UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T M.3210.1

(01/2001)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

SÉRIE M: RGT ET MAINTENANCE DES RÉSEAUX: SYSTÈMES DE TRANSMISSION, DE TÉLÉGRAPHIE, DE TÉLÉCOPIE, CIRCUITS TÉLÉPHONIQUES ET CIRCUITS LOUÉS INTERNATIONAUX

Réseau de gestion des télécommunications

Services de gestion RGT pour la gestion de la sécurité des réseaux IMT-2000

Recommandation UIT-T M.3210.1

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE M

RGT ET MAINTENANCE DES RÉSEAUX: SYSTÈMES DE TRANSMISSION, DE TÉLÉGRAPHIE, DE TÉLÉCOPIE, CIRCUITS TÉLÉPHONIQUES ET CIRCUITS LOUÉS INTERNATIONAUX

Introduction et principes généraux de maintenance et organisation de la maintenance	M.10–M.299
Systèmes de transmission internationaux	M.300–M.559
Circuits téléphoniques internationaux	M.560–M.759
Systèmes de signalisation à canal sémaphore	M.760–M.799
Systèmes internationaux de télégraphie et de phototélégraphie	M.800–M.899
Liaisons internationales louées par groupes primaires et secondaires	M.900–M.999
Circuits internationaux loués	M.1000–M.1099
Systèmes et services de télécommunication mobile	M.1100–M.1199
Réseau téléphonique public international	M.1200–M.1299
Systèmes internationaux de transmission de données	M.1300–M.1399
Appellations et échange d'informations	M.1400–M.1999
Réseau de transport international	M.2000–M.2999
Réseau de gestion des télécommunications	**M.3000–M.3599**
Réseaux numériques à intégration de services	M.3600–M.3999
Systèmes de signalisation par canal sémaphore	M.4000–M.4999

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

Recommandation UIT-T M.3210.1

Services de gestion RGT pour la gestion de la sécurité des réseaux IMT-2000

Résumé

La présente Recommandation fait partie de la série de Recommandations M.3200 *Services de gestion du réseau de gestion des télécommunications* qui contient une description des services de gestion, des objectifs et du contexte des aspects liés à la gestion des réseaux IMT-2000. Elle fournit un profil pour la gestion de la fraude dans un réseau mobile IMT-2000. Elle s'appuie sur l'ensemble des fonctions identifiées dans l'UIT-T M.3400 et définit des ensembles de fonctions, des fonctions et des paramètres nouveaux en y ajoutant des éléments sémantiques et limitations additionnelles.

Source

La Recommandation M.3210.1 de l'UIT-T, préparée par la Commission d'études 4 (2001-2004) de l'UIT-T, a été approuvée le 19 janvier 2001 selon la procédure définie dans la Résolution 1 de l'AMNT.

Mots clés

Détection des fraudes et maintien, gestion de la sécurité, réseau de gestion des télécommunications (RGT), service de gestion du RGT, systèmes hertziens de troisième génération – Systèmes 3G, télécommunications mobiles internationales: IMT-2000.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

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

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

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

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

Page

Recommandation UIT-T M.3210.1

Services de gestion RGT pour la gestion de la sécurité des réseaux IMT-2000

1 Introduction

La présente Recommandation décrit les besoins et l'analyse de la gestion de la sécurité (administration) des systèmes IMT-2000. L'accent est mis sur l'interface X entre deux fournisseurs de services et sur les services de gestion nécessaires entre ces deux fournisseurs de services afin de détecter et prévenir toute forme de fraude. La méthodologie utilisée dans la présente Recommandation s'appuie sur l'UIT-T M.3020.

1.1 Objet et domaine d'application

La présente Recommandation décrit un sous-ensemble des services de gestion de la sécurité identifiés dans l'UIT-T M.3200 comme un domaine géré du RGT pour la gestion des IMT-2000. Elle décrit les caractéristiques et l'analyse du fonctionnement du système de collecte des informations de fraude (FIGS, *fraud information gathering system*) entre fournisseurs de services. Le système FIGS donne au fournisseur de services hertziens le moyen de surveiller un ensemble défini d'activités d'abonné. L'objectif est de permettre aux fournisseurs de services/opérateurs de réseau d'utiliser le système FIGS pour limiter leurs risques financiers face à des factures impayées conséquentes produites par des comptes d'abonné pendant que ces abonnés se trouvent en situation d'itinérance en dehors de leur zone d'origine.

La vérification de l'authenticité du système de détection des fraudes du réseau d'origine et du fournisseur de services visité sort du cadre de ce service de gestion.

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

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

[3] UIT-T Q.1721 (2000), *Flux d'informations pour l'ensemble de capacités 1 des IMT-2000.*

[4] UIT-T M.3010 (2000), *Principes des réseaux de gestion des télécommunications.*

[5] UIT-T M.3020 (2000), *Méthodologie pour la spécification des interfaces du réseau de gestion des télécommunications.*

[6] UIT-T M.3200 (1997), *Services de gestion du réseau de gestion des télécommunications et domaines gérés des télécommunications: aperçu général.*

[7] UIT-T M.3400 (2000), *Fonctions de gestion du réseau de gestion des télécommunications.*

3 Définitions

La présente Recommandation définit les termes suivants:

3.1 réseau visité: réseau visité ou étranger qui fournit à l'abonné le service d'itinérance.

3.2 réseau d'origine: réseau d'origine auprès duquel l'abonné hertzien a souscrit un contrat de service.

3.3 FDS du réseau d'origine (HN-FDS, *home network fraud detection system*): système de détection des fraudes mis en oeuvre par le réseau d'origine.

3.4 rapport de fraude: ensemble des erreurs possibles de procédure commises par un abonné qui peuvent révéler une fraude potentielle. Ce rapport détaille typiquement les dépassements par rapport aux critères ou aux modes d'utilisation courants de l'abonné (par exemple les pays appelants ou des dépassements de limites d'utilisation).

3.5 Définitions liées au rôle

La présente Recommandation utilise les rôles suivants définis dans l'UIT-T M.3208.1 :

– clients du service (*service customer*);

– opérateur de réseau (*network operator*).

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations suivantes:

FDS	système de détection des fraudes (*fraud detection system*)
FIGS	système de collecte des informations de fraude (*fraud information gathering system*)
GDMI	lignes directrices pour la définition des interfaces de gestion RGT (*guidelines for the definition of TMN management interface*)
IMT-2000	télécommunications mobiles internationales 2000 (*international mobile telecommunications 2000*)
MS	services de gestion (*management services*)
NML	couche de gestion de réseau (*network management layer*)
RGT	réseau de gestion des télécommunications
SML	couche de gestion de service
s/o	sans objet
UIT	Union internationale des télécommunications

4.1 Conventions

Symbole	Explication
m	Obligatoire
m(=)	Le destinataire doit fournir la même valeur en réponse que celle fournie dans la demande du requérant.
o	Facultatif: le caractère facultatif doit faire l'objet d'une définition conformément à l'accord signé entre les deux fournisseurs de services. En d'autres termes, un paramètre indiqué comme étant facultatif peut être rendu obligatoire.
o(=)	Le renvoi de la valeur par le répondeur est facultatif. Toutefois, si le répondeur choisit de renvoyer une valeur, celle-ci doit être identique à celle fournie par le requérant dans sa demande. Le répondeur n'est pas autorisé à modifier ce champ.
c	Paramètre conditionnel: la définition de la condition doit être spécifiée dans la colonne Remarques. Un suffixe numérique est utilisé pour permettre la réutilisation des instructions conditionnelles.
c(=)	Si la valeur est fournie dans la demande du requérant, le répondeur doit fournir la même valeur dans sa réponse.
Blanc	Un blanc signale que le paramètre est sans objet.

5 Service de gestion de la sécurité

5.1 Problèmes de sécurité

Les réseaux de télécommunication modernes, notamment les réseaux mobiles présentent la possibilité pour des fraudeurs d'utiliser des services de télécommunication (voix, données, télécopie, etc.) sans intention de payer. Un certain nombre de scénarios sont exploités et il est de la responsabilité de l'opérateur de réseau ou du fournisseur de services de détecter toute utilisation abusive et de l'empêcher le plus rapidement possible.

