Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1243

(12/2010)

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

Sécurité du cyberespace – Lutte contre le pollupostage

Système de passerelle interactive pour lutter contre le spam

Recommandation UIT-T X.1243

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	
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	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 pollupostage	**X.1230–X.1249**
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
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

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

Recommandation UIT-T X.1243

Système de passerelle interactive pour lutter contre le spam

Résumé

La Recommandation UIT-T X.1243 spécifie le système de passerelle interactive pour lutter contre le spam comme moyen technique de lutte contre le spam interdomaine. Le système de passerelle permet la notification des spams au sein de différents domaines et empêche le trafic de spam de passer d'un domaine à un autre.

De plus, cette Recommandation spécifie l'architecture du système de passerelle, décrit les entités, protocoles et fonctions de base du système de passerelle et fournit les mécanismes de détection du spam, de partage d'informations et des actions propres au système de passerelle pour lutter contre le spam.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T X.1243	2010-12-17	17

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 œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1243

Système de passerelle interactive pour lutter contre le spam

1 Domaine d'application

Le système de passerelle interactive pour lutter contre le spam est un mécanisme interactif général de lutte contre les divers messages de spam interdomaine, y compris le spam par courriel, le spam par SMS, etc., destiné à permettre le partage d'informations pour lutter contre le spam entre les différents domaines, et à empêcher l'envoi et la réception de spams. La présente Recommandation prend en charge la diversité des techniques de filtrage pour lutter contre le spam, et offre une certaine souplesse pour les techniques à venir.

Avant d'adopter la présente Recommandation, il convient de s'assurer de sa conformité avec toutes les lois et réglementations nationales applicables.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T X.509] Recommandation UIT-T X.509 (2000) | ISO/IEC 9594-8:2001, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 spam [b-UIT-T X.1240]: le sens du mot "spam" dépend de la perception du respect de la vie privée et de ce que constitue le spam au niveau de 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.

3.1.2 spammeur [b-UIT-T X.1240]: entité ou personne qui crée et envoie des spams.

3.2 Termes définis dans la présente Recommandation

Les termes suivants sont définis dans la présente Recommandation:

3.2.1 système de passerelle interactive pour lutter contre le spam (IGCS, *interactive gateway system for countering spam*): le système de passerelle interactive pour lutter contre le spam est une entité qui est responsable de la détection et du blocage du spam. Elle dispose d'une paire de fonctions, à savoir la fonction de passerelle d'expédition (SGF) et la fonction de passerelle de

réception (RGF). Un système IGCS devrait travailler avec d'autres homologues pour mettre en œuvre toutes les fonctions de lutte contre le spam.

3.2.2 base de données locale de lutte contre le spam: ce terme désigne une base de données utilisée pour l'enregistrement des informations concernant les spams, des listes noires, des règles de lutte contre les spams pour les fonctions de passerelle de réception et fonctions de passerelle d'expédition.

3.2.3 modalité: une modalité fait référence au(x) codage(s) des informations contenant des informations perceptibles pour un être humain.

3.2.4 message multimodal: un message multimodal fait référence au message multimédia contenant des informations codées de différentes manières pour interagir avec de multiples modalités.

3.2.5 agent de réception: un agent de réception est un serveur qui reçoit des messages pour des récepteurs de messages. Dans les applications de courriels, un serveur POP fait office d'agent de réception.

3.2.6 fonction de passerelle de réception: la fonction de passerelle de réception est une fonction de la partie réceptrice pour lutter contre le spam, qui détecte et bloque le spam au cours du processus de réception des messages.

3.2.7 agent d'expédition: un agent d'expédition est un serveur qui envoie des messages pour des expéditeurs de messages. Dans les applications de courriels, un serveur SMTP fait office d'agent d'expédition.

3.2.8 fonction de passerelle d'expédition: une fonction de passerelle d'expédition est une fonction de la partie expéditrice pour lutter contre le spam, qui détecte et bloque le spam au cours du processus d'expédition des messages.

3.2.9 homologue de lutte contre le spam: au cours du processus de lutte contre le spam, deux systèmes IGCS travaillent ensemble pour identifier et bloquer le spam, donc un système IGCS est un homologue de lutte contre le spam pour un autre système IGCS.

3.2.10 protocole d'échange entre homologues de lutte contre le spam: le protocole est défini pour échanger les messages d'alerte et listes noires entre passerelles de lutte contre le spam.

3.2.11 protocole de signalisation des spams par les utilisateurs: le protocole est défini pour que les récepteurs de messages puissent signaler les spams aux passerelles.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et les acronymes suivants:

Email courrier électronique (courriel) (*electronic mail*)

FE entité fonctionnelle (*functional entity*)

IGCS système de passerelle interactive pour lutter contre le spam (*interactive gateway system for countering spam*)

IM message instantané (*instant message*)

IRC conversation relayée par l'Internet (*Internet relay chat*)

LscDB base de données locale de lutte contre le spam (*local spam-countering database*)

POP protocole postal (*post office protocol*)

RA agent de réception (*receiver agent*)

RBL liste noire en temps réel (*real-time blackhole list*)

RGF fonction de passerelle de réception (*receiver gateway function*)

SA agent d'expédition (*sender agent*)

SCPP protocole d'échange entre homologues de lutte contre le spam (*spam-countering peering protocol)*

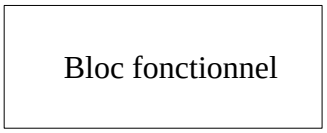
SGF fonction de passerelle d'expédition (*sender gateway function*)

SMTP protocole de transfert de courrier simple (*simple mail transfer protocol*)

WPF filtre fondé sur des paramètres pondérés (*weighted parameter filter*)

5 Conventions

Bloc fonctionnel: dans le contexte d'un système de passerelle interactive pour lutter contre le spam, un "bloc fonctionnel" se définit comme un ensemble de fonctionnalités. Il est représenté par le symbole suivant:



6 Architecture

6.1 Entités et fonctions de lutte contre le spam

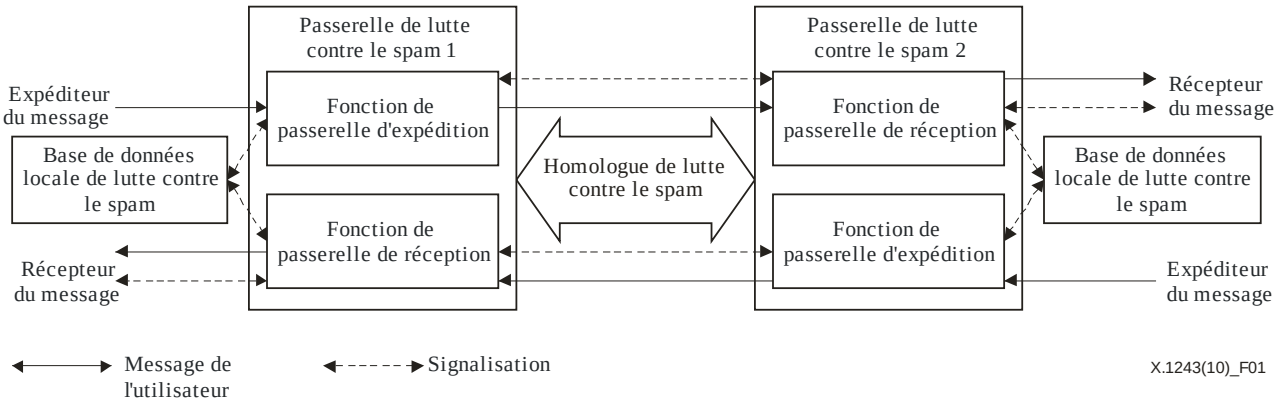


Figure 1 – Architecture d'un système de passerelle interactive pour lutter contre le spam

Système de passerelle interactive pour lutter contre le spam (IGCS)

Un système IGCS se compose d'une passerelle de lutte contre le spam et d'une base de données locale de lutte contre le spam. La passerelle de lutte contre le spam a deux entités: les fonctions SGF et RGF. Ces deux entités fonctionnelles agissent toutes les deux comme des points de décision des politiques et comme des points de mise en application des politiques. La fonction SGF est utilisée pour traiter le spam sortant et la fonction RGF est utilisée pour traiter le spam entrant. La base de données locale de lutte contre le spam (lscDB) fournit les règles de lutte contre le spam pour l'identification du spam et les mesures de lutte contre le spam. La passerelle locale de lutte contre le spam est également responsable de la mise à jour des règles de lutte contre le spam dans la base de données lscDB.

Les responsabilités des fonctions RGF et SGF se définissent comme suit:

Une fonction RGF de base a trois responsabilités:

- Prendre des mesures de lutte contre le spam (bloquer, isoler ou alerter, etc.) sur le spam entrant connu.
- Détecter le nouveau spam par le biais des rapports de spam du récepteur et mettre à jour les règles locales de lutte contre le spam dans la base de données lscDB.
- Lorsqu'un spam est détecté, envoyer une notification à la fonction SGF de l'expéditeur du spam.

Une fonction SGF a deux responsabilités:

- Prendre des mesures de lutte contre le spam (bloquer, isoler ou alerter, etc.) sur le spam sortant connu.
- Traiter les notifications de spam émises par la fonction RGF du récepteur et mettre à jour les règles locales de lutte contre le spam dans la base de données lscDB.

Base de données locale de lutte contre le spam (lscDB*, local spam-countering database*)

Une base de données lscDB est utilisée pour enregistrer les informations de lutte contre le spam. Ces informations peuvent ensuite être classées selon les trois types suivants:

- Information d'identification du spam: par exemple l'adresse d'origine du spam et les mots clés dans le champ "objet" du spam.
- Règles de lutte contre le spam: par exemple une liste noire et une liste blanche.
- Enregistrement du spam suspect: les échantillons de spam suspect signalés par les fonctions RGF et SGF.

6.2 Identification du spam

Les fonctions RGF et SGF identifient le spam connu en se basant sur les informations d'identification du spam enregistrées dans la base de données lscDB. Le spam est classé en différents niveaux et traité avec les mesures correspondantes.

6.3 Mesures de lutte contre le spam

Une fois le spam identifié, les fonctions RGF et SGF correspondantes vont prendre des mesures basées sur le niveau du spam identifié. Les mesures de lutte contre le spam peuvent notamment être les suivantes:

- Alerte au spam: la fonction RGF/SGF envoie une alerte au récepteur/à l'expéditeur du message.
- Mise en quarantaine du spam: la fonction RGF/SGF isole le message de spam et envoie périodiquement un rapport de quarantaine au récepteur/à l'expéditeur du message.
- Blocage du spam: la fonction RGF/SGF bloque le message de spam.

6.4 Découverte du spam

6.4.1 Découverte du spam par la fonction RGF

Le récepteur peut signaler les règles antispam à sa fonction RGF de service. Les règles antispam comprennent, entre autres, la liste noire d'adresses d'origine/de destination et les mots clés du champ "objet" du courriel. La fonction RGF met à jour l'identification du spam et les règles dans la base de données lscDB. Lorsqu'un message suspect entre, la fonction RGF commence le processus d'évaluation pour déterminer si le message est un spam, selon les règles de lutte contre le spam enregistrées dans la base de données lscDB. Si le message est considéré comme un spam, la fonction RGF va prendre les mesures correspondantes.

6.4.2 Découverte du spam par la fonction SGF

Le processus de découverte du spam par la fonction SGF est similaire à celui utilisé par la fonction RGF. La fonction SGF reçoit également des notifications de spam de la part de la fonction RGF du récepteur. La fonction SGF évalue les notifications de la fonction RGF et met à jour les règles de spam vérifiées dans la base de données lscDB.

