OPÉRER UN SERVICE DE LISTES DE DIFFUSION

Best Practice Document

Document rédigé par le groupe de travail «listes de diffusion»
animé par le GIP RENATER
(BPD R7.1)

Auteurs:

Odile GERMES – odile.germes@univ-rennes1.fr – Université Rennes 1/GIP RENATER
Dominique LALOT – dominique.lalot@univ-amu.fr – Aix Marseille Université/GIP RENATER
José-Marcio MARTINS DA CRUZ- jose-marcio.martins@mines-paristech.fr – Institut Mines Télécom/GIP RENATER
Laurence MOINDROT – moindrot@unistra.fr – Université de Strasbourg/GIP RENATER
Luc VEILLON – luc.veillon@ac-orleans-tours.fr – Académie d'Orléans/GIP RENATER
David VERDIN – david.verdin@renater.fr - GIP RENATER

V1 - 27/11/14

Document No: GN3plus-NA3-T2-R7.1
Version / date: V1 – 27/11/14
Original language : French
Original title: “Opérer un service de listes de diffusion”
Original version / date: V1 - 27/11/14
Contact: cbp@listes.renater.fr

RENATER bears responsibility for the content of this document. The work has been carried out by a RENATER led working group on metropolitan network as part of a joint-venture project within the HE sector in France.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 605243, relating to the project 'Multi-Gigabit European Research and Education Network and Associated Services (GN3plus)'.

Table des matières

Introduction

Dès qu'une organisation grossit, il devient nécessaire de disposer d'un système pour pousser des informations vers ses membres. C'est la raison pour laquelle les services de listes de diffusion sont omniprésents dans les établissements d'enseignement et de recherche.

Un système de listes de diffusion présente plusieurs caractéristiques notables:

- **la masse importante d'informations qui y transitent** ; il n'est pas rare que certains systèmes de listes diffusent plusieurs millions de messages par jours,
- **la criticité des informations contenues** ; adresses électroniques et contenus des messages sont des informations critiques qui doivent être protégées,
- **la proximité avec le système d'informations** ; nécessaire afin d'assurer que les listes de diffusion reflètent de manière cohérente l'organisation réelle de l'établissement,
- **l'ouverture nécessaire du système hors de l'établissement** ; un service de listes étant lié à la communication d'une organisation, il doit nécessairement offrir un degré d'ouverture vers les partenaires extérieurs.

L'ensemble de ces caractéristiques font qu'on ne peut déployer un service de listes qu'en respectant un certain nombre de bonnes pratiques présentées dans ce document.

Note: Bien qu'il existe de nombreux logiciels de listes de diffusion, l'ensemble des exemples et illustrations du présent document s'appuient sur le logiciel Sympa, particulièrement bien adapté aux établissements d'enseignement et de recherche.

1 Messagerie

Un serveur de listes peut être vu comme un amplificateur : à chaque message en entrée peut correspondre un nombre très important de messages en sortie. Du point de vue « serveur de messagerie », on peut identifier trois composantes :

- un serveur MTA, en entrée, pour la soumission de messages ;
- un logiciel de gestion de listes de diffusion, avec toutes ses composantes ;
- un serveur MTA en sortie, pour la diffusion des messages.

1.1 Filtrage Antispam

Du spam peut être inséré dans le flot de messages soit par le MTA en entrée, soit par l'interface de composition Web (si le serveur en possède).

Le problème d'insertion de spams par l'interface Web résulte, généralement, soit de la compromission de l'identifiant d'un utilisateur, soit d'un acte intentionnel d'un abonné indélicat. Les mesures techniques doivent être complétées par une surveillance par les modérateurs et/ou le gestionnaire du serveur.

1.1.1 Filtrage en entrée

L'effort de filtrage doit être effectué en priorité sur le trafic entrant, d'une part, parce que ce trafic est bien plus faible qu'en sortie et, d'autre part, pour ne pas insérer des données indésirables dans les différents sous-systèmes du gestionnaire de listes.

Les filtres antispam classent, généralement, les messages en trois catégories, selon un score : des « hams », des « spams » et des « unsure ». Une bonne stratégie de traitement par le serveur de listes peut ressembler à ceci :

- les “hams” sont traités normalement ;
- les “unsure” sont soumis à modération;
- les “spams” sont détruits.

Les messages détruits ne doivent pas générer des notifications à l'expéditeur supposé (pour ne pas générer du rétro-spam) mais doivent être journalisés de façon à assurer leur traçabilité.

1.1.2 Traitement du spam en sortie

En sortie, il ne s'agit pas à proprement parler de filtrage de spam mais des mesures visant à éviter que le serveur de listes soit vu comme étant un spammeur. En effet, tout serveur inconnu délivrant un nombre important de messages à un nombre important de destinataires peut être vu, à priori, comme étant un spammeur. Quelques mesures, non exhaustives, sont :

- Ne pas s'acharner lorsqu'un serveur distant rejette temporairement un message (greylisting, ...). Il est possible éventuellement de faire une deuxième tentative au bout d'une dizaine de minutes mais par la suite l'intervalle entre deux tentatives ne doit pas être inférieur à 30 minutes [Klensin 2008]
- Limiter le nombre de destinataires de même domaine pour chaque message dans une même transaction (une vingtaine est un nombre raisonnable);
- Limiter le nombre de transactions (messages) dans la même connexion SMTP avec un serveur distant ;
- Lorsque cela est possible techniquement, ralentir la cadence d'émission si le serveur destinataire commence à refuser tous les messages avec des rejets temporaires;
- Gérer les erreurs et supprimer les utilisateurs inconnus ou ayant déménagé sans avoir changé l'adresse d'abonnement.

En effet, nombreux sont les domaines où le MTA en entrée impose des limitations dans les différentes cadences. Lorsqu'on les dépasse, on se trouve bloqué jusqu'à ce que la cadence en question descende à un niveau normal. Ce genre de blocage est catastrophique pour un serveur de listes de diffusion dont le niveau de trafic est important. D'autant plus que des blocages répétés peuvent se transformer en blocage définitif.

1.2 Authentification du domaine émetteur (DKIM, SPF, DMARC)

DKIM [Allman et al. 2007], SPF [Wong & Schlitt 2006] et DMARC [DMARC 2014-2] sont des méthodes d'authentification du domaine émetteur d'un message, permettant de vérifier qu'un message supposé avoir été envoyé par un certain domaine, l'a effectivement été.

L'intérêt de l'utilisation de ces mécanismes est de permettre les domaines destinataires (que ce soient des domaines amis ou, sans les citer, les fournisseurs importants de services de messagerie) de mettre en place des règles de filtrage allégées ou alors d'être plus condescendants vis à vis des messages envoyés par le serveur de listes.

La protection DMARC peut être extrêmement préjudiciable aux services de listes de diffusion si elle est appliquée de manière drastique. [Levine 2014] Les conséquences peuvent être dramatiques si un grand nombre d'adresses du serveur de listes sont dans un domaine ayant une politique DMARC définissant la valeur « p=reject ». Dans ce cas, les messages émis depuis ces adresses provoqueront des erreurs de type « Rejected for policy reasons ». En effet, un message issu d'un serveur de listes ne respectera jamais ou presque, par construction, les enregistrements DMARC, DKIM ou SPF du domaine de l'émetteur du message. Ceci est dû au fait que, du point de vue du destinataire du message, le serveur ayant émis le message est le MTA du serveur de listes, et non celui du domaine émetteur.

La seule parade connue à ce problème est le remplacement du champ « From : » d'un message issu d'un domaine avec une politique DMARC agressive par une adresse email du domaine de listes.[DMARC 2014]

Ceci présente l'inconvénient de casser une éventuelle signature S/MIME. Cela reste un inconvénient très relatif, car les seuls domaines utilisant « p=reject » sont des domaines de service de messagerie privés qui ne permettent pas l'utilisation de S/MIME.

Dans le logiciel Sympa, la protection contre DMARC est activée simplement en ajoutant la directive suivante dans le fichier de configuration principal, sympa.conf, et redémarrer le service :

```
dmarc_protection_mode dmarc_reject
```

1.3 Infrastructure

Pour les serveurs de listes de diffusion assurant un niveau de trafic important, il est préférable d'avoir des instances différentes pour les MTAs entrant et sortant. Le MTA sortant est beaucoup plus sollicité, l'utilisation d'une instance unique peut perturber la réception de messages lorsqu'il y en a beaucoup d'autres en cours de distribution.

1.4 Placement en DMZ ou en intranet

La décision de placer un serveur de listes dans la DMZ ou dans l'intranet dépend du contenu du serveur et de la diversité des abonnés, mais en général, il s'agit d'un service dont le placement est typiquement en DMZ.

Le serveur de listes doit être placé dans la zone Intranet, avec un éventuel accès extérieur par VPN ou similaire, si :

- il s'agit d'un service purement interne à l'organisme ;
- le serveur abrite des données confidentielles, dans les archives ou dans des zones de partage de documents.

Le placement en DMZ est nécessaire lorsque :

- le serveur héberge des listes de diffusion ouvertes ;
- le serveur contient des abonnés externes sans lien particulier avec l'organisme.

Dans le cas de contraintes contradictoires, et selon le niveau d'étanchéité exigé, l'utilisation de serveurs virtuels peut ne pas suffire.Il faut privilégier la mise en place d'instances séparées de serveurs de listes : un en intranet et l'autre en DMZ.

1.5 Chiffrement et Signature

S/MIME permet de chiffrer et signer des courriels. La signature permet de vérifier l'intégrité du courriel à son arrivée. Le chiffrement empêche que le contenu du courriel soit lu s'il est intercepté.[Ramsdell & Turner 2010] [Ramsdell & Turner 2010-2]

Pour que la signature S/MIME soit respectée, le serveur de listes doit pouvoir ne pas modifier le corps du courriel lors du traitement d'un message signé.

