 et 7 sont identiques aux flux d'informations 1, 2 et 3 à part que la périodicité n'est pas incluse dans le flux d'informations 5. Elles sont valables seulement dans le cas de l'option B, dans laquelle le réseau de rattachement prend en en charge la périodicité. Ces étapes se répètent suivant la périodicité prescrite.

10.3 Notification de message en attente (MWN)

10.3.1 Flux d'informations de MWN

Ce scénario présente le flux d'informations relatif à la notification de message en attente (MWN, *message waiting notification*) pour des systèmes IMT-2000 dans une situation d'itinérance globale. La notification de message en attente (MWN) est une fonctionnalité grâce à laquelle les utilisateurs abonnés sont notifiés lorsque des messages de type voix, fax ou e-mail et autres, ont été déposés dans leurs systèmes de messagerie, et sont disponibles en vue de leur récupération. Voir Figure 10.3.1-1.

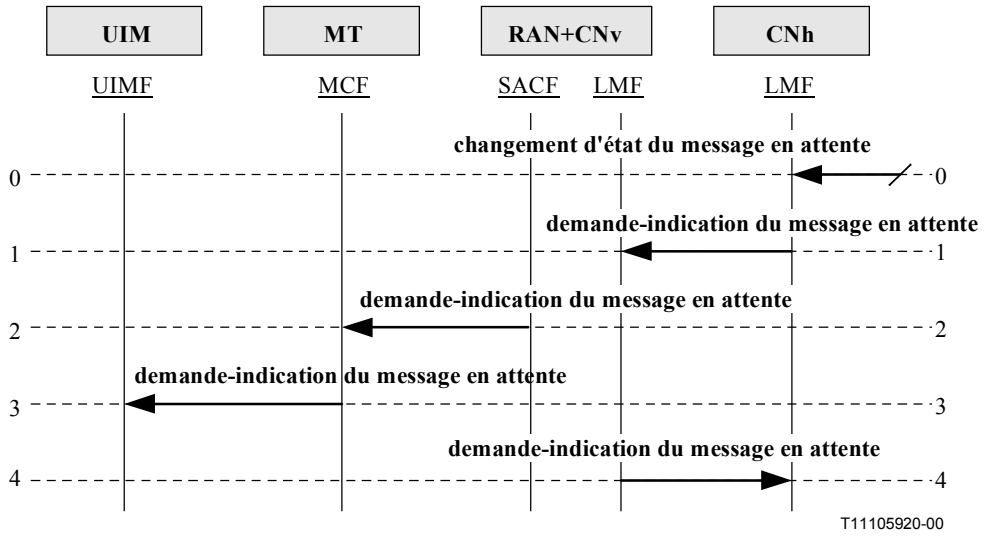


Figure 10.3.1-1/Q.1721 – Notification de messages en attente

0. **Changement d'état du message en attente**: il s'agit du stimulus initial par lequel un système de messagerie, fax ou serveur d'e-mail, ou une entité du même type, rapporte au LMFh, un changement d'état du message de voix, fax ou e-mail du terminal mobile.

FEA0	– Changement de l'état du message en attente.

1. **Demande-indication du message en attente:** pour chaque type de message (voix, fax, e-mail, etc.) une demande-indication individuelle peut être envoyée. Ou bien, en utilisant les paramètres du fabricant, les informations sur un ou plusieurs types de message peuvent être regroupées et envoyées en une seule demande-indication. Ce scénario illustre le mécanisme précédent.

Message en attente (réponse: succès)	demande-indication
IMUI	M
Indicateur du message en attente	M (Note 1)
Type de message en attente	O (Note 2)
Priorité du message	O (Note 3)
Nombre de messages en cours	O (Note 4)
Langue choisie	O (Note 5)

FEA1	– Effectue le relais du contenu vers le SACF afin d'être envoyé vers l'entité MCF.
NOTE 1 – Peut présenter deux valeurs "Oui" ou "Non". NOTE 2 – Indique si les messages sont des messages de type voix, fax, e-mail, ou autres. NOTE 3 – Inclut pour indiquer si la diffusion est normale (par défaut), interactive, pressante ou d'urgence. NOTE 4 – Indique le nombre de messages en cours. NOTE 5 – Indique la langue à utiliser si l'annonce de notification est faite.	

2. **Demande-indication de message en attente**: transfère les informations sur le message en attente vers l'entité MCF.

Message en attente (réponse: succès)	demande-indication
<Eléments d'information identiques à ceux trouvés dans le flux d'informations 1>	<Voir IF 1>

FEA2	– Effectue le relais du contenu vers l'UIMF.

3. **Demande-indication de message en attente**: transfère la notification du message en attente vers UIMF.

Notification de message en attente (MWN) (réponse: succès)	demande-indication
<Eléments d'information identiques à ceux trouvés dans le flux d'informations 1>	<Voir IF 1>

FEA3	– Utilise les informations reçues pour fournir le type de notification spécifiée à l'utilisateur.

4. **Réponse-confirmation de message en attente**: accuse réception de la notification de message en attente.

Notification de message en attente (MWN)	réponse-confirmation
Aucune	(Note)

FEA6	– Aucune action requise.
NOTE – La réponse-confirmation est vide. Sa seule présence suffit à indiquer un succès.	

11 Procédures de services complémentaires

Les fonctions suivantes peuvent ne pas être applicables à tous les membres de la famille IMT-2000.

Ces procédures indépendantes sont utilisées pour contrôler les services complémentaires (SS, *supplementary service*) d'un utilisateur. Elles sont initiées par l'utilisateur[7], normalement en appuyant sur les touches du terminal mobile.

Les procédures suivantes de services complémentaires sont décrites:

– obtenir le mot de passe;
– enregistrer le mot de passe;
– enregistrer le SS;
– effacer le SS;
– activer le SS;
– désactiver le SS;
– interroger le SS;
– invoquer le SS;
– traiter demande de SS non structuré;
– demande de SS non structuré;
– notification de SS non structuré;
– notification d'invocation de SS.

11.1 Obtenir le mot de passe

Cette procédure est initialisée par le réseau de rattachement pour demander un mot de passe à l'utilisateur, lorsque le réseau de rattachement reçoit une demande de l'utilisateur pour une opération de commande de service complémentaire qui nécessite un mot de passe. Cette procédure peut être utilisée en relation avec les autres procédures de commande de service complémentaire mais ne sera pas indiquée de façon explicite dans chacune d'entre elles. Voir Figure11.1-1.

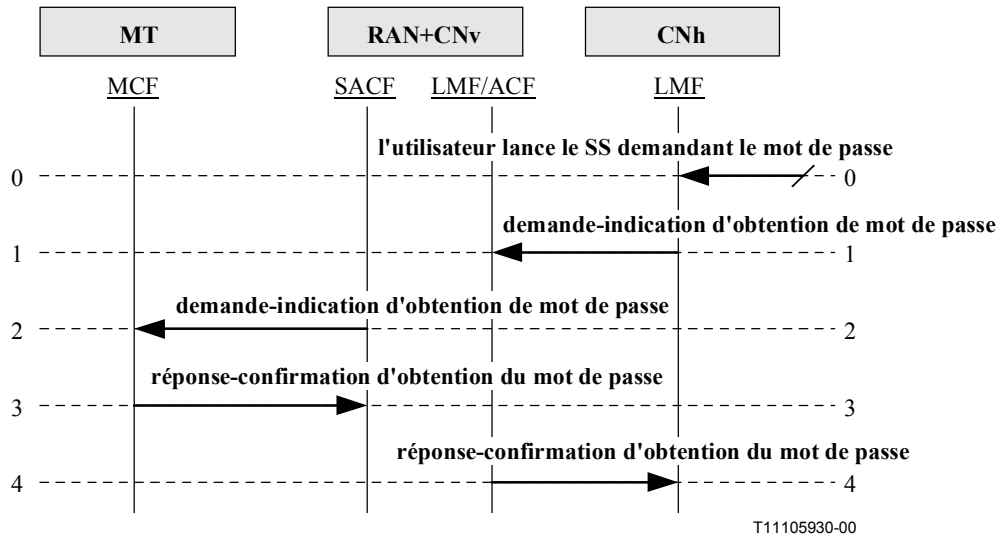


Figure 11.1-1/Q.1721 – Obtenir le mot de passe

[7] les procédures "obtenir mot de passe" et "notification de service complémentaire non structuré" sont lancées par le HLR (LMFh), mais sont déclenchées par d'autres procédures de commande de service complémentaire précédemment lancées par l'utilisateur.

0. **L'utilisateur lance le SS demandant le mot de passe**: la LMFh reçoit un SS initié par l'utilisateur demandant le mot de passe.

FEA0	– Détecte la nécessité de demander un mot de passe de l'utilisateur en réponse à une procédure SS initiée. – Prépare et envoie une demande-indication d'obtention de mot de passe dans le réseau visité.

1. **Demande-indication d'obtention de mot de passe**: est utilisée pour demander à l'utilisateur de fournir un mot de passe.

Obtenir le mot de passe (réponse: succès ou échec)	**demande-indication**
Informations d'aide	M

FEA1	– Relaie la demande-indication d'obtention de mot de passe à la SACF.

2. **Demande-indication d'obtention de mot de passe**: est utilisée pour demander à l'utilisateur de fournir un mot de passe via la MMI.

Obtenir le mot de passe (réponse: succès ou échec)	**demande-indication**
Informations d'aide	M

FEA2	– Interprète l'élément information d'aide et affiche l'information voulue à l'utilisateur via la MMI. – Reçoit le mot de passe de l'utilisateur via la MMI. – Prépare et envoie une réponse-confirmation d'obtention de mot de passe à la SACF, éventuellement en utilisant plusieurs messages, par exemple pour l'émulation DTMF (DTMF, *dual-tone multifrequency*).

3. **Réponse-confirmation d'obtention du mot de passe**: envoie le mot de passe courant et le résultat à la SACF.

Obtenir le mot de passe	**réponse-confirmation**
Mot de passe courant	M
Résultat	M

FEA3	– Retransmet la réponse-confirmation d'obtention du mot de passe à l'entité LMFv. – Prépare et envoie une réponse-confirmation d'obtention de mot de passe à la LMFh, éventuellement en utilisant plusieurs messages, par exemple pour l'émulation DTMF.

4. **Réponse-confirmation d'obtention du mot de passe**: envoie le mot de passe actuel et le résultat à la LMFh.

Obtenir le mot de passe	**réponse-confirmation**
Mot de passe actuel	M
Résultat	M

FEA4	– Mot de passe confirmé contrôlé.

11.2 Enregistrer le mot de passe

Cette procédure est initiée par le réseau de rattachement pour demander l'ancien mot de passe de l'utilisateur. Quand le réseau de rattachement reçoit l'ancien mot de passe, une demande est envoyée à l'utilisateur pour demander le nouveau mot de passe. Le réseau de rattachement demandera à l'utilisateur de confirmer ce nouveau mot de passe. Voir Figure11.2-1.

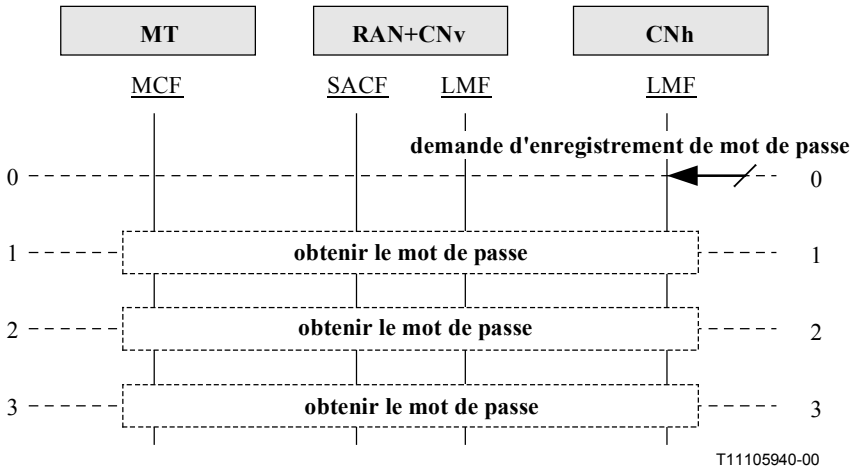


Figure 11.2-1/Q.1721 – Enregistrement du mot de passe

0. **Demande d'enregistrement de mot de passe**: l'utilisateur demande de changer le mot de passe pour un service complémentaire.

1. **Obtenir le mot de passe**: la LMFh demande l'ancien mot de passe à l'utilisateur.

2. **Obtenir le mot de passe**: la LMFh demande à l'utilisateur de donner le nouveau mot de passe.

3. **Obtenir le mot de passe**: la LMFh demande à l'utilisateur de confirmer le nouveau mot de passe.

11.3 Enregistrer le SS

Cette procédure est utilisée pour enregistrer des données relatives à un service complémentaire dans le réseau de rattachement. Voir Figure 11.3-1.

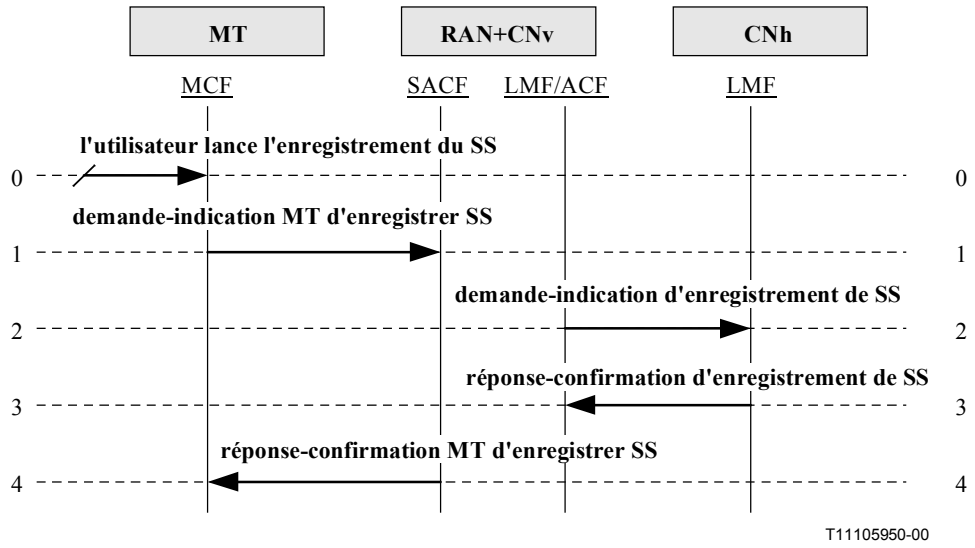


Figure 11.3-1/Q.1721 – Enregistrement du SS

0. **L'utilisateur lance l'enregistrement du SS**: la MCF reçoit un enregistrement du SS initié par l'utilisateur.

FEA0	– Détecte une procédure de commande de SS initiée par l'utilisateur via la MMI pour demander un enregistrement de service complémentaire. – Prépare et envoie l'information reçue à la SACF.

1. **Demande-indication MT d'enregistrer SS**: est utilisée pour demander d'enregistrer un service complémentaire.

MT enregistrer SS (réponse: succès ou échec)	demande-indication
Code SS	M
Données SS	M

FEA1	– Prépare et envoie une demande-indication d'enregistrer SS à l'entité LMFv.

2. **Demande-indication d'enregistrer de SS**: est utilisée pour demander à la LMFh d'enregistrer un service complémentaire.

Enregistrer le SS (réponse: succès ou échec)	demande-indication
Code SS	M
Données SS	M

FEA2	– Identifie le service complémentaire concerné. – Sauvegarde les données du SS reçues en fonction de la commande. – Prépare et envoie une réponse-confirmation d'enregistrement de SS à l'entité LMFv.

3. **Réponse-confirmation d'enregistrer SS**: est utilisée pour renvoyer une réponse à l'utilisateur et l'informer du résultat de l'enregistrement.

Enregistrer le SS (réponse: succès ou échec)	réponse-confirmation
Résultat	M

FEA3	– Relaie l'information à la SACF. – Prépare et envoie une réponse-confirmation MT enregistrer SS de la SACF.

4. **Réponse-confirmation MT enregistrer SS**: envoie le résultat de l'enregistrement du service complémentaire à l'utilisateur.

MT enregistrer SS	réponse-confirmation
Résultat	M

FEA4	– Confirme à l'utilisateur que les données correspondant au service complémentaire ont été sauvegardées dans la LMFh.

11.4 Effacer le SS

Cette procédure est initiée par l'utilisateur pour effacer l'information sauvegardée pour un service complémentaire particulier par un enregistrement précédent dans le réseau de rattachement. Voir Figure 11.4-1.

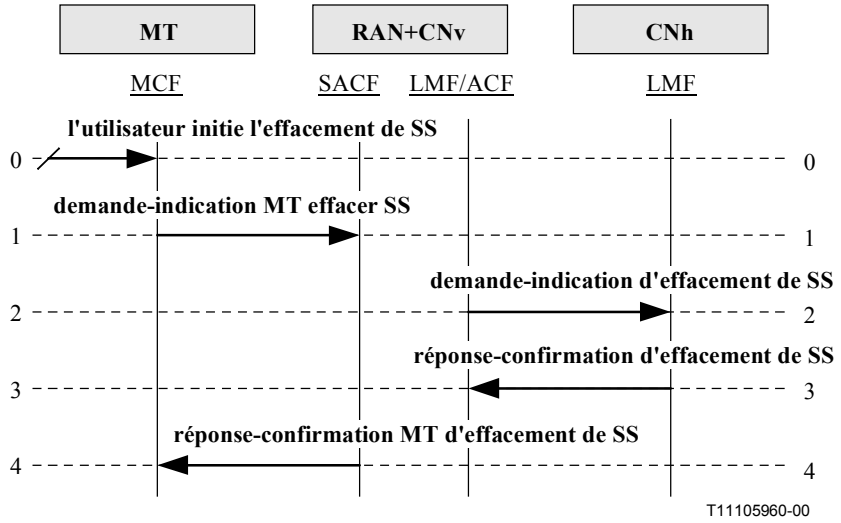


Figure 11.4-1/Q.1721 – Effacement de SS

0. **L'utilisateur initie l'effacement de SS**: la MCF reçoit un effacement de SS initié par l'utilisateur.

FEA0	– Détecte une procédure de commande de SS initiée par l'utilisateur via la MMI pour demander l'effacement d'un service complémentaire. – Prépare et envoie l'information reçue à la SACF.

1. **Demande-indication MT effacer SS**: est utilisée pour demander d'effacer un service complémentaire.

MT effacer SS (réponse: succès ou échec)	demande-indication
Code SS	M
Données SS	O (Note)

FEA1	– Demande d'effacer les données SS.
NOTE – Uniquement demandé pour les services complémentaires qui ont des données.	

2. **Demande-indication d'effacement de SS**: est utilisée pour demander à la LMFh d'effacer un service complémentaire.

