Union internationale des télécommunications

# UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

# X.1248

(09/2017)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité du cyberespace – Lutte contre le spam

## Exigences techniques pour lutter contre le spam par messagerie instantanée

Recommandation UIT-T X.1248

Union internationale des télécommunications

RECOMMANDATIONS UIT-T DE LA SÉRIE X

**RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ**

| | |
|---|---|
| RÉSEAUX PUBLICS DE DONNÉES | X.1–X.199 |
| INTERCONNEXION DES SYSTÈMES OUVERTS | X.200–X.299 |
| INTERFONCTIONNEMENT DES RÉSEAUX | X.300–X.399 |
| SYSTÈMES DE MESSAGERIE | X.400–X.499 |
| ANNUAIRE | X.500–X.599 |
| RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES | X.600–X.699 |
| GESTION OSI | X.700–X.799 |
| SÉCURITÉ | X.800–X.849 |
| APPLICATIONS OSI | X.850–X.899 |
| TRAITEMENT RÉPARTI OUVERT | X.900–X.999 |
| SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX | |
| Aspects généraux de la sécurité | X.1000–X.1029 |
| Sécurité des réseaux | X.1030–X.1049 |
| Gestion de la sécurité | X.1050–X.1069 |
| Télébiométrie | X.1080–X.1099 |
| APPLICATIONS ET SERVICES SÉCURISÉS (1) | |
| Sécurité en multidiffusion | X.1100–X.1109 |
| Sécurité des réseaux domestiques | X.1110–X.1119 |
| Sécurité des télécommunications mobiles | X.1120–X.1139 |
| Sécurité de la toile | X.1140–X.1149 |
| Protocoles de sécurité (1) | X.1150–X.1159 |
| Sécurité d'homologue à homologue | X.1160–X.1169 |
| Sécurité des identificateurs en réseau | X.1170–X.1179 |
| Sécurité de la télévision par réseau IP | X.1180–X.1199 |
| SÉCURITÉ DU CYBERESPACE | |
| Cybersécurité | X.1200–X.1229 |
| **Lutte contre le spam** | **X.1230–X.1249** |
| Gestion des identités | X.1250–X.1279 |
| APPLICATIONS ET SERVICES SÉCURISÉS (2) | |
| Communications d'urgence | X.1300–X.1309 |
| Sécurité des réseaux de capteurs ubiquitaires | X.1310–X.1319 |
| Sécurité des réseaux électriques intelligents | X.1330–X.1339 |
| Courrier certifié | X.1340–X.1349 |
| Sécurité de l'Internet des objets (IoT) | X.1360–X.1369 |
| Sécurité des systèmes de transport intelligents | X.1370–X.1389 |
| Sécurité de la technologie des registres distribués | X.1400–X.1429 |
| Protocoles de sécurité (2) | X.1450–X.1459 |
| ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ | |
| Aperçu général de la cybersécurité | X.1500–X.1519 |
| Echange concernant les vulnérabilités/les états | X.1520–X.1539 |
| Echange concernant les événements/les incidents/l'heuristique | X.1540–X.1549 |
| Echange de politiques | X.1550–X.1559 |
| Heuristique et demande d'informations | X.1560–X.1569 |
| Identification et découverte | X.1570–X.1579 |
| Echange garanti | X.1580–X.1589 |
| SÉCURITÉ DE L'INFORMATIQUE EN NUAGE | |
| Aperçu de la sécurité de l'informatique en nuage | X.1600–X.1601 |
| Conception de la sécurité de l'informatique en nuage | X.1602–X.1639 |
| Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage | X.1640–X.1659 |
| Mise en oeuvre de la sécurité de l'informatique en nuage | X.1660–X.1679 |
| Sécurité de l'informatique en nuage (autres) | X.1680–X.1699 |

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

# Recommandation UIT-T X.1248

## Exigences techniques pour lutter contre le spam par messagerie instantanée


### Résumé

La Recommandation UIT-T X.1248 définit les caractéristiques du spam par messagerie instantanée (SPIM) et indique les exigences techniques à respecter pour lutter contre ce phénomène. En raison du succès croissant de la messagerie instantanée (IM), la multiplication du SPIM est devenue un problème de plus en plus préoccupant. Les caractéristiques de la messagerie instantanée, outil largement répandu et gratuit qui repose sur le protocole Internet (IP), font que le SPIM est susceptible de se propager à grande échelle et de façon incontrôlable. Si les problèmes liés au SPIM ne sont pas traités avec le plus grand soin, ils risquent d'avoir des incidences négatives sur l'utilisation du service de messagerie instantanée lui-même.



### Historique

| Edition | Recommandation | Approbation | Commission d'études | Identifiant unique* |
|---|---|---|---|---|
| 1.0 | UIT-T X.1248 | 06-09-2017 | 17 | 11.1002/1000/13262 |

### Mots clés

Spam par messagerie instantanée; SPIM.


* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

## AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) 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.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

## DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en oeuvre 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 oeuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

## TABLE DES MATIÈRES

## Introduction

En raison du développement rapide de l'Internet et de l'Internet sur mobile, la messagerie instantanée (IM), qui était auparavant un simple outil de discussion, est devenue une plate-forme d'information intégrée qui regroupe la communication, l'information, les loisirs, la recherche, le commerce en ligne, la collaboration entre entreprises et les services à la clientèle dans leur ensemble. De plus en plus d'utilisateurs se tournent aujourd'hui vers la messagerie instantanée en raison de son coût modique et de sa commodité d'utilisation, ce qui a des incidences considérables sur les secteurs de communication classiques. A l'heure actuelle, les opérateurs de télécommunication fournissent de plus en plus des services IM, mais parallèlement, la messagerie instantanée est de plus en plus exposée au spam qui se propage sur les services vocaux et le service de messages courts (SMS). La mesure dans laquelle les opérateurs de télécommunication du monde entier mesurent l'ampleur du phénomène que constitue le spam par messagerie instantanée (SPIM) ou en subissent les conséquences varie d'un opérateur à part l'autre. Le SPIM entraîne non seulement un gaspillage des ressources du réseau, mais fait perdre du temps aux utilisateurs et nuit à leur productivité. En outre, le SPIM est utilisé pour le hameçonnage (phishing) et la propagation de virus, de vers informatiques, de logiciels espions et d'autres types de logiciels malveillants et peut même contenir des informations préjudiciables insultantes pour les utilisateurs. En conséquence, le SPIM nuit à la satisfaction des utilisateurs qui ont recours à la messagerie instantanée et constitue un facteur important qui en freine l'utilisation.

Bien que de nombreuses mesures de lutte contre le spam aient été prises en ce qui concerne les systèmes IM, il subsiste encore dans ces systèmes de nombreuses failles susceptibles d'engendrer des SPIM, telles que le taux d'enregistrement non limité, l'absence de confirmation lors de la réception de messages, les mécanismes de transmission réseau non fiables, l'absence de contrôle de la fréquence d'envoi des messages pour les utilisateurs et les vulnérabilités inévitables des systèmes IM.

La présente Recommandation définit les exigences techniques à prévoir pour lutter contre le SPIM, compte tenu des fonctions d'un système IM, afin de stopper les moyens de production et de propagation du SPIM. Ainsi, il est important d'exiger qu'un mécanisme d'enregistrement soit conçu pour empêcher les enregistrements automatiques de masse et que le système IM offre aux utilisateurs la possibilité de recevoir ou de bloquer tous les messages provenant d'entités autorisées/non autorisées ainsi que pour limiter la fréquence d'envoi de messages d'un utilisateur si ceux-ci ont dépassé un seuil normal.

# Recommandation UIT-T X.1248

## Exigences techniques pour lutter contre le spam par messagerie instantanée

### 1 Domaine d'application

La présente Recommandation recense les types et les caractéristiques du spam par messagerie instantanée (SPIM). Afin d'atténuer la production et la propagation du SPIM, la présente Recommandation indique les exigences techniques à respecter pour lutter contre le SPIM, tant en ce qui concerne le client de la messagerie instantanée (IM) que le serveur IM. La présente Recommandation porte principalement sur les mesures de lutte contre le SPIM de la couche du système IM et est applicable aux opérateurs de services IM.

### 2 Références

Aucune.

### 3 Définitions

#### 3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

**3.1.1 messagerie instantanée (IM)** [b-IETF RFC 3428]: échange de contenus entre un ensemble de participants en temps quasi réel. Les contenus sont généralement des messages de texte courts, mais tel n'est pas nécessairement le cas.

**3.1.2 spam** [b-UIT-T X.1240]: la signification du terme "spam" dépend de la façon dont la vie privée est perçue dans chaque pays et de ce que constitue le spam dans chaque pays, du point de vue technologique, économique, social et pratique. En particulier, ce sens évolue et se diversifie au fur et à mesure du développement des technologies, donnant lieu à de nouvelles possibilités d'utilisation abusive des communications électroniques. Bien qu'aucune définition du spam n'ait été adoptée à l'échelle mondiale, ce terme est couramment employé pour décrire des communications électroniques de masse non sollicitées transmises par courrier électronique (courriel) ou par messagerie mobile pour promouvoir des produits ou services commerciaux.

**3.1.3 spam par messagerie instantanée (SPIM)** [b-UIT-T X.1244]: spam visant des utilisateurs d'un service de messagerie instantanée.

**3.1.4 spimmeur** [b-UIT-T X.1244]: expéditeur de SPIM.

#### 3.2 Termes définis dans la présente Recommandation

Aucun.

### 4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ID identité

IM messagerie instantanée (*instant messaging*)

IP protocole Internet (*Internet protocol*)

SMS service de messages courts (*short message service*)

SPIM spam par messagerie instantanée (*spam over instant messaging*)

## 5 Conventions

Aucune.