Lors de l'envoi d'un courriel chiffré à une liste, on se heurte à la difficulté suivante : un courriel est chiffré avec la clé publique du destinataire. Or, dans le cas d'une liste, le destinataire initial est la liste, et les destinataires finaux du message sont multiples. Il est donc nécessaire que le courriel soit traité de la manière suivante [Aumont & Salaün 2000] :

1. chiffrement du courriel avec la clé publique de l'adresse de la liste de diffusion
2. déchiffrement par le moteur de listes à l'aide de la clé privée de la liste
3. pour chaque abonné, chiffrement du courriel à l'aide de la clé publique de l'abonné.

La faille de ce système est que le serveur de listes, au contraire d'un simple MTA, dispose des moyens de déchiffrer tous les courriels chiffrés qui lui sont adressés. En cas de compromission du serveur de listes la confidentialité des messages chiffrés qui y transitent est elle aussi compromise.

1.6 Conformité aux normes (RFCs et autres normes techniques)

Pour éviter tout dysfonctionnement dans la distribution des messages (par exemple, les rejets d'un filtre antispam trop « sensible »), il est important que le serveur de listes respecte scrupuleusement les normes techniques.

Les deux normes principales sont la RFC 5321 [Klensin 2008], qui traite du protocole SMTP et qui concerne surtout le MTA sortant du serveur de listes, et la RFC 5322 [Resnik 2008] qui traite de la mise en forme des messages et de ses entêtes et qui concerne surtout le moteur du serveur de listes.

A ces deux normes s'ajoutent un nombre assez important d'autres normes permettant de spécifier des extensions, soit applicables à tout serveur de messagerie, soit spécifiques aux moteurs de listes de diffusion. Des exemples de telles extensions sont la RFC 6531 sur l'internationalisation des adresses électroniques, ou la RFC 6729 sur la traçabilité des périodes de rétention des messages.

Les différents logiciels du serveur de listes sont développés dans le respect des normes, mais malgré cela, des réglages particuliers, bénins en apparence, peuvent rendre le serveur de listes non conforme.

2 Intégration dans le système d'information (SI)

Les différents services de listes de diffusion proposés sur le marché aujourd'hui sont beaucoup plus que de simples serveurs de publipostage à un ensemble d'utilisateurs. En effet, de nombreux systèmes hébergeurs de listes permettent de répondre aux usages avancés des outils collaboratifs. Ils doivent ainsi s'intégrer au mieux dans les systèmes d'information et répondre aux politiques des établissements.

Les principales briques du SI qui seront discutées dans ce document sont les portails d'accès numériques, les services d'authentification, les sources de données d'approvisionnement des listes (bases de données, annuaires d'entreprise), et les web-services d'échanges de données. Nous verrons les bonnes pratiques d'intégration et d'échanges de données, ainsi que quelques possibilités d'utilisation des listes créées pour alimenter le SI.

2.1 Principes de base

Dans un premier temps, l'intégration du service de listes de diffusion dans le système d'information doit respecter les principes de sécurité en termes de confidentialité et de restriction d'accès aux données. Ensuite il est recommandé de choisir un service de listes ouvert respectant les normes et les standards pour permettre une meilleure compatibilité et interopérabilité à long terme.

2.2 Portail d'accès

Le portail d'accès (encore appelé environnement numérique de travail) est devenu dans nos établissements un outil indispensable qui permet aux différents utilisateurs, en fonction de leur profil (étudiant, chercheur, enseignant, administratif, etc.), de disposer d'un environnement de travail spécifique lui donnant facilement accès aux outils de travail collaboratifs, de communication, aux données le concernant, etc.

Il est essentiel que le service de listes de diffusion puisse facilement s'intégrer dans le portail d'accès offert aux utilisateurs. Le service de listes de diffusion doit ainsi supporter les fonctionnalités de :

- SSO Web CAS ou Shibboleth, pour permettre un accès direct via le portail
- Web-services, pour permettre un affichage et une configuration des listes d'un utilisateur via le portail.

Note : l'interface du moteur doit rester accessible à l'ensemble des acteurs d'une liste (abonné, modérateur ou propriétaire). On doit prévoir deux accès supplémentaires :

- un accès par fédération d'identité (le protocole SAMLv2 est préconisé)
- un accès direct, pour les abonnés qui restent en dehors de l'établissement et de la fédération.

2.3 Sources de données

Dans la majorité des services de listes de diffusion, la gestion (création, alimentation, mise à jour, suppression) peut se faire manuellement, mais également automatiquement à partir de différentes sources de données. Dans le contexte des établissements de l'enseignement supérieur et du secondaire, nous recommandons un système capable de s'interconnecter avec un maximum de sources différentes et notamment les sources de données métier comme les bases des ressources humaines, les bases des étudiants ou encore l' annuaire d'établissement [Aumont & Salaün 2001] :

- fichier à plat local ;
- fichier à plat distant via HTTP(S) ;
- autre liste de diffusion ;
- requêtes SQL sur différents systèmes de gestion de bases de données ;
- requêtes LDAP.

2.3.1 Avantages

Les avantages à utiliser les sources de données métier sont nombreux. On peut noter la mise à jour automatique des listes lors de l'arrivée ou du départ d'une personne. Ceci améliore la qualité des données des listes et diminue les coûts d'exploitation.

2.3.2 Inconvénients

L'un des inconvénients est la répercussion des erreurs de votre système d'information dans les listes de diffusion.

2.3.3 Exemples d'utilisation

Automatisation de la création et de la suppression de listes

L'automatisation de la création, de la suppression et du paramétrage de certaines listes de diffusion est utile lorsqu'il faut créer un très grand nombre de listes avec un paramétrage semblable. Exemple : constitution des listes des étudiants en début d'année universitaire. Ces listes sont constituées à partir des bases de données des formations proposées dans les établissements (listes par niveau ou type de formation, par promotion, par UFR, par code étape, etc.)

Automatisation de l'abonnement et du désabonnement des utilisateurs

L'automatisation de l'abonnement et du désabonnement est également très utile. Cela se fait à partir des bases de données ou des annuaires d'établissements dans lesquels sont référencés les utilisateurs. Exemple : abonnement automatique d'un étudiant lors de son inscription aux listes des différentes filières ou options qu'il a choisies ; abonnement / désabonnement d'un personnel aux canaux de communication de son établissement (listes syndicales, lettre d'information générale, listes de discussion) lors de son arrivée ou de son départ.

En pratique

Dans la pratique ces créations automatiques de listes peuvent se faire via les outils fournis par le système de gestion de liste qui est utilisé. Pour l'outil SYMPA il est possible de le faire au travers de l'utilisation des familles de liste. En ce qui concerne l'abonnement et le désabonnement à ces listes, SYMPA offre deux modes d'utilisation :

- Adossement de la liste à une source de données externe (ldap ; sql, fichier à plat déposé par un processus métier, liste incluse, web service métier)
- Pilotage par activation du webservice SOAP de SYMPA (qui permet d'abonner ou désabonner une personne), depuis une API métier.

2.4 Authentification

Afin de répondre aux nouvelles méthodes d'authentification utilisées aujourd'hui, il est recommandé que le système de listes de diffusion puisse supporter les systèmes d'authentification suivants :

- Authentification simple sur une base de données locale
- Authentification simple LDAP
- Authentification unique via SSO Web CAS
- Authentification déléguée via une fédération d'identités respectant le format SAMLv2 (Shibboleth, RSA FIM, SimpleSAMLphp etc.)

Comme on l'a vu précédemment, on devra combiner plusieurs méthodes d'authentification pour les populations différentes d'utilisateurs [Aumont & Salaün 2003].

2.4.1 Authentification simple sur une base de données locale

Cette méthode d'authentification est la plus simple à mettre en œuvre. Son inconvénient majeur est la gestion d'une base d'identifiants (login/mot de passe) non intégrée dans le système d'information. Elle est donc à proscrire pour vos utilisateurs locaux. Par contre elle doit être activée si l'on souhaite ouvrir le système de gestion de listes de diffusion à certains utilisateurs qui ne seraient par référencés dans votre système d'information, ou dans une fédération d'identités. Lors de l'authentification d'un utilisateur sur le système de listes, ce système d'authentification sera consulté en dernier.

Note : il faudra s'assurer que la base de données est bien sécurisée si on a fait le choix (le plus souvent inévitable) d'y héberger les comptes et leur mot de passe (cf § sécurité).

2.4.2 Authentification simple LDAP

Cette méthode d'authentification est la plus simple à mettre en œuvre pour connecter un système de listes de diffusion à votre système d'information. Elle permet l'accès à tous les utilisateurs référencés dans votre SI. L'identification peut être réalisée sur un panel d'attributs (uid, mail, mailalternateaddress), la seule condition étant que chaque valeur d'attribut ne puisse faire référence qu'à un seul mot de passe (donc une seule fiche LDAP).

2.4.3 Authentification unique via SSO Web CAS

Cette méthode d'authentification est dite unique (ou Single Sign On en anglais). Elle peut facilement se connecter à l'annuaire LDAP de votre système d'information et a comme avantage par rapport à la solution précédente de permettre à un utilisateur de ne procéder qu'à une seule identification pour l'accès aux divers outils proposés par son établissement. Cette méthode sera utilisée pour l'accès au service via le portail d'accès de votre établissement.

2.4.4 Authentification déléguée via une fédération d'identités respectant le format SAMLv2

Cette méthode d'authentification est la plus avancée. Nous la recommandons dans le contexte de nos établissements quand les abonnés aux listes que nous hébergeons appartiennent à divers établissements. Elle permet de déléguer l'authentification à un ou plusieurs établissements et ainsi ouvrir l'accès au service à l'ensemble de notre communauté.

2.5 Les différentes interfaces d'accès aux services de listes

Afin de s'intégrer au mieux dans le système d'information, le service de listes de diffusion mis en place dans nos établissements doit avoir différentes interfaces de connexion et d'administration pour permettre une interopérabilité maximale avec le système et ses applications.

2.5.1 Ligne de commande

Une interface de gestion en ligne de commande pour « scripter » les fonctions d'exploitation est indispensable. On peut ainsi créer ou supprimer en masse des listes, via par exemple l'instanciation de familles de listes dans un outil comme SYMPA.

2.5.2 Messagerie électronique

Avant l'arrivée du Web, les abonnements/désabonnements ainsi que la gestion des listes de diffusion se faisaient par l'envoi de courriels au service de listes. Moins utilisée aujourd'hui, cette interface reste un standard indépendant du logiciel qui gère les listes.