Effacer SS (réponse: succès ou échec)	demande-indication
Code SS	M
Données SS	O (Note)

FEA2	– Identifie le service complémentaire concerné. – Efface les données SS en fonction de la commande.
NOTE – Uniquement demandé pour les services complémentaires qui ont des données.	

3. **Réponse-confirmation d'effacement de SS**: est utilisée pour renvoyer une réponse à l'utilisateur pour l'informer du résultat de l'effacement.

Supprimer SS (réponse: succès ou échec)	réponse-confirmation
Résultat	M

FEA3	– Relaie l'information à la SACF.

4. **Réponse-confirmation MT d'effacement de SS**: envoie le résultat de l'effacement de service complémentaire à l'utilisateur.

MT effacer SS	réponse-confirmation
Résultat	M

FEA4	– Aucune action requise.

11.5 Activer le SS

Cette procédure est utilisée pour activer l'exécution d'un procédé de la façon et au moment prescrit par le service concerné, aboutissant à la phase active. Certains services peuvent être soit "opérationnels", soit "passifs" (non opérationnels) pendant la phase active, selon que le système est ou non capable d'invoquer ou d'utiliser le service. L'information est stockée dans le réseau de rattachement et pour certains services significatifs, elle est également sauvegardée dans le réseau serveur. Voir Figure 11.5-1.

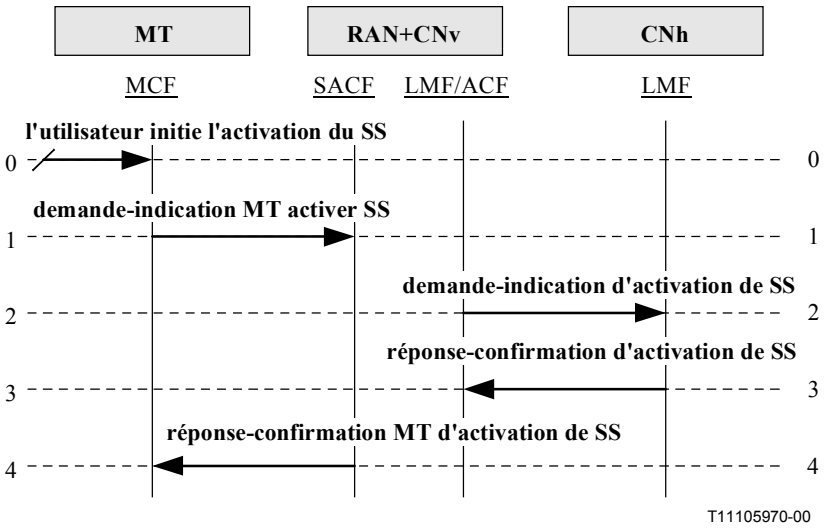


Figure 11.5-1/Q.1721 – Activation du SS

0. **L'utilisateur initie l'activation du SS**: la MCF reçoit une activation de SS initiée par l'utilisateur.

FEA0	– Détecte une procédure de commande SS initiée par l'utilisateur via la MMI pour demander l'activation d'un service complémentaire. – Prépare et envoie l'information reçue à la SACF.

1. **Demande-indication MT activer SS**: est utilisée pour demander d'activer un service complémentaire.

MT activer SS (réponse: succès ou échec)	demande-indication
Code SS	M
Données SS	O (Note)

FEA1	– Demande d'activer un SS.
NOTE – Uniquement demandé pour les services complémentaires qui ont des données.	

2. **Demande-indication d'activation de SS**: est utilisée pour demander à la LMFh d'activer un service complémentaire.

Activer SS (réponse: succès ou échec)	demande-indication
Code SS	M
Données SS	O (Note)

FEA2	– Identifie le service complémentaire concerné. – Données d'activation du SS en fonction de la commande.
NOTE – Uniquement demandé pour les services complémentaires qui ont des données.	

3. **Réponse-confirmation d'activation de SS**: est utilisée pour renvoyer une réponse à l'utilisateur pour l'informer du résultat de l'activation.

Activer SS (réponse: succès ou échec)	réponse-confirmation
Résultat	M

FEA3	– Relaie l'information à la SACF.

4. **Réponse-confirmation MT d'activation de SS**: envoie le résultat de l'activation de service complémentaire à l'utilisateur.

MT activer SS	réponse-confirmation
Résultat	M

FEA4	– Aucune action requise.

11.6 Désactiver le SS

Cette procédure est initiée par l'utilisateur pour mettre fin à la procédure commencée avec l'activation. L'information sera stockée dans le réseau de rattachement et pour certains services significatifs enregistrée également dans le réseau serveur. Voir Figure 11.6-1.

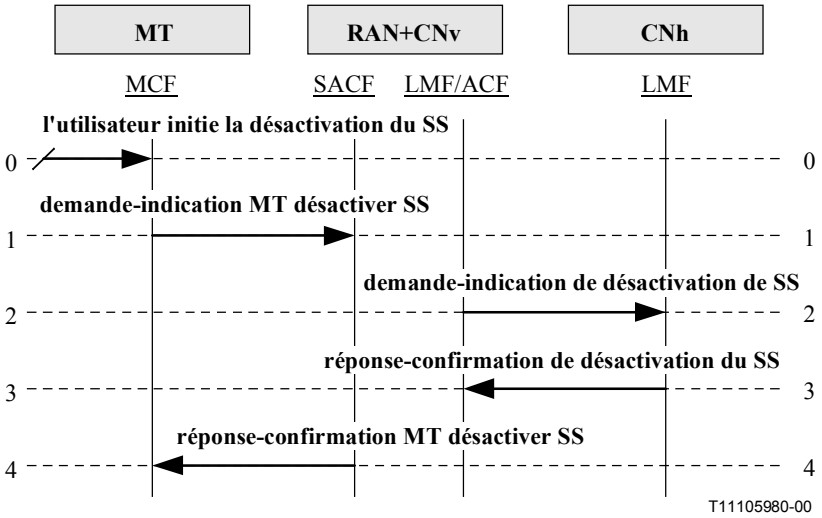


Figure 11.6-1/Q.1721 – Désactivation de SS

0. **L'utilisateur initie la désactivation du SS**: la MCF reçoit une désactivation de SS initiée par l'utilisateur.

FEA0	– Détecte une procédure de commande SS initiée par l'utilisateur via la MMI pour demander la désactivation d'un service complémentaire. – Prépare et envoie l'information reçue à la SACF.

1. **Demande-indication MT désactiver SS**: est utilisée pour demander de désactiver un service complémentaire.

MT désactiver SS (réponse: succès ou échec)	demande-indication
Code SS	M
Données SS	O (Note)

FEA1	– Demande de désactivation de SS.
NOTE – Uniquement demandé pour les services complémentaires qui ont des données.	

2. **Demande-indication de désactivation de SS**: est utilisée pour demander à la LMFh de désactiver un service complémentaire.

Désactiver SS (réponse: succès ou échec)	demande-indication
Code SS	M
Données SS	O (Note)

FEA2	– Identifie le service complémentaire concerné. – Désactive les données SS en fonction de la commande.
NOTE – Uniquement demandé pour les services complémentaires qui ont des données.	

3. **Réponse-confirmation de désactivation du SS**: est utilisée pour renvoyer une réponse à l'utilisateur pour l'informer du résultat de la désactivation.

Désactiver SS (réponse: succès ou échec)	réponse-confirmation
Résultat	M

FEA3	– Relaie l'information à la SACF.

4. **Réponse-confirmation MT désactiver SS**: envoie le résultat de la désactivation de service complémentaire à l'utilisateur.

MT désactiver SS	réponse-confirmation
Résultat	M

FEA4	– Aucune action requise.

11.7 Interroger le SS

Cette procédure est initiée par l'utilisateur pour fournir une information sur un service complémentaire spécifique. L'information est recherchée dans le réseau de rattachement. Voir Figure11.7-1.

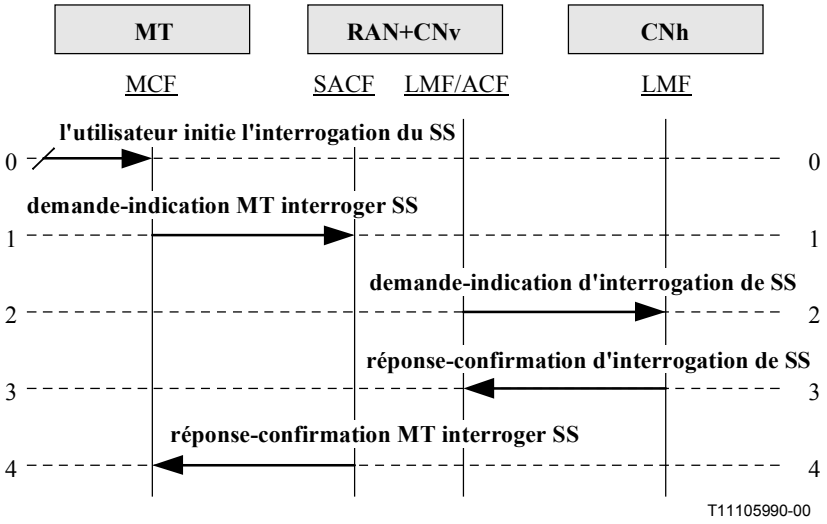


Figure 11.7-1/Q.1721 – Interrogation de SS

0. **L'utilisateur initie l'interrogation du SS**: la MCF reçoit une interrogation de SS initiée par l'utilisateur.

FEA0	– Détecte une procédure de commande de SS initiée par l'utilisateur via la MMI pour demander l'interrogation d'un service complémentaire. – Prépare et envoie l'information reçue à la SACF.

1. **Demande-indication MT interroger SS**: est utilisée pour demander d'extraire l'information relative à un service complémentaire.

MT interroger SS (réponse: succès ou échec)	**demande-indication**
Code SS	M
Données SS	O (Note)

FEA1	– Demande d'interrogation des données du SS.
NOTE – Uniquement demandé pour les services complémentaires qui ont des données.	

2. **Demande-indication d'interrogation de SS**: est utilisée pour demander à la LMFh si nécessaire d'extraire l'information relative à un service complémentaire.

Interroger SS (réponse: succès ou échec)	**demande-indication**
Code SS	M
Données SS	O (Note)

FEA2	– Identifie le service complémentaire concerné. – Interroge les données SS en fonction de la commande.
NOTE – Uniquement demandé pour les services complémentaires qui ont des données.	

3. **Réponse-confirmation d'interrogation de SS**: est utilisée pour renvoyer une réponse à l'utilisateur pour l'informer du résultat de l'interrogation.

Interroger SS (réponse: succès ou échec)	réponse-confirmation
Résultat	M

FEA3	– Relaie l'information à la SACF.

4. **Réponse-confirmation MT interroger SS**: envoie à l'utilisateur le résultat de l'information extraite pour le service complémentaire.

MT interroger SS	réponse-confirmation
Résultat	M

FEA4	– Aucune action requise.

11.8 Invoquer le SS

Cette procédure est initiée par l'utilisateur. La procédure est utilisée pour vérifier l'abonnement de l'utilisateur à un service complémentaire donné dans le réseau serveur. Voir la Figure 11.8-1.

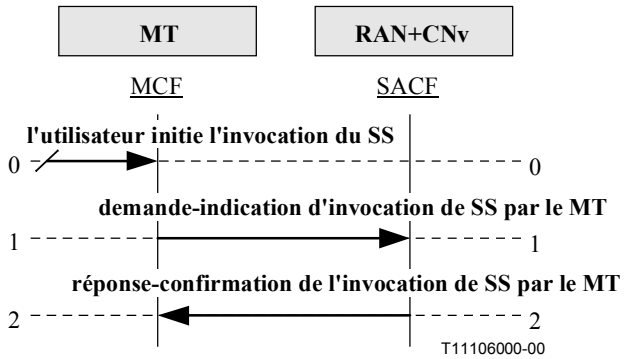


Figure 11.8-1/Q.1721 – Invocation de SS

0. **L'utilisateur initie l'invocation du SS**: la MCF reçoit une invocation de SS initiée par l'utilisateur.

FEA0	– Détecte une procédure de commande SS initiée par l'utilisateur via la MMI pour demander une invocation de service complémentaire. – Prépare et envoie l'information reçue à la SACF.

1. **Demande-indication d'invocation de SS par le MT**: est utilisée pour demander de vérifier l'abonnement de l'abonné à un service complémentaire donné (par exemple, mise en attente ou appel multiparticipants) dans l'entité LMFv, en relation avec une invocation d'appel de ce service complémentaire, c'est-à-dire après que la phase d'établissement d'appel est achevée.

Invocation de SS par le MT (réponse: succès ou échec)	demande-indication
Code SS	M
Données SS	O (Note)

FEA1	– Identifie le service complémentaire concerné. – Vérifie l'abonnement de l'utilisateur en fonction de l'information reçue. – Prépare et envoie l'information à la SACF.
NOTE – Uniquement demandé pour les services complémentaires qui ont des données.	

2. **Réponse-confirmation de l'invocation de SS par le MT**: envoie à l'utilisateur le résultat de l'information d'abonnement vérifiée de l'abonné au service complémentaire.

Interrogation de SS par le terminal mobile	réponse-confirmation
Résultat	M

FEA2	– Présente le résultat pour l'utilisateur.

11.9 Traitement de la demande de SS non structuré

Cette procédure est utilisée pour relayer l'information, afin de permettre une exploitation des services complémentaires non structurés. L'entité de réseau reçue transmet les données reçues à l'application gérant l'application de services complémentaires non structurés et attend la réponse de l'application. Voir Figure11.9-1.

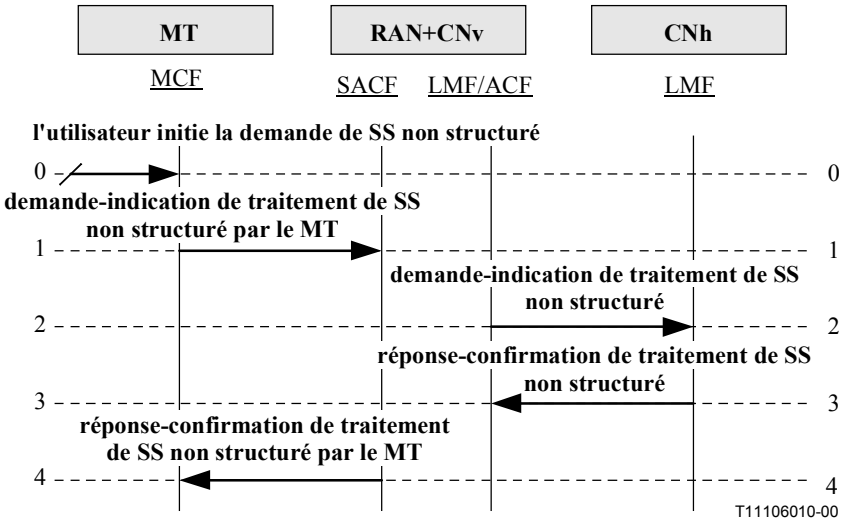


Figure 11.9-1/Q.1721 – Traitement de demande de SS non structuré

0. **L'utilisateur initie la demande de SS non structuré**: la MCF reçoit une demande de traitement de SS non structuré initiée par l'utilisateur.

FEA0	– Détecte une procédure de commande SS initiée par l'utilisateur via la MMI pour demander le traitement d'une demande non structurée d'un service complémentaire. – Prépare et envoie l'information reçue à la SACF.

1. **Demande-indication de traitement de SS non structuré par le MT**: est utilisée pour demander d'autoriser une opération de service complémentaire non structuré.

Traitement de SS non structuré par le terminal mobile (réponse: succès ou échec)	demande-indication
Schéma de codage de données USSD	M
Chaîne USSD	M

FEA1	– Demande de données de SS non structuré dans la procédure.

2. **Demande-indication de traitement de SS non structuré par le MT**: est utilisée pour demander à la LMFh de traiter la demande USSD.

Traitement de SS non structuré (réponse: succès ou échec)	demande-indication
Schéma de codage de données USSD	M
Chaîne USSD	M

FEA2	Exécute une ou plusieurs des fonctions suivantes comme exigé par la logique de service: – Etablir ou libérer les canaux de parole. – Transmettre la demande à une autre entité de réseau (inchangée ou changée). – Passer une demande USSD différente à une autre entité de réseau. – Demander une information complémentaire à l'utilisateur.

3. **Réponse-confirmation de traitement de SS non structuré**: est utilisée pour renvoyer une réponse à l'utilisateur pour l'informer du résultat de la demande de SS non structuré dans la procédure.

Traitement de SS non structuré (réponse: succès ou échec)	réponse-confirmation
Schéma de codage de données USSD	O (Note 1)
Chaîne USSD	O (Note 2)
Résultat	O (Note 3)

FEA3	– Relaie l'information à la SACF.
NOTE 1 – Si cet IE est présent, l'IE de la chaîne USSD doit être présent. NOTE 2 – Si cet IE est présent, l'IE du schéma de codage des données USSD doit être présent. NOTE 3 – Utilisé uniquement si une situation d'erreur s'est produite.	

4. **Réponse-confirmation de traitement de SS non structuré par le MT**: envoie le résultat de l'information de service complémentaire extraite à l'utilisateur.

Traitement de SS non structuré par le terminal mobile	réponse-confirmation
Schéma de codage USSD	O (Note 1)
Chaîne USSD	O (Note 2)
Résultat	O (Note 3)

FEA4	– Confirmation permettant le fonctionnement du service complémentaire non structuré d'être utilisé.
NOTE 1 – Si cet IE est présent, l'IE de la chaîne USSD doit être présent. NOTE 2 – Si cet IE est présent, l'IE du schéma de codage des données USSD doit être présent. NOTE 3 – Utilisé uniquement si une situation d'erreur s'est produite.	

11.10 Demande de SS non structuré

Cette procédure est utilisée par l'entité qui effectue l'invocation quand une information de l'utilisateur mobile est requise en relation avec la gestion du service complémentaire non structuré.

Dans certaines circonstances, le SCFh peut générer (ou recevoir) une demande de SS non structuré vers (ou depuis) la LMFh. Ceci se produit en principe quand un service spécifique de l'exploitant, fourni par la SCF de rattachement, exige un dialogue avec l'utilisateur mobile. Ce dialogue peut être initié par l'utilisateur ou le service SCF. Les données de service complémentaire fournissent un mécanisme de transport transparent, qui permet à ce dialogue utilisateur mobile/service d'avoir lieu. Voir Figure11.10-1.