L'ampleur des fraudes (par jour sur un seul compte) peut être substantielle, notamment lorsque des numéros internationaux ou de tarif kiosque sont appelés. Les types de fraude les plus courants affectant les réseaux 3G sont liés à la possibilité de vendre des appels à un tarif inférieur à celui du marché en exploitant des équipements/temps d'utilisation volés sachant que l'utilisateur de l'équipement n'a pas l'intention de payer l'opérateur de réseau ou le fournisseur de services. Les abonnés fraudeurs évitent souvent toute facturation en se procurant un combiné et un abonnement à un réseau en fournissant de manière frauduleuse des renseignements et des justificatifs à l'opérateur de réseau/fournisseur de services. S'il n'existe pas de systèmes de contrôle efficaces sur le réseau, l'abonné peut passer un nombre important d'appels vers des destinations coûteuses pour un montant conséquent.

5.2 Description du service de gestion

Compte tenu que des abonnés hertziens peuvent passer d'un opérateur de réseau à un autre (et compte tenu de l'existence de fournisseurs de services nombreux), le service de gestion de la sécurité revêt une importance capitale. La présente Recommandation décrit les informations relatives à la gestion de la sécurité échangées par l'intermédiaire du point de référence x entre deux systèmes d'exploitation (OS, *operating system*) RGT (le réseau visité et le réseau d'origine).

Les relations RGT entre le service de gestion de la sécurité IMT-2000 et le système de collecte des informations de fraude (FIGS) sont illustrées à la Figure 1. Elle illustre l'abonné hertzien en itinérance vers le réseau d'un fournisseur de services visité.

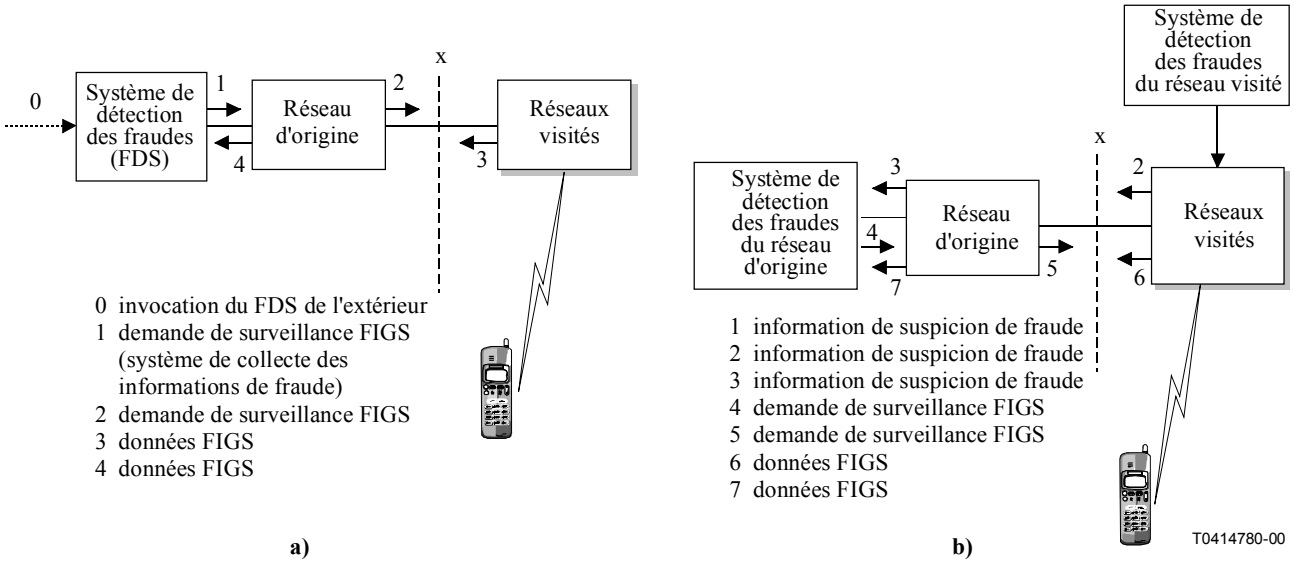

Figure 1/M.3210.1 – Service de gestion de la sécurité des systèmes IMT-2000: schémas de collaboration pour la collecte d'informations de fraude

Sur la Figure 1a), le système de détection des fraudes du réseau d'origine (HN-FDS) demande au réseau visité de lui fournir certains renseignements concernant l'abonné à partir du moment où cet abonné a été enregistré par ce réseau visité jusqu'au moment où la dernière des activités surveillées s'est terminée sur ce réseau visité, qui peut se situer au-delà de la suppression d'enregistrement de l'abonné du réseau visité. Les informations reçues par le réseau d'origine seront transmises au HN-FDS. L'analyse de ces informations peut provoquer la transmission d'instructions complémentaires au réseau visité qui lui permettront d'agir de manière appropriée.

Les opérations illustrées à la Figure 1b) sont comparables à celles de la Figure 1a) à la différence près que l'invocation des opérations est déclenchée par le fournisseur de services visité.

6 Exigences fondamentales en matière de gestion

Le HN-FDS ou le réseau visité peuvent prendre des mesures préventives pour contrôler et empêcher des activités frauduleuses conformément à des politiques de sécurité établies. Les services de gestion de la sécurité décrits dans la présente Recommandation sont applicables sur les réseaux de différents fournisseurs de services exploitant des réseaux hertziens semblables ou différents. Ces services de gestion offrent au réseau visité et au HN-FDS la capacité d'échanger des informations et de contrôler l'échange d'informations relatives à des activités potentiellement frauduleuses sur le réseau visité.

Les capacités du système de collecte des informations de fraude (FIGS) sont détaillées dans le Tableau 1:

Tableau 1/M.3210.1 – Capacités minimales requises pour le système de collecte des informations de fraude

Domaine	Référence	Conditions
Capacités à l'échelle du système	1	La surveillance FIGS doit être activée lorsque: 1 Le réseau visité reçoit des demandes du HN-FDS de surveillance d'activités d'abonné suspectes. 2 Le HN-FDS reçoit des alertes non sollicitées de l'abonné en provenance du réseau visité, notamment si l'abonné en itinérance reçoit un service du réseau visité pendant des périodes prolongées.
	2	Le système FIGS ne doit pas modifier le service du réseau visité.
	3	Le système FIGS ne doit modifier aucune fonction hertzienne 3G standard vue par l'abonné ni affecter la qualité de service.
	4	La fonction de surveillance du système FIGS s'applique à tous les services supports (par exemple circuit, IP, etc.), téléservices et services complémentaires souscrits par l'abonné. Il n'est pas possible d'appliquer le système FIGS de manière individuelle à des services donnés.
	5	Les informations doivent être transmises du réseau visité au HN-FDS par des liaisons de communication existantes (par exemple interface X du RGT, liaisons de signalisation SS7).
	6	Un mécanisme permettant à un réseau visité de taxer un HN-FDS pour le transfert global de données effectué vers cet HN-FDS est nécessaire.
Capacités du réseau d'origine	7	La collecte des informations de fraude est contrôlée par le HN-FDS et peut être activée/désactivée par le HN-FDS uniquement.
	8	Le réseau d'origine doit signaler le niveau de surveillance des fraudes nécessaire: **Niveau 1 –** procédure de comptabilité accélérée associée à un mécanisme du type facturation en temps réel/quasi réel. **Niveau 2 –** des informations d'appel partielles sont collectées, uniquement en début et en fin d'appel. **Niveau 3 –** informations d'appel complètes relatives aux activités de l'abonné, par exemple heure de début et de fin d'appel et enregistrements partiels des appels. La notification de l'invocation de transfert explicite de communication, de transfert d'appel, de renvoi d'appel, de mise en attente et de service à multiparticipants est également fournie.
	9	Le HN-FDS doit être en mesure d'indiquer s'il souhaite recevoir des informations d'appel relatives aux sessions provenant de mobiles (MO), aux sessions aboutissant à des mobiles (MT) ou aux deux types de sessions.
	10	Le réseau d'origine ne doit pas autoriser l'enregistrement de nouveaux abonnés si la prise en charge du système FIGS provoque une surcharge dans le réseau visité. Le réseau visité doit en conséquence gérer, jusqu'à un niveau réaliste, toute demande d'enregistrement d'abonné et être capable de prendre en charge le transfert de données associé. Le réglage de cette limite sort du cadre de la présente Recommandation.
	11	Le réseau d'origine doit marquer un abonné comme étant surveillé par le système FIGS.
	12	Le réseau d'origine doit recevoir des données FIGS du réseau visité.

