RECOMMANDATION UIT-R M.1078

PRINCIPES DE SÉCURITÉ POUR LES TÉLÉCOMMUNICATIONS MOBILES INTERNATIONALES-2000 (IMT-2000)

(Question UIT-R 39/8)

(1994)

TABLE DES MATIÈRES

1. Introduction

Les télécommunications mobiles internationales-2000 (IMT-2000) sont des systèmes mobiles de la troisième génération (SMTG) dont l'entrée en service est prévue autour de l'an 2000 selon la conjoncture. Ils permettront d'accéder, au moyen d'une ou plusieurs liaisons radioélectriques, à un vaste éventail de services de télécommunication assurés par les réseaux du service fixe (par exemple, RTPC/RNIS), ainsi qu'à divers services mobiles spécifiques.

Ces systèmes font appel à différents types de stations mobiles reliées à des réseaux de Terre ou à des réseaux à satellites. Ces stations peuvent être conçues pour être utilisées en poste fixe ou en poste mobile.

Les principales caractéristiques des IMT-2000 sont les suivantes:

– une grande communauté de conception à l'échelle mondiale,

– une compatibilité des services au sein des IMT-2000 et avec les réseaux fixes,

– une qualité élevée,

– la possibilité d'utiliser dans le monde entier la même station de poche.

Les IMT-2000 sont définies dans une série de Recommandations de l'UIT interdépendantes dont la présente Recommandation qui est relative aux principes de sécurité.

Les IMT-2000 sont des systèmes complexes et leur représentation sous forme de Recommandations évolue. Afin de ne pas freiner les progrès accomplis dans ce domaine, il est préférable d'élaborer une série de Recommandations portant sur les divers aspects de ces systèmes tout en s'efforçant d'éviter les contradictions entre elles. Toutefois, si tel était le cas, ces contradictions seraient levées par de nouvelles Recommandations ou par la révision de Recommandations existantes.

Compte tenu de la nature même des communications sans fil, il faut doter les IMT-2000 de certaines sécurités pour rendre difficile une réception par des personnes autres que le destinataire prévu. De plus, en raison de la nature des communications mobiles des IMT-2000, des mesures de sécurité sont nécessaires pour éviter un accès frauduleux aux services.

2. Objet

La présente Recommandation a pour objet de préciser les principes et le cadre des dispositions de sécurité applicables aux IMT-2000 et les dispositions prises en la matière. Elle traite de tous les aspects relatifs à la sécurité pour les IMT-2000 et servira de base à d'autres Recommandations UIT-R ou UIT-T plus détaillées sur les spécifications des IMT-2000 en matière de sécurité à un stade ultérieur.

La présente Recommandation recense les exigences des IMT-2000 en matière de sécurité et définit les mesures à prendre en la matière. Elle contient également une Annexe d'information qui présente une analyse des menaces et des risques qui justifient les différentes mesures de sécurité qui sont exposées. Les exigences en matière de sécurité des systèmes évoqués dans la présente Recommandation n'impliquent pas qu'une responsabilité juridique incombe aux parties en cause en ce qui concerne la sécurité des communications et de l'information associée, ces questions étant du ressort de la législation nationale des pays.

En revanche, la présente Recommandation ne traite ni des mécanismes de sécurité envisageables pour les IMT-2000 ni de leurs conditions de leur mise en œuvre tout comme des procédures entre les différentes parties intervenant dans l'exploitation des IMT-2000, ni des algorithmes de sécurité, ces éléments devant faire l'objet de la future Recommandation UIT-R relative aux procédures de sécurité dans les IMT-2000. La gestion des mesures de sécurité sera traitée dans la future Recommandation UIT-R sur la gestion du réseau IMT-2000.

Les mesures relatives à la sécurité recommandées pour les IMT-2000 ainsi définies visent à garantir l'interfonctionnement avec les mobiles en déplacement à travers les frontières des réseaux internationaux et nationaux. Une certaine souplesse de mise en œuvre est prévue dans le cadre de ces contraintes.

Bien que des exigences en matière de sécurité et les fonctions de sécurité soient clairement considérées comme étant propres à l'accès radioélectrique, il en existe d'autres qui ne sont pas nécessairement en relation directe avec cet accès mais qui peuvent s'y rapporter par certains aspects; elles ont été incluses dans la présente Recommandation accompagnées de la mention «non nécessairement directement liées à l'interface radioélectrique».

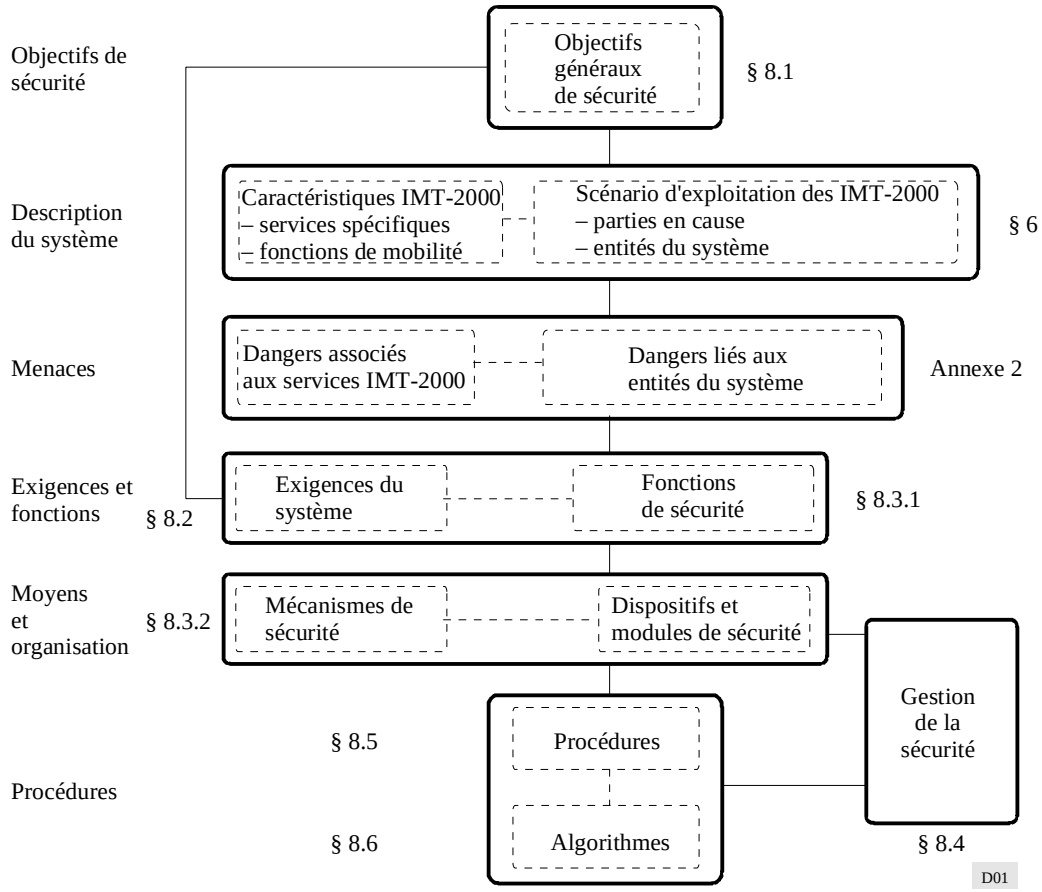
3. Structure de la Recommandation

La Fig. 1 présente la méthodologie associée à la présente Recommandation ainsi que sa structure. Le § 6 décrit le système IMT-2000 et identifie les parties qui interviennent dans les services IMT-2000. Le § 8.1 énonce les objectifs généraux en matière de sécurité, le § 8.2 spécifie les exigences auxquelles le système doit répondre en matière de sécurité et le § 8.3 recense les fonctions de sécurité offertes par les IMT-2000 et renvoie à la future Recommandation relative aux mécanismes de sécurité pour les IMT-2000.

Le § 8.4 fait référence aux futures Recommandations qui traiteront de la gestion des réseaux IMT-2000 et les § 8.5 et 8.6 se rapportent respectivement aux futures Recommandations sur les procédures de sécurité et sur les algorithmes de sécurité pour les IMT-2000. Enfin, l'Annexe 1 définit les termes utilisés dans la présente Recommandation et l'Annexe 2 analyse les menaces et les risques qui conditionnent les mesures de sécurité pour les IMT-2000. L'Annexe 3 donne la liste des procédures relatives à la sécurité que l'on peut envisager pour la future Recommandation sur les procédures de sécurité pour les IMT-2000.

FIGURE 1

Méthodologie et structure de la Recommandation



4. Documents de référence

Les documents de l'UIT suivants contiennent des renseignements sur les IMT-2000 en liaison avec la présente Recommandation:

– Recommandation UIT-R M.687: Télécommunications mobiles internationales-2000 (IMT-2000)

– Recommandation UIT-R M.816: Cadre de description pour des services assurés par les télécommunications mobiles internationales-2000 (IMT-2000)

– Recommandation UIT-R M.817: Télécommunications mobiles internationales-2000 (IMT-2000) – *Architectures de réseau*

– Recommandation UIT-R M.818: Utilisation des satellites dans les télécommunications mobiles internationales-2000 (IMT-2000)

– Recommandation UIT-R M.819: Télécommunications mobiles internationales-2000 (IMT-2000) au service des pays en développement

– Projet de Recommandation UIT-T F.115: Dispositions d'exploitation et de service relatives aux FSMTPT

– Recommandation UIT-R M.1034: Exigences imposées à la ou aux interfaces radioélectriques des télécommunications mobiles internationales-2000 (IMT-2000)

– Recommandation UIT-R M.1035: Cadre de description de la ou des interfaces radioélectriques et fonctionnalité des sous-systèmes radioélectriques pour les télécommunications mobiles internationales-2000 (IMT-2000)

– Recommandation UIT-R M.1036: Considérations relatives au spectre pour la mise en œuvre des télécommunications mobiles internationales-2000 (IMT-2000) dans les bandes 1 885-2 025 MHz et 2 110-2 200 MHz

– Recommandation UIT-R M.1079: Exigences imposées à la qualité de la parole et des données dans la bande vocale pour les télécommunications mobiles internationales-2000 (IMT-2000).

5. Définitions

L'Annexe 1 donne une liste partielle des définitions relatives à la présente Recommandation.

6. Description du système

6.1 Hypothèses du système concernant la sécurité

Les hypothèses et leur impact possible sur l'architecture de sécurité des IMT-2000 sont formulés ci-dessous:

a) les IMT-2000 seront exploitées dans un contexte faisant intervenir de nombreux exploitants de réseau et de nombreux fournisseurs de service, publics ou privés, qui seront pour certains en concurrence directe. On peut considérer que toutes les parties concernées auront leur propre politique de sécurité;

b) les IMT-2000 seront exploitées à travers les frontières des réseaux internationaux et nationaux et bénéficieront de possibilités de déplacement internationales et nationales;

c) les IMT-2000 auront une architecture ouverte, fondée sur les concepts de réseau intégré et le RGT;

d) les IMT-2000 permettent les télécommunications personnelles universelles (UPT);

e) les IMT-2000 offriront divers services sur une gamme de débits binaires. Plusieurs services pourront être utilisés simultanément et les services et/ou leur débit binaire pourront varier au cours de la communication;

f) les IMT-2000 utiliseront différents types de station et notamment des stations intégrées et des stations dotées d'interfaces standard pour connexion câblée avec d'autres terminaux standard;

g) les utilisateurs et les stations IMT-2000 sont logiquement identifiés par des identités uniques;

h) un utilisateur IMT-2000 a un profil de service personnel auquel il a directement accès. Ce profil contient les données personnelles de l'utilisateur IMT-2000 qui pourront être partiellement modifiées par lui ou par l'abonné IMT-2000. Les données du profil de service comprennent les services auxquels l'abonné IMT-2000 a souscrit pour l'utilisateur IMT-2000, ainsi que les diverses options d'abonnement et certains paramètres de service.