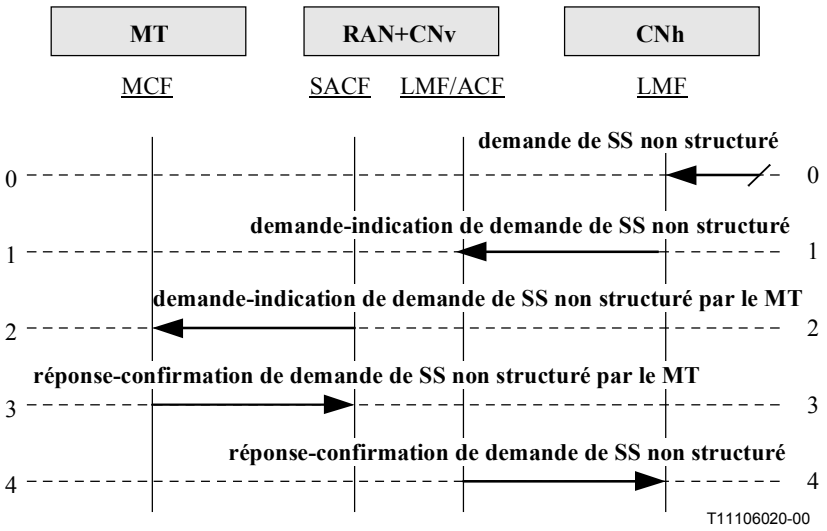


Figure 11.10-1/Q.1721 – Demande de SS non structuré

0. **Demande de SS non structuré**: l'entité qui effectue l'invocation exige une information de l'utilisateur mobile.

FEA0	– Prépare et envoie une demande-indication de SS non structuré à l'entité LMFv.

1. **Demande-indication de demande de SS non structuré**: est utilisée pour demander une information à l'utilisateur mobile.

Demande de SS non structuré (réponse: succès ou échec)	demande-indication
Schéma de codage de données USSD	M
Chaîne USSD	M
Schéma d'alerte	O (Note)

FEA1	– Prépare et envoie une demande-indication de SS non structuré à la SACF.
NOTE – Présent en cas de réception dans l'opération de connexion de la SCFh, sinon absente.	

2. **Demande-indication de demande de SS non structuré par le MT**: est utilisée pour demander à l'utilisateur mobile.

MT demande de SS non structuré (réponse: succès ou échec)	demande-indication
Schéma de codage de données USSD	M
Chaîne USSD	M
Schéma d'alerte	O (Note)

FEA2	– Prépare et envoie une réponse-confirmation de demande de SS non structuré par le MT à la SACF.
NOTE – Présent en cas de réception dans l'opération de connexion de la SCFh, sinon absente.	

3. **Réponse-confirmation de demande de SS non structuré par le MT**: est utilisée pour renvoyer une réponse à la LMFh via la SACF et l'entité LMFv au sujet du résultat de la demande.

Demande de SS non structuré par le MT (réponse: succès ou échec)	réponse-confirmation
Schéma de codage de données USSD	O (Note 1)
Chaîne USSD	O (Note 2)
Résultat	O (Note 3)

FEA3	– Prépare et envoie une réponse-confirmation de demande de SS non structuré à l'entité LMFv.
NOTE 1 – Si cet IE est présent, l'IE de la chaîne USSD doit être présent.	
NOTE 2 – Si cet IE est présent, l'IE du schéma de codage des données USSD doit être présent.	
NOTE 3 – Utilisé uniquement si une situation d'erreur s'est produite.	

4. **Réponse-confirmation de demande de SS non structuré**: envoie le résultat des informations extraites de l'utilisateur mobile.

Demande de SS non structuré	réponse-confirmation
Schéma de codage de données USSD	O (Note 1)
Chaîne USSD	O (Note 2)
Résultat	O (Note 3)

FEA4	– L'information requise a été recherchée chez l'utilisateur.
NOTE 1 – Si cet IE est présent, l'IE de la chaîne USSD doit être présent.	
NOTE 2 – Si cet IE est présent, l'IE du schéma de codage des données USSD doit être présent.	
NOTE 3 – Utilisé uniquement si une situation d'erreur s'est produite.	

11.11 Notification de SS non structuré

Cette procédure est utilisée par l'entité qui effectue l'invocation lorsqu'il est nécessaire d'envoyer une notification à l'utilisateur mobile, en relation avec la gestion des services complémentaires non structurés.

Dans certaines circonstances, la SCFh peut générer (ou recevoir) une demande de notification de SS non structuré vers (ou depuis) la LMFh. Ceci se produit en principe, quand un service exploitant spécifique, qui est fourni par la SCF de rattachement demande un dialogue avec l'utilisateur mobile. Ce dialogue peut être initié par l'utilisateur ou par le service SCF. Les données du service complémentaire non structuré fournissent un mécanisme de transport transparent qui permet à ce dialogue utilisateur mobile/service d'avoir lieu. Voir Figure 11.11-11.

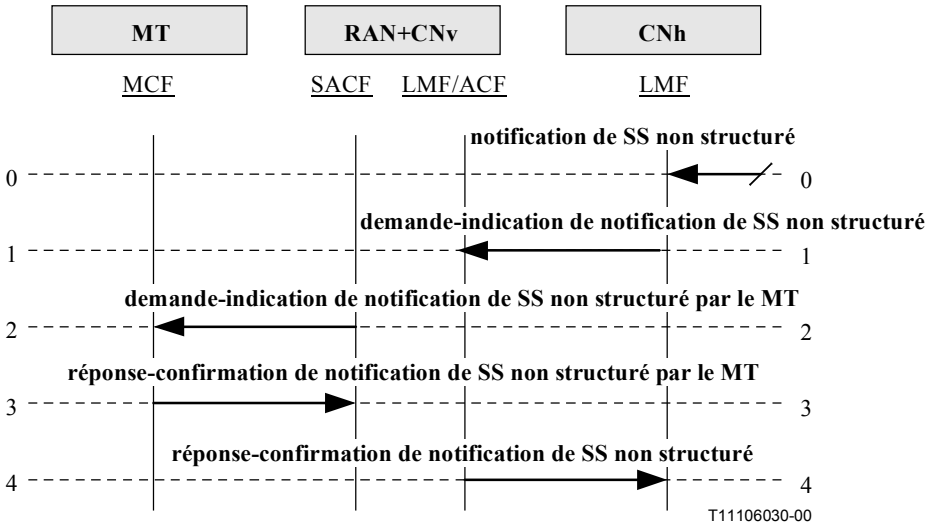


Figure 11.11-1/Q.1721 – Notification de SS non structuré

0. **Notification de SS non structuré**: indique qu'une notification sera envoyée à l'utilisateur mobile.

FEA0	– Envoie une demande de notification de SS non structuré à l'entité LMFv.

1. **Demande-indication de notification de SS non structuré**: est utilisée pour envoyer une information à l'utilisateur mobile.

Notification de SS non structuré (réponse: succès ou échec)	demande-indication
Schéma de codage de données USSD	M
Chaîne USSD	M
Schéma d'alerte	O (Note)

FEA1	– Envoie une demande de notification de SS non structuré à la SACF.
NOTE – Présent en cas de réception dans l'opération de connexion de la SCFh, sinon absente.	

2. **Demande-indication de notification de SS non structuré par le MT**: est utilisée pour envoyer une information à l'utilisateur mobile.

Notification de SS non structuré par le terminal mobile (réponse: succès ou échec)	demande-indication
Schéma de codage de données USSD	M
Chaîne USSD	M
Schéma d'alerte	O (Note)

FEA2	– Envoie une réponse de notification de SS non structuré par le MT à la SACF.
NOTE – Présent en cas de réception dans l'opération de connexion de la SCFh, sinon absente.	

3. **Réponse-confirmation de notification de SS non structuré par le MT**: est utilisée pour renvoyer une réponse à la LMFh via la SACF et l'entité LMFv au sujet du résultat de la demande.

Notification de SS non structuré par le terminal mobile (réponse: succès ou échec)	réponse-confirmation
Résultat	O (Note)

FEA3	– Envoie une réponse de notification de SS non structuré par le MT.
NOTE – Uniquement utilisé si une situation d'erreur se produit.	

4. **Réponse-confirmation de notification de SS non structuré**: envoie le résultat de l'information extraite de l'utilisateur mobile.

Notification de SS non structuré	réponse-confirmation
Résultat	O (Note)

FEA4	– Confirme la réception de l'information extraite.
NOTE – Uniquement utilisé si une situation d'erreur se produit.	

11.12 Notification d'invocation de SS

Cette procédure est utilisée entre la SACF et la SCF lors de l'invocation de certains services complémentaires par l'utilisateur. Les services sont le transfert d'appel, le détournement d'appel et le service d'appel multiparticipants. La SACF vérifie si les critères d'envoi d'une notification sont remplis. Si c'est le cas, une notification est envoyée au SCF de rattachement. Si les critères de notification ne sont pas satisfaits, le traitement du service complémentaire particulier reste inchangé et aucune notification n'est envoyée. Voir Figure11.12-1.

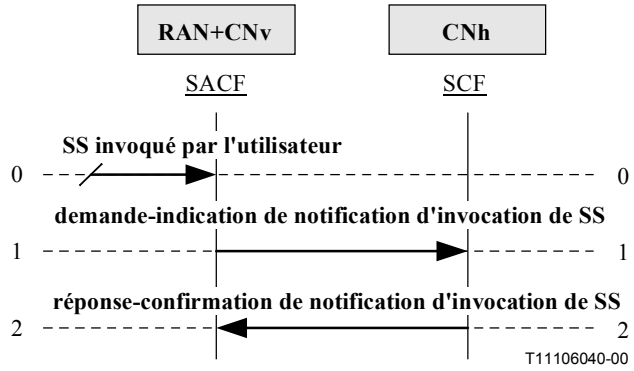


Figure 11.12-1/Q.1721 – Notification d'invocation

0. **SS invoqué par l'utilisateur**: la SACF reçoit une invocation de SS initiée par l'utilisateur.

FEA0	– Détecte l'invocation d'un service complémentaire donné. – Prépare et envoie une demande-indication de notification d'invocation de SS à la SCF.

1. **Demande-indication de notification d'invocation de SS**: est utilisée quand un abonné invoque un service complémentaire donné.

Notification d'invocation de SS (réponse: succès ou échec)	demande-indication
MSISDN	M
IMUI	M
Evénement-SS	M
Données SS	O (Note)

FEA1	– Si l'information reçue est comprise, prépare et envoie une réponse-confirmation de notification d'invocation de SS avec accusé de réception positif. – Si l'information reçue n'est pas comprise, prépare et envoie une réponse-confirmation de notification d'invocation de SS avec accusé de réception négatif.
NOTE – Les services complémentaires ne contiennent pas tous des données.	

2. **Réponse-confirmation de notification d'invocation de SS**: renvoie le résultat de la notification d'invocation à la SACF.

Notification d'invocation de SS	réponse-confirmation
Résultat	M

FEA2	– Confirme l'achèvement de la procédure de notification d'invocation de SS.

12 Services par voie hertzienne

La fonctionnalité suivante peut ne pas être applicable à tous les membres de la famille des IMT-2000.

12.1 Fourniture de services par voie hertzienne (OTASP)

Le présent paragraphe fournit des schémas fonctionnels d'information pour l'un des services par voie hertzienne (OTA, *over-the-air*) appelé fourniture de service sur voie hertzienne (OTASP, *over-the-air service provisioning*) pour les systèmes IMT-2000.

12.2 Aperçu général

La fonctionnalité OTASP répond à un besoin de l'industrie des sans fil basée IMT-2000 et définit de façon sûre le processus par lequel les abonnés potentiels du service IMT-2000 peuvent activer (c'est-à-dire, recevoir l'autorisation pour) de nouveaux services. En outre, les abonnés peuvent demander des changements dans leur service existant, sans l'intervention d'un tiers. L'un des composants de processus est la fonctionnalité hertzienne dans l'entité CNh.

L'un des tout premiers objectifs OTASP est de pouvoir fournir une clé d'authentification sûre à un UIM pour faciliter l'authentification. L'authentification est la procédure par laquelle l'information est échangée entre un UIM et le réseau dans le but de confirmer et de valider l'identité de l'UIM.

La fonctionnalité OTASP intègre une procédure de génération de clé d'authentification cryptographique. Cette procédure permet au réseau d'échanger des paramètres de clé d'authentification avec un UIM. Ces paramètres sont utilisés pour générer la clé d'authentification. La procédure de génération de clé d'authentification accroît la sécurité de l'abonné (c'est-à-dire, le chiffrement de la parole et des données peut être activé pour permettre le transfert sûr d'un nouveau crédit de l'abonné et l'information IMUI). La possibilité d'usage frauduleux du service de télécommunications IMT-2000 en est ainsi réduite.

12.3 Description

Le flux d'informations OTASP illustre la progression logique d'événements suivante:

- **invocation d'activation avec le fournisseur de service désiré**: où un "attachement" se produit entre l'entité CNv et la fonctionnalité par voie hertzienne (modélisée dans SCF et décrite dans le flux d'informations comme SCF_{OTA}) dans le CN du fournisseur de service désiré et une corrélation entre le trajet de la parole (utilisateur vers représentant du client (CR, *customer representative*) ou une unité de réponse vocale (VRU, *voice response unit*) au centre de service client (CSC, *customer service center*) et le trajet de données (entre l'UIM et la fonctionnalité par voie hertzienne) est établi. Le terminal mobile assure l'accès système initial basé sur une liste de sélection de systèmes préférentiels qui est chargée d'avance dans l'UIMF. L'utilisateur numérote les chiffres OTASP prescrits pour initier le processus d'activation. Le réseau visité doit être capable de reconnaître et de traiter les chiffres reçus du terminal mobile afin d'initier la session OTASP. Avec les chiffres, le réseau visité devra reconnaître qu'il s'agit d'une origine OTASP et router l'appel de façon appropriée au CSC. Ce traitement spécial des chiffres reçus exigera un accord commercial bilatéral entre le réseau de rattachement et les systèmes visités qui dépasse le domaine d'application de la présente recommandation;
- **génération de la clé d'authentification**: où la clé d'authentification est générée séparément dans l'entité AMF et l'entité UIMF. La clé d'authentification est alors utilisée pour le chiffrement et la sécurité pendant le processus OTASP;
- **réauthentification pour chiffrement de la parole et de la signalisation**: cette procédure calcule et transfère l'information de chiffrement à l'entité CNv pour invoquer le chiffrement

du plan utilisateur (parole) et du plan de commande (messages de signalisation), avant d'échanger par voie hertzienne des informations financières et de fourniture sensibles;

- **transfert de données OTASP**: où l'information de fourniture réelle est transférée entre le réseau de rattachement et l'UIM.

12.4 Flux d'informations de fourniture de services par voie hertzienne

12.4.1 Invocation d'activation auprès du fournisseur de service désiré

Un abonné potentiel ("utilisateur") veut activer un terminal mobile IMT-2000 dans le réseau d'un fournisseur de service voulu (le réseau de "rattachement"), tout en étant dans un autre réseau (le réseau "visité"). Ce flux d'informations montre la première étape de l'OTASP appelée procédure "d'attachement", par lequel l'appel de parole de l'utilisateur est mis en corrélation avec le trajet de données et l'information nécessaire est téléchargée dans l'UIM. L'origine de l'appel de parole de l'utilisateur est redirigée du réseau visité vers un représentant du client (CR – humain) ou une unité de réponse vocale (VRU – machine), au Centre de service clients (CSC) dans le réseau de rattachement. Le réseau visité attribue un numéro de référence temporaire (TNR, *temporary reference number)* pour la corrélation des trajets parole et données. Le pool TRN est administré par des accords bilatéraux entre les fournisseurs de services partenaires, afin de conserver le caractère unique des TRN utilisés dans chaque réseau visité. Le réseau de rattachement attribue une IMUI d'"activation" qui est utilisée pendant le processus d'activation. Voir Figure 12.4-1.

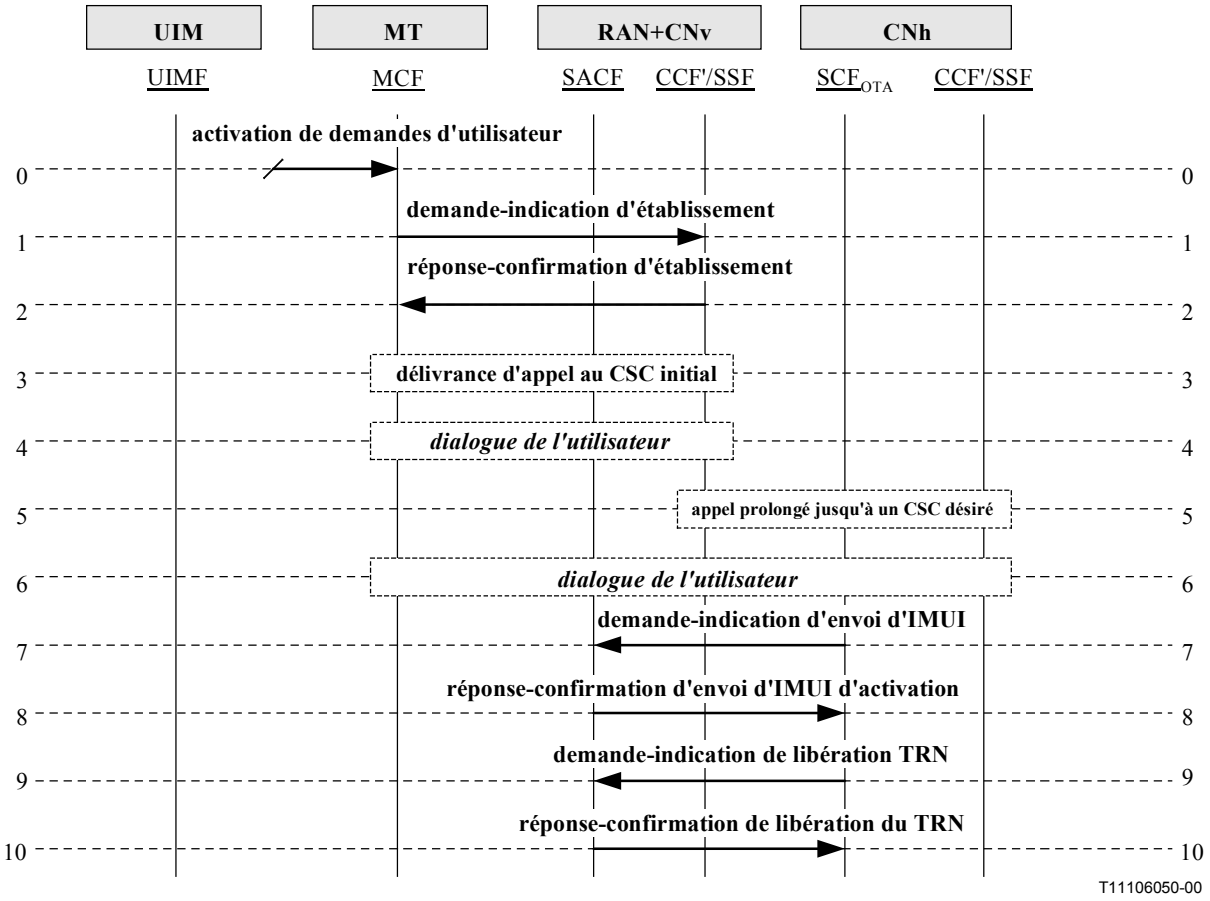


Figure 12.4-1/Q.1721 – Schéma des flux d'informations d'invocation d'activation auprès du fournisseur de service désiré

0. **Activation de demandes d'utilisateur**: le stimulus initial, lorsque l'utilisateur désire l'activation mais se trouve dans un système autre que le système du choix.