Tableau 1/M.3210.1 – Capacités minimales requises pour le système de collecte des informations de fraude *(fin)*

Domaine	Référence	Conditions
	13	Le réseau d'origine met fin à la surveillance par le système FIGS des activités de l'abonné.
Capacités du réseau visité	14	En se fondant sur les accords d'itinérance, le réseau visité doit signaler au HN-FDS toute information susceptible de révéler des activités frauduleuses.
	15	Si le réseau visité ne dispose pas des ressources suffisantes pour prendre en compte une demande du système FIGS, il doit en informer le HN-FDS.
	16	Chaque réseau visité doit limiter le nombre d'abonnés dont le HN-FDS peut demander la surveillance au moyen du système FIGS. Dans le cas contraire, un HN-FDS du réseau d'origine risque d'accaparer plus que sa "juste part" de la capacité de traitement FIGS d'un réseau visité.
	17	Les informations doivent être transmises du réseau visité au HN-FDS dans les deux minutes qui suivent le déclenchement de l'événement surveillé par le système FIGS. Ceci est une conséquence du fait que la fraîcheur des informations est une qualité essentielle de tout système d'informations de fraude. Plus les données sont transférées précocement au HN-FDS, plus rapidement la fraude peut être arrêtée.
	18	En s'appuyant sur des accords d'itinérance, transmettre des données du système FIGS au HN-FDS selon: 1 la fréquence demandée par le HN-FDS; 2 des événements spécifiés dans le HN-FDS; 3 à la demande.

6.1 Présentation d'ensemble du service de gestion

Le service de gestion de la sécurité comprend les groupes d'ensembles de fonctions suivants d'après l'UIT-T M.3400:

- prévention;
- détection;
- maintien et reprise;
- administration de la sécurité.

Parmi les groupes d'ensembles de fonctions décrits dans l'UIT-T M.3400, la présente Recommandation ne traite que des aspects des groupes d'ensembles de fonctions de détection dans le but de détecter un piratage hertzien.

Une liste clé des caractéristiques de gestion de "Sécurité – vérifications: comptage des utilisations frauduleuses" comprend les éléments suivants:

- détermination des événements liés à la sécurité;
- enregistrement des événements liés à la sécurité;
- signalement des événements liés à la sécurité.

Il existe plusieurs méthodes de détection de violations de mesures de sécurité dans un réseau hertzien. Les processus mis en œuvre dans le HN-FDS et sur le réseau visité appliquent divers critères tels que la facturation de l'utilisation et l'analyse de structure d'utilisation afin de produire des rapports de sécurité. Les rapports et événements échangés entre les deux fournisseurs de services constituent la base sur laquelle se fondent les aspects de détection de la présente Recommandation. Les renseignements que ces rapports sont susceptibles de contenir concernent: indication de date et heure, données d'utilisation déviante, enregistrements de données relatives à l'utilisation, rapports d'événements d'alarme et renseignements concernant l'abonné.

6.2 Ressources de télécommunication

6.2.1 Système de collecte des informations de fraude (FIGS)

Le HN-FDS reçoit des données relatives aux activités des abonnés dans un réseau visité au moyen du système de collecte des informations de fraude. Il peut dès lors émettre des hypothèses sur l'activité de l'abonné et prendre des décisions portant sur les opérations que l'abonné est autorisé à effectuer. Les opérations suivantes peuvent être invoquées au niveau du système FIGS. Elles sont décrites ci-après dans les cas d'utilisation:

1) alerte de fraude: le réseau visité invoque cette opération lorsqu'une fraude est suspectée;
2) activation de la collecte d'informations: cette opération lance le processus de surveillance des activités d'un abonné donné;
3) rapport FIGS: cette opération est invoquée par le réseau visité pour transmettre des informations recueillies;
4) désactivation de la collecte d'informations: cette opération met fin au processus de surveillance des activités de l'abonné;
5) modification du rapport FIGS: cette opération modifie le niveau de surveillance et/ou le calendrier de remise des informations relatives aux activités de l'abonné;
6) avis de suspension de la surveillance FIGS: cette opération est invoquée par le réseau visité pour informer le HN-FDS que la collecte d'informations est suspendue;
7) avis de reprise de la surveillance FIGS: cette opération est invoquée par le réseau visité pour informer le HN-FDS que la collecte d'informations est reprise après une suspension.

6.2.2 Réseau visité

Un réseau visité (fournisseur de services visité) peut recevoir des demandes de surveillance par le système FIGS. Un réseau visité peut alors effectuer certaines des opérations suivantes:

– activer la surveillance FIGS pour l'abonné en itinérance considéré. Le HN-FDS reçoit alors des rapports contenant le résultat des activités de surveillance;
– le réseau visiteur peut être surchargé. La demande est alors mise en attente jusqu'à ce que la capacité de surveillance soit rétablie. La surveillance FIGS est ensuite activée pour l'abonné en itinérance considéré.

6.2.3 Système de détection des fraudes du réseau d'origine (HN-FDS, *home network fraud detection system*)

Le HN-FDS demande une surveillance FIGS aux réseaux visités qui se mettent alors à collecter des données relatives aux activités d'abonnés particuliers.

Le HN-FDS programme ensuite la réception de rapports d'événements de seconde, selon un intervalle de temps convenu. Le HN-FDS peut également demander au réseau visité de lui fournir à tout moment des rapports d'événements de sécurité. Dans les deux cas, les renseignements relatifs à la sécurité doivent être remis dans un délai aussi court que possible.