6.2 Scénario d'exploitation et parties logiquement en cause (parties logiques)

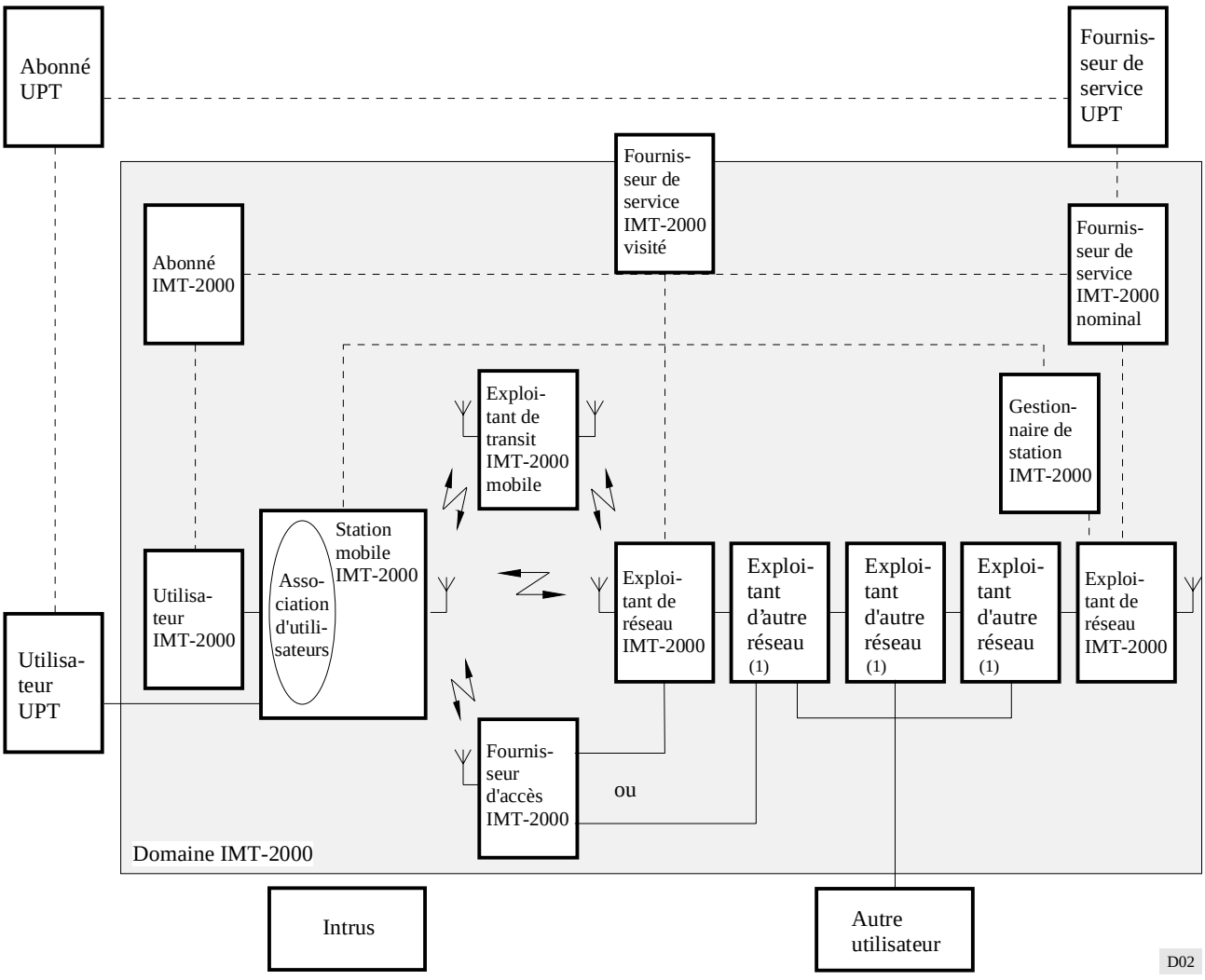
Le présent paragraphe décrit le scénario d'exploitation des IMT-2000 sur le plan de la sécurité et précise tous les intervenants logiques (dits parties logiques) dans l'exploitation normale du service IMT-2000, au niveau de son utilisation ou de sa fourniture. Ce scénario d'exploitation maximum est défini pour chaque intervenant logique, on dispose ainsi d'une certaine souplesse et ce scénario peut être adapté à la réglementation de différents pays ou de régions différentes.

On notera que ce scénario met en présence les parties (rôles) logiques qui interviennent dans l'utilisation et la fourniture du service IMT-2000 et pas d'entité juridique, personne ou machine réelle. C'est le scénario d'exploitation maximum et certains intervenants peuvent ne pas exister ou être regroupés sous une même entité. Par exemple, dans un environnement donné, le fournisseur de service IMT-2000 de rattachement ou visité et l'exploitant de réseau IMT-2000 peuvent appartenir à une même entité. Il convient en outre de noter que le scénario d'exploitation maximum a été déterminé afin de définir les exigences en matière de sécurité globale pour la fourniture et l'utilisation du service IMT-2000, et que sa définition détaillée ne fait pas nécessairement partie de la présente Recommandation dans tous les domaines, mais seulement dans ceux qui concernent la sécurité.

Le scénario d'exploitation maximum qui fait intervenir les parties en cause est illustré à la Fig. 2. Il convient de noter que les parties qui ne sont pas directement concernées par la fourniture et l'exploitation du service IMT-2000 au quotidien, par exemple les responsables de la réglementation ou les autorités chargées de l'homologation, ne sont pas prises en compte. Il convient par ailleurs de noter que la Fig. 2 représente le scénario général, c'est-à-dire le cas où un utilisateur IMT-2000 est appelé par un utilisateur (appel IMT-2000 entrant) et vice versa (appel IMT-2000 sortant). Le cas d'appels IMT-2000 de mobile à mobile est simplement une combinaison des deux et, dans un souci de simplicité, n'est pas inclus dans la Figure.

FIGURE 2

Scénario d'exploitation IMT-2000 et parties logiques intervenantes



(1) Ces exploitants peuvent se trouver ou non dans le domaine IMT-2000.

Le scénario d'exploitation maximum des parties en cause en ce qui concerne l'utilisation et la fourniture du service IMT-2000 comprend les parties logiques suivantes:

– les utilisateurs IMT-2000,

– les stations mobiles IMT-2000,

– les abonnés IMT-2000,

– les fournisseurs de service IMT-2000 de rattachement,

– les fournisseurs de service IMT-2000 visités,

– les exploitants du réseau IMT-2000,

– le gestionnaire du terminal IMT-2000,

– les exploitants de transit IMT-2000 mobiles,

– les fournisseurs d'accès aux IMT-2000,

– les autres exploitants de réseau;

– les autres utilisateurs,

– les intrus.

Il faut noter que les IMT-2000 permettent des déplacements internationaux avec accès local aux ressources radioélectriques et que, par conséquent, le fournisseur de service IMT-2000 visité pourra intervenir dans une communication, en plus du fournisseur de service IMT-2000 de rattachement. De plus, comme les IMT-2000 sont compatibles avec les télécommunications personnelles universelles, les parties suivantes peuvent également intervenir:

– les utilisateurs UPT,

– les abonnés UPT,

– les fournisseurs de service UPT.

Dans les paragraphes suivants, les responsabilités et fonctions de ces parties IMT-2000 (domaines de sécurité) sont définies pour l'angle de la sécurité, ce qui n'exclut pas que ces parties aient d'autres responsabilités et fonctions non liées à la sécurité.

6.2.1 Rôle du fournisseur de service IMT-2000 de rattachement

Le rôle du fournisseur de service IMT-2000 de rattachement est de fournir des services aux utilisateurs IMT-2000, sous réserve des restrictions de capacité de service des réseaux IMT-2000 qui participent à la fourniture du service et de traiter toutes les informations relatives à l'abonnement concernant un utilisateur IMT-2000. Un ensemble d'identités d'utilisateur appartiennent au fournisseur de service IMT-2000 de rattachement.

Dans le cadre de ses attributions, le fournisseur de service IMT-2000 de rattachement doit mettre en correspondance les numéros IMT-2000 avec l'identité des utilisateurs IMT-2000 et/ou avec l'identité des stations mobiles IMT-2000.

Note 1 – Les conséquences concernant l'utilisation frauduleuse des identités de station et leurs liens avec les identités d'utilisateur sont un point essentiel qui appelle un complément d'étude.

L'association d'un numéro IMT-2000 et d'une identité de l'utilisateur IMT-2000 est toujours statique, à moins que les abonnements ou les plans de numérotage IMT-2000 n'aient été administrativement modifiés; en revanche, l'association d'une identité de l'utilisateur IMT-2000 et d'une identité de station mobile IMT-2000 peut être statique ou dynamique pendant l'exploitation normale de l'IMT-2000 selon le choix du fournisseur de service IMT-2000 de rattachement et de ses abonnés. L'identité d'utilisateur IMT-2000 dans le cas de plusieurs utilisateurs IMT-2000 peut être mise en correspondance avec l'identité d'une seule station mobile IMT-2000.

Note 2 – L'importante question de savoir s'il est utile de permettre à plusieurs utilisateurs IMT-2000 d'être associés simultanément avec une identité de station mobile IMT-2000 – ce qui est par ailleurs possible pour les utilisateurs UPT – appelle un complément d'étude. La situation est différente selon qu'il s'agit d'appels IMT-2000 entrants ou sortants. En ce qui concerne ces derniers, un seul utilisateur IMT-2000 peut être associé à un instant donné à une identité de station, puisqu'un seul appel IMT-2000 sortant ne peut être émis à un instant donné à partir d'une station mobile IMT-2000. Pour les appels entrants, la situation est différente, et on peut envisager que plusieurs utilisateurs IMT-2000 soient associés simultanément à une même identité de station mobile IMT-2000.

Le fournisseur de service IMT-2000 de rattachement peut utiliser soit l'identité de l'utilisateur IMT-2000 soit celle de la station mobile IMT-2000 pour la communication avec le fournisseur de service IMT-2000 visité, afin d'atteindre respectivement l'utilisateur ou la station mobile IMT-2000.

Le fournisseur de service IMT-2000 de rattachement utilise l'identité de la station mobile IMT-2000 pour communiquer avec l'exploitant du réseau IMT-2000 afin d'atteindre l'utilisateur IMT-2000. Il faut noter que les exploitants de réseau IMT-2000 ne connaissent pas nécessairement l'identité des utilisateurs IMT-2000.

Le fournisseur de service IMT-2000 de rattachement est responsable de l'authentification des utilisateurs IMT-2000 et de la gestion de l'information d'authentification des utilisateurs. Le fournisseur de service IMT-2000 de rattachement peut refuser aux utilisateurs et abonnés IMT-2000 l'accès aux services dans certains cas.

Les fournisseurs de service IMT-2000 de rattachement ont conclu des accords concernant les utilisateurs itinérants avec plusieurs fournisseurs de service IMT-2000 visités. Des mécanismes de sécurité devront être mis en place dans les IMT-2000 afin que le fournisseur de service IMT-2000 de rattachement et le fournisseur de service IMT-2000 visité puissent échanger librement des informations.

Note 3 – La définition des liens entre exploitants de réseaux et fournisseurs de service et leurs responsabilités respectives pour ce qui est des utilisateurs itinérants appellent un complément d'étude.