FEA0	– L'utilisateur initie la procédure en effectuant une origine d'appel OTASP, c'est-à-dire en numérotant les chiffres appropriés pour l'activation (par exemple, un numéro de code de service de fonctionnalité et un numéro de répertoire local, selon l'annonce ou les instructions d'emballage du terminal mobile). – L'entité MCF demande un canal porteur pour établir l'appel vers le CSC local.

1. **Demande-indication d'établissement**: de l'entité MCF à l'entité CCF'/SSF dans l'entité CNv. A la réception des chiffres d'origine d'appel OTASP que l'utilisateur a entré, le MCF envoie les chiffres numérotés à l'entité CCF'/SSF dans l'entité CNv.

Etablissement (réponse: succès)	demande-indication
IMUI initiale (INIT_IMUI)	M (Note)

FEA1	– En recevant la chaîne de chiffres et en reconnaissant le code de service de fonctionnalité (FSC) comme une tentative OTASP, l'entité CNv peut bipasser ou effectuer une autorisation d'accès au réseau normal ou encore une validation de l'abonné et une authentification, avant le traitement. Indépendamment du résultat de cette procédure, l'entité CNv connecte la communication vocale à un centre de service clients (CSC, *customer service centre*) local. – L'entité CCF'/SSF attribue un unique numéro de référence temporaire (TRN) pour cette session OTASP. – L'entité CNv transfère le TRN au CSC pendant l'établissement de l'appel. Noter que le TRN peut être envoyé comme numéro appelant ou numéro appelé, en fonction des schémas de signalisation utilisés. – Le CCF'/SSF accorde un canal support pour transporter l'appel.
NOTE – INIT_IMUI est l'IMUI placée dans l'UIM en usine. Sa durée de vie est courte et elle est remplacée par la nouvelle IMUI (NEW_IMUI) attribuée qui est accordée par l'entité CNh avant l'achèvement de la session OTASP.	

2. **Réponse-confirmation d'établissement**: de l'entité CCF'/SSF à l'entité MCF.

Etablissement	réponse-confirmation
Identification du support	M

FEA2	– L'entité MCF acquiert le canal support accordé et poursuit en établissant l'appel.

3. **Délivrance d'appel au CSC initial**: la connexion d'appel entre l'utilisateur et le CSC associé à l'entité CNv est effectuée.

4. **Dialogue entre l'utilisateur et CR ou la VRU du CSC initial**: un représentant du client ou une unité de réponse vocale sur le CSC de l'entité CNv entame un dialogue avec l'utilisateur.

FEA4	– Le représentant du client ou une unité de réponse vocale du CSC détermine que l'utilisateur désire avoir le terminal mobile activé sur un autre CN qui devient le CN de rattachement de l'utilisateur (CNh). – Etant donné qu'il existe un accord commercial entre l'exploitant de l'entité CNv et de l'entité CNh, le CSC initie un réacheminement d'appel vers le CSC dans l'entité CNh désirée. – Le CSC initial peut utiliser une table à consulter interne pour obtenir l'adresse du CSC désiré pour réacheminer l'appel. Aucune numérotation de numéro ne sera autorisée à l'utilisateur pour éviter toute fraude.

5. **Appel prolongé jusqu'à un CSC désiré**: le représentant du client ou une unité de réponse vocale dans le CSC obtient ainsi l'information de l'utilisateur concernant le système auquel il désire être connecté.

FEA5	– Le représentant du client du CSC ou une unité de réponse vocale étend la communication vocale à un autre CSC (sous réserve que les accords commerciaux pour un tel transfert existent), qui est associé au fournisseur de service souhaité (exploitant). – Transmet le TRN au nouveau CSC.

6. **Dialogue entre l'utilisateur et le représentant du client ou l'unité de réponse vocale du CSC désiré**: un représentant du client ou une unité de réponse vocale dans l'entité CSC désirée entame un dialogue avec l'utilisateur.

FEA6	– Le CSC contacte alors la fonctionnalité par voie hertzienne désirée pour activer la fourniture de service via le SCF_{OTA}.

7. **Demande-indication d'envoi d'IMUI**: du SCF_{OTA} dans le réseau de rattachement au SACF dans le réseau visité. Le représentant du CSC fait initier ce flux par le SCF_{OTA}. L'entité CNh est capable de déterminer l'adresse de routage de l'entité CNv provenant du TRN précédemment fourni. Ce flux demande à l'entité SACF d'attacher à l'entité CNh pour cette session OTASP. L'entité CNh attribue également une IMUI "d'activation" à utiliser uniquement pendant cette session OTASP.

Envoi de l'IMUI d'activation (réponse: succès)	**demande-indication**
IMUI d'activation (ACT_IMUI)	M (Note 1)
Numéro de référence provisoire (TRN)	M (Note 2)
Code d'action (ACTCODE)	M (Note 3)

FEA7	– L'entité CNv associe l'appel en question avec l'entité CNh et donc une corrélation entre le trajet de la parole et le trajet de signalisation est établie.
NOTE 1 – L'ACT_IMUI est utilisée uniquement pour cette session OTASP.	
NOTE 2 – Le TRN est utilisé pour associer le CNh avec cet appel OTASP.	
NOTE 3 – L'ACTCODE commande au SACF d'attacher à ce CNh pour cet appel.	

8. **Réponse-confirmation d'envoi d'IMUI d'activation**: du SACF du réseau visité au SCF_{OTA} dans le réseau de rattachement.

Envoi de l'IMUI d'activation	réponse-confirmation
INIT_IMUI	M (Note 1)
Identité CNv (CNv ID)	M (Note 2)
Capacités d'authentification CNv (CNv_AUTHCAP)	M (Note 3)
Autorisation refusée (AUTHDEN)	O (Note 4)

FEA8	– Le CNh informe le CSC que l'attachement avec le CNv a été accompli. – Le CSC informe le CNh qu'il doit indiquer au CNv de libérer le TRN.
NOTE 1 – L'INIT_IMUI est reçue de l'UIM lors de l'établissement d'appel et est utilisée pour la génération de la clé d'authentification. NOTE 2 – L'identité CNv est nécessaire pour retourner ultérieurement les messages vers le CNv dans la procédure OTASP. NOTE 3 – Le CNv_AUTHCAP informe l'entité CNh des capacités d'authentification du CNv utilisées pour la réauthentification. NOTE 4 – Inclut l'AUTHDEN, si cet UIM s'était vu précédemment (à l'étape 2) refuser une autorisation d'accès au réseau ou a échoué dans la validation ou l'authentification de l'abonné.	

9. **Demande-indication de libération TRN**: de l'entité SCF_{OTA}dans le réseau de rattachement au SACF du réseau visité. Le représentant CSC initie ce flux par l'entité SCF_{OTA}. Etant donné que l'attachement du terminal au système désiré (CSC et CNh) s'est achevé avec succès, le TRN n'est plus nécessaire et l'entité CNh décide de libérer le TRN (ressource en principe limitée), de sorte qu'il puisse être réutilisé.

Libération du TRN (réponse: succès)	demande-indication
ACT_IMUI	M
ACTCODE	M (Note)

FEA9	– Le SACF dans l'entité CNv libère le TRN, permettant ainsi de le réutiliser pour une autre session OTASP.
NOTE – ACTCODE indique au SACF de libérer le TRN.	

10. **Réponse-confirmation de libération du TRN**: du SACF du réseau visité à l'entité SCF_{OTA} du réseau de rattachement.

Libération TRN	réponse-confirmation
Néant	(Note)

FEA10	– Le SACF accuse réception de l'instruction, après avoir libéré le TRN. – Fin de la procédure d'attachement.
NOTE – La réponse-confirmation est vide. Sa présence est suffisante pour indiquer le succès.	

12.4.2 Génération de la clé d'authentification

Avant d'activer le terminal mobile IMT-2000 de l'utilisateur, vérifier que les trajets de parole et de données ont bien été établis. Ceci est réalisé en générant des clés d'authentification identiques séparément dans le réseau (LMF) et l'UIM (UIMF), en utilisant une méthode de cryptage publique (telle que l'algorithme Diffie-Hellman; voir Appendice II pour la description). La clé

d'authentification (jamais émise sur la voie hertzienne) est alors utilisée pour produire les masques nécessaires pour établir le chiffrement de la parole et des données. Ce flux d'informations montre comment la clé d'authentification est générée pour l'OTASP IMT-2000. Voir Figure 12.4-2.

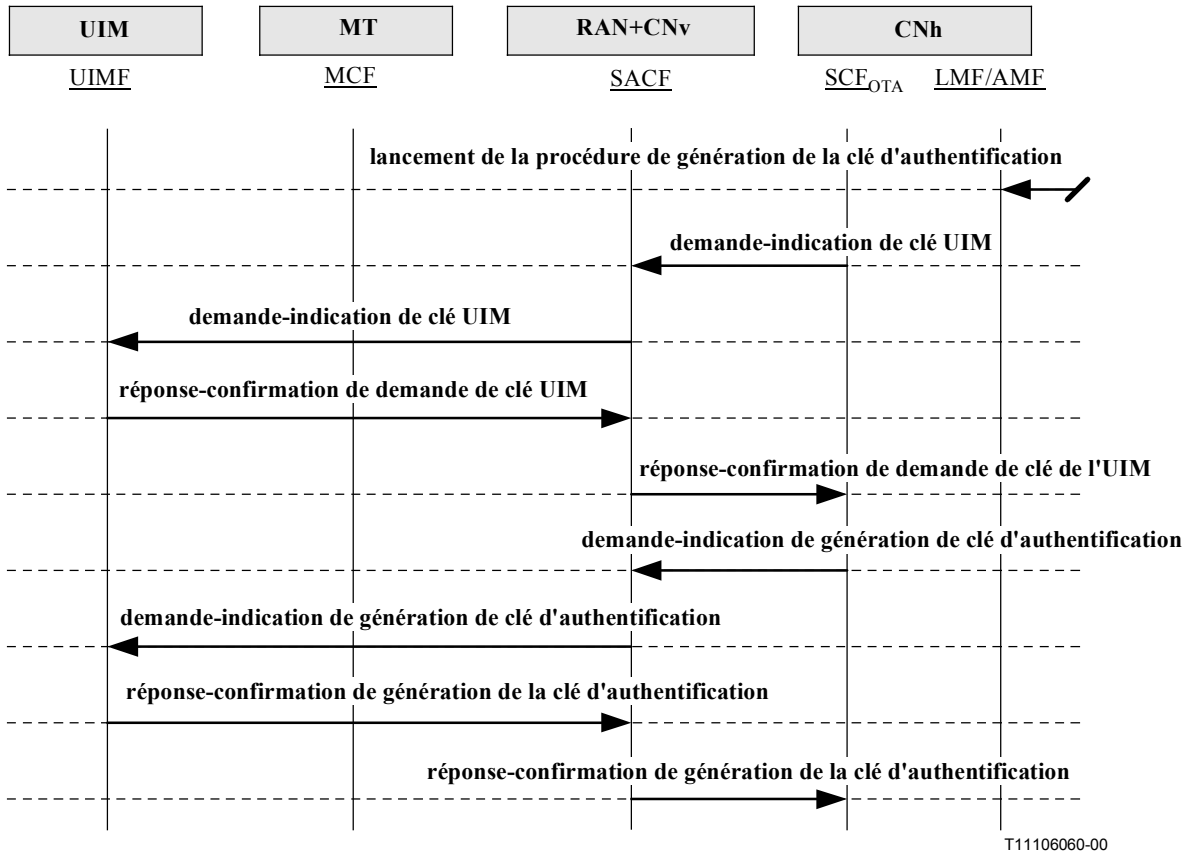


Figure 12.4-2/Q.1721 – Schéma des flux d'informations de génération de la clé d'authentification

0. **Lancement de la procédure de génération de la clé d'authentification**: est le stimulus initial, où l'entité CSC initie la procédure de génération de clé d'authentification.

FEA0	– L'entité CSC initie la procédure de génération de clé d'authentification. – La fonctionnalité par voie hertzienne envoie à l'entité LMFh une demande qui inclut la version de protocole de la clé d'authentification, correspondant aux capacités[8] de génération de clé d'authentification de l'UIM, l'IMUI de l'UIM et l'IMUI d'activation. – L'entité LMFh répond en retournant la version du protocole de la clé d'authentification qu'elle utilisera et les clés publiques appelées valeur de module (N*) et valeur primitive (g*). Cela comprend également la valeur de clé CN-Key (Y*), que la fonctionnalité par voie hertzienne stocke.

[8] Le modèle de l'algorithme de Diffie-Hellman est donné ici, dans la mesure où il fait partie du domaine public et qu'il est évolutif puisqu'il permet d'utiliser différentes combinaisons d'exposants et des valeurs de cryptage publiques (module et primitive) pour répondre au degré de sécurité désiré par l'exploitant.

1. **Demande-indication de clé UIM**: de l'entité SCF_{OTA} du réseau de rattachement au SACF du réseau visité. Le représentant CSC commande à l'entité SCF_{OTA} d'initier ce flux. Cela inclut la version du protocole de la clé d'authentification et les clés publiques. La fonctionnalité de la voie hertzienne mémorise la valeur de la clé CN et ne l'envoie pas au SACF.

Demande de clé UIM (réponse: succès)	demande-indication
Version de protocole de la clé d'authentification (AKEYPV)	M (Note)
Valeur du module (MODVAL)	M
Valeur primitive (PRIMVAL)	M

FEA1	– Le SACF dans le CNv relaie le contenu, de façon à ce qu'il puisse être envoyé par l'interface radio.
NOTE – L'indication AKEYPV fournit la version du protocole de la clé d'authentification correspondant à la combinaison spécifique de la valeur de module (N*), la valeur primitive (g*) et l'exposant (y*), que l'entité CNh (et l'UIM) utilisera, selon ce qui est souhaité par l'exploitant.	

2. **Demande-indication de clé UIM**: de l'entité SACF du réseau visité à l'UIMF via l'entité MCF. Le SACF transmet simplement le contenu reçu à l'étape 1 de la fonctionnalité de la voie hertzienne à l'UIMF.

Demande de clé UIM (réponse: succès)	demande-indication
Version de protocole de la clé d'authentification (AKEYPV)	M
Valeur de module (MODVAL)	M
Valeur primitive (PRIMVAL)	M

FEA2	– L'UIMF calcule avec succès la valeur de la clé de l'UIM (X*) en fonction des valeurs de clés publiques: MODVAL et PRIMVAL et l'exposant, comme le spécifie la version de protocole de la clé d'authentification.

3. **Réponse-confirmation de demande de clé UIM**: ce flux est établi depuis l'UIMF (via l'entité MCF) au SACF dans le réseau visité. L'UIMF calcule avec succès la valeur de clé de l'UIM et indique ce fait au SACF dans l'entité CNv.

Demande de clé UIM	réponse-confirmation
Résultat	M (Note)

FEA3	– Le SACF dans le CNv relaie le contenu à la fonctionnalité de la voie hertzienne.
NOTE – Le résultat indique que l'UIMF a calculé avec succès la valeur de la clé de l'UIM.	

4. **Réponse-confirmation de demande de clé de l'UIM**: du SACF dans le réseau visité à l'entité SCF_{OTA} dans le réseau de rattachement. Le SACF transmet simplement les contenus reçus à l'étape 3 de l'UIMF, à la fonctionnalité de la voie hertzienne.

Demande de la clé de l'UIM	réponse-confirmation
Résultat	M

FEA4	– La fonctionnalité de la voie hertzienne de l'entité CNh calcule la valeur de la clé du réseau central CN.

5. **Demande-indication de génération de clé d'authentification**: de l'entité SCF_{OTA} dans le réseau de rattachement au SACF dans le réseau visité. Le représentant du CSC fait initier ce flux par l'entité SCF_{OTA}. La fonctionnalité de la voie hertzienne inclut la valeur de la clé du CN (Y*), que la fonctionnalité de la voie hertzienne a enregistrée à l'étape 1.

Génération de la clé d'authentification (réponse: succès)	demande-indication
Valeur de clé du CN (CNKEY)	M

FEA5	– Le SACF de CNv relaie le contenu pour qu'il puisse être envoyé sur l'interface radio.

6. **Demande-indication de génération de clé d'authentification**: du SACF dans le réseau visité à l'UIMF (via l'entité MCF). Le SACF transmet simplement le contenu reçu à l'étape 5 de la fonctionnalité de la voie hertzienne à l'UIMF.

Génération de la clé d'authentification (réponse: succès)	demande-indication
CNKEY	M

FEA6	– L'UIMF calcule avec succès la clé d'authentification, en utilisant CNKEY, MODVAL et le même exposant utilisés en calculant la valeur de la clé de l'UIM.

7. **Réponse-confirmation de génération de la clé d'authentification**: de l'UIMF (via l'entité MCF) au SACF dans le réseau visité. L'UIMF a calculé avec succès la valeur de la clé d'authentification et indique ce fait au SACF dans l'entité CNv. Il envoie la valeur de la clé de l'UIM calculée au SACF, mais non la valeur de la clé d'authentification (qui n'est jamais transmise par voie hertzienne).

Génération de la clé d'authentification	réponse-confirmation
Résultat	M (Note)
Valeur de la clé UIM (UIMKEY)	M

FEA7	– Le SACF relaie le contenu à la fonctionnalité de la voie hertzienne.
NOTE – Le résultat indique que l'UIMF a calculé avec succès la valeur de clé d'authentification.	

8. **Réponse-confirmation de génération de la clé d'authentification**: ce flux est établi depuis le SACF dans le réseau visité à l'entité SCF_{OTA} dans le réseau de rattachement. Le SACF envoie simplement le contenu reçu à l'étape 7 de l'UIMF, à la fonctionnalité de la voie hertzienne.

Génération de la clé d'authentification	réponse-confirmation
Résultat	M
UIMKEY	M

FEA8	– La fonctionnalité de la voie hertzienne indique à l'entité LMFh de générer également la clé d'authentification en utilisant la clé UIMKEY, la valeur MODVAL et le même exposant utilisé à l'étape 1 pour calculer la clé CNKEY. – Ainsi l'UIM et l'entité CNh génèrent des clés d'authentification identiques.