6.5 Notification de spam par protocole d'échange entre homologues de lutte contre le spam

6.5.1 Découverte d'un homologue

Lorsqu'un agent d'expédition (SA) essaye d'envoyer un message à un agent de réception (RA), la procédure de découverte d'un homologue est lancée pour découvrir un système IGCS homologue actif sur le trajet de livraison du message. La procédure de découverte peut être lancée par l'un des systèmes IGCS. La relation entre homologues sera établie après le processus de prise de contact de l'authentification d'un homologue.

6.5.2 Notification des spams entre homologues

Après l'établissement d'une relation entre homologues, le système IGCS peut échanger des notifications de spam avec son homologue grâce au protocole d'échange entre homologues de lutte contre le spam. Comme le spam est à la base identifié par le récepteur, la fonction RGF du récepteur est responsable de l'identification du spam et de la fourniture des informations concernant le spam à la fonction SGF de l'expéditeur. Une fois que la fonction RGF détecte un message de spam, elle va avertir la fonction SGF de l'expéditeur par un processus de notification du spam. Après avoir reçu la notification du spam, la fonction SGF devra décider si elle l'accepte ou non en fonction de la politique locale de lutte contre le spam.

6.5.3 Aspect de sécurité

Il est recommandé d'inclure un mécanisme de certification, tel que spécifié dans [UIT-T X.509], dans le processus de notification des spams pour l'authentification des homologues. Il est recommandé de faire signer numériquement un message de notification par la fonction RGF. Il est recommandé de n'accepter un message de notification que s'il émane d'une fonction RGF fiable.

7 Techniques de filtrage pour lutter contre le spam

7.1 Considération indépendante de la technique

Un système IGCS doit prendre en charge la diversité des techniques de lutte contre le spam et être suffisamment souple pour pouvoir intégrer les techniques de filtrage du spam existantes et à venir. Chaque technique de filtrage peut être mise en œuvre de manière facultative. Afin de détecter efficacement les messages de spam, un système IGCS peut prendre en charge plusieurs techniques de filtrage et les intégrer dans un seul équipement de réseau physique. La mise en œuvre spécifique des techniques de filtrage est en dehors du domaine d'application de la présente Recommandation. La présente Recommandation ne définit que les interfaces, les formats de données pour chaque technique de filtrage permettant d'assurer l'interopérabilité dans l'échange d'informations pour lutter contre le spam entre homologues IGCS.

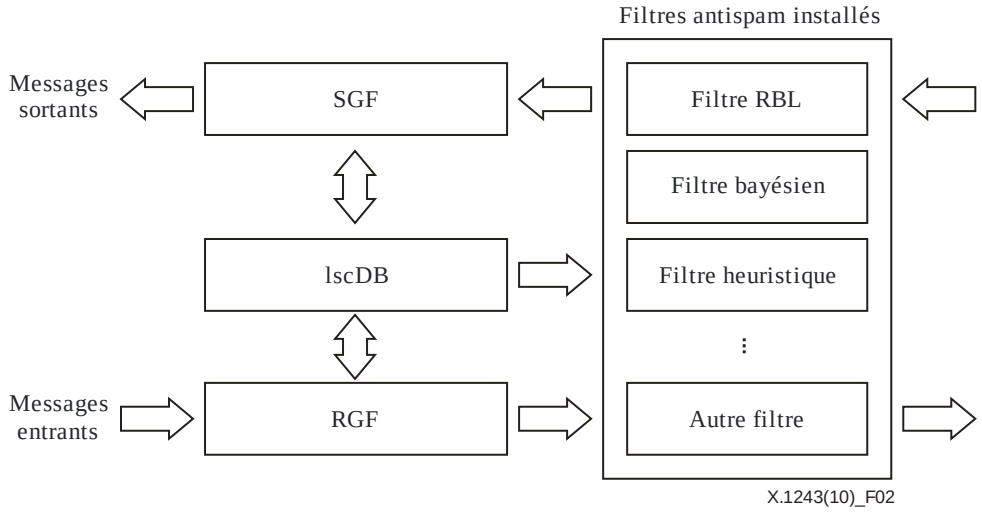


Figure 2 – Un système IGCS avec de multiples filtres de spams

7.2 Techniques de lutte contre le spam prises en charge

7.2.1 Liste d'adresses

Liste noire en temps réel (RBL, *real-time blackhole list*): une RBL est fournie par différentes organisations qui étudient le spam et développent des listes d'adresses d'origine. Un système de lutte contre le spam peut souscrire à cette liste, et déterminer si un message est un spam ou non en procédant à une vérification dans la liste.

Listes noires: les listes noires sont un mécanisme de contrôle d'accès de base qui autorise l'accès à tout le monde, excepté aux membres des listes noires. De plus, comme pour les RBL, les listes peuvent être constamment mises à jour, et le mécanisme souffre également du fait que de nombreux messages de spam ne contiennent pas d'adresses d'origine. Certains systèmes permettent également aux utilisateurs de tenir des listes blanches d'expéditeurs autorisés, qui peuvent cependant empêcher les utilisateurs de recevoir des messages qui ne sont pas des spams s'ils proviennent d'origines auparavant inconnues.

7.2.2 Filtrage heuristique

Ces filtres consistent à tester la présence dans le message de certaines caractéristiques typiques du spam, comme l'utilisation exclusive du HTML ou le type de clients auxquels le message est adressé. Le filtre attribue à chaque critère une pondération calculée par apprentissage par référence à une série de messages connus et une série de courriels connus comme légitimes.

Ces filtres présentent le risque qu'un message utilisant des techniques relatives aux spams – messages spectaculaires en HTML, par exemple – soit classé comme un spam.

Ces filtres peuvent détecter une grande proportion de messages et ne nécessitent ni apprentissage ni configuration. Toutefois, comme ils utilisent un grand nombre de tests, il vaut mieux changer la configuration des tests qui sont réalisés et des résultats retenus pour classer les messages comme spams.