6.3 Cas d'utilisation du système de collecte des informations de fraude

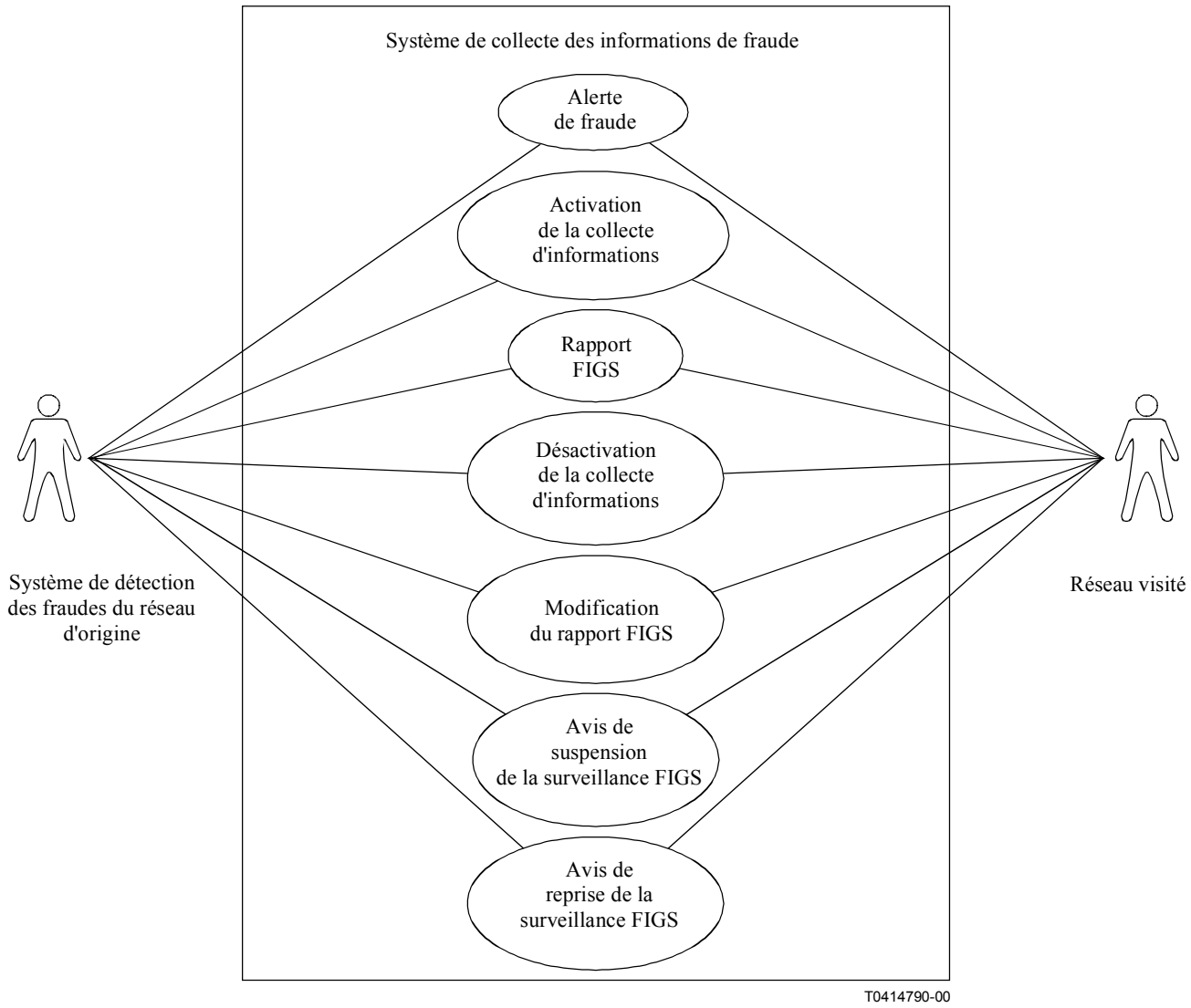

Figure 2/M.3210.1 – Cas d'utilisation du système FIGS

6.3.1 Cas d'utilisation de la fonction alerte de fraude

Nom	Alerte de fraude
Résumé	Cette opération est invoquée par le réseau visité suspectant une fraude pour informer le HN-FDS de la nécessité de déclencher la surveillance FIGS.
Acteur(s)	1) HN-FDS 2) réseau visité
Préconditions	Suspicion de fraude d'abonné.
Débute lorsque	L'abonné se déplace vers le réseau visité.
Description	A l'issue d'une session d'itinérance d'un abonné particulier dans un réseau visité, ce réseau peut informer le HN-FDS qu'il suspecte une utilisation frauduleuse. Cette alerte peut être, par exemple, la conséquence d'une structure d'utilisation inhabituelle de la part de l'abonné en itinérance.
Se termine lorsque	Sans objet
Exceptions	Sans objet
Postconditions	Surveillance FIGS demandée. Plus de suspicion de fraude. Terminal de l'abonné désactivé.
Rattachement	Ce cas d'utilisation remplit les conditions suivantes: 1 (Tableau 1).

6.3.2 Cas d'utilisation de la fonction activation de la collecte d'informations

Nom	Activation de la collecte d'informations
Résumé	Cette opération déclenche la demande de démarrage du processus de surveillance des activités d'un abonné donné.
Acteur(s)	1) HN-FDS 2) réseau visité
Préconditions	Suspicion de fraude d'abonné.
Débute lorsque	Réception d'une demande de la part du: – HN-FDS – réseau visité.
Description	Le HN-FDS peut considérer nécessaire de surveiller un abonné particulier. Cette décision peut être prise en réponse à un message d'alerte de fraude du réseau visité.
Se termine lorsque	Le HN-FDS demande de mettre fin à la surveillance de l'abonné.
Exceptions	Le réseau visité n'est pas en mesure de déclencher la surveillance.
Postconditions	Plus de suspicion de fraude. Terminal de l'abonné désactivé.
Rattachement	Ce cas d'utilisation remplit les conditions suivantes: 1, 8, 9, 10, 12 et 15 (Tableau 1).

6.3.3 Cas d'utilisation de la fonction rapport FIGS

Nom	Rapport FIGS
Résumé	Cette opération est invoquée par le réseau visité pour transmettre au HN-FDS des informations collectées.
Acteur(s)	1) HN-FDS 2) réseau visité
Préconditions	Suspicion de fraude d'abonné.
Débute lorsque	L'abonné se déplace vers le réseau visité.
Description	Le réseau visité recueille des informations relatives aux activités de l'abonné en itinérance à l'attention du HN-FDS. Ces informations ne sont collectées que si le réseau d'origine demande l'activation de la surveillance de l'abonné. Elles sont ensuite transmises au réseau d'origine en fonction des critères définis.
Se termine lorsque	La surveillance FIGS est désactivée ou le système FIGS est suspendu à la suite d'une surcharge du réseau visité.
Exceptions	Sans objet
Postconditions	Plus de suspicion de fraude. Terminal de l'abonné désactivé.
Rattachement	Ce cas d'utilisation remplit les conditions suivantes: 2, 3, 4, 5, 6, 7, 12, 13, 14, 15, 17 et 18 (Tableau 1).

6.3.4 Cas d'utilisation de la fonction désactivation de la collecte d'informations

Nom	Désactivation de la collecte d'informations
Résumé	Cette opération est invoquée par le HN-FDS pour demander qu'il soit mis fin au processus de surveillance des activités de l'abonné visiteur.
Acteur(s)	1) HN-FDS 2) réseau visité
Préconditions	L'une des deux situations suivantes se présente: • pas de fraude de l'abonné suspectée; • l'abonné met fin à sa situation d'itinérance.
Débute lorsque	Une demande est reçue du HN-FDS.
Description	La demande est acceptée et transmise au réseau visité.
Se termine lorsque	Sans objet
Exceptions	Sans objet
Postconditions	Plus de suspicion de fraude. Terminal de l'abonné désactivé.
Rattachement	Ce cas d'utilisation remplit les conditions suivantes: 7 et 13 (Tableau 1).

6.3.5 Cas d'utilisation de la fonction modification du rapport FIGS

Nom	Modification du calendrier de remise des informations de fraude
Résumé	Le HN-FDS envoie une demande au réseau visité le sollicitant de modifier la fréquence de remise des rapports de surveillance.
Acteur(s)	1) HN-FDS 2) réseau visité
Préconditions	• Une surveillance FIGS est en cours pour un abonné. • Le HN-FDS demande que les activités d'un abonné soient surveillées à un niveau différent ou selon un calendrier différent de ceux définis dans l'accord d'itinérance.
Débute lorsque	Une demande est reçue du HN-FDS.
Description	Le HN-FDS peut estimer nécessaire de modifier: a) le calendrier de remise de rapports de surveillance pour un abonné donné; b) le niveau de surveillance de fraude demandé.
Se termine lorsque	La demande est acceptée et transmise au réseau visité.
Exceptions	Le système visité n'est pas en mesure de traiter la demande.
Postconditions	Un nouveau calendrier de remise ou un nouveau niveau de surveillance sont définis.
Rattachement	Ce cas d'utilisation remplit les conditions suivantes: 8 et 18 (Tableau 1).

6.3.6 Cas d'utilisation de la fonction avis de suspension de la surveillance FIGS

Nom	Avis de suspension de la surveillance FIGS
Résumé	Cette opération est invoquée par le réseau visité pour informer le HN-FDS de la suspension de la collecte d'informations FIGS pour des raisons de pénurie de ressources.
Acteur(s)	1) HN-FDS 2) réseau visité
Préconditions	Suspicion de fraude d'abonné et pénurie de ressources sur le réseau visité.
Débute lorsque	Les ressources du réseau visité ne sont pas en mesure de répondre à la demande de surveillance des abonnés en itinérance actuels.
Description	Il existe un problème de pénurie de ressources de surveillance sur le réseau visité. Ce problème peut être, par exemple, la conséquence d'un accroissement des activités d'un grand nombre d'abonnés en itinérance sous surveillance. En conséquence, un message est envoyé aux réseaux d'origine d'un certain nombre de ces abonnés pour les informer que la surveillance est suspendue.
Se termine lorsque	Le fonctionnement normal du réseau visité est restauré et un message signalant au réseau d'origine la reprise de la surveillance est envoyé.
Exceptions	Sans objet
Postconditions	Plus de suspicion de fraude. Terminal de l'abonné désactivé.
Rattachement	Ce cas d'utilisation remplit les conditions suivantes: 10, 15 et 16 (Tableau 1).

6.3.7 Cas d'utilisation de la fonction avis de reprise de la surveillance FIGS

Nom	Avis de reprise de la surveillance FIGS
Résumé	Cette opération est invoquée par le réseau visité pour informer le HN-FDS de la reprise de la collecte d'informations FIGS.
Acteur(s)	1) HN-FDS 2) réseau visité
Préconditions	Suspicion de fraude d'abonné.
Débute lorsque	L'abonné se déplace vers le réseau visité.
Description	Les ressources du réseau visité sont restaurées et celui-ci peut reprendre la surveillance des abonnés en itinérance marqués comme tels.
Se termine lorsque	La surveillance de l'abonné est arrêtée ou une surcharge du système FIGS du réseau visité se produit à nouveau.
Exceptions	Sans objet
Postconditions	Plus de suspicion de fraude. Terminal de l'abonné désactivé.
Rattachement	Ce cas d'utilisation remplit les conditions suivantes: 10, 15 et 16 (Tableau 1).

7 Analyse des fonctions de gestion

Le présent paragraphe contient la description de haut niveau du service de gestion de la sécurité du système FIGS. En d'autres termes, il présente les messages nécessaires à la prise en charge des fonctions de gestion pour solliciter et collecter les informations de sécurité entre fournisseurs de services.

7.1 Ensemble de fonctions de collecte des informations de fraude

L'ensemble de fonctions FIGS est capable de prendre en charge une demande émanant d'un fournisseur de services et le signalement d'un rapport de données d'utilisation provenant d'un autre fournisseur de services. Le Tableau 2 contient la liste des fonctions FIGS illustrant les activités de gestion de la source et du destinataire.