12.4.3 Réauthentification pour le chiffrement de la parole et de la signalisation

Ce scénario décrit les paramètres de réauthentification de l'UIM dans le but de calculer et d'émettre des paramètres de cryptage à l'entité CNv. Ces paramètres sont utilisés pour invoquer respectivement le cryptage de messages de signalisation et la confidentialité des communications vocales sur l'interface hertzienne. Voir Figure 12.4-3.

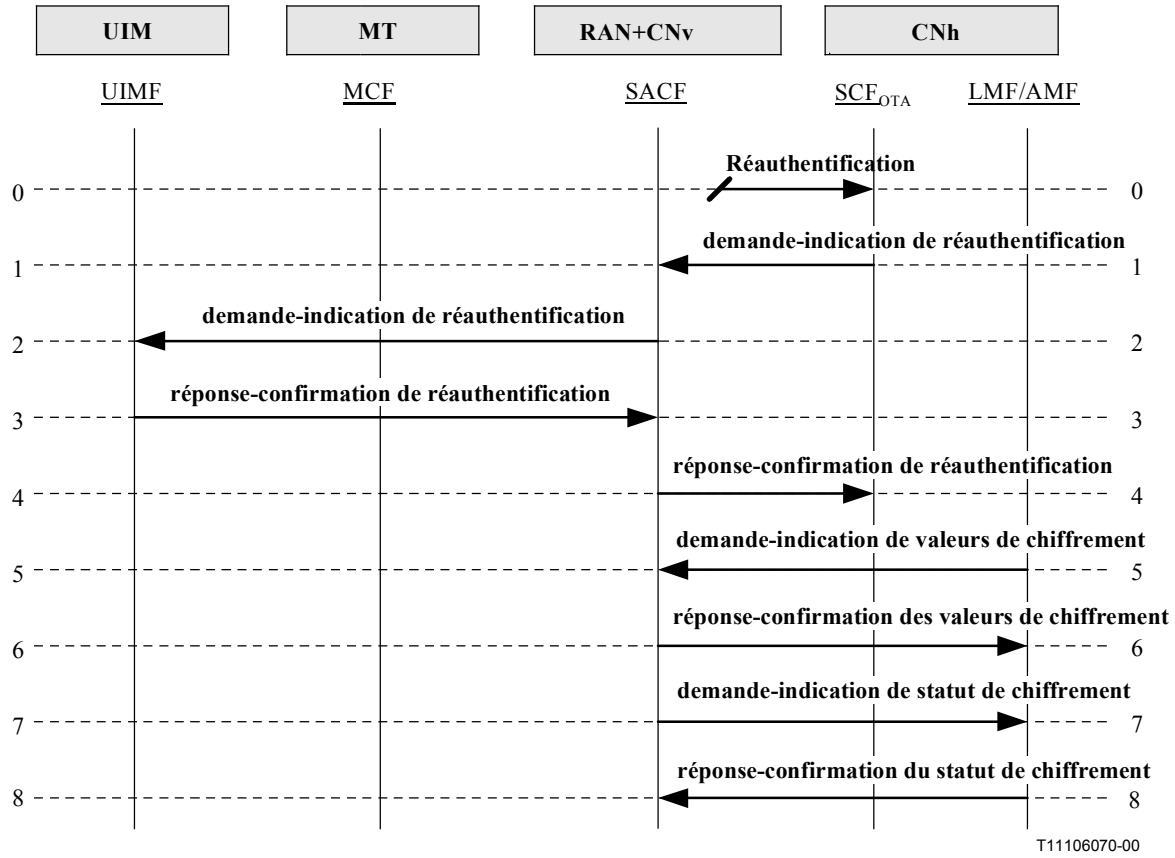


Figure 12.4-3/Q.1721 – Schéma des flux d'informations de réauthentification pour le chiffrement de la parole et de la signalisation

0. **Réauthentification**: le stimulus initial où l'entité CSC initie la procédure de réauthentification.

FEA0	– Le CSC initie la procédure de réauthentification. – Il détermine si le chiffrement est nécessaire sur l'interface radio. – La fonctionnalité de la voie hertzienne génère une valeur aléatoire de mise à l'épreuve (RAND) et l'envoie au SACF.

1. **Demande-indication de réauthentification**: établie entre l'entité SCF$_{OTA}$ dans le réseau de rattachement et le SACF dans le réseau visité. Le représentant CSC fait initier ce flux par l'entité SCF$_{OTA}$. La fonctionnalité de voie hertzienne génère une valeur aléatoire de mise à

l'épreuve (RAND, *random challenge value*) et l'envoie au SACF. L'objet est d'authentifier l'UIM (à nouveau, telle qu'elle l'a été), à la suite d'une génération de clé d'authentification pour s'assurer que c'est toujours le même UIM qui est impliqué dans la procédure OTASP avant d'activer le chiffrement.

Réauthentification (réponse: succès)	**demande-indication**
Valeur aléatoire de mise à l'épreuve (RAND)	M (Note)

FEA1	– Le SACF dans le CNv retransmet le contenu à l'UIMF via l'entité MCF.
NOTE – La valeur RAND est utilisée par l'UIMF pour répondre avec un résultat correspondant qui permettra à l'entité CNh de déterminer que l'UIM a été réauthentifiée correctement.	

2. **Demande-indication de réauthentification**: du SACF dans le réseau visité à l'UIMF (via l'entité MCF). Le SACF envoie simplement le contenu reçu à l'étape 1 de la fonctionnalité de la voie hertzienne à l'UIMF.

Réauthentification (réponse: succès)	**demande-indication**
RAND	M

FEA2	– L'UIMF calcule avec succès une réponse correspondante qui indique qu'elle a été réauthentifiée correctement.

3. **Réponse-confirmation de réauthentification**: depuis l'UIMF (via l'entité MCF) au SACF dans le réseau visité. L'UIMF effectue une réauthentification et calcule une réponse de mise à l'épreuve aléatoire correspondante (RANDC, *random challenge response*), basée sur la valeur RAND reçue, sa propre IMUI et d'autres attributs. Le calcul peut être fondé sur un algorithme compris exclusivement par l'UIMF et l'entité CNh.

Réauthentification	**réponse-confirmation**
Réponse de mise à l'épreuve aléatoire (RANDC)	M

FEA3	– Le SACF dans le CNv relaie le contenu à la fonctionnalité de la voie hertzienne via le SCF_{OTA}.

4. **Réponse-confirmation de réauthentification**: du SACF à l'entité SCF_{OTA} dans le réseau visité.

Réauthentification	**réponse-confirmation**
RANDC	M

FEA4	– La fonction hertzienne envoie les informations à l'entité LMFh, ainsi que la valeur RAND. – L'entité LMFh calcule indépendamment une valeur RANDC au moyen de l'algorithme comme à l'étape 3. – L'entité LMFh compare cette valeur à la valeur RANDC reçue. – L'entité LMFh détermine que le module UIM a été correctement réauthentifié. – L'entité LMFh entreprend ensuite la production de valeurs associées au chiffrement.

5. **Demande-indication de valeurs de chiffrement**: de l'entité LMFh dans le réseau de rattachement à l'unité SACF dans le réseau visité. Après avoir déterminé que l'UIM a été correctement réauthentifié, l'entité LMFh calcule les valeurs de chiffrement et les envoie au SACF.

Valeurs de chiffrement (réponse: succès)	demande-indication
Identité CNv (CNv ID)	M (Note 1)
Clé de chiffrement du plan de commande (CPCKEY)	M (Note 2)
Clé de chiffrement du plan utilisateur (UPCKEY)	M (Note 3)

FEA5	– Le SACF dans le CNv utilise les clés CPCKEY et UPCKEY pour activer le chiffrement.
NOTE 1 – L'identité CNv est utilisée pour router la demande-indication de valeurs de chiffrement au SACF correct. NOTE 2 – Cette clé est utilisée pour activer le chiffrement de l'information des niveaux de contrôle, tels que les messages de signalisation. NOTE 3 – Cette clé est utilisée pour activer le chiffrement de l'information du plan utilisateur, tel que la parole.	

6. **Réponse-confirmation des valeurs de chiffrement**: du SACF dans le réseau visité à l'entité LMFh dans le réseau de rattachement.

Valeurs de chiffrement	réponse-confirmation
Aucune	(Note)

FEA6	L'entité LMFh dans le CNh a une indication que les valeurs de chiffrement ont atteint avec succès le SACF.
NOTE – La réponse-confirmation est vide. Sa présence est suffisante pour indiquer le succès.	

7. **Demande-indication de statut de chiffrement**: ce flux est établi depuis le SACF dans le réseau visité à l'entité LMFh dans le réseau de rattachement. Le chiffrement du plan utilisateur (parole) ou le chiffrement du plan de commande (messages de signalisation) ou les deux sont activés par l'interface radio.

Statut du chiffrement (réponse: succès)	demande-indication
Rapport de chiffrement du plan de contrôle (CPCRPT)	M (Note 1)
Rapport de chiffrement du plan utilisateur (UPCRPT)	M (Note 2)

FEA7	– L'entité LMFh dans le CNh a une information concernant le statut actuel du chiffrement sur l'interface radio.
NOTE 1 – Indique si le chiffrement du plan de commande a été activé. NOTE 2 – Indique si le chiffrement du plan utilisateur a été activé.	

8. **Réponse-confirmation du statut de chiffrement**: ce flux est établi depuis le SACF dans le réseau visité à l'entité LMFh dans le réseau de rattachement. L'entité LMFh envoie cette information à la fonctionnalité de la voie hertzienne qui indique alors au représentant du CSC dans le CNh si les données utilisateur sensibles peuvent être échangées en toute sécurité sur la voie hertzienne.

Statut de chiffrement	réponse-confirmation
Néant	(Note)

FEA8	– L'entité LMFh dans le CNh envoie cette information à la fonctionnalité de la voie hertzienne. – Ceci indique au CSC si les données peuvent être échangées en toute sécurité sur la voie hertzienne. – Le CSC et l'abonné échangent alors des informations sensibles (financières, etc.). – Fin du processus de réauthentification.
NOTE – La réponse-confirmation est vide. Sa présence est suffisante pour indiquer le succès.	

12.4.4 Transfert de données OTASP

Ce scénario décrit l'échange de messages de données OTASP qui transportent les informations liées à l'activation, entre la fonctionnalité de la voie hertzienne dans l'entité CNh et l'UIMF via le MCF et le SACF dans le CNv. Cette opération est réalisée généralement après l'activation du chiffrement. Voir Figure 12.4-4.

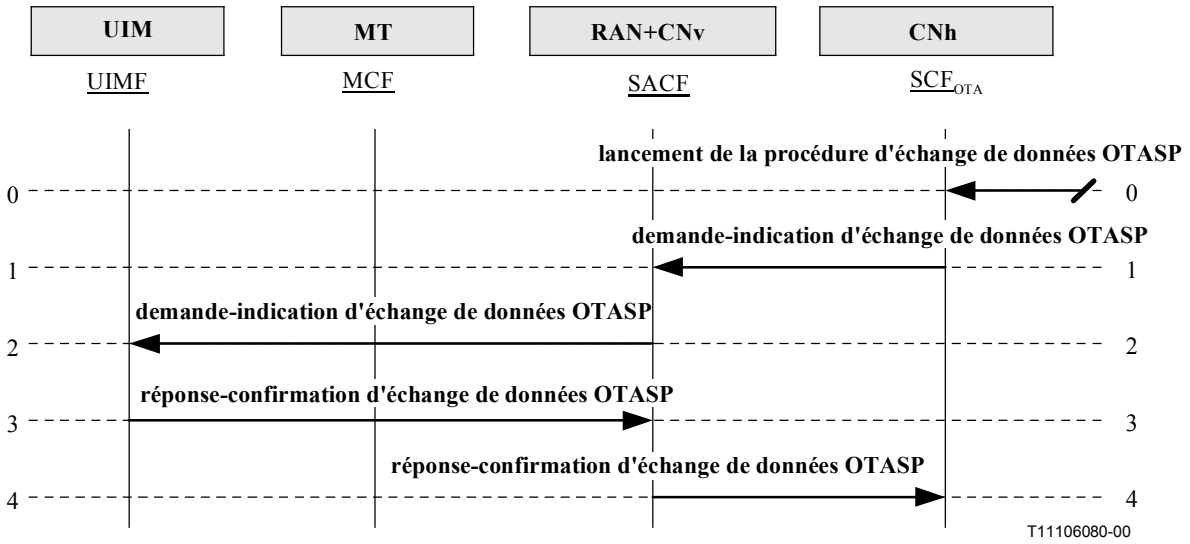


Figure 12.4-4/Q.1721 – Schéma des flux d'informations d'échange de données OTASP

0. **Lancement de la procédure d'échange de données OTASP**: le stimulus initial où le représentant CSC indique à l'entité SCF_{OTA} d'initier la procédure d'échange de données OTASP.

FEA0	– Le CSC initie le processus d'échange de données OTASP. – Après avoir confirmé que le chiffrement est présent sur l'interface radio, il demande à la fonctionnalité par voie hertzienne d'envoyer les données OTASP au SACF dans le CNv. – Ceci inclut la nouvelle IMUI attribuée destinée à être téléchargée dans l'UIMF et d'autres informations liées aux services complémentaires.

1. **Demande-indication d'échange de données OTASP**: de l'entité SCF_{OTA} dans le réseau de rattachement au SACF dans le réseau visité.

Echange de données OTASP (réponse: succès)	demande-indication
IMUI (NEW_IMUI) nouvellement attribué	M (Note 1)
ACTCODE	M (Note 2)

FEA1	– Le SACF dans le CNv relaie le contenu à l'UIMF via le MCF. – Le SACF libère également d'autres ressources lorsque la session OTASP est terminée.
NOTE 1 – La NEW_IMUI est l'identité permanente attribuée et installée dans l'UIM utilisateur. NOTE 2 – En fonction de l'échange de données, l'ACTCODE peut demander selon le cas: – au SACF d'envoyer la NEW_IMUI à l'UIMF; – à l'UIMF d'installer la NEW_IMUI dans sa mémoire permanente; – à l'UIM de réenregistrer l'utilisateur après que la NEW_IMUI a été installée dans sa mémoire permanente; – au SACF et l'UIMF de libérer des ressources après avoir achevé les tâches OTASP.	

2. **Demande-indication d'échange de données OTASP**: ce flux est établi depuis le SACF dans le réseau visité à l'UIMF (via le MCF).

Echange de données OTASP (réponse: succès)	demande-indication
IMUI (NEW_IMUI) nouvellement attribuée	M

FEA2	– L'UIMF remplace l'ACT_IMUI par la NEW_IMUI. – Il enregistre la NEW_IMUI dans la mémoire permanente. – Il utilise la procédure d'enregistrement de terminal (TRP, *terminal registration procedure*) pour réenregistrer l'utilisateur.

3. **Réponse-confirmation d'échange de données OTASP**: ce flux est établi depuis l'UIMF (via le MCF) au SACF dans le réseau visité.

Echange de données OTASP	réponse-confirmation
Néant	(Note)

FEA3	– Le SACF envoie la réponse-confirmation d'échange de données OTASP à la fonctionnalité de la voie hertzienne.
NOTE – La réponse-confirmation est vide. Sa présence est suffisante pour indiquer le succès.	

4. **Réponse-confirmation d'échange de données OTASP**: ce flux est établi depuis le SACF dans le réseau visité à l'entité SCF_{OTA} dans le réseau de rattachement.

Echange de données OTASP	réponse-confirmation
Néant	(Note)

FEA4	– La fonctionnalité de voie hertzienne informe le CSC que l'échange de données OTASP s'est terminé avec succès.
NOTE – La réponse-confirmation est vide. Sa présence est suffisante pour indiquer le succès. Ceci termine avec succès la session OTASP. A ce stade, le terminal mobile et l'UIM sont activés et l'abonné peut recevoir le service.	

13 Définitions des éléments d'information

13.1 code d'action (ACTCODE): spécifie la nature de l'action à effectuer par l'entité fonctionnelle désignée. Par exemple, dans l'OTASP, le code d'action est utilisé par le SCF sans le réseau de rattachement pour ordonner au SACF dans le réseau de rattachement d'effectuer les opérations suivantes:

– attacher au réseau de rattachement pendant une session OTASP particulière;

– libérer un TRN, permettant ainsi de réutiliser le TRN pour une autre session OTASP;

– envoie l'IMUI nouvellement attribuée à l'UIM;

– stocke la nouvelle IMUI dans la mémoire permanente de l'UIM;

– réenregistre l'utilisateur après que la nouvelle IMUI a été stockée dans l'UIM;

– libère les ressources au niveau du CNv à la fin de la session OTASP.

13.2 IMUI d'activation (ACT_IMUI): l'IMUI temporaire attribuée par l'entité SCF dans le réseau de rattachement qui est uniquement utilisée pour la durée d'une session OTASP particulière. Elle est finalement remplacée par la nouvelle IMUI attribuée.

13.3 raison d'alerte: indique la raison pour laquelle le centre de service de messages est alerté. Elle peut prendre l'une des valeurs suivantes:

– terminal mobile présent,

– mémoire disponible.

13.4 schéma d'alerte: une indication qui peut être utilisée par le terminal mobile pour alerter l'utilisateur d'une manière spécifique en cas de trafic à destination du mobile (appel commuté ou données complémentaires non structurées). Cette indication peut être un niveau d'alerte ou une catégorie d'alerte.

13.5 autorisation refusée (AUTHDEN): indique qu'un UIM a eu un refus d'autorisation d'accès ou un échec de validation et d'authentification de l'abonné.

13.6 clé d'authentification (A-Key): valeur liée à la sécurité dans le chiffrement de message de parole/données et signalisation. Cette clé n'est jamais envoyée sur l'interface radio. Elle peut être établie au niveau du CNh et de l'UIM par les procédures OTASP ou peut être programmée dans l'UIM par des méthodes spécifiées par le fournisseur de services.

13.7 version du protocole de la clé d'authentification (AKEYPV): indique la combinaison spécifique (telle qu'elle est demandée par l'exploitant de rattachement) de la valeur de module "N," la valeur primitive "g", et l'exposant "y", que le CNh et l'UIM utiliseront pendant un processus de génération de clé d'authentification OTASP (voir Appendice II).

13.8 AUTHBS: une réponse d'authentification générée par le réseau en réponse à une mise à l'épreuve aléatoire envoyée par l'UIM lors d'une procédure de "mise à jour de SSD".

13.9 AUTH_R: une réponse d'authentification à une mise à l'épreuve globale basée SSD.

13.10 AUTH_U: une réponse d'authentification à une mise à l'épreuve unique basée SSD.

13.11 capacité support: indique la fourniture d'un service support RNIS demandé au réseau. (Voir la Recommandation UIT-T Q.931 [10].)

13.12 identificateur de support: est utilisé pour spécifier le support (par exemple, numéro de canal).