7.2.3 Filtrage bayésien

Le principe du filtrage bayésien est que son moteur de lutte contre le spam est conditionné par un ensemble de spams connus et un ensemble de messages connus pour être légitimes. Après le processus de conditionnement, les caractéristiques du vocabulaire utilisé par les messages de spam sont rassemblées. Le filtre bayésien va utiliser des probabilités bayésiennes pour calculer si un message est un spam ou non. Dans le cas d'un filtrage de groupe, l'apprentissage est en général mené par l'administrateur système.

Basé sur l'algorithme des probabilités bayésiennes, le filtrage bayésien nécessite de nombreux calculs et peut introduire des problèmes d'extensibilité dans un vaste système de lutte contre le spam. Dans un environnement de petites dimensions et très uniforme (par exemple, un réseau d'entreprise ou universitaire), ce type de filtrage peut être acceptable. Mais ce ne sera certainement pas le cas pour un grand fournisseur de services et en particulier un fournisseur public.

Bien que le filtrage bayésien ait été utilisé pour lutter contre le spam, on touche à ses limites lorsque les spammeurs falsifient leurs informations.

7.2.4 Filtrage multimodal

Si un système IGCS doit procéder au filtrage multimodal, les fonctions SGF et RGF mettent en œuvre le filtrage multimodal, respectivement, au moyen de l'entité FE de détection de modalité, de l'entité FE de filtrage et d'autres entités fonctionnelles nécessaires telles que l'entité FE de traitement des messages multimodaux. Afin de prendre en charge l'enregistrement et l'échange des informations, les ensembles de données concernant les informations de lutte contre le spam multimodal doivent être définis. La base de données lscDB va enregistrer les informations de lutte contre le spam multimodal selon des catégories (et des thèmes) de messages multimodaux et des critères de filtrage (qui ont été saisis par les utilisateurs ou opérateurs, ou appris des systèmes IGCS homologues) appropriés.

Si la description des métadonnées multimodales est disponible et que la description des métadonnées est considérée comme fiable, les applications multimodales peuvent filtrer les informations multimodales sur la base de la description des métadonnées du contenu multimodal. Dans le cas contraire, il est préférable que le filtrage prenne en considération les informations multimodales complètes, les entités fonctionnelles suivantes devant accomplir les tâches ci-après:

- Une base de données ou un répertoire comporte les catégories de messages multimodaux et critères de filtrage appropriés. La base de données ou le répertoire peut être hébergé dans les mêmes locaux/le même domaine que l'entité FE d'agent d'interface de DB, l'entité FE de détection de modalité, l'entité FE de traitement multimodal et l'agent utilisateur multimodal. Dans un autre cas, la base de données ou le répertoire peut être hébergé dans d'autres locaux ou domaines que l'entité FE de filtrage.
- Un élément fonctionnel de détection de modalité inspecte un message multimodal envoyé ou reçu pour identifier les modalités qu'il contient.
- Une entité fonctionnelle d'agent d'interface de DB récupère les critères de filtrage de la base de données dans les modalités et catégories de messages données.
- Une entité fonctionnelle de filtrage filtre les messages multimodaux selon les critères de filtrage. L'entité FE de filtrage peut entièrement ou partiellement bloquer les parties multimodales du message multimodal traité.

La Figure 3 décrit l'architecture générale de filtrage des messages multimodaux et les entités fonctionnelles nécessaires. L'architecture de filtrage englobe l'entité FE de détection de modalité, l'entité FE de filtrage, l'entité FE d'agent d'interface de DB et la DB multimodale. La Figure 3 présente toutefois d'autres entités fonctionnelles qui n'accomplissent généralement aucune tâche de filtrage multimodal, comme l'entité FE de traitement des messages multimodaux et l'agent utilisateur multimodal.

L'entité FE de traitement des messages multimodaux traite les messages multimodaux (filtrés), synchronise les messages multimodaux reçus des agents utilisateurs multimodaux et multiplexe ou distribue les messages multimodaux filtrés vers les agents utilisateurs multimodaux. Chacun des divers agents utilisateurs multimodaux gère les modalités spécifiques telles que les entrées et/ou sorties modales (propres à l'équipement).

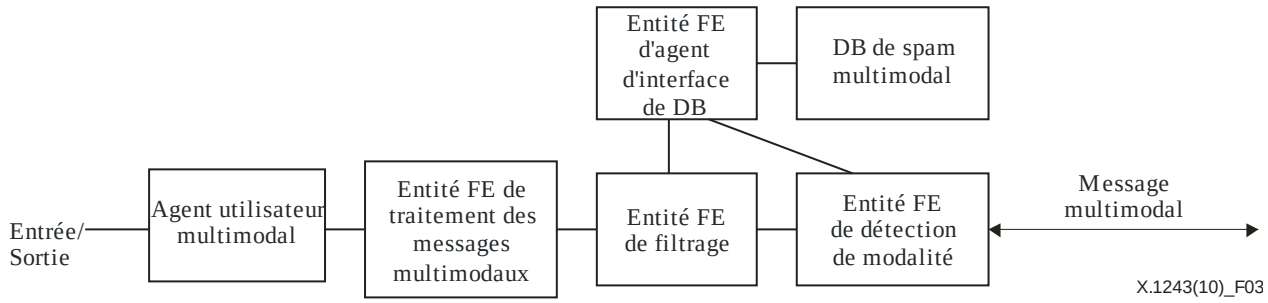


Figure 3 – Architecture de filtrage multimodal

La Figure 4 détaille l'architecture de filtrage multimodal générique en mettant en correspondance les entités fonctionnelles et la fonction de passerelle de réception (RGF). Les étapes suivantes décrivent la procédure suivie lorsque les entités FE reçoivent un message multimodal:

1) La fonction RGF reçoit un message multimodal.