2.5.3 Web

L'interface web est souvent la plus utilisée. Elle doit, selon le profil des utilisateurs, donner accès à différentes fonctionnalités. Les outils de listes de diffusion étant de plus en plus complets, elle peut facilement devenir complexe et doit être personnalisable (cf notion de domaine virtuel, §exploitation).

2.5.4 Web-services

Pour finir, le service de listes de diffusion doit pouvoir facilement s'intégrer dans un portail d'accès Web offert aux utilisateurs. Le service de listes de diffusion doit ainsi supporter des standards comme SOAP ou REST et permettre l'interopérabilité entre applications. Cette fonctionnalité, orientée métier, est de plus en plus utilisée dans nos établissements.

2.6 Les serveurs de listes comme fournisseurs de service

Les listes de diffusion créées peuvent facilement devenir des groupes réutilisables dans vos différentes applications ou dans vos référentiels. Il faut cependant faire attention à la qualité des données, certaines listes manuelles n'étant pas mises à jour, et garder en mémoire que les données des serveurs de listes sont des données applicatives, elles permettent d'alimenter et enrichir un référentiel, mais ne sont pas le référentiel. Voici quelques exemples d'utilisation des listes de diffusion dans les applications de nos établissements.

2.6.1 Carnet d'adresses

Il est recommandé d'ajouter les adresses de listes de diffusion au carnet d'adresses général de l'établissement, pour que les utilisateurs en aient connaissance et les utilisent. Cependant, toutes les adresses ne doivent pas être ajoutées. Il faut réfléchir aux listes qui peuvent être visible ou non, par exemple en utilisant les attributs de visibilité de la liste.

Note : si on fait à cette occasion le choix d'insérer les adresses des listes dans le même domaine de messagerie que celui des utilisateurs, il faut veiller à ce que le moteur de listes contrôle aussi dans le référentiel des utilisateurs que l'adresse n'a pas déjà été attribuée avant d'autoriser la création d'une nouvelle liste.

2.6.2 Agenda partagé et dossiers partagés

Les listes de diffusion peuvent également être utilisées par le gestionnaire de groupe de vos outils de travail collaboratif comme par exemple l'agenda partagé. Cela peut être utilisé pour le partage de calendrier ou l'invitation aux événements d'un groupe défini. Des règles de synchronisation entre les différentes applications doivent être mises en place pour garantir la cohérence entre la confidentialité des listes configurées dans l'outil de gestion de listes et celles de votre outil de gestion d'agenda. Nous conseillons de ne synchroniser que les petites listes, inférieures à quelques centaines d'abonnés, et dont la liste des membres est publique ou accessible aux possesseurs d'une adresse de votre établissement.

3 Usages

Un moteur de listes a pour objectif de faciliter la diffusion de messages électroniques à un grand nombre de destinataires. Lorsque l'usage de la messagerie s'est développé, en particulier dans le milieu professionnel, les utilisateurs ont été confrontés à plusieurs difficultés :

- La fiabilité de leur carnet d'adresses (validité des adresses électroniques, oubli d'une adresse, diffusion à une adresse non concernée).
- Le partage des échanges (pour les nouveaux arrivants dans la discussion).
- La capacité des destinataires à se « faire oublier ».

Le moteur de listes propose des solutions techniques à ces besoins. Pour cela, il s'appuie sur un référentiel d'utilisateurs et sur un référentiel de listes. Une liste est une adresse de messagerie appartenant au périmètre du moteur de listes, qui extrait de son référentiel d'utilisateurs ceux qui sont rattachés à cette liste.

En termes d'usage, on va donc distinguer :

- L'abonné : il reçoit les courriels envoyés aux listes auxquelles il s'est (ou a été) abonné.
- Le propriétaire : il décide qui doit recevoir les courriels, et gère son référentiel d'abonnés (ajout, suppression, modification d'identification ou des caractéristiques de réception).
- Le modérateur : il décide quel courriel peut être envoyé à la liste qu'il modère.
- Le listmaster : il contrôle la configuration technique du moteur de listes, il met en place les paramétrages par défaut, et les différents scénarii applicables.

3.1 Contrôle de l'information et scénarii

L'échange de l'information peut être libre (chacun participe aux échanges, sans modération) ou restreint (l'information doit être validée avant publication, ou ne peut être émie que par une source autorisée). La liste peut être ouverte (tout le monde peut s'y abonner), restreinte ou fermée. Les abonnés peuvent être visibles ou pas. Pour répondre à ces différents usages, le moteur de listes dispose de « scenarii » qui couvrent tous ces champs. [Aumont & Salaün 1999]

3.1.1 Envoi des messages

Les scenarii de type « send. » décident qui peut ou ne peut pas envoyer des messages à la liste.

Sur SYMPA, une liste totalement ouverte s'appuie sur le scénario send.public dont le cœur de définition est :

```
true()        smtp,dkim,md5,smime     -> do_it
```

A contrario, une liste très restrictive bloquera les messages s'ils ne sont pas envoyés par un des modérateurs. Exemple du scenario send.editorkeyonlyauth :

```
is_editor([listname],[sender])    md5,smime              -> do_it

is_editor([listname],[sender])    smtp,dkim              -> request_auth

true()                            smtp,dkim,smime,md5    -> editorkey
```

Dans cet exemple, les courriels envoyés à la liste sont renvoyés aux modérateurs (editorkey), les courriels des modérateurs leur sont renvoyés pour confirmation (request_auth) à moins qu'ils ne soient signés S/MIME et seules les confirmations envoyées par les modérateurs (de type MD5 ou SMIME), lancent la diffusion effective (do_it).

Les bonnes pratiques déconseillent l'ouverture totale : la prise en compte des stratégies de lutte contre le spamming exige de recourir au minimum à une authentification du diffuseur :

```
true() smtp -> request_auth
true() dkim,md5,smime -> do_it
```

On peut ensuite combiner différentes commandes pour répondre à des besoins très précis comme :

- Autoriser l'envoi aux abonnés, à son domaine de messagerie ou aux membres d'une liste particulière

  ```
  (resp.      is_subscriber([listname],[sender]) ;      match([sender],/[conf->host]$/) ; is_subscriber(liste.autorisee,[sender]) )
  ```

- Bloquer l'envoi lorsqu'une liste devient inactive mais doit rester visible (pour accéder à ses archives)

  ```
  true()     smtp,dkim,smime,md5    -> reject(reason='send_closed')
  ```

- Traiter différemment les courriels selon leur contenu. Exemple : renvoi des courriels multipart chez le modérateur :

  ```
  match([header->Content-Type],/multipart/) smtp,dkim,smime,md5 -> editorkey
  ```

3.1.2 Contrôle des abonnés

Les adresses électroniques représentent un capital qui attire les convoitises et peut contribuer à détourner les scénarii d'envoi. Le listmaster devra mettre en place des stratégies de protection qui répondent aux exigences des utilisateurs. C'est le rôle des scénarii définis dans la famille « review » et pour une moindre mesure « subscribe » et « add ».

Il est possible de déterminer des droits distincts pour le listmaster, les propriétaires, les modérateurs, les abonnés et toute autre personne. Dans ce dernier cas, on peut appliquer des tests pour appliquer des droits différents selon le domaine de messagerie, l'adresse IP… Ex. :

```
is_subscriber([listname],[sender]) smtp,dkim,md5,smime -> do_it
is_listmaster([sender])            smtp,dkim,md5,smime -> do_it
is_owner([listname],[sender])      smtp,dkim,md5,smime -> do_it
is_editor([listname],[sender])     smtp,dkim,md5,smime -> do_it
verify_netmask('1.12.123.0/24')    smtp,dkim,md5,smime -> do_it
match([sender],/[conf->host]$/)    smtp,dkim,md5,smime -> do_it
```

```
true()    smtp,dkim,md5,smime → reject(reason='review_local_user_sub')
```

Dans certains cas, il n'est pas souhaitable que l'identité des abonnés soit connue, y compris du listmaster, des propriétaires et des modérateurs (listes syndicales, listes de patients atteints de maladies particulières, listes de victimes etc.). On appliquera alors des règles de rejet très restrictives, y compris au listmaster :

```
is_listmaster([sender])    -> reject(reason='review_closed')
```

Si la visualisation des abonnés est interdite aux propriétaires et aux listmaster, il faut veiller à ne pas positionner un scénario d'abonnement se faisant l'écho de chaque adhésion ! Ce scénario d'abonnement libre avec notification (subscribe.open_notify) est contre-indiqué :

```
true()      smtp,dkim,smime,md5 -> do_it,notify
```

De même, on doit s'interroger sur la pertinence de laisser au propriétaire la possibilité de lancer un rappel d'abonnement (à l'issue de ce rappel, le propriétaire recevrait une notification de tous les répondeurs activés).

3.1.3 Accès des non abonnés

Lorsqu'un moteur de listes héberge des listes en abonnement libre hors de tout périmètre imposé[1], il est nécessaire d'ouvrir l'accès de l'interface web au grand public. De ce fait, les listes hébergées sont plus vulnérables aux attaques (spam, appropriation des abonnés).

Les listes qui ne proposent pas de scénario d'abonnement ouvert (de type subscribe.open) doivent toutes être cachées, et peuvent appartenir à un groupe à visibilité réduite :

```
#list_data/nom_liste/config
visibility conceal
#default/scenari/topics_visibility.conceal
!equal([sender],'nobody')      smtp,dkim,smime,md5 -> do_it
true()        smtp,dkim,md5,smime -> reject(reason='topic_identified')
#default/topics.conf
Listes-internes
title      Listes réservees aux employes
visibility conceal
```

Toutes les listes doivent être protégées contre la récupération de leurs abonnés, ce qui impose au minimum des scénarii de type review.intranet ou review.private. Exemple :

```
is_subscriber([listname],[sender])      smtp,dkim,md5,smime -> do_it
match([sender],/[conf->host]$/)            smtp,dkim,md5,smime -> do_it
true()                                     smtp,dkim,md5,smime ->
reject(reason='review_subscriber')
```

La création des listes doit être contrôlée par les listmaster, au minimum, voire être interdite à toute autre personne que le listmaster (le scénario automatic_list_creation.public est exclu).