Tableau 2/M.3210.1 – Interactions des ensembles de fonctions du système FIGS

	Fonction	Source	Destinataire
1	Fonction alerte de fraude	Réseau visité	HN-FDS
2	Fonction activation de la collecte d'informations	HN-FDS	Réseau visité
3	Fonction rapport FIGS	Réseau visité	HN-FDS
4	Fonction désactivation de la collecte d'informations	HN-FDS	Réseau visité
5	Fonction modification du calendrier de remise des rapports FIGS	HN-FDS	Réseau visité
6	Fonction avis de suspension de la surveillance FIGS	Réseau visité	HN-FDS
7	Fonction avis de reprise de la surveillance FIGS	Réseau visité	HN-FDS

7.2 Classes d'objets et diagrammes d'état

L'automate décrivant les interactions avec le système FIGS est illustré à la Figure 3. A mesure que des messages sont échangés entre le réseau visité et le HN-FDS, le lien de message entre ces deux entités se situe dans l'un ou l'autre des états décrits (voir Figure 4).

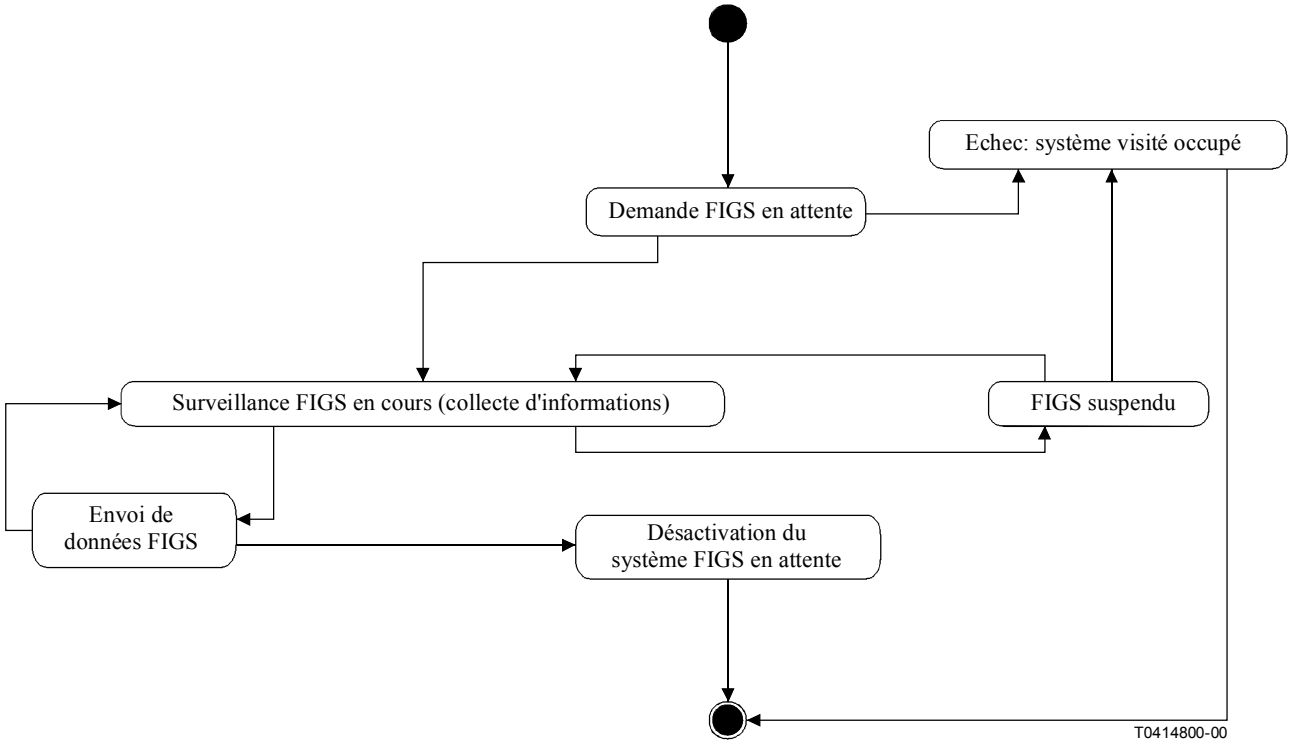

Figure 3/M.3210.1 – Diagramme d'état du système FIGS

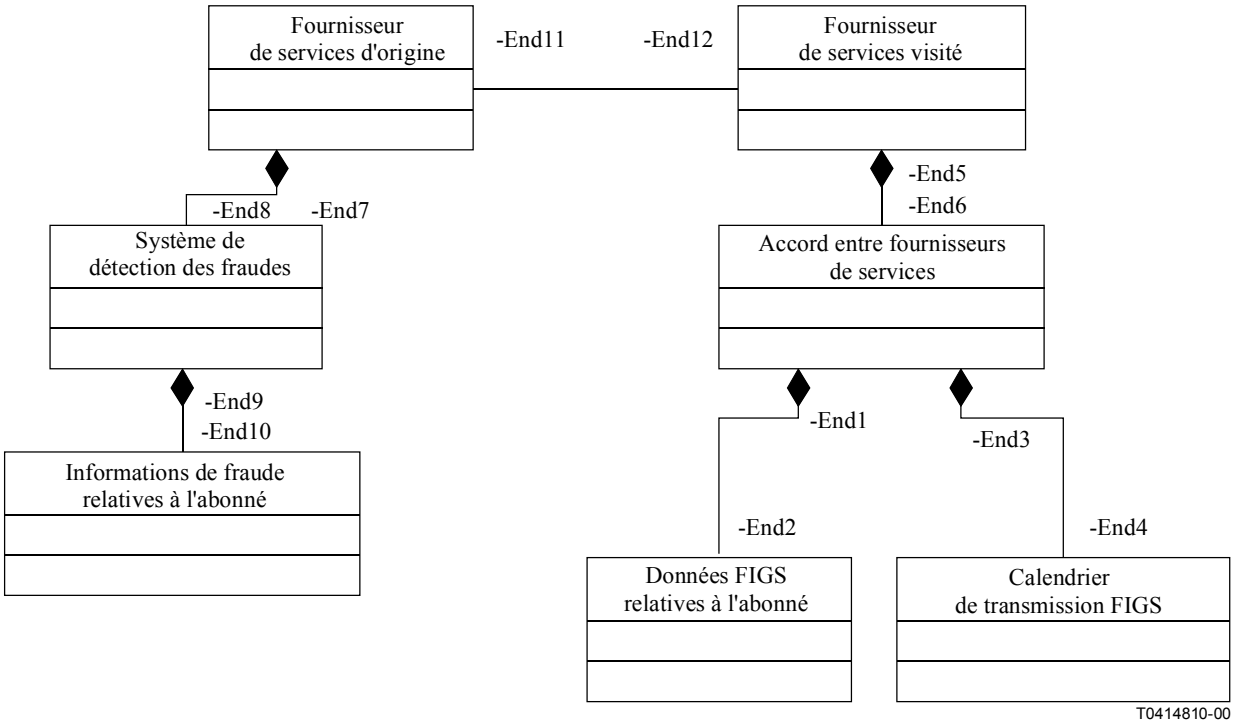

Figure 4/M.3210.1 – Diagramme de classe du système FIGS

7.3 Fonctions de collecte des informations de fraude et diagrammes d'enchaînement

7.3.1 Fonction alerte de fraude

A l'issue d'une session d'itinérance d'un abonné donné dans un réseau visité, ce dernier peut informer le HN-FDS de l'abonné qu'il suspecte une utilisation frauduleuse. Cette alerte peut, par exemple, être la conséquence d'une structure d'utilisation inhabituelle de la part de l'abonné en itinérance, comme dans la Figure 5:

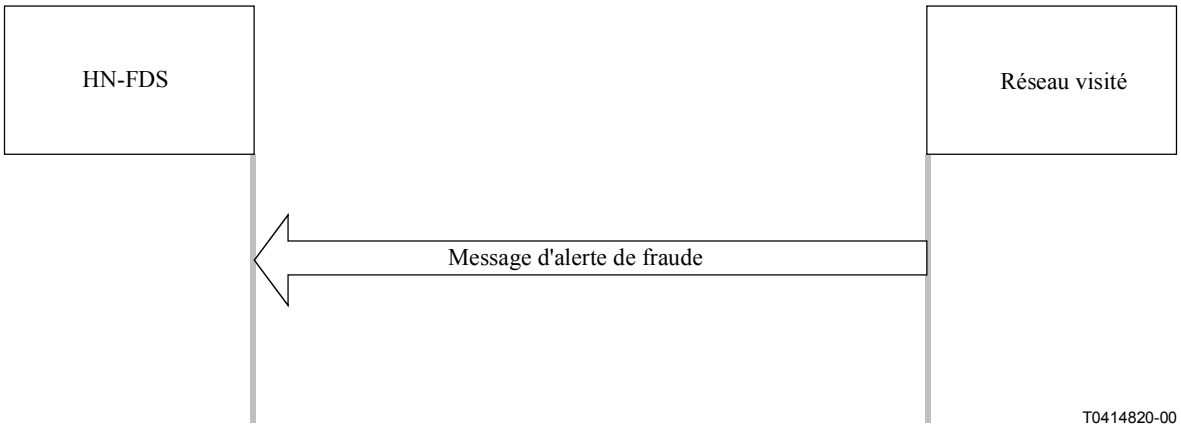

Figure 5/M.3210.1 – Flux du message d'alerte

En conséquence, le HN-FDS est informé. Dans ce scénario, illustré à la Figure 5, le réseau visité informe le HN-FDS de la présence d'un abonné en itinérance particulier.