2) L'entité FE de détection de modalité identifie les modalités transportées et le(s) type(s) de message transporté dans le message multimodal reçu.

3) L'entité FE de filtrage peut avoir été configurée de manière statique avec des règles de filtrage pour tous les messages multimodaux potentiels (i.e. indépendamment du message multimodal reçu en particulier) ou peut être configurée de manière dynamique avec une règle dépendant du message et/ou du mode pour chaque message multimodal reçu.

   a) L'entité FE de détection de modalité peut soit soumettre les modalités identifiées et les paramètres types du message à un agent d'interface de DB, soit joindre les paramètres au message multimodal reçu.

   b) L'entité FE de détection de modalité transmet le message multimodal, éventuellement annoté avec les paramètres de modalité et de type de message extraits, à l'entité FE de filtrage.

4) Dans le cas où l'entité FE de filtrage ne serait pas encore configurée avec des règles, elle fait passer les paramètres de modalité et de type de message à l'agent d'interface de DB, à moins que celui-ci n'ait obtenu ces paramètres directement de l'entité FE de détection de modalité.

5) L'entité FE d'agent d'interface de DB demande à la DB multimodale les modalités et critères de messages correspondants. L'entité FE d'agent d'interface de DB compile ces valeurs en règles spécifiques et fournit ces règles à l'entité FE de filtrage.

6) L'entité FE de filtrage applique les règles disponibles et réalise le filtrage selon le message multimodal reçu. En fonction des règles et paramétrages de politique, le message multimodal est autorisé à passer, ou bloqué entièrement ou bloqué partiellement lorsque seules certaines modalités au sein du message multimodal sont bloquées.

7) L'entité FE de filtrage transmet le message multimodal filtré à l'entité FE de traitement des messages multimodaux, éventuellement annoté avec quelques résultats de filtrage (c'est-à-dire informations à journaliser ou alertes de sécurité).

8) L'entité FE de traitement des messages multimodaux traite le message multimodal (filtré) reçu. L'entité FE synchronise la ou les entrées reçues des divers agents utilisateurs multimodaux d'entrée, décompose le message multimodal en ses composantes de modalité et les transmet aux agents utilisateurs multimodaux de sortie.

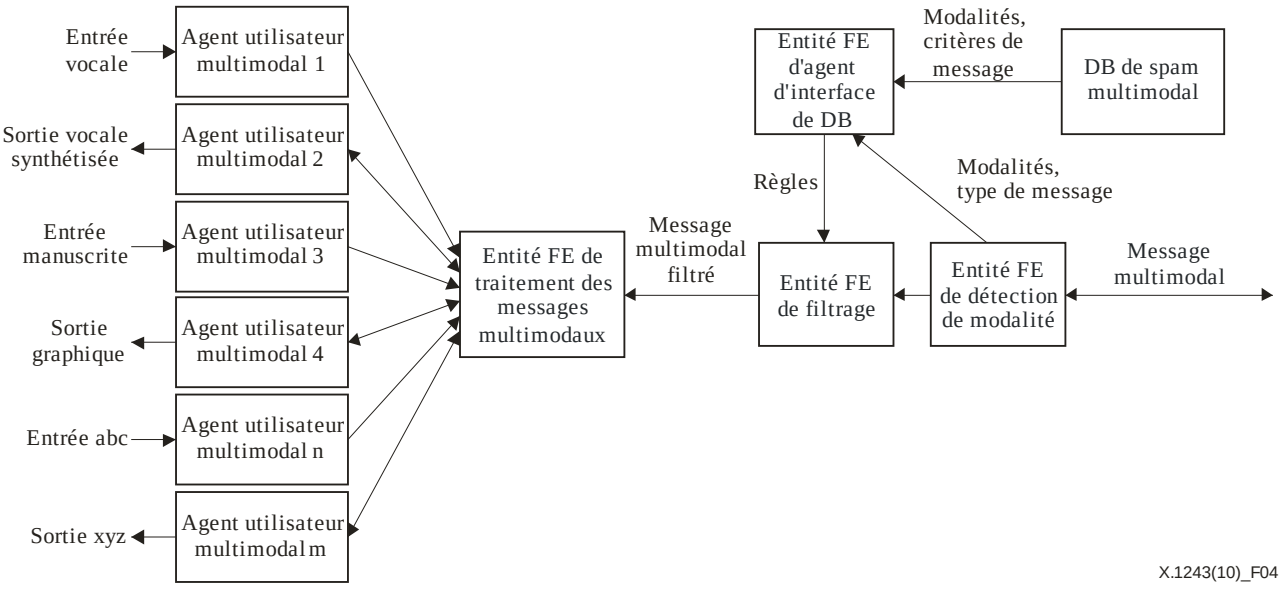


Figure 4 – Filtrage multimodal dans une fonction de passerelle de réception (RGF)

NOTE – La Figure 4 décrit divers agents utilisateurs multimodaux. La fonction RGF peut ne pas exiger que tous les agents utilisateurs multimodaux indiqués soient présents.

7.2.5 Filtre antispam amortisseur

Le filtre antispam amortisseur est utilisé pour contrôler le taux de réception des messages. Un paramètre d'entrée important pour ce filtre est le coefficient d'amortissement des spams. Ce paramètre est une mesure des messages suspects et contrôle le taux de réception des messages. Lorsque des messages hautement suspects sont réceptionnés, le coefficient augmente en conséquence et le filtre antispam amortisseur va réduire le taux de réception des courriels suspects. Ce paramètre est en général généré par des systèmes externes de lutte contre le spam, tel que des bases de données d'expérience ou de réputation. Le filtre antispam amortisseur peut également affecter le délai de réponse, la taille de la fenêtre de transport et la durée du cycle d'amortissement, etc.