6.2.2 Rôle du fournisseur de service IMT-2000 visité

Le fournisseur de service IMT-2000 visité a un accord concernant les utilisateurs itinérants avec le fournisseur de service IMT-2000 de rattachement et il lui incombe d'aider les utilisateurs IMT-2000 du fournisseur de service IMT-2000 de rattachement qui se déplacent dans le réseau d'un exploitant de réseau IMT-2000 ayant une connexion directe avec lui.

6.2.3 Rôle de l'exploitant de réseau IMT-2000

L'exploitant de réseau IMT-2000 est chargé d'assurer un accès au réseau aux stations mobiles IMT-2000 et d'offrir des possibilités de service aux utilisateurs IMT-2000 qui se déplacent dans son réseau; il traite aussi toute information liée aux communications pour toutes les stations mobiles et utilisateurs IMT-2000 qui se trouvent dans ses zones de couverture.

Il est responsable de:

– la gestion des positions,

– l'attribution des numéros d'acheminement temporaires.

L'exploitant de réseau IMT-2000 traite certaines informations d'utilisateur et d'abonnement IMT-2000 lorsque des utilisateurs IMT-2000 se déplacent dans son réseau. Néanmoins, cette information se limite aux renseignements nécessaires pour une exploitation normale et elle n'est qu'indirectement associée à l'identité des utilisateurs IMT-2000.

L'identité des utilisateurs IMT-2000 ne relève pas logiquement de la responsabilité de l'exploitant de réseau IMT-2000; cet exploitant ne connaît donc pas nécessairement les numéros IMT-2000 ou l'identité explicite des utilisateurs IMT-2000.

L'exploitant de réseau IMT-2000 est toutefois responsable de l'exploitation et du fonctionnement corrects des stations mobiles IMT-2000 qui accèdent à son réseau. Le cryptage et le décryptage des informations d'interface radioélectrique IMT-2000 sont également exécutés localement par l'exploitant de réseau IMT-2000.

6.2.4 Rôle du gestionnaire des stations IMT-2000

Le gestionnaire des stations IMT-2000 est responsable de l'identité des stations mobiles IMT-2000 et en dernier ressort, de l'authentification de ces stations et de la gestion de l'information d'authentification des stations. Il peut enregistrer l'identité de ces stations, afin de faciliter le refus d'accès aux services dans certains cas.

Ce gestionnaire peut être indépendant ou dépendant du fournisseur de service IMT-2000 ou de l'exploitant du réseau IMT-2000.

La décision concernant le rôle du gestionnaire des stations IMT-2000 appelle un complément d'étude.

Note 1 – L'utilisation du gestionnaire des stations IMT-2000 et d'une identité de station mobile IMT-2000 pour la gestion de mobilité et à d'autres fins, ainsi que son authentification appellent un complément d'étude. Il n'a pas encore été décidé s'il y a lieu de recommander plutôt d'autres réalisations techniques. Les avantages et le coût des solutions possibles devront être évalués avant de prendre une décision.

6.2.5 Autres exploitants de réseau

On distingue plusieurs catégories d'autres exploitants de réseau:

– les exploitants de réseau du service fixe intermédiaire, situé entre le fournisseur de service IMT-2000 de rattachement et l'exploitant de réseau IMT-2000 (par exemple, un exploitant du réseau de transit), ou

– les exploitants de réseau du service fixe intermédiaire entre l'exploitant du réseau du service fixe de départ ou celui du réseau fixe de destination et l'exploitant de réseau IMT-2000 (par exemple, un exploitant du réseau de transit), ou encore

– l'exploitant du réseau du service fixe de départ ou de destination (par exemple, exploitant du réseau local).

Quelle que soit la catégorie de ces autres exploitants de réseau, ils n'ont pas nécessairement besoin d'avoir connaissance pour chaque communication des informations relatives à la sécurité des IMT-2000 et ils ne sont pas activement concernés par les procédures de sécurité applicables aux IMT-2000 pour chaque appel. Les informations relatives à la sécurité des IMT-2000:

– ne seront jamais transmises à travers les réseaux de ces exploitants, ou

– seront protégées lors de leur passage dans ces réseaux, ou encore

– n'auront aucune signification pour ces réseaux.

6.2.6 Rôle de l'exploitant de transit IMT-2000 mobile

On distingue deux catégories d'exploitant de transit IMT-2000 mobile:

– l'opérateur d'une station mobile de base (par exemple dans les autobus, les trains, les navires, etc.), ou

– l'exploitant d'une IMT-2000 par satellite (secteur spatial).

Les exploitants de transit IMT-2000 mobiles retransmettent toujours dans les deux sens en transparence les informations relatives à la sécurité. L'information cryptée ne sera pas décryptée par l'exploitant de transit IMT-2000 mobile. Celui-ci n'aura pas accès aux clés ou aux algorithmes d'authentification ou de cryptage; il convient donc de le considérer comme une tierce partie à l'interface radioélectrique IMT-2000 ou comme appartenant à une catégorie d'autres exploitants de réseau du point de vue de la sécurité.

Note 1 – Selon ces principes, un exploitant de transit mobile est une entité indépendante de l'exploitant de réseau IMT-2000 (par exemple, l'exploitant de transit mobile pourrait être l'exploitant d'un secteur spatial de satellite, l'exploitant de réseau IMT-2000 étant l'exploitant du secteur terrien de satellite). On notera que ces deux entités peuvent également n'en constituer qu'une. Cependant, dans ce cas, l'exploitant de transit IMT-2000 mobile est simplement un autre exploitant de réseau IMT-2000.

6.2.7 Rôle du fournisseur d'accès IMT-2000

Le fournisseur d'accès IMT-2000 est chargé d'assurer l'accès radioélectrique IMT-2000 aux utilisateurs IMT-2000 dans une zone de couverture limitée, mais il n'assure pas de fonctions de mobilité dans une zone étendue. Pour fournir une capacité de mobilité en dehors de sa zone de couverture, le fournisseur d'accès IMT-2000 doit s'adresser à un exploitant de réseau IMT-2000.

Note 1 – Un fournisseur d'accès IMT-2000 pourra être, par exemple, un hôtel ou une société offrant un accès hertzien au IMT-2000 à ses clients ou à son personnel. Un fournisseur d'accès IMT-2000 peut être également un exploitant IMT-2000 national (utilisateur national de téléphone sans cordon).

Le fournisseur d'accès IMT-2000 peut avoir conclu des accords avec un exploitant de réseau IMT-2000 ou avec un exploitant de réseau du service fixe, selon les fonctions et la mobilité requises. Du point de vue de la sécurité, le fournisseur d'accès IMT-2000 exécute toutes les fonctions qui incomberaient autrement à l'exploitant de réseau IMT-2000.

Note 2 – En principe, les fournisseurs d'accès (par exemple, dans le cas d'utilisateurs de téléphone sans cordon nationaux) peuvent avoir des stations mobiles ou des utilisateurs mobiles qui ne sont pas rattachés à un fournisseur de service IMT-2000 ou à un gestionnaire de station IMT-2000. Dans ce cas, ces stations mobiles ou utilisateurs mobiles ne possèdent pas de numéro IMT-2000 ou d'identité d'utilisateur ou de station mobile IMT-2000, et ne font donc pas partie du système IMT-2000 global. Un fournisseur de service IMT-2000 de rattachement et un gestionnaire de stations IMT-2000 sont toujours associés pour l'exploitation des IMT-2000.

6.2.8 Station mobile IMT-2000

Les stations mobiles IMT-2000 sont sur le marché libre et possèdent une identité de station mobile IMT-2000 qui leur est propre. Cette identité peut être assignée par le gestionnaire de stations IMT-2000 au moment de l'enregistrement ou attribuée à l'avance.

Les stations mobiles IMT-2000 peuvent effectuer le cryptage et le décryptage de l'information d'interface radioélectrique IMT-2000.

6.2.9 Utilisateur IMT-2000

Un utilisateur IMT-2000 est associé à un abonné IMT-2000.

Un utilisateur IMT-2000 possède sa propre identité d'utilisateur IMT-2000, qui lui est assignée par le fournisseur de service IMT-2000 de rattachement au moment de la souscription de l'abonnement et qui ne peut être modifiée, sauf lors de modifications administratives apportées à l'abonnement. L'utilisateur IMT-2000 a également son propre numéro IMT-2000.

L'utilisateur IMT-2000 peut souhaiter avoir accès à son profil de service IMT-2000 personnel pour obtenir une information d'état ou modifier des paramètres de service. Cette capacité suppose un accès interactif en temps réel aux données du profil de service du fournisseur de service IMT-2000 de rattachement, et l'authentification de l'utilisateur IMT-2000 dont les détails appellent un complément d'étude.

6.2.10 Association de l'utilisateur

L'association de l'utilisateur avec la station mobile IMT-2000 s'accompagne de l'aptitude du fournisseur de service IMT-2000 de rattachement à authentifier l'utilisateur IMT-2000; elle doit donc être commode pour l'utilisateur.

Un exemple de réalisation de l'association de l'utilisateur est fourni par l'emploi du module d'identité d'utilisateur (UIM) qui est logiquement remis à l'utilisateur IMT-2000 par le fournisseur de service IMT-2000 de rattachement au moment de l'abonnement. L'UIM contient au minimum l'identité de l'utilisateur IMT-2000, la clé de son authentification et les données destinées au contrôle du détenteur de l'UIM; il peut contenir en outre l'algorithme d'authentification de l'utilisateur. L'UIM pourra être intégré dans la station mobile IMT-2000 ou être amovible.

L'association de l'utilisateur avec la station mobile IMT-2000 pourrait être facilitée par les capacités du réseau (exemple: reconnaissance vocale pour authentifier l'utilisateur et déterminer son identité). La reconnaissance vocale pourrait incomber à l'exploitant du réseau IMT-2000 ou au fournisseur de service IMT-2000, tandis que l'information de clé d'authentification de l'utilisateur se trouve chez le fournisseur de service IMT-2000 de rattachement.

6.2.11 Abonné IMT-2000

Un abonné IMT-2000 est responsable des taxes occasionnées par ses utilisateurs IMT-2000 associés. Un abonné IMT-2000 est associé avec un ou plusieurs utilisateurs IMT-2000, mais il s'agit d'une relation purement administrative et l'abonné IMT-2000 n'intervient pas dans le fonctionnement normal des IMT-2000.

L'abonné IMT-2000 peut posséder une identité d'abonné IMT-2000 et souhaiter avoir accès aux profils de service des utilisateurs IMT-2000 qui lui sont associés, individuellement ou en bloc, afin d'obtenir une information d'état ou de modifier des paramètres de service pour les utilisateurs IMT-2000 qui lui sont associés. Cela implique un accès interactif limité en temps réel aux données du profil d'utilisateur du fournisseur de service IMT-2000 de rattachement et l'authentification de l'abonné IMT-2000 est ici nécessaire. Les modalités d'accès appellent un complément d'étude.

6.2.12 Autres utilisateurs

On distingue deux catégories d'autres utilisateurs:

– ceux qui établissent des communications avec des utilisateurs IMT-2000 (les demandeurs), ou

– ceux qui reçoivent des communications d'utilisateurs IMT-2000 (les demandés).

Quelle que soit leur catégorie, les autres utilisateurs n'ont pas connaissance des informations relatives à la sécurité des IMT-2000 et n'interviennent pas dans les procédures de sécurité des IMT-2000 sauf dans des cas spécifiques.

Parmi ces cas spécifiques, on peut citer certaines interactions entre les services de sécurité attendus par l'autre utilisateur et ceux offerts à l'utilisateur IMT-2000.

6.2.13 Intrus

Les intrus sont des parties qui trompent le réseau ou les services IMT-2000 dans le but d'accéder aux informations confidentielles relatives aux utilisateurs IMT-2000 ou de frauder les fournisseurs de service, les exploitants de réseau, les gestionnaires de stations IMT-2000 ou d'autres parties logiques.