7.3.1.1 Flux d'information

Les informations d'alerte de fraude échangées sont détaillées au Tableau 3.

Tableau 3/M.3210.1 – Informations d'alerte de fraude échangées

	HN-FDS	Réseau visité	Remarques
Liste d'identification d'utilisateur 3G		m	Liste d'identification unique de l'abonné hertzien (par exemple IMSI (identité internationale de station mobile) ou numéro de télécommunications personnelles universelles)
Numéro de série électronique		m	Le numéro de série électronique du terminal de l'abonné tel que défini dans les normes de signalisation hertzienne.

7.3.2 Fonction activation de la collecte d'informations

Le HN-FDS peut juger nécessaire de surveiller un abonné particulier. Cette décision peut, par exemple, être prise en réponse à un message d'alerte de fraude du réseau visité. Dans ce scénario, le HN-FDS demande au réseau visité de surveiller un abonné en itinérance particulier. Le réseau visité doit accuser réception de cette demande.

La demande d'activation de la collecte d'informations ne peut être déclenchée que par le HN-FDS et transmise au réseau visité comme illustré à la Figure 6.

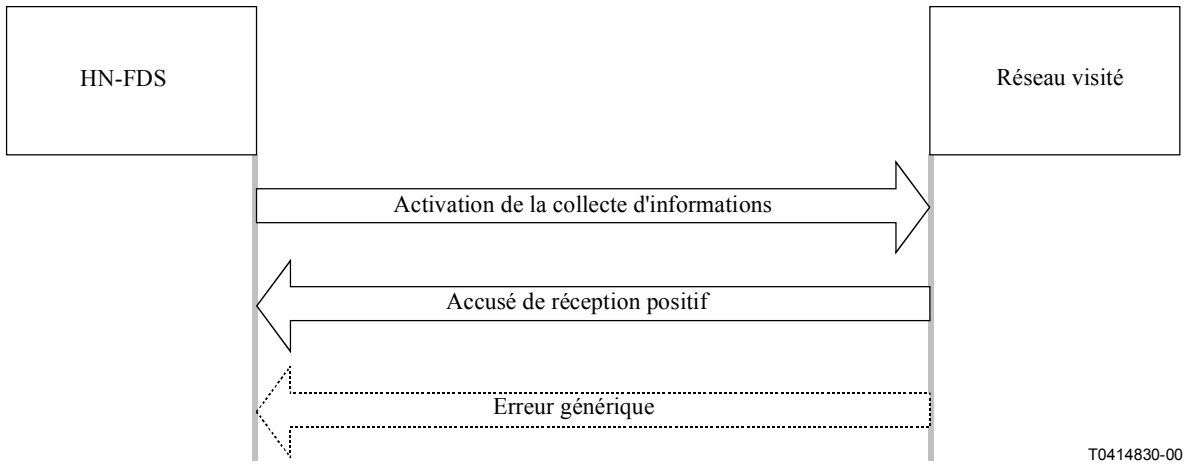

Figure 6/M.3210.1 – Flux du message d'activation du système FIGS

7.3.2.1 Flux d'information

Les informations d'activation du système FIGS échangées sont détaillées au Tableau 4.

Tableau 4/M.3210.1 – Informations d'activation du système FIGS échangées

	HN-FDS	Réseau visité	Remarques
Liste d'identification d'utilisateur 3G	m		Liste d'identification unique de l'abonné hertzien (par exemple IMSI (identité internationale de station mobile) ou numéro de télécommunications personnelles universelles).
Numéro de série électronique	m		Le numéro de série électronique du terminal de l'abonné tel que défini dans les normes de signalisation hertzienne.
Motif d'activation du système FIGS	c		Code de motif: – fraude suspectée; – autre.
Niveau de surveillance demandé	m		Niveau de surveillance: Niveau 1 – facturation en (quasi) temps réel; Niveau 2 – enregistrements d'appels partiels, Niveau 3 – enregistrements d'appels complets.
Confirmation		m	Code de résultat: R0: autre; R1: succès; R2: abonné(s) inconnu(s).

7.3.3 Fonction Rapport FIGS

Le réseau visité rassemble des informations relatives à l'utilisation faite par l'abonné en itinérance pour le HN-FDS. Ces informations ne sont collectées que sur demande d'activation de la surveillance d'un abonné par le réseau d'origine.

Dans ce scénario, illustré à la Figure 7, le réseau visité envoie périodiquement des informations concernant un abonné en itinérance particulier au HN-FDS.

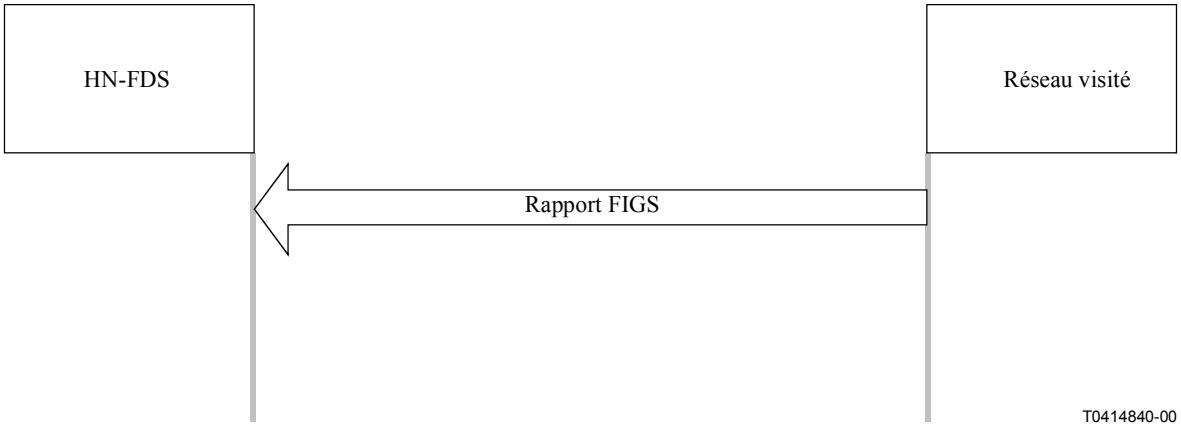

Figure 7/M.3210.1 – Flux de messages d'envoi d'informations

7.3.3.1 Flux d'information

Les informations relatives au rapport FIGS sont détaillées au Tableau 5.

Tableau 5/M.3210.1 – Informations relatives au rapport FIGS

	HN-FDS	Réseau visité	Remarques
Liste d'identification d'utilisateur 3G	m		Liste d'identification unique de l'abonné hertzien (par exemple IMSI (identité internationale de station mobile) ou numéro de télécommunications personnelles universelles).
Numéro de série électronique	m		Le numéro de série électronique du terminal de l'abonné tel que défini dans les normes de signalisation hertzienne.
Rapport FIGS	c		Code de motif: – fraude suspectée; – autre.
Confirmation		m	Code de résultat: R0: autre; R1: succès; R2: abonné(s) inconnu(s).

7.3.4 Fonction Désactivation de la collecte d'informations

Le HN-FDS peut juger nécessaire de mettre fin à la surveillance d'un abonné particulier. Cette décision peut, par exemple, résulter de la détermination que la structure d'utilisation d'un abonné est considérée comme normale après vérification. Dans ce scénario, le HN-FDS demande au réseau visité de mettre fin à la surveillance d'un abonné en itinérance particulier. Le réseau visité doit accuser réception de cette demande et mettre fin à la surveillance.