7.2.6 Filtre d'en-tête de courriel

Le filtre d'en-tête de courriel (EHF, *email header filter*) surveille la conversation SMTP et vérifie sa conformité avec les protocoles pertinents. Il peut être utilisé pour identifier les incohérences de protocole et les en-têtes de courriel falsifiés. Afin de reconstruire les sessions SMTP et de suivre les états des protocoles, le filtre EHF peut exiger la défragmentation de paquets, l'assemblage de flux TCP, etc. Le filtre EHF se concentre sur l'analyse au niveau protocole et fournit des informations supplémentaires pour améliorer la précision de l'identification des spams en général. Le filtre EHF est communément intégré dans de nombreux systèmes antispam commerciaux, ainsi que dans certains systèmes antispam à code source libre.

7.2.7 Filtre fondé sur des paramètres pondérés (WPF)

Le filtre fondé sur des paramètres pondérés (WPF) est utilisé pour détecter le spam en analysant de multiples paramètres. Les paramètres sont basés sur des informations statistiques, parmi lesquelles le nombre de sessions de courriel, le nombre de serveurs de destination, le nombre d'essais de courriels, la période d'envoi des courriels, la fréquence d'envoi des courriels, le taux de courriers d'essai et de courriers fructueux, et ainsi de suite. Chaque paramètre a un seuil configuré et une valeur de poids configurée. En outre, l'ensemble complet des valeurs pondérées, qui peuvent être justifiées à l'avance par plusieurs expériences, est également nécessaire. Pour chaque courriel, tous les paramètres des règles seront vérifiés. Les seuls paramètres au-dessus du seuil configuré seront

ajoutés de façon pondérée. Si la somme des paramètres franchit le seuil prédéfini, le filtre WPF peut distinguer les spams des courriels normaux.

8 Exécution du protocole d'échange entre homologues de lutte contre le spam

8.1 Découverte d'un homologue

Le processus de découverte d'un homologue établit la relation entre homologues pour deux systèmes IGCS. Ce processus est initialisé lorsqu'un système IGCS essaye de découvrir un système IGCS valide sur le trajet de distribution du message. Lorsqu'une fonction RGF détecte un message suspect de spam, le processus de découverte d'un homologue commence.

Il est recommandé d'inclure les informations suivantes dans le message de découverte d'homologue:

- Liste des adresses des fonctions RGF/SGF du système IGCS de départ: adresse d'origine (par exemple, adresse IP d'origine et paire de ports). Pour qu'il n'y ait pas de points individuels de défaillance, un système IGCS peut intégrer de multiples fonctions RGF et SGF afin de créer des redondances. La liste des adresses peut contenir toutes les adresses des fonctions RGF/SGF du système IGCS de départ.
- Adresse de l'équivalent du système IGCS: IGCS@{adresse du proxy de l'équivalent}.
- Auteur du spam: adresse de l'expéditeur du spam.
- Type de spam suspecté: connu (WELL_KNOWN), signalé par l'utilisateur (USER_REPORTED) ou autre (OTHER).
- Spam suspect joint: le spam suspect est joint.

Lorsqu'un message de découverte d'homologue est envoyé, le système IGCS de départ va mettre en route un temporisateur. Si aucun message de réponse n'est reçu avant l'expiration du délai configuré, le système IGCS de départ n'arrive pas à découvrir un système IGCS homologue. Un message de réponse de découverte d'homologue peut contenir les informations suivantes:

- Liste des adresses des fonctions RGF/SGF du système IGCS qui répond.
- Confirmation du spam suspecté: pour confirmer que le spam suspecté a bien été considéré comme du spam par le système IGCS qui répond.

8.2 Configuration d'un homologue

Avant l'expiration du délai, si le système IGCS de départ reçoit le message de réponse de découverte d'homologue, il peut commencer à établir une relation entre homologues, qui consiste en deux actions principales:

- Le système IGCS met à jour la liste d'homologues: il ajoute la liste d'adresses du système IGCS équivalent dans la liste d'homologues.
- Il nomme la liste du filtre antispam pris en charge: filtres antispam pris en charge dans chaque système IGCS.

8.3 Echange de messages pour lutter contre le spam

Après le processus de configuration des homologues, le système IGCS commence l'échange de messages pour lutter contre le spam. Au cours de ce processus, deux systèmes IGCS homologues échangent des informations concernant les filtres antispam communs pris en charge. Chaque système IGCS met à jour en conséquence sa base de données lscDB compte tenu des messages échangés.

8.4 Libération d'un homologue

Si aucun spam n'a été détecté au cours d'une période de temps donnée, un système IGCS peut mettre fin à la relation entre homologues en envoyant un message de libération d'homologue. Après réception du message de libération d'homologue, le système IGCS va retirer ou réutiliser les informations en relation avec l'homologue, en fonction de la politique.

9 Modèle de mise en œuvre des systèmes de passerelle pour lutter contre le spam

9.1 Modèle intégré

9.1.1 Description du modèle

Dans le modèle intégré, le système IGCS est intégré avec un système de messages qui consiste en un agent RA et un agent SA. Chaque système a une passerelle (une fonction RGF et une fonction SGF) et une base de données lscDB. Dans un système de courriels, par exemple, l'agent RA peut être un serveur POP3 et l'agent SA peut être un serveur SMTP. Les fonctions RGF/SGF peuvent être mises en œuvre sous forme de serveur intégré fournissant les deux services POP3 et SMTP. Une base de données lscDB est également requise pour que le système de courriels puisse fournir des règles de lutte contre le spam. Un modèle intégré est décrit dans la Figure 5.