13.13 identificateur de facturation: est utilisé pour identifier le plan de tarification (tarif, titulaire de compte, etc.) associé à l'appel.

13.14 numéro appelé: identifie l'appelé d'un appel. (Voir Recommandation UIT-T Q.931[10].)

13.15 historique de compte d'appel (CHCNT): compteur contenu et mis à jour dans le réseau et l'UIM. Ce compteur peut être mis à jour par le réseau de rattachement ou le réseau visité et sert de détecteur d'éventuels UIM "clonés".

13.16 identité d'appel: indique l'identité d'un appel dans un point de transfert de signalisation.

13.17 numéro appelant: identifie l'origine d'un appel. (Voir Recommandation UIT-T Q.931 [10].)

13.18 identité de l'abonné demandeur: identifie le demandeur d'un appel.

13.19 catégorie: fournit une indication d'une matière spécifique (par exemple, urgence, annonce de l'exploitant du système, nouvelles, publicité, sports, etc.) transportée dans la charge utile *(payload)* envoyée à un ou plusieurs utilisateurs (par exemple, SMS ou messagerie de diffusion de téléservices).

13.20 mise à l'épreuve (ou RANDU): une mise à l'épreuve aléatoire unique générée par le réseau pour authentifier l'UIM.

13.21 réponse de mise à l'épreuve: une réponse d'authentification calculée par l'UIM à la mise à l'épreuve aléatoire unique initiée par le réseau. Egalement connue sous le nom de SRES (signature de résultat) dans certains systèmes.

13.22 valeur de réponse de mise à l'épreuve: valeur générée par le terminal mobile (PSCAF) utilisant la valeur de mise à l'épreuve et les données secrètes qu'elle partage avec son réseau de rattachement (LMFp/AMFp).

13.23 valeur de mise à l'épreuve: valeur aléatoire générée par le réseau visité utilisée pour l'authentification du terminal mobile visité.

13.24 clé(s) de chiffrement: clé(s) secrète(s) pour le chiffrement du trafic de l'interface radio.

13.25 capacités d'authentification de CNv (CNv_AUTHCAP): fournit des informations concernant des capacités d'authentification du réseau serveur/réseau visité; utilisées par exemple dans la réauthentification pendant une session OTASP.

13.26 identité de CNv (CNvID): fournit l'identité du réseau serveur/réseau visité pour les besoins de routage. Par exemple, dans l'OTASP, elle est fournie par une entité CNv à l'entité CNh, de sorte que l'entité CNh peut l'utiliser plus tard pendant une session OTASP pour router les messages à l'entité CNv.

13.27 valeur de clé CN (CNKEY): nombre "Y" généré par le réseau de rattachement (c'est-à-dire dans l'entité LMFh) qui est envoyé au réseau visité et sur l'UIM pour la génération de la clé d'authentification pendant une session OTASP. Elle est calculée selon la formule:

$$Y = g^{y} \text{ Mod } N$$

13.28 confirmation de RANDG: une forme de RAND envoyée par l'entité MCF, cohérente avec les interfaces radio spécifiques.

13.29 identification de ligne connectée: identifie l'abonné connecté d'un appel.

13.30 clé de chiffrement du plan de commande (CPCKEY): contient la clé à utiliser pour le chiffrement des champs de données appropriées dans les messages de signalisation envoyés dans les deux directions de l'interface radio. Elle est calculée au niveau de l'entité CNh. Sa présence indique également au réseau serveur/réseau visité d'activer le chiffrement du plan de commande.

13.31 rapport de chiffrement du plan de commande (CPCRPT): ce rapport est envoyé par un réseau serveur/visité au réseau de rattachement pour indiquer si le chiffrement du plan de commande a été ou non activé.

13.32 mot de passe courant: le mot de passe utilisé par un utilisateur pour la commande de services complémentaires.

13.33 durée de vie de session de données: la durée allouée à la connexion au tunnel d'une session de données. Cette durée est déterminée et étendue par la PSCAF lors de la demande d'établissement d'une nouvelle session de données. Une connexion au tunnel est supprimée lorsque sa durée de vie expire.

13.34 données utilisateur supprimées: décrit les données de profil de l'utilisateur à supprimer dans les procédures de gestion de données de l'abonné. Elles peuvent comprendre les données suivantes:

– une liste des services de base;

– une liste des services complémentaires (sous la forme de codes complémentaires);

– données de services complémentaires;

– données d'abonnement VHE;

– diffusion et/ou données d'abonnement d'appel de groupe.

13.35 méthode d'encapsulage: un schéma du plan utilisateur pour empêcher la livraison hors séquence d'unités de paquets de l'utilisateur sur la connexion au tunnel. Le choix de la méthode d'encapsulage est suggéré par la fonction PSACF lors de l'envoi d'une demande d'établissement/rétablissement d'une session de données au LMFp du réseau visité.

13.36 référence de point final (point): le numéro/l'adresse de routage de l'utilisateur (c'est-à-dire, ITDN), l'abonné à ajouter ou supprimer dans un appel multipartite.

13.37 qualité attendue: cet élément d'information est utilisé pour rapporter la qualité attendue d'un support radio que le réseau peut allouer au terminal mobile basé sur le résultat de mesure.

13.38 information de fonctionnalité: code de fonctionnalité, capacités du système visité, action en cours du système visité.

13.39 informations guide: se réfère aux informations guide données à un utilisateur à qui il est demandé de fournir une commande de service complémentaire par mot de passe. Les informations suivantes peuvent être données:

– "entrer mot de passe": ce message est utilisé pour demander à l'utilisateur son mot de passe courant;

– "entrer nouveau mot de passe": ce message est utilisé pour demander à l'utilisateur un nouveau mot de passe pendant l'enregistrement d'un nouveau mot de passe;

– "entrer de nouveau mot de passe": ce message est utilisé pour demander à l'utilisateur d'entrer à nouveau le nouveau mot de passe.

13.40 compatibilité de la couche supérieure: fournit un moyen pour l'utilisateur disant de vérifier la compatibilité. (Voir Recommandation UIT-T Q.931 [10].)

13.41 adresse LMFh: adresse pouvant être routée à la fonction de gestion d'emplacement de rattachement, par exemple, le numéro RNIS du HLR.

13.42 numéro de répertoire mobile IMT-2000 (IMDN): un numéro composable qui identifie de façon unique un utilisateur IMT-2000 et qui est utilisé pour effectuer, envoyer un appel à cet utilisateur ou pour identifier un utilisateur au moment de l'origine de l'appel.

NOTE – Le numéro RNIS E.164 MS peut être appliqué à cet effet.

13.43 identité d'utilisateur mobile international (IMUI): identité utilisée pour adresser un terminal mobile et identifier l'utilisateur mobile de façon unique auprès d'une fonction de fourniture de services.

13.44 capacité de transfert d'information: indique le type de capacité support demandé par l'appelant (par exemple, communication vocale). (Voir Recommandation UIT-T Q.931 [10].)

13.45 numéro de répertoire temporaire international (ITDN): un numéro E.164 qui porte un numéro pouvant être composé et acheminé, qu'un abonné appelé se voit attribuer dans et par un système visité pour une durée courte pour faciliter le routage d'appel alors qu'il se déplace globalement.

13.46 IMUI initiale (INIT_IMUI): l'IMUI d'origine qui est placée dans l'UIM au moment de la fabrication et qui est utilisée pendant le processus de génération de clé d'authentification OTASP. Sa durée de vie est courte car elle est remplacée par la nouvelle IMUI attribuée par le réseau de rattachement avant la conclusion d'une session OTASP.

13.47 niveau d'interférence: cet élément d'information est utilisé pour rapporter le niveau d'interférence en tant que partie d'un rapport de mesure.

13.48 adresse IP (X): adresse IP de l'entité X (par exemple, PSCAF, PSCF, et PSGCF). Cette adresse est utilisée dans le point de terminaison du tunnel.

13.49 identité de zone d'emplacement (LAI): identifie la zone dans laquelle le terminal mobile est situé dans le réseau visité.

13.50 adresse LMFv: une adresse pouvant être routée à la fonction de gestion de l'emplacement visité, par exemple, le numéro RNIS du VLR.

13.51 information d'emplacement: indique la position d'un utilisateur mobile aussi précisément que possible avec les informations disponibles. Ces informations peuvent par exemple être l'identité d'une cellule, l'identité d'une zone d'emplacement, l'adresse VLR ou des informations géographiques.

13.52 compatibilité de couches inférieures: fournit un moyen qu'il convient d'utiliser pour la vérification de compatibilité par une entité appelée (par exemple, un utilisateur distant ou une unité en interfonctionnement ou un nœud de réseau d'une fonction de couche supérieure appelée par l'appelant). (Voir Recommandation UIT-T Q.931 [10].)

13.53 identificateur de média: utilisé pour identifier/sélectionner un type de média.

13.54 type de média: se rapporte à un médium de transport de services spécifique. Le mot média se rapporte à une série de supports alloués pour prendre en charge une diversité de services génériques tels que la parole, les données, les images et la vidéo.

13.55 condition de mesure: cet élément d'information est utilisé pour communiquer au terminal mobile la condition selon laquelle la mesure est effectuée. Des informations telles qu'un intervalle de répétition sont incluses.

13.56 message: ce paramètre contient le message SMS.

13.57 adresse de centre de messages: représente l'adresse E.164 d'un centre de messages SMS.

13.58 type de notification de message: indique la manière pour notifier l'utilisateur (par exemple, audible, visuel, vibratoire, combinaisons de ces modes ou autres).

13.59 compte de message en attente: indique le nombre de messages qui attendent d'être extraits par l'utilisateur.

13.60 priorité de message: fournit un ordre croissant, une indication du niveau de priorité (par exemple, normal, interactif, urgent, urgence) d'un message (par exemple, SMS ou diffusion de téléservices).

13.61 statut de message: fournit une indication si un message est nouveau, le remplacement ou la suppression d'un message existant (par exemple, SMS ou diffusion de téléservices) avec la même identification (voir type de message).

13.62 type de message: fournit une identification pour un message (par exemple, SMS ou diffusion de téléservices) dans un réseau serveur.

13.63 indicateur de message en attente: indique s'il s'agit d'un message qui attend ou non.

13.64 type de message en attente: indique si les messages en attente sont du type vocal, fax, e-mail ou autre.

13.65 valeur de module (MODVAL): un nombre "N" généré par le réseau de rattachement (c'est-à-dire, dans l'entité LMFh) qui est envoyé au réseau visité et sur l'UIM pour la génération de la clé d'authentification pendant une session OTASP. Sa longueur est fixée par l'exploitant (par exemple, 512 bits, 768 bits, etc.) et plus le nombre est élevé, plus la sécurité fournie pendant le processus de génération de la clé d'authentification est élevée.

13.66 MS RNIS: se réfère à un des numéros RNIS affectés à un abonné mobile conformément à la Recommandation UIT-T E.213 [8].

13.67 identificateur d'accès au réseau (NAI): chaîne qui identifie de façon unique l'entité fonctionnelle (FE), dans ce cas le PSCF.

13.68 nouvelle IMUI attribuée (New_IMUI): l'identité permanente attribuée par le réseau de rattachement (LMFh) à l'UIM d'un nouvel abonné et qui est enregistrée dans l'UIM à la fin d'une session OTASP où elle remplace l'IMUI d'activation.

13.69 nombre d'appels mesurés: cet élément d'information est utilisé pour indiquer au terminal mobile le nombre maximal de cellules environnantes sur lesquelles il convient que la mesure soit effectuée si les conditions radio le permettent.

13.70 résultat d'opération: fournit le résultat de l'opération tel qu'une opération rejetée (par exemple, opération non valide), une opération acceptée et achevée ou une opération acceptée et non achevée (par exemple, erreur).

13.71 adresse d'origine: l'adresse de l'expéditeur du message d'origine (par exemple, dans le SMS ou la diffusion de téléservices). Les formats typiques incluent les nombres en DCB, le codage IA5 et les variantes d'adresses IP.

13.72 charge utile: dans tout texte transporté (par exemple, par SMS ou diffusion de téléservices) pour l'affichage ou pour l'utilisation par une entité réceptrice. Elle n'a un sens que pour les points finaux de protocole et est interprétée par l'identificateur de téléservice.

13.73 périodicité: fournit une indication de l'heure de démarrage, la durée et le taux de répétition avec lequel un message (par exemple, SMS ou diffusion de téléservices) doit être livré à un ou des destinataires.

13.74 niveau de réception du canal pilote: cet élément d'information est utilisé pour rapporter le niveau de réception d'un canal pilote en tant que partie d'un rapport de mesure.

13.75 numéro d'identification personnel (PIN): numéro utilisé dans la vérification d'une identité revendiquée par l'utilisateur, utilisé ici pour débloquer l'UIM. Le numéro PIN est attribué par le fournisseur de services au moment de la fourniture du service.

13.76 indicateur de langue préférée: indique la langue de choix d'un destinataire d'une annonce parlée ou d'un message texte (par exemple, pour notifier à un utilisateur la présence de messages en attente qu'il faut extraire, pour envoyer un message d'accueil à un abonné itinérant, pour afficher un message court).

13.77 valeur primitive (PRIMVAL): un nombre "g" fixé par le réseau de rattachement (c'est-à-dire, dans l'entité LMFh) qui est envoyé au réseau visité et sur l'UIM pour la génération de la clé d'authentification pendant une session OTASP. Sa longueur est fixée par l'exploitant et plus le nombre est élevé, plus la sécurité fournie pendant le processus de génération de la clé d'authentification est élevée.

13.78 information de contrôle de puissance: information utilisée pour indiquer au terminal mobile le niveau de puissance initial qu'il doit régler pour le support radio alloué.

13.79 erreur de fournisseur: indique un type d'erreur lié à un protocole:

– identité d'invocation double;
– service non pris en charge;
– paramètre mal saisi;
– limitation de ressource;
– initier libération, c'est-à-dire l'homologue a déjà initié la libération du dialogue et le service doit être libéré;
– réponse inattendue de l'homologue;
– panne d'exécution de service;
– pas de réponse de l'homologue;
– réponse non valide reçue.

13.80 qualité de service (QS): la QS est utilisée pour spécifier la qualité de service requise, telle que le BER.

13.81 RANDBS: mise à l'épreuve aléatoire envoyée par l'entité MCF pour valider le réseau dans les systèmes basés SSD.

13.82 RANDG: diffusion d'une mise à l'épreuve globale (nombre aléatoire) sur le canal d'information du système. Cette mise à l'épreuve est utilisée dans les systèmes basés SSD en liaison avec la clé SSD et les autres paramètres, s'il y a lieu, pour authentifier l'utilisateur.

13.83 RANDSSD: un nombre aléatoire envoyé à l'UIM utilisé dans le processus de mise à jour de la clé SSD.

13.84 RANDU: mise à l'épreuve aléatoire unique utilisée pour authentifier l'utilisateur du terminal dans les systèmes basés SSD. (Elle peut être générée par le réseau visité lorsque le SSD est partagé.)

13.85 durée de session restante: calculée par l'entité LMFp de rattachement en utilisant la durée de vie de la session d'origine. Elle est envoyée à l'entité LMFp d'ancrage pendant une session de données.

13.86 action distante: tonalité ou annonce pour lire.

13.87 information demandée: indique le type d'information demandé, par exemple, information d'emplacement, état d'utilisateur ou les deux.

13.88 information de radiofréquence: information utilisée pour spécifier les informations de la radiofréquence allouée au terminal mobile.

13.89 information de liaison inverse: information utilisée pour spécifier l'information de liaison radio inverse qui est allouée au terminal mobile.

13.90 résultat: utilisé pour indiquer le succès ou l'échec d'une procédure demandée.

13.91 adresse d'acheminement: utilisée pour l'acheminement au réseau visité/support/de prise en charge d'arrivée.

13.92 clé de sécurité: clé générée par l'entité LMFp envoyée au terminal mobile, à l'entité PSCF visitée et à l'entité PSGCF pour la prise en charge du cryptage et l'association de sécurité entre ces entités.

13.93 indice de paramètre de sécurité: indice généré par l'entité LMFp envoyé au terminal mobile, à l'entité PSCF visitée et à l'entité PSGCF pour la prise en charge du cryptage et l'association de sécurité entre ces entités.

13.94 sélection: spécifie les données qui doivent être extraites de l'entité SDF.

13.95 information d'adresse de service: cette information est utilisée par l'entité SCF pour sélectionner l'application correcte.

13.96 discriminateur de service: indicateur utilisé par l'entité LMFp de rattachement pour déterminer la fonction PSGCF et pour indiquer au terminal mobile le réseau sur lequel se connecter (par exemple, ISP spécifique, réseau d'entreprise spécifique, accès Internet générique). Il indique également si l'accès se fait ou non de préférence par l'intermédiaire d'une entité PSGCF dans le réseau visité ou dans le réseau de rattachement.

13.97 identification de service: identifie le type de service pour lequel l'utilisateur veut s'enregistrer (les types de service possibles sont les suivants: téléphone, télécopie, videotex, données, etc.).

13.98 groupe de service: fournit des informations qui identifient les stations mobiles cible destinées à recevoir le service SMS ou le service de diffusion de téléservices. Sa forme est libre, son format est déterminé et compris uniquement par les points finaux du protocole (par exemple, pour la diffusion de téléservices, les points finaux seront le centre de messages et les mobiles).

13.99 type de service: désigne les types de services lorsque l'établissement d'une session de données en paquets est demandée (par exemple, voix et données).

13.100 identification de session: fournie par la PSCAF (lorsqu'une demande "annonce" est reçue). Elle permet de supprimer l'ambiguïté de la réponse au terminal mobile lors d'une étape ultérieure de la procédure "d'établissement/rétablissement d'une session de données". Les identifications sont uniques pour chaque session de données en paquets dans un environnement de sessions multiples.

13.101 adresse source de session: dans le cas de sessions multiples, désigne les informations d'adresse d'une session (c'est-à-dire, l'identification de la session), utilisée pour associer le signal de réponse de "désenregistrement" à la session à terminer.

13.102 données SS: contient des informations supplémentaires liées à l'invocation de services complémentaires. En fonction du service invoqué, les données SS peuvent contenir les informations suivantes:

– une liste avec tous les numéros des abonnés appelés impliqués;

– le numéro de l'appelé impliqué.

13.103 données secrètes partagées (SSD): une valeur dérivée de la clé d'authentification utilisée pour authentifier l'abonné dans les environnements de "rattachement" et "itinérants", dans les systèmes SSD. La clé SSD est divisée en deux sous-ensembles distincts, SSD-A et SSD-B, utilisés respectivement pour la réponse d'authentification et la génération de la clé de chiffrement.

13.104 événement SS: indique le service complémentaire pour lequel une notification d'invocation est envoyée vers le SCF. Peut indiquer l'un des services suivants:

– transfert d'appel explicite;

– détournement d'appel;

– appel multiparticipants.