La demande de désactivation de la collecte d'informations ne peut être déclenchée que par le HN-FDS et transmise au réseau visité, comme l'illustre la Figure 8.

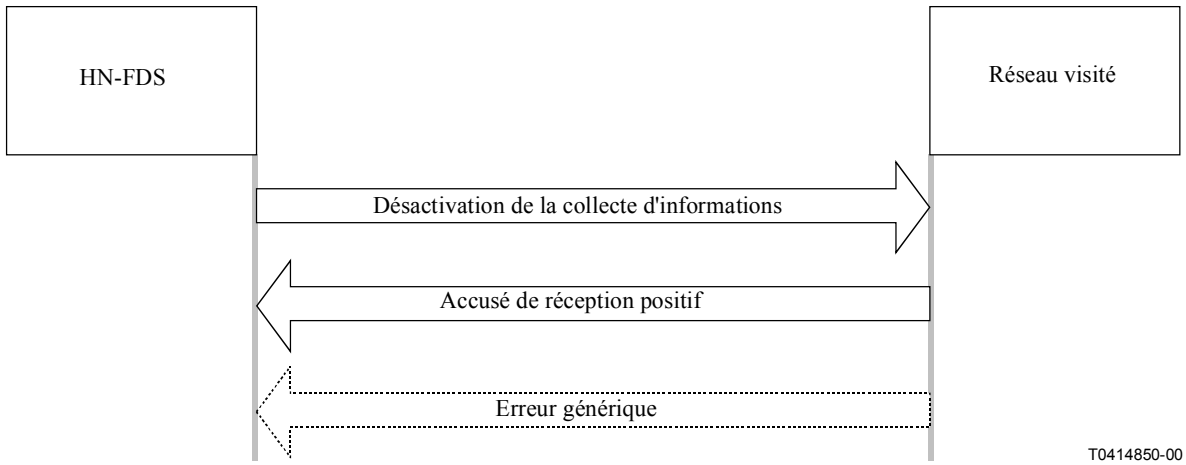

Figure 8/M.3210.1 – Flux de messages de la désactivation de la surveillance FIGS

7.3.4.1 Flux d'information

Les informations de désactivation du système FIGS échangées sont détaillées au Tableau 6.

Tableau 6/M.3210.1 – Informations de désactivation du système FIGS échangées

	HN-FDS	Réseau visité	Remarques
Liste d'identification d'utilisateur 3G	m		Liste d'identification unique de l'abonné hertzien (par exemple IMSI (identité internationale de station mobile) ou numéro de télécommunications personnelles universelles).
Numéro de série électronique	m		Le numéro de série électronique du terminal de l'abonné tel que défini dans les normes de signalisation hertzienne.
Motif de désactivation du système FIGS	c		Code de motif: – une fraude est détectée – l'abonné est suspendu; – aucune fraude n'est avérée.
Confirmation		m	Code de résultat: R0: autre; R1: succès; R2: abonné(s) inconnu(s).

7.3.5 Fonction Modification du rapport FIGS

Le HN-FDS peut juger nécessaire de modifier le calendrier de remise des rapports de surveillance d'un abonné donné. Cette décision peut être la conséquence d'une situation de surcharge.

Dans ce scénario, illustré à la Figure 9, le HN-FDS demande au réseau visité de modifier le calendrier de remise des rapports. Le réseau visité doit accuser réception de cette demande et modifier le calendrier de remise.

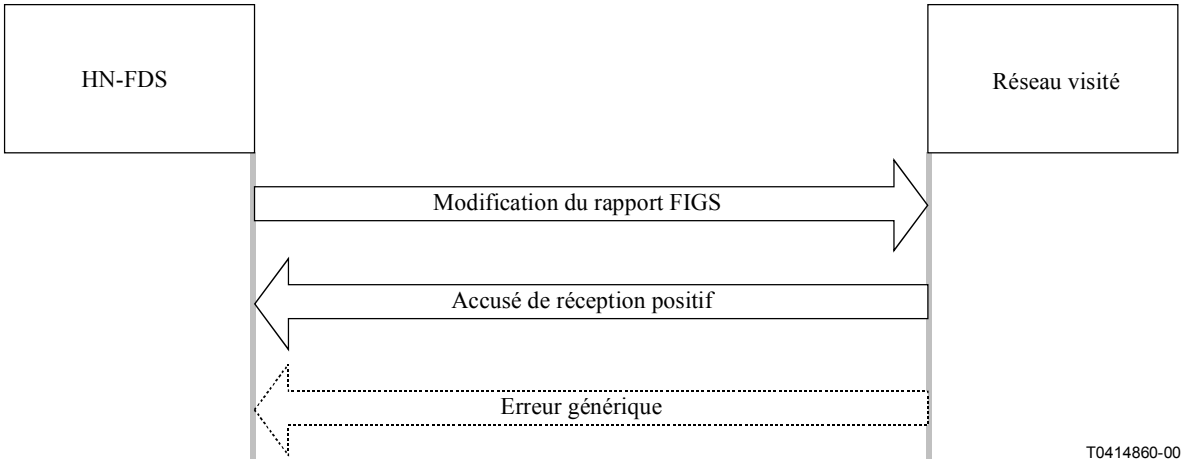

Figure 9/M.3210.1 – Flux de messages de la modification du calendrier d'établissement de rapports

7.3.5.1 Flux d'information

Les informations de modification de la remise de rapports FIGS échangées sont détaillées au Tableau 7.

Tableau 7/M.3210.1 – Informations de modification de la remise de rapports FIGS échangées

	HN-FDS	Réseau visité	Remarques
Liste d'identification d'utilisateur 3G	m		Liste d'identification unique de l'abonné hertzien (par exemple IMSI (identité internationale de station mobile) ou numéro de télécommunications personnelles universelles).
Numéro de série électronique	m		Le numéro de série électronique du terminal de l'abonné tel que défini dans les normes de signalisation hertzienne.
Nouveau calendrier	c		Si la demande de modification concerne une modification de calendrier, cet élément est obligatoire. Vous avez le choix entre: – intervalle de temps; – heures absolues.
Nouveau niveau de surveillance	c		Si la demande de modification concerne une modification du niveau de surveillance, cet élément est obligatoire. Vous avez le choix entre: – niveau 1; – niveau 2; – niveau 3.
Confirmation		m	Code de résultat: R0: autre; R1: succès; R2: abonné(s) inconnu(s)

7.3.6 Fonction Avis de suspension de la surveillance FIGS

Les ressources de surveillance du réseau visité peuvent faire l'objet d'un problème de pénurie. Cette pénurie peut être, par exemple, la conséquence d'un accroissement des activités d'un grand nombre d'abonnés en itinérance en cours de surveillance, comme dans la Figure 10:

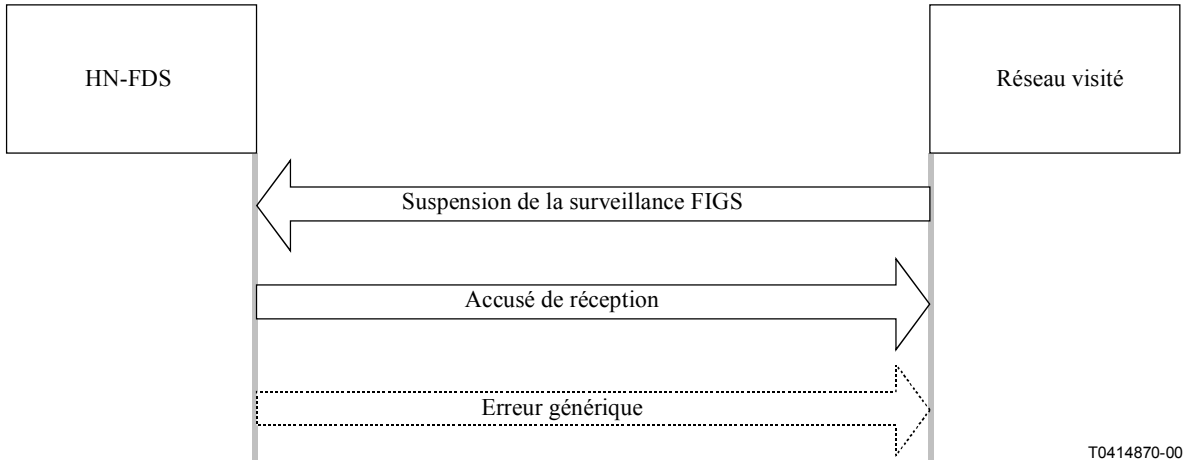

Figure 10/M.3210.1 – Flux de messages de la fonction avis de suspension de la surveillance FIGS

En conséquence, comme illustré à la Figure 10, la surveillance d'abonnés sélectionnés peut être suspendue et le HN-FDS en est informé. Dans ce scénario, le HN-FDS informe le réseau visité de sa décision de suspendre la surveillance des informations d'un abonné en itinérance particulier.