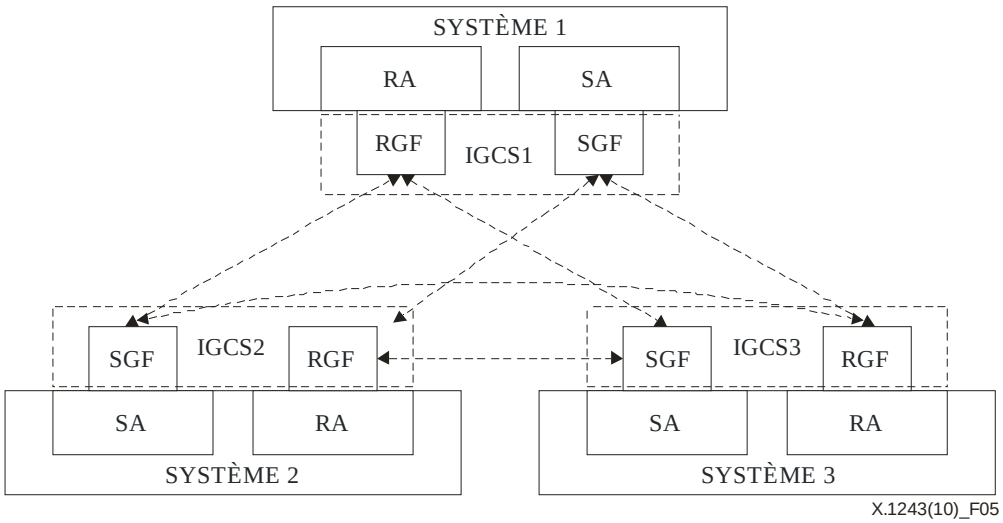


Figure 5 – Modèle intégré de système IGCS

9.1.2 Cas d'utilisation

Un modèle intégré est adapté au modèle client/serveur, dans lequel un serveur est responsable de l'envoi/la réception des nombreux messages des clients. Dans ce cas, le serveur agit comme point de décision et point d'application de la politique pour les activités antispam.

9.2 Modèle basé sur le domaine

9.2.1 Description du modèle

Dans le modèle basé sur le domaine, le système IGCS agit comme un proxy de distribution des messages dans un domaine qui peut avoir de multiples agents SA et RA afin de respecter les prescriptions en matière d'équilibre de la charge. Les fonctions SGF/RGF peuvent avoir plusieurs instances réparties dans un domaine. Chaque instance SGF/RGF est en charge de plusieurs agents SA/RA dans un domaine et est responsable de la lutte à la fois contre les messages de spam dans le domaine local et entre les domaines.

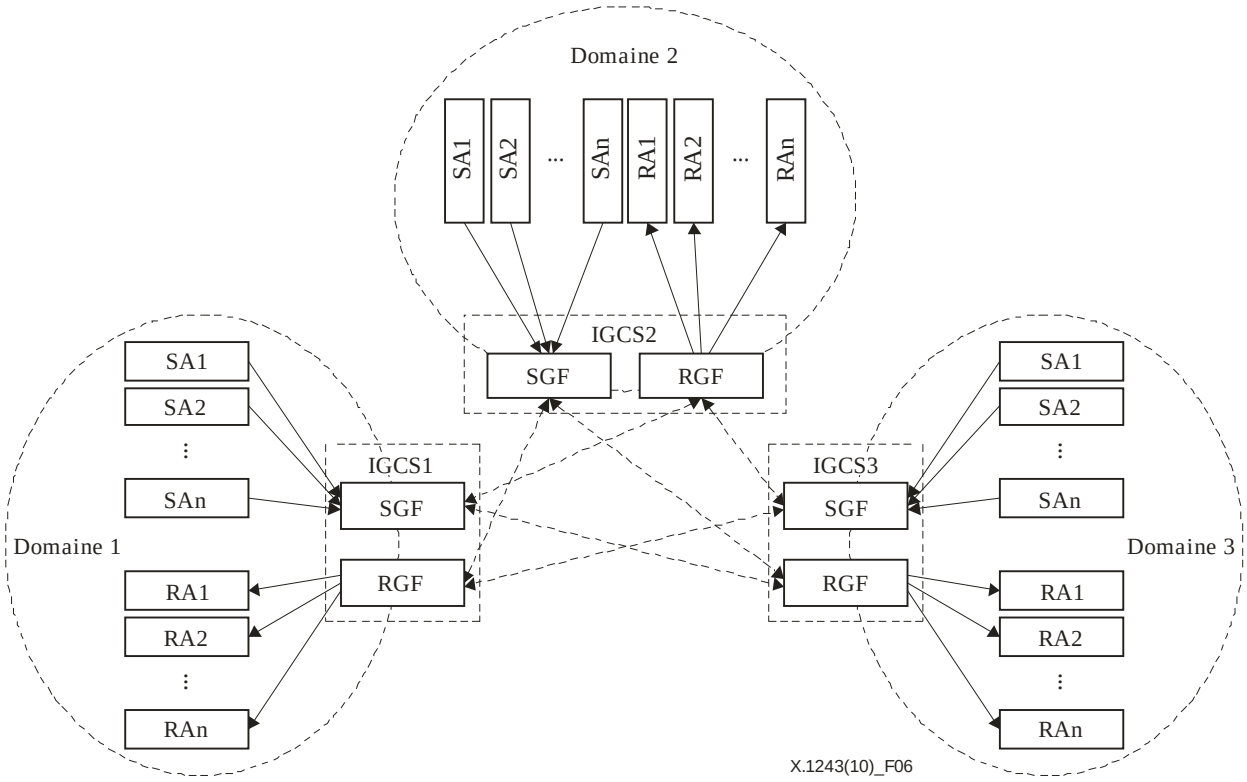


Figure 6 – Modèle basé sur le domaine

9.2.2 Cas d'utilisation

Le modèle basé sur le domaine peut être utilisé à des fins de lutte contre le spam basée sur le domaine. Il convient particulièrement aux systèmes de communication entre homologues, par exemple à de nombreuses applications IM courantes: IRC, etc. Pour un modèle entre homologues, un système du côté utilisateur agit lui-même en même temps comme un agent RA et SA. Il sera très difficile de gérer un grand nombre d'agents RA et SA côté utilisateur avec un modèle IGCS intégré. Toutefois, un modèle basé sur le domaine permet de régler le problème de manière répartie.