13.105 code SS: indique un service complémentaire ou un ensemble de services complémentaires.

13.106 données SS: un élément d'information général incluant des données utilisées par différents services complémentaires, par exemple, information d'envoi d'appel ou information d'interdiction d'appel.

13.107 identificateur du CCF cible: est utilisé pour indiquer le CCF dans lequel le support d'accès doit être établi.

13.108 informations TC: désigne les informations de capacité du terminal qui déterminent les services que le terminal peut prendre en charge.

13.109 type de téléservice: désigne des services tels que messagerie, parole, télécopie, radiorecherche, etc.

13.110 numéro de référence temporaire (TRN): est attribué par le SCF dans le réseau de rattachement et est utilisé pour corréler la connexion vocale (entre le mobile de l'utilisateur et le centre de service clients) avec la connexion de données (entre le réseau serveur et le réseau de rattachement), pendant une session OTASP.

13.111 statut de terminal: identifie le statut d'un terminal mobile et son utilisateur (c'est-à-dire, terminal mobile actif ou inactif, service accordé, interdiction déterminée par l'exploitant, etc.).

13.112 informations de traitement de terminaison: utilisées pour fournir des informations concernant le mode de traitement d'une tentative de terminaison particulière (par exemple, répondre à une radiorecherche).

13.113 demande de traitement de terminaison: utilisée pour demander comment traiter une tentative de terminaison donnée (par exemple, répondre ou non à une radiorecherche).

13.114 identité temporaire de mobile (TMUI): identité utilisée pour l'adresse d'un terminal mobile et pour identifier un utilisateur IMT-2000. Elle est allouée et utilisée par le réseau visité temporairement pour préserver l'anonymat.

13.115 identité de la source d'attribution de la TMUI: identité utilisée pour identifier une entité LMFv qui a attribué la TMUI.

13.116 temporisateur d'expiration de la TMUI: temporisateur utilisé avec la TMUI pour fournir une confidentialité améliorée de l'utilisateur.

13.117 sélection de réseau de transit: indique le ou les réseaux de transit demandés pour être utilisés dans l'appel. (Voir Recommandation UIT-T Q.762 [11].)

13.118 demande d'information UIM: désigne les informations demandées à l'UIM pour fournir les données suivantes:

– numéro appelé associé au numéro abrégé;
– informations spécifiques associées à l'authentification;
– informations spécifiques associées à l'abonné;
– informations spécifiques associées à l'adresse.

13.119 réponse d'information UIM: contient les informations UIM demandées.

13.120 valeur de la clé UIM (UIMKEY): un nombre "X" généré par l'UIM et envoyé au réseau de rattachement (c'est-à-dire, dans l'entité LMFh), via le réseau visité pendant un processus de génération de clé d'authentification OTASP. Ce nombre est calculé comme suit:

$$X = g^x \text{ Mod } N$$

13.121 erreur utilisateur: indique qu'une erreur s'est produite pendant le traitement d'un service de message court.

13.122 taux d'information utilisateur: ce taux est utilisé pour indiquer le taux d'information réel qui est transmis sur le support radio et le canal terrestre. Il peut également indiquer l'adaptation de taux lorsque le taux d'information utilisateur et la capacité du support radio ne sont pas les mêmes.

13.123 clé de chiffrement de plan utilisateur (UPCKEY): contient la clé utilisée pour le chiffrement de la parole/des données envoyées dans les deux directions sur l'interface radio. Sa présence indique également au réseau serveur/visité d'activer le chiffrement du plan utilisateur.

13.124 rapport de chiffrement de plan utilisateur (UPCRPT): ce rapport est envoyé par un réseau visité/serveur à un réseau de rattachement pour indiquer si le chiffrement du plan utilisateur a été ou non activé.

13.125 profil utilisateur: désigne les données qui spécifient les services souscrits et les données liées à l'authentification pour l'utilisateur IMT-2000. De plus, le profil utilisateur peut comprendre les attributs suivants:

– données d'abonnement d'appel de diffusion et/ou de groupe (s'il y a lieu);
– numéro de répertoire mobile IMT-2000 (IMDN), par exemple, un numéro composable;
– identité de l'utilisateur mobile IMT-2000 (IMUI);
– identité de l'utilisateur mobile temporaire IMT-2000 (TMUI);
– état du terminal;
– informations d'emplacement utilisateur/terminal;
– données de service de base (par exemple, services supports de base);
– téléservices (par exemple données d'abonnement d'appel de diffusion et/ou de groupe);
– données de services complémentaires;
– fonctionnalités/services déterminés par l'exploitant (par exemple, données d'interdiction d'appel);
– fonctionnalités/services déterminés par l'abonné (par exemple, données de filtrage d'appel);
– données de restriction d'itinérance;
– données d'abonnement régional;
– données d'abonnement VHE.

13.126 schéma de codage de données USSD: contient les informations de l'alphabet et de la langue utilisée pour les informations non structurées dans une opération de données de service complémentaire non structuré.

13.127 chaîne USSD: contient une chaîne d'informations non structurées dans une opération de données de service complémentaire non structuré. L'utilisateur mobile ou le réseau envoie la chaîne.

13.128 identificateur de zone: fournit une indication de la zone géographique (par exemple, RAN complets ou parties de RAN dans un réseau serveur ou la totalité du réseau serveur) sur laquelle un message doit être diffusé, comme dans le cas d'une messagerie de téléservices. Sa forme est libre, son format est déterminé et compris uniquement par les points finaux du protocole (par exemple, pour la diffusion de téléservices, les points finaux seront le centre de messages et le réseau serveur).

ANNEXE A

Liste des modules de procédure communs utilisés dans la présente Recommandation

Nom de la procédure commune	Paragraphe n°	Procédure utilisée dans
Calcul d'authentification	6.1.2.2.3	Authentification de l'utilisateur
Libération d'appel	7.5	Suppression d'un correspondant (initié par un correspondant racine et initié par un correspondant feuille)
Routage d'appel	7.3	VHE "Commande de rattachement directe", ajout d'un correspondant (initié par un correspondant racine)
Obtention du mot de passe	11.1	Enregistrement du mot de passe
Extraction de l'identité de l'utilisateur IMT-2000	6.2.2	Mise à jour d'emplacement du terminal

Nom de la procédure commune	Paragraphe n°	Procédure utilisée dans
Mise à jour de la LAI	6.2.2.1.5	Enregistrement d'emplacement de terminal, mise à jour d'emplacement du terminal
Mise à jour d'emplacement		Enregistrement d'emplacement de terminal
Libération d'appel mobile	7.5	Suppression de correspondant
Appel mobile entrant	7.4	Ajout de correspondant
Assistance de ressource spécialisée	Procédure RI	VHE "Commande directe de rattachement"
Activation du chiffrement	6.1.2.5	Enregistrement d'emplacement de terminal, mise à jour d'emplacement du terminal, appel mobile sortant initial, appel mobile entrant initial, message court envoyé par le mobile, message court à destination du mobile
Transfert de profil de l'abonné	6.2.1.3	Restauration des données LMF
Enregistrement d'emplacement de terminal	6.2.3.1	Appel mobile sortant initial, session de données en paquets
Radiorecherche du terminal	7.2	Appel mobile entrant initial, message court à destination du mobile
Attribution de la TMUI	6.1.2.6	Enregistrement d'emplacement de terminal, mise à jour d'emplacement du terminal, appel mobile sortant initial, appel mobile entrant initial
Demande de TMUI	6.2.2.1.1	Mise à jour d'emplacement du terminal, détachement, radiorecherche du terminal, attachement
Mise à jour de la TMUI	6.2.2.1.4	Attribution de la TMUI
Authentification de l'utilisateur	6.1.2	Enregistrement d'emplacement de terminal, mise à jour d'emplacement du terminal, détachement, appel mobile sortant initial, appel mobile entrant initial, message court envoyé par le mobile, message court à destination du mobile, attachement
Extraction de l'identité de l'utilisateur	6.2.2.2	Enregistrement d'emplacement de terminal, détachement, attachement
Demande d'informations sur l'utilisateur	6.2.1.2	Demande d'informations sur l'utilisateur, message court à destination du mobile
Invocation de service VHE	9	Appel mobile sortant initial, routage d'appel, appel mobile entrant initial

APPENDICE I

Q.1721 Couverture du Tableau 1/Q.1701, Exigences de l'ensemble de capacités 1 (CS-1)

Le présent appendice utilise le Tableau 1/Q.1701 copié in extenso de la Recommandation Q.1701. Une troisième colonne est ajoutée pour indiquer si la Recommandation Q.1721 couvre la capacité identifiée.

Il convient d'interpréter les entrées de la troisième colonne comme suit:

Entrée	Interprétation
Non applicable	Cette capacité est celle d'un type pour lequel aucun flux d'informations spécifique ne lui est associée.
Oui	Cette capacité est prise en charge par le flux d'informations décrit dans le paragraphe indiqué.
Non	Cette capacité n'est pas prise en charge par le flux d'informations de la Recommandation Q.1721. Les raisons sont indiquées.
Partiel	Cette capacité est partiellement supportée par le flux d'informations décrit dans le paragraphe indiqué. Les aspects non pris en charge sont indiqués avec les raisons.

Tableau I.1/Q.1701 – Ensemble de capacités 1 pour les IMT-2000

Catégorie	Capacités	Couverture
A) Capacité existante	1 Capacités et services fixes et mobiles essentiels existants de la deuxième génération largement utilisés, éventuellement améliorés	1 Non applicable
B) Objectifs à long terme	1 Prise en charge de capacités de réseau qui apportent une amélioration nette par rapport aux capacités des réseaux hertziens 2G (de la deuxième génération) largement utilisées, dans les domaines de la téléphonie, de la transmission de données, de la messagerie, de la transmission d'image et du multimédia, notamment: 1.1 Mobilité améliorée 1.2 Débits plus élevés 1.3 Services par voie hertzienne Internet et multimédias	1 Non applicable. Les capacités nécessaires pour prendre en charge ces améliorations sont traitées plus loin dans ce tableau
C) Capacité support	1 Pour l'accès de Terre: 1.1 Au moins 144 kbit/s dans un environnement radioélectrique de type véhicule, BER $\leq 10^{-6}$, pour les services en mode circuit et pour les services en mode paquet 1.2 Au moins 384 kbit/s dans un environnement radioélectrique de type extérieur vers intérieur et dans un environnement radioélectrique de type piéton, BER $\leq 10^{-6}$, pour les services en mode circuit et pour les services en mode paquet	1 Oui. Sous-paragraphe 7.1

Tableau I.1/Q.1701 – Ensemble de capacités 1 pour les IMT-2000 *(suite)*

Catégorie	Capacités	Couverture
	1.3 Au moins 2048 kbit/s dans un environnement radioélectrique de type intérieur de bureaux, BER ≤ 10^{-6}, pour les services en mode circuit et pour les services en mode paquet	
	2 Intervalle de qualité de service avec négociation indépendante:	2 Oui. Sous-paragraphe 7.1
	2.1 En temps réel/pas en temps réel	
	2.2 Caractéristiques de temps de transmission	
	2.3 Taux d'erreurs binaires maximal acceptable	
	2.4 Débit	
	3 Prise en charge de services en mode paquet (à l'interface radioélectrique et aux interfaces fixes).	3 Oui. Sous-paragraphe 8.4
	4 Pour l'interface d'accès par satellite:	4 Oui. Sous-paragraphe 7.1
	4.1 Le débit de transmission d'un utilisateur quelconque de la composante satellite des IMT-2000 pourra aller de 9,6 kbit/s à 144 kbit/s selon les conditions d'exploitation et le type de terminal de repli	
	5 Configurations de communication:	5 Oui. Paragraphes 7 et 8
	5.1 PTP: service point à point bidirectionnel (connexion de type 1)	
	5.2 PTM: service point à multipoint (connexion de type 2)	
	5.2.1 Diffusion générale	
	5.2.2 Capacités de multidiffusion	
	5.2.2.1 Préassignées, c'est-à-dire racine sélectionnée à l'établissement de l'appel	
	6 Types de communication:	6 Oui. Capacité support
	6.1 CLNS: service de réseau en mode sans connexion	
	6.2 CONS: service de réseau en mode connexion	
	7 Symétrie des liaisons d'accès:	7 Oui. Capacité support
	7.1 Symétriques (débits égaux sur la liaison montante et sur la liaison descendante)	
	7.2 Asymétriques (débits différents sur la liaison montante et sur la liaison descendante)	
	8 Trafic à débit fixe ou variable	8 Oui. Capacité support
	9 Procédures d'interfonctionnement de support:	9 Non traité explicitement
	9.1 Adaptation/conversion de connexion de support	

Tableau I.1/Q.1701 – Ensemble de capacités 1 pour les IMT-2000 *(suite)*

Catégorie	Capacités	Couverture
	9.2 Support, composante de service et téléservice 9.2.1 Mappage 9.2.2 Négociation 9.2.3 Procédures de repli	
D) Capacité de réseau d'accès – Généralités	1 Prise en charge de services en mode paquet y compris: 1.1 Négociabilité du débit de remise (débit crête et débit moyen) 1.2 Négociabilité de la tolérance sur le temps de transmission 1.3 Négociabilité des classes de fiabilité (elles déterminent la probabilité de perte de données, la remise hors séquence, la remise en double et les données altérées)	1 Oui. Paragraphe 8
	2 Prise en charge: 2.1 D'un débit constant avec synchronisation: mode connexion 2.2 D'un débit variable avec synchronisation: mode connexion 2.3 D'un débit variable sans synchronisation: mode sans connexion 2.4 D'un débit variable sans synchronisation: mode connexion 2.5 D'une récupération efficace de la couche Liaison de données	2 Oui. Paragraphes 7, 8; QS
	3 Capacités de commande de ressources radioélectriques: 3.1 Surveillance et supervision des canaux radioélectriques et de l'environnement radioélectrique 3.1.1 Surveillance de la qualité des canaux radioélectriques 3.1.2 Surveillance de la macrodiversité 3.2 Affectation et annulation d'affectation de ressources radioélectriques 3.3 Commande et positionnement de la puissance radiofréquence	3 Non. Gestion des ressources radio
	4 Prise en charge d'applications FWA avec une fonctionnalité de type RNIS	4 Non traité spécifiquement

Tableau I.1/Q.1701 – Ensemble de capacités 1 pour les IMT-2000 *(suite)*

Catégorie	Capacités	Couverture
E) Capacité de réseau central – Généralités	1 Prise en charge: 1.1 D'un débit constant avec synchronisation: mode connexion 1.2 D'un débit variable avec synchronisation: mode connexion 1.3 D'un débit variable sans synchronisation: mode sans connexion 1.4 D'un débit variable sans synchronisation: mode connexion	1 Oui. Paragraphes 7, 8. QS et capacité support
	2 Prise en charge de communications en mode circuit et en mode paquet pour le traitement simultané de signaux vocaux, de données et de signaux vidéo	2 Oui. Paragraphes 7 et 8
	3 Interfonctionnement: 3.1 Avec les RNIS: prise en charge de services "de type" RNIS à 56 kbit/s, 64 kbit/s, 128 kbit/s et 144 kbit/s (y compris le canal D) 3.2 Avec l'ensemble de capacités 2.1 du RNIS-LB 3.3 Avec les RPD X.25: prise en charge de support avec accès au PAD aux débits de 300, 1200, 2400, 4800 et 9600 bit/s. Prise en charge du support en mode paquet X.25 aux débits de 2400, 4800 et 9600 bit/s 3.4 Avec les réseaux IP pour les contextes lancés par l'utilisateur et lancés par le réseau 3.5 Avec les RTPC (téléphonie, télécopie et données via un modem)	3 Non traité explicitement
	4 Mobilité: 4.1 Mobilité de terminal 4.2 Mobilité de personne 4.3 Mobilité de service (par exemple, environnement de rattachement virtuel)	4 Oui. Paragraphe 6
	5 Applications Internet et de données: 5.1 Les IMT-2000 doivent assurer un interfonctionnement avec les réseaux IP (y compris intranet, IPv4 et IPv6) 5.2 Les IMT-2000 peuvent assurer des services de type Internet indépendants	5 Oui. Sous-paragraphe 8.5
	6 Déplacement à l'échelle mondiale et interopérabilité au niveau des services entre membres de la famille des IMT-2000	6 Oui. Paragraphe 6 pour l'itinérance et paragraphe 9 pour les services VHE

Tableau I.1/Q.1701 – Ensemble de capacités 1 pour les IMT-2000 *(suite)*

Catégorie	Capacités	Couverture
	7 Capacités de transport associées au réseau central: 7.1 Prise en charge du fonctionnement à commutation de paquets et du fonctionnement à commutation de circuits 7.2 Prise en charge d'une architecture évoluée pour les réseaux des membres de la famille (PDH/SDH/ATM) 7.3 Prise en charge d'interfaces ouvertes avec des serveurs du RI, des serveurs dédiés de fournisseurs de services	7 Oui. Paragraphes 7 et 8
F) Capacités de réseau – Commande d'appel	1 Séparation de la commande d'appel et de la commande de connexion/de canal support	1 Oui. Paragraphe 7
	2 Adresse/nom/numéro d'annuaire uniques pour un utilisateur, pour faciliter la transportabilité de service. Cela n'empêche pas d'avoir des numéros d'abonnés multiples	2 Non traité explicitement
	3 Prise en charge de l'ensemble de capacités 1/2 du RI pour permettre l'accès aux services utilisant le RI	3 Oui. Paragraphe 9
	4 Fourniture d'une fonctionnalité de machine BCSM améliorée en ce qui concerne la mobilité	4 Oui. Paragraphe 9
	5 Plusieurs appels simultanés par terminal ou numéro d'annuaire	5 Non traité explicitement
	6 Enregistrement et retransmission de messages multimédias	6 Non. Fonction d'un FE MM
	7 Appels multimédias (voir les ensembles de capacités 1 et 2.1 de la signalisation à large bande, y compris l'ajout/la suppression d'une connexion dans le cas de configurations de communication point à point et l'ajout/le retrait d'un participant)	7 Oui. Paragraphe 8
	8 Procédures d'interréseautage: 8.1 Appel utilisant différents réseaux IMT-2000 (interréseautage de membres de la famille des IMT-2000) 8.2 Appel utilisant des réseaux IMT-2000 et des réseaux fixes [RTPC, RDCP, INTERNET(IP), RNIS(LB)]	8 Non traité explicitement
	9 Appel d'urgence: 9.1 Identification des appels d'urgence 9.2 Traitement des appels d'urgence 9.3 Détermination de la provenance des appels d'urgence	9 Oui. Sous-paragraphe 7.6
	10 Appel prioritaire: 10.1 Identification des appels prioritaires 10.2 Traitement des appels prioritaires	10 Oui. Sous-paragraphe 7.7