## 6 Caractéristiques et scénarios de création du SPIM

On entend par SPIM un message instantané reçu par un utilisateur qui est considéré comme indésirable ou qui gêne cet utilisateur. En conséquence, le SPIM présente les caractéristiques suivantes:

– En général, le SPIM se produit en temps réel. Dans le cas où l'expéditeur et le destinataire sont tous deux en ligne, le SPIM est reçu pratiquement en même temps qu'il est envoyé. Même si le destinataire n'est pas actuellement en ligne, le SPIM peut être reçu immédiatement après que le destinataire est en ligne.

– Les SPIM sont souvent envoyés en masse, de sorte qu'un grand nombre de messages ayant le même contenu sont transmis en même temps.

– Le terme "spimmeur" est employé pour définir un expéditeur non autorisé de SPIM vers des destinataires IM. Toutefois, il arrive que le compte d'un ami soit infecté et chargé d'envoyer un SPIM en raison d'une infection par un code malveillant ou de la divulgation des informations sur le compte et le mot de passe. Un SPIM envoyé par des amis induit davantage en erreur, en particulier lorsqu'il contient des liens vers des sites web malveillants ou des fichiers exécutables sur lesquels cliqueront la plupart des destinataires; en conséquence, leurs systèmes ont davantage de chances d'être infectés par un code malveillant.

– Il n'est pas facile de suivre la trace d'un SPIM, dans la mesure où des comptes, qui ne correspondent généralement pas à une identité réelle, peuvent être créés de manière arbitraire.

La création d'un SPIM est étroitement liée aux fonctions du système IM (voir l'Appendice I) et les scénarios susceptibles de conduire à la création d'un SPIM sont les suivants:

– Des spimmeurs peuvent utiliser un logiciel d'enregistrement automatique pour enregistrer un grand nombre de comptes, puis utiliser ces comptes pour propager des SPIM.

– Des utilisateurs malveillants peuvent utiliser de faux comptes IM, puis les utiliser pour envoyer des SPIM.

– Si l'auteur d'une attaque malveillante a obtenu le contrôle du compte d'un utilisateur légitime sans autorisation, il peut modifier les informations de l'utilisateur (mot de passe par exemple) ou d'autres informations d'authentification pour utiliser ce compte (souvent pendant longtemps) pour envoyer des SPIM.

– Si les paramètres de réception d'un client IM sont modifiés sans autorisation, des SPIM pourront être reçus sans restriction aucune.

– Des messages instantanés peuvent être altérés volontairement pendant la transmission. Des messages publicitaires ou un code malveillant peuvent être insérés dans un message instantané puis transformés en SPIM.

– Etant donné qu'il n'existe pas de mécanisme de confirmation, un spimmeur peut être libre d'ajouter des amis, puis leur envoyer un SPIM.

Pour empêcher l'envoi de SPIM, il est nécessaire de tenir dûment compte de leurs caractéristiques et des scénarios susceptibles de conduire à des SPIM, afin de prendre des mesures de prévention complètes.

## 7 Architecture fonctionnelle IM pour lutter contre le SPIM

### 7.1 Vue d'ensemble

L'architecture fonctionnelle IM pour lutter contre le SPIM est représentée sur la Figure 7-1.

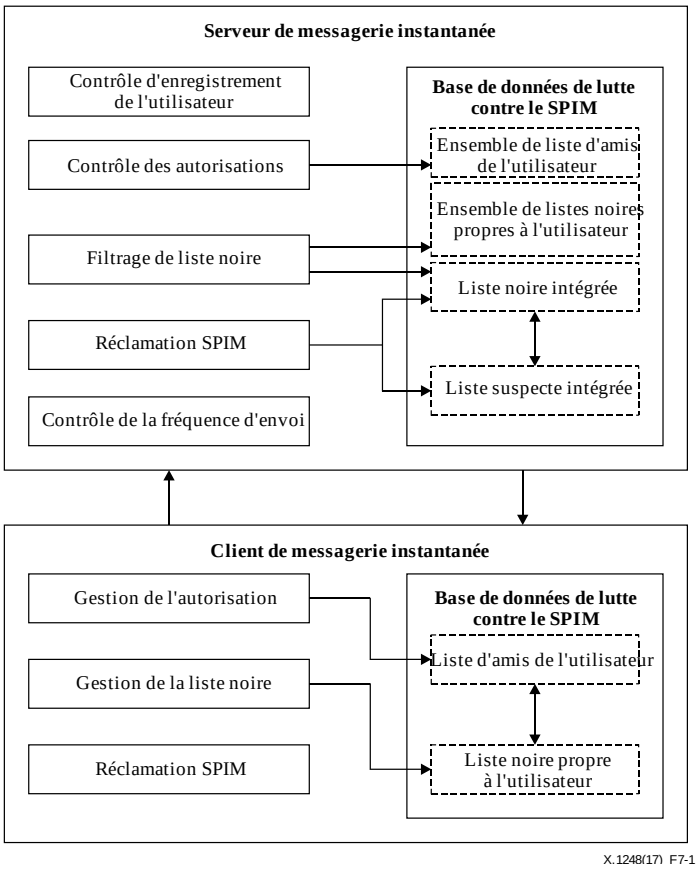


**Figure 7-1 – Architecture fonctionnelle IM pour lutter contre le SPIM**

Cette architecture intègre les fonctionnalités de lutte contre le SPIM, notamment les filtres de liste noire, les contrôles d'enregistrement de l'utilisateur et les réclamations SPIM. Elle prend surtout en charge le filtrage fondé sur la limitation de la fréquence d'envoi de la messagerie instantanée et le contrôle de l'autorisation de l'expéditeur d'un message instantané.