6.2.14 Utilisateur d'UPT

Relié aux IMT-2000, l'utilisateur d'UPT accède aux services UPT par l'intermédiaire d'une interface radio-électrique IMT-2000.

Les méthodes d'accès au service UPT via une interface radioélectrique IMT-2000 n'entrent pas dans le cadre des IMT-2000; elles sont décrites dans les Recommandations UIT-T F.850 et UIT-T F.851.

6.2.15 Abonné UPT

L'abonné UPT est défini dans les Recommandations UIT-T F.850 et UIT-T F.851. Un abonné UPT n'a pas de connexion directe avec les IMT-2000.

6.2.16 Fournisseur de service UPT

Les Recommandations UIT-T F.850 et UIT-T F.851 définissent le fournisseur de service UPT. En ce qui concerne les IMT-2000, les fournisseurs de service UPT ont conclu des accords avec les fournisseurs de service IMT-2000 pour la fourniture de services UPT par l'intermédiaire des réseaux IMT-2000.

7. Considérations

Lors de l'élaboration de cette Recommandation, les facteurs ci-après ont été pris en considération:

a) la nécessité d'offrir pour les IMT-2000 une qualité de service des IMT-2000 analogue à celle offerte par le RTPC ou le RNIS;

b) l'importance croissante des divers types de services non téléphoniques;

c) la facilité de réception par des tiers non destinataires des communications hertziennes compte tenu de la nature même de ces communications;

d) la nécessité de prendre au minimum des dispositions concrètes dans les IMT-2000 afin d'assurer le secret des communications à l'interface radioélectrique et d'empêcher toute utilisation frauduleuse du service;

e) la description générale du système donnée au § 6;

f) les Recommandations UIT-T et UIT-R pertinentes et les travaux en cours;

g) le recours aux satellites pour les IMT-2000 susceptibles de faciliter la mise en place de services de télécommunication dans les pays en développement;

h) la nécessité d'une structure adaptable pour le système permettant d'ajuster les investissements dans le réseau à la croissance des recettes et de s'adapter facilement à l'environnement et de répondre aux nouveaux développements sans faire obstacle aux innovations;

j) la mobilité nécessaire des stations mobiles (dont celles qui utilisent les satellites) qui doivent pouvoir se déplacer d'un réseau de télécommunication mobile à l'autre d'un pays à l'autre;

k) la nécessité pour les IMT-2000 de fonctionner dans des environnements très divers avec des caractéristiques de propagation, des densités de trafic et des mobilités différentes;

l) la possibilité d'augmenter sensiblement la couverture globale et l'attrait des services IMT-2000 grâce à l'utilisation de satellites.

8. Recommandations

L'Assemblée des radiocommunications de l'UIT recommande d'appliquer les principes de sécurité suivants aux IMT-2000.

8.1 Objectifs généraux de sécurité

Les objectifs généraux suivants sont applicables à la sécurité des IMT-2000:

– la sécurité offerte à un utilisateur IMT-2000 doit être comparable à celle qu'offrent les réseaux du service fixe à la même époque;

– la sécurité offerte à un fournisseur de service ou un exploitant de réseau IMT-2000 doit être comparable à celle qu'offrent les réseaux du service fixe à la même époque;

– les aspects juridiques, réglementaires et commerciaux de la sécurité offerte aux IMT-2000 doivent être compatibles avec une disponibilité à l'échelon mondial;

– la sécurité offerte par les IMT-2000 doit être suffisamment normalisée pour permettre un interfonctionnement et une mobilité dans le monde entier entre différents fournisseurs de service ou exploitants de réseau;

– des dispositions doivent être prises pour qu'une interception légale des communications radioélectriques d'un utilisateur soit possible dans le cadre de la législation nationale;

– les IMT-2000 ne devraient pas utiliser des dispositions de sécurité propres au type d'interface radioélectrique, de manière que tous les types d'interface radioélectrique puissent être utilisés sans nuire à la sécurité et au secret.

8.2 Exigences du système en matière de sécurité

Le présent paragraphe donne la liste des exigences du système en matière de sécurité, lesquelles s'appliquent à une ou plusieurs des parties intervenant dans le service IMT-2000.

D'une manière générale, ces exigences peuvent intéresser un ou plusieurs éléments suivants:

– confidentialité,

– authentification,

– intégrité,

– autorisation et contrôle d'accès,

– secret et anonymat,

– disponibilité du service,

– limitation de l'événement,

– signalisation de l'événement.

Les exigences du système en matière de sécurité des IMT-2000 sont regroupées dans les catégories suivantes:

– exigences liées au service,

– exigences liées à l'accès,

– exigences liées à l'interface radioélectrique,

– exigences liées aux stations,

– exigences liées à l'association de l'utilisateur,

– exigences liées à la taxation,

– exigences liées à l'exploitation du réseau,

– exigences liées à la gestion de la sécurité.

8.2.1 Exigences liées au service

En ce qui concerne les exigences de sécurité des IMT-2000 liées au service, il faut que:

– les fonctions de sécurité offertes pour la protection des utilisateurs IMT-2000 soient faciles à utiliser et si possible, transparentes pour les utilisateurs tout en demandant une intervention minimale des utilisateurs à chaque communication;

– les fonctions de sécurité offertes pour la protection des utilisateurs IMT-2000 n'augmentent pas notablement le temps d'établissement des communications;

– les fonctions de sécurité offertes pour la protection des utilisateurs IMT-2000 ne soient pas moindres pendant les transferts ou lors des déplacements;

– les fonctions de sécurité offertes par les IMT-2000 soient compatibles avec les divers environnements radioélectriques des IMT-2000 et ne soient pas restreintes par une couche physique ou par une méthode d'accès;

– le secret des communications pour des utilisateurs autres que ceux des IMT-2000 ne soit pas remis en cause par l'utilisation d'équipements ou de services IMT-2000;

– l'on puisse, dans des cas bien précis, transmettre en clair une information sur la voie support des IMT-2000. En cas de défaillance de cryptage, des transmissions d'urgence identifiées devraient être autorisées en clair sur la voie de données;

– les fonctions de sécurité pour les IMT-2000 aient un impact minimal sur la capacité de l'interface radioélectrique en ce qui concerne l'écoulement du trafic pour le service de l'utilisateur.

8.2.2 Exigences liées à l'accès

En ce qui concerne les exigences de sécurité des IMT-2000 liées à l'accès:

– il doit être pratiquement impossible pour des intrus de se faire passer pour l'utilisateur ou l'abonné IMT-2000;

– il doit être pratiquement impossible pour des intrus de se faire passer pour un fournisseur de service ou exploitant de réseau IMT-2000 lors d'une communication avec un utilisateur IMT-2000 ou avec un autre fournisseur de service IMT-2000;

– il doit être pratiquement impossible pour des intrus à une interface radioélectrique IMT-2000 de restreindre volontairement la disponibilité des services offerts à un utilisateur IMT-2000;

– il doit être pratiquement impossible pour des intrus de «pirater», à une interface radioélectrique IMT-2000, une voie de trafic déjà utilisée par un utilisateur IMT-2000;

– il doit être pratiquement impossible pour des intrus de manipuler, à une interface radioélectrique IMT-2000, une information d'utilisateur ou de commande transmise et de transformer cette information en une information choisie par eux;

– il doit être pratiquement impossible pour des intrus d'accéder aux informations d'abonnement enregistrées de l'utilisateur (informations qui ne sont pas nécessairement liées à l'interface radioélectrique), de les lire ou de les modifier;

– la fourniture de service IMT-2000 doit intégrer des mécanismes pour prouver la validité et l'authenticité des transactions effectuées avec des utilisateurs IMT-2000;

– il doit être pratiquement impossible pour des intrus d'accéder à la structure de signalisation du réseau IMT-2000 et aux fonctions de commande corrélatives ou d'y insérer de fausses commandes.

8.2.3 Exigences liées à l'interface radioélectrique

En ce qui concerne les exigences de sécurité des IMT-2000 au niveau des interfaces radioélectriques:

– il doit être pratiquement impossible de décoder la communication d'un utilisateur IMT-2000 à une interface radioélectrique IMT-2000. Cela est valable pour tout type d'information de service (téléphonique, texte, données, etc.) ou de signalisation;

– il doit être pratiquement impossible pour des intrus de déterminer physiquement la position de l'utilisateur IMT-2000 par une interception à une interface radioélectrique IMT-2000;

– il doit être pratiquement impossible pour des intrus d'identifier, grâce à une interception à une interface radioélectrique IMT-2000, l'utilisateur IMT-2000 associé à une communication donnée;

– il doit être pratiquement impossible pour des intrus d'intercepter une information de signalisation ou de commande à une interface radioélectrique IMT-2000.

8.2.4 Exigences liées aux stations

En ce qui concerne les exigences des IMT-2000 au niveau des stations:

– il doit être possible pour le fournisseur de service ou l'exploitant de réseau IMT-2000 d'identifier une station mobile IMT-2000 non autorisée ou volée de consigner cette information et d'empêcher l'accès aux services pour cet équipement;

– il doit être possible pour le fournisseur de service ou l'exploitant de réseau IMT-2000 de déceler l'existence d'une station mobile IMT-2000 clonée et de l'empêcher d'accéder aux services;

– il doit être pratiquement impossible pour des intrus d'obtenir l'identité de stations mobiles IMT-2000 et en particulier l'information d'authentification d'une station mobile IMT-2000;

– il doit être possible pour l'exploitant de réseau IMT-2000 de déceler et d'empêcher l'utilisation d'une station mobile IMT-2000 dont le type n'est pas homologué par cet exploitant;

– il doit être possible pour un exploitant de réseau IMT-2000 d'identifier une station mobile IMT-2000 en dérangement, de consigner cette information et d'empêcher l'utilisation de cet équipement.

Note 1 – L'utilisation de l'identité d'une station mobile pour son authentification, pour la gestion des déplacements et à d'autres fins appelle un complément d'étude. On n'a pas encore décidé s'il convenait de recommander d'autres exigences. Les avantages et le coût de solutions éventuelles devront être évalués avant qu'une décision soit prise.

Note 2 – On entend par station mobile IMT-2000 clonée une station mobile ayant exactement la même identité de station mobile et la même clé d'authentification que la station mobile IMT-2000 autorisée. Une station mobile IMT-2000 de type homologué est un équipement mobile qui est autorisé à accéder au réseau du point de vue de la réglementation.

8.2.5 Exigences liées à l'association de l'utilisateur

Lorsque l'association utilisateur-station mobile IMT-2000 est assurée par un dispositif situé du côté utilisateur – par le module d'identité d'utilisateur (UIM), par exemple – il faut pour cette association respecter les exigences suivantes (on considère ici que le dispositif est un UIM):

– le fournisseur de service IMT-2000 doit pouvoir identifier les UIM volés (ce sont des stations mobiles IMT-2000 volées lorsque l'UIM est intégré dans ces stations) puis consigner cette information et empêcher l'utilisation de ces UIM (stations mobiles);

– le fournisseur de service IMT-2000 doit pouvoir déceler les UIM clonés et empêcher pour ces clones l'accès aux services;

– le fournisseur de service IMT-2000 doit pouvoir authentifier directement ou indirectement la personne qui utilise l'UIM;

– il doit être pratiquement impossible pour des intrus de lire illicitement l'information de sécurité associée à l'utilisateur IMT-2000 contenue dans un UIM;

– il doit être pratiquement impossible pour des intrus d'écrire illicitement l'identité de l'utilisateur IMT-2000 et son information de sécurité corrélative dans un UIM.

Lorsque l'association utilisateur-station mobile IMT-2000 est assurée par le réseau, par exemple, par reconnaissance vocale, il faut respecter de nouvelles exigences spécifiques, à savoir:

– il devrait être très difficile pour des intrus de se faire passer pour des utilisateurs IMT-2000,

– les autres exigences appellent un complément d'étude.