Tableau I.1/Q.1701 – Ensemble de capacités 1 pour les IMT-2000 *(suite)*

Catégorie	Capacités	Couverture
	11 Positionnement géographique d'un terminal/d'un utilisateur: 11.1 Détermination de la position géographique 11.2 Notification de la position géographique 11.3 Contrôle par l'utilisateur des informations relatives au service de localisation auquel l'utilisateur est abonné, y compris la capacité à empêcher la désactivation malencontreuse d'une fonctionnalité de localisation de service obligatoire	11 Oui. Sous-paragraphe 6.2
	12 Indépendance des caractéristiques des connexions dans le cas d'appels multiconnexions	12 Oui. Sous-paragraphe 8.4
G) Capacités de réseau – Procédures relatives à la sécurité	1 Authentification d'utilisateur et chiffrement pour le mode circuit et pour le mode paquet	1 Oui. Sous-paragraphe 6.1.2
	2 Identification de terminal y compris la capacité à détecter les terminaux volés et les terminaux non homologués	2 Non traité explicitement
	3 Authentification mutuelle utilisateur-réseau	3 Oui. Sous-paragraphe 6.1.2
	4 Prise en charge de mécanismes d'authentification et de chiffrement qui dépendent du service	4 Non traité explicitement
	5 Protection contre les mauvaises utilisations d'un réseau, c'est-à-dire protection contre les utilisations frauduleuses par des utilisateurs non autorisés ou par des utilisateurs autorisés dépassant leur autorité	5 Non traité explicitement
	6 Chiffrement à l'interface radioélectrique (informations d'utilisateur et de commande)	6 Non. Problème d'interface radio
	7 Interception légale (telle qu'applicable selon la réglementation nationale)	7 Non traité explicitement
	8 Confidentialité des données liées aux utilisateurs et aux abonnés (y compris l'identité des utilisateurs)	8 Sujet se rapportant à la gestion.
	9 Confidentialité des données de facturation	9 Sujet se rapportant à la gestion
	10 Confidentialité des messages des utilisateurs	10 Sujet se rapportant à la gestion
	11 Négociation du mécanisme d'authentification entre l'utilisateur, le réseau de desserte et le réseau de rattachement	11 Non traité explicitement
	12 Signalisation des événements et limitation des événements pour assurer une protection contre les fraudes	12 Fonction interne AMF

Tableau I.1/Q.1701 – Ensemble de capacités 1 pour les IMT-2000 *(suite)*

Catégorie	Capacités	Couverture
H) Capacités de réseau – Affectation des ressources	1 Affectation sur la base de la qualité de service négociée	1 Non traité explicitement
	2 Contrôle des surcharges	2 Non traité explicitement
	3 Prise en charge spectralement efficace de configurations de services mixtes (par exemple, services à faible débit/à débit élevé, en temps réel/pas en temps réel)	3 Problème d'interface radio
	4 Optimisation de le routage au moment de l'établissement de l'appel ou en cours d'appel	4 Non traité explicitement
I) Capacités de réseau – Numérotage et adressage	1 Prise en charge de la portabilité relative au numérotage et à l'adressage	1 Non traité explicitement
	2 Identification, plan d'adressage et de numérotage: 2.1 Gestion des identités 2.1.1 Terminal 2.1.2 Utilisateur mobile international 2.1.3 Abonné RNIS 2.1.4 Groupe de multidiffusion 2.2 Prise en charge de plans d'adressage et de numérotage existants et améliorés, notamment: 2.2.1 Recommandation E.164 2.2.2 Recommandation E.212 2.2.3 Recommandation E.213 2.2.4 Recommandation X.121 2.2.5 NSAP (point d'accès au service de réseau), 2.2.6 IPv4/v6 2.2.7 Adresses de messagerie électronique et de type Internet 2.2.8 Autres mécanismes, par exemple appel par nom 2.3 Encapsulage et mappage d'adresses 2.4 Prise en charge de l'adressage selon la Recommandation E.214 (appellation globale du mobile terrestre)	2 Non traité explicitement

Tableau I.1/Q.1701 – Ensemble de capacités 1 pour les IMT-2000 *(suite)*

Catégorie	Capacités	Couverture
J) Capacités de réseau – Taxation et comptabilité	Ces éléments reflètent les choix opérés pour la taxation et la comptabilité relatives aux IMT-2000.	
	1 Profils utilisateur normalisés pour la facturation et la taxation	1 Voir M.3210
	2 Signalisation d'événements et enregistrement de données d'utilisation normalisés:	2 Voir M.3210
	2.1 Enregistrement des données d'appel	
	2.2 Génération d'informations de taxation pour:	
	2.2.1 Les communications en mode circuit	
	2.2.2 Les sessions de transmission de données en paquets	
	2.2.3 Les services assurés exclusivement par l'échange d'informations de signalisation	
	2.2.4 La transmission de données sur le canal transparent du réseau de rattachement associé au module UIM	
	3 Nouveaux mécanismes de taxation (par exemple, volume (nombre de paquets ou d'octets y compris par couple d'adresses d'origine/de destination), qualité de service, durée, etc.)	3 Voir M.3210
	4 Taxation en temps réel	4 Voir M.3210
	5 Mécanismes souples de taxation/facturation:	5 Non. Problèmes importants non résolus dans les dispositions commerciales de travail avec Internet, partage de tarif, conversion de devise, précision, etc.
	5.1 Notification de taxes à l'utilisateur avant, pendant et après des événements importants	
	5.2 Transmission presque en temps réel des enregistrements de données d'utilisation	
	6 Taxation de tiers (par exemple, taxation d'autres participants pendant des communications multiparticipants)	6 Voir M.3210
	7 Facturation des communications prépayées	7 Non: sujet relatif au réseau serveur
	8 Facturation et taxation dépendant de la localisation	8 Voir M.3210
	9 Accès en temps réel aux informations de facturation	9 Voir M.3210
K) Capacités de réseau – Mobilité	1 Interopérabilité et déplacement entre systèmes de la famille des IMT-2000 avec un seul abonnement	1 Oui. Paragraphe 6
	2 Capacité à compléter la gestion de la mobilité avec une logique de service de type RI	2 Oui. Paragraphe 9
	3 Capacité à compléter le contrôle d'authentification avec une logique de service de type RI. Cette capacité n'inclut pas la génération de paramètres d'authentification (par exemple, triplets).	3 Oui. Paragraphe 9

Tableau I.1/Q.1701 – Ensemble de capacités 1 pour les IMT-2000 *(suite)*

Catégorie	Capacités	Couverture
	4 Mobilité et déplacement à l'échelle mondiale: 4.1 Gestion de la localisation, y compris la mise à jour automatique 4.2 Enregistrement d'utilisateur, mise à jour et annulation 4.3 Enregistrement relatif à la surveillance de service, mise à jour, activation, désactivation et annulation 4.4 Gestion et contrôle de la base de données des profils d'utilisateur 4.5 Gestion et contrôle de la base de données de sécurité et d'authentification	4 Oui. Paragraphe 6
L) Capacités de réseau – Portabilité de service	1 Le système de desserte devrait permettre de prendre en charge les services d'un utilisateur en déplacement sur la base des informations relatives au profil de l'utilisateur	1 Oui. Paragraphe 9
	2 Portabilité de service imperceptible (c'est-à-dire transparente pour les utilisateurs) avec d'autres réseaux IMT-2000 indépendamment des techniques utilisées (par exemple cellulaire, sans cordon, satellite)	2 Oui. Paragraphe 9
	3 Prise en charge de l'environnement de rattachement virtuel pour permettre d'offrir à un utilisateur les mêmes services lorsqu'il se déplace que lorsqu'il est dans son réseau de rattachement, pour les services propres à l'exploitant 3.1 Commande de rattachement directe 3.2 Contrôle de service par relais	3 Oui. Paragraphe 9
	4 Prise en charge des TPU	4 Non traité explicitement
	5 Prise en charge de la gestion des profils de services	5 Oui. Paragraphe 12
	6 Prise en charge de services complémentaires normalisés	6 Oui. Paragraphe 11
M) Services/ éléments de service de réseau – Transfert	1 Le transfert entre membres de la famille est pris en charge 1.1 Prise en charge d'une structure cellulaire hiérarchique 1.1.1 Transfert d'appel entre couches de cellules 1.1.2 Gestion de la localisation à l'intérieur de plusieurs couches de cellules	1 Sujet interfamilles
N) Services/ éléments de service de réseau – Fourniture de service	1 Fourniture de service par voie hertzienne: 1.1 Prise en charge de services téléphoniques et de services de données 1.2 Possibilité de téléchargement dans les deux sens (par exemple, de paramètres de service)	1 Oui. Paragraphe 12

Tableau I.1/Q.1701 – Ensemble de capacités 1 pour les IMT-2000 *(suite)*

Catégorie	Capacités	Couverture
	1.3 Prise en charge de la sécurité et de l'authentification	
O) Services/ éléments de service de réseau – Qualité de service	1 Définie lors de l'abonnement	1 Oui
	2 Négociation de la qualité de service pendant l'invocation de service	2 Oui. Paragraphe 7
	3 Renégociation de la qualité de service pendant une session de service (par exemple un appel)	3 Oui. Sous-paragraphe 8.1
	4 Qualité de services multimédias aussi bonne que dans le cas d'un accès filaire (en fonction des classes de services supports)	4 Problème d'interface radio
	5 Qualité vocale équivalente à celle obtenue dans le cas d'un accès filaire	5 Problème d'interface radio
	6 Respect des spécifications de délais minimaux (incidence sur les temporisateurs de signalisation, etc.)	6 Non traité explicitement
P) Services/ éléments de service de réseau – Prise en charge supplé-mentaire	1 Accès téléphonique sans cordon	1 Non traité explicitement
	2 Réseaux privés virtuels	2 Non traité explicitement
	3 Services pris en charge par l'exploitant	3 Non traité explicitement
	4 Services utilisant le protocole IP	4 Oui. Paragraphe 8
	5 Accès par satellite: considérations relatives au temps de propagation sur longues liaisons, à la puissance limitée et à la gestion du spectre	5 Non traité explicitement
	6 Transparence des médias (c'est-à-dire remise des données d'utilisateur sans modification)	6 Non traité explicitement
Q) Services/ éléments de service de réseau – Terminaux et modules d'identité d'utilisateur (UIM)	1 Modèle de réseau prenant en charge:	1 Oui. Paragraphe 12.
	1.1 Un réseau avec téléchargement, dans les deux sens, de profils d'utilisateurs, d'informations sur les données, etc., pour prendre en charge la fonctionnalité UIM via des canaux de communication fonctionnelle	
	1.2 Des terminaux configurables par logiciel, pour assurer une certaine souplesse de fonctionnement (par exemple pour la prise en charge d'applications proactives)	
	1.3 Un réseau suffisamment souple pour prendre en charge de futures améliorations apportées aux fonctions radioélectriques définies par logiciel, pour assurer une certaine souplesse de fonctionnement	
	2 Mobiles et modules UIM avec capacités de téléchargement en aval par voie hertzienne pour les données et les applications. Des procédures appropriées devraient exister afin de protéger les informations sensibles et confidentielles transférées par voie hertzienne	2 Oui.Paragraphe 12
	3 Plusieurs appels sur un même terminal	3 Problème d'interface radio

Tableau I.1/Q.1701 – Ensemble de capacités 1 pour les IMT-2000 *(suite)*

Catégorie	Capacités	Couverture
	4 Prise en charge de la mobilité de terminal avec un module UIM extractible ou intégré et fourniture d'informations nécessaires à partir du module UIM pour associer un abonné au terminal mobile et pour personnaliser le terminal mobile	4 Oui. Paragraphe 6
	5 Mobilité de personne fondée sur un module UIM indépendant du terminal (carte à circuits intégrés)	5 Non traité explicitement
	6 Enregistrement multiple d'un même utilisateur sur plusieurs terminaux pour différents services	6 Non traité explicitement
R) Capacités de réseau – Commande de transfert de paquets	1 Enregistrement/authentification	1 Oui. Paragraphe 6
	2 Affectation d'adresse: 2.1 Statique 2.2 Dynamique	2 Non traité explicitement
	3 Mode de veille pour faire des économies d'énergie	3 Problème d'interface radio
	4 Routage optimal des paquets	4 Non traité explicitement
	5 Prise en charge de plusieurs protocoles	5 Non traité explicitement
	6 Compression des données	6 Non traité explicitement
	7 Interréseautage (par exemple, mode tunnel, prise en charge du protocole IP au niveau des mobiles)	7 Oui. Paragraphe 8
	8 Identification de la localisation	8 Oui. Paragraphe 6
	9 Equilibrage de charge entre les canaux radiofréquences	9 Problème d'interface radio
	10 Plusieurs enregistrements d'adresses simultanés (par exemple, adresses IP) sur un même terminal	10 Non traité explicitement
	11 Accès prioritaire (pour l'enregistrement et le transfert de données)	11 Oui. Sous-paragraphe 7.7
	12 Sessions multimédias	12 Oui. Paragraphe 8

APPENDICE II

Génération de la clé d'authentification

II.1 Introduction

La génération de la clé d'authentification est prise en charge dans l'OTASP en utilisant la méthode de cryptage à clé publique. Un exemple de cette méthode est la méthode de cryptage à clé publique Diffie-Hellman décrite ici. La méthode Diffie-Hellman offre certains avantages dans la mesure où elle est disponible dans le domaine public et qu'elle est évolutive, c'est-à-dire que les différentes valeurs utilisées dans cet algorithme peuvent être définies par l'exploitant pour atteindre le niveau de sécurité voulu. La station mobile et le réseau établissent la série de valeur prise en charge pour la génération de la clé d'authentification avant le processus effectif de génération de la clé d'authentification.

II.2 Génération de la clé d'authentification en utilisant l'algorithme de Diffie-Hellman

Dans le schéma Diffie-Hellman, la clé d'authentification est générée dans l'entité UIMF et l'entité LMFh/AMF en utilisant les informations qui sont partagées entre les deux entités. L'entité LMFh/AMF génère pour un module public N et une primitive g. L'entité LMFh/AMF génère une clé secrète, y, qui est au moins un nombre aléatoire de 160 bits. L'entité LMFh/AMF envoie à l'entité UIMF: N, g, et Y, où:

$$Y = g^y \text{ Mod } N$$

L'UIMF, à la réception de N, g et Y génère une clé secrète, x, qui est au moins un nombre aléatoire de 160 bits, puis calcule et envoie X à l'entité LMFh/AMF, où:

$$X = g^x \text{ Mod } N$$

La clé d'authentification dans l'entité UIMF est calculée comme les 64 bits les moins significatifs de:

$$Y^x \text{ mod } N = (g^y)^x \text{ mod } N$$

Le LMFh/AMF calcule la même valeur de clé d'authentification que les 64 bits les moins significatifs de:

$$X^y \text{ mod } N = (g^x)^y \text{ mod } N$$

Après la génération réussie de la clé d'authentification, l'entité LMFh/AMF et l'entité UIMF échange les confirmations. La génération par l'entité UIMF de x et la génération par l'entité LMFh/AMF de N, g et y sortent du domaine d'application de la présente Recommandation. Les exigences et les propriétés pour la génération de ces nombres peuvent être obtenues des documents cryptographiques disponibles dans le domaine public.

APPENDICE III

Bibliographie

Les références qui suivent ne sont pas explicitement utilisées dans le corps de la présente Recommandation mais fournissent un arrière-plan et des informations associées utiles.

[1] Recommandation UIT-T M.3100 (1995), *Modèle générique d'information de réseau*.

[2] Recommandation UIT-R M.687-2 (1997), *Télécommunications mobiles internationales-2000 (IMT-2000)*.

[3] Recommandation UIT-R M.816-1 (1997), *Cadre de description des services assurés par les Télécommunications mobiles internationales-2000 (IMT-2000)*.

[4] Recommandation UIT-R M.817 (1992), *Télécommunications mobiles internationales-2000 (IMT-2000) Architecture de réseau*.

[5] Recommandation UIT-R M.818-1 (1993), *Utilisation des satellites dans les télécommunications mobiles internationales-2000 (IMT-2000)*.

[6] Recommandation UIT-R M.819-2 (1997), *Télécommunications mobiles internationales-2000 (IMT-2000) au servcie des pays en voie de développement*.

[7] Recommandation UIT-R M.1034-1 (1997), *Exigences imposées à la ou aux interfaces radioélectriques des Télécommunications mobiles internationales-2000 (IMT-2000)*.

[8] Recommandation UIT-R M.1035 (1993), *Cadre de description de la ou des interfaces radioélectriques et fonctionnalité des sous-systèmes radioélectriques pour les Télécommunications mobiles internationales-2000 (IMT-2000)*.

[9] Recommandation UIT-R M.1078 (1993), *Principes de sécurité pour les Télécommunications mobiles internationales-2000 (IMT-2000)*.

[10] Recommandation UIT-R M.1167 (1995), *Cadre de description de l'élément satellite des Télécommunications mobiles internationales-2000 (IMT-2000)*.

[11] Recommandation UIT-R M.1168 (1995), *Cadre de description de la gestion des Télécommunications mobiles internationales-2000 (IMT-2000)*.

[12] Recommandation UIT-R M.1223 (1997), *Evaluation des mécanismes de sécurité pour les IMT-2000*.

[13] Recommandation UIT-R M.1224 (1997), *Terminologie des Télécommunications mobiles internationales-2000 (IMT-2000)*.

[14] Recommandation UIT-T F.115 (1995), *Objectifs de service et principes relatifs aux futurs systèmes mobiles terrestres publics de télécommunication*.

[15] Recommandation UIT-T F.116 (2000), *Fonctionnalités de service et dispositions d'exploitation des télécommunications IMT-2000*.

[16] Recommandation UIT-T F.700 (2000), *Recommandation cadre sur les services multimédias*.

[17] Recommandation UIT-T I.211 (1993), *Aspects service du RNIS à large bande*.

[18] Recommandation UIT-T I.374 (1993), *Recommandation cadre relative aux capacités réseau pour la prise en charge de services multimédias (Retirée en 1998 – Remplacée par I.375.1 et I.375.2*.

[19] Recommandation UIT-T Q.1001 (1988), *Aspects généraux des réseaux mobiles terrestres publics*.

[20] Recommandation UIT-T Q.1290 (1995), *Glossaire utilisé dans la définition des réseaux intelligents*.

[21] Recommandation UIT-R M.1311 (1997), *Cadre de description de la modularité et de la communauté de conception radioélectrique au sein des systèmes IMT-2000*.

[22] Recommandation UIT-T E.214 (1988), *Structure de l'appellation globale du mobile terrestre (AGMT) sous-système de commande des connexions sémaphores*.

[23] Recommandation UIT-R M.1457 (2000), *Spécifications détaillées des interfaces radio des IMT-2000*.

SERIES 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	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, de télégraphie, de télécopie, circuits téléphoniques 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 informatiques généraux des systèmes de télécommunication

Genève, 2001