L'Appendice I décrit de manière plus détaillée le client IM et les fonctionnalités du serveur IM ainsi que les rôles respectifs de l'expéditeur IM, du destinataire IM et du spimmeur.

## 7.2 Fonctionnalités des éléments

### 7.2.1 Serveur IM

Les fonctionnalités de l'élément serveur IM comprennent les six éléments suivants:

1) Contrôle de l'enregistrement de l'utilisateur

   Il faut obligatoirement utiliser des méthodes de confirmation manuelles, telles que les codes de vérification, les vérifications par courrier électronique et les codes de vérification par SMS, pour empêcher l'enregistrement automatique d'utilisateurs. Cela empêchera les spimmeurs qui disposent d'un grand nombre de comptes enregistrés automatiquement d'envoyer des SPIM.

2) Contrôle d'autorisation

   Il faut obligatoirement retransmettre la demande d'un utilisateur visant à ajouter un ami et autoriser les relations entre cet ami et l'utilisateur sur la base des informations fournies en retour par le client IM.

3) Filtrage par liste noire

   Le serveur IM doit obligatoirement filtrer les messages instantanés sur la base d'une liste noire intégrée et d'un ensemble de listes noires propres à l'utilisateur.

4) Réclamations SPIM

Les réclamations des utilisateurs concernant les comptes qui envoient des SPIM doivent obligatoirement être acceptées et il faut obligatoirement déterminer s'il y a lieu d'ajouter ces comptes dans la liste noire suspecte intégrée ou dans la liste noire intégrée. Il faut obligatoirement avoir une interface avec les systèmes de traitement des réclamations extérieures concernant le SPIM et importer et exporter la liste noire intégrée.

5) Contrôle de la fréquence d'envoi

Il faut obligatoirement que le nombre de messages instantanés envoyés par le même compte pendant une période donnée soit contrôlé. Il y a lieu de supprimer les messages instantanés dépassant ce seuil.

6) Base de données de lutte contre le SPIM

- Ensemble de listes d'amis de l'utilisateur: comprend les listes d'amis de tous les utilisateurs gérés par le serveur IM. Il faut obligatoirement que l'ensemble de listes d'amis de l'utilisateur du serveur IM soit synchronisée avec les listes d'amis de l'utilisateur des clients IM.
- Ensemble de listes noires propres à l'utilisateur: comprend les listes noires propres à l'utilisateur de tous les utilisateurs gérés par le serveur IM. Il faut obligatoirement que l'ensemble de listes noires propres à l'utilisateur soit synchronisé dans le serveur IM avec les listes noires propres à l'utilisateur des clients IM.
- Liste noire intégrée: comprend les comptes contenus dans les réclamations signalées par des utilisateurs et les comptes détectés par le serveur IM. Par exemple, quand la fréquence des messages envoyés par un utilisateur IM dépasse un seuil donné, l'identificateur de l'expéditeur doit être classé et ajouté dans la liste noire intégrée par le serveur IM. La liste noire intégrée comprend également les comptes qui sont importés depuis d'autres systèmes, tels que les autres serveurs IM.
- Liste suspecte intégrée: il faut obligatoirement qu'une liste de tous les comptes suspects gérés par le serveur soit créée. La liste suspecte intégrée peut être créée par le biais des réclamations des utilisateurs, de l'importation d'autres systèmes, etc.

### 7.2.2 Client IM

La fonctionnalité de l'élément client IM comprend les quatre éléments suivants:

1) Gestion d'autorisation

Les deux principaux éléments à prendre en compte devraient être le contrôle de visibilité de l'identité IM (ID) et la gestion des demandes émanant d'entités non autorisées. En ce qui concerne le contrôle de visibilité d'un identificateur IM, il est nécessaire qu'un utilisateur détermine si les informations qui le concernent (identificateur IM, surnom, lieu) devraient être visibles par un utilisateur non autorisé. Pour ce qui est de la gestion des demandes émanant d'entités non autorisées, un utilisateur doit obligatoirement pouvoir choisir une politique appropriée lui permettant de traiter ces demandes. Un utilisateur devrait pouvoir procéder à une approbation manuelle, exiger une réponse précise à une question personnelle, voire bloquer toutes les demandes. De plus, un utilisateur devrait pouvoir indiquer quels sont ses amis de confiance et gérer sa liste d'amis au niveau du client IM.

2) Gestion de la liste noire

Les utilisateurs devraient pouvoir gérer eux-mêmes leur liste noire propre à l'utilisateur et tous les messages envoyés depuis des comptes indiqués dans leur liste noire propre à l'utilisateur devraient être bloqués. L'utilisateur devrait pouvoir ajouter et supprimer, voire partager, leur liste noire propre à l'utilisateur.

