Pourquoi DKIM n’est-il pas activé automatiquement ?

E-mail · https://kyzoe.be/fr/docs/pourquoi-dkim-n-est-pas-active-automatiquement/

Pourquoi DKIM ne peut pas toujours être activé automatiquement

Le panneau de contrôle peut toujours générer la clé DKIM, mais il ne peut pas toujours publier lui-même l’enregistrement DNS correspondant. Et sans cette publication, DKIM ne sert à rien. Tout dépend de qui contrôle la zone DNS et le flux de courrier sortant.

1. La zone DNS est gérée en externe

DKIM réside dans le DNS, pas sur le serveur de messagerie. Le panneau de contrôle ne peut écrire des enregistrements que dans les zones qu’il gère lui-même. Si les serveurs de noms de votre domaine pointent vers Cloudflare, vers votre registrar (p. ex. Openprovider, Combell, GoDaddy) ou vers un serveur DNS tiers, Enhance n’y dispose d’aucun droit d’écriture. La clé est créée et affichée, mais vous devez reporter l’enregistrement manuellement.

C’est la raison la plus fréquente. L’hébergement est chez nous, le DNS ne l’est pas.

2. L’e-mail passe par un fournisseur externe

Si votre courrier n’est pas envoyé via nos serveurs, mais par exemple via :

- Microsoft 365 / Exchange Online
- Google Workspace
- Amazon SES
- Mailchimp, Brevo, Mailjet, ActiveCampaign
- un logiciel CRM ou ERP qui envoie lui-même des e-mails

… c’est alors **ce** fournisseur qui signe les e-mails, et non notre serveur. Chaque fournisseur possède sa propre paire de clés et son propre sélecteur (p. ex. `selector1._domainkey` chez Microsoft 365, ou `s1._domainkey` et `s2._domainkey` dans une configuration SES). La clé DKIM

générée par notre panneau de contrôle en est totalement indépendante et ne vérifierait rien sur ces e-mails.

Le panneau ne peut pas deviner quels services externes vous utilisez, quels sélecteurs ils emploient ni quelles clés ils attendent. Ces enregistrements doivent provenir du tableau de bord de ce fournisseur.

3. Flux de courrier mixtes

Dans la pratique, de nombreux domaines envoient des e-mails depuis plusieurs sources à la fois : le formulaire de contact du site via le serveur d'hébergement, la correspondance quotidienne via Microsoft 365 et la newsletter via Mailchimp. Chacune de ces trois sources a besoin de son propre enregistrement DKIM.

Plusieurs enregistrements DKIM côte à côte ne posent aucun problème — tant que les sélecteurs diffèrent. Mais une activation automatique ne peut pas évaluer cette situation et couvrirait tout au plus une des trois sources. Une configuration à moitié en place donne un faux sentiment de sécurité et produit malgré tout `dkim=fail` pour deux des trois flux de courrier.

4. Enregistrements existants et risque de conflit

Certains domaines disposent déjà d'un enregistrement DKIM, issu d'une migration antérieure ou d'un ancien hébergeur. Un écrasement automatique pourrait interrompre des flux de courrier en cours. C'est pourquoi la publication passe volontairement par un contrôle humain.

5. Délégation et limitations du registrar

Certains registrars et panneaux DNS n'acceptent pas les longues valeurs TXT, les tronquent au-delà de 255 caractères ou ne proposent aucune API permettant à un système externe de créer des enregistrements. Même si le panneau de contrôle voulait publier l'enregistrement, il ne le pourrait techniquement pas.

Quand cela se fait automatiquement

DKIM est publié automatiquement lorsque toutes les conditions ci-dessous sont remplies :

- La zone DNS du domaine tourne sur nos serveurs de noms et est gérée dans Enhance ;
- Le courrier sortant du domaine passe par nos serveurs de messagerie ;
- La zone ne contient pas encore d'enregistrement `_domainkey` conflictuel.

Dans tous les autres cas, le panneau génère la clé, mais c’est vous qui publiez l’enregistrement — ou qui le récupérez auprès du fournisseur de messagerie externe.

Règle pratique

> DKIM appartient à l’**expéditeur**, pas à l’**hébergeur**.

Pour chaque flux de courrier, posez-vous la question : *quel serveur envoie réellement cet e-mail sur Internet ?* C’est cette partie qui fournit l’enregistrement DKIM. Si vous envoyez depuis trois systèmes, il vous faut trois enregistrements.