8.2.6 Exigences liées à l'exploitation du réseau

Les exigences de sécurité liées à l'exploitation du réseau et applicables aux IMT-2000 sont les suivantes:

– la sécurité offerte par les IMT-2000 doit être suffisamment normalisée pour assurer un interfonctionnement international et une mobilité internationale fiables. Cependant, les mécanismes de sécurité des IMT-2000 devraient être aussi peu contraignants que possible tout en laissant aux parties concernées une marge de manœuvre maximale dans le choix de leurs propres politiques de sécurité;

– les mécanismes de sécurité des IMT-2000 devraient exiger le moins possible de connexions de signalisation à longue distance en temps réel (par exemple, afin d'éviter la présence de connexions de signalisation internationales à chaque réactualisation des positions ou pour chaque communication pendant les déplacements).

8.2.7 Exigences liées à la gestion de la sécurité

Les exigences de sécurité liées à la gestion de la sécurité applicables aux IMT-2000 sont les suivantes:

– les clés et les dispositifs éventuels de sécurité, comme l'UIM le cas échéant, remis aux utilisateurs IMT-2000 devraient être aisément gérés et actualisés de manière fiable;

– les clés de sécurité devraient être gérées de manière sûre par les fournisseurs de service IMT-2000 et aussi entre fournisseurs;

– le fournisseur de service IMT-2000 devrait disposer de mécanismes sûrs pour consigner les événements concernant les utilisateurs ou les abonnés IMT-2000;

– il devrait être très difficile pour des intrus de se faire passer pour un fournisseur de service IMT-2000 en communication avec des exploitants de réseau IMT-2000 et réciproquement;

– les mécanismes de sécurité offerts par les IMT-2000 devraient permettre la gestion des versions, et leur mise à jour devrait être facile.

8.3 Sécurité assurée par les IMT-2000

8.3.1 Fonctions de sécurité

Le présent paragraphe décrit les fonctions de sécurité offertes par les IMT-2000. Ces fonctions peuvent faire partie intégrante du service IMT-2000 ou constituer un service spécifique de sécurité des IMT-2000.

Les fonctions de sécurité correspondent en général à au moins l'un des pouvoirs suivants:

– pouvoir de prévention,

– pouvoir de signalisation,

– pouvoir de limitation,

– pouvoir de rétablissement,

– pouvoir dissuasif.

Les fonctions de sécurité ont été classées en fonctions essentielles ou facultatives et également en deux autres catégories, selon qu'elles sont liées à l'utilisateur ou au fournisseur de service.

Les fonctions liées à l'utilisateur présentent un avantage direct pour les utilisateurs IMT-2000 en matière de sécurité, tandis que celles liées au fournisseur de service sont offertes aux fournisseurs de service IMT-2000 pour les besoins de la sécurité générale du système, besoins qui ne concernent qu'indirectement les utilisateurs IMT-2000.

Note 1 – Toutes ces fonctions de sécurité appellent un complément d'étude. Leur inclusion éventuelle dépendra des résultats de l'analyse des menaces et des risques figurant à l'Annexe 2 ainsi que des décisions ultérieures concernant les IMT-2000.

8.3.1.1 Fonctions de sécurité liées à l'utilisateur

8.3.1.1.1 Fonctions de sécurité essentielles relatives à l'utilisateur

Les IMT-2000 offrent les fonctions de sécurité essentielles suivantes, relatives à l'utilisateur:

– **Contrôle d'accès aux données relatives aux abonnements**: des restrictions sont imposées à l'accès aux données personnelles d'un utilisateur IMT-2000 ou d'un abonné IMT-2000 stockées dans le réseau.

– **Contrôle d'accès aux données de profil de service**: des restrictions sont imposées à l'accès au profil de service personnel d'un utilisateur IMT-2000 ou d'un abonné IMT-2000 stocké dans le réseau.

– **Autorisation d'action pour l'utilisateur**: les diverses actions d'un utilisateur IMT-2000 sont soumises à des restrictions plus ou moins importantes. L'utilisateur IMT-2000 doit donc obtenir pour ses actions les autorisations nécessaires.

– **Autorisation d'action pour les stations**: les différentes actions effectuées par une station mobile IMT-2000 sont soumises à des restrictions plus ou moins importantes. La station mobile IMT-2000 doit donc obtenir les autorisations nécessaires pour ses actions.

– **Confidentialité des données de l'utilisateur**: les données d'un utilisateur IMT-2000 sont protégées contre leur divulgation à l'interface radioélectrique IMT-2000. Cette fonction s'applique aux signaux vocaux comme à tout autre type de données d'utilisateur.

– **Confidentialité de l'information de signalisation**: les informations de signalisation sont protégées contre leur divulgation à une interface radioélectrique IMT-2000.

– **Confidentialité de l'identité de l'utilisateur**: l'identité d'un utilisateur IMT-2000 est protégée contre sa divulgation à une interface radioélectrique IMT-2000.

– **Confidentialité de la position de l'utilisateur**: la position physique d'un utilisateur IMT-2000 est protégée contre sa divulgation à une interface radioélectrique IMT-2000.

– **Authentification de l'identité de l'utilisateur**: l'identité de l'utilisateur IMT-2000 est reconnue après vérification comme étant celle annoncée.

– **Authentification de l'identité de la station**: l'identité d'une station mobile IMT-2000 est reconnue, après vérification comme étant celle annoncée. Cette fonction peut être utilement assurée par l'authentification de l'identité de l'utilisateur.

– **Vérification du détenteur de l'UIM**: la personne qui utilise l'UIM est authentifiée. Cette fonction est uniquement applicable au cas où l'UIM est utilisé pour l'association utilisateur-station mobile IMT-2000.

– **Intégrité des données de transaction**: l'utilisateur et le fournisseur de service IMT-2000 sont pratiquement sûrs que les données transmises par l'autre extrémité de la communication au cours d'une transaction n'ont pas été modifiées pendant leur acheminement.

– **Intégrité de la position de l'utilisateur**: le fournisseur de service IMT-2000 de rattachement, le fournisseur de service IMT-2000 visité et/ou l'exploitant de réseau IMT-2000 sont pratiquement sûrs que l'information relative à la position de l'utilisateur IMT-2000 ne peut pas être modifiée par des intrus.

– **Intégrité de la position de la station**: le fournisseur de service IMT-2000 de rattachement, le fournisseur de service IMT-2000 visité et/ou l'exploitant de réseau IMT-2000 sont pratiquement sûrs que l'information relative à la position de la station mobile IMT-2000 ne peut pas être modifiée par des intrus. Cette fonction peut être efficacement assurée par l'intégrité de la position de l'utilisateur.

– **Sûreté de programmation de l'identité d'utilisateur IMT-2000 et de l'information de sécurité corrélative**: l'identité de l'utilisateur IMT-2000 et l'information de sécurité corrélative peuvent être programmées en toute sécurité dans l'UIM par le fournisseur de service IMT-2000 de rattachement au moment de l'enregistrement de l'utilisateur IMT-2000. Cette fonction est uniquement valable pour le cas où l'UIM est utilisé pour l'association utilisateur-station mobile IMT-2000 (**elle n'est pas nécessairement directement liée à l'interface radioélectrique**).

– **Sûreté de programmation de l'identité de la station mobile IMT-2000 et de l'information de sécurité corrélative**: l'identité de la station mobile IMT-2000 et l'information de sécurité corrélative peuvent être programmées en toute sécurité dans la station mobile IMT-2000, si ces données sont attribuées par le gestionnaire des stations IMT-2000, ou à ce dernier lorsqu'elles sont attribuées par les fabricants de stations, au moment de l'enregistrement de la station mobile IMT-2000 (**cette fonction n'est pas nécessairement directement liée à l'interface radioélectrique**).

– **Système MFDT protégé**: le système MFDT est protégé contre les écoutes indiscrètes à l'interface (aux interfaces) radioélectrique(s) IMT-2000, si ce système est mis en œuvre dans la station mobile IMT-2000.

8.3.1.1.2 Fonctions de sécurité facultatives relatives à l'utilisateur

Les IMT-2000 offrent les fonctions facultatives de sécurité liées à l'utilisateur suivantes:

– **Authentification du fournisseur de service**: vérification que l'identité d'un fournisseur de service IMT-2000 correspond bien à celle annoncée.

– **Réauthentification des utilisateurs**: l'identité d'un utilisateur IMT-2000, après nouvelle vérification, est bien celle annoncée. Cette fonction peut être déclenchée de manière répétée ou à tout moment.

– **Réauthentification des stations**: l'identité d'une station mobile IMT-2000, après nouvelle vérification, est bien celle annoncée. Cette fonction peut être déclenchée de manière répétée ou à tout moment.

– **Rapports d'événements d'utilisateur**: l'utilisateur IMT-2000 reçoit des annonces ou des indications d'avertissement à des moments critiques de l'utilisation des services IMT-2000 (par exemple, information sur les taxes accumulées ou indication précisant que la communication n'est pas codée, etc.).

– **Accès de l'abonné au profil de service**: l'abonné IMT-2000 a un accès direct et limité au profil de service personnel des utilisateurs qui lui sont associés, il peut ainsi restreindre l'accès aux services, etc.

8.3.1.2 Fonctions de sécurité liées à la fourniture du service

8.3.1.2.1 Fonctions de sécurité essentielles

Les IMT-2000 offrent les fonctions de sécurité essentielles suivantes relatives à la fourniture du service:

– **Refus d'accès au service pour les utilisateurs**: le fournisseur de service IMT-2000 refuse à un utilisateur IMT-2000 particulier l'accès au service (**cette fonction n'est pas nécessairement directement liée à l'interface radioélectrique**).

– **Sauvegarde des données d'abonnement**: le fournisseur de service IMT-2000 peut rétablir des données relatives à des utilisateurs ou des abonnés en cas de panne (**cette fonction n'est pas nécessairement directement liée à l'interface radioélectrique**).

– **Lutte contre l'utilisation abusive ou frauduleuse du réseau**: fonction qui permet à un exploitant de réseau qui est lié à un fournisseur de service/gestionnaire de station IMT-2000, de disposer des données nécessaires pour lutter contre l'utilisation abusive ou frauduleuse de son réseau **(qui n'est pas nécessairement au niveau de l'interface radioélectrique).**

8.3.1.2.2 Fonctions de sécurité facultatives

Les IMT-2000 offrent les fonctions de sécurité facultatives suivantes liées à la fourniture du service:

– **Consignation des événements**: le fournisseur de service IMT-2000 peut consigner les activités concernant un utilisateur ou un abonné IMT-2000 (**cette fonction n'est pas nécessairement directement liée à l'interface radioélectrique**).

– **Refus d'accès au service pour les stations mobiles**: le fournisseur de service IMT-2000/exploitant de réseau IMT-2000 peut refuser à une station mobile IMT-2000 particulière l'accès au service (**cette fonction n'est pas nécessairement directement liée à l'interface radioélectrique**).

8.3.1.3 Fonctions de sécurité de l'IMT-2000 relatives à l'exploitation du réseau de télécommunication générique

Les fonctions de sécurité de l'IMT-2000 relatives à l'exploitation du réseau de télécommunication générique sont des fonctions de sécurité qui sont jugées importantes dans le contexte du système IMT-2000 global mais qui peuvent être déjà définies ou qui le seront dans des Recommandations UIT-T traitant de l'exploitation du réseau de télécommunication générique.

8.3.2 Mécanismes de sécurité

Alors que les fonctions de sécurité indiquent **le type** de sécurité assuré, les mécanismes de sécurité indiquent **les modalités** de fourniture de cette sécurité. Ces mécanismes seront traités dans la future Recommandation relative aux procédures de sécurité des IMT-2000.