3) Réclamations concernant un SPIM

Le client IM devrait être doté d'une fonction lui permettant de soumettre des réclamations sur les comptes qui envoient des SPIM. Un compte faisant l'objet d'une réclamation peut être un contact dans la liste d'amis de l'utilisateur, un membre d'un groupe IM, voire un compte non autorisé qui envoie des demandes d'autorisation.

4) Base de données pour la lutte contre le SPIM

- Liste d'amis de l'utilisateur: il faut obligatoirement stocker une liste d'amis approuvée par l'utilisateur.
- Liste noire propre à l'utilisateur: cette liste est définie par les utilisateurs et comprend les comptes dans lesquels l'utilisateur veut bloquer des messages.

La base de données située au niveau du client IM doit être automatiquement transférée dans le serveur IM.

# 8 Procédures de travail

## 8.1 Procédure de travail pour le contrôle de la fréquence d'envoi

Le seuil qui définit le nombre maximal de messages pouvant être envoyés d'un compte IM donné pendant une période donnée devrait être fixé au niveau du serveur IM.

Ce seuil devrait être étudié ou défini au moyen d'un grand nombre d'échantillons de messages de l'utilisateur, par le biais de technologies telles que l'apprentissage machine, l'apprentissage profond, etc. Il devrait être défini respectivement pour différents scénarios, notamment, sans toutefois que cette liste soit limitative, pour les scénarios suivants:

– les messages instantanés sont envoyés à un groupe et l'expéditeur est un membre de ce groupe;
– les messages instantanés sont envoyés à un groupe, mais l'expéditeur n'est pas un membre de ce groupe;
– les messages instantanés sont envoyés à un ou plusieurs amis de l'expéditeur;
– les messages instantanés sont envoyés à des personnes qui ne sont pas des amis de l'expéditeur.

Lorsque le serveur IM reçoit des messages envoyés par un compte donné, il doit mettre en oeuvre le contrôle de la fréquence d'envoi par le biais du processus ci-après, illustré sur la Figure 8-1:

– Compter le nombre de messages envoyés par le compte pendant une période donnée.
– Comparer le nombre de messages envoyés (n) avec le seuil minimal fixé pour tous les scénarios. Si le nombre (n) dépasse le seuil minimal, le serveur IM détermine plus avant à quel scénario il correspond et si le nombre (n) dépasse le seuil de ce scénario donné. Si tel n'est pas le cas, le serveur IM envoie les messages.
– Si le nombre de messages envoyés (n) dépasse le seuil donné, le serveur IM vérifie si le compte figure dans la liste suspecte intégrée. Si tel est le cas, le serveur IM rejette les messages; si tel n'est pas le cas, il retransmet les messages, mais compte le nombre de dépassements du seuil (m). Si ce nombre (m) est supérieur à un nombre donné ($\alpha$), le serveur IM ajoute le compte dans la liste suspecte.

Le processus de mise en oeuvre du contrôle de la fréquence d'envoi est illustré sur la Figure 8-1:

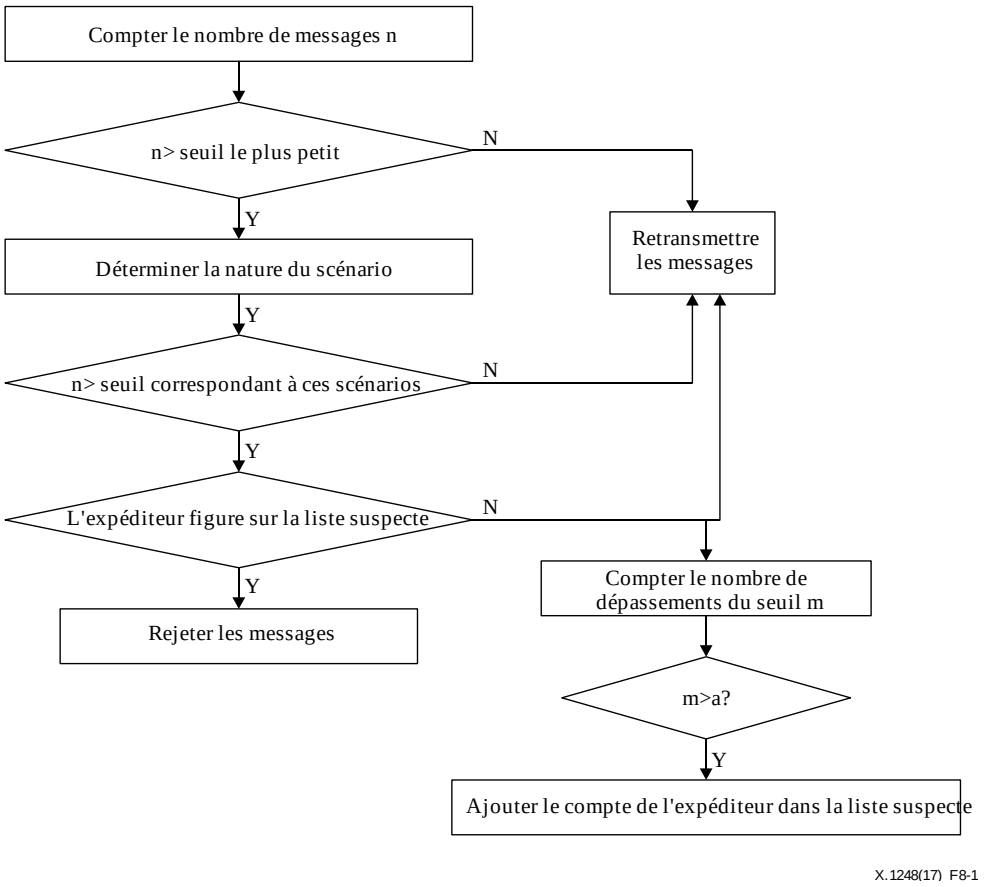


**Figure 8-1 – Processus de mise en oeuvre du contrôle de la fréquence d'envoi**

## 8.2 Procédures de travail pour les listes noires

Les systèmes IM sont relativement indépendants, de sorte que les fournisseurs de services IM sont tenus d'établir leurs propres listes noires intégrées pour leurs serveurs IM. De plus, dans l'intérêt des utilisateurs, les listes noires propres à l'utilisateur doivent obligatoirement être fournies au niveau des clients IM.

Le processus d'interaction entre tous les types de listes noires d'un système IM est le suivant:

– L'utilisateur modifie sa liste noire propre à l'utilisateur au niveau du client IM. Le serveur IM surveille en temps réel la liste noire propre à l'utilisateur et met à jour l'ensemble de listes noires propres à l'utilisateur en cas de changements apportés à cette liste.

– Le serveur IM suit le nombre de fois que le même compte a été ajouté dans les listes noires propres à l'utilisateur. Si ce nombre dépasse un seuil donné, le serveur IM ajoute ce compte dans la liste noire intégrée.

– Le serveur IM ajoutera le compte référencé dans la réclamation d'un client dans la liste noire suspecte intégrée, si le compte ne se trouve ni dans la liste noire suspecte intégrée, ni dans la liste noire intégrée. Le serveur IM compte le nombre de fois qu'une réclamation a été enregistrée pour le compte; si ce nombre dépasse un seuil donné, le serveur IM ajoute ce compte dans la liste noire intégrée.

Le processus de filtrage des messages fondé sur les listes noires est le suivant:

– Lorsque le serveur IM reçoit un message, il vérifie si le compte de l'expéditeur se trouve dans la liste noire intégrée; si tel est le cas, le serveur IM rejette le message.

– Si le compte de l'expéditeur ne se trouve pas dans la liste noire intégrée, le serveur IM peut vérifier plus en détail si ce compte se trouve dans la liste noire propre à l'utilisateur du

destinataire et, si tel est le cas, il rejette le message. Dans le cas contraire, le serveur IM retransmet le message.

### 8.3 Procédures de gestion d'autorisation

Il est recommandé qu'un client IM soit doté d'une fonction permettant aux utilisateurs de définir la nature des messages qui peuvent être reçus, et le serveur IM devrait pouvoir filtrer les messages non désirés en fonction de la définition de l'utilisateur, afin d'empêcher les expéditeurs non autorisés (personnes qui ne sont pas des amis, membres d'un groupe qui ne sont pas des amis, amis d'autres systèmes IM, contacts téléphoniques, par exemple) d'envoyer des messages non désirés. Les scénarios qui autorisent des expéditeurs comportent, sans toutefois que cette liste soit limitative, les cinq étapes ci-après:

1) Définir le client IM à "recevoir uniquement les messages d'amis". Lorsque le serveur IM reçoit un message envoyé par l'utilisateur B à l'utilisateur A, il vérifie si l'utilisateur B se trouve dans la liste d'amis de l'utilisateur A. Si tel n'est pas le cas, le serveur rejette le message.
2) Définir le client IM à "recevoir des messages provenant d'un groupe que le client a expressément rejoint". Lorsque le serveur IM reçoit un message envoyé par le groupe B à l'utilisateur A, il vérifie si l'utilisateur A est un membre du groupe B. Si tel n'est pas le cas, le serveur rejette le message. De plus, lorsque le serveur IM reçoit une invitation envoyée par un membre du groupe B à l'utilisateur A, il devrait être autorisé par l'utilisateur A avant que le serveur IM n'ajoute l'utilisateur A dans le groupe B.
3) Définir le client IM à "recevoir des messages provenant d'un membre du groupe avec lequel le client est ami ". Lorsque le serveur IM reçoit un message envoyé par l'utilisateur B du groupe A à l'utilisateur A, il vérifiera si l'utilisateur B se trouve dans la liste d'amis de l'utilisateur A. Si tel n'est pas le cas, le serveur rejette le message.
4) Définir le client IM à "recevoir des messages provenant de comptes d'autres systèmes IM ou contacts téléphoniques, uniquement après avoir expressément ajouté ces comptes ou contacts en tant qu'amis". Lorsque le serveur IM reçoit un message envoyé par le compte B associé à l'utilisateur A, il vérifie si le compte B se trouve dans la liste d'amis de l'utilisateur A. Si tel n'est pas le cas, le serveur rejette le message. De plus, lorsque le serveur IM reçoit une demande visant à ajouter un ami du compte B dans la liste d'amis de l'utilisateur A, il devrait être autorisé par l'utilisateur A avant que le serveur n'ajoute le compte B dans la liste d'amis de l'utilisateur A.
5) Définir le client IM à "limiter aux amis l'établissement d'une connexion point à point". Lorsque le serveur IM reçoit une demande de l'utilisateur B visant à établir une connexion point à point avec l'utilisateur A, il vérifiera si l'utilisateur B se trouve dans la liste d'amis de l'utilisateur A. Si tel est le cas, le serveur IM enverra la demande de l'utilisateur B à l'utilisateur A et aidera l'utilisateur A ainsi que l'utilisateur B à établir une connexion point à point. Dans le cas contraire, le serveur IM rejettera la demande de l'utilisateur B.

