




eMill

SOLUTION D'EMAILING PROFESSIONNELLE



LIVRE BLANC

**LES SYSTÈMES D'AUTHENTIFICATION
DES EXPÉDITEURS D'E-MAILS**



Parmi les procédés utilisés pour détecter les émetteurs de Spam, les méthodes permettant d'authentifier l'identité de l'expéditeur sont de plus en plus présentes.

En effet, une des techniques privilégiées par les émetteurs de Spam est d'**utiliser l'identité (spoofing) et le PC d'une personne tierce** afin qu'ils restent anonymes et ne puissent être reconnus et bloqués. Ces **PC appelés zombies** sont, en général, la propriété d'individus qui ne disposent pas de systèmes de protection suffisants. Ainsi, les émetteurs de Spam ont la possibilité de s'y connecter, d'envoyer le contenu d'un e-mail et de leur donner l'ordre d'envoyer plusieurs messages.

Les dernières études considèrent que **2 à 5 millions de machines** sont infectées et peuvent être utilisées pour relayer du Spam.

Les **systèmes d'authentification** sont une réponse à cette problématique. Ils sont, pour la plupart, basés sur le fonctionnement suivant :

1. **Identifier l'expéditeur d'un message grâce à son adresse IP** qui est contenue dans l'en-tête des e-mails.
2. **Vérifier si cette adresse IP correspond à un nom de domaine** connu et si elle est autorisée à diffuser des e-mails.

L'implémentation de la plupart des systèmes d'authentification va donc consister à associer l'adresse IP de l'ordinateur utilisé pour diffuser des campagnes à un nom de domaine et à l'autoriser « officiellement » à émettre des e-mails.

1. Définitions

Avant de commencer à détailler le fonctionnement de ces systèmes et des éventuels réglages à entreprendre, il est nécessaire de définir les mots clés suivants.

1.1 Serveur SMTP

Le Simple Mail Transfer Protocol (littéralement « Protocole simple de transfert de courrier »), généralement abrégé SMTP, est un protocole de communication qui établit la connexion entre l'expéditeur et le destinataire afin d'envoyer un courrier électronique. Lors de l'envoi d'un e-mail, 2 serveurs SMTP vont donc entrer en communication, celui de l'expéditeur et celui du destinataire. Les procédures d'authentification sont, en général, réalisées par le serveur SMTP de réception.

1.2 Adresse IP

Adresse composée d'une série de 4 nombres (ex. : 192.168.78.90) compris entre 0 et 255 qui sert à identifier chaque ordinateur connecté sur Internet. La plupart des abonnés résidentiels à Internet dispose d'une adresse IP dynamique ce qui signifie qu'elle change à intervalle régulier. Par opposition, l'adresse IP fixe correspond au fait qu'elle est attribuée définitivement à un ordinateur.

1.3 Nom de domaine

Le nom de domaine est l'équivalent 'littéraire' de l'adresse IP. Il permet d'identifier un ordinateur ou un serveur plus facilement qu'à travers une série de nombres (ex. : le nom de domaine d'eMill est eMill.net). Dans le cas d'un site Internet, le nom de domaine correspond à l'adresse IP du serveur qui héberge le site.

1.4 Serveur DNS

Le serveur DNS est un logiciel qui a pour principale mission de faire la conversion entre les adresses IP et les noms de domaine ou de sous domaine.

Par exemple, lorsque vous tapez l'adresse <http://www.emill.net> dans votre navigateur, un ensemble de serveurs DNS vont être interrogés afin de connaître l'adresse IP de ce site et pouvoir l'afficher.

Le serveur DNS contient plusieurs types de champ :

- **le champ A** qui indique une adresse IP. Il sert, par exemple, à fournir une adresse IP lorsqu'on va interroger le serveur DNS à propos du nom de domaine 'emill.net'.
- **le champ CNAME** qui indique un nom de domaine (alias).
- **le champ MX** qui indique le nom de domaine des serveurs SMTP autorisés à envoyer et recevoir des e-mails.
- **le champ NS** qui indique l'adresse du serveur DNS primaire et le serveur DNS secondaire.
- **les champs TXT** qui servent à des implémentations spécifiques.

Le réglage correct du serveur DNS est un pré-requis indispensable à l'envoi d'e-mails mais aussi à toute communication sur les réseaux locaux ou distants. Par conséquent, il est en général correctement configuré. Cependant, si vous avez des doutes, vous pouvez entrer le nom de domaine de votre entreprise à l'adresse <http://www.dnsreport.com/> (dans le champ DNS Report). Si un des éléments est affiché en rouge, consultez votre administrateur réseau.