[1] A contrario, un moteur de listes interne à une entreprise peut proposer des listes en abonnement ouvert, mais restreint au seul périmètre des employés de cet établissement.

La modification des sources de données ne doit pas être autorisée aux propriétaires. En effet, un propriétaire de listes pourrait alors utiliser comme source d'abonnés les membres d'autres listes. Par défaut, un moteur de listes comme SYMPA l'interdit :

```
#default/edit_list.conf

user_data_source          owner,privileged_owner              hidden
include_list              owner,privileged_owner              hidden
```

Il est fortement conseillé de placer le moteur de listes dans une zone interne, protégée, et d'accéder à l'interface par l'intermédiaire d'un reverse-proxy. Dans tous les cas, la base de données ne peut pas rester sur une zone directement accessible au public.

L'ouverture au grand public, particulièrement si la cible visée est internationale (différents fuseaux horaires), doit s'accompagner d'une réflexion sur le niveau de service à offrir (en particulier sur la disponibilité).

3.1.4 Répartition des rôles propriétaire/modérateur

Si les rôles de propriétaire et de modérateur peuvent être remplis par les mêmes personnes, ils sont pourtant bien distincts et il est préférable de les attribuer formellement, même si cela revient à saisir deux fois les mêmes données. Cela permet aux abonnés de visualiser clairement qui assure chaque rôle, et facilite l'évolution indépendante des deux fonctions.

```
owner
email jean.durand@domaine.org
editor
email jean.durand@domaine.org
```

Lorsque le moteur de listes est affilié à un établissement (association etc.), au moins un propriétaire doit appartenir au référentiel de l'établissement. Cela permet de suivre plus facilement le cycle de vie des listes, et d'éviter d'encombrer le moteur de listes avec des listes orphelines. S'il s'agit d'un service volontairement ouvert au grand public, le cycle de vie devra être soigneusement décrit, et la disparition des propriétaires conduire à la fermeture puis la suppression des listes.

Les modérateurs qui disposent de plusieurs adresses doivent toutes les inscrire, surtout si chacune de leurs adresses de messagerie est installée sur un poste de travail indépendant.

Il est préférable de positionner un modérateur sur les listes d'échange libre, au moins pour une raison : en cas de campagne réussie de spam, il sera plus facile de mettre en place un scénario de modération pour endiguer l'attaque.

3.2 Typologie des listes

3.2.1 Identification et catégorisation des listes

Dès qu'il se développe, le service de listes exige une grande rigueur dans le nommage et le tri des listes par rubriques :

- Le listmaster, qui est amené à effectuer des actions à risques (fermetures de listes !) doit éviter toute confusion ;
- Les propriétaires, qui ont également des actions impactant les abonnés (ajout, suppression), doivent éviter d'intervenir sur une liste inadéquate .

Lorsque l'on gère des centaines, voire des milliers de listes, il est nécessaire de mettre en place des règles de nommage pour homogénéiser les libellés et éviter les ambiguïtés. Plusieurs règles de nommage existent dans nos divers établissements. Nous recommandons de mettre en place un comité de nommage dans votre établissement qui garantit et édicte les règles de nommage.

Dans beaucoup d'établissements, les adresses des listes sont insérées dans le carnet de contacts des employés : il faut éviter d'introduire une ambiguïté entre la liste de diffusion associée à un service et l'adresse fonctionnelle de ce service. Ex. : dsi@domaine.org est-elle l'adresse du responsable de la DSI ou une liste de diffusion permettant d'atteindre tous les employés de la DSI ?

- Lorsque le carnet d'adresses proposé aux utilisateurs mixe les adresses des listes avec les adresses des employés, le nom des listes doit être préfixé par un terme compris de tous dans l'établissement. Ex. : list-dsi@domaine.org ou l.dsi@domaine.org
- Lorsqu'on met en place des listes, correspondant à une partie réduite d'une liste existante, leurs noms doivent rappeler la liste principale. Ex. : list-dsi-networks@domain.org, list-dsi-system@domain.org
- Le nom de la liste doit rappeler le plus clairement possible le périmètre des abonnés (lorsque la liste correspond à une structure sociale) ou la thématique qui rapproche les abonnés. Ex. : les passionnés du théorème de Fermat s'abonneront à theoreme.fermat@domaine.org plutôt que math.students@domaine.org.

En ce qui concerne les listes étudiantes, leur nom peut être déduit des codes étapes définis dans les logiciels de scolarité, des UFR, ou du niveau de formation (globales ou par UFR) licence, master, doctorat. Certains établissements suffixent les listes étudiantes par l'année universitaire en cours pour permettre un recouvrement des listes sur plusieurs années. Ceci nécessite plus de ressources sur les serveurs de listes de diffusion.

Pour les autres listes structurelles, deux possibilités sont à votre disposition pour les adresses des listes de diffusion. Il est possible de préfixer vos listes PREF-<liste>@domaine.fr ou bien de créer des sous-domaines <liste>@SOUS-DOMAINE.domaine.fr dans votre domaine de messagerie qui correspondent alors à différents robots de listes dans l'outil de gestion de listes de diffusion.

Voici quelques exemples de préfixes ou sous-domaine utilisés dans nos différents établissements : drh, dgs, ac, dri, di, dfi, labo, projet, conf, asso, etc.

Lors de la création du moteur de listes, il faut déterminer quelles sont les thématiques susceptibles de discriminer les listes par thèmes, et s'assurer que ces thèmes soient compréhensibles par les futurs utilisateurs : cela comprend également la mise en place d'une traduction pour toutes leurs langues. Ex. :

```
# default/topics.conf
arts
title          Arts and Humanities
title.de       Kunst und Kultur
title.fr       Art et Culture
title.hu       MĆ±vÃ©szet, kultÃșra
visibility noconceal
```

3.2.2 Les listes syndicales

Les listes syndicales cristallisent toutes les tensions qui peuvent exister entre les fonctions de propriétaire et d'éditeur. Selon la culture sociale de chaque pays, la gestion de ce type de liste est plus ou moins facile à aborder.

Quelle que soit la situation, on doit distinguer :

- Les listes d'adhérents : quel que soit l'hébergeur (extérieur ou non à l'entreprise), le syndicat œuvre alors comme n'importe quelle association. L'adhésion au syndicat suppose l'acceptation d'un certain nombre de traitements automatisés, dont la saisie dans un fichier d'adhérents, qui peut être utilisé comme source de données pour constituer une liste de diffusion.
- Les listes d'information du personnel : les syndicats ont la possibilité de contacter toute personne travaillant dans une entreprise pour l'informer de ses droits ou pour assurer la publicité préalable à des élections professionnelles.

C'est le second type qui pose le plus de difficultés. Le listmaster doit s'appuyer sur un accord entre les partenaires sociaux afin de déterminer les modalités de constitution d'une liste d'informations syndicales. Il ne doit pas prendre l'initiative de créer de lui-même ce type de liste, ni en définir le cadre de fonctionnement technique (source de données, modération).

Deux techniques d'alimentation des abonnés sont envisageables : opt-in et opt-out.

- La méthode de opt-in fonctionne sur la base d'une adhésion volontaire : le processus de gestion des ressources humaines doit intégrer une phase d'information (ex. : envoi d'un courriel) donnant des indications suffisamment précises pour qu'un nouvel employé puisse s'abonner (immédiatement ou pas) à une liste d'information syndicale. Ex pour s'abonner :

  (mailto:sympa@domaine.org?subject=sig%20nom_liste)

Nous déconseillons fortement de mettre en place des procédures de rafraîchissement régulier (mise à jour d'une liste d'abonnés à partir du référentiel des ressources humaines). En régénérant la liste des abonnés, il permet rarement de respecter le vœu des employés qui se sont désabonnés après un chargement précédent pour ne plus recevoir l'information syndicale. L'opt-in est assez simple à mettre en place.

- La méthode d'opt-out impose l'abonnement en préalable, mais permet à tout employé de se désabonner à sa guise : dans ce cas, le processus de gestion des ressources humaines abonne l'employé à une ou plusieurs listes d'informations syndicales, mais le message de bienvenue doit impérativement rappeler les modalités de désabonnement, et chaque message envoyé par la liste doit

disposer d’un pied de page permettant de retrouver les modalités du désabonnement.[Verdin 2013] On pourra abonner d'office le personnel à l'ensemble des listes syndicales (ou pas) lors de la procédure d'activation des comptes. Ces listes peuvent être rafraîchies automatiquement si une procédure de désabonnement est mise en place, par exemple via des listes d'exclusion. Il faut alors développer une interface spéciale pour ces listes afin de gérer les désabonnements via des requêtes SOAP. La liste des abonnées doit être cachée des propriétaires et abonnés.

3.2.3 Les listes d’étudiants

Les scolarités inscrivent les étudiants. Ceux-ci suivent un cursus menant à un diplôme se déroulant sur plusieurs années (on parle d'étapes) avec certaines spécificités (version d'étapes). Les besoins sont variés :

- enseignants contactant leurs élèves
- scolarités
- forums

En général, les abonnements à ces listes sont fermés, les abonnements se font via une source de donnée LDAP. Il faut mettre au point des scenarii qui permettent aux enseignants d'une composante ou de l'université de poster dans ces listes. Les facultés doivent pouvoir décider des modes de transmission des informations (newsletters institutionnelles ou à l'inverse groupe de travail, avec ou sans modération)

Une école d'ingénieur aura tendance à suivre un groupe d’élèves jusqu'à son diplôme, elle nommera alors les listes sous la forme promo-biomat-2015, 2015 étant la date de sortie de la promo. Pour les universités ayant de très nombreuses formations, ceci est plus difficile à réaliser. En général elles mettent en place des listes par étape de diplômes avec ou sans suffixe lié à l'année, par ex :

etape-bcgu00-2014 (étape bcgu00 de l'année 2014-2015)

ou plus simplement

etape-bcgu00

Remarque : ajouter un suffixe lié à l'année double le nombre de listes et induit chaque année de changer le nom de la liste.