8.4 Gestion de la sécurité

La gestion de la sécurité consiste à contrôler et à distribuer l'information relative à la sécurité aux différentes parties en cause (utilisateurs et systèmes par exemple) afin de protéger les utilisateurs IMT-2000 et les autres intervenants dans les IMT-2000. Elle sert à signaler les événements intéressant la sécurité qui influent sur la protection des parties en cause.

La gestion de la sécurité dans les IMT-2000, fera l'objet des futures Recommandations relatives à la gestion des réseaux IMT-2000.

8.5 Architecture sécuritaire et procédures associées

Les exigences relatives à la mise en œuvre des mécanismes de sécurité dans les IMT-2000 sous la forme de procédures intéressant les différentes parties participant aux IMT-2000 seront spécifiées dans la future Recommandation sur les procédures de sécurité pour les IMT-2000.

8.6 Algorithmes de sécurité

La future Recommandation sur les procédures de sécurité pour les IMT-2000 définira les algorithmes de sécurité ou les contraintes imposées à ces algorithmes.

ANNEXE 1

Vocabulaire

Les termes et définitions suivants ont été utilisés dans la présente Recommandation:

– **Fonction de sécurité**: fonction qui offre une certaine assurance contre une ou plusieurs menaces potentielles sur la sécurité.

– **Mécanisme de sécurité**: moyen permettant d'offrir une fonction de sécurité.

– **Service de sécurité**: service qui offre une fonction de sécurité déterminée comme un service complémentaire.

– **Architecture sécuritaire**: architecture de parties et d'entités relatives à la sécurité et ensemble complet de procédures et de flux d'informations concernant la sécurité et destinés à l'exécution des fonctions de sécurité.

– **Gestion de sécurité**: traitement des aspects de la sécurité relatifs à la gestion du réseau et du service, qu'il s'agisse de questions administratives, opérationnelles ou de maintenance.

– **Politique de sécurité**: ensemble des règles qui définissent et imposent aux entités et aux parties les types d'activités relatives à la sécurité.

– **Utilisateur IMT-2000**: personne, entité ou processus qui a effectivement recours aux services IMT-2000. Un utilisateur IMT-2000 se voit attribuer une identité spécifique.

– **Abonné IMT-2000**: personne morale ou entité s'étant abonnée aux IMT-2000 et responsable du règlement des taxes dues par les utilisateurs IMT-2000 qui lui sont associés. Un abonné IMT-2000 peut être responsable de plusieurs utilisateurs IMT-2000.

– **Fournisseur de service IMT-2000**: personne morale ou entité chargée de la délivrance des abonnements IMT-2000 aux abonnés IMT-2000.

– **Exploitant de réseau IMT-2000**: personne morale ou entité à laquelle incombe en dernier ressort d'assurer en totalité le fonctionnement du réseau IMT-2000 pour les utilisateurs IMT-2000. Certaines fonctions du réseau IMT-2000 peuvent, néanmoins, être fournies par d'autres parties.

– **Utilisateur UPT**: utilisateur des services UPT.

– **Abonné UPT**: abonné associé à un utilisateur UPT. Un abonné UPT obtient son abonnement auprès d'un fournisseur de service UPT.

– **Fournisseur de service UPT**: personne morale ou entité chargée de la délivrance des abonnements UPT aux abonnés UPT.

– **Confidentialité**: consiste à ne pas mettre une information relative à une entité ou à une partie à la disposition de tiers, d'entités ou de processus non autorisés ou de ne pas la leur communiquer.

– **Authentification**: permet d'établir avec la certitude nécessaire l'identité correcte d'une entité ou d'une partie.

– **Intégrité**: fonction qui interdit toute modification du contenu d’information d’un objet.

– **Autorisation**: fonction selon laquelle les droits d'accès aux ressources sont établis et assurés.

– **Secret**: droit reconnu aux personnes de contrôler ou d'agir sur les informations les concernant qui peuvent être recueillies ou enregistrées et de décider par qui ces informations peuvent être recueillies ou enregistrées et à qui elles peuvent être communiquées.

ANNEXE 2

Analyse des menaces et des risques

TABLE DES MATIÈRES

1. Introduction

La présente Annexe contient une analyse des menaces et des risques qui peuvent affecter la sécurité des IMT-2000.

2. Méthodologie

La méthodologie utilisée pour l'analyse des menaces dans la présente Annexe comporte les étapes suivantes:

– **identification du scénario du système** et des parties concernées (traités au § 6 du corps de la présente Recommandation),

– **identification des menaces** et des points vulnérables du système,

– **évaluation des menaces et des risques** propres à chaque système,

– **évaluation des contre-mesures et de leur coût**, et

– **définition des mécanismes de détection, de résistance et de rétablissement** nécessaires pour faire face aux menaces potentielles et assurer la sécurité et l'intégrité du système; évaluation et justification de la mise en œuvre de ces mécanismes (points traités aux § 8.5 et 8.6 du corps de la présente Recommandation).

3. Identification des menaces

Dans le présent paragraphe, on recense les menaces liées à la fourniture et à l'utilisation des services IMT-2000. Bien que les hypothèses du système sur la sécurité et les parties participant à la fourniture des services IMT-2000 soient présentées aux § 6.1 et 6.2 du corps de la présente Recommandation, les indications fournies ci-après ne concordent pas entièrement avec les informations données dans ces paragraphes. En effet, les indications ci-dessous reposent sur une architecture du système et sur des termes génériques quelque peu simplifiés.

Les menaces peuvent être classées selon les trois catégories générales suivantes:

– les menaces intentionnelles,

– les menaces accidentelles, et

– les menaces administratives.

3.1 Menaces intentionnelles

On entend par menaces intentionnelles celles qui proviennent d'intrus malveillants. On peut à nouveau les subdiviser en trois catégories.

3.1.1 Utilisation frauduleuse

3.1.1.1 Vol d'une station mobile

Après avoir dérobé une station mobile, ou un module d'identité d'utilisateur s'il s'agit d'un dispositif physiquement détachable, le voleur établira des communications frauduleuses et le propriétaire de la station mobile ou du module d'identité d'utilisateur pourra être redevable des taxes correspondantes, selon la politique commerciale pratiquée par le fournisseur de service.

3.1.1.2 Vol des justificatifs d'identité de l'utilisateur

3.1.1.2.1 Clonage

Si une station mobile est momentanément exposée à des personnes malhonnêtes (par exemple, des ouvriers malhonnêtes d'un atelier de réparation), les données secrètes sur l'utilisateur qui sont normalement utilisées par le fournisseur de service ou l'exploitant de réseau pour authentifier l'utilisateur pendant les transactions d'établissement des communications, peuvent être extraites puis chargées dans une station clandestine mobile. Cette station clandestine est en quelque sorte un clone d'une station mobile autorisée et il ne peut être en général décelé ni par le propriétaire de la station mobile ni par les fournisseurs de service ou les exploitants de réseau avant que des taxes liées à l'utilisation frauduleuse se soient accumulées pendant 30 jours ou plus.

Le clonage est aggravé par des insuffisances au niveau de l'administration et de la gestion de la sécurité chez le fournisseur de service ou l'exploitant de réseau.

3.1.1.2.2 Usurpation d'identité

Si la signalisation s'effectue en clair sur la voie radioélectrique, un pirate peut décoder les données secrètes contenues dans la station mobile ou le module d'identité d'utilisateur en écoutant les transactions lors de l'établissement de la communication puis en les analysant. Il peut ensuite se faire passer pour un utilisateur légitime en imitant les transactions licites d'établissement des communications.

3.1.1.3 Détournement

Un pirate pourrait interrompre une communication juste après qu'elle a été établie mais avant que la station mobile légitime commence la conversation. Cela peut aussi se produire quand une liaison radioélectrique est établie de nouveau au cours d'une communication, comme c'est le cas lors de l'opération de transfert dans le système téléphonique cellulaire.

3.1.2 Menaces sur l'intégrité

3.1.2.1 Manipulation cohérente des données de l'utilisateur

La manipulation cohérente des données d'utilisateur est un danger en ce sens que ces données sont volontairement manipulées par un intrus de manière que le résultat ait une signification différente de la signification originelle mais qu'il semble chargé de sens pour les utilisateurs.

3.1.2.2 Enregistrement malveillant de position

L'enregistrement malveillant de position est une tentative intentionnelle par laquelle un intrus enregistre un utilisateur légitime sur une position fausse.

3.1.2.3 Manipulation malveillante du profil de service de l’utilisateur

La manipulation malveillante du profil de service de l'utilisateur est une tentative intentionnelle par laquelle un intrus manipule le profil de service d'un utilisateur légitime ou de tous les utilisateurs légitimes. Un exemple de manipulation du profil de service de tous les utilisateurs légitimes consiste à insérer un virus dans la base de données du profil de service de l'utilisateur.

3.1.3 Menaces sur la confidentialité, le secret et l'anonymat

3.1.3.1 Divulgation de l'identité des utilisateurs

La confidentialité de l'identité des utilisateurs, qu'il s'agisse de demandeurs ou de demandés, en communication est un autre domaine qui peut être soumis à des menaces.

3.1.3.2 Divulgation de la position de l’utilisateur

La confidentialité de la position géographique d'un utilisateur constitue un autre domaine qui peut être soumis à des menaces.

3.1.3.3 Ecoute indiscrète d'une communication de l'utilisateur

Comme il s'agit par nature d'une radiocommunication, la conversation sur la voie radioélectrique devrait être tout aussi vulnérable aux agissements de personnes indiscrètes qui écoutent.

3.2 Menaces accidentelles

Les menaces accidentelles sont celles qui sont causées par des manipulations erronées de la part de l'utilisateur, par des erreurs de transmission, etc.

L'étude de ces menaces appelle un complément d'étude.

3.3 Menaces administratives

Ce sont des menaces qui résultent d'une mauvaise administration et gestion de la sécurité, de l'abus de privilèges, etc. Les menaces administratives ne sont pas nécessairement directement liées à l'interface radioélectrique.

3.3.1 Intrusion dans la base de données de l'abonné ou de l'utilisateur

Une base de données d'abonné/d'utilisateur qui contient les données confidentielles relatives à l'utilisation exige en général que soient prises des dispositions pour sa vérification, sa maintenance et sa sauvegarde, ce qui la rend vulnérable à des intrus. L'intrus pourra être ou non un employé du fournisseur de service ou de l'exploitant de réseau. L'intrusion dans la base de données de l'abonné ou de l'utilisateur peut aboutir à un clonage (voir le § 3.1.1.2.1).

3.3.2 Piratage des justificatifs d'identité des utilisateurs dans d'autres réseaux

Lorsque les abonnés/utilisateurs sont autorisés à se déplacer au niveau national et international, la menace de piratage des données secrètes est réelle lorsqu'un utilisateur se déplace dans un réseau étranger. Le piratage de données secrètes peut déboucher sur un clonage (voir le § 3.1.1.2.1).

3.3.3 Intrusion dans la base de données du système ou dans les fonctions de commande du réseau

Il peut arriver que des intrus accèdent à la base de données des fonctions de commande du réseau et la modifient. Il peut aussi arriver qu'un intrus introduise un virus dans la base de données des fonctions de commande du réseau.

4. Evaluation des menaces et des risques

4.1 Menaces intentionnelles

4.1.1 Utilisation frauduleuse

L'utilisation frauduleuse se traduit par un préjudice économique à la fois pour les utilisateurs et pour les fournisseurs de service et les exploitants de réseau.