7.3.6.1 Flux d'information

Les informations échangées entre le HN-FDS et le réseau visité concernant la suspension de la surveillance d'un abonné en itinérance sont détaillées au Tableau 8.

Tableau 8/M.3210.1 – Informations de suspension de la surveillance FIGS échangées

	HN-FDS	Réseau visité	Remarques
Liste d'identification d'utilisateur 3G	m	m=	Liste d'identification unique de l'abonné hertzien (par exemple IMSI (identité internationale de station mobile) ou numéro de télécommunications personnelles universelles).
Numéro de série électronique	m	m=	Le numéro de série électronique du terminal de l'abonné tel que défini dans les normes de signalisation hertzienne.
Suspension du code de service	m		Code de motif: – problèmes de système; – autre.
Confirmation		m	Code de confirmation: R0: autre; R1: succès; R2: abonné inconnu.

7.3.7 Fonction Avis de reprise de la surveillance FIGS

Dès que les ressources de surveillance du réseau visité sont rétablies après une situation de pénurie, la surveillance suspendue d'abonnés en itinérance est rétablie. Le HN-FDS en est informé.

Dans ce scénario, illustré à la Figure 11, le réseau visité informe le HN-FDS de sa décision de reprendre la surveillance, antérieurement suspendue, de l'abonné en itinérance.

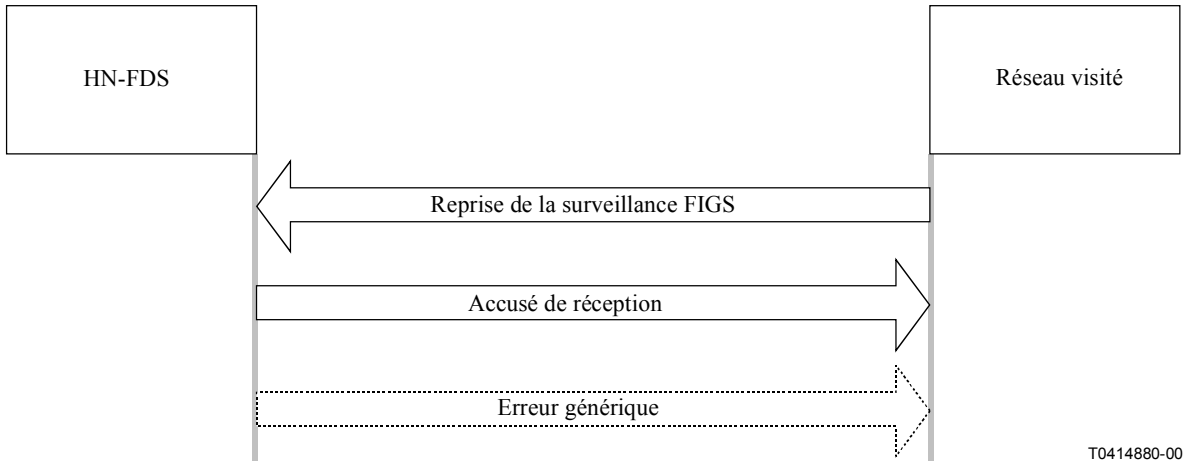

Figure 11/M.3210.1 – Flux de messages de la fonction avis de reprise de la surveillance FIGS

7.3.7.1 Flux d'information

Les informations d'avis de reprise de la surveillance FIGS échangées sont détaillées au Tableau 9.

Tableau 9/M.3210.1 – Informations de reprise de la surveillance FIGS échangées

	HN-FDS	Réseau visité	Remarques
Liste d'identification d'utilisateur 3G	m	m=	Liste d'identification unique de l'abonné hertzien (par exemple IMSI (identité internationale de station mobile) ou numéro de télécommunications personnelles universelles).
Numéro de série électronique	m	m=	Le numéro de série électronique du terminal de l'abonné tel que défini dans les normes de signalisation hertzienne.
Reprise du code de service	m		Code de motif: – système restauré; – autre.
Confirmation		m	Code de confirmation: R0: autre; R1: succès; R2: abonné inconnu.

ANNEXE A

Critères de gestion de la fraude

Les réseaux de gestion des télécommunications doivent être dotés des moyens de gestion appropriés pour détecter et analyser toute violation aux règles de sécurité et doivent comprendre des aspects de sécurité liés à la mobilité des utilisateurs. Des situations de détection d'utilisation frauduleuse peuvent être le résultat d'une:

- analyse des informations d'abonné collectées à propos d'un abonné suspecté de violations de mesures de sécurité, par exemple un simple clonage MIN/ESN (numéro d'identification du mobile/numéro de série électronique);
- analyse des informations de réseau collectées sur le réseau pour détecter une violation de sécurité suspectée;
- analyse de la structure d'utilisation de l'abonné révélant une variation significative par rapport aux structures d'utilisation habituelles;
- analyse du trafic interne et de la structure d'activité résultant de la détection d'une violation de mesure de sécurité par un abonné ou un utilisateur (externe ou interne).

L'utilisation frauduleuse peut être ou non la conséquence de l'une des incapacités détectées suivantes:

- incapacité du réseau à décrypter des messages cryptés de l'abonné;
- incapacité de l'abonné à produire des réponses correctes à des sollicitations d'authentification;
- discordances des valeurs signalées par l'abonné pour le paramètre "call-count" (décompte d'appels);
- rapports de défaillance signalant des difficultés à mettre à jour les données secrètes communes (SSD, *shared secret data*) des utilisateurs.

ANNEXE B

Informations transmises par le réseau visité

Information	Description
Numéros composés	Les **numéros composés** sont une information obligatoire car ils constituent un indicateur important permettant de décider si un appel est frauduleux ou non. Certaines destinations d'appel sont plus susceptibles d'être appelées frauduleusement que d'autres.
Abonné A	La mention **Abonné A** peut être utilisée pour identifier l'abonné.
Abonnés B, C	Les mentions **Abonnés B, C** sont pertinentes dans la mesure où certaines destinations d'appel sont plus sujettes à des fraudes que d'autres.
CGI	L'information identifiant global de cellule (**CGI**, *cell global identifier*) est pertinente dans la mesure où certaines cellules d'un réseau mobile terrestre public sont plus sujettes à des fraudes que d'autres.
IMSI	L'information **IMSI** (identité internationale d'abonné mobile) est utilisée pour faire référence à l'abonné.
IMEI	L'information **IMEI** (identificateur international d'équipement mobile) est utilisée pour vérifier si un combiné volé a été utilisé.
Heure/date de début d'appel	L'information **Heure/date de début d'appel** est nécessaire pour calculer la durée de l'appel (si l'heure de fin d'appel et non la durée d'appel est donnée en fin d'appel) et parce que l'heure de début d'appel peut également être un indicateur important de comportement frauduleux.
Durée d'appel	L'information **Durée d'appel** indique la durée de l'appel au moment de l'envoi des informations d'appel partielles. La durée d'appel peut être un indicateur important de comportement frauduleux. Si l'heure de fin d'appel est envoyée à la place, la durée peut être calculée au moyen des heures de début et de fin d'appel.
Référence d'appel	L'information **Référence d'appel** est utilisée pour faire référence à un appel particulier.
Indicateur MO/MT	L'information **Indicateur MO/MT** est nécessaire parce que la taxation de l'appel est différente selon qu'il s'agit d'un appel MO (au départ d'un mobile) ou MT (se terminant sur un mobile).
Adresse du MSC visité	L'information **Adresse du MSC visité** (centre de commutation pour système mobile) indique le réseau mobile terrestre public à partir duquel l'appel a été établi.
Type d'événement SS	L'information **Type d'événement SS** (service complémentaire) est envoyée si le début de "l'appel" correspond en fait à l'invocation d'un service complémentaire, par exemple ECT (transfert explicite de communication). L'information de type d'événement SS est nécessaire car elle peut indiquer si le mobile est utilisé de manière frauduleuse ou non.
Type de service de base	L'information **Type de service de base** signale si un téléservice ou un service support est utilisé, et, le cas échéant, le type de téléservice ou service support utilisé. Cette information est envoyée si l'événement est un appel et non un service complémentaire. L'information **Type de service de base** est nécessaire car elle peut indiquer si la station mobile est utilisée de manière frauduleuse ou non.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	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