3.3 Cycle de vie

Lorsque l'on travaille sur un campus universitaire ou dans un établissement du secondaire, les listes de diffusion liées à la gestion des étudiants suivent le cycle de vie d'une année universitaire ou scolaire. Il est alors nécessaire d'automatiser au maximum la gestion (création, mise à jour et suppression) de ces listes.

D'autres listes peuvent également être gérées automatiquement, comme par exemple la liste des membres du personnel, ou bien des listes spécifiques par entité, catégorie de personnel, fonction, etc. Si l’on travaille dans un établissent de l'enseignement supérieur, on sera également amené à mettre en place les métalistes de l'enseignement supérieur et de la recherche.

Les sources de données de la majorité des listes de l'établissement listes sont les divers référentiels personnels et étudiants (bases de données, annuaires, etc.).

3.3.1 Création et suppression des listes étudiantes

Les listes de diffusion liées à la gestion des étudiants suivent le cycle de vie d'une année universitaire ou scolaire. Elles sont créées à la rentrée. Leur suppression est liée aux règles de nommage adoptées. Si les listes étudiantes ne sont pas suffixées par l'année en cours, elles doivent être supprimées et recréées à la rentrée. Ceci à comme inconvénient de ne plus pouvoir contacter les anciennes promotions, mais comme avantage d'avoir une seule adresse à gérer. Si l'on suffixe les listes étudiantes avec l'année universitaire ou scolaire en cours, cela permet de conserver plus longtemps les anciennes listes. Il faut déterminer avec les responsables de la scolarité le délai de conservation de ces listes.

3.3.2 Gestion des années scolaires

On peut conserver en permanence les listes de l'année N et celles de l'année N-1. Cela impose des contraintes, car il faut alors figer les listes de l'année N-1 pour conserver les abonnés tels qu'ils étaient à la fin de l'année. Ce problème peut être contourné en conservant, dans le référentiel de l'établissement, les informations relatives aux deux années. Ce contournement déporte cependant la complexité sur la gestion du référentiel.

Ces listes peuvent avoir des archives car les abonnés restent les mêmes.

Une autre solution est de garder toujours le même nom, mais cela pose des problèmes si une personne veut contacter en septembre les étudiants de l'année N-1. Afin de garder une certaine souplesse, on peut faire varier les filtres des sources LDAP via des scripts de génération de famille. Par exemple, de juillet à novembre, on considère deux populations, soit Pn et Pn-1. Si Pn vaut trois quart de Pn-1, alors le filtre prend l'année N, sinon il prend les deux années N et N-1. En faisant ainsi, on glisse progressivement d'une année sur l'autre, et si la période d'inscription est courte, les listes convergent plus vite.

Les archives : les abonnés changeant d'une année sur l'autre, il vaut mieux ne pas archiver ces listes.

3.3.3 Autorisation de postage

L'autorisation de postage à ces listes peut être diverse. Voici quelques exemples de droits :

- Postage autorisé à tous
- Postage autorisé aux adresses internes de votre établissement (intranet)
- Postage autorisé aux membres de la liste
- Postage autorisé à la direction de l'établissement pour les listes générales des membres du personnel
- Postage autorisé à un nombre limité de personnes à définir (responsable d'une entité, responsable de scolarité, responsable de service, etc.)

Plus le droit de postage est ouvert, plus la gestion est facile et moins la diffusion des messages est contrôlée. Il faut trouver le juste équilibre pour chaque liste en fonction de leur utilisation.

3.3.4 Mise à jour des abonnés

Les abonnés des listes automatiques sont mis à jour automatiquement à partir des sources de données auxquelles les listes se rapportent. On peut cependant se poser la question de la mise à jour manuelle des listes si les référentiels ne sont pas à jour ou si l'on souhaite ajouter des abonnés supplémentaires. C'est un choix à faire en fonction de votre établissement.

- L'autorisation de la mise à jour manuelle offre de la flexibilité, mais peut dégrader la qualité des données.
- La non autorisation de la mise à jour manuelle, demande plus de temps en cas de problème dans le référentiel et nécessite une réactivité importante de la part des administrations comme les scolarités et les services de ressources humaines.

3.3.5 Archivage

Lorsqu'une liste est supprimée, il est souvent utile d'archiver les données (listes des membres, courriel) pendant une certaine période. Une année de rétention des archives semble suffisante dans nos établissements.

4 Exploitation

La déclinaison des rôles (listmaster, propriétaire, modérateur, abonnés) dans un moteur de listes permet de déléguer une grande partie de l'exploitation fonctionnelle à des tiers.

L'exploitation du moteur de listes est souvent assurée par l'équipe qui endosse le rôle de listmaster. Ce chapitre décrit les tâches et difficultés les plus fréquemment rencontrées par un exploitant/listmaster.

- La relation avec les propriétaires. Elle nécessite un travail préalable sur la répartition en domaines de messagerie puis sur le nommage des listes, Des questions subsidiaires se posent sur les référentiels d'abonnés, et le cycle de vie des listes.
- La relation avec les modérateurs. Elle porte principalement sur le flux des messages.
- La mise à jour des versions du moteur de listes
- Le maintien en condition opérationnelle.
- Le développement de scripts pour créer et mettre à jour les familles de listes
- La validation du nommage des listes en relation avec une charte de nommage
- Il est déconseillé d'avoir des relations directes avec les usagers pour les questions relevant de leur abonnement (c'est le rôle du propriétaire) ou de leurs contributions (c'est le rôle du modérateur).

4.1 Exploitation en relation avec les propriétaires

4.1.1 Distinction des domaines virtuels

Avant même d'aborder les questions d'exploitation, on doit accorder l'architecture du moteur de listes au service attendu :

- Dans le cas d'une diffusion institutionnelle interne à l'organisation, le domaine de diffusion doit être protégé, les sources de données des listes doivent utiliser autant que possible les référentiels du personnel et des étudiants (bases de données et/ou annuaires), le nommage des listes doit être construit selon des règles précises, voire automatisables ; les scénarios doivent être travaillés pour pouvoir répondre aux règles communes de diffusion ; le serveur est localisé en interne.
- Dans le cas d'un service public, le domaine de diffusion doit être ouvert, les sources de données sont rarement automatisées, les scénarios doivent rester le plus standard possible ; le serveur peut être localisé en DMZ, même s'il est préférable de le protéger par un reverse-proxy.

Règles à suivre :

- même si l'on mutualise ces deux types de listes sur un seul serveur, il faut mettre en place plusieurs domaines virtuels et monter un robot distinct pour chaque domaine. Ex. : domaine réservé aux étudiants, domaine réservé aux enseignants et administratifs, domaine réservé aux listes hébergées pour le compte des partenaires de recherche etc.
- Pour chaque domaine virtuel, on adaptera (en l'élaguant au plus juste), la liste des groupes de listes (« topics », dans SYMPA).
- Le robot dédié au « service public » doit afficher une charte qui spécifie clairement que les listes « orphelines » (Qui n'ont plus de propriétaire) sont fermées sans préavis.

Les tâches d'exploitation sont plus lourdes dans le cas d'un domaine destiné à la diffusion institutionnelle, en particulier pour industrialiser la création et l'alimentation des listes et élaborer des scénarios répondant aux nécessités d'un contrôle fin de la diffusion.

4.1.2 Industrialisation de la création de listes

Les grandes organisations comme les universités, segmentent leur diffusion sur un emboîtement de critères mêlant la temporalité (quelle année), la scolarité (quelle étape, quelle matière, quel cursus) et les ressources humaines (quel statut, quel corps...).

Règles à suivre :

- Les listes doivent être regroupées par typologie et suivre le même modèle en termes d'autorisations, de modes de diffusion, de taille de message, de définition des rôles et des sources de données. On peut tolérer une variation ultérieure de certains paramètres, mais l'instanciation part d'un modèle (template) unique. Avec SYMPA, cette instanciation générique s'appuiera sur la notion de famille.
- Le nommage de la liste doit être automatisé et déduit des critères d'extraction des abonnés. Ex. : « etape-hhi303 » est le nom construit par extraction des étudiants appartenant à l'étape hhi303 dans l'annuaire de l'université, lui-même alimenté par la base de données de la scolarité.

- Si l'automatisation du nommage obscurcit l'objet de la liste, le processus de création doit enrichir l'extraction de manière à construire un libellé plus détaillé : avec SYMPA, on renseignera le fichier « info ».

Chaque famille de listes [Bouteille 2004] utilise un scénario disponible sur le moteur de listes, pour les différentes fonctionnalités (qui peut s'abonner, qui peut se désabonner, qui peut diffuser, etc.). Dans un cadre institutionnel, les scénarios fournis avec le moteur de listes ne suffiront pas. Il sera nécessaire de les enrichir avec les autorités responsables de chaque famille de listes : selon les cas, il s'agira de la direction des études, de la scolarité, du recteur ou de son secrétaire général, des ressources humaines, de la direction de la communication. En pratique, l'exploitant doit échanger avec le propriétaire de la source de données des abonnés (pour les extractions et les scénarios liés aux abonnements) et avec le diffuseur principal (pour les scénarios liés à la modération)

Règles à suivre :

- Une liste dynamique (issue de ce processus d'industrialisation) ne doit pas avoir d'abonnés autres que ceux renvoyés par l'extraction automatique. S'il est nécessaire d'ajouter (ou de supprimer) un abonné, cela doit passer par la correction du référentiel des abonnés. Toutefois, on pourra construire des scénarios d'abonnement autorisant les enseignants ou secrétaires pédagogiques à s'abonner ou à poster dans les listes des formations.
- La fréquence d'extraction est déduite du processus d'alimentation des données dans le référentiel, de la lourdeur de cette extraction et du risque de contournement manuel en cas de rafraîchissement trop lent. Cas d'école :
    - Processus d'alimentation de la source de données clos avant la mise en fonction de la liste ; mise à jour rare ; liste utilisée pour des informations sans caractère d'urgence (liste d'étudiants) : la mise à jour peut être quotidienne ;
    - alimentation de la source de données en flux continu ; mise à jour à tout moment en entrée et en sortie ; l'abonnement à la liste est un prérequis pour accéder à plusieurs services critiques (liste de prestataires et contractuels conditionnant l'accès à des systèmes protégés) : la mise à jour doit être faite toutes les heures (pour éviter un fort risque de contournement et d'abonnement manuel)
- Quel que soit le choix de modération pour chaque famille, il faut prévoir une liste de « VIP » qui sera autorisée à publier sur les listes institutionnelles. Il est judicieux de rajouter ces listes aux différents scenarii
- L'instanciation d'une liste à partir d'un *template* peut être réalisée par *batch* quotidien ou dynamiquement, au premier envoi de message concernant la liste. Lorsqu'on présume qu'un nombre réduit de listes sera instancié dans une famille donnée, il est préférable de différer l'instanciation au premier envoi de message. Cas d'école :
    - Lors d'élection professionnelle, le listmaster doit créer une liste par organisation syndicale (environ 12), pour chaque scrutin (environ 35), dans chaque académie (environ 32). La création par batch générerait 13440 listes alors que la majorité des listes ne sera jamais utilisée. La création dynamique est préférable.
    - Pour les besoins d'une communication régulière avec les étudiants, une université doit créer une liste par étape de formation pour une année scolaire donnée, soit 2000 listes environ. Les listes sont déterminées plusieurs jours avant leur utilisation effective : le *batch* de création est conseillé.