4.1.1.1 Vol d'une station mobile

Le vol cause généralement un préjudice économique à l'utilisateur dont la station mobile, ou le module d'identité d'utilisateur s'il s'agit d'un dispositif amovible, a été volé. Cependant, ce préjudice peut être limité à la taxation des communications qui lui est imputable entre le moment du vol et celui de la déclaration de vol au fournisseur de service ou à l'exploitant de réseau. En effet, le fournisseur de service ou l'exploitant de réseau peut imposer des restrictions aux appels à destination et en provenance de la station mobile dès qu'il reçoit cette déclaration. Le préjudice sera dans ces conditions assez faible, sauf si l'utilisateur n'a connaissance du vol que longtemps après qu'il a eu lieu.

4.1.1.2 Vol des justificatifs d'identité de l'utilisateur

4.1.1.2.1 Clonage

Le clonage entraîne d'ordinaire un préjudice économique pour un utilisateur dont la station mobile, ou le module d'identité d'utilisateur s'il s'agit d'un dispositif amovible, a fait l'objet d'un clonage. Le clonage peut aussi causer un préjudice économique au fournisseur de service ou à l'exploitant de réseau, parce que cette fraude est parfois indétectable pendant une longue période, d'où une forte probabilité que l'utilisateur qui en est victime refuse une facture qu'il n'attend pas.

Comme le clonage passe souvent inaperçu pendant de longues périodes, il cause un préjudice économique considérable pour l'utilisateur, le fournisseur de service et l'exploitant de réseau.

Le clonage peut en outre empêcher l'utilisateur qui en est victime de faire aboutir ses communications, étant donné que l'enregistrement de position par la station mobile ayant fait l'objet d'un clonage correspond à un enregistrement malveillant de position (voir le § 3.1.2.2).

4.1.1.2.2 Usurpation d'identité

L'usurpation d'identité cause d'ordinaire un préjudice économique à l'utilisateur dont la station mobile, ou le module d'identité d'utilisateur s'il s'agit d'un dispositif amovible, a été imité et par un préjudice potentiel pour le fournisseur de service, l'exploitant du réseau, analogue au préjudice causé par le clonage.

L'usurpation d'identité empêche en outre l'utilisateur qui en est victime de faire aboutir ses communications, étant donné que l'enregistrement de position par la station mobile frauduleuse correspond à un enregistrement malveillant de position (voir le § 3.1.2.2).

4.1.1.3 Détournement

Le piratage cause en général un préjudice économique à l'utilisateur qui en est victime. Néanmoins, comme le piratage affecte les communications de façon aléatoire et qu'ainsi un utilisateur donné est en général victime une seule fois du piratage, le préjudice est relativement faible pour les utilisateurs.

Le piratage est une cause potentielle de préjudice économique pour le fournisseur de service et l'exploitant de réseau parce que l'utilisateur qui en est victime se plaindra de l'interruption intempestive de la communication. Si le fournisseur de service ou l'exploitant de réseau accepte de telles réclamations des utilisateurs, le préjudice économique qu'il subira sera plus important.

4.1.2 Menaces sur l'intégrité

4.1.2.1 Manipulation cohérente des données des utilisateurs

La manipulation cohérente des données d'utilisateurs lors des communications a pour résultat que l'utilisateur qui en est victime reçoit un message erroné, et subit donc un préjudice ou des inconvénients. L'importance du préjudice ou de la gêne causé varie selon le cas. Cette menace est difficile à déceler.

4.1.2.2 Enregistrement malveillant de position

L'enregistrement malveillant de position rend impossible l'aboutissement des appels, ce qui occasionne un préjudice ou des inconvénients pour les utilisateurs qui en sont victimes. L'importance du préjudice ou des inconvénients varie selon les cas.

4.1.2.3 Manipulation malveillante du profil de service de l'utilisateur

La manipulation malveillante du profil de service de l'utilisateur se traduit par l'indisponibilité de certains services, d'où un préjudice ou des inconvénients pour les utilisateurs qui en sont victimes. L'importance du préjudice ou des inconvénients varie selon les cas. L'intrusion dans la base de données du profil de service de l'utilisateur, consistant par exemple à y insérer un virus, peut causer des dommages à tout le réseau qui est associé au fournisseur de service victime de cette attaque.

4.1.3 Menaces sur la confidentialité, le secret et l'anonymat

4.1.3.1 Divulgation de l'identité des utilisateurs

La divulgation de l'identité des utilisateurs, qu'il s'agisse du demandeur ou du demandé en cours de communication place ceux qui en sont victimes devant un risque impossible à préciser.

4.1.3.2 Divulgation de la position des utilisateurs

La divulgation de la position physique des utilisateurs permet à un intrus et à d'autres utilisateurs de suivre les déplacements des utilisateurs qui en sont victimes et place par conséquent ces derniers devant un risque impossible à préciser.

4.1.3.3 Ecoute indiscrète d'une communication d'utilisateur

L'écoute indiscrète d'une conversation d'utilisateur place celui-ci devant un risque impossible à préciser. S'il s'agit d'une communication d'affaires, le risque d'espionnage économique peut être très important. Si l'utilisateur est une personnalité publique ou politique, le risque de préjudice économique et d'atteinte à la sécurité nationale résultant d'une violation du secret peut être également très important.

4.2 Menaces accidentelles

L'évaluation des menaces et des risques accidentels exige une étude ultérieure visant à déterminer ces dangers.

4.3 Menaces administratives

4.3.1 Intrusion dans la base de données d'abonné/utilisateur

L'intrusion dans la base de données d'abonné/utilisateur donne à un intrus la possibilité de réaliser un clone. Par conséquent, les risques évoqués en ce qui concerne le clonage sont applicables ici (voir le § 4.1.1.2.1).

L'intrusion permet aussi à un intrus d'obtenir ou de manipuler le profil d'un abonné/utilisateur, ce qui peut compromettre le secret des données d'abonné ou d'utilisateur ou de créer un préjudice ou des inconvénients impossibles à préciser pour l'abonné ou l'utilisateur qui en est victime. L'intrusion dans la base de données d'abonné ou d'utilisateur peut provoquer une panne catastrophique de tout le réseau IMT-2000.

4.3.2 Piratage des justificatifs d'identité des utilisateurs dans d'autres réseaux

Le piratage des justificatifs d'identité des abonnés et des utilisateurs offre au pirate la possibilité de réaliser un clone, de sorte que les risques indiqués pour le clonage s'appliquent ici aussi (voir le § 4.1.1.2.1).

4.3.3 Intrusion dans la base de données du système ou dans les fonctions de commande du réseau

L'intrusion dans la base de données du système ou dans les fonctions de commande du réseau provoque une anomalie intempestive de fonctionnement du réseau et affecte l'intégrité du réseau; elle peut aboutir à une panne catastrophique de tout le réseau.

5. Evaluation des contre-mesures et des coûts corrélatifs

5.1 Menaces intentionnelles

5.1.1 Utilisation frauduleuse

5.1.1.1 Vol de la station mobile

Le propriétaire de la station mobile ou du module d'identité d'utilisateur volé peut être protégé de deux manières contre des communications frauduleuses.

a) *Restriction d'accès lorsque le vol est déclaré*

Cette contre-mesure est semblable à la pratique habituelle adoptée pour les cartes de crédit: dès que le vol est signalé au fournisseur de service ou à l'exploitant du réseau, celui-ci enregistre le vol dans la base de données de l'abonné afin que les prochaines tentatives d'appel frauduleuses soient rejetées. Ce qui limite la responsabilité du propriétaire.

b) *Authentification de l'utilisateur*

Cette contre-mesure consiste à instaurer une fonction d'authentification de l'utilisateur (et non de la station mobile ou du module d'identité d'utilisateur) dans les stations mobiles ou dans les réseaux IMT-2000. L'authentification n'est pas nécessaire entre l'utilisateur et le fournisseur de service ou l'exploitant de réseau.

La méthode la plus courante utilisée jusqu'à présent repose sur l'emploi du numéro d'identification personnelle (PIN) qui devrait être connu seulement du propriétaire légitime des stations mobiles ou du module d'identité de l'utilisateur. Un exemple d'application est donné par le «verrou électronique» utilisé dans le service téléphonique cellulaire, où le processus est entièrement exécuté dans la station mobile.

5.1.1.2 Vol des justificatifs d'identité de l'utilisateur

5.1.1.2.1 Clonage

a) *Utilisation d'un dispositif spécial*

Pour empêcher des personnes malhonnêtes de réaliser des clones, on peut utiliser un dispositif spécial dont le contenu est difficile à lire pour enregistrer les données secrètes concernant l'utilisateur. Cette contre-mesure est surtout importante si le module d'identité de l'utilisateur est un composant physiquement intégré dans la station mobile.

b) *Utilisation d'un dispositif amovible*

Une autre contre-mesure possible consiste à utiliser un module d'identité d'utilisateur amovible de la station mobile, c'est-à-dire à conserver les données secrètes liées à l'utilisateur dans un dispositif qui est rarement remis par le propriétaire à d'autres utilisateurs. Une carte à mémoire (à circuits intégrés) que l'on insère dans les unités mobiles quand elles sont utilisées est un exemple particulier de ce type de dispositif.

c) *Authentification du fournisseur de service ou de l'exploitant de réseau*

On complétera les deux solutions en a) et b) ci-dessus en mettant en œuvre une fonction d'authentification du fournisseur de service ou de l'exploitant de réseau dans laquelle le module d'identité d'utilisateur ne répond pas aux demandes du réseau avant l'authentification positive du fournisseur de service ou de l'exploitant de réseau. Cela empêche en effet un intrus de tenter d'obtenir les données secrètes liées à l'utilisateur au moyen d'une analyse cryptographique fondée sur le nombre de paires de demandes/réponses.

d) *Clé valable pour une seule utilisation*

Comme contre-mesure destinée à éviter une utilisation frauduleuse par clonage, on peut aussi recourir à une clé valable pour une seule utilisation; cette clé servira à l'authentification de l'utilisateur pendant le processus d'établissement de la communication; elle est actualisée à chaque tentative d'appel et enregistrée à la fois dans le module d'identité de l'utilisateur et chez le fournisseur de service ou l'exploitant de réseau. Par ce procédé, un clone ne pourra jamais fonctionner dès que l'unité mobile établit une communication avant que le clone ne fasse une tentative d'appel; en effet, à cette occasion, une tentative d'authentification a lieu qui a pour résultat l'enregistrement d'une nouvelle clé que les clones ne connaissent pas. En revanche, l'utilisateur légitime ne peut pas établir une communication lorsqu'un clone a réussi à établir une communication avant lui. Ce dernier scénario donne au propriétaire légitime de la station mobile ou du module d'identité d'utilisateur amovible une chance de se rendre compte rapidement de l'existence d'un clone.

L'inconvénient de cette méthode tient néanmoins à la difficulté de conserver l'alignement des compteurs d'appel entre le module d'identité d'utilisateur et le fournisseur de service ou l'exploitant de réseau dans un contexte de radiocommunication relativement peu fiable.

e) *Authentification de l'utilisateur par le fournisseur de service*

L'authentification de l'utilisateur (et non de la station mobile ou du module d'identité d'utilisateur) par le fournisseur de service empêche le détenteur d'un clone de réussir à établir une communication, à moins que le clone ne soit utilisé par l'utilisateur légitime lui-même. Si l'authentification de l'utilisateur a lieu à l'échelon local, l'authentification locale de l'utilisateur devrait être associée et corrélée avec l'authentification de la station ou du module d'identité de l'utilisateur.

Pour que l'authentification de l'utilisateur soit fiable, il est nécessaire que celui-ci compose une longue chaîne de chiffres ou de caractères, mais alors l'utilisation du service devient plus compliquée. En revanche, le niveau de protection offert par cette méthode est d'autant plus faible que la chaîne servant à l'authentification de l'utilisateur est courte.