1.5 Résolution et résolution inverse

Lorsque vous entrez l'adresse d'un site Internet (ex. : <http://www.emill.net>) dans votre navigateur, des serveurs DNS vont être interrogés pour **connaître l'adresse IP correspondant au nom de domaine** 'emill.net'. Ce processus s'appelle une résolution.

Le procédé de **résolution inverse** (Reverse DNS) consiste lui à interroger un serveur DNS afin d'**obtenir un nom de domaine à partir d'une adresse IP**. Cela correspond à un des systèmes d'authentification les plus utilisés. Par exemple, le serveur d'AOL qui utilise cette technique va récupérer l'adresse IP de l'émetteur contenue dans l'en-tête de l'e-mail et va demander à des serveurs DNS si un nom de domaine correspond à cette IP. S'il ne trouve aucune correspondance alors il refusera de délivrer le message

2. Le Sender Policy Framework

Le SPF est un **standard ouvert** établissant une norme d'authentification du nom de domaine de l'expéditeur d'un message.

Afin de comprendre son fonctionnement, il est essentiel de savoir que **2 adresses d'email d'expéditeur sont utilisées lorsque vous envoyez un e-mail** (dans 80% des cas, ces 2 adresses sont les mêmes) :

- Le **'Mail From'** ou 'Expéditeur SMTP' ou 'Sender' est l'adresse e-mail utilisée lors de la communication entre le serveur SMTP qui envoie le message et celui qui le reçoit. Elle correspond à l'enveloppe de l'e-mail.
- Le **'From'** ou 'De' est l'adresse e-mail de l'expéditeur qui est indiquée lorsque vous envoyez un e-mail en utilisant votre client mail habituel et qui sera visible par le destinataire. Elle correspond à l'en-tête de l'e-mail.

Le SPF étant une norme qui concerne la communication entre les serveurs SMTP, seule l'adresse e-mail indiquée dans le 'Mail From' sera utilisée.

L'authentification de l'expéditeur se déroule en **2 étapes** :

1. **Le serveur de réception du message récupère le nom de domaine** de l'adresse e-mail indiquée dans le champ 'Mail From'. Par exemple, si l'adresse e-mail est philippe@mail.emilltest.com, le serveur de réception va récupérer le nom de domaine 'mail.emilltest.com'.
2. **Le serveur de réception du message interroge un serveur DNS** pour savoir si ce nom de domaine est autorisé à envoyer des e-mails.

Afin de répondre à ce système, il est donc nécessaire d'ajouter dans les réglages de votre serveur DNS, le nom de domaine des machines autorisées à diffuser des e-mails. La ligne de configuration prendra la forme suivante :

```
emill.net.  TXT  "v=spf1 a:mail.emill.net -all"
```

Nom de domaine Champ TXT du serveur DNS Nom de domaine autorisé à diffuser des e-mails

Pour créer un enregistrement tel que celui-ci, la communauté SPF met à votre disposition un assistant à l'adresse <http://www.openspf.org/wizard.html>.

3. Sender ID

Sender ID est un protocole standard combinant le **Sender Policy Framework** (voir ci-dessus) et le **CallerID** créé par Microsoft. Il a pour objectif d'authentifier le nom de domaine de l'expéditeur d'un e-mail.

Reconnu par l'IETF (Internet Engineering Task Force) qui établit les standards de l'Internet, le Sender ID est une des normes d'authentification les plus utilisées : AOL, Gmail, Live, B2B... Selon Microsoft, **39,2% des e-mails envoyés ont un Sender ID** et 6% des domaines l'ont adopté. Parmi les principaux webmails, Yahoo est un des seuls à ne pas intégrer Sender ID ; sans doute pour privilégier la norme d'authentification qu'ils ont créé, DomainKeys (voir 4).

Le fonctionnement de Sender ID est basé sur le **même système que le SPF** que nous avons étudié en 2^{ème} partie :

1. **Le serveur de réception du message récupère le nom de domaine** de l'expéditeur dans les en-têtes de l'e-mail. A la différence du SPF, le Sender ID ne va pas chercher uniquement le nom de domaine indiqué dans le 'Mail From' mais va aussi parcourir d'autres en-têtes de l'e-mail.
2. **Le serveur de réception va interroger le serveur DNS** du nom de domaine pour savoir si l'adresse IP ou le nom de domaine de l'expéditeur sont autorisés à diffuser des e-mails.

Afin de répondre positivement à la requête du serveur de réception, un champ TXT spécifique doit être ajouté au serveur DNS. Pour implémenter Sender ID, il vous faut suivre **4 étapes** :

1. **Déterminer les adresses IP des machines de votre domaine** susceptibles de diffuser des e-mails. Si un prestataire tierce envoie des e-mails de votre part (solutions d'e-mailing en ASP, hébergeur), vous devez connaître leur nom de domaine (et non les adresses IP des machines à condition que ces prestataires implémentent Sender ID).
2. **Créer l'enregistrement Sender ID** en utilisant l'assistant proposé par Microsoft : <http://www.microsoft.com/mscorp/safety/content/technologies/senderid/wizard/>.
3. **Publier l'enregistrement Sender ID** sur votre DNS. Celui-ci aura la forme suivante :

<code>emill.net. TXT "v=spf2.0 ip4:152.163.225.0 +a:mail.emill.net -all"</code>			
Nom de domaine	Champ TXT du serveur DNS	Adresse IP autorisée à diffuser des e-mails	Nom de domaine autorisé à diffuser des e-mails

4. **Tester l'implémentation de Sender ID** à partir du site <http://senderid.espcoalition.org/>.

Voici quelques ressources complémentaires disponibles en ligne afin d'en savoir plus sur Sender ID et son implémentation :

- Site dédié à Sender ID (en anglais) : <http://www.microsoft.com/mscorp/safety/technologies/senderid/default.aspx>

- Fiche de présentation (en français) :
http://download.microsoft.com/download/d/f/0/df0b1f68-a05e-4949-be0a-26d6787da6af/fr_sidf.pdf
- Standard RFC établi par l'IETF (en anglais - utilisateurs expérimentés) :
<http://www.ietf.org/rfc/rfc4406.txt?number=4406>

4. DomainKeys

DomainKeys est une norme créée par **Yahoo!** qui a pour objectif d'authentifier le nom de domaine de l'expéditeur de l'email mais aussi **l'intégrité du message** afin de s'assurer qu'il n'a pas été modifié lors de son transfert. La poursuite de ce double objectif rend le déploiement de DomainKeys plus complexe et plus gourmand en ressources. C'est la raison pour laquelle seuls **Yahoo et Gmail** supportent ce protocole parmi les webmails et les entreprises sont peu nombreuses à l'avoir intégré.

Notez que Yahoo! travaille actuellement avec d'autres structures (AOL, EarthLink, Microsoft, Sendmail, StrongMail...) afin de **standardiser ce protocole** sous le nom de DomainKeys Identified Mail (DKIM).

Le **fonctionnement de DomainKeys** est le suivant :

1. Le propriétaire du domaine génère une **clé publique et privée**.
2. La clé publique est ajoutée au serveur DNS et les clés privées sont stockées sur les serveurs sur le réseau diffusant des e-mails.
3. Lors de l'envoi d'un e-mail, le serveur d'envoi utilise sa clé privée pour signer électroniquement le message. La signature est ajoutée dans l'en-tête du message.
4. L'e-mail est transféré au serveur de réception correspondant au destinataire du message.
5. Le serveur de réception récupère la signature de l'e-mail et le nom de domaine indiquée dans l'adresse e-mail de l'expéditeur (champs 'From' et 'Sender' de l'en-tête).
6. Le serveur de réception se tourne vers le serveur DNS du domaine de l'expéditeur. Il vérifie que la clé publique du serveur DNS correspond bien à la clé privée de l'e-mail.

Ce processus permet d'authentifier le nom de domaine de l'adresse email de l'expéditeur et, grâce à la signature, de s'assurer que les en-têtes et le contenu n'ont pas été modifié à l'insu de l'expéditeur.

Afin d'implémenter cette méthode d'authentification, vous devez tout d'abord **disposer de serveurs mail (MTA) supportant DomainKeys** pour pouvoir y ajouter la clé privée. Parmi ces serveurs mail on retrouve Sendmail, Qmail, Exchange 2003, Postfix, Etype, XMServer, Eclerity, StrongMail, MDAemon, IronPort, L-Soft... Consultez la documentation de votre serveur mail pour vous assurer qu'il est compatible avec DomainKeys.

Ensuite, vous pouvez **démarrer l'implémentation de DomainKeys** :

- **Générer les clés** : Les serveurs mail cités ci-dessus proposent pour la plupart un outil pour générer les clés privés et publiques. Vous pouvez également consulter le site suivant pour générer vous-mêmes les clés : <http://domainkeys.sourceforge.net/keygen.html>.
- **Ajouter au serveur DNS un champ TXT avec la clé publique**. Il aura la forme suivante :



- **Ajouter au serveur mail la clé privée** (consultez le mode d'emploi de votre serveur mail)

Voici quelques **ressources complémentaires** disponibles en ligne afin d'en savoir plus sur Sender ID et son implémentation :

- Site dédié à DomainKeys : <http://antispam.yahoo.com/domainkeys>
- Assistant d'implémentation pour différents serveurs mail (en anglais) : <http://domainkeys.sourceforge.net/>