4.1.3 Cycle de vie des listes

Une fois réglées les modalités de création de listes, la difficulté principale d'un exploitant réside dans le nettoyage des listes obsolètes. Pour éviter tout problème, en particulier dans le cas d'un service ouvert à l'extérieur, il est indispensable d'anticiper les différents cas de figure que l'on pourra rencontrer, en détaillant les processus que l'exploitant mettra en œuvre :

- le propriétaire n'est plus joignable. Selon les cas de figure, l'exploitant peut fermer la liste, solliciter l'entité à laquelle appartenait le propriétaire, contacter les modérateurs (s'il y en a) ou les abonnés (si le scénario le lui permet) pour demander la nomination d'un nouveau propriétaire.
- La liste présente un taux élevé d'erreurs. Avant de contacter le propriétaire, il est préférable d'effectuer une analyse sommaire des incidents, qui peuvent venir d'un dysfonctionnement de la plate-forme de messagerie elle-même (ex. : enregistrements SPF erronés...)
- La liste n'est plus utilisée depuis une longue période. L'exploitant peut suggérer ou décider de sa fermeture.

4.2 Exploitation en relation avec les modérateurs

Les questions à régler dans ce cadre relèvent de la gestion des flux de messagerie et appartiennent à deux catégories :

- régler l'antispam pour que les listes soient peu ou pas spammées ;
- répondre ou réagir aux sollicitations des modérateurs qui s'inquiètent des délais de distribution de leurs messages.

4.3 Changement de version du moteur de listes

Dans le cadre d'un changement de version, on conserve le même domaine d'adressage pour ses listes, même si le serveur physique (ou la machine virtuelle) peut être différent.

Pour garantir la continuité du service de listes, il faudra préparer la mise à jour de manière à réduire le risque de retour arrière. En effet, le retour arrière ne pourra se faire qu'en restaurant les données et le code correspondant à la sauvegarde faite lors du changement de version : si les diffusions de courriels restent acquises, les mises à jour de données (archives des courriels envoyés, configuration et contenu des listes, configuration des abonnés) seront perdues.

Il faut noter qu'un service de liste peut être utilisé pour des alias fonctionnels de type publics. Un arrêt du service de listes équivaut à un arrêt du système de messagerie. Il conviendra donc de bien préparer un serveur de test avant de se lancer dans une migration. On ne peut pas arrêter le service une journée.

Règles à suivre :

- Bien lire la RELEASE NOTES (pour SYMPA: http://www.sympa.org/distribution/latest-stable/NEWS et plus particulièrement les lignes qui débutent par des *****. Ces lignes signalent les changements qui ne sont pas compatibles avec la version antérieure)

- Un moteur de listes en production doit être doublé par un moteur en pré-production. Cette plate-forme de pré-production ne peut pas être une copie conforme de la production (la configuration de l'interface web et le domaine de messagerie vont différer), mais il doit disposer des mêmes connecteurs (ldap, base de données, web-services etc.). La mise à jour doit être testée sur cet environnement et être qualifiée par une suite de tests correspondant aux cas de figure couramment rencontrés (alimentation dynamique d'une liste, instanciation d'une famille, accès au web service etc.). L'ensemble des actions doit être noté, commandes comprises, pour pouvoir accélérer la mise à niveau suivante (en production).
- En production et en pré-production, la mise à jour commence par une sauvegarde de l'ensemble du moteur de listes, librairies comprises. Dans le cas de SYMPA, on aura intérêt à dédier les principaux composants (apache, perl, monharc et mysql) au moteur de listes, et à en effectuer la sauvegarde.
- En production, la configuration et la compilation peuvent avoir lieu pendant que la version précédente continue de fonctionner : la plupart des difficultés apparaissent à cette étape, avec des versions de composants incompatibles entre eux.
- En production, avant de lancer le processus de mise à jour des données, il faut arrêter l'arrivée des courriels en amont et s'assurer que les dernières diffusions sont terminées. Le rétablissement du courriel est réalisé une fois les listes totalement et correctement migrées.
- En cas d'incident majeur, on restaure la configuration précédente : les courriels diffusés entre la mise à jour et la restauration disparaîtront alors des traces. Il peut être nécessaire de conserver une sauvegarde avant retour arrière pour des raisons administratives ou juridiques.

Voir Annexe B pour une note sur la mise à jour d'un serveur Sympa.

4.4 Maintien en condition opérationnelle

L'exploitant doit assurer :

- La sauvegarde, qui concerne les données fichier (principalement etc, list_data et arc sur SYMPA) ainsi que la base de données. Il doit également s'assurer, en amont de son périmètre, que ses sources de données (annuaire, web service, bases de données métiers) soient bien sauvegardées.
- La disponibilité des sources de données externes, du moteur lui-même, de la base interne et du portail web : un suivi nagios (ou équivalent) est indispensable.
- Le suivi des performances du serveur hébergeant le moteur de listes et de la messagerie (en particulier l'occupation des spools pour SYMPA).
- Une mesure du temps de traitement par envoi régulier d'un courriel à une liste de test, avec un suivi graphique, permet à la fois d'être alerté lorsqu'un dysfonctionnement intervient sur un des éléments de la chaîne de traitement, y compris sur la messagerie entrante et sortante, mais également de disposer du profil de fonctionnement annuel de son moteur de listes. Ce graphique est particulièrement utile pour planifier les mises à jour de version, et aider les gros consommateurs à planifier leurs envois. Plusieurs utilisateurs de SYMPA ont développé des scripts permettant d'automatiser ce type de mesures.

5 Informatique et libertés

5.1 Données concernées

Les données à caractère personnel qui sont concernées par les services de liste sont :

- l'adresse électronique;
- le nom et le prénom;
- éventuellement : une image représentant l'utilisateur (avatar);
- éventuellement : certaines autres données, selon la liste, qui ne sont jamais des données faisant apparaître "les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci."

Les contenus échangés, eux relèvent plus du contenu éditorial, mais peuvent contenir les données précédentes et doivent donc être protégés au même titre.

On trouve des données personnelles dans trois cas de figure :

- le maintien d'une liste de personnes abonnées à une liste de diffusion ;
- les archives de la liste : certaines listes conservent un historique des messages envoyés. Cet historique peut être public ;
- les journaux des applications.

5.2 Quand et comment protéger des données ?

5.2.1 Confidentialité

Avant tout, il convient de distinguer les informations relevant de l'activité professionnelle et celles relevant de la vie privée. Ensuite, parmi les données professionnelles, il faut distinguer celles qui doivent rester confidentielles et celles qui peuvent être publiques.

En fonction de ces critères, on peut établir les règles ci-dessous :

	Archives	Visibilité liste	Accès liste abonnés
Vie privée	Réservées aux abonnés	Réservée aux abonnés	Réservé aux abonnés
Professionnel public	publiques	publique	Réservé aux abonnés

Professionnel confidentiel	Réservées aux abonnés	dissimulée	Réservé aux abonnés Voire bloqué

On peut définir des listes totalement masquées, où toute action est limitée voire impossible, hors l'envoi de message. SYMPA dispose de réglages permettant de rester sans réponse lorsqu'un accès non autorisé est tenté sur une liste cachée. Tout se passe en fait comme si la liste n'existait pas

À l'extrême, l'existence même de la liste doit rester secrète.

5.2.2 Droit de se désabonner d'une liste

Le droit de modification peut avoir des limites, si l'abonnement à une liste de diffusion entre dans les obligations liées à l'occupation d'une fonction. Une liste d'information du personnel, par exemple, peut interdire le désabonnement, parce que le fait d'appartenir à l'établissement impose de recevoir les messages d'information du personnel. Dans tout autre cas, l'utilisateur doit disposer de moyens clairs de désabonnement, dans l'idéal par l'insertion d'un lien de désabonnement dans le pied de page des messages,

5.2.3 Droit d'accès à ses données personnelles

Tout abonné doit pouvoir facilement savoir quelles données personnelles le concernant sont utilisées par le service de listes.

5.2.4 Traçabilité de l'activité des listes

La traçabilité des échanges est indispensable pour vérifier l'intégrité des données. Cette sécurisation est rendue possible par le biais de plusieurs mécanismes :

La signature des messages : l'emploi de signatures S/MIME ne garantit pas contre la présence d'un MITM (Man In The Middle), mais pourra garantir l'intégrité du contenu des messages.

La conservation de journaux sur une durée légale maximale (un an en France) permet de contrôler les accès aux données.

Traces : SYMPA permet l'analyse des MDN et des DSN par utilisateur, ce qui permet d'avoir, pour chaque message envoyé, la liste des destinataires et l'état de délivrance (reçu, erreur, accusé de réception envoyé, etc.) Attention : ce mécanisme a un coût : il impose une session SMTP sortante par destinataire. Ceci offre une possibilité de garder des traces reposant sur les protocoles standards. L'usage de méthodes plus discutables telles que les pixels espions est découragé. D'une part parce que c'est un moyen relativement déloyal de s'assurer de la lecture d'un courriel à l'insu du lecteur, d'autre part parce que ce mécanisme est de toute façon discutable, l'affichage d'une image étant en général soumis à l'approbation du lecteur par la plupart des clients

de messagerie. Par ailleurs, ce genre de contenu augmente les chances que votre message soit considéré comme un spam.