On pourra prévoir ultérieurement une authentification plus pratique pour l'utilisateur en recourant aux possibilités du réseau, par exemple la reconnaissance vocale.

f) *Détection d'appels quasi simultanés*

Bien qu'il s'agisse d'une mesure préventive contre le clonage, la détection par le réseau de deux appels simultanés pour une même identité d'utilisateur, ou la détection par le réseau de deux appels quasi simultanés pour une même identité d'utilisateur mais provenant de positions géographiques très éloignées l'une de l'autre aidera le fournisseur de service/exploitant de réseau à prendre conscience rapidement de l'existence d'un clone.

g) *Protection renforcée contre les menaces administratives*

Un renforcement des contre-mesures contre les menaces administratives diminue le risque d'apparition de clones (voir le § 5.3).

5.1.1.2.2 Usurpation d'identité

a) *Utilisation d'un système cryptographique pour les opérations de signalisation sur la voie radioélectrique*

D'une manière générale pour lutter contre l'usurpation d'identité, il faut éviter la transmission sur la voie radioélectrique de messages en clair contenant les données secrètes relatives à l'utilisateur. Pour cela, on peut crypter les signaux envoyés dans les deux sens lors des procédures d'établissement des communications. Le type de système cryptographique utilisé à cette fin et les moyens permettant d'assurer la sécurité des clés appellent un complément d'étude.

b) *Authentification qui ne révèle pas d'information secrète*

Une autre contre-mesure possible consiste à adopter un schéma d'authentification de l'utilisateur dans lequel les données secrètes liées à l'utilisateur ne sont jamais transmises en clair sur la voie radioélectrique et dans lequel les données de la transaction d'authentification varient toujours d'un appel à l'autre.

Exemple d'une authentification de ce type: la méthode appliquée dans le système PDC (système personnel numérique cellulaire) du Japon et le système GSM, selon laquelle la réponse d'authentification est produite par une station mobile d'après un numéro aléatoire effaçable envoyé par le réseau. C'est ce qu'on appelle la méthode «interrogation et réponse».

La fiabilité de l'authentification par interrogation et réponse en cas d'usurpation d'identité dépend de l'invulnérabilité du système cryptographique utilisé pour produire la réponse.

5.1.1.3 Détournement

5.1.1.3.1 Utilisation d'un système cryptographique pour les transactions de signalisation sur la voie radioélectrique

On peut déjouer une tentative de piratage en utilisant un système cryptographique dans les messages de commande d'appel envoyés dans les deux sens pendant la communication. Comme dans le cas de l'usurpation d'identité, le type de système cryptographique et les moyens permettant d'assurer la sécurité des clés appellent un complément d'étude.

5.1.1.3.2 Répétition d'authentification pendant la communication

La répétition d'authentification pendant la communication peut également dissuader le piratage. Cependant, de fréquentes tentatives d'authentification peuvent avoir pour origine un intrus désireux de procéder à une analyse cryptographique afin d'obtenir les données secrètes liées à l'utilisateur en se fondant sur le nombre de paires

demande/réponse. Par conséquent, il convient d'étudier soigneusement la fréquence d'authentification; une authentification de l'utilisateur accompagnée simultanément de celle du fournisseur de service ou de l'exploitant de réseau peut être souhaitable si l'on fait appel à la répétition d'authentification (voir le point c) du § 5.1.1.2.1).

5.1.1.3.3 Cryptage des données de la conversation

Pour faire échouer les tentatives de piratage, on peut aussi crypter les données de conversation et utiliser des clés qui ne sont pas connues de l'intrus, il s'agit là d'une protection plutôt passive. Dans ce cas, le «pirate» ne peut pas obtenir une liaison de communication transparente lorsque le piratage a lieu après l'échange des clés de crytage.

5.1.2 Menaces sur l'intégrité

5.1.2.1 Manipulation cohérente des données des utilisateurs

5.1.2.1.1 Adjonction d'une signature aux données de l'utilisateur

En général, on protège les données contre une manipulation cohérente en ajoutant une «signature» aux données de l'utilisateur. On peut se servir de l'algorithme de «codage de clé secrète» ou de «codage de clé publique» pour produire la signature. En cas de transmission successive de données en temps réel comme lors d'une conversation téléphonique, il est parfois impossible dans la pratique d'ajouter la signature en raison de la plus grande complexité de traitement et il est en pareil cas préférable de recourir au cryptage dont les clés ne sont pas connues de l'intrus et des autres utilisateurs. Le cryptage rend également impossible toute manipulation volontaire.

5.1.2.1.2 Répétition de l'authentification pendant une communication

La répétition de l'authentification pendant une communication pourrait servir de contre-mesure à la place de la méthode de protection décrite au § 5.1.2.1.1 ci-dessus. Les précautions à prendre (voir le § 5.1.1.3.2) pour la répétition de l'authentification ne devraient pas être négligées.

5.1.2.2 Enregistrement malveillant de la position

5.1.2.2.1 Authentification pour chaque transaction d'enregistrement de position

D'une manière générale, on assure la protection contre un enregistrement malveillant de position en procédant à l'authentification lors de chaque transaction d'enregistrement de position.

5.1.2.2.2 Utilisation d'un système cryptographique pour les transactions d'enregistrement de position

Une autre contre-mesure consiste à crypter les transactions d'enregistrement de position, mais il faut alors disposer d'une méthode sûre d'échange des clés.

5.1.2.2.3 Enregistrement de position à chaque appel

Pour réduire le préjudice subi par l'utilisateur par suite d'un enregistrement malveillant de position, on peut procéder à l'enregistrement de position à chaque tentative d'appel authentifiée, mais il ne s'agit pas là d'une mesure préventive.

5.1.2.3 Manipulation malveillante du profil de service d'un utilisateur

5.1.2.3.1 Authentification à chaque transaction de manipulation

On assure en général la protection contre une manipulation malveillante du profil de service d'un utilisateur en procédant à une authentification pour chaque transaction de manipulation du profil de service d'un utilisateur.

5.1.2.3.2 Utilisation d'un système cryptographique pour les transactions de manipulation

Une autre contre-mesure peut consister à crypter les transactions de manipulation du profil de service d'un utilisateur, mais il faut alors disposer d'une méthode sûre d'échange des clés.

5.1.3 Menaces sur la confidentialité, le secret et l'anonymat

5.1.3.1 Divulgation de l'identité des utilisateurs

5.1.3.1.1 Utilisation d'un système cryptographique pour les identités

Comme contre-mesure destinée à garantir la confidentialité de l'identité des utilisateurs, on peut crypter l'identité d'utilisateur dans les messages de commande d'appel.

5.1.3.1.2 Utilisation d'identités temporaires pour les utilisateurs

Une autre contre-mesure consiste à employer des identités temporaires pour les utilisateurs dont la validité est limitée à une courte période.

5.1.3.2 Divulgation de la position des utilisateurs

5.1.3.2.1 Utilisation d'un système cryptographique pour les identités

Pour assurer la confidentialité de la position des utilisateurs, on peut crypter l'identité de l'utilisateur dans les messages d'enregistrement de position.

5.1.3.2.2 Utilisation d'identités temporaires pour les utilisateurs

Une autre contre-mesure consiste à employer des identités temporaires pour les utilisateurs dont la validité est limitée à une courte période.

5.1.3.3 Ecoute indiscrète d'une communication de l'utilisateur

5.1.3.3.1 Utilisation d'un système cryptographique

On assure la protection contre l'écoute indiscrète en employant un système cryptographique dans les voies de communication de l'utilisateur. Plusieurs types de systèmes cryptographiques et différentes méthodes de distribution des clés ont été mis au point. L'échange des clés dans le cadre de l'authentification de l'utilisateur peut être assuré par l'«algorithme d'échange de clé secrète» ou par l'«algorithme d'échange de clé publique».

5.2 Menaces accidentelles

Un complément d'étude est nécessaire pour identifier ces menaces, avant de pouvoir en évaluer les coûts et les contre-mesures à adopter.

5.3 Menaces administratives

5.3.1 Intrusion dans la base de données de l'abonné/utilisateur

L'intrusion dans la base de données de l'abonné/utilisateur pose un problème difficile.

5.3.1.1 Limitation d'accès

Pour obtenir un minimum de protection contre ce danger, on peut limiter l'accès à la base de données en le réservant à un nombre minimum d'employés et exclusivement à des employés.

5.3.1.2 Chiffrement des données stockées dans la base de données

Le chiffrement des données stockées au moyen d'une clé principale permet d'améliorer la sécurité, mais il faut alors prendre des dispositions pour assurer la sécurité de cette clé. Une méthode d'«échange de clé publique» rend inutile l'échange préliminaire de l'information secrète d'utilisateur. Une telle méthode devra faire l'objet d'une étude approfondie.

5.3.2 Piratage des justificatifs d'identité des utilisateurs dans d'autres réseaux

5.3.2.1 Interdiction de transfert des données secrètes concernant l'utilisateur

Une protection contre cette menace peut consister à interdire l'envoi des données secrètes concernant l'utilisateur vers des réseaux étrangers. Cela oblige le fournisseur de service ou l'exploitant de réseau visité à demander un ensemble de données non secrètes utilisé par le fournisseur de service nominal ou exploitant de réseau de rattachement pour l'authentification ou le codage lors de chaque transaction relative à l'établissement de la communication ou à l'enregistrement de position.

5.3.3 Intrusion dans la base de données du système ou dans les fonctions de commande du réseau

5.3.3.1 Isolation de la base de données du système ou des fonctions de commande du réseau vis-à-vis des réseaux publics

Une méthode prometteuse pour assurer une protection contre l'intrusion dans la base de données du système ou dans les fonctions de commande du réseau consiste à les isoler vis-à-vis des réseaux de télécommunication publics. Toutefois, cela limite considérablement la maintenabilité d'éléments du réseau tels que les stations de base qui sont réparties entre différents points géographiques.

5.3.3.2 Autorisation et authentification de l'entité d'accès à la base de données du système ou aux fonctions de commande du réseau

Quand les éléments du réseau possédant des fonctions de commande et la base de données peuvent faire l'objet d'un accès à distance par l'intermédiaire des réseaux publics de télécommunication, l'accès doit être limité aux personnes habilitées et aux fonctions spécifiques des personnes, et la personne qui y accède doit être authentifiée par l'élément de réseau.

ANNEXE 3

Procédures relatives à la sécurité

La présente Annexe spécifie les types de procédure de sécurité que l'on peut envisager d'inclure dans la future Recommandation relative aux procédures de sécurité applicables aux IMT-2000. Ces procédures sont les suivantes:

- procédures élémentaires relatives à la sécurité:
  - confidentialité de l'identité de l'utilisateur et de la station à l'interface radioélectrique,
  - confidentialité de l'identité de l'utilisateur et de la station à travers l'interface fournisseur de service ou exploitant de réseau,
  - authentification de l'utilisateur,
  - authentification de la station,
  - cryptage;
- procédures relatives à la sécurité applicables pendant la mise à jour de la position:
  - mise à jour de la position initiale,
  - mise à jour de la position dans la zone de responsabilité d'un exploitant de réseau IMT-2000,
  - mise à jour de la position à la frontière des zones de différents exploitants de réseau IMT-2000;
- procédures relatives à la sécurité applicables pendant l'établissement des communications:
  - appel IMT-2000 entrant,
  - appel IMT-2000 sortant;
- procédures relatives à la sécurité applicables aux communications:
  - procédures de sécurité lors du transfert,
  - procédures de sécurité applicables aux modifications en cours de communication;
- procédures de sécurité applicables à la libération des communications:
  - libération des communications;
- procédures de sécurité correspondant à des services de sécurité spécifiques:
  - authentification périodique,
  - authentification du fournisseur de service IMT-2000 de rattachement,
  - authentification de l'exploitant de réseau IMT-2000.