9.3 Modèle de déploiement par déviation

9.3.1 Description du modèle

Dans un réseau sans fil, le système IGCS peut également être déployé au niveau d'un point d'accès sans fil. Les points d'accès sans fil dévient tous les messages vers le système IGCS. Le système IGCS juge les messages entrants selon les règles enregistrées dans la base de données lscDB et injecte les messages normaux dans le réseau sans fil.

9.3.2 Cas d'utilisation

Le modèle de déploiement par déviation peut être utilisé dans un réseau sans fil. Le spam peut être filtré avant d'entrer dans le réseau sans fil, afin de réduire le coût inutile de la livraison du trafic de spam aux utilisateurs finaux.

Appendice I

Exemple de définition de message SCPP

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

Ci-dessous se trouve un exemple de messages SCPP définis en langage ASN.1, qui a été vérifié par le compilateur ASN.1:

```
-- SCPP-MESSAGES {itu-t(0) recommendation(0) x(24) igscs(1243)
asn1-module(0) scpp-messages(1)}
DEFINITIONS AUTOMATIC TAGS::=
BEGIN

-- SCPP Message body definition
SCPP-PDU ::= SEQUENCE {
     sourceAddress        IGCS-Address,
     destAddress          IGCS-Address,
     igcs-message-body    CHOICE {
               peerDiscovery   PeerDiscoveryDEF,
               peerSetup       PeerSetupDEF,
               dataExchange    DataExchangeDEF,
               peerKeepAlive   PeerKeepAliveDEF,
               peerRelease     PeerReleaseDEF},
     nonStandardData      OCTET STRING OPTIONAL,
     ...
}

-- PeerDiscovery Message definition
PeerDiscoveryDEF::=SEQUENCE {
     setupRequest    BOOLEAN,
     igcsSignature   IGCS-Signature
}

-- PeerSetup Message definition
PeerSetupDEF::=SEQUENCE {
     setupResponse        BOOLEAN,
     sgfList              SEQUENCE OF IGCS-Address,
     rgfList              SEQUENCE OF IGCS-Address,
     supportedFilters     SupportedSpamFilters,
     igcsSignature        IGCS-Signature
}

-- Countering Spam Data Exchange Message definition
DataExchangeDEF::=SEQUENCE {
     csData               SET OF SpamFilterData,
     ...
}

-- Peer Keep Alive Message definition
PeerKeepAliveDEF::=SEQUENCE {
     sgfUpdates      GF-Updates,
     rgfUpdates      GF-Updates,
     filtersUpdates  SupportedSpamFilters
}
-- Peer Release Message definition
PeerReleaseDEF::=SEQUENCE {
     peerRelease     ENUMERATED{request(0), confirm(1)},
     nonStandardData OCTET STRING OPTIONAL,
     ...
}
```

```
-- IGCS supported addresses, include IGCS,SGF,RGF address definition
-- Support IP address, Email ID and other types of address
IGCS-Address::=CHOICE{
     ipAddress
     SEQUENCE { ip OCTET STRING(SIZE(4)),
                port INTEGER(0..65535) },
                ip6Address
                SEQUENCE { ip OCTET STRING(SIZE(16)),
                                        port INTEGER(0..65535) },

     emailAddress              IA5String(SIZE(1..512)),
     nonStandardAddress   OCTET STRING,
     ...
}

-- Signature data for authentication
IGCS-Signature::=SEQUENCE {
     igcsID                    INTEGER(0..65535),
     signatureData        OCTET STRING,
     ...
}

-- RGF/SGF status update information
GF-Updates::=SEQUENCE {
     gateType             ENUMERATED {sgf(0),rgf(1)},
     gateAdd              IGCS-Address,
     gateRemove      IGCS-Address
}

-- IGCS Supported Spam filters and related data

SupportedSpamFilters::= SEQUENCE {
     supportedFilter SEQUENCE OF SpamFilters

}

SpamFilters::=SEQUENCE{
     filterID             INTEGER(0..128),
     filterName      IA5String(SIZE(1..512))
}

SpamFilterData::=SEQUENCE {
     filterID             INTEGER(0..128),
     filterData      OCTET STRING,
     ...
}

END
```

Bibliographie

[b-UIT-T X.680] Recommandation UIT-T X.680 (2008) | ISO/CEI 88242-1:2008, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification de la notation de base*.

[b-UIT-T X.681] Recommandation UIT-T X.681 (2008) | ISO/CEI 8824-2:2008, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des objets informationnels*.

[b-UIT-T X.682] Recommandation UIT-T X.682 (2008) | ISO/CEI 8824-3:2008 *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des contraintes*.

[b-UIT-T X.683] Recommandation UIT-T X.683 (2008) | ISO/CEI 8824-4:2008, *Technologies de l'information – Notation de syntaxe abstraite numéro un: paramétrage des spécifications de la notation de syntaxe abstraite numéro un*.

[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.1241] Recommandation UIT-T X.1241(2008), *Cadre technique pour lutter contre les spams par courrier électronique*.

[b-IETF RFC 1869] IETF RFC 1869 (1995), *SMTP Service Extensions*.

[b-IETF RFC 1939] IETF RFC 1939(1996), *Post Office Protocol – Version 3*.

[b-IETF RFC 2060] IETF RFC 2060(1996), *Internet Message Access Protocol -Version 4rev1*.

[b-IETF RFC 2505] IETF RFC 2505(1999), *Anti-Spam Recommendations for SMTP MTAs*.

[b-IETF RFC 2635] IETF RFC 2635 (1999), *ON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*)*.

[b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol*.

[b-IETF RFC 2822] IETF RFC 2822 (2001), *Internet Message Format*.

[b-IETF RFC 3685] IETF RFC 3685 (2004), *SIEVE Email Filtering: Spamtest and VirusTest Extensions*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	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	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2011