Pour aller au-delà, on peut chiffrer les messages de toute une liste, mais cela impose que la liste ainsi que tous ses abonnés dispose d'un certificat.

Voir Annexe A pour une étude plus détaillée du cas français.

6 Niveau de service

Un moteur de listes intervient dans un mécanisme de diffusion asynchrone par nature, puisque s'appuyant sur la messagerie électronique.

Néanmoins, il peut proposer des interfaces, pour les utilisateurs et pour son administration, qui peuvent faire l'objet d'une négociation sur un accord de niveau de service.

Les points que pourra lister un catalogue de service, et qui pourront être associés à un niveau de service sont :

- La disponibilité du mécanisme de messagerie,
- en réception (envoi des commandes au robot – abonnement, désabonnement, consultation des abonnés, etc. - envoi des courriels à rediffuser, validation ou rejet des courriels à modérer, etc.)
- en émission (diffusion des courriels aux abonnés, transmission des demandes de modération aux modérateurs, etc.)
- La disponibilité des interfaces (utilisateurs, administrateurs)
- La réactivité des administrateurs pour toutes les tâches qui sont soumises à leur contrôle (validation de l'ouverture d'une liste, modification d'un scénario, ajout ou augmentation des droits d'un propriétaire, mise en place d'une source de données ou d'un connecteur à une source de donnée non répertoriée)
- La capacité à hiérarchiser les envois selon les listes
- La volumétrie supportée (en particulier, la taille des courriels, mais également le type de pièce jointe, le nombre d'abonnés)

Les leviers d'action pour augmenter le niveau de service couvrent le domaine organisationnel comme le domaine technique.

6.1 Organisation du service de listes

Le service de listes repose sur une équipe clé, le "listmaster". Administrateur du moteur de listes, il reçoit et doit traiter dans les délais requis les requêtes des utilisateurs transmises par le serveur.

- La fonction de listmaster doit être partagée par plusieurs intervenants. Ex :

  ```
  listmaster listmaster@domaine.org, jean.dupont@domain.org,
  john.bull@domain.org, pietro.bruni@domain.org, hans.muller@backupdomain.org
  ```

- On peut augmenter le niveau de service en répartissant les listmaster sur différents domaines de messagerie (leur adresse ne doit évidemment pas être l'adresse d'une liste) et en organisant des plages horaires plus larges.
- Le catalogue de services doit être rédigé, publié, et accessible : utiliser le bouton « Help » pour positionner un lien sur le document.

Une équipe de supervision doit surveiller le fonctionnement du moteur de listes :

- Etat du service de messagerie (postfix, sendmail…)
- Etat du service de publication http (ex. : contrôle page /wws)

- Contrôle des files d'attente de messagerie
- Mesure du temps de parcours d'un message au travers du système de diffusion [Racvision]

La mise à disposition de l'annuaire des listes dans un annuaire du personnel peut faciliter leur usage. Les mécanismes mis en place doivent tenir compte du caractère caché ou non des listes dont on déduira l'affichage ou non de l'adresse de la liste dans le carnet de contacts.

Le listmaster, qui a un rôle opérationnel, dépend d'une instance décisionnelle qui décide de la politique de diffusion du moteur de listes :

- Quelles sont les priorités données au moteur de listes ? (diffusion institutionnelle descendante, groupes informels échangeant librement, etc…) : le listmaster traduira ces directives en « templates » et niveau de priorité pour chaque catégorie.
- Quels sont les scénarios qui s'imposent à tous ? (certains abonnés peuvent-ils écrire à toutes les listes, la visibilité des abonnés est-elle interdite par défaut, la taille des courriels est-elle contrainte, etc…) : le listmaster traduira ces directives en scenarii, paramètres de configuration, listes d'abonnés particuliers.

Si les listes font appels à des modérateurs, on leur appliquera les mêmes règles qu'aux listmaster : plusieurs intervenants, étendue des horaires. En matière de modération, les utilisateurs peuvent présenter des exigences de service, comme être (ou ne pas être) prévenu que leur courriel est envoyé au modérateur. Dans l'exemple suivant, les courriels envoyés par ceo@domaine.fr sont modérés par l'éditeur sans que ceo soit pollué par des notifications. Les autres diffuseurs reçoivent encore les notifications.

```
# modération silencieuse pour un VIP
match([sender],/^ceo\@domaine\.\.org$/) smtp,dkim,smime,md5 -> editorkey,quiet
is_editor([listname],[sender]) smime,md5 -> do_it
true smtp,dkim,smime,md5 -> editorkey
```

6.2 Mécanismes techniques pour augmenter le niveau de service

Certains points critiques ont un impact direct sur le niveau de service rendu par un moteur de listes

Pour la base de données, on augmentera le niveau de service :

- en mettant en place des sauvegardes online/offline à un rythme plus ou moins soutenu ;
- en mettant en place un système de cluster pour les SGBD qui le supportent.

Pour le frontal web (apache, etc.), on augmentera la sécurité et le niveau de service :

- En positionnant à l'amont un mécanisme de proxy et traitement de certificat (par un firewall/routeur/accélérateur physique ou par le couplage logiciel de ldirectord/heartbeat/apache ssl/haproxy) ;
- En déployant le moteur de liste sur un cluster.

Pour la fiabilisation des sources de données, on augmentera le niveau de service :

- En mettant en place des sources de données redondées, soit au niveau de la configuration de la liste, soit en positionnant un mécanisme de redondance entre le moteur de listes et la source de données. Dans cet exemple, on utilise un proxy sur une source de donnée SQL

```
include_sql_query
db_name sgbd_redonde
name mabase
db_port 3306
host proxysql.priv.domaine.org
passwd XXXX
db_type mysql
user sympa
sql_query SELECT DISTINCT email FROM table WHERE condition = "valeur"
```

Pour le mécanisme d'émission SMTP, le moteur de listes étant couplé à un service SMTP local, il faut utiliser un cluster pour fiabiliser le point de départ SMTP. Par contre, le moteur de listes étant un système de spam, même sous contrôle, le niveau de service sera amélioré en mettant en place des mesures de contrôle du débit sortant :

Lorsque des domaines sont réputés sévères en matière de "flood", on dirige le courriel des abonnés dépendant de ces domaines à un relais SMTP volontairement lent. Dans cet exemple, les courriels destinés aux abonnés ayant une adresse de type @strict.fr sont renvoyés vers un relais dont les paramètres d'envoi ont été fortement réduits. Voici un exemple en utilisant le MTA POSTFIX :

```
#/etc/postfix/transport moteur de liste
strict.fr smtp:[172.1.1.3]:25
* smtp:[172.1.1.100]:25

#/etc/postfix/main.cf 172.1.1.3
# Pour limiter l'envoi en parallèle pour une même destination :
default_destination_concurrency_limit = 3
# Pour contrôler la fréquence d'émission de chaque paquet :
default_destination_rate_delay = 3s
# La tolérance au démarrage avant restriction si envoi plus massif
initial_destination_concurrency = 3
```

Annexes

1 Annexe A : Informatique et libertés : le cas français

La France dispose d'une réglementation précise en matière de protection de la vie privée. Il convient donc de l'exposer à part.

1.1 Première préoccupation : les listes elles-mêmes

Jusqu'il y a quelques années, la situation semblait claire. Elle était exprimée par la voix de la FAQ de la liste droit-net [Aumont & De Marco 2002].

La CNIL avait mis en place les normes simplifiées 15 et 23 permettant de faire une déclaration d'adoption de ces normes via le formulaire CERFA 99001.

Tout ceci a été modifié par la loi n° 2004-801 du 6 août 2004 [Loi 2004]. Comme on le voit sur la même FAQ de droit-net [Aumont & De Marco 2004], ceci remet en question les recommandations préalables vis à vis des listes de diffusion.

En effet : ces normes simplifiées ont disparu.

Ça ne date pas d'hier :

- la dispense de déclaration n° 7 [CNIL 2006] abroge la norme simplifiée 15
- la dispense de déclaration n° 8 [CNIL 2010] abroge la norme simplifiée 23

Il semble donc que la dispense n° 7 dispense les services de listes non commerciaux de toute déclaration CNIL, et la dispense n° 8 fait de même pour les associations.

Il ne reste désormais que la norme simplifiée n° 48 [CNIL 2012] qui porte sur les clients et prospects.

Conclusion qui semble cohérente :

- Pour une association ne faisant pas de démarchage commercial : pas de déclaration CNIL

- Si l’on est responsable d'un serveur de listes où toute activité commerciale est prohibée (ce qui est le cas d'Universalistes) : pas de déclaration CNIL
- Si l’on est responsable d'un serveur de listes où une activité de démarchage commercial est possible, on doit déclarer le service et s'engager à respecter la norme simplifiée n° 48.

S'il existe un CIL dans l'établissement, nul besoin de "déclaration CNIL" à proprement parler : une description/inscription au Registre suffit (sauf si les données sont réputées sensibles).

1.2 Seconde préoccupation : les archives

Là c'est plus flou. Il semble qu'on en reste à l'article 36 de la loi de 1978 [Loi 1978] qui indique qu'on ne peut conserver des archives "qu’en vue d’être traitées à des fins historiques, statistiques ou scientifiques".

Les archives des listes de démarchage commercial ne rentrent pas dans ce cadre mais, sur un service de listes d’établissement, un bon nombre de messages échangés dans les listes peuvent servir de référence et ont donc un intérêt "historique ou scientifique". D'autres, en revanche, devraient disparaître au nom du droit à l'oubli.

En tout état de cause, la conservation sur le long terme des adresses électroniques dans les archives de listes ne semble pas forcément "adéquate, pertinente et non excessive" : l'identité de l'émetteur d'un message est-elle forcément nécessaire ?