Les relations entre l'utilisateur A, l'utilisateur B, le groupe A, le groupe B et le compte B sont illustrées sur la Figure 8-2.

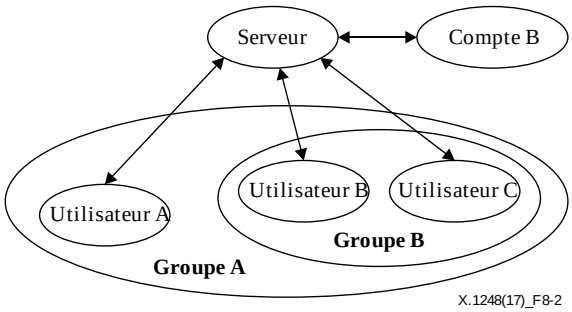


**Figure 8-2 – Relations entre les utilisateurs et les groupes**

## 8.4 Procédures de gestion de l'enregistrement des utilisateurs

Afin d'empêcher l'enregistrement automatique de comptes, les systèmes IM devraient prendre une ou plusieurs mesures de confirmation manuelles, par exemple le code de vérification, la vérification par courrier électronique, le code de vérification par SMS.

Lorsqu'un utilisateur soumet des informations d'enregistrement (nom d'utilisateur, mot de passe, numéro de téléphone mobile, adresse électronique par exemple) au niveau du client IM ou sur la page web de l'enregistrement de l'utilisateur IM, le serveur IM renvoie une confirmation d'enregistrement à l'utilisateur, par exemple un code de vérification, un code de vérification par SMS ou un courrier électronique de confirmation d'enregistrement.

Une fois que l'utilisateur renvoie la confirmation d'enregistrement au serveur IM, le serveur IM vérifie la confirmation d'enregistrement soumise par l'utilisateur. Si la vérification est valable, le serveur IM renvoie à l'utilisateur un message d'enregistrement réussi et sauvegarde les informations d'enregistrement de l'utilisateur dans la base de données. Dans le cas contraire, il renvoie un message d'échec de l'enregistrement.

Le système IM devrait assurer l'interface avec une passerelle ou un serveur de messagerie déployé, afin de mettre en oeuvre la fonction d'envoi à l'utilisateur d'un code de vérification par SMS ou d'un message électronique de confirmation d'enregistrement.

## 8.5 Procédures applicables aux réclamations concernant un SPIM

Les procédures ci-après de signalement des réclamations concernant un SPIM devraient être prises en charge:

1) Réclamation par l'intermédiaire du client IM. Selon cette méthode, la procédure de traitement des réclamations est illustrée de la façon suivante:

   Les utilisateurs IM indiquent le compte du SPIM au niveau du client IM après avoir reçu le SPIM; la réclamation est envoyée au serveur IM. Le serveur IM devrait disposer d'un seuil de réclamation prédéfini. Dès réception d'une réclamation d'un utilisateur, le serveur IM vérifie en premier lieu si le compte figure déjà dans la liste noire suspecte intégrée ou dans la liste noire intégrée. Si tel n'est pas le cas, le serveur IM ajoute le compte dans la liste suspecte intégrée et compte le nombre de fois que le compte a fait l'objet de réclamations. Si ce nombre dépasse le seuil prédéfini, le serveur IM ajoute le compte dans la liste noire intégrée. Si le compte figure déjà dans la liste noire suspecte intégrée, le serveur IM additionne le nombre de fois que le compte a fait l'objet de plaintes. Si cette valeur dépasse le seuil prédéfini pendant une période donnée, le serveur IM ajoute ce compte dans la liste noire intégrée. Si le compte figure déjà dans la liste noire intégrée, le serveur IM ne fait rien. Les messages envoyés par ce compte ultérieurement devraient être rejetés par le serveur IM.

2) Réclamation par l'intermédiaire d'un système extérieur de traitement des réclamations concernant un SPIM. Selon cette méthode, la procédure de traitement des réclamations est illustrée de la façon suivante:

Les utilisateurs IM soumettent une réclamation à un système extérieur de traitement des réclamations concernant un SPIM après avoir reçu un SPIM. Le système extérieur de traitement des réclamations concernant un SPIM est chargé d'analyser la réclamation de l'utilisateur et de déterminer s'il y a lieu d'ajouter le compte concerné dans la liste noire. Le serveur IM assure une interface avec le système extérieur de traitement des réclamations concernant un SPIM et importe ou exporte la liste noire depuis l'interface. Les messages envoyés par les comptes figurant dans la liste noire devraient être rejetés par le serveur IM.

### 8.6 Procédure de filtrage de SPIM

Lorsqu'un serveur IM reçoit des messages instantanés, il procède à un filtrage de SPIM sur la base de la liste noire intégrée et de l'ensemble de listes noires propres à l'utilisateur; ce processus est décrit au § 8.2.

Si le compte de l'expéditeur IM ne se trouve pas dans la liste noire intégrée et dans l'ensemble de listes noires propres à l'utilisateur, le serveur IM procède au filtrage de SPIM sur la base du contrôle de l'autorisation et analyse si l'expéditeur est autorisé à envoyer des messages au destinataire (autorisation qui est définie par le destinataire). Si tel n'est pas le cas, le message est supprimé. Le scénario d'autorisation est décrit au § 8.3.

Si tel est le cas, le serveur IM procède au filtrage de SPIM sur la base de la limite de la fréquence d'emploi; ce processus est décrit au § 8.1.

# Appendice I

## Rôle et fonctions du système IM

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

Le modèle de base du système IM est représenté sur la Figure I.1.

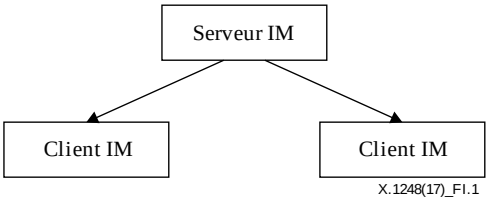


**Figure I.1 – Modèle de base du système IM**

Le modèle de base du système IM comprend le serveur IM et plusieurs clients IM homogènes. Le serveur IM est utilisé pour recevoir et retransmettre des messages instantanés qui sont envoyés par les clients IM. Le client IM joue un double rôle: celui d'expéditeur IM et de destinataire IM. L'expéditeur IM retransmet les messages instantanés au serveur IM pour la remise et le serveur IM s'efforce de remettre les messages aux destinataires IM correspondants. Si un expéditeur IM envoie un SPIM, il est alors considéré comme un spimmeur.

Les fonctions du système IM doivent être menées à bien par le serveur IM, les clients IM et l'interaction entre eux.

Les principales fonctions du serveur IM sont les suivantes:

– Gestion de l'utilisateur, par exemple enregistrement, connexion et déconnexion et modification du compte de l'utilisateur.
– Gestion de messages instantanés, par exemple envoi, réception et transmission de messages.
– Gestion des amis, par exemple recherche d'amis, gestion de la liste d'amis.
– Gestion du système, par exemple configuration, mise à jour, démarrage/redémarrage/sortie du système.

Les principales fonctions du client IM sont les suivantes:

– Gestion de l'utilisateur, par exemple enregistrement, connexion et déconnexion de l'utilisateur.
– Gestion de messages instantanés, par exemple envoi et réception de messages.
– Gestion des amis, par exemple adjonction, suppression et recherche d'amis.
– Gestion du client, par exemple configuration de paramètres, mise à jour et démarrage/redémarrage/sortie au niveau du client.

# Bibliographie


[b-UIT-T X.1231] Recommandation UIT-T X.1231 (2008), *Stratégies techniques de lutte contre le spam*.

[b-UIT-T X.1240] Recommandation UIT-T X.1240 (2008), *Technologies intervenant dans la lutte contre le spam par courrier électronique*.

[b- UIT-T X.1244] Recommandation UIT-T X.1244 (2008), *Aspects généraux de la lutte contre le spam dans les applications multimédias IP*.

[b-IETF RFC 2778] IETF RFC 2778 (2000), *A Model for Presence and Instant Messaging*.

[b-IETF RFC 3428] IETF RFC 3428 (2002), *Session Initiation Protocol (SIP) Extension for Instant Messaging*.

## SÉRIES DES RECOMMANDATIONS UIT-T

| | |
|---|---|
| Série A | Organisation du travail de l'UIT-T |
| Série D | Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC |
| Série E | Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains |
| Série F | Services de télécommunication non téléphonique |
| Série G | Systèmes et supports de transmission, systèmes et réseaux numériques |
| Série H | Systèmes audiovisuels et multimédias |
| Série I | Réseau numérique à intégration de services |
| Série J | Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias |
| Série K | Protection contre les perturbations |
| Série L | Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures |
| Série M | Gestion des télécommunications y compris le RGT et maintenance des réseaux |
| 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 et mesures et tests associés |
| 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, communication entre systèmes ouverts et sécurité** |
| Série Y | Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes |
| Série Z | Langages et aspects généraux logiciels des systèmes de télécommunication |

Imprimé en Suisse
Genève, 2017