Il est tout-à-fait possible d'adapter le serveur de listes pour que les messages soient anonymisés au bout d'un certain temps. La question est de savoir quand. En effet, le droit à l'oubli pourrait s'appliquer légitimement, suivant le type de liste, dès qu'un des événements suivants se produit :

- quand une personne se désabonne
- quand une liste est fermée
- au bout d'un certain temps dans tous les cas de figure
- jamais tant que la liste est active.

Il y a une délibération de la CNIL qui porte sur les archives publiques [CNIL 2012-2]

Ce n'est pas exactement le cas de figure des listes de diffusion mais ça peut porter un éclairage.

1.3 Dernière préoccupation : les journaux

Nous conservons pendant un an des journaux de l'application SYMPA qui gère les listes. Ces journaux contiennent, quand elle est disponible, l'adresse électronique de la personne effectuant une action sur le serveur.

L’accès à ces journaux doit être protégé mais rendu accessible en cas de saisie par des services judiciaires.

1.4 Questions en suspens

Nous avons fait de notre mieux pour éclaircir les questions liées à l'informatique et les libertés dans le cas des listes de diffusion, mais certaines restent en suspens.

Quelles déclarations devons-nous faire pour les journaux et plus généralement en tant que responsables du traitement des données sur les services de listes ?

Que faisons-nous pour les archives ?

- Le propriétaire des données doit-il faire une déclaration ? Si oui, laquelle ?
- Comment le droit à l'oubli doit-il s'appliquer ?
    - Un an après le désabonnement d'une personne ?
    - Ou jamais tant que la liste est active ?
- La conservation des archives est-elle légitime plus d'un an après la fermeture d'une liste ?
- Si oui, doit-on anonymiser ces archives ? Au bout de combien de temps ?

2 Annexe B : Mise à jour d'un serveur Sympa

En pratique, voici quel peut-être le processus de mise à jour d'une plate-forme SYMPA :

Les étapes suivantes peuvent être facilitées par l'usage de la virtualisation et le clonage du serveur de production. Mais le déploiement final nécessitera de recopier les données qui ont évolué entre la phase de test et la phase production. Un rsync des principaux répertoires (spool, archives, list_data) est à prévoir.

- Duplication de l'environnement SYMPA sur un répertoire versionné. Ex. :

```
ls -ald sympa*
sympa → sympa_v619
sympa_v619
sympa_v620
```

- Dump de la base mysql, import sur une nouvelle base versionnée.
- Chargement des sources correspondant à la nouvelle version dans un répertoire dédié.
- Récupération du fichier de configuration utilisé pour la version précédente. Adaptation nécessaire pour prendre en compte le répertoire versionné, et ajouter de nouveaux paramètres si les notes de version les mentionnent.
- Lancement de la configuration puis de la compilation : à ce stade, les mises à jour de composants (perl, ssl, apache, mhonarc etc.) devront être appliquées dans le répertoire versionné. Si le CPAN permet d'appliquer les mises à jour à un répertoire donné de Perl, cela peut exclure certaines mises à jour automatisées de type yum.
- Arrêt en amont de la réception des messages (en fonction de l'architecture de messagerie et du produit utilisé, on peut couper le flux entrant, arrêter le serveur de messagerie ou le reconfigurer provisoirement pour émettre une erreur de type 4XX).
- Au choix : examen des spools de SYMPA pour s'assurer que les dernières diffusions sont terminées ou arrêt de SYMPA.
- Transfert des répertoires de configuration (~sympa/etc), des listes (~sympa/list_data), des archives (~sympa/arc), des bounces (~sympa/bounce) et du spool (si le serveur a été arrêté en cours de fonctionnement, ~sympa/spool) du répertoire de l'ancienne version vers la nouvelle.
- Lancement de l'installation de la nouvelle version, suivi par un upgrade : sympa.pl --upgrade [--from=X] [--to=Y].
- Modification des scripts de démarrage automatique SYMPA et apache, ou modification des liens des répertoires génériques ~sympa et ~httpd.
- Relance de SYMPA et d'Apache.
- Relance de la messagerie en amont.

Références

[Allman et al. 2007] E. Allman, J. Callas, M. Delany, M. Libbey, J. Fenton, M. Thomas, 2007: « RFC 4871 : DomainKeys Identified Mail (DKIM) Signatures » http://www.ietf.org/rfc/rfc4871.txt

[Aumont 2009] S. Aumont, 2009: « Mailing lists and DKIM » https://spaces.internet2.edu/display/ddx/Mailing+lists+and+DKIM

[Aumont & De Marco 2002] S. Aumont and E. De Marco, 2002 : « FAQ de la liste droit-net » https://groupes.renater.fr/droit-net/fom-serve/cache/82.html

[Aumont & De Marco 2004] . Aumont and E. De Marco, 2004 : « FAQ de la liste droit-net » https://groupes.renater.fr/droit-net/fom-serve/cache/42.html

[Aumont & Salaün 1999] S. Aumont and O. Salaün, 1999 (updated 2011): « Sympa reference manual : authorization scenarios » https://www.sympa.org/manual/authorization-scenarios

[Aumont & Salaün 2000] S. Aumont and O. Salaün, 2000 (updated 2010): « Sympa reference manual : S/MIME and HTTPS » https://www.sympa.org/manual/x509

[Aumont & Salaün 2001] S. Aumont and O. Salaün, 2001 (updated 2013): « Sympa reference manual for handling external data sources » https://www.sympa.org/manual/parameters-data-sources

[Aumont & Salaün 2003] S. Aumont and O. Salaün, 2003 (updated 2014): « Sympa reference manual : I authentication » https://www.sympa.org/manual/authentication

[Bouteille 2004] G. Bouteille, 2004 (updated 2013) : « Sympa reference manual : list families » https://www.sympa.org/manual/list-families

[CNIL 2006] CNIL, 2006 : « Dispense de déclaration n° 7 » http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/107/

[CNIL 2010] CNIL, 2010 : « Dispense de déclaration n° 8 » http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/106/

[CNIL 2012] CNIL, 2012 : « Norme simplifiée n° 48 » http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/184/

[CNIL 2012-2] CNIL, 2012 : « Délibération de la CNIL sur les archives publiques » http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article/quelles-sont-les-donnees-a-caractere-personnel-concernees-par-la-diffusion-sur-internet-de-docum/

[DMARC 2014] dmarc.org, 2014: « DMARC FAQ » http://www.dmarc.org/faq.html#s_3

[DMARC 2014-2] dmarc.org, 2014: « Domain-based Message Authentication, Reporting and Conformance (DMARC) Specification » http://www.dmarc.org/specification.html

[Hoffman 1999] P. Hoffman, editor, 1999: « RFC 2634: Enhanced security services for S/MIME » http://tools.ietf.org/html/rfc2634

[Klensin 2008] J. Klensin, 2008: « RFC 5321: Simple Mail Transfer Protocol – section 5.4.5 » http://tools.ietf.org/html/rfc5321#section-4.5.4

[Levine 2014] J.R. Levine, 2014: « Yahoo addresses a security problem by breaking every mailing list in the world » http://jrl.guru/Email/yahoobomb.html

[Loi 1978] Texte de loi, 1978 : « Article 36 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés » http://www.cnil.fr/en-savoir-plus/textes-fondateurs/loi78-17/#Article36

[Loi 2004] Texte de loi, 2004 : « Loi n° 2004-801 du 6 août 2004 » http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441676

[Racvision] Projet du Ministère de l'éducation nationale, normalisant les pages de supervision à insérer dans chaque application afin d'en mesurer différents indicateurs de disponibilité. Des pages et procédures spécifiques sont développées pour surveiller le fonctionnement de la messagerie et d'un porteur de liste. http://racvision.orion.education.fr/presentation/index.html

[Ramsdell & Turner 2010] B. Ramsdell and S. Turner, 2010: « RFC 5750: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2: Certificate Handling » http://tools.ietf.org/html/rfc5750

[Ramsdell & Turner 2010-2] B. Ramsdell and S. Turner, 2010: « RFC 5750: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2: Message Specification » http://tools.ietf.org/html/rfc5751

[Resnik 2008] P. Resnik, 2008: « RFC 5322: Internet message format » http://tools.ietf.org/html/rfc5322

[Verdin 2013] D. Verdin, 2013: « User-friendly automatic lists » https://www.sympa.org/manual/list-families#user-friendly_automatic_lists

[Verdin 2014] D. Verdin, 2014: « Sympa online help on DMARC » https://www.sympa.org/manual/dmarc

[Wong & Schlitt 2006] M. Wong and W. Schlitt, 2006: « RFC 4408 : Sender Policy Framework (SPF) for

Authorizing Use of Domains in E-Mail, Version 1 » http://www.ietf.org/rfc/rfc4408.txt

[Zhuk 2002] S. Zhuk, 2002: « Sympa reference manual : list_check_smtp parameter » https://www.sympa.org/manual/conf-parameters/part2#list_check_smtp

Glossaire

DKIM : Domain Key Identfied Mail – RFC 6376

DMARC: Domain-based Message Authentication, Reporting & Conformance

DMZ : Zone démilitarisée

DSN : Delivery Status Notification ou Message électronique automatique contenant le code de livraison d'un courriel.

Ham : Mot utilisé pour se référer, généralement, aux messages pertinents, utiles ou légitimes.

Listmaster : administrateur du service de listes

Modérateur : personne chargée de valider les contenus diffusés dans le cadre d'une liste de diffusion

Moteur de listes : alias de “serveur de listes”, application gérant un ensemble de listes de diffusion, leurs abonnés, la réception des commandes et la diffusion des messages selon des règles configurées par un ensemble de personnes autorisées

MDN : Message Disposition Notification ou accusé de réception envoyé en réponse à un message AS2

MITM : man in the middle, type d'attaque avec interception d'un flux entre un émetteur et un récepteur ; l'attaquant se fait passer pour le récepteur vis à vis de l'émetteur, et pour l'émetteur vis à vis du récepteur.

MTA : Message Transport Agent

Propriétaire : gestionnaire d'une liste de diffusion

Spam : Mot utilisé pour se référer généralement à tout message qui n'aurait pas du arriver dans une boîte aux lettres : non sollicité, non souhaité, nuisible, non pertinent, …

SPF: Sender Policy Framework